

Panduan Keamanan Linux

By [Rob Tougher](#)

[1. Perkenalan](#)

[2. Mengamankan Mesin Linux](#)

[2.1 Instalasi](#)

[2.2 Setelah Instalasi](#)

[2.3 Forensik Setelah Penyerangan \(tidak ada seorangpun yang sempurna\)](#)

[3. Transmisi yang Aman](#)

[4. Kesimpulan](#)

[a. Referensi](#)

1. Perkenalan

Artikel ini akan menjelaskan langkah-langkah yang saya lakukan untuk mengamankan komputer dan komunikasi data yang terjadi. Jika anda seorang pendukung aktif keamanan komputer, artikel ini akan menjadi sebuah bahan pertimbangan. Jika anda saat ini tidak memiliki pengalaman mengenai keamanan komputer, anda harus membaca agar mendapatkan ide umum mengenai bagaimana mengamankan sebuah mesin Linux. Artikel ini jelas bukanlah sebuah referensi keamanan komputer yang lengkap - saya mempelajari keamanan komputer secara serius, namun tentunya kewaspadaan saya terbatas. Anda harus melihat dan menentukan sendiri apakah artikel ini cukup bagi pengamanan yang anda butuhkan.

2. Mengamankan Mesin Linux

Saya menjalankan Debian di rumah. Saya selalu membiarkannya menyala dan terhubung ke Internet sepanjang waktu. Ada dua alasan mengapa saya ingin menjaga agar komputer ini selalu aman - untuk menyembunyikan data-data saya dari orang-orang yang tidak seharusnya melihat data tersebut, dan untuk menjaga resource komputer saya dari orang-orang yang tidak seharusnya menggunakan resource tersebut. Saya menyimpan hal-hal yang penting pada mesin tersebut - data yang tidak seharusnya dibaca (dan tentunya juga tidak boleh dimodifikasi) oleh orang lain selain saya. Dan saya tidak ingin seorang penyusup bisa menggunakan mesin saya sebagai medan pertahanan untuk menyerang target-target yang lain. Saya akan merasa sangat dipermainkan jika menemukan seseorang sedang menggunakan mesin saya untuk berusaha menyerang mesin yang lain.

2.1 Instalasi

Setelah proses instalasi Linux berakhir, hal pertama yang saya lakukan adalah [mengkonfigurasi iptables](#) pada kernel. Iptables memungkinkan saya untuk memblokir paket-paket yang masuk atau meninggalkan komputer saya. Hal ini penting mengingat saya selalu terhubung ke Internet, sehingga komputer saya selalu terbuka untuk diserang. Mengkonfigurasi iptables bukanlah hal yang menakutkan - anda harus mendownload kode sumber kernel, mengkonfigurasinya dengan benar, dan menginstalnya tanpa mengganggu proses lainnya. Jika anda belum pernah melakukannya, anda harus melihat

[Linux Kernel HOWTO](#), dan mencoba mengcompile kernel anda beberapa kali sebelum mencoba mengkonfigurasi iptables.

Selanjutnya adalah **LIDS** - Linux Intrusion Detection System. LIDS terdiri dari sebuah patch untuk kernel, dan dua buah utilitas - lidsconf dan lidsadm. Tujuan dari sistem ini adalah untuk meningkatkan level keamanan komputer anda dengan membatasi akses menuju file dan proses, dan memberi peringatan jika ada yang mencoba untuk membobol pembatasan ini. Bagian yang terbaik dari LIDS adalah anda bahkan dapat membatasi ijin account root. Hal ini akan mengurangi kekuatan account root, dan membatasi kerusakan yang bisa terjadi jika seorang penyusup mendapatkan hak root. Saya menggunakan LIDS untuk menjaga binary sistem, file-file log di /var/log, dan file-file konfigurasi di /etc. Binary-binary tersebut ditandai sebagai READONLY sehingga tidak ada user, selain root, yang bisa memodifikasi atau menghapusnya. File-file log ditandai sebagai APPEND sehingga program dapat menuliskan data ke dalam file-file di dalam direktori ini, namun tidak dapat menghapus atau mengubah data yang sudah ada.

Hal selanjutnya yang saya lakukan adalah mengurangi jumlah service yang berjalan pada komputer. Makin sedikit service yang berjalan, makin sedikit pula peluang seseorang untuk dapat masuk ke dalam mesin. Distribusi Linux secara default cenderung mengijinkan banyak sekali daemon yang berjalan, yang menurut pendapat saya, ini merupakan hal yang buruk. Saya mematikan telnet, FTP, named, dan semua daemon R*. Pokoknya saya mematikan semuanya sehingga tidak perlu khawatir untuk selalu menjaga service-service tersebut tetap terupdate dengan security fix dan sebagainya. Untuk service-service yang tetap saya jalankan, saya menginstal semua security patch yang ada secepat mungkin. Dan jika terjadi situasi dimana terdapat vulnerability yang telah diketahui oleh publik tanpa tersedia perbaikan terhadapnya, saya akan mematikan service tersebut.

Setelah mengurangi jumlah service yang berjalan pada komputer, saya mengetikkan "netstat -l" untuk melihat socket-socket manakah yang mengawasi koneksi. Saya melakukan ini hanya untuk meyakinkan bahwa saya tidak melewatkan service-service yang tidak dibutuhkan. Setiap kali saya kehilangan sesuatu yang penting, saya mendapatkannya dengan netstat.

2.2 Setelah Instalasi

Setelah menginstal di komputer, saya menjalankan [chkrootkit](#) setiap sekitar satu minggu sekali. Program ini akan memberikan peringatan akan keberadaan rootkit pada komputer. Rootkit adalah satu set tool yang bisa digunakan cracker untuk menyembunyikan jejaknya - kit ini terdiri dari banyak utilitas seperti ps, ifconfig, dan sebagainya yang sudah dimasukkan trojan ke dalamnya. Jika seorang penyusup masuk ke dalam mesin saya dan menginstal rootkit, ia pada dasarnya bisa menggunakan resource komputer saya untuk apapun yang ia inginkan, dan saya hanya dapat mendeteksi keberadaannya jika saya memberi perhatian yang *sangat* besar kepada sistem saya. Anda dapat mendownload dan menganalisa banyak rootkit (hanya untuk dipelajari!) di [packetstorm](#). Satu yang banyak disebut adalah LRK5, yang menghabiskan sekitar setengah halaman web tersebut.

Jika saya mendownload file dari Internet, saya membuat checksums dengan menggunakan [md5sum](#). Kebanyakan situs yang menyediakan file-file yang bisa didownload juga menyertakan checksum, sehingga saya bisa mengecek apakah file yang didownload cocok dengan file yang mereka sediakan. Ini adalah pengecekan yang sederhana, dan membuat hati saya tenang karena saya mendapatkan bit-bit yang benar. Tentunya ada kemungkinan bahwa baik file maupun checksumnya telah dirusakkan, tetapi pada situasi seperti ini website penyedia file tersebut kemungkinan akan segera mengetahuinya, dan memperbaiki permasalahannya.

2.3 Forensik Setelah Penyerangan (tidak ada seorangpun yang sempurna)

Segala macam pengamanan di dunia tidak bisa *menjamin* bahwa mesin anda akan aman dari para craker. Sejujurnya saya mengatakan bahwa saya tidak berpikir komputer saya pernah diserang, namun saya tidak 100% yakin. Pada beberapa bulan pertama saya menggunakan Linux, saya tidak terlalu memperhatikan masalah keamanan - saya hanya berusaha agar sistem operasi ini bisa bekerja. Saya lebih tertarik untuk mempelajari perintah-perintah dasar, dan tidak ingin diganggu oleh hal-hal lain. Sistem saya **terbuka lebar untuk diserang**. Saya mempunyai sebuah mesin VA Linux dengan sebuah sistem RedHat yang berjalan di dalamnya. Mungkin saya telah menjalankan banyak server, dan saya sama sekali tidak mengetahuinya. Malang benar.

Baiklah, jika mesin saya nanti diserang, pertama saya akan segera menuju ke situs utama dari [The Coroner's Toolkit](#). TCT adalah satu set tool yang membantu anda memikirkan apa yang terjadi pada komputer yang diserang. Anda menjalankan tool tersebut, dan duduk santai sambil menunggu tool tersebut mengumpulkan data dari hard disk anda. Saya pribadi belum pernah menggunakan tool tersebut, namun dari apa yang dikatakan website, tool tersebut melakukan pekerjaannya dengan baik. Kesan lain yang saya dapatkan dari website adalah bahwa tool tersebut sangat sulit digunakan bagi para pemula, jadi anda harus banyak membaca dan belajar jika anda tidak memiliki pengalaman dalam menggunakan TCT. Pada akhir halaman utama website tersebut, mereka memiliki beberapa link ke dokumen HOWTO, sehingga sebaiknya anda mulai dari sini.

Saya juga mengunjungi [Honeynet Project](#). Tujuan dari proyek ini adalah untuk melakukan riset mengenai analisis forensik, dan mengumumkan hasilnya kepada publik dengan harapan meningkatkan kesadaran akan keamanan. Mereka mempunyai kontes forensik bulanan, dimana mereka menampilkan informasi mengenai penyerangan yang benar-benar terjadi pada jaringan mereka, dan meminta tulisan mengenai bagaimana menyelidiki penyusupan tersebut. Arsip kontes ini memiliki banyak sekali kiriman-kiriman yang sangat bagus dari para ahli keamanan profesional - saya mempelajari The Coroner's Toolkit dengan melihatnya banyak disebutkan pada penyelidikan-penyelidikan tersebut. Setiap orang yang tertarik pada forensik komputer harus mengunjungi situs ini dan membaca sebanyak mungkin informasi yang bisa ditemukan - cukup untuk menyibukkan anda sementara waktu.

3. Transmisi yang Aman

Secara default, transmisi tidaklah aman. Data anda terbang melewati Internet sehingga dapat dilihat oleh semua orang, dan anda tidak dapat melakukan apapun untuk mencegahnya. Anda dapat menggunakan program traceroute untuk melihat contohnya. Ketikkan "traceroute www.google.com" pada command prompt, dan anda akan mengetahui mesin mana saja yang melihat data yang anda kirimkan ke google saat melakukan pencarian di web.

Saya meyakinkan diri bahwa kapanpun saya login ke sebuah situs, saya harus menggunakan halaman yang aman - https. HTTPS menggunakan SSL, yang mengenkrip data anda ketika dalam perjalanan. Jika saya tidak melakukan hal ini, password saya bisa saja tercium. Sebagai contoh, Yahoo! menyediakan sebuah metode login yang aman ketika mengirimkan nama dan password saya ke servis-servis mereka. Saya mempunyai sebuah account email Yahoo!, dan menggunakan login yang aman ini kapanpun saya mengecek email.

Untuk administrasi secara remote, saya menggunakan [ssh dan scp](#). Kedua program ini merupakan pengganti bagi telnet dan FTP. Mereka mudah diinstal, dan bekerja sebaik program yang mereka gantikan. Setelah terinstal, saya membuka port yang bersangkutan pada konfigurasi iptables saya sehingga saya dapat terhubung ke mesin tersebut dari luar.

Untuk email, saya menggunakan [GnuPG](#) untuk mengenkrip data yang tidak boleh dibaca oleh orang lain. Jika saya ingin mengirimkan informasi yang sensitif kepada seseorang, saya menggunakan public key mereka untuk mengenkripnya. Saya meminta hal yang sama kepada orang lain yang mengirimkan informasi sensitif kepada saya. Public key saya bisa didownload di [web site](#) saya, dan juga tersedia pada banyak [public key server](#). Langkah ini menjamin bahwa hanya saya sajalah orang yang membaca email yang ditujukan ke inbox saya.

4. Kesimpulan

Saya harap anda menikmati artikel ini - saya berusaha menjelaskan se jelas-jelasnya, langkah-langkah yang saya ambil untuk mengamankan komputer dan komunikasi data. Jika anda merasa terdapat kesalahan atau kekurangan pada artikel ini, [beritahu saya](#). Kebijakan pengamanan yang saya ambil masih jauh dari sempurna, dan saya ingin sekali mendengar pengalaman anda.

a. Referensi

Di bawah ini adalah daftar situs yang secara rutin saya kunjungi untuk mendapatkan informasi mengenai berbagai macam topik keamanan komputer:

- **Laporan**
 - [CERT](#)
 - [SecurityFocus Online](#)
- **Exploit** (hanya untuk pembelajaran!)
 - [packetstorm](#)
 - [SecuriTeam](#)

- [Fyodor's Exploit World](#)
- **Forensik**
 - [The Coroner's Toolkit](#)
 - [The Honeynet Project](#)
- **Umum**
 - [Linux Security](#)
 - [packetstorm](#)
 - [www.startplaza.nu](#)
- **Tool**
 - [GnuPG](#)
 - [Insecure.org Top 50](#)
 - [LIDS Project - Secure Linux System](#)
 - [NMAP Port Scanner](#)
 - [SNORT Intrusion Detection System](#)

Rob Tougher

Rob adalah seorang ahli perangkat lunak C++ di daerah NYC. Jika tidak sedang mengetik kode pada platform favoritnya, anda bisa menemukan Rob sedang berjalan-jalan di pantai bersama kekasihnya, Nicole, dan anjing mereka, Halley.



Copyright © 2002, Rob Tougher.

Copying license <http://www.linuxgazette.com/copying.html>

Published in Issue 80 of Linux Gazette, July 2002

Diterjemahkan oleh [Triyan W. Nugroho](#)