Linux Security HOWTO versi Bahasa Indonesia

Kevin Fenzi, kevin@scrye.com & Dave Wreski, dave@nic.com

v.0.9.11, 1 Mei 1998

Dokumen ini merupakan ringkasan umum mengenai isu-isu keamanan yang dihadapi administrator sistem Linux. Ia mencakup beberapa filosofi keamanan umum dan sejumlah contoh khusus tentang bagaimana membuat lebih aman sistem Linux anda dari para penyusup. Juga disertakan pointer ke materi dan program keamanan. **Catatan**: Ini merupakan dokumen versi beta. Perbaikan, kritik yang membangun, penambahan dan koreksi akan diterima dengan senang hati. Silakan layangkan surat umpan balik anda kepada kedua penulis. Pastikan dan sertakan "Linux", "security" atau "HOWTO" dalam baris subyek surat anda untuk menghindari penyaring spam agar surat anda dapat segera mendapat perhatian dari penulis.

Contents

1 Pendahuluan

Dokumen ini mencakup beberapa isu utama keamanan yang mempengaruhi keamanan Linux. Filosofi umum dan sumber daya Internet didiskusikan.

Sejumlah dokumen HOWTO yang lain berkaitan dengan isu keamanan, dan mereka akan diacu bilamana sesuai.

Dokumen ini tidak bertujuan sebagai sebuah dokumen mengenai eksploitasi yang terbaru. Banyak eksploitasi baru terjadi setiap saat. Dokumen ini akan menceritakan di mana informasi terbaru untuk hal tersebut, dan beberapa metode umum untuk mencegah eksploitasi tersebut terjadi.

1.1 Versi Baru Dokumen ini

Versi baru dokumen ini akan diposkan secara periodik ke comp.os.linux.answers. Mereka juga akan ditambahkan ke beberapa site FTP anonim yang mengarsip informasi semacam itu, termasuk : `<ftp://sunsite.unc.edu/pub/Linux/docs/HOWTO>`

Sebagai tambahan, anda dapat memperoleh dokumen ini di homepage Linux Worldwide Web melalui : `<http://sunsite.unc.edu/mdw/linux.html>`

Akhirnya, versi terakhir dokumen ini juga tersedia dalam berbagai format di : `<http://scrye.com/~kevin/lsh/>`

1.2 Umpan balik

Seluruh komentar, laporan kesalahan, tambahan informasi dan kritik dialamatkan ke : *kevin@scrye.com* dan *dave@nic.com*

Catatan: Silakan kirim umpan balik anda kepada kedua penulis. Juga, yakin dan masukkan "Linux" "security" atau "HOWTO" dalam subyek anda untuk menghindari penyaring spam kevin.

1.3 Klaim

Tanggung jawab atas isi dokumen ini tidak dapat diterima. Silakan anda tanggung risiko atas penggunaaan konsep, contoh dan isi lain. Sebagai tambahan, ini merupakan versi awal, dengan berbagai kemungkinan ketidaktepatan dan kesalahan.

Sejumlah contoh dan deskripsi menggunakan tata letak dan setup sistem paket RedHat(tm). Sistem anda mungkin berbeda.

Sejauh yang kami ketahui, hanya program-program yang dalam beberapa hal dapat digunakan atau dievaluasi demi kepentingan personal yang akan dideskripsikan. Kebanyakan program tersedia dengan kode sumber sesuai persyaratan serupa GNU.

1.4 Informasi Hak Cipta

di seluruh salinan. Redistribusi komersil diperbolehkan dan dianjurkan; namun, para penulis mohon diberitahu untuk distribusi demikian.

- Seluruh terjemahan, pekerjaan turunan, atau keseluruhan kerja yang menggunakan dokumen-dokumen Linux HOWTO harus dilingkupi oleh pernyataan hak cipta ini. Artinya, anda tidak boleh memproduksi pekerjaan turunan dari sebuah HOWTO dan menambahkan hambatan pada distribusinya. Perkecualian untuk aturan ini dapat diberikan untuk kondisi tertentu; silakan hubungi koordinator Linux HOWTO di alamat di bawah ini.
- Jika anda memiliki pertanyaan, silakan hubungi Tim Bynum, koordinator Linux HOWTO di *linux-howto@sunsite.unc.edu*

2 Gambaran Umum

Dokumen ini akan berusaha menjelaskan beberapa prosedur dan software-software yang biasa digunakan untuk membantu membuat lebih aman sistem Linux anda. Mendiskusikan konsep-konsep dasar dahulu adalah penting, dan memberi landasan sebelum kita memulai.

2.1 Mengapa kita perlu keamanan ?

Dalam dunia komunikasi data global yang selalu berubah, hubungan Internet yang murah, dan cepatnya perkembangan software, keamanan menjadi isu yang semakin penting. Keamanan saat ini menjadi suatu kebutuhan dasar karena komputasi global tidak aman. Sebagai contoh, dengan berpindahnya data anda dari titik A ke titik B di Internet, ia mungkin melalui beberapa titik lain selama perjalanan, membuka kesempatan bagi orang lain untuk memotongnya, atau pun merubah data anda. Bahkan pengguna lain pada sistem anda dapat merubah data anda ke sesuatu yang tidak anda inginkan. Akses yang tidak diijinkan ke dalam sistem anda mungkin dapat diperoleh oleh penyusup, juga dikenal sebagai "cracker", yang kemudian menggunakan pengetahuannya untuk berpura-pura sebagai anda, mencuri informasi dari anda, atau bahkan menolak akses anda ke sumber daya anda sendiri. Jika anda masih bertanya-tanya mengenai perbedaan antara "Hacker" dan "Cracker", silakan lihat dokumen Eric Raymond, "How to Become A Hacker", tersedia di `<http://sagan.earthspace.net/~esr/faqs/hacker-howto.html>`.

2.2 Seberapa amankah aman ?

Pertama, ketahuilah bahwa tidak ada sistem komputer yang dapat diamankan secara total. Yang dapat anda lakukan adalah membuat kesulitan bagi orang untuk mengganggu sistem anda. Bagi kebanyakan pengguna Linux, tidak terlalu banyak yang diperlukan untuk menjaga sistem anda dari cracker. Sedang bagi pengguna Linux profil tinggi (bank, perusahaan telekomunikasi, dsb), banyak lagi pekerjaan dibutuhkan.

Faktor lain yang perlu diperhatikan adalah semakin aman sistem anda semakin intrusif keamanan anda. Anda perlu menentukan tindakan yang membuat sistem anda masih dapat dipakai dan juga aman demi kebutuhan anda. Sebagai contoh, anda dapat memaksa setiap orang yang mendial ke sistem anda untuk menggunakan modem call back untuk memanggil mereka kembali di rumah mereka. Ini lebih aman, tetapi jika seseorang tidak berada di rumah, maka akan menjadi sulit bagi mereka untuk login. Anda dapat juga mensetup sistem Linux anda dengan tanpa jaringan atau hubungan ke Internet, tetapi ini membuatnya sulit untuk menelusuri web.

Jika anda adalah site yang berukuran besar hingga menengah, anda perlu menetapkan suatu Kebijakan Keamanan (Security Policy) yang berisikan tingkat keamanan yang dibutuhkan oleh site anda dan auditing apa yang digunakan untuk memeriksanya. Anda dapat menemukan contoh kebijakan keamanan terkenal di `<http://ds.internic.net/rfc/rfc2196.txt>`. Belum lama ini telah diperbaharui, dan berisikan kerangka kerja yang baik bagi penetapan kebijakan keamanan perusahaan anda.

2.3 Apa yang ingin anda lindungi ?

Sebelum anda berusaha mengamankan sistem anda, anda perlu menentukan tingkat ancaman yang anda hadapi, risiko apa yang perlu atau tidak perlu anda ambil, dan seberapa rentan sistem anda sebagai hasilnya. Anda perlu menganalisis sistem anda untuk mengetahui apa yang anda lindungi, mengapa anda melindunginya, nilai apa yang dimilikinya, dan siapa yang memiliki tanggung jawab terhadap data dan aset lain anda.

- Risiko adalah kemungkinan seorang penyusup berhasil dalam usahanya mengakses komputer anda. Dapatkah penyusup membaca, menulis, atau mengeksekusi program-program yang dapat menyebabkan kerusakan ? Dapatkah mereka menghapus data kritis ? Mencegah anda atau perusahaan anda menyelesaikan pekerjaan penting ? Jangan lupa, seseorang yang memperoleh akses ke rekening anda, atau sistem anda, dapat pula berpura-pura sebagai anda.

  Sebagai tambahan, memiliki satu rekening yang tidak aman di sistem anda dapat menyebabkan seluruh jaringan anda terganggu. Dengan adanya pemakai tunggal yang dibolehkan login menggunakan file rhost, atau dibolehkan menggunakan pelayanan yang tidak aman, seperti tftp, anda menghadapi risiko seorang penyusup menggunakannya untuk masuk ke pintu anda (`get his foot in the door`). Sekali seorang penyusup memiliki rekening pemakai di sistem anda, atau sistem orang lain, akan dapat digunakan untuk memperoleh akses ke sistem lain atau rekening lain.

- Ancaman biasanya berasal dari seseorang dengan motivasi untuk memperoleh akses yang tidak diijinkan ke jaringan atau komputer anda. Anda perlu memutuskan siapa yang anda percayai untuk memiliki akses ke sistem anda, dan ancaman apa yang dapat muncul.

  Terdapat beberapa macam penyusup, dan penting mengeahui beragam karakteristiknya saat mengamankan sistem anda.

  – The Curious (Si Ingin Tahu) - tipe penyusup ini pada dasarnya tertarik menemukan jenis sistem dan data yang anda miliki.
  – The Malicious (Si Perusak) - tipe penyusup ini berusaha untuk merusak sistem anda, atau merubah web page anda, atau sebaliknya membuat waktu dan uang anda kembali pulih.
  – The High-Profile Intruder (Si Profil Tinggi) - tipe penyusup ini berusaha menggunakan sistem anda untuk memperoleh popularitas dan ketenaran. Dia mungkin menggunakan sistem profil tinggi anda untuk mengiklankan kemampuannya.
  – The Competition (Si Pesaing) - tipe penyusup ini tertarik pada data yang anda miliki dalam sistem anda. Ia mungkin seseorang yang beranggapan bahwa anda memiliki sesuatu yang dapat menguntungkannya secara keuangan atau sebaliknya.

- Kerentanan menggambarkan seberapa terlindung komputer anda dari jaringan lain, dan potensi seseorang memperoleh akses yang tidak diijinkan.

Hal-hal apa yang dipertaruhkan bila seseorang masuk ke sistem anda? Tentu saja perhatian pemakai rumahan PPP dinamis akan berbeda dengan perusahaan yang menghubungkan mesinnya ke Internet, atau jaringan besar lain.

Berapa banyak waktu yang diperlukan untuk mengembalikan/menciptakan data yang hilang? Investasi awal saat ini dapat menghemat puluhan kali lebih banyak jika kemudian anda perlu menciptakan kembali data yang hilang. Sudahkah anda mengkaji strategi backup anda, dan memastikan data anda benar?

2.4 Membangun Kebijakan Keamanan

Ciptakan kebijakan umum dan sederhana bagi sistem anda yang dapat dipahami dan diikuti oleh pemakai anda. Ia harus dapat melindungi data yang anda simpan, juga privasi pemakai. Beberapa hal yang perlu dipertimbangkan adalah siapa yang meiliki akses ke sistem (Dapatkah teman saya menggunakan rekening saya?), siapa yang diijinkan untuk menginstal software pada sistem, siapa memiliki data apa, perbaikan bencana, dan penggunaan yang tepat sistem.

Kebijakan keamanan yang diterima umum dimulai dengan frase :

```
"Hal-hal apa yang tidak dijinkan adalah dilarang"
```

Artinya, kecuali anda memberi akses suatu pelayanan kepada pemakai, maka pemakai tidak boleh menggunakan pelayanan tersebut hingga anda memberi akses. Pastikan kebijakan berlaku untuk rekening pemakai reguler anda. Mengatakan, "Ah, saya tidak dapat memecahkan masalah permisi ini, saya akan lakukannya sebagai root" dapat menyebabkan lubang keamanan yang sangat jelas, dan bahkan yang belum tereksploitasi.

2.5 Alat-alat untuk mengamankan site anda

Dokumen ini akan mendiskusikan berbagai alat yang dapat mengamankan aset yang telah anda kerjakan dengan keras: mesin lokal anda, data, pemakai, jaringan, bahkan reputasi anda. Apa yang akan terjadi pada reputasi anda jika seorang penyusup menghapus data beberapa pemakai anda? Atau merubah web page anda ? Atau meneberbitkan rencana proyek perusahaan anda untuk empat bulan berikut ? Jika anda merencanakan instalasi jaringan, ada berbagai faktor yang harus anda perhatikan sebelum menambahkan sebuah mesin tunggal ke jaringan anda.

Bahkan jika anda memiliki sebuah rekening PPP dialup, atau site kecil, tidaklah berarti penyusup tidak tertarik kepada sistem anda. Site besar dan profil tinggi bukanlah target satu-satunya, banyak penyusup hanya ingin mengeksploitasi site sebanyak mungkin, tanpa memandang ukurannya. Tambahan lagi, mereka mungkin menggunakan lubang keamanan di site anda untuk memperoleh akses ke site lain yang terhubung dengan site anda.

Para penyusup memiliki banyak waktu, dan dapat memperkirakan bagaimana anda menyembunyikan sistem anda dengan hanya mencoba seluruh kemungkinan. Terdapat pula beberapa alasan seorang penyusup tertarik pada sistem anda, yang akan kita diskusikan nanti.

2.5.1 Keamanan Host

Mungkin area yang paling banyak mendapat perhatian dalam keamanan adalah berkaitan dengan keamanan berbasis host. Hal ini biasanya melibatkan pemastian bahwa sistem anda aman, dan berharap setiap orang di jaringan anda melakukan hal yang sama. Memiliki password yang baik, mengamankan pelayanan jaringan lokal host anda, menyimpan catatan akuntansi yang baik, dan memperbaharui program dengan eksploitasi keamanan yang diketahui adalah beberapa hal yang menjadi tanggung jawab administrator keamanan lokal, ini dapat merupakan tugas yang mengerikan pada saat jaringan anda bertambah besar.

2.5.2 Keamanan Jaringan Anda

Keamanan jaringan juga merupakan suatu keharusan sebagaimana keamanan host lokal. Dengan sistem tunggal anda, atau jaringan komputasi terdistribusi, Internet, atau ratusan, bila tidak ribuan atau lebih komputer pada jaringan yang sama, anda tidak dapat mengandalkan setiap sistem aman. Memastikan pemakai yang dijinkan hanyalah satu-satunya yang menggunakan sumber daya jaringan anda, membangun firewall, menggunakan enkripsi yang baik, dan meyakinkan tidak ada mesin yang buruk, atau tidak aman pada jaringan anda adalah tugas administrator keamanan jaringan.

Dokumen ini akan mendiskusikan beberapa teknik yang digunakan untuk mengamankan site anda, dan berharap dapat menunjukkan kepada anda cara-cara mencegah penyusup memperoleh akses ke apa yang ingin anda lindungi.

2.5.3 Keamanan Melalui Penyembunyian

Salah satu tipe keamanan yang perlu didiskusikan adalah "keamanan melalui penyembunyian". Artinya dengan melakukan sesuatu seperti merubah nama login "root" ke "toor", sebagai contoh, untuk mencoba dan membingungkan seseorang masuk ke sistem anda sebagai root adalah perkiraan yang salah tentang keamanan, dan akan mengakibatkan konsekuensi yang tidak mengenakkan. Hampir pasti bahwa penyerang sistem akan secara cepat mengetahui keamanan kosong semacam itu. Hanya karena anda memiliki site kecil atau secara relatif rendah profil tidaklah berarti penyusup tidak akan tertarik pada apa yang anda miliki. Kita akan mendiskusikan apa yang anda lindungi pada bagian selanjutnya.

2.6 Organisasi Dokumen Ini

Dokumen ini telah dibagi ke dalam sejumlah bagian. Mereka mencakup berbagai macam isu keamanan yang luas. Yang pertama, keamanan fisik, mencakup bagaimana anda butuh melindungi mesin anda dari gangguan. Yang kedua mendeskripsikan bagaimana melindungi sistem anda dari gangguan pemakai lokal. Yang ketiga, keamanan file dan sistem file menunjukkan bagaimana mensetup file sistem anda dan permisi file. Berikutnya, keamanan password dan enkripsi mendiskusikan bagaimana menggunakan enkripsi untuk lebih mengamankan mesin dan jaringan anda. Keamanan kernel mendiskusikan pilihan kernel apa yang perlu diset atau perlu diperhatikan untuk memperoleh mesin yang lebih aman. Keamanan jaringan, mendeskripsikan bagaimana lebih mengamankan sistem Linux anda dari serangan jaringan. Persiapan keamanan mendiskusikan bagaimana mempersiapkan mesin anda sebelum membuatnya on-line. Berikutnya mendiskusikan apa yang perlu dilakukan ketika anda mendeteksi adanya bahaya pada sistem anda atau yang telah terjadi. Kemudian link ke sumber keamanan lain disebutkan, dan akhirnya beberapa pertanyaan dan jawaban dan kata-kata penutupan.

Dua hal utama yang perlu diperhatikan ketika membaca dokumen ini adalah :

- Perhatikan sistem anda. Periksa log sistem seperti /var/log/messages dan perhatikan sistem anda, dan

- Buatlah sistem anda selalu "up to date" dengan memastikan bahwa anda telah menginstal versi terbaru software dan telah mengupgrade setiap ada pemberitahuan keamanan. Dengan melakukan hal-hal ini akan menjadikan sistem anda lebih aman.

3 Keamanan Fisik

Lapis pertama keamanan yang perlu anda perhatikan adalah keamanan fisik sistem komputer anda. Siapa yang memiliki akses fisik ke mesin anda? Perlukah mereka? Dapatkah anda melindungi mesin anda dari gangguan mereka? Perlukah anda?

Seberapa banyak keamanan fisik yang anda perlukan pada sistem anda sangat tergantung pada situasi anda, dan/atau anggaran.

Jika anda adalah pemakai rumahan, anda mungkin tidak perlu banyak (meskipun anda mungkin butuh untuk melindungi mesin anda dari gangguan anak-anak atau kerabat lainnya). Jika anda dalam lingkungan lab, anda perlu lebih, tetapi pemakai masih dapat melakukan pekerjaan pada sistem. Bagian-bagian berikut akan membantu. Jika anda ada dalam kantor, anda mungkin atau tidak butuh untuk mengamankan mesin anda pada saat selesai atau pada saat anda pergi. Pada beberapa perusahaan, meninggalkan konsol tidak aman adalah suatu pelanggaran.

Metode-metode keamanan fisik yang jelas seperti kunci pintu, kabel, kabinet yang terkunci, dan video pengawasan adalah ide yang baik, tetapi di luar cakupan dokumen ini. :)

3.1 Kunci Komputer

Banyak case PC modern menyertakan atribut "penguncian". Biasanya ini adalah soket pada bagian depan case yang memungkinkan anda memutar kunci yang disertakan ke posisi terkunci atau tidak. Kunci case dapat membantu mencegah seseorang mencuri PC anda, atau membuka case yang secara langsung memanipulasi/mencuri hardware anda. Mereka dapat pula suatu saat mencegah seseorang mereboot komputer anda menggunakan floppy atau hardware mereka.

Kunci case ini melakukan hal-hal yang berbeda sesuai dengan dukungan dalam motherboard dan bagaimana case dirancang. Pada banyak PC mereka membuatnya sehingga anda harus menghancurkan case untuk membukanya. Pada yang lain, mereka membuatnya sehingga tidak memungkinkan anda memasang keyboard dan mouse baru. Periksa instruksi motherboard atau case anda untuk informasi lebih lanjut. Alat ini sewaktu-waktu dapat sangat berguna, meskipun kuncinya biasanya memiliki kualitas rendah dan dapat secara mudah dibuka oleh penyerang dengan locksmithing.

Beberapa case (kebanyakan SPARC dan MAC) memiliki "dongle" di belakang sehingga jika anda menaruh kabel sepanjangnya, para penyerang harus memotong kabel atau membongkar case untuk masuk. Dengan hanya menaruh padlock atau combo lock melaluinya dapat mencegah seseorang mencuri mesin anda.

3.2 Keamanan BIOS

BIOS adalah software tingkat terendah yang mengkonfigurasi atau memanipulasi hardware berbasis x86 anda. LILO dan metode boot Linux lainnya mengakses BIOS untuk menentukan bagaimana memboot mesin Linux anda. Hardware lain yang menjalankan Linux memiliki software yang serupa (OpenFirmware pada

MAC dan SUN, SUN boot prom, dsb). Anda dapat menggunakan BIOS anda untuk mencegah penyerang mereboot ulang mesin anda dan memanipulasi sistem Linux anda.

Pada Linux/x86 banyak PC BIOS membolehkan anda menset password boot. Hal ini tidak memberikan banyak keamanan (BIOS dapat direset, atau dihapus jika seseorang dapat masuk ke case), namun mungkin dapat berguna (misalnya hal ini memerlukan waktu dan meninggalkan bekas).

Banyak BIOS x86 juga membolehkan anda menspesifikasikan beragam setting keamanan yang baik lainnya. Periksa manual BIOS anda atau lihat saat anda boot up. Beberapa contoh adalah : tidak membolehkan booting dari floppy drive dan password untuk mengakses beberapa atribut BIOS.

Pada Linux/SPARC, SPARC EEPROM anda dapat diset agar memerlukan password boot-up. Ini mungkin akan memperlambat penyerang.

Catatan: Jika anda memiliki mesin server, dan anda mensetup password boot, mesin anda tidak akan memboot secara otomatis. Ingat bahwa anda perlu memasukkan password pada saat terjadi suatu kegagalan daya. ;(

3.3 Keamanan Boot Loader

Berbagai boot loader Linux dapat juga memasang password boot. Dengan lilo, lihat pada setting "restricted" dan "password". "password" memungkinkan anda mensetup password bootup. "restricted" akan membiarkan mesin boot kecuali seseorang menspesifikasikan option di lilo prompt (seperti 'single').

Ingatlah ketika menset seluruh password ini bahwa anda perlu mengingat mereka. :(Juga ingat bahwa password ini akan memperlambat penyerang yang gigih. Hal ini tidak akan mencegah seseorang membooting dari floppy, dan melakukan mount partisi root anda. Jika anda menggunakan keamanan bersama dengan boot loader, anda perlu juga mematikan booting dari floppy di BIOS anda, dan juga memberi password protecting BIOS komputer anda.

Jika seseorang memiliki informasi keamanan bagi boot loader lain, kami sangat ingin mendengarnya. (grub, silo, milo, linload, dsb).

Catatan: Jika anda memiliki mesin server, dan anda mensetup password boot, mesin anda tidak akan memboot secara otomatis. Ingat bahwa anda perlu memasukkan password pada saat terjadi suatu kegagalan daya. ;(

3.4 xlock dan vlock

Jika anda sering meninggalkan mesin anda, adalah baik untuk dapat mengunci konsol anda sehingga tidak seorang pun dapat mengganggu atau melihat kerja anda. Dua buah program yang melakukannya adalah : xlock dan vlock.

Xlock adalah sebuah pengunci tampilan X. Ia seharusnya disertakan di setiap distribusi Linux yang mendukung X. Periksa man pagenya untuk pilihan lebih banyak, tetapi secara umum anda dapat menjalankan xlock dari sembarang xterm di konsol anda dan ia akan mengunci tampilan dan membutuhkan password anda untuk membukanya.

vlock adalah program kecil sederhana yang memungkinkan anda mengunci beberapa atau seluruh konsol virtual pada mesin Linux anda. Anda dapat mengunci hanya satu tempat kerja anda atau seluruhnya. Jika anda hanya mengunci satu, orang lain dapat menggunakan konsol, mereka hanya tidak dapat menggunakan vty anda hingga anda membukanya. vlock diedarkan dengan RedHat Linux, tetapi sistem anda mungkin berbeda.

Tentu saja mengunci konsol anda akan mencegah seseorang mengganggu pekerjaan anda, tetapi tidak mencegah mereka mereboot mesin anda atau merusak pekerjaan anda. Hal ini juga tidak mencegah mereka mengakses mesin anda dari mesin lain dalam jaringan dan menyebabkan masalah.

3.5 Mendeteksi Gangguan Keamanan Fisik

Hal pertama yang harus diperhatikan adalah pada saat mesin ada direboot. Oleh karena Linux adalah Sistem Operasi (SO) yang kuat (robust) dan stabil, saat bagi mesin anda untuk reboot adalah ketika anda mengupgrade SO, penukaran hardware, dan sejenisnya. Jika mesin anda direboot tanpa anda lakukan, kesukaran akan muncul. Banyak cara mesin anda dapat diganggu tanpa membutuhkan penyusup untuk reboot atau mematikan mesin anda.

Periksa tanda-tanda gangguan pada case dan daerah komputer. Meskipun banyak penyusup membersihkan jejaknya dari log, namun sebaiknya anda memeriksa keseluruhannya dan mencatat kejanggalan.

Beberapa hal untuk diperiksa pada log anda :

- Log pendek atau tidak lengkap.
- Log yang berisikan waktu yang aneh.
- Log dengan permisi atau kepemilikan yang tidak tepat.
- Catatan pelayanan reboot atau restart.
- Log yang hilang.
- Masukan su atau login dari tempat yang janggal

Kita akan mendiskusikan data sistem log kemudian.

4 Keamanan Lokal

Hal berikutnya yang perlu dilihat adalah keamanan sistem anda menghadapi serangan pemakai lokal. Apakah kita baru saja menyebut "pemakai lokal"? ya.

Memperoleh akses ke pemakai lokal adalah salah satu hal yang diusahakan penyusup, pada saat berusaha mengeksploitasi rekening root. Dengan kurangnya keamanan lokal, mereka lalu dapat meng"upgrade" akses pemakai normal mereka ke akses root menggunakan berbagai bug atau setup pelayanan lokal yang tidak baik. Jika anda memastikan keamanan lokal anda ketat, maka penyusup akan perlu melompati rintangan lain.

Para pemakai lokal dapat pula menyebabkan banyak kerusakan terhadap sistem anda meski (khususnya) jika mereka benar-benar siapa yang mereka katakan. Dengan memberikan rekening kepada orang-orang yang tidak anda kenal atau tidak memiliki kontak informasi adalah sebuah ide yang buruk.

4.1 Membuat Rekening Baru

Anda perlu memastikan untuk memberikan rekening pemakai hanya sesuai dengan kebutuhan untuk menyelesaikan tugas mereka. Jika anda memberikan anak anda (usia 10) sebuah rekening, anda mungkin ingin mereka hanya dapat mengakses pengolah kata atau program gambar, tetapi tidak dapat menghapus data yang bukan miliknya.

Beberapa aturan yang baik ketika membolehkan orang lain berhak mengakses mesin Linux anda :

- Beri mereka fasilitas minimal yang diperlukan.
- Hati-hati terhadap saat/dari mana mereka login, atau tempat seharusnya mereka login.
- Pastikan dan hapus rekening mereka ketika mereka tidak lagi membutuhkan akses.

Banyak rekening pemakai lokal digunakan dalam gangguan keamanan adalah yang tidak pernah digunakan selama berbulan-bulan atau bertahun-tahun. Karena tidak ada yang menggunakannya mereka menjadi alat penyerangan yang ideal.

4.2 Keamanan Root

Rekening yang paling dicari di mesin anda adalah rekening superuser. Rekening ini memiliki otoritas atas seluruh mesin, yang mungkin juga mencakup otoritas atas mesin lain yang ada di jaringan. Ingatlah bahwa anda hanya perlu menggunakan rekening root untuk tugas tertentu yang singkat dan gunakanlah rekening pemakai normal untuk hal lainnya. Menggunakan rekening root sepanjang waktu adalah ide yang sangat sangat sangat buruk.

Beberapa trik untuk menghindari pengacauan komputer anda sebagai root:

- Ketika melakukan perintah yang kompleks, cobalah dalam cara yang tidak merusak dulu...terutama perintah yang menggunakan globbing: contoh, anda ingin melakukan "rm foo*.bak", pertama coba dulu: "ls foo*.bak" dan pastikan anda ingin menghapus file-file yang anda pikirkan. Menggunakan echo sebagai pengganti perintah merusak terkadang juga dapat dilakukan.
- Beberapa orang merasa terbantu ketika melakukan "touch /-i" pada sistem mereka. Hal ini akan membuat perintah-perintah seperti : "rm -fr *" menanyakan apakah anda benar-benar ingin menghapus seluruh file. (Shell anda menguraikan "-i" dulu, dan memberlakukannya sebagai option -i ke rm). Hal ini tidak akan membantu terhadap pernyataan rm yang tidak memiliki * di dalamnya. ;(
- Hanya menjadi root ketika melakukan tugas tunggal tertentu. Jika anda berusaha mengetahui bagaimana melakukan sesuatu, kembali ke shell pemakai normal hingga anda yakin apa yang perlu dilakukan oleh root.
- Jalur perintah untuk pemakai root sangat penting. Jalur perintah, atau variabel lingkungan PATH mendefinisikan lokal yang dicari shell untuk program. Cobalah dan batasi jalur perintah bagi pemakai root sedapat mungkin, dan jangan pernah menggunakan '.', yang berarti 'direktori saat ini', dalam pernyataan PATH anda. Sebagai tambahan, jangan pernah menaruh direktori yang dapat ditulis pada jalur pencarian anda, karena hal ini memungkinkan penyerang memodifikasi atau menaruh file biner dalam jalur pencarian anda, yang memungkinkan mereka menjadi root ketika anda menjalankan perintah tersebut.

- Jangan pernah menggunakan seperangkat utilitas rlogin/rsh/rexec (disebut utilitas r) sebagai root. Mereka menjadi sasaran banyak serangan, dan sangat berbahaya bila dijalankan sebagai root. Jangan membuat file .rhosts untuk root.

- File /etc/securetty berisikan daftar terminal-terminal tempat root dapat login. Secara baku (pada RedHat Linux) diset hanya pada konsol virtual lokal (vty). Berhati-hatilah saat menambahkan yang lain ke file ini. Anda seharusnya login dari jarak jauh sebagai pemakai biasa dan kemudian 'su' jika anda butuh (mudah-mudahan melalui ssh atau saluran terenkripsi lain), sehingga tidak perlu untuk login secara langsung sebagai root.

- Selalu perlahan dan berhati-hati ketika menjadi root. Tindakan anda dapat mempengaruhi banyak hal. Pikir sebelum anda mengetik!

Jika anda benar-benar butuh untuk mengijinkan seseorang (semoga sangat dapat dipercaya) untuk memiliki akses superuser pada mesin anda, terdapat beberapa alat yang dapat membantu. Sudo memungkinkan pemakai menggunakan password mereka untuk mengakses sejumlah perintah terbatas sebagai root. Hal ini akan memungkinkan anda untuk, sebagai contoh, mengijinkan pemakai untuk mengeluarkan dan melakukan mount media removable pada sistem Linux anda, tetapi tidak memiliki kewenangan root lainnya. Sudo juga mencatat usaha yang berhasil dan gagal, memungkinkan anda untuk melacak siapa yang menggunakan perintah apa untuk melakukan hal apa. Untuk alasan ini sudo bekerja dengan baik bahkan di tempat banyak orang memiliki akses root, tetapi gunakan sudo sehingga anda dapat melacak perubahan-perubahan yang terjadi.

Meskipun sudo dapat digunakan untuk memberi kewenangan khusus bagi pemakai untuk tugas khusus, ia juga memiliki beberapa kelemahan. Ia seharusnya digunakan untuk sejumlah tugas tertentu, seperti memulai kembali server, atau menambahkan pemakai baru. Program-program yang memberikan `shell escape` akan memberi akses pemakai root. Ini mencakup kebanyakan editor, sebagai contoh. Juga, program seperti /bin/cat dapat digunakan untuk menulisi file, yang dapat menyebabkan root tereksploitasi. Pertimbangkan sudo sebagai cara bagi akuntabilitas, dan jangan mengharapkannya untuk mengganti pemakai root yang juga aman.

5 Keamanan File dan Sistem File

Beberapa menit persiapan dan perencanaan sebelum menaruh sistem anda online dapat membantu melindungi sistem anda, dan data yang disimpan.

- Tidak ada alasan bagi direktori home pemakai agar memungkinkan menjalankan program SUID/SGID dari sana. Gunakan opsi "nosuid" dalam /etc/fstab untuk partisi yang dapat ditulis oleh orang selain root. Anda mungkin ingin menggunakan "nodev" dan "noexec" di partisi home pemakai, juga di /var, yang melarang eksekusi program, dan penciptaan device karakter atau blok, yang sebenarnya tidak perlu.

- Jika anda mengekspor sistem file menggunakan NFS, pastikan mengkonfigurasi /etc/exports dengan akses yang seketat mungkin. Artinya tidak menggunakan wildcard, tidak membolehkan root akses menulis, dan melakukan mount read-only jika mungkin.

- Konfigurasi umask penciptaan file pemakai anda seketat mungkin. Setting yang biasa digunakan adalah 022, 033, dan yang paling ketat adalah 077, dan ditambahkan ke /etc/profile.

- Set limit sistem file. Anda dapat mengendalikan limit tiap pemakai menggunakan module PAM dan /etc/pam.d/limits.conf. Sebagai contoh, limit untuk kelompok "users" mungkin tampak sebagai berikut :

```
@users     hard  core    0
@users     hard  nproc   50
@users     hard  rss     5000
```

  Perintah ini berarti melarang penciptaan file core, membatasi jumlah proses hingga 50, dan membatasi penggunaan memori tiap user hingga 5M.

- File /var/log/wtmp dan /var/run/utmp berisi catatan login seluruh pemakai sistem anda. Integritasnya harus dipelihara karena dapat digunakan untuk menentukan kapan dan dari mana seorang pemakai (atau penyusup potensial) memasuki sistem anda. File-file ini harus memiliki permisi 644, tanpa mempengaruhi operasi sistem normal.

- Bit immutable dapat digunakan untuk mencegah penghapusan atau penimpahan sebuah file yang harus dilindungi tanpa sengaja. Juga dapat mencegah seseorang menciptakan link simbolik ke file ini, yang telah merupakan sumber penyerangan melibatkan penghapusan /etc/passwd atau /etc/shadow. Lihat man page chattr(1) untuk informasi bit immutable.

- File-file SUID dan SGID pada sistem anda adalah risiko keamanan potensial, dan harus diawasi dengan baik. Oleh karena program-program ini memberi ijin khusus bagi pemakai yang mengeksekusinya, maka perlu dipastikan bahwa program yang tidak aman tidak diinstal. Trik favorit cracker adalah mengeksploitasi program SUID "root", lalu meninggalkan program SUID sebagai backdoor untuk masuk di saat lain, meski lubang yang asli telah ditutup.

  Carilah seluruh program SUID/SGID di sistem anda, dan catatlah, sehingga anda mengerti setiap perubahan yang dapat mengindikasikan penyusup potensial. Gunakan perintah berikut untuk mencari seluruh program SUID/SGID di sistem anda:

```
root#  find / -type f \( -perm -04000 -o -perm -02000 \)
```

  Anda dapat menghapus ijin SUID atau SGID pada program yang dicurigai menggunakan chmod(1), lalu rubah kembali jika anda rasa perlu.

- File-file world-writable, utamanya file sistem, dapat menjadi lubang keamanan jika seorang cracker memperoleh akses ke sistem anda dan memodifikasinya. Selain itu direktori world-writable berbahaya, karena memungkinkan cracker menambah atau menghapus file sesuai keinginannya. Untuk mencari seluruh file world-writable di sistem anda, gunakan perintah berikut:

```
root# find / -perm -2 -print
```

  dan pastikan anda paham mengapa file tersebut world-writable. Dalam operasi normal, terdapat beberapa file writable, termasuk beberapa dari /dev, dan link simbolik.

- File-file yang tidak ada pemiliknya juga dapat menjadi indikasi penyusup telah mengakses sistem anda. Anda dapat menemukan file-file di sistem anda yang tidak memiliki pemilik, atau milik suatu kelompok dengan perintah :

```
root# find / -nouser -o -nogroup -print
```

- Mencari file .rhosts seharusnya menjadi bagian tugas reguler anda sebagai sistem administrator, karena file ini tidak diijinkan ada di sistem anda. Ingat, cracker hanya perlu satu rekening tidak aman untuk secara potensial memperolah akses ke seluruh jaringan anda. Anda dapat melihat seluruh file .rhosts di sistem anda dengan perintah :

```
root# find /home -name .rhosts -print
```

- Akhirnya, sebelum merubah permisi di sembarang sistem file, pastikan anda paham apa yang anda lakukan. Jangan pernah merubah permisi suatu file hanya karena ini tampaknya merupakan cara termudah menyelesaikan sesuatu. Selalu tentukan mengapa file memiliki permisi tersebut sebelum merubahnya.

5.1 Setting Umask

Perintah umask dapat digunakan untuk menentukan mode penciptaan file baku di sistem anda. Ia merupakan komplemen oktal mode file yang diinginkan. Jika file diciptakan tanpa mengindahkan setting permisi, pemakai secara tidak sengaja dapat memberi permisi membaca atau menulis kepada seseorang yang tidak seharusnya memiliki permisi ini. Umumnya setting umask mencakup 022, 027, dan 077, yang paling terbatas. Normalnya umask diset dalam /etc/profile, sehingga berlaku untuk semua pemakai sistem. Sebagai contoh, anda mungkin memiliki sebuah baris yang tampak seperti berikut:

```
# Set the user's default umask
umask 033
```

Pastikan untuk membuat umask root 077, yang akan meniadakan permisi membaca, menulis, dan mengeksekusi bagi pemakai lain, kecuali dirubah secara eksplisit menggunakan chmod(1).

Jika anda menggunakan RedHat, dan mengikuti skema penciptaan ID pemakai dan kelompok (User Private Groups), hanya perlu menggunakan 002 sebagai umask. Hal ini disebabkan kenyataan bahwa konfigurasi baku adalah satu orang untuk satu kelompok.

5.2 Permisi File

Penting untuk memastikan bahwa file sistem anda tidak terbuka untuk pengeditan oleh pemakai dan grup yang tidak seharusnya melakukan pemeliharaan sistem semacam itu.

UNIX membedakan kendali akses pada file dan direktori berdasarkan tiga karakteristik: pemilik (`owner`), grup, dan yang lain (`other`). Selalu terdapat satu pemilik, sejumlah anggota grup, dan setiap orang lain.

Penjelasan singkat permisi UNIX:

Kepemilikan - Pemakai dan grup mana saja yang memperoleh kendali atas setting permisi node dan node induk.

Permisi - Bit yang mampu diset atau direset untuk memungkinkan beberapa tipe akses tertentu terhadapnya. Permisi direktori mungkin memiliki arti berbeda dengan permisi set yang sama untuk file.

Read (Baca):

- Mampu melihat isi file.
- Mampu membaca direktori.

Write (Menulis):

- Mampu menambah atau merubah file.

- Mampu menghapus atau memindah file dalam sebuah direktori.

Execute (Eksekusi):

- Mampu menjalankan program biner atau script shell.
- Mampu mencari dalam sebuah direktori, dikombinasikan dengan permisi read.

Menyimpan atribut teks: (untuk direktori) Bit sticky juga memiliki arti lain ketika diaplikasikan pada direktori. Jika bit sticky diset pada direktori, maka seorang pemakai hanya boleh menghapus file yang dimiliki atau diberi ijin menulis secara eksplisit, walaupun ia memiliki akses ke direktori. Hal ini dirancang untuk direktori seperti /tmp, yang bersifat world-writable, tetapi tidak diinginkan setiap pemakai dapat menghapus file sesukanya. Bit sticky dilihat sebagai sebuah 't' dalam daftar direktori.

Atribut SUID: (untuk file) Atribut ini menggambarkan permisi set ID pemakai atas file. Ketika mode akses permisi set ID diset dalam permisi pemilik, dan file adalah eksekutabel, proses yang menjalankannya diberi ijin akses kepada sumber daya sistem berdasarkan pemakai yang membuat proses. Inilah penyebab eksploitasi 'buffer overflow'.

Atribut SGID: (untuk file) Jika diset dalam permisi grup, bit ini mengendalikan status "set group id" file. Ia berlaku serupa dengan SUID, kecuali grup terpengaruh. File harus eksekutabel agar dapat berlaku.

Atribut SGID: (untuk direktori) Jika anda menset bit SGID pada direktori (dengan "chmod g+s direktori"), file yang tercipta di direktori akan memiliki grup yang sama dengan grup direktori.

Anda - Pemilik file

Grup - Grup anda berada.

Orang lain - Setiap orang yang ada di sistem yang bukan pemilik atau anggota grup.

Contoh File :

```
-rw-r--r--  1 kevin  users         114 Aug 28  1997 .zlogin
1st bit - direktori?               (tidak)
 2nd bit - baca oleh pemilik?       (ya, oleh kevin)
  3rd bit - tulis oleh pemilik?      (ya, oleh kevin)
   4th bit - eksekusi oleh pemilik?   (tidak)
    5th bit - baca oleh grup?          (ya, oleh users)
     6th bit - tulis oleh grup?         (tidak)
      7th bit - eksekusi oleh grup?      (tidak)
       8th bit - baca oleh tiap orang?    (ya, o/ tiap orang)
        9th bit - tulis oleh tiap orang?   (tidak)
         10th bit - eksekusi o/ tiap orang? (tidak)
```

Baris berikut merupakan contoh set minimum permisi yang dibutuhkan untuk melakukan akses yang dideskripsikan. Anda mungkin ingin memberi permisi lebih daripada yang ditampilkan, tetapi ini akan mendeskripsikan apa yang dilakukan oleh permisi minimum :

```
-r--------  Membolehkan akses baca file oleh pemilik
--w-------  Membolehkan pemilik untuk modifikasi/hapus file
---x------  Pemilik dapat mengeksekusi program, tapi bukan shell script,
            yang masih perlu ijin baca
```

```
---s------  Akan mengeksekusi dengan ID pemakai efektif = pemilik
-------s--  Akan mengeksekusi dengan ID pemakai efektif = grup
-rw------T  Tdk ada update "last modified time". Biasanya untuk file swap
---t------  Tidak ada efek. (dulunya bit sticky)
```

Contoh direktori:

```
drwxr-xr-x  3 kevin  users         512 Sep 19 13:47 .public_html/
1st bit - direktori?             (ya, berisi banyak file)
 2nd bit - baca oleh pemilik?     (ya, oleh kevin)
  3rd bit - tulis oleh pemilik?    (ya, oleh kevin)
   4th bit - eksekusi oleh pemilik? (ya, oleh kevin)
    5th bit - baca oleh grup?        (ya, oleh pemakai)
     6th bit - tulis oleh grup?       (tidak)
      7th bit - eksekusi oleh grup?    (ya, oleh pemakai)
       8th bit - baca oleh tiap orang?  (ya, oleh setiap orang)
        9th bit - tulis oleh tiap orang?  (tidak)
         10th bit - eksekusi oleh everyone? (ya, oleh tiap orang)
```

Baris-baris berikut adalah contoh set permisi minimum yang diperlukan untuk melakukan akses yang dideskripsikan. Anda mungkin ingin memberi lebih permisi daripada yang didaftarkan, namun contoh ini dapat menggambarkan apa yang dilakukan permisi minimum pada direktori:

```
dr--------  Isi dpt ditampilkan, tapi atribut file tidak dapat dibaca
d--x------  Direktori dapat dimasuki, dan digunakan dl path eksekusi penuh
dr-x------  Atribut file dapat dibaca oleh pemilik
d-wx------  File dapat diciptakan/dihapus, meski bukan direktori saat ini
d------x-t  Mencegah file dihapus oleh orang lain dengan akses tulis.
            Digunakan di /tmp
d---s--s--  Tidak ada efek
```

File konfigurasi sistem (biasanya di /etc/) biasanya mode 640 (-rw-r—–), dan dimiliki oleh root. Tergantung pada persyaratan keamanan site anda, anda mungkin perlu menyesuaikannya. Jangan pernah meninggalkan file sistem dapat ditulisi oleh grup atau tiap orang. Beberapa file konfigurasi, termasuk /etc/shadow, hanya boleh dibaca oleh root, dan direktori dalam /etc tidak boleh diakses oleh orang lain.

Script Shell SUID Script shell SUID merupakan risiko keamanan yang serius, dan oleh karena itu kernel tidak akan menganggapnya. Meski anda menganggap betapa aman script shell, ia dapat dieksploitasi untuk memberi cracker shell root.

5.3 Pemeriksaan Integritas dengan Tripwire

Cara baik lain untuk mendeteksi serangan lokal (dan juga jaringan) pada sistem anda adalah dengan menjalankan pemeriksa integritas seperti Tripwire. Tripwire menjalankan sejumlah checksum di seluruh file biner dan config penting anda dan membandingkannya dengan database terdahulu, yang diketahui baik sebagai referensi. Oleh karena itu, setiap perubahan dalam file akan diketahui.

Merupakan ide yang baik untuk menginstal tripwire ke floppy, dan kemudian mengeset write protect secara fisik pada floppy. Dengan demikian penyusup tidak dapat mengganggu tripwire atau merubah database.

Sekali anda telah memiliki setup tripwire, merupakan ide yang baik untuk menjalankannya sebagai tugas administrasi keamanan normal anda untuk melihat jika ada perubahan.

Anda bahkan dapat menambahkan entry crontab untuk menjalankan tripwire dari floppy setiap malam dan mengirimkan hasilnya kepada anda di pagi hari. Sesuatu seperti :

```
# set mailto
MAILTO=kevin
# run tripwire
15 05 * * * root /usr/local/adm/tcheck/tripwire
```

akan mengirimkan laporan kepada anda di jam 5:15 pagi hari.

Tripwire dapat pula menjadi petunjuk yang baik untuk mendeteksi penyusup sebelum anda mengetahuinya. Oleh karena banyaknya file yang berubah pada rata-rata sistem, anda harus berhati-hati tentang aktivitas cracker dan apa yang anda lakukan.

5.4 Trojan Horses (Kuda-kuda Troya)

Kuda troya diambil namanya dari fabel sastra besar Homer. Idenya adalah anda menaruh program atau biner yang tampaknya bagus, dan membuat orang lain mendownloadnya dan menjalankannya sebagai root. Kemudian, anda dapat mengganggu sistem mereka sementara mereka tidak memperhatikan. Sementara mereka berpikir bahwa file biner yang mereka ambil hanya melakukan satu hal (dan mungkin sangat baik), namun ia juga mengganggu keamanan mereka.

Anda perlu waspada terhadap program apa yang anda instal di mesin anda. RedHat menyediakan checksum MD5, dan tanda PGP, file RPM sehingga anda dapat memverifikasi bahwa anda menginstal hal yang sebenarnya. Distribusi lain memiliki metode yang serupa. Anda sebaiknya tidak menjalankan sembarang file biner yang kode sumbernya tidak anda miliki atau kenal sebagai root! Sedikit penyerang yang bersedia mengeluarkan kode sumber untuk dilihat publik.

Meski dapat menjadi kompleks, pastikan anda memperoleh kode sumber untuk beberapa program dari site distribusi sebenarnya. Jika program akan berjalan sebagai root pastikan anda atau seseorang yang anda percayai telah melihat kode sumber dan memverifikasinya.

6 Keamanan Password dan Enkripsi

Salah satu feature keamanan yang penting yang digunakan saat ini adalah password. Penting bagi anda dan seluruh pemakai anda untuk memiliki password yang aman dan tidak dapat diterka. Kebanyakan distribusi Linux terbaru menyertakan program 'passwd' yang tidak membolehkan anda menset password yang mudah diterka. Pastikan program passwd anda terbaru dan memiliki feature ini.

Diskusi mendalam tentang enkripsi adalah di luar lingkup dokumen ini, tetapi pendahuluannya tidak. Enkripsi sangat berguna, mungkin sangat perlu di saat ini. Terdapat berbagai metode enkripsi data, yang memiliki karateristiknya sendiri.

Kebanyakan unicies (dan Linux bukanlah perkecualian) utamanya menggunakan algoritma enkripsi satu arah (one-way), disebut DES (Data Encryption Standard) untuk mengenkripsi password anda. Password terenkripsi ini kemudian disimpan (umumnya) di /etc/passwd (atau kurang umum) di /etc/shadow. Ketika anda berusaha login, apapun yang anda ketikkan dienkripsi dibandingkan dengan masukan dalam file yang menyimpan password anda. Jika cocok, pastilah passwordnya sama, dan anda dibolehkan mengakses. Meskipun DES merupakan algoritma enkripsi dua arah (anda dapat menkode dan mendekode pesan, dengan memberi kunci yang tepat), varian yang digunakan kebanyakan unicies adalah satu arah. Artinya tidak mungkin membalik enkripsi untuk memperoleh password dari isi /etc/passwd (atau /etc/shadow).

Serangan brute force, seperti "Crack" atau "John the Ripper" (lihat di bawah) sering dapat digunakan untuk menerka password meski password anda cukup acak. Modul PAM (lihat di bawah) memungkinkan anda menggunakan rutin enkripsi yang berbeda dengan password anda (MD5 atau sejenisnya).

Anda dapat ke *http://consult.cern.ch/writeup/security/security_3.html* untuk informasi bagaimana memilih password yang baik.

6.1 PGP dan Public Key Cryptography

Public Key Cryptography, seperti yang digunakan untuk PGP, melibatkan kriptografi yang menggunakan satu kunci untuk enkripsi, dan satu kunci untuk dekripsi. Secara tradisional, kriptografi menggunakan kunci yang sama untuk enkripsi dan dekripsi. "Kunci pribadi" ini harus diketahui oleh kedua pihak, dan ditransfer dari satu ke lainnya secara aman.

Enkripsi kunci publik membebaskan kebutuhan untuk secara aman mentransmisi kunci yang diperlukan untuk enkripsi dengan menggunakan dua buah kunci berbeda, kunci pribadi dan kunci publik. Kunci publik setiap orang tersedia bagi semua orang untuk melakukan enkripsi, sementara pada saat yang sama setiap orang menjaga kunci pribadinya untuk mendekripsi pesan terenkripsi dengan kunci publik yang tepat.

Terdapat keuntungan public key dan private key cryptography, dan anda dapat membaca tentang perbedaan-perbedaan ini dalam RSA Cryptography FAQ, didaftarkan pada akhir bagian ini.

PGP (Pretty Good Privacy) didukung dengan baik pada Linux. Versi 2.6.2 dan 5.0 dikenal bekerja dengan baik. Untuk perkenalan tentang PGP dan bagaimana menggunakan, silakan lihat PGP FAQ *http://www.pgp.com/service/export/faq/55faq.cgi*. Pastikan menggunakan versi yang dapat digunakan di negara anda, berkaitan dengan pembatasan ekspor oleh pemerintah AS, enkripsi kuat dianggap sebuah senjata militer, dan terlarang untuk ditransfer dalam bentuk elektronik ke luar negeri.

Terdapat pula panduan langkah-demi-langkah untuk mengkonfigurasi PGP pada Linux di . Ditulis untuk versi internasional PGP, tetapi dapat diterapkan secara mudah ke versi AS. Anda mungkin butuh patch bagi versi terbaru Linux, yang tersedia di .

Informasi lebih jauh tentang cryptography dapat dijumpai dalam RSA Cryptography FAQ, tersedia di *http://www.rsa.com/rsalabs/newfaq*. Di sini anda akan menjumpai informasi mengenai istilah seperti "Diffie-Hellman", "public-key cryptography", "Digital Certificates", dsb.

6.2 SSL, S-HTTP, HTTPS dan S/MIME

Seringkali pemakai bertanya mengenai perbedaan-perbedaan antara berbagai protokol keamanan, dan bagaimana menggunakannya. Meski ini bukan dokumen enkripsi, merupakan ide yang baik untuk menjelaskan secara singkat setiap protokol dan di mana mencari informasi yang lebih banyak.

- SSL : SSL, atau Secure Sockets Layer, adalah metode enkripsi yang dikembangkan oleh Netscape untuk memberikan keamanan di Internet. Ia mendukung beberapa protokol enkripsi dan memberikan autentikasi client dan server. SSL beroperasi pada layer transpor, menciptakan saluran enkripsi yang aman untuk data, dan dapat mengenkripsi banyak tipe data. Hal ini dapat dilihat ketika mengunjungi site yang aman untuk melihat dokumen online aman dengan Communicator, dan berfungsi sebagai dasar komunikasi yang aman dengan Communicator, juga dengan enkripsi data Netscape Communication lainnya. Informasi lebih banyak dapat dijumpai di *http://www.consensus.com/security/ssl-talk-faq.html.* Informasi mengenai implementasi keamanan Netscape lainnya dan sebagai titik awal yang baik untuk protokol-protokol ini tersedia di *http://home.netscape.com/info/security-doc.html.*

- S-HTTP : S-HTTP adalah protokol lain yang memberikan pelayanan keamanan di Internet. Ia dirancang untuk memberikan `confidentiality`, `authenticity`, `integrity`, dan `non-repudiability` (tidak dapat dianggap sebagai orang lain) sementara mendukung banyak mekanisme manajemen kunci dan algoritma kriptografi melalui pilihan negosiasi antar pihak-pihak yang terlibat dalam setiap transaksi. S-HTTP terbatas pada software khusus yang mengimplementasikannya dan mengenkripsi setiap pesan secara individual. (Dari RSA Cryptography FAQ, hlm. 138)
- S/MIME: - S/MIME, atau Secure Multipurpose Internet Mail Extension, adalah standar enkripsi yang digunakan untuk mengenkripsi surat elektronik, atau tipe pesan lain di Internet. Ini merupakan standar terbuka yang dikembangkan RSA, sehingga kemungkinan akan kita jumpai di Linux suatu hari. Informasi lebih lanjut tentang S/MIME dapat ditemukan di *http://home.netscape.com/assist/security/smime/overview.html.*

6.3 Implementasi IPSEC pada Linux x-kernel

Bersama dengan CIPE, dan berbagai bentuk lain data enkripsi, terdapat pula implementasi IPSEC untuk Linux. IPSEC adalah sebuah usaha oleh IETF untuk menciptakan komunikasi yang aman secara kriptografi di tingkat jaringan IP, yang juga memberikan autentikasi, integritas, kendali akses, dan konfidensial. Informasi mengenai IPSEC dan draft Internet dapat dijumpai di *IETF Homepage.* Anda dapat pula menemukan link ke berbagai protokol yang mencakup manajemen kunci, dan sebuah mailing list dan arsip.

Implementasi Linux, yang sedang dikembangkan di Universitas Arizona, menggunakan kerangka kerja berbasis obyek untuk mengimplementasikan protokol jaringan yang disebut x-kernel, dan dapat dijumpai di *http://www.cs.arizona.edu/xkernel/hpcc-blue/linux.html.* Secara sederhana, x-kernel adalah metode penyerahan pesan pada tingkat kernel, yang memudahkan dalam implementasi.

Sama seperti berbagai bentuk kriptografi lainnya, x-kernel tidak didistribusikan dengan kernel secara default karena adanya pembatasan ekspor.

6.4 SSH (Secure Shell), stelnet

SSH dan stelnet adalah program yang memungkinkan anda untuk login ke sistem remote dan memiliki koneksi yang terenkripsi.

SSH adalah paket program yang digunakan sebagai pengganti yang aman untuk rlogin, rsh dan rcp. Ia menggunakan public-key cryptography untuk mengenkripsi komunikasi antara dua host, demikian pula untuk autentikasi pemakai. Ia dapat digunakan untuk login secara aman ke remote host atau menyalin data antar host, sementara mencegah *man-in-the-middle attacks* (pembajakan sesi) dan *DNS spoofing.* Ia akan melakukan kompresi data pada koneksi anda, dan komunikasi X11 yang aman antar host. SSH homepage dapat dijumpai di *http://www.cs.hut.fi/ssh*

Anda dapat pula menggunakan SSH dari stasiun kerja Windows anda ke server SSH Linux. Terdapat beberapa implementasi client Windows yang tersedia gratis, termasuk satu di *http://guardian.htu.tuwien.ac.at/therapy/ssh/* dan juga implementasi komersil dari DataFellows, di *http://www.datafellows.com*

SSLeay adalah implementasi bebas protokol Secure Sockets Layer Netscape, termasuk beberapa aplikasi, seperti Secure telnet, modul untuk Apache, beberapa database, dan juga beberapa algoritma termasuk DES, IDEA dan Blowfish.

Dengan menggunakan pustaka ini, pengganti secure telnet telah diciptakan yang melakukan enkripsi pada koneksi telnet. Tidak seperti SSH, stelnet menggunakan SSL, protokol Secure Sockets Layer yang dikembangkan Netscape. Anda dapat menjumpai Secure telnet dan Secure FTP dengan melihat dulu SSLeay FAQ, tersedia di *http://www.psy.uq.oz.au*

6.5 PAM - Pluggable Authentication Modules

Versi baru distribusi RedHat Linux dikirimkan dengan skema autentikasi yang terpadu disebut "PAM". PAM memungkinkan anda merubah secara *on the fly* metode autentikasi anda, persyaratan, dan menyembunyikan seluruh metode autentikasi lokal tanpa perlu mengkompilasi ulang biner anda. Konfigurasi PAM adalah di luar lingkup dokumen ini, tetapi pastikan untuk melihat web site PAM untuk informasi lebih banyak *http://www.kernel.org/pub/linux/libs/pam*

Beberapa hal yang dapat anda lakukan dengan PAM:

- Menggunakan enkripsi non DES untuk password anda. (Membuatnya sulit untuk didekodekan secara brute force)
- Menset batasan sumber daya pada seluruh pemakai anda sehingga mereka tidak dapat melakukan serangan Denial of Service (jumlah proses, jumlah memori, dsb)
- Memungkinkan shadow password secara on the fly
- Membolehkan pemakai tertentu untuk login hanya pada waktu tertentu dari tempat tertentu.

Dalam beberapa jam setelah instalasi dan konfigurasi sistem anda, anda dapat mencegah banyak serangan sebelum mereka terjadi. Sebagai contoh, menggunakan PAM untuk meniadakan pemakain secara system-wide file dot-rhosts dalam direktori home pemakai dengan menambahkan baris-baris berikut ke /etc/pam.d/login:

```
#
# Disable rsh/rlogin/rexec for users
#
login auth required pam_rhosts_auth.so no_rhosts
```

6.6 Cryptographic IP Encapsulation (CIPE)

Tujuan utama software ini adalah memberikan fasilitas bagi interkoneksi subnetwork yang aman (menghadapi eavesdropping, termasuk traffic analysis, dan faked message injection) melintasi jaringan paket yang tidak aman seperti Internet.

CIPE mengenkripsi data pada level jaringan. Paket-paket yang berjalan antar host pada jaringan dienkripsi. Mesin enkripsi ditempatkan dekat driver yang mengirim dan menerima paket.

Tidak seperti SSH, yang mengenkripsi data dengan hubungan, pada level soket. Koneksi logika antara program yang berjalan di host yang berbeda dienkripsi.

CIPE dapat digunakan dalam *tunnelling*, dalam rangka menciptakan Virtual Private Network. Enkripsi level rendah memiliki keuntungan yaitu dapat dibuat transparan antar dua jaringan yang terhubung dalam VPN, tanpa merubah software aplikasi.

Ringkasan dari dokumentasi CIPE: Standar-standar IPSEC mendefinisikan sejumlah protokol yang dapat digunakan (di antara berbagai hal lain) untuk membangun VPN yang terenkripsi. Namun demikian, IPSEC lebih seperti himpunan protokol kelas berat dan rumit dengan banyak pilihan, implementasi seluruh himpunan protokol masih jarang digunakan dan beberapa isu (seperti manajemen kunci) masih belum terpecahkan. CIPE menggunakan pendekatan yang lebih sederhana, yaitu banyak hal yang dapat diparameterkan (seperti pilihan algoritma enkripsi yang digunakan) adalah pilihan tetap pada saat instalasi. Hal ini membatasi fleksibilitas, namun memungkinkan implementasi yang sederhana (maka efisien, mudah didebug..).

Informasi lebih lanjut dapat ditemukan di *http://www.inka.de/~bigred/devel/cipe.html*

Serupa dengan bentuk kriptografi lainnya, ia tidak didistribusikan dengan kernel secara default karena adanya pembatasan ekspor.

6.7 Kerberos

Kerberos adalah sebuah sistem autentikasi yang dikembangkan oleh Proyek Athena di MIT. Ketika pemakai login, Kerberos mengautentikasi pemakai tersebut (menggunakan password), dan memberikan pemakai suatu cara untuk membuktikan identitasnya ke server dan host lain yang tersebar di jaringan.

Autentikasi ini kemudian digunakan oleh program seperti rlogin untuk membolehkan pemakai login ke host lain tanpa password (seperti file .rhosts). Autentikasi juga digunakan oleh sistem surat dalam rangka menjamin bahwa surat dikirimkan kepada orang yang tepat, dan juga menjamin bahwa pengirim adalah benar orang yang diklaimnya.

Efek keseluruhan menginstalasi Kerberos dan berbagai program bersamanya adalah secara virtual menghilangkan kemampuan pemakai untuk menipu (spoof) sistem agar mempercayai bahwa mereka adalah orang lain. Sayangnya, instalasi Kerberos sangat sulit, membutuhkan modifikasi atau mengganti berbagai program standar.

Anda dapat menemukan informasi lebih banyak tentang kerberos di *http://www.veritas.com/common/f/97042301.htm* dan kodenya dapat ditemukan di *http://nii.isi.edu/info/kerberos/*

(Dari: Stein, Jennifer G., Clifford Neuman, dan Jeffrey L. Schiller. "Kerberos: An Authentication Service for Open Network Systems." USENIX Conference Proceedings, Dallas, Texas, Winter 1998.)

6.8 Shadow Passwords

Shadow password adalah suatu cara menjaga password terenkripsi anda dari pemakai normal. Normalnya, password terenkripsi ini disimpan di file /etc/passwd dapat dibaca semua pemakai. Mereka lalu dapat menjalankan program penerka password dan berusaha menentukan passwordnya. Shadow password menyimpan informasi ini ke file /etc/shadow yang hanya dapat dibaca oleh pemakai yang berhak. Dalam rangka menjalankan shadow password anda perlu memastikan bahwa seluruh utilitas anda yang perlu mengakses informasi password dikompilasi ulang untuk mendukungnya. PAM juga membolehkan anda untuk hanya memasukkan modul shadow dan tidak perlu mengkompilasi ulang eksekutabel. Anda dapat mengacu pada Shadow-Password HOWTO untuk informasi lebih lanjut jika perlu. Tersedia di *http://sunsite.unc.edu/LDP/HOWTO/Shadow-Password-HOWTO.html*. Ini sudah kuno, dan tidak dibutuhkan untuk distribusi yang mendukung PAM.

6.9 Crack dan John the Ripper

Jika untuk beberapa alasan program passwd anda tidak memaksa password yang tidak mudah diterka, anda mungkin ingin menjalankan program password cracking dan memastikan password pemakai anda aman.

Program password cracking bekerja berdasarkan ide yang mudah. Mereka mencoba setiap kata yang ada di kamus, dan kemudian variasi dari kata-kata tersebut. Mereka mengenkripsi satu kata dan membandingkannya dengan password terenkripsi anda. Jika cocok dicatat.

Terdapat sejumlah program ini...dua yang paling dikenal adalah "Crack" dan "John the Ripper" *http://www.false.com/security/john/*. Mereka akan mengambil banyak waktu cpu anda, tetapi anda seharusnya dapat mengetahui jika penyerang dapat masuk dengan menggunakan mereka dengan terlebih dulu menjalankan mereka dan memberitahu pemakai dengan password lemah. Perhatikan bahwa penyerang harus menggunakan beberapa lubang lain untuk memperoleh file passwd anda, namun ini lebih umum daripada yang anda pikirkan.

6.10 CFS- Cryptographic File System dan TCFS - Transparent Cryptographic File System

CFS adalah suatu cara mengenkripsi seluruh sistem file dan memungkinkan pemakai untuk menyimpan file-file terenkripsi di dalamnya. Ia menggunakan server NFS yang berjalan pada mesin lokal. rpms tersedia di *http://www.replay.com/redhat/* dan informasi mengenai bagaimana bekerjanya ada di *ftp://ftp.research.att.com/dist/mab*

TCFS memperbaiki CFS, menambahkan lebih banyak integrasi dengan sistem file, sehingga transparan bagi semua pemakai yang menggunakan sistem file yang terenkripsi. Informasi lebih banyak di *http://edu-gw.dia.unisa.it/tcfs/*

6.11 X11, SVGA dan keamanan tampilan

6.11.1 X11

Penting bagi anda untuk mengamankan tampilan grafis anda untuk mencegah penyerang melakukan hal-hal seperti : mengambil password anda ketika anda ketikan tanpa anda ketahui, membaca dokumen atau informasi yang sedang anda baca, atau bahkan menggunakan lubang untuk memperoleh akses superuser. Dengan menjalankan aplikasi X remote melalui jaringan dapat pula menjadi ancaman, memungkinkan sniffer melihat seluruh interaksi anda dengan remote system.

X memiliki sejumlah mekanisme kendali akses. Yang termudah adalah berdasarkan host. Anda dapat menggunakan xhost untuk menspesifikasikan host-host mana saja yang dibolehkan mengakses tampilan anda. Namun ini tidak begitu aman. Jika seseorang memperoleh akses ke mesin anda mereka dapat xhost + mesin mereka dan dapat masuk secara mudah. Juga, jika anda membolehkan akses dari mesin yang tidak terpercaya, siapapun di sana dapat mengganggu tampilan anda.

Ketika menggunakan xdm (x display manager) untuk login, anda memperoleh metode akses yang jauh lebih baik: MIT-MAGIC-COOKIE-1. Cookie 128-bit dihasilkan dan disimpan dalam file .Xauthority. Jika anda butuh untuk membolehkan remote mesin mengakses tampilan anda, anda dapat menggunakan perintah xauth dan informasi dalam file .Xauthority untuk memberikan hanya akses koneksi. Lihat Remote-X-Apps mini-howto, tersedia di *http://sunsite.unc.edu/LDP/HOWTO/mini/Remote-X-Apps.html*

Anda dapat pula menggunakan ssh (lihat ssh di atas) untuk membolehkan koneksi X yang aman. Keuntungannya adalah tranparan bagi pemakai akhir, dan berarti tidak ada data yang tidak terenkripsi melalui jaringan.

Silakan lihat Xsecurity man page untuk informasi lebih jauh tentang keamanan X. Pilihan terbaik adalah menggunakan xdm untuk login ke konsol anda dan kemudian menggunakan ssh untuk ke remote site yang ingin anda jalankan program X-nya.

6.11.2 SVGA

Program-program SVGAlib umumnya SUID-root dalam rangka mengakses hardware video mesin Linux anda. Ini menjadikan mereka sangat berbahaya. Jika mereka crash, anda biasanya perlu mereboot mesin anda untuk memperoleh konsol kembali. Pastikan program-program SVGA yang anda jalankan autentik, dan paling tidak dapat dipercaya. Lebih baik lagi, jangan jalankan mereka sama sekali.

6.11.3 GGI (Generic Graphics Interface Project)

Proyek Linux GGI berusaha memecahkan beberapa masalah dengan antar muka video pada Linux. GGI akan memindahkan bagian kecil code video ke kernel Linux, dan kemudian mengendalikan akses ke sistem video. Artinya GGI akan dapat mengembalikan konsol anda setiap waktu ke keadaan yang baik. Mereka juga akan memungkinkan kunci atensi yang aman, sehingga anda dapat memastikan bahwa tidak ada program login kuda Troya berjalan di konsol anda. *http://synergy.caltech.edu/~ggi/*

7 Keamanan Kernel

Ini adalah deskripsi pilihan konfigurasi kernel yang terkait dengan keamanan, dan sebuah penjelasan apa yang dilakukannya, dan bagaimana menggunakan mereka.

Oleh karena kernel mengendalikan jaringan komputer anda, penting agar kernel sangat aman, dan kernel sendiri tidak akan diganggu. Untuk mencegah serangan jaringan terkini, anda harus berusaha dan memelihara versi kernel anda. Anda dapat menemukan kernel terbaru di *ftp://ftp.kernel.org*

7.1 Pilihan Kompilasi Kernel

- IP: Drop source routed frames (CONFIG_IP_NOSR) Pilihan ini seharusnya diset. Source routed frame berisikan seluruh jalur ke tujuan. Artinya router yang dilalui paket tidak perlu memeriksa paket, dan hanya memforwardnya saja. Hal ini dapat mengakibatkan masuknya data ke sistem anda yang mungkin menjadi eksploitasi potensial.
- IP: Firewalling (CONFIG_IP_FIREWALL) Pilihan ini perlu jika anda ingin mengkonfigurasi mesin anda sebagai firewall, melakukan masquerading, atau ingin melindungi stasiun kerja dial-up anda dari seseorang yang masuk melalui antar muka dial-up PPP anda.

- IP: forwarding/gatewaying (CONFIG_IP_FORWARD) Jika anda menset IP forwarding, mesin Linux anda maka menjadi router. Jika mesin anda ada pada jaringan, anda harus memforward data dari satu jaringan ke yang lain, dan mungkin membalik firewall yang ada di sana untuk mencegah hal ini terjadi. Pemakai dial-up normal mungkin ingin meniadakannya, dan pemakai lain harus berkonsentrasi pada implikasi keamanan melakukan hal ini. Mesin-mesin firewall akan mengadakannya, dan digunakan bersamaan dengan software firewall.

  Anda dapat mengadakan IP forwarding secara dinamik menggunakan perintah berikut :

```
root#  echo 1 > /proc/sys/net/ipv4/ip_forward
```

  dan meniadakannya dengan perintah :

```
root#  echo 0 > /proc/sys/net/ipv4/ip_forward
```

  File ini (dan banyak file lain di /proc) akan selalu tampak berukuran nol, tetapi kenyataannya tidak. Ini adalah feature kernel yang baru diperkenalkan, sehingga pastikan anda menggunakan kernel 2.0.33 atau lebih baru.

- IP: firewall packet logging (CONFIG_IP_FIREWALL_VERBOSE) Pilihan ini memberi anda informasi tentang paket yang diterima firewall anda, seperti pengirim, penerima, port, dsb.

- IP: always defragment (CONFIG_IP_ALWAYS_DEFRAG) Umumnya pilihan ini ditiadakan, tetapi jika anda membangun host firewall atau masquerading, anda mungkin ingin mengadakannya. Ketika data dikirim dari satu host ke yang lain, ia tidak selalu dikirim sebagai satu paket data, tetapi dipecah-pecah ke beberapa bagian. Masalah dengan hal ini adalah nomor port selalu disimpan dalam bagian pertama. Artinya seseorang dapat memasukkan informasi ke paket-paket sisanya yang tidak seharusnya ada.

- IP: syn cookies (CONFIG_SYN_COOKIES) SYN Attack adalah serangan denial of service (DoS) yang menghabiskan seluruh sumber daya mesin anda, memaksa anda untuk reboot. Kami tidak dapat memikirkan alasan anda meniadakan pilihan ini.

- Packet Signatures (CONFIG_NCPFS_PACKET_SIGNING) Ini adalah pilihan yang tersedia pada seri kernel 2.1 yang akan menandai paket NCP untuk keamanan yang lebih kuat. Secara normal anda dapat membiarkannya tidak ada, tetapi ia ada jika anda membutuhkannya.

- IP: Firewall packet netlink device (CONFIG_IP_FIREWALL_NETLINK) Ini adalah pilihan yang baik yang memungkinkan anda menganalisa 128 byte pertama paket dalam program userspace, untuk menentukan bilamana anda ingin menerima atau menolak paket, berdasarkan validitasnya.

7.2 Device Kernel

Terdapat sejumlah device blok dan karakter untuk Linux yang dapat membantu anda dengan keamanan.

Dua device /dev/random dan /dev/urandom disediakan oleh kernel untuk menerima data random setiap saat.

/dev/random dan /dev/urandom keduanya cukup aman digunakan dalam menghasilkan kunci PGP, tantangan SSH, dan aplikasi lain di mana bilangan random yang aman dibutuhkan. Penyerang seharusnya tidak dapat memperkirakan nomor berikutnya bila diberi urutan awal nomor-nomor dari sumber ini. Telah ada banyak usaha untuk memastikan bahwa nomor yang anda peroleh dari sumber ini adalah random dalam setiap arti kata random.

Perbedaannya adalah bahwa /dev/random menghasilkan byte random dan membuat anda menunggu lebih banyak untuk dikumpulkan. Perhatikan bahwa pada beberapa sistem, ia dapat memblok untuk waktu lama menunggu masukan baru pemakai untuk diberi ke sistem. Sehingga anda perlu berhati-hati sebelum menggunakan /dev/random. (Mungkin hal terbaik yang dapat dilakukan adalah menggunakan ketika anda menciptakan informasi sensitif, dan anda mengatakan kepada pemakai untuk menekan keyboard secara berulang-ulang hingga anda mencetak "OK, enough").

/dev/random adalah entropi kualitas tinggi, dihasilkan dari pengukuran waktu inter-interrupt dsb. Ia memblok hingga cukup data random bit tersedia.

/dev/urandom adalah serupa, kecuali ketika penyimpanan entropi berjalan rendah ia akan mengembalikan hash kuat secara kriptografi. Ini tidak aman, tetapi cukup bagi kebanyakan aplikasi.

Anda mungkin membaca dari device menggunakan sesuatu seperti:

```
root# head -c 6 /dev/urandom | uuencode -
```

Ini akan mencetak enam karakter random di layar, sesuai untuk pembuatan password.

Lihat /usr/src/linux/drivers/char/random.c untuk deskripsi algoritma.

Terima kasih kepada Theodore Y. Ts'o, John Lewis, dan yang lain dari Linux-kernel atas bantuannya kepada saya (Dave) untuk hal ini.

8 Keamanan Jaringan

Keamanan jaringan menjadi semakin penting dengan semakin banyaknya waktu yang dihabiskan orang untuk berhubungan. Mengganggu keamanan jaringan sering lebih mudah daripada fisik atau lokal, dan lebih umum.

Terdapat sejumlah alat yang baik untuk membantu keamanan jaringan, dan semakin banyak disertakan dalam distribusi Linux.

8.1 Packet Sniffers

Salah satu cara umum yang digunakan penyusup untuk memperoleh akses ke banyak sistem di jaringan anda adalah dengan menggunakan sebuah packet sniffer pada host yang telah diganggu. Sniffer ini mendengarkan port Ethernet untuk hal-hal seperti "Password" dan "Login" dan "su" dalam aliran paket dan kemudian mencatat lalu lintas setelahnya. Dengan cara ini, penyerang memperoleh password untuk sistem yang bahkan tidak mereka usahakan untuk dibongkar. Password teks biasa adalah sangat rentan terhadap serangan ini.

Contoh: host A telah diganggu. Penyerang menginstal sebuah sniffer. Sniffer mencatat login admin ke host B dari host C. Ia memperoleh password personal admin ketika ia login ke B. Kemudian, admin melakukan 'su' untuk mengatasi suatu masalah. Mereka sekarang memiliki password root untuk Host B. Kemudian admin membolehkan seseorang telnet dari rekeningnya ke host Z di site lain. Sekarang penyerang memiliki password/login di host Z.

Di masa sekarang, penyerang bahkan tidak perlu mengganggu sebuah sistem untuk melakukan hal ini, mereka dapat membawa laptop atau pc ke suatu gedung dan menyadap ke jaringan anda.

Dengan menggunakan ssh atau metode password terenkripsi lainnya dapat mencegah serangan ini. Hal-hal seperti APOP untuk rekening pop juga dapat mencegah serangan ini. (Login pop normal sangat rentan untuk hal ini, sama seperti segala sesuatu yang mengirim password teks biasa melalui kabel).

8.2 Pelayanan sistem dan tcp_wrappers

Segera setelah anda menaruh sistem Linux anda di sembarang jaringan, hal pertama yang harus dilihat adalah pelayanan yang butuh anda tawarkan. Pelayanan-pelayanan yang tidak perlu anda tawarkan seharusnya ditiadakan sehingga anda memiliki satu hal yang tidak perlu dikhawatirkan dan penyerang memiliki satu hal kurangnya untuk mencari lubang.

Terdapat sejumlah cara untuk meniadakan pelayanan dalam Linux. Anda dapat melihat pada file /etc/inetd.conf dan melihat pelayanan apa yang ditawarkan oleh inetd anda. Tiadakan segala yang tidak anda butuhkan dengan mengkomentari mereka (taruh # di awal baris), dan kemudian mengirimkan proses inetd anda sebuah SIGHUP.

Anda dapat pula menghilangkan (atau mengkomentari) pelayanan-pelayanan di file /etc/services. Hal ini berarti client lokal anda tidak akan menemukan pelayanan (contoh, jika anda menghilangkan ftp, dan berusaha dan ftp ke site remote dari mesin tersebut maka akan gagal dengan pesan pelayanan yang tidak dikenal). Tidaklah berharga untuk menghilangkan pelayanan, karena tidak memberikan keamanan tambahan. Jika orang lokal ingin menggunakan ftp bahkan yang telah anda komentari, mereka ingin membuat client mereka menggunakan port ftp umum dan masih dapat bekerja baik.

Beberapa pelayanan yang ingin anda biarkan ada adalah:

- ftp
- telnet
- mail, seperti pop-3 atau imap
- identd
- time

Jika anda tahu anda tidak ingin menggunakan beberapa paket tertentu, anda dapat menghapusnya. rpm -e dalam distribusi Red Hat akan menghapus seluruh paket. Dalam debian dpkg akan melakukan hal yang sama.

Sebagai tambahan, anda benar-benar ingin meniadakan utilitas rsh/rlogin/rcp, termasuk login (digunakan oleh rlogin), shell (digunakan oleh rcp), dan exec (digunakan oleh rsh) dari dimulai dalam /etc/inetd.conf. Protokol-protokol ini sangat tidak aman dan menjadi penyebab eksploit dahulu.

Anda perlu memeriksa /etc/rc.d/rcN.d, dengan N adalah run level sistem anda dan melihat apakah pelayanan dimulai dalam direktori tersebut tidak dibutuhkan. File dalam /etc/rc.d/rcN.d sebenarnya adalah link simbolik ke direktori /etc/rc.d/init.d. Mengganti nama file dalam direktori init.d memiliki efek meniadakan seluruh link simbolik dalam /etc/rc.d/rcN.d. Jika anda hanya ingin meniadakan pelayanan untuk runlevel tertentu, ganti nama file yang sesuai dengan huruf kecil.

Jika anda memiliki file rc bergaya BSD, anda mungkin ingin memeriksa /etc/rc* untuk program-program yang tidak anda butuhkan.

Kebanyakan distribusi Linux menyertakan tcp_wrappers "wrapping" seluruh pelayanan tcp. Sebuah tcp_wrappers (tcpd) dipanggil dari inetd selain dari server sebenarnya. tcpd kemudian memeriksa host yang membutuhkan pelayanan dan kemudian mengeksekusi atau menolak akses server sebenarnya dari host tersebut. tcpd memungkinkan anda membatasi akses ke pelayanan tcp anda. Anda perlu membuat /etc/hosts.allow dan menambahkan hanya host yang membutuhkan akses ke pelayanan mesin anda.

Jika anda adalah pemakai dialup rumahan, kami menyarankan anda menolak seluruhnya. tcpd juga mencatat usaha yang gagal untuk mengakses pelayanan, sehingga ini dapat memberi anda ide bahwa anda sedang diserang. Jika anda menambahkan pelayanan baru, anda harus pasti mengkonfigurasinya untuk menggunakan tcp_wrappers berbasis TCP. Sebagai contoh, pemakai dial-up normal dapat mencegah orang luar koneksi ke mesin anda, namun masih memiliki kemampuan untuk menerima surat, dan membuat hubungan jaringan ke Internet. Untuk melakukan ini, anda mungkin menambahkan perintah berikut ke /etc/hosts.allow:

ALL: 127.

Dan tentu saja /etc/hosts.deny akan berisi:

ALL: ALL

yang akan mencegah koneksi eksternal ke mesin anda, namun masih memungkinkan anda dari dalam berhubungan ke server di Internet.

8.3 Memverifikasi Informasi DNS Anda

Memelihara informasi DNS tentang seluruh host di jaringan anda agar tetap baru dapat membantu meningkatkan keamanan. Bilamana ada host yang tidak dijinkan terhubung ke jaringan anda, anda dapat mengenalinya dengan tidak adanya masukan DNS. Banyak pelayanan dapat dikonfigurasi untuk tidak menerima koneksi dari host yang tidak memiliki masukan DNS yang valid.

8.4 identd

identd adalah program kecil yang umumnya berjalan di inetd. Ia mencatat pelayanan tcp apa yang dijalankan pemakai, dan kemudian melaporkannya kepada yang meminta.

Banyak orang salah mengerti kegunaan identd, sehingga meniadakannya atau memblok seluruh site yang memintanya. identd ada bukan untuk membantu remote site. Tidak ada cara untuk mengetahui jika data yang anda peroleh dari remote identd benar atau tidak. Tidak ada autentikasi dalam permintaan identd.

Lalu mengapa anda ingin menjalankannya? Karena ia membantu anda, dan adalah titik data lain dalam penelusuran. Jika identd anda tidak terganggu, maka anda mengerti ia memberi tahu remote site nama pemakai atau uid orang-orang yang menggunakan pelayanan tcp. Jika admin pada remote site datang kepada anda dan memberitahu pemakai anda berusaha menghack ke site mereka, anda dapat secara mudah mengambil tindakan terhadap pemakai tersebut. Jika anda tidak menjalankan identd, anda harus melihat banyak catatan, memperkirakan siapa yang ada pada saat itu, dan secara umum membutuhkan waktu yang lebih banyak untuk menelusuri pemakai.

identd yang disertakan dalam banyak distribusi lebih mudah dikonfigurasi daripada yang diperkirakan orang. Anda dapat meniadakan identd untuk pemakai tertentu (mereka dapat membuat file .noident), anda dapat mencatat seluruh permintaan identd (Saya menyarankannya), anda bahkan dapat memiliki identd mengembalikan uid daripada nama pemakai atau bahkan NO-USER.

8.5 SATAN, ISS, dan Scanner Jaringan Lainnya

Terdapat sejumlah paket software berbeda yang melakukan penelusuran berdasarkan port dan pelayanan mesin atau jaringan. SATAN dan ISS adalah dua yang paling dikenal. Software ini berhubungan ke mesin sasaran (atau seluruh mesin sasaran di suatu jaringan) di semua port yang ada, dan berusaha menentukan pelayanan apa yang sedang berjalan. Berdasarkan informasi ini, anda dapat menemukan mesin yang rentan terhadap eksploitasi tertentu pada server.

SATAN (Security Administrators Tool for Analyzing Networks) adalah sebuah penelusur port dengan antara muka web. Ia dapat dikonfigurasi untuk melakukan pemeriksaan ringan, menengah, atau berat pada mesin atau pada jaringan mesin. Akan merupakan ide yang baik untuk memperoleh SATAN dan memeriksa mesin atau jaringan anda, dan membenahi masalah-masalah yang ditemukan. Pastikan anda memperoleh SATAN dari sun-site atau FTP atau web site yang bereputasi. Terdapat salinan Troya SATAN yang didistribusikan di net. *http://www.trouble.org/˜zen/satan.html*

ISS (Internet Security Scanner) adalah penelusur berdasarkan port yang lain. Ia lebih cepat daripada SATAN, dan mungkin lebih baik untuk jaringan yang besar. Namun demikian, SATAN memberikan lebih banyak informasi.

Abacus-Sentry adalah penelusur port komersil dari www.psionic.com. Lihat informasi lebih lanjut di homepagenya. *http://www.psionic.com*

Mendeteksi penelusuran port. Terdapat beberapa alat yang dirancang untuk memberitahu anda adanya probe SATAN dan ISS dan software penelusuran lainnya. Namun demikian, dengan pemakaian tcp_wrappers yang liberal dan memastikan untuk melihat file log anda secara berkala, anda dapat mengetahui probe tersebut. Bahkan pada setting terendah, SATAN masih meninggalkan jejak pada log di sistem Red Hat.

8.6 Sendmail, qmail dan MTA

Salah satu pelayanan penting yang dapat anda sediakan adalah server surat. Sayangnya, ia juga sangat rentan diserang, karena banyaknya tugas yang harus dilakukan dan dibutuhkannya ijin khusus.

Jika anda menggunakan sendmail, penting untuk menjaga versi anda agar up to date. Sendmail memiliki sejarah panjang di eksploitasi keamanan. Selalu pastikan anda menjalankan versi terbaru. *http://www.sendmail.org*

Jika anda bosan mengupgrade versi sendmail anda setiap minggu, anda dapat mempertimbangkan beralih ke qmail. qmail dirancang dengan perhatian pada keamanan sejak awalnya. Ia cepat dan stabil dan aman. *http://www.qmail.org*

8.7 Serangan Denial of Service

Serangan denial of service adalah saat ketika penyerang berusaha menggunakan beberapa sumber daya hingga terlalu sibuk untuk menjawab permintaan yang resmi, atau menolak pemakai resmi mengakses mesin anda.

Serangan-serangan semacam ini meningkat dengan cepat pada tahun-tahun belakangan ini. Beberapa yang populer dan terbaru ditampilkan di bawah ini. Perhatikan bahwa yang baru selalu muncul setiap saat, sehingga ini hanya merupakan contoh. Baca list Linux security dan list serta archive bugtraq untuk informasi terkini.

- SYN Flooding - SYN flooding adalah serangan denial of service jaringan. Ia mengambil keuntungan dari "loophole" dalam koneksi TCP yang tercipta. Kernel Linux terbaru (2.0.30 ke atas) memiliki beberapa pilihan konfigurasi untuk mencegah serangan SYN flood dari menolak orang akses ke mesin atau pelayanan anda. Lihat bagian keamanan kernel untuk pilihan perlindungan kernel yang tepat.
- Pentium "F00F" Bug - Ini baru ditemukan bahwa serangkaian kode assembly yang dikirim ke prosesor asli Intel Pentium akan mereboot mesin. Ini mempengaruhi setiap mesin dengan prosesor Pentium (bukan klon, atau Pentium Pro atau PII), tidak tergantung pada sistem operasi yang dijalankan. Kernel Linux 2.0.32 ke atas memiliki pemecahan atas bug ini, mencegahnya mengunci mesin anda. Kernel 2.0.33 memiliki versi perbaikan atas hal ini, dan disarankan daripada 2.0.32. Jika anda menggunakan Pentium, anda harus upgrade sekarang!
- Ping Flooding - Ping flooding adalah serangan denial of service brute force sederhana. Penyerang mengirim "flood" paket ICMP ke mesin anda. Jika mereka melakukan ini dari host dengan bandwidth yang lebih baik daripada milik anda, mesin anda tidak akan mampu mengirim sesuatu ke jaringan. Variasi serangan ini, disebut "smurfing" mengirim paket ICMP ke host dengan IP kembalian mesin anda, memungkinkan mereka membanjiri anda dengan sedikit terdeteksi. Anda dapat menumukan informasi lebih jauh tentang serangan "smurf" di *http://www.quadrunner.com/~chuegen/smurf.txt*

  Jika anda diserang ping flood, gunakan alat seperti tcpdump untuk menentukan asal paket (atau tampaknya berasal), kemudian hubungi provider anda dengan informasi ini. Ping flood dapat secara mudah dihentikan di level router atau dengan menggunakan firewall.
- Ping o' Death - Serangan Ping o' Death disebabkan lebih besarnya paket ICMP ECHO REQUEST yang datang daripada yang dapat ditangani struktur data kernel . Oleh karena mengirim sebuah paket "ping" besar (65.510 byte) ke banyak sistem akan membuat mereka hang atau bahkan crash, masalah ini secara cepat disebut "Ping o' Death". Ini telah lama diperbaiki, dan tidak perlu dikhawatirkan lagi.
- Teardrop / New Tear - Salah satu eksploit terbaru yang melibatkan bug yang ada di kode fragmentasi IP pada platform Linux dan Windows. Telah diperbaiki dalam kernel versi 2.0.33, dan tidak membutuhkan pilihan pada saat kompilasi untuk menggunakan perbaikan. Linux tampaknya tidak rentan terhadap eksploitasi "new tear".

Anda dapat menemukan banyak kode eksploitasi, dan deskripsi lebih mendalam tentang bagaimana mereka bekerja di *http://www.rootshell.com* menggunakan mesin pencari mereka.

8.8 Keamanan NFS (Network File System)

NFS adalah protokol file sharing yang paling banyak digunakan. Ia memungkinkan server menjalankan nfsd dan mountd untuk mengekspor seluruh filesystem ke mesin lain dengan dukungan nfs filesystem pada kernelnya (atau beberapa dukungan client jika mereka bukan mesin Linux). Mountd mencatat filesystem yang termount di /etc/mtab, dan dapat menampilkannya.

Banyak site menggunakan NFS untuk bertugas sebagai direktori home untuk pemakai, sehingga tak peduli mesin apa yang dimasuki, mereka akan selalu memiliki file-filenya.

Terdapat sedikit "keamanan" dibolehkan dalam mengekspor filesystem. Anda dapat membuat peta nfsd pemakai root remote (uid=0) ke pemakai nobody, membatasi akses total ke file-file yang diekspor. Namun demikian, karena pemakai individu memiliki akses ke file-file mereka (atau paling tidak uid yang sama), superuser remote dapat login atau su ke rekening mereka dan memiliki akses total ke file-file mereka. Ini hanya penghalang kecil bagi seorang penyerang yang memiliki akses untuk melakukan mount filesystem remote anda.

Jika harus menggunakan NFS, pastikan anda mengekspor ke mesin-mesin yang anda butuh untuk ekspor saja. Jangan pernah mengekspor seluruh direktori root anda, ekspor hanya direktori yang perlu anda ekspor.

Lihat NFS HOWTO untuk informasi lebih jauh tentang NFS.

8.9 NIS (Network Information Service) (dahulu YP)

Network Information Service (dahulu YP) adalah suatu cara mendistribusikan informasi ke sekelompok mesin. Master NIS menyimpan tabel informasi dan mengkonversinya ke file peta NIS. Peta ini kemudian melayani jaringan, memungkinkan mesin klien NIS untuk memperoleh login, password, direktori home dan informasi shell (seluruh informasi di file /etc/passwd standar). Hal ini memungkinkan pemakai merubah password mereka sekali dan berlaku pula di seluruh mesin dalam domain NIS.

NIS tidak seluruhnya aman. Ia tidak pernah dimaksudkan demikian. Ia dimaksudkan untuk berguna dan sederhana. Setiap orang dapat menduga nama domain NIS anda (di setiap tempat di Net) dapat memperoleh salinan file passwd, dan menggunakan Crack dan John the Ripper terhadap password pemakai anda. Juga, adalah mungkin untuk menipu NIS dan melakukan berbagai trik kotor. Jika anda harus menggunakan NIS, pastikan anda paham bahayanya.

Terdapat pengganti NIS yang lebih aman, disebut NIS+. Silakan periksa NIS HOWTO untuk informasi lebih banyak. *http://sunsite.unc.edu/mdw/HOWTO/NIS-HOWTO.html*

8.10 Firewall

Firewall adalah suatu cara untuk membatasi informasi yang dibolehkan masuk dan keluar dari jaringan lokal anda. Umumnya host firewall terhubung ke Internet dan LAN lokal anda, dan akses LAN anda ke Internet hanya melalui firewall. Dengan demikian firewall dapat mengendalikan apa yang diterima dan dikirim dari Internet dan LAN anda.

Terdapat beberapa tipe dan metode setting firewall. Mesin-mesin Linux dapat menjadi firewall yang baik dan murah. Kode firewall dapat dibangun langsung ke dalam kernel 2.0 atau lebih tinggi. Alat ipfwadm user space memungkinkan anda merubah tipe lalu lintas jaringan yang anda bolehkan secara on the fly. Anda dapat pula mencatat tipe lalu lintas jaringan tertentu.

Firewall adalah teknik yang sangat berguna dan penting dalam mengamankan jaringan anda. Penting untuk menyadari bahwa anda tidak boleh pernah berpikir bahwa dengan memiliki firewall, anda tidak perlu mengamankan mesin-mesin di baliknya. Ini kesalahan fatal. Periksa Firewall-HOWTO yang sangat bagus di arsip terbaru sunsite untuk informasi mengenai firewall dan Linux.*http://sunsite.unc.edu/mdw/HOWTO/Firewall-HOWTO.html*

Informasi lebih banyak juga dapat ditemukan di IP-Masquerade mini-howto:*http://sunsite.unc.edu/mdw/HOWTO/mini/IP-Masquerade.html*

Informasi lebih lanjut tentang ipfwadm (Alat yang memungkinkan anda merubah setting firewall anda, dapat ditemukan di homepagenya: *http://www.xos.nl/linux/ipfwadm*

9 Persiapan Keamanan (sebelum on-line)

OK, jadi anda telah memeriksa seluruh sistem anda, dan menentukan bahwa ia aman, dan siap menaruhnya online. Terdapat beberapa hal yang perlu anda lakukan kini agar siap bila penyusupan benar terjadi, sehingga anda dapat secara cepat meniadakan penyusup, dan dapat kembali dan berjalan.

9.1 Buat Backup Menyeluruh Sistem Anda

Diskusi mengenai metode backup dan penyimpanan di luar lingkup dokumen ini, tetapi beberapa kata berkaitan dengan backup dan keamanan: Jika anda memiliki kurang dari 650mb data untuk disimpan dalam partisi, salinan data anda pada CD-R adlah cara yang baik (karena sulit merubahnya dan jika dikembalikan dengan tepat dapat lestari). Tape dan media rewritable lainnya harus di write protect segera setelah backup anda selesai dan diverifikasi untuk mencegah perubahan. Pastikan anda menyimpan backup anda di tempat yang aman. Backup yang baik akan memastikan anda memiliki titik yang baik untuk mengembalikan sistem anda.

9.2 Memilih Jadwal Backup yang Baik

Siklus six-tape adalah mudah dipelihara. Ini mencakup empat tape selama satu minggu, satu tape untuk Jumat genap, dan satu tape untuk Jumat ganjil. Lakukan incremental backup setiap hari, dan full backup pada tape Jumat yang tepat. Jika anda membuat perubahan penting atau menambah data penting ke sistem anda, lakukan backup.

9.3 Backup File Database RPM atau Debian Anda

Bila ada penyusupan, anda dapat menggunakan database RPM sebagaimana anda menggunakan tripwire, tetapi hanya bila anda pasti ia belum dimodifikasi. Anda perlu menyalin database RPM ke floppy, dan memeliharanya. Distribusi Debian tampaknya memiliki hal serupa.

Secara khusus, file /var/lib/rpm/fileindex.rpm dan /var/lib/rpm/packages.rpm tidak akan cukup di satu floppy. Kompreslah maka masing-masing akan cukup di floppy terpisah.

Kini, bila sistem anda terganggu, anda dapat menggunakan perintah:

```
root# rpm -Va
```

untuk memverifikasi setiap file di sistem. Lihat man page RPM, ada beberapa pilihan lain yang dapat disertakan untuk membuatkan kurang detil.

Artinya setiap kali RPM baru ditambahkan ke sistem, database RPM perlu diarsip ulang. Anda perlu memutuskan keunggulan versus kelemahan.

9.4 Pelihara Data Akuntansi Sistem Anda

Sangat penting bahwa informasi yang berasal dari syslog belum diganggu. Membuat file dalam /var/log dapat dibaca dan ditulis oleh sejumlah pemakai terbatas adalah awal yang baik.

Yakinkan untuk memperhatikan apa yang ditulis di sana, khususnya dalam fasilitas 'auth'. Banyaknya kegagalan login, sebagai contoh, dapat mengindikasikan usaha break-in.

Ke mana untuk melihat file log anda tergantung pada distribusi anda. Dalam sistem Linux yang sesuai dengan "Linux Filesystem Standard", seperti Red Hat, anda ingin melihat ke /var/log dan memeriksa pesan-pesan, mail.log dan lainnya.

Anda dapat menemukan di mana distribusi anda mencatat dengan melihat pada file /etc/syslog.conf. Ini file yang memberitahu syslogd (the system logging daemon) di mana mencatat berbagai pesan.

Anda mungkin ingin mengkonfigurasi script log-rotating anda atau daemon untuk menjaga log lebih panjang sehingga anda memiliki waktu untuk memeriksanya. Lihat paket 'logrotate' dalam distribusi Red Hat terkini. Distribusi lain juga memiliki proses yang serupa.

Jika file log anda telah diganggu, lihat bila anda dapat menentukan kapan terjadinya, dan hal-hal apa yang diganggu. Apakah ada periode waktu yang tidak dapat dihitung? Periksa tape backup (jika anda punya) untuk file log yang tidak terganggu adalah ide yang baik.

File log umumnya dimodifikasi oleh penyusup dalam rangka menutup jejaknya, tetapi mereka harus juga memeriksa kejadian-kejadian aneh. Anda mungkin memperhatikan penyusup berusaha memperoleh jalan masuk, atau mengeksploitasi program dalam rangka memperoleh rekening root. Anda mungkin melihat masukan log sebelum penyusup memiliki waktu memodifikasi mereka.

Anda harus juga yakin untuk memisahkan fasilitas 'auth' dari data log lain, termasuk usaha untuk mengganti pemakai menggunakan 'su', usaha login, dan informasi akuntansi pemakai lainnya.

Jika mungkin, konfigurasi syslog untuk mengirim salinan data yang paling penting ke sistem yang aman. Hal ini akan mencegah penyusup menutupi jejaknya dengan menghapus usaha login/su/ftp/etc. Lihat syslog.conf man page, dan acu pilihan '@'.

Akhirnya, file log kurang berguna ketika tak seorang pun membacanya. Lihatlah log file anda sewaktu-waktu, dan kenali tampaknya untuk hari normal. Dengan mengetahui hal ini dapat membantu mengenali hal-hal yang tidak biasa.

9.5 Aplikasikan Seluruh Update Sistem Baru

Kebanyakan pemakai Linux menginstal dari CDROM. Oleh karena tingginya fase perbaikan keamanan, program-program baru(perbaikan) selalu dikeluarkan. Sebelum anda menghubungkan mesin anda ke jaringan, adalah ide yang baik untuk memeriksa site ftp distribusi anda (sebagai contoh ftp.redhat.com) dan memperoleh seluruh paket yang diperbaharui sejak anda menerima CDROM distribusi anda. Seringkali paket-paket ini berisikan perbaikan keamanan yang penting, sehingga merupakan ide yang baik untuk menginstal mereka.

10 Apa yang Harus Dilakukan Ketika dan Setelah Break-In

Jadi anda telah mengikuti beberapa nasehat di sini (atau di tempat lain) dan telah mendeteksi breakin? Hal pertama yang harus dilakukan adalah tetap tenang. Tindakan yang ceroboh akan mengakibatkan kerugian yang lebih daripada yang dapat dilakukan penyerang.

10.1 Usaha penggangguan sedang berlangsung

Menemukan gangguan keamanan yang sedang berlangsung dapat menjadi pekerjaan yang berat. Bagaimana anda bereaksi dapat memberi konsekuensi besar.

Jika gangguan yang anda lihat adalah fisik, ganjil bila anda menemukan seseorang yang telah masuk ke rumah anda, kantor atau lab. Anda perlu memberitahu otoritas lokal anda. Dalam setting lab anda mungkin menemukan seseorang berusaha membuka case atau mereboot mesin. Tergantung pada otoritas dan prosedur lokal, anda mungkin meminta mereka untuk berhenti, atau hubungi orang-orang keamanan lokal anda.

Jika anda mendeteksi pemakai lokal berusaha mengganggu keamanan anda, hal pertama yang dilakukan adalah memastikan mereka adalah siapa yang anda pikirkan. Periksa site darimana mereka login. Apakah itu site yang biasa tempat mereka masuk? Kemudian gunakan media non elektronik untuk berhubungan. Sebagai contoh, telpon mereka atau kunjungi kantor/rumah mereka dan berbicara kepada mereka. Jika mereka yakin mereka memang masuk, anda dapat meminta mereka menjelaskan apa yang mereka lakukan atau minta mereka untuk menghentikan hal tersebut. Jika mereka tidak masuk, dan tidak tahu apa yang anda bicarakan, insiden ini tidak memerlukan investigasi lebih lanjut. Lihat insiden-insiden semacam ini, dan ambillah banyak informasi sebelum melakukan tuduhan.

Jika anda mendeteksi gangguan jaringan, hal pertama yang harus dilakukan (jika anda mampu) adalah memutuskan jaringan anda. Jika mereka terhubung melalui modem, putuskan kabel modem, jika mereka terhubung melalui ethernet, putuskan kabel ethernet. Hal ini akan mencegah mereka melakukan kerusakan yang lebih parah, dan mereka mungkin akan melihatnya sebagai masalah jaringan daripada deteksi.

Jika anda tidak mampu memutuskan jaringan (jika anda memiliki site yang sibuk, atau tidak memiliki kendali fisik atas mesin anda), langkah terbaik berikutnya adalah menggunakan sesuatu seperti tcp_wrappers atau ipfwadm untuk menolak akses dari site penyusup.

Jika anda tidak dapat menolak seluruh orang dari site yang sama dengan penyusup, anda dapat mengunci rekening pemakai. Perhatikan bahwa mengunci rekening bukanlah hal yang mudah. Anda harus mengingat file .rhosts, akses FTP, dan host backdoor).

Setelah anda selesai melakukan salah satu langkah di atas (memutuskan jaringan, menolak akses dari site mereka, dan/atau meniadakan rekening mereka), anda butuh membunuh seluruh proses pemakai mereka dan mencatat mereka.

Anda perlu memonitor site anda dengan baik untuk beberapa menit selanjutnya, karena penyerang akan berusaha dan masuk kembali. Mungkin dengan menggunakan rekening yang berbeda, dan/atau dari alamat jaringan yang berbeda.

10.2 Gangguan Keamanan sudah terjadi

Jadi anda telah mendeteksi gangguan yang telah terjadi atau anda telah mendeteksinya dan mengunci (mudah-mudahan) penyerang dari sistem anda. Lalu apa?

10.2.1 Menutup Lubang

Jika anda mampu menentukan cara apa yang digunakan penyerang untuk masuk ke sistem anda, anda perlu berusaha dan menutup lubang itu. Sebagai contoh, mungkin anda melihat beberapa masukan FTP sebelum pemakai login. Tiadakan pelayanan FTP dan periksa dan lihat jika ada versi perbaikan atau daftar perbaikan.

Periksa seluruh log file anda, dan kunjungi list dan halaman keamanan anda dan lihat apakah ada eksploitasi umum baru yang dapat anda perbaiki. Anda dapat menemukan perbaikan keamanan Caldera di *http://www.caldera.com/tech-ref/security*. Red Hat belum memisahkan perbaikan keamanan dengan perbaikan bug, tetapi errata distribusi tersedia di *http://www.redhat.com/errata*. Tampaknya bila satu vendor mengeluarkan perbaikan keamanan, maka vendor Linux lainnya juga akan melakukan hal yang sama.

Jika anda tidak mengunci penyerang, mereka cenderung akan kembali. Tidak hanya ke mesin anda, tetapi kembali ke suatu tempat di jaringan anda. Jika mereka menjalankan paket sniffer, mereka akan memiliki akses ke mesin lainnya.

10.2.2 Memperkirakan Kerusakan

Hal pertama adalah memperkirakan kerusakan. Apa yang telah diganggu? Jika anda menjalankan Integrity Checker seperti Tripwire anda dapat membuat tripwire berjalan dan memberitahu anda. Jika tidak, anda harus melihat seluruh data penting anda.

Oleh karena sistem Linux menjadi semakin mudah diinstal, anda perlu mempertimbangkan menyimpan file config anda dan kemudian menghapus seluruh disk dan melakukan instal ulang, kemudian mengembalikan file-file pemakai dari backup dan config anda. Hal ini akan memastikan bahwa anda memiliki sistem yang bersih. Jika anda memiliki file backup dari sistem yang terganggu, hati-hati terhadap biner yang anda kembalikan karena mungkin itu adalah kuda troya yang ditempatkan oleh penyusup.

10.2.3 Backup, Backup, Backup

Memiliki backup reguler adalah tindakan keamanan yang baik. Jika sistem anda diganggu, anda dapat mengembalikan data yang dibutuhkan dari backup. Tentu saja beberapa data bernilai bagi penyerang juga, dan mereka tidak hanya menghancurkannya, mereka juga mencurinya dan menyalinnya, tetapi paling tidak anda masih memiliki data.

Anda perlu memeriksa beberapa backup masa lampau sebelum mengembalikan suatu file yang telah terganggu. Penyusup mungkin telah mengganggu file anda dahulu, dan anda dapat membuat banyak backup yang berhasil untuk file terganggu!!!

Tentu saja, ada keprihatinan keamanan dengan backup. Pastikan anda menyimpannya di tempat yang aman. Mengetahui siapa yang mengakses mereka. (Jika penyerang dapat memperoleh backup anda, mereka dapat memiliki akses ke seluruh data anda tanpa pernah anda ketahui).

10.2.4 Melacak Penyusup

OK, anda telah mengunci penyusup, dan mengembalikan sistem anda, tetapi anda belum selesai. Meskipun kebanyakan penyusup sangat jarang akan ditangkap, anda perlu melaporkan serangan.

Anda perlu melaporkan serangan ke kontak admin di site di mana penyerang menyerang sistem anda. Anda dapat melihat kontak ini melalui "whois" atau database internic. Anda mungkin mengirimi mereka email dengan seluruh catatan log. Jika anda menjumpai sesuatu yang berbeda tentang penyusup anda, anda mungkin menyebutkannya juga. Setelah mengirimkan email, anda perlu (jika anda begitu ingin) menindaklanjuti dengan telpon. Jika admin tersebut menemukan penyerang anda, mereka mungkin dapat berbicara dengan admin site darimana mereka berasal dan seterusnya.

Hacker yang baik selalu menggunakan sistem perantara. Beberapa (atau banyak) di antaranya bahkan tidak tahu bahwa mereka telah diganggu. Berusaha melacak cracker ke sistem home mereka dapat menjadi sulit. Bersikap sopan dengan admin yang anda ajak bicara akan memudahkan mendapat bantuan dari mereka.

Anda perlu juga memberitahu organisasi keamanan dengan anda sebagai bagiannya (CERT atau yang serupa).

11 Sumber-sumber Keamanan

Terdapat banyak site bagus bagi keamanan UNIX secara umum dan keamanan Linux secara khusus. Sangat penting berlangganan ke satu (atau lebih) milis keamanan dan terus mengikuti perbaikan-perbaikan keamanan. Kebanyakan list ini bervolume sangat rendah, dan sangat informatif.

11.1 Site FTP

CERT adalah Computer Emergency Response Team. Mereka sering mengirimkan peringatan serangan-serangan dan perbaikan terkini. cert.org

Replay memiliki arsip banyak program keamanan. Karena mereka berada di luar AS, mereka tidak perlu mematuhi pembatasan kripto AS. replay.com

Matt Blaze adalah penulis CFS dan penasihat keamanan yang hebat. Barang-barang Matt Blaze's *ftp://ftp.research.att.com/dist/mab*

ftp.win.tue.nl adalah ftp site keamanan yang hebat terdapat di Belanda.

11.2 Site Web

FAQ Hacker adalah FAQ tentang hacker.

Arsip COAST memiliki banyak program keamanan UNIX dan informasi.

Rootshell.com adalah site bagus untuk melihat apa eksploitasi yang sedang digunakan oleh cracker.

BUGTRAQ menaruh nasihat pada isu-isu keamanan.

CERT, Computer Emergency Response Team, menaruh nasihat-nasihat atas serangan umum pada platform UNIX.

Dan Farmer adalah penulis SATAN dan banyak alat keamanan lain, home sitenya memiliki informasi survei keamanan dan juga alat keamanan.

Linux security WWW adalah site yang baik untuk informasi keamanan Linux.

Reptile memiliki banyak informasi keamanan Linux pada sitenya.

Infilsec memiliki mesin kerentanan yang dapat memberitahu anda kerentanan apa yang mempengaruhi platform tertentu.

CIAC mengirim buletin keamanan periodik mengenai eksploitasi umum.

Titik awal baik untuk Linux Pluggable Authentication Module dapat ditemukan di *http://www.kernel.org/pub/linux/libs/pam.*

11.3 Milis

Bugtraq: untuk berlangganan ke bugtraq, kirim surat ke listserv@netspace.org berisi pesan subscribe bugtraq. (lihat link di atas untuk arsip).

CIAC: kirim email ke majordomo@tholia.llnl.gov. Dalam tubuh surat (bukan subyek) taruh : subscribe ciac-bulletin

11.4 Buku - Materi Bacaan Tercetak.

Terdapat sejumlah buku keamanan yang bagus. Bagian ini akan mendaftarkan beberapa. Sebagai tambahan ke buku keamanan tertentu, keamanan dicakup pula dalam sejumlah buku lain mengenai administrasi sistem.

```
Building Internet Firewalls oleh D. Brent Chapman & Elizabeth D. Zwicky
Edisi Pertama September 1995
ISBN: 1-56592-124-0

Practical UNIX & Internet Security, Edisi kedua oleh Simson Garfinkel &
Gene Spafford
Edisi Kedua April 1996
ISBN: 1-56592-148-8

Computer Security Basics oleh Deborah Russell & G.T. Gangemi, Sr.
Edisi Pertama Juli 1991
ISBN: 0-937175-71-4

Linux Network Administrator's Guide oleh Olaf Kirch
Edisi Pertama Januari 1995
ISBN: 1-56592-087-2

PGP: Pretty Good Privacy oleh Simson Garfinkel
Edisi Pertama Desember 1994
ISBN: 1-56592-098-8

Computer Crime A Crimefighter's Handbook oleh David Icove, Karl Seger &
William VonStorch (Consulting Editor Eugene H. Spafford)
Edisi Pertama Agustus 1995
ISBN: 1-56592-086-4
```

12 Daftar Istilah

- Host: Suatu sistem komputer yang terhubung ke suatu jaringan
- Firewall: Sebuah komponen atau seperangkat komponen yang membatasi akses antara jaringan terlindungi dan Internet, atau antara beberapa jaringan lain.
- Bastion Host: Suatu sistem komputer yang harus diamankan dengan baik karena rentan untuk diserang, biasanya karena ia diekspos ke Internet dan merupakan titik utama hubungan pemakai jaringan internal. Ia memperoleh namanya dari proyek penguatan dinding luar benteng jaman dahulu. Bastion melihat area kritis pertahanan, biasanya memiliki dinding yang kuat, ruang untuk pasukan tambahan, dan bak tempat minyak panas untuk menghambat penyerang.
- Dual-homed Host: Sistem komputer serba guna yang paling tidak memiliki dua antar muka jaringan.
- Packet: Unit dasar komunikasi di Internet.
- Packet Filtering: Aksi yang dilakukan device untuk secara selektif mengendalikan aliran data dari dan ke jaringan. Packet filter membolehkan atau memblok paket, biasanya ketika meroute mereka dari satu jaringan ke jaringan lain (kebanyakan Internet ke jaringan internal, dan sebaliknya). Dengan memasang packet filtering, anda mensetup seperangkat aturan yang menspesifikasikan tipe paket (dari atau ke alamat IP atau port tertentu) yang dibolehkan dan tipe apa yang diblok.
- Perimeter network: Jaringan yang ditambahkan antara jaringan terlindung dan jaringan eksternal, dalam rangka memberikan layer tambahan keamanan. Jaringan perimeter kadang disebut DMZ.
- Proxy server: Suatu program yang berkaitan dengan server eksternal atas nama clien internal. Klien proxy berbicara ke server proxy, yang merelay permintaan klien yang disetujui ke server sebenarnya, dan merelay jawaban ke klien.
- Denial of Service: Serangan denial of service adalah ketika penyerang menghabiskan seluruh sumber daya komputer anda untuk hal-hal yang tidak ditujukan untuk dikerjakan, karena itu mencegah pemakaian normal sumber daya jaringan anda untuk tujuan yang sah.
- Buffer Overflow: Gaya pengkodean umum adalah tidak pernah mengalokasikan buffer "cukup besar" dan tidak memeriksa overflow. Ketika buffer tersebut overflow, program yang mengeksekusi (daemon atau set-uid) dapat ditipu untuk melakukan hal lain. Secara umum ini bekerja dengan menulisi alamat kembalian suatu fungsi di stack untuk menunjuk ke lokasi lain.
- IP Spoofing: IP-Spoofing adalah serangan teknis yang rumit yant terdiri dari beberapa komponen. Ini adalah eksploitasi keamanan yang bekerja dengan menipu komputer dalam hubungan kepercayaan bahwa anda adalah orang lain. Terdapat banyak makalah ditulis oleh daemon9, route, dan infinity di Volume Seven, Issue Fourty-Eight majalah Phrack.
- Authentication: Sifat mengetahui bahwa data yang diterima adalah sama dengan data yang dikirim dan bahwa pengirim yang mengklaim adalah benar-benar pengirim sebenarnya.
- Non-repudiation: Sifat bahwa penerima mampu membuktikan bahwa pengirim data benar-benar mengirim data bahkan bilamana pengirim kemudian berusaha menyangkal pernah mengirim data tersebut.

13 Pertanyaan-pertanyaan Yang Sering Diajukan

1. Apakah lebih aman mengkompilasi dukungan driver secara langsung ke dalam kernel, daripada membuatnya jadi modul?

   Jawab: Beberapa orang berpikir bahwa lebih baik untuk meniadakan kemampuan untuk meload device driver menggunakan modul, karena penyusup dapat memuat modul troya atau memuat modul yang dapat mempengaruhi keamanan sistem.

   Namun demikian, dalam rangka memuat modul, anda perlu menjadi root. File obyek modul juga hanya dapat ditulis oleh root. Artinya penyusup perlu akses root untuk menyisipkan modul. Jika penyusup memperoleh akses root, terdapat hal-hal yang lebih serius yang perlu dikhawatirkan daripada apakah ia akan memuat modul.

   Modul adalah untuk dukungan pemuatan secara dinamis untuk device tertentu yang mungkin jarang digunakan. Pada mesin server, atau firewall sebagai contoh, ini sangat jarang terjadi. Oleh karena alasan ini, akan lebih masuk akal untuk mengkompilasi dukungan secara langsung ke kernel untuk mesin yang berfungsi sebagai server. Modul juga lebih lambat daripada dukungan yang dikompilasi secara langsung dalam kernel.

2. Log in sebagai root dari mesin remote selalu gagal. Jawab: Lihat bagian keamanan root. Hal ini dilakukan dengan sengaja untuk mencegah pemakai remote berusaha berhubungan melalui telnet ke mesin anda sebagai root, yang merupakan kerentanan keamanan yang serius. Jangan lupa, penyusup potensial memiliki waktu di pihaknya, dan dapat menjalankan program otomatis untuk menemukan password anda.

3. Bagaimana saya mengadakan shadow password di sistem Linux Red Hat 4.2 atau 5.0 saya ? Jawab: Shadow password adalah mekanisme penyimpanan password anda dalam file selain file /etc/passwd. Hal ini memiliki beberapa keunggulan. Yang pertama adalah file shadow, /etc/shadow, hanya dapat dibaca oleh root, tidak seperti /etc/passwd, yang harus dapat dibaca oleh setiap orang. Keunggulan lain adalah sebagai administrator, anda dapat mengadakan atau meniadakan rekening tanpa setiap orang mengetahui status rekening pemakai lain.

   File /etc/passwd kemudian digunakan untuk mengembalikan name pemakai dan grup, digunakan oleh program seperti '/bin/ls' untuk memetakan ID pemakai ke username yang sesuai dalam listing direktori.

   File /etc/shadow kemudian hanya berisi username dan passwordnya, dan mungkin informasi akuntansi, seperti kapan rekening kadaluarsa, dsb.

   Untuk memasang shadow password, jalankan 'pwconv' sebagai root, dan /etc/shadow perlu ada, dan digunakan oleh aplikasi. Karena anda menggunakan RH 4.2 atau selanjutnya, modul PAM secara otomatis mengadaptasi perubahan dari /etc/passwd normal ke shadow password tanpa perubahan lain.

   Karena anda tertarik pada pengamanan password anda, mungkin anda juga tertarik untuk membuat password yang baik sebagai awal. Untuk hal ini anda dapat menggunakan modul 'pam_cracklib', yang merupakan bagian PAM. Ia membandingkan pustaka Crack dengan password anda untuk membantu anda memutuskan bila ia terlalu mudah diterka oleh program pemecah password.

4. Bagaimana saya mengadakan ekstensi Apache SSL? Jawab:

   (a) Ambil SSLeay 0.8.0 atau selanjutnya dari *ftp://ftp.psy.uq.oz.au/pub/Crypto/SSL*

   (b) Bangun, coba dan instalah!

   (c) Ambil sumber Apache 1.2.5
   (d) Ambil Apache SSLeay extensions dari
   (e) Buka di dalam direktori sumber apache-1.2.5 dan patch Apache sesuai README.
   (f) Konfigurasi dan bangunlah.

   Anda mungkin juga ingin mencoba Replay Associates yang memiliki banyak paket sudah dibangun, dan terletak di luar Amerika Serikat.

5. Bagaimana saya memanipulasi rekening pemakai, dan masih mempertahankan keamanan ? Jawab: Distribusi Red Hat, terutama RH 5.0, berisi sejumlah tool bagus untuk merubah properti rekening pemakai.

   - Program pwconv dan unpwconv dapat digunakan untuk mengkonversi dan mengkonversi balik antara password shadow dan non-shadowed
   - Program pwck dan grpck dapat digunakan untuk memverifikasi organisasi file passwd dan grup yang tepat.
   - Program useradd, usermod, dan userdel dapat digunakan untuk menambah, menghapus dan mengubah rekening pemakai. Program groupadd, groupmod, dan groupdel akan melakukan hal yang sama untuk grup.
   - Password grup dapat dibuat dengan gpasswd.

   Seluruh program ini 'shadow-aware' – yaitu; jika anda mengadakan shadow ia akan menggunakan /etc/shadow untuk informasi password, sebaliknya ia tidak akan.

   Lihat man page yang sesuai untuk informasi lebih lanjut.

6. Bagaimana saya memproteksi dengan password dokumen HTML tertentu menggunakan Apache? Saya bertaruh anda tidak tahu tentang *http://www.apacheweek.org* bukan ?

   Anda dapat menemukan informasi tentang User Authentication di *http://www.apacheweek.com/features/userauth* juga tip keamanan server web lainnya dari *http://www.apache.org/docs/misc/security_tips.html*

14 Kesimpulan

Dengan berlangganan milis peringatan keamanan, dan selalu mengikuti perkembangan, anda dapat melakukan banyak hal untuk mengamankan mesin anda. Jika anda memperhatikan file-file log anda dan menjalankan sesuatu seperti tripwire secara rutin, anda dapat melakukan yang lebih jauh lagi.

Tingkat keamanan komputer yang cukup tidak sulit dipelihara untuk mesin rumahan. Upaya lebih banyak dibutuhkan oleh mesin bisnis, tetapi Linux dapat menjadi platform yang aman. Oleh karena sifat pengembangan Linux, perbaikan keamanan sering dikeluarkan lebih cepat daripada pada sistem operasi komersil, membuat Linux platform yang ideal ketika keamanan menjadi suatu persyaratan.

15 Terima Kasih Kepada

Informasi di sini dikumpulkan dari berbagai sumber. Terima kasih kepada yang telah berkontribusi baik secara langsung maupun tidak langsung:

```
Rob Riggs <rob@DevilsThumb.com>
S. Coffin <scoffin@netcom.com>
Viktor Przebinda <viktor@CRYSTAL.MATH.ou.edu>
Roelof Osinga <roelof@eboa.com>
Kyle Hasselbacher <kyle@carefree.quux.soltec.net>
"David S. Jackson" <dsj@dsj.net>
"Todd G. Ruskell" <ruskell@boulder.nist.gov>
Rogier Wolff <R.E.Wolff@BitWizard.nl>
```

16 Catatan Penerjemah

Diterjemahkan oleh *Tedi Heriyanto*

Tanggal 29 Maret 1999.

Kritik, saran atau komentar mengenai terjemahan ini, silakan kirimkan ke email saya.