18. Sicurezza in Linux

Tanti utenti di computer hanno verso la sicurezza informatica un atteggiamento molto disinvolto. Credono che prendere precauzioni contro intrusioni informatiche sia necessario quanto portare con sé lo spray accecante per difendersi in caso di *avances* pesanti da parte di Claudia Schiffer.

"Tanto a me non capita". Il fatto è che invece capita, ma non se ne accorgono. Ricordo ancora quanto mi ha lasciato scioccato l'installazione di ZoneAlarm (un firewall per Windows, prelevabile gratuitamente da http://www.zonelabs.com). Mi sembrava di navigare tranquillo, come un pesce qualsiasi nel mare degli utenti; poi ho attivato ZoneAlarm e ho scoperto invece quanta gente, a mia insaputa, veniva a sbirciare alla mia finestra su Internet, risalendo su per il filo del telefono fino ad essere fermata soltanto dalla presenza del firewall (e di una configurazione un po' prudente di Windows). È stato come svegliarsi e trovare un ladro in casa.

Figura 18−1. ZoneAlarm rivela i tentativi di incursione in Windows durante l'accesso a Internet.

Molti utenti sono attratti da Linux per la sua reputazione in fatto di sicurezza, soprattutto per quanto riguarda Internet. Ma attenzione: se c'è una cosa che Odo è riuscito a inculcarmi durante la lavorazione di questo libro, è che l'illusione della sicurezza è più pericolosa della mancanza di sicurezza.

Faccio un paragone: immaginate due persone che viaggiano in autostrada. Una guida una Saab nuova di zecca, con airbag, ABS, cinture con pretensionatori e barre anti−intrusione. L'altra guida una Fiat 850 del 1975, con le gomme lisce, i freni sballati e il volante allentato. Improvvisamente la sezione centrale del ponte che stanno imboccando crolla: a cinquanta metri davanti a loro si è aperto un baratro. Secondo voi, chi si salva?

La Fiat, perché il suo conducente, consapevole di essere su una bagnarola, andava molto piano e teneva gli occhi aperti. L'altro, confidando nelle tecnologie del suo bolide, filava come un pazzo mentre parlava al telefonino. La sua protezione non contemplava questo tipo di imprevisto.

Lo stesso ragionamento vale per la sicurezza informatica. La sicurezza non si compra; bisogna guadagnarsela. Non illudetevi che basti installare Linux per essere totalmente blindati contro le intrusioni. Linux è in effetti un sistema operativo molto sicuro, ma soltanto se lavorate per impostarlo correttamente e tenete gli occhi ben aperti, altrimenti la protezione è solo apparente.

Nonsolospie

Inoltre la sicurezza non è soltanto una questione di difendere i propri dati dagli sguardi indiscreti degli intrusi. Per la maggior parte degli utenti, soprattutto quelli alle prime armi o che condividono il proprio computer con altre persone, la vera priorità in fatto di sicurezza è difendersi dai pasticcioni.

E sia ben chiara una cosa: il pasticcione più pericoloso di tutti, specialmente in questa fase di apprendimento, siete proprio voi. È per questo che vi ho raccomandato, e continuerò a raccomandarvi, di usare l'utente *root* esclusivamente per la manutenzione e soltanto dopo averci pensato attentamente e dopo aver creato una copia di sicurezza di tutti i file che modificate.

I maldestri, tuttavia, esistono anche in Internet. Uno dei motivi per cui potreste trovarvi vittima di un'incursione è semplicemente il gusto della sfida o la curiosità di un aspirante hacker (dove per *hacker* si intende semplicemente uno che si diverte a studiare a fondo il funzionamento delle cose e specialmente dei computer). Per questo motivo qualunque computer collegato a Internet può subire intrusioni, magari benevole, magari no, e magari maldestre: l'hacker non voleva far danni, ma li ha fatti involontariamente.

Per semplicità di esposizione, in questo capitolo userò la parola *intruso* per indicare sia chi aggredisce intenzionalmente il vostro Linux, sia chi gli arreca danni involontari.

La sicurezza totale non esiste

Toglietevi subito dalla testa l'idea che possiate blindare completamente il vostro computer. Un intruso sufficientemente deciso riuscirà comunque, alla fine, a penetrarvi. Magari con metodi poco informatici (pistola puntata, furto del computer, eccetera), ma ci riuscirà.

Altra idea da eliminare subito: questo capitolo non spiega *tutto* quello che c'è da sapere. È, come il resto del libro, soltanto una guida introduttiva all'argomento. Ci sono ottimi manuali e interi siti Internet dedicati alla sicurezza informatica in Linux e in Windows, e ogni giorno si scoprono tecniche nuove di intrusione e, corrispondentemente, nuove misure di protezione. Restare aggiornati è fondamentale.

Non è comunque il caso di farsi prendere dal panico e dalla paranoia. La sicurezza totale non esiste, ma la sicurezza ragionevole sì. Occorre sempre trovare un compromesso fra quello che bisognerebbe fare in teoria e quello che si riesce a fare in pratica. Questo è l'approccio che troverete qui.

Vi presenterò qualche suggerimento di sicurezza, con il contributo preponderante di Odo, su due livelli:

- la protezione da incursioni *fisiche*, nel senso di ciò che una persona (o un utente sbadato) può fare se ha modo di sedersi davanti al vostro computer;
- la protezione da incursioni *via Internet* o tramite rete locale.

A entrambi i livelli, gran parte dei sistemi di protezione si basa sull'uso di password. È da qui che cominciamo.

Password innanzi tutto

Le password sono il cardine su cui poggia la maggior parte delle tecniche di sicurezza. Potete usare le tecniche più sofisticate al mondo, ma se le adoperate con password scadenti, l'intruso avrà gioco facile. Qualunque cosa facciate, vi servono delle buone password. Ecco un po' di suggerimenti su come *non* crearle.

Qualche cattivo esempio

Un sondaggio condotto dalla Visa (quella delle carte di credito) verso la metà del 2000 ha rilevato che il 67% delle password scelte per proteggere le informazioni consiste di nomi o numeri facili da indovinare. La maggior parte delle persone sceglie come password la propria data di nascita, il proprio nomignolo o la squadra sportiva preferita.

Di solito si pensa che un pirata informatico debba disporre di chissà quali diavolerie per poter scoprire i codici di accesso delle proprie vittime. Mica vero. Il peggior nemico dell'utente è l'utente stesso, con la sua sbadataggine, pigrizia e indifferenza ai problemi della sicurezza.

Che l'utente medio si ponga pochi problemi di sicurezza lo posso anche capire e perdonare. Ma che personalità di spicco come il presidente americano Bill Clinton diano il cattivo esempio mi impensierisce non poco. Di recente ha firmato con gran pompa la legge americana che autorizza l'uso delle firme digitali: un codice univoco usa e getta che identifica il firmatario perché solo lui conosce la password che può generare quel codice.

Secondo la legge, in Italia come negli USA, se c'è il codice di una persona in calce a un documento, vuol dire che il documento è stato firmato da quella persona. La firma digitale ha insomma valore legale esattamente come la firma tradizionale. Ovviamente, visto l'argomento, Clinton ha firmato usando una firma digitale. Be', sapete che password ha usato per la propria firma? Il nome del suo cane: *Buddy*. Confido che usi delle password un po' più robuste per proteggere la valigetta nucleare.

Ecco la classifica delle password più comuni, secondo il sondaggio Visa:

1. il proprio nome o nomignolo (19%)
2. il nome o nomignolo del proprio partner (11%)
3. la propria data di nascita o segno zodiacale (11%)
4. la squadra per cui si tifa (8%)
5. la località dove si va in vacanza (8%)
6. la popstar preferita (5%)
7. il proprio luogo di nascita (5%)

Qualche buon esempio di password

Ovviamente non posso scrivere qui un elenco di password da usare. Posso soltanto spiegarvi alcune regole generali su come si crea una buona password.

- Non usate nessuna delle voci citate nella classifica.
- Non usate nomi propri o parole di senso compiuto, nemmeno se le scrivete a ritroso o le racchiudete fra asterischi o fra X o simili.
- Mescolate lettere e cifre, come in *a47bxc12*, ma non sostituite la I con la cifra 1, la O con lo zero, la E con il 3 e la A con il 4 per creare parole di senso compiuto facili da ricordare come C*3S1R4* ("Cesira"). È un vecchio trucco, e tutti i programmi di *cracking* (decifrazione) delle password lo conoscono bene.
- Se possibile, usate le maiuscole e le minuscole, come in *46FcA7AAq*.
- Se possibile, usate anche i segni di punteggiatura, come in *!47mcP;aa45*.

- Non scrivete la password su un'etichetta sul bordo del monitor. Non sto scherzando, capita spesso: sapeste quante volte mi è capitato di entrare in un ufficio e vedere la password scritta in bella mostra in questo modo. Odo mi dice che c'è ad esempio un server AIX di un ospedale lombardo che ha la password di *root* appiccicata al monitor.
- Non usate la stessa password per proteggere più di un'informazione (ad esempio l'abbonamento a Internet e il vostro accesso al Bancomat).
- Non rivelate mai le vostre password per telefono a chiunque, anche se il vostro interlocutore si spaccia per un addetto all'assistenza tecnica o simile.
- Non sceglietevi una password che fate fatica a digitare: se siete costretti a scriverla lentamente, è più facile da decifrare per chi sbircia.
- Cambiate spesso le password che usate.

Queste regole, fra l'altro, non valgono soltanto per l'attività informatica: dovreste applicarle anche al PIN che protegge la tessera Bancomat, a quello che evita l'uso illecito del vostro telefonino, al codice che controlla l'allarme antifurto in casa, e così via.

Ricordarsi una buona password

Il problema delle password che non hanno senso compiuto è che sono dannatamente difficili da ricordare. Odo suggerisce un trucco per facilitare l'impresa: usate le lettere iniziali delle parole di un verso di una poesia o di una canzone.

Ad esempio, *Nel mezzo del cammin di nostra vita* diventa *Nmdcdnv*; *Io penso positivo perché son vivo perché son vivo* genera *ipppsvpsv*. *Quarantaquattro gatti in fila per sei col resto di due* produce una password davvero eccezionale: *44gifp6crd2*.

Un altro metodo che potete usare è scrivere da qualche parte una frase che vi ricordi qual è la password grazie a un indizio che solo voi potete capire (ad esempio *Canzone dei Beatles preferita*).

Tecnologia del cracker

Non mi riferisco al prodotto alimentare friabile, ma al "cugino cattivo" dell'hacker: un intruso che cerca di decifrare le vostre password. Sapere come opera un cracker, oltre a essere molto educativo, vi renderà più chiari i motivi dei consigli che ho appena dato.

La prima cosa che fa un buon cracker è informarsi su di voi e tentare manualmente le password più ovvie (quelle citate nella classifica). In genere questo è sufficiente: sapeste quanti siti Internet sono protetti da password patetiche.

Se però la password è scelta con un minimo di criterio, il cracker cambia tattica: con uno dei tanti facili stratagemmi disponibili, si procura una copia del file che contiene le password del vostro computer (in Linux le password sono in */etc/passwd* e/o in */etc/shadow*) e la analizza con un programma che tenta automaticamente tutte le parole del dizionario: sono tante, ma alla velocità del computer si fa in fretta a farle passare. Se anche questo fallisce, prova con le sequenze di numeri e le varianti "semplici" (1 al posto della I e simili, parole scritte a rovescio, eccetera). Anche questo è un tentativo relativamente rapido.

Se però non ha successo, è necessario ricorrere alla forza bruta: tentare tutte le possibili combinazioni di lettere maiuscole e minuscole, numeri, segni di punteggiatura eccetera. Siccome questo tipo di approccio richiede molta potenza di calcolo oppure molto tempo, viene adottato per gradi: prima si tentano le combinazioni di sole lettere, poi quelle di soli numeri, poi lettere e numeri insieme, e così via, arrivando alla punteggiatura soltanto dopo aver tentato tutte le altre strade.

È per questo che password di senso compiuto sono considerate facili, mentre la combinazione di lettere maiuscole e minuscole, numeri e punteggiatura è più sicura: il tempo necessario per la decifrazione è immensamente maggiore. Facciamo due conticini molto spannometrici. Gli esperti di crittografia mi perdoneranno le semplificazioni.

Volendo essere abbondanti, le parole di senso compiuto sono circa centomila. Una password di sole sette lettere minuscole o maiuscole senza senso compiuto può avere circa otto miliardi di combinazioni (26 moltiplicato per se stesso sette volte), e quindi richiede *ottantamila* volte più tempo di una password di senso compiuto.

Non male. Ma una password di lettere maiuscole e minuscole (totale 52 caratteri), cifre (altri 10 caratteri) e punteggiatura (altri 25 caratteri circa) ha circa trentasettemila miliardi di combinazioni (87 moltiplicato per se stesso sette volte); richiede cioè un tempo 470 volte maggiore di una password di sole lettere senza senso.

Adesso potete confrontare i livelli di sicurezza offerti dai vari tipi di password, ma non dimenticate una cosa fondamentale: grazie alla potenza di calcolo dei computer (e spesso il cracker usa più computer in parallelo, magari non suoi) è comunque solo questione di tempo prima che anche la password più sicura venga svelata. Di conseguenza bisogna cambiare password spesso, in modo che il cracker non abbia tempo sufficiente per i suoi tentativi.

Primo livello: sicurezza fisica

Vi racconto qualche tecnica abbastanza semplice per rendere più difficile la vita a chi ha modo di accedere fisicamente al computer, sia in casa, sia sul posto di lavoro. Sia ben chiaro, nessuna di queste soluzioni vi proteggerà contro un intruso particolarmente determinato e che abbia molto tempo a disposizione, perché gli basta arrivare con un cacciavite e asportare il disco rigido dal computer. Tuttavia queste semplici precauzioni basteranno a scoraggiare la maggior parte dei curiosi e sicuramente bloccheranno i maldestri.

Se siete realmente affetti da esigenze di sicurezza tali che è plausibile che qualcuno vi rubi il computer per i dati che contiene, considerate l'adozione di un *filesystem cifrato* (*encrypted filesystem*) in Linux e/o in Windows. Un ottimo programma per questo tipo di protezione è *BestCrypt* (http://www.jetico.com), disponibile sia per Windows, sia per Linux. Non impedirà che vi rubino il computer, ma perlomeno non potranno leggerne il contenuto.

Presa di corrente e pulsante di reset

Lo so che sembra sciocco preoccuparsi della presa di corrente, ma nessuna delle protezioni che descriverò nelle pagine successive ha molto senso se chiunque può allungare una mano e staccare la spina del computer (o inciampare nel cavo di alimentazione), causando un collasso immediato della macchina.

Lo stesso discorso vale per l'eventuale pulsante di reset sul corpo del computer: è consigliabile disattivarlo (basta scollegare i fili) o bloccarlo fisicamente in modo che solo voi possiate premerlo quando serve.

Più in generale, è senz'altro consigliabile rendere difficile accedere fisicamente al computer (specificamente alla CPU, cioè alla "scatola" che contiene tutta la ferraglia). Questo consiglio diventa un obbligo se avete bambini in casa: le lucine del computer e i suoi pulsanti sono una tentazione irresistibile, e le fessure dei drive sono un ricettacolo ideale per pezzetti di carta, tessere di *puzzle* e quant'altro. Ne so qualcosa grazie a Linda e Lisa, le mie due gemelline.

Password di boot nel BIOS

Praticamente tutti i computer hanno nel BIOS (o *setup*) l'opzione di protezione tramite password. Attivandola, soltanto chi conosce la password può avviare il computer. Esistono tecniche piuttosto semplici per scavalcare questa protezione, ma richiedono una certa competenza; comunque la password sul BIOS è un ostacolo in più da superare.

Sequenza di boot

Il BIOS o setup del computer definisce anche l'ordine in cui la macchina analizza i drive alla ricerca di un sistema operativo da caricare: in termini tecnici, quest'ordine si chiama *sequenza di boot*. Impostatela, se potete, in modo che il computer cerchi prima sul disco rigido e poi sul floppy, anziché il contrario (che è la norma), e che non cerchi del tutto sul CD−ROM.

Ovviamente, se usate un dischetto per avviare Linux, questa soluzione non è praticabile.

Antivirus nel BIOS

Il BIOS di molti computer ha anche una rudimentale protezione antivirus, che blocca l'accesso al Master Boot Record del disco rigido, cioè al posto dove si insediano parecchi virus e programmi analoghi di intrusione. Una volta conclusa l'installazione di Linux, attivatela. Ricordatevi di disattivarla se dovete modificare il Master Boot Record, ad esempio in occasione di una modifica di LILO.

Password su LILO

Normalmente, per avviare Linux è sufficiente battere Invio quando compare la schermata grafica di scelta del sistema operativo (in Red Hat 7.0) o il prompt *LILO* (in Red Hat 6.2) durante l'avvio del computer. Per impedire a un intruso di avviare Linux, potete proteggere LILO con una password.

Modificate il file */etc/lilo.conf* in modo da includere l'opzione *password*, come mostrato in Figura 18−2 e in Figura 18−3. Nel primo caso, la password viene chiesta sempre e comunque, sia che si voglia avviare Windows, sia che si desideri avviare Linux; nel secondo viene chiesta soltanto sull'avvio di Linux, mentre l'avvio di Windows non è protetto da password.

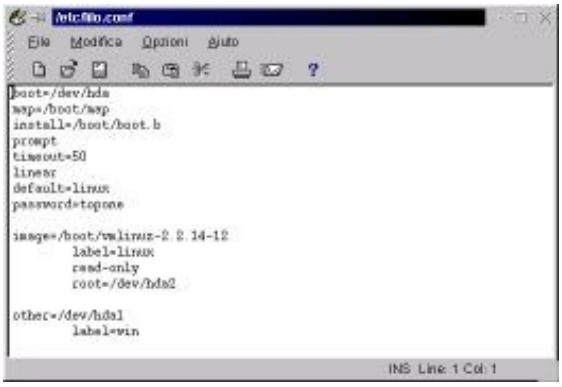

Figura 18−2. Configurazione di */etc/lilo.conf* per proteggere sia Windows, sia Linux.

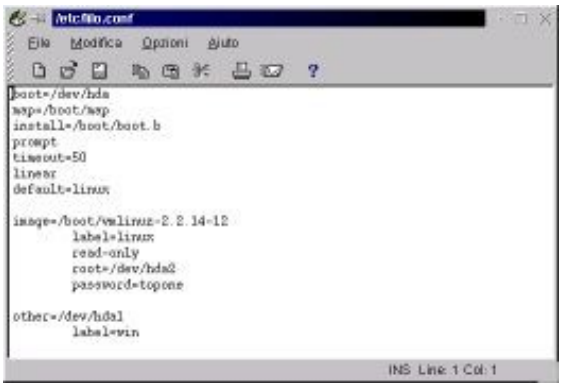

Figura 18−3. Configurazione per proteggere soltanto Linux.

Eseguite */sbin/lilo* per aggiornare il Master Boot Record (ovviamente la protezione a livello BIOS sull'MBR deve essere temporaneamente disattivata). Riavviate il computer: LILO vi chiederà la password prima di lasciarvi proseguire.

Un'altra forma di protezione di LILO che potreste trovare interessante è data dal parametro *restricted*, da aggiungere dopo *password*: consente il normale avvio di Linux (o di Windows) senza disturbarvi con richieste di password, ma protegge con la richiesta di password ogni tentativo di avviare Linux aggiungendo parametri dopo la normale risposta al prompt di LILO.

In altre parole, se digitate **linux** non vi verrà chiesta la password; se digitate qualsiasi cosa oltre a **linux**, ad esempio **linux −s** per scavalcare la password di root come descritto più avanti, vi verrà richiesta la password.

Attenzione: la password che protegge l'avvio di LILO è scritta *in chiaro* nel file */etc/lilo.conf*, per cui chiunque può leggerla se trova Linux già avviato. Modificate i diritti di lettura di questo file in modo che sia leggibile soltanto da *root*: accedete come *root* e date i comandi **chmod −r /etc/lilo.conf** e **chown root.root /etc/lilo.conf**. Un intruso che avvia Windows e adopera Explore2fs riuscirà comunque a leggere il file e carpirvi la password, ma perlomeno dovrà tribolare un po'.

Uso cauto del comando su e delle sessioni di root

Quando usate il comando **su** per passare dall'utente *root* all'utente normale, è facile dimenticarsi che siete onnipotenti, perché avete davanti agli occhi il prompt dell'utente normale (l'unico promemoria del fatto che avete i poteri di *root* è il fatto che il prompt termina con un cancelletto anziché col dollaro). Ricordatevi sempre di uscire dalla sessione digitando **exit**. Se avete sovrapposto più sessioni **su**, uscite da ciascuna.

Non lasciate mai incustodita una sessione di questo tipo: l'intruso potrebbe essere più osservatore di voi e notare il cancelletto, potendo quindi lavorare come *root*, ad esempio per crearsi un accesso da remoto da usare in seguito o semplicemente fare strage dei vostri file.

Più in generale, non dovete mai allontanarvi dal computer quando c'è aperta una sessione dell'utente *root*. Chiunque può passare di lì e far danni.

Che danni fa un intruso che diventa *root*?

Una volta che un intruso si trova a disposizione una sessione di *root* incustodita, può divertirsi in molti modi. Ne accenno soltanto alcuni per darvi un'idea di quanto sia rapido e facile carpire informazioni pericolose se lasciate il computer alla mercé del primo che passa. Ciascuna delle intrusioni descritte qui richiede meno di un minuto.

- **Rubare la password di accesso a Internet.** Dato che oggigiorno gli accessi a Internet non sono cari, non è la facoltà di collegarsi a Internet che fa gola all'intruso: è l'occasione di collegarsi spacciandosi per voi. Questo gli consente di commettere qualsiasi reato e di far ricadere la colpa su di voi. Leggete bene il vostro contratto di accesso a Internet: siete legalmente responsabili di qualunque atto compiuto usando il vostro nome di login e la vostra password di accesso alla Rete. La password, fra l'altro, è in chiaro, nel file */.kde/share/config/kppprc* contenuto nella home directory di ciascun utente.
- **Copiare i file */etc/passwd* e */etc/shadow*.** Questi file contengono i nomi degli utenti e le loro password. Le password sono in forma cifrata, ma basta dare in pasto la copia del file a un programma di *cracking* e in capo a qualche giorno (nel caso peggiore) l'intruso avrà trovato le password di tutti gli utenti. In sostanza, copiando questi due file è come se un ladro si portasse via una copia delle chiavi di casa, per poi poter tornare a suo piacimento.
- **Cancellare il vostro disco rigido con un solo comando**. No, non ho intenzione di dirvi qual è. Studiate e lo scoprirete.
- **Cambiarvi la password di root** e chiudere la sessione di *root*. Questo equivale sostanzialmente a un intruso che vi chiude fuori di casa vostra cambiandovi tutte le serrature.

Screensaver inutili

Potreste essere tentati di proteggere una sessione di Linux usando lo screensaver dotato di password (attivabile dal Pannello con il pulsante Blocca schermo). Come no. State dimenticando che siete in Linux, non in Windows: lo screensaver protegge soltanto la sessione grafica, ma lascia completamente scoperte le console.

L'intruso non deve fare altro che digitare Ctrl−Alt−tasto funzione (da F1 a F6) per avere una console a disposizione. Se è fortunato e voi siete sbadati, troverà qualche console in cui è già stato fatto login, per cui potrà dare un'occhiatina in giro (se il login è quello di *root*, potrà fare tutto quel che gli pare).

Disattivare Ctrl−Alt−Canc

Una cosa che di certo non gradireste è che un burlone passasse davanti al computer e ve lo riavviasse premendo semplicemente **Ctrl−Alt−Canc** in una console.

Per impedire questa nefasta possibilità, modificate il file */etc/inittab*, alla riga che inizia con *ca::ctrlaltdel*, facendola diventare commento, cioè prefissandola con un carattere "#". Anzi, per ricordarvi che siete stati voi a trasformarla in commento, prendete l'abitudine di usare *due* simboli di cancelletto in tutti i file che modificate.

Una volta salvato il file e riavviato Linux, la combinazione di tasti **Ctrl−Alt−Canc** non avrà più alcun effetto.

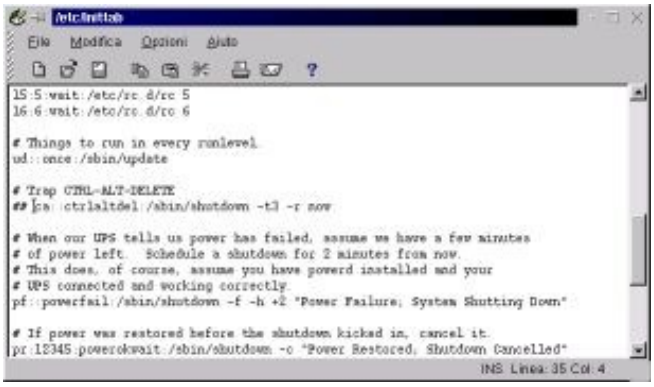

Figura 18−4. Modificare il file */etc/inittab* per evitare scherzi.

Ovviamente questa modifica ha il risultato che non potete usare Ctrl−Alt−Canc neppure intenzionalmente per tirarvi fuori da una situazione in cui dovete chiudere Linux ma non riuscite a farlo con altri mezzi.

Se volete, invece di cambiare le impostazioni di */etc/inittab* potete modificare il file */etc/shutdown.allow*, scrivendovi *root*, in modo che Ctrl−Alt−Canc funzioni, ma soltanto se l'utente *root* ha una sessione attiva. In questo modo il buontempone di passaggio non potrà fare danni (sempre che non siate così incauti da lasciare una sessione di *root* aperta), ma voi avrete la possibilità di usare Ctr−Alt−Canc quando vi serve.

Un altro modo per contenere i danni che può produrre un intruso è cambiare il contenuto della riga già citata di */etc/inittab* in modo che al posto di *shutdown −r*, che riavvia il sistema, ci sia *shutdown −h*, che lo chiude ordinatamente senza riavviarlo.

In questo modo, l'eventuale gesto sconsiderato dell'intruso aumenterà le difese del vostro Linux, dato che l'intruso dovrà superare la password sul BIOS, la password su LILO e la password di login prima di riuscire a fare qualcosa di concreto. È un po' come un antifurto che blocca tutte le porte in caso di tentativo di intrusione.

Disattivare Ctrl−Alt−Backspace

Questa combinazione di tasti consente di chiudere piuttosto brutalmente l'interfaccia grafica ed è quindi interessante per i buontemponi. Se volete impedire che nuocciano e prenderli in castagna, modificate il file */etc/X11/XF86Config*. Cercate la sezione *Server flags* e, poco più sotto, la riga che inizia con *#DontZap*.

Togliendo il simbolo di cancelletto da questa riga e riavviando il server X (l'interfaccia grafica, insomma), la combinazione di tasti sarà disabilitata.

Scavalcare la password di root

Una delle buone ragioni per cui conviene mettere una password su LILO è che è molto facile usare LILO per scavalcare le password di login e accedere completamente al sistema senza conoscere la password di *root*. Vi spiego come si fa non soltanto per dimostrarvi quanto è importante proteggere LILO, ma anche perché potrebbe capitarvi di dimenticarvi la password di root e quindi non riuscire più a fare la manutenzione del vostro Linux.

Certo che se mettete la password su LILO e ve la dimenticate, e in più vi siete dimenticati anche la password di root, avete due problemi:

- il primo è che l'installazione di Linux è da rifare (salvo smontare il disco e rimontarlo su un'altra macchina che ha un Linux funzionante, o avviare dal floppy d'emergenza);
- il secondo è che la vostra memoria fa veramente schifo.

Ma torniamo a noi. Per scavalcare la password di root procedete come segue. All'avvio, in Red Hat 7.0, quando compare la schermata grafica iniziale di scelta fra Linux e Windows digitate **Ctrl−X** per uscire dalla schermata grafica e poi **linux −s**; in Red Hat 6.2, quando compare la richiesta di LILO, digitate direttamente **linux −s**. Attenzione: all'avvio la tastiera non è ancora impostata sulla configurazione italiana, per cui il trattino non è al solito posto. Potete usare quello presente sul tastierino numerico oppure premere il tasto che reca il simbolo di apostrofo.

Questo fa comparire il prompt *bash*. In pratica avete avviato un Linux "minimo" che non chiede password. Non funziona l'interfaccia grafica, per cui dovete destreggiarvi con i comandi dell'interfaccia testuale. Non che ce ne vogliano molti: basta digitare **/usr/bin/passwd**. Vi verrà chiesta due volte la nuova password che volete dare a *root*, senza chiedere quella vecchia. Fatto questo, riavviate e il gioco è fatto.

Ora siete convinti dell'utilità di proteggere LILO con una password?

Secondo livello: sicurezza di rete

Per un intruso, una macchina Linux è più appetibile di una su cui gira Windows. Siccome in genere chi usa Linux è piuttosto bravo in informatica, è probabile che usi massicciamente il computer per lavoro e quindi vi depositi informazioni importanti.

Inoltre Linux viene spesso utilizzato per servizi Internet avanzati (ad esempio come web server o come firewall in ambienti commerciali), per cui "bucare" un computer di questo tipo può portare a ricompense più stimolanti: si va dal riscrivere le pagine Web di un sito al carpire numeri di carta di credito, passando per la contabilità aziendale.

Infine, le macchine Linux sono interessanti perché sono spesso collegate permanentemente a Internet. Di conseguenza sono un'ottima testa di ponte per attacchi informatici basati sull'esecuzione simultanea di programmi depositati furtivamente su decine o centinaia di computer altrui, come i *distributed denial of service* (DDOS) che hanno colpito i più importanti siti commerciali di Internet (Yahoo, eBay, Amazon) nei mesi scorsi.

La sicurezza di rete in Linux è quindi orientata non tanto verso i virus, che invece sono la principale minaccia per Windows, quanto verso la protezione contro le intrusioni. Chi attacca una macchina Linux non vuole piantarvi un virus: vuole acquisire l'accesso come *root*.

In questa sezione del capitolo vi presento un po' di consigli su come blindare una macchina Linux, sia verso Internet, sia verso altri utenti di una rete locale. Come, anche contro le intrusioni dei colleghi di lavoro e degli amici? Certamente. Innanzi tutto, se vi fate di questi scrupoli, si vede che non avete idea delle cattiverie che avvengono in un vero posto di lavoro. In secondo luogo, è inutile blindare la vostra macchina se le altre alle quali è collegata sono lasciate spalancate: l'intruso le userà per aggirare le vostre difese. Vi dice niente l'espressione *linea Maginot*?

Le regole fondamentali sono queste:

- Riducete al minimo indispensabile i servizi di rete. Ogni servizio è un possibile appiglio per il piede di porco digitale dell'intruso.
- Chiudete tutti gli accessi ai programmi e servizi di rete non necessari e riapriteli manualmente solo quando avete ottime ragioni per farlo e soltanto per il tempo strettamente necessario.
- Fate un elenco degli utenti di cui potete fidarvi ciecamente e consentite solo a loro di accedere ai servizi di rete indispensabili.
- Verificate periodicamente i file di log di Linux. Ogni accesso, o tentativo di accesso, viene registrato nei file presenti in */var/log* (ad esempio in *messages* e *secure*). Su Internet troverete programmi che esaminano automaticamente questi file alla ricerca di anomalie (ad esempio 1000 tentativi di login, uno al secondo, alle 4 del mattino). Potete anche sorvegliare i messaggi d'errore in tempo reale modificando il file */etc/syslog.conf* in modo da includere una riga che specifichi ***.* /dev/tty12**: i messaggi verranno trasmessi anche alla console 12, che si porta sul monitor con **Ctrl−Alt−F12** o **Alt−F12**.
- Non eseguite *mai* programmi o pacchetti d'installazione di dubbia provenienza.

Alcune di queste regole si spiegano da sole. Vi spiego brevemente quelle che richiedono un po' di lavoro per essere messe in pratica.

Ridurre i servizi disponibili: la teoria

Come già accennato nel Capitolo 17, i servizi di rete in Linux sono gestiti tramite programmi chiamati *demoni*. Ad esempio, per trasferire file da un computer Windows a una macchina Linux potreste usare ftp. Quando lanciate il

programma per ftp sulla macchina Windows, quest'ultima manda all'altra una richiesta di attivare il demone *ftpd*.

Se il demone ftpd risponde automaticamente, offre un appiglio all'intruso. È un po' come bussare a una porta chiusa: se qualcuno risponde, può darsi che chi bussa riesca a farsi aprire, raccontando qualche bugia molto convincente o insistendo e implorando. Ma se non risponde nessuno, la parlantina dell'aspirante intruso non ha speranze.

Fate un esame molto critico della vostra attività e valutate attentamente quali servizi di rete usate e quali no (magari non ne usate nessuno). Ricordate che ciascuno dei demoni, se lasciato attivo, può fare da breccia per un'intrusione devastante. Disattivate tutto quello che non usate, e ricordate che state soltanto disabilitando la risposta automatica: potete sempre rispondere manualmente se e quando lo decidete voi. Ecco un po' di spunti:

- Prevedete di consentire l'accesso al vostro computer da altre macchine? Assicuratevi di avere una ragione veramente buona per farlo, e se lo dovete fare, *non usate telnet*: chiunque può leggere il flusso di dati di una sessione telnet ed estrarne nome di login e password. Usate invece *ssh* (se avete la distribuzione Red Hat 6.2) oppure *openssh* (se avete la 7.0), entrambi descritti nel Capitolo 19, che consentono l'accesso remoto protetto con sistemi di crittografia. Comunque sia, disattivate il servizio telnet.
- Vi serve davvero a qualcosa permettere agli altri di fare finger al vostro computer? Non avete la più pallida idea di cosa voglia dire "fare finger"? Benissimo: allora disattivate il servizio finger.
- Davvero volete consentire a chiunque di fare ftp sul vostro computer senza preavviso? Se non è così, disattivate il servizio ftp.

Ridurre i servizi disponibili: la pratica (Red Hat Linux 7.0)

In Red Hat Linux 7.0, i file che controllano l'attivazione dei demoni di rete sono nella directory */etc/xinetd.d*. Per ciascun servizio è presente un file: ad esempio, il demone *telnetd* (risposta automatica alle richieste di telnet prevenienti dall'esterno) è controllato dal file */etc/xinetd.d/telnet*; il demone *ftpd* (risposta automatica alle richieste di trasferimento file tramite FTP) è controllato dal file */etc/xinetd.d/wu−ftpd*.

Per disabilitare un servizio, aprite il file corrispondente con un editor di testi e trasformate in commento tutte le righe (lo so che esistono metodi più raffinati, ma sono anche più complessi) digitando a inizio riga un simbolo "#" (cancelletto). Meglio ancora, digitatene due, così potete distinguere le righe che avete modificato.

Per attivare la modifica, salvate il file e digitate il comando **/etc/rc.d/init.d/xinetd restart**. Se in futuro decidete di riattivare il servizio, riaprite il file che definisce quel servizio e togliete i simboli di cancelletto che avete inserito, poi ridate il comando **/etc/rc.d/init.d/xinetd restart**.

Ridurre i servizi disponibili: la pratica (Red Hat Linux 6.2)

Disattivare l'avvio automatico di un servizio di rete in Red Hat Linux 6.2 è molto semplice: basta trasformare in commento (anteponendo il carattere "#") la riga del file */etc/inetd.conf* che lo definisce.

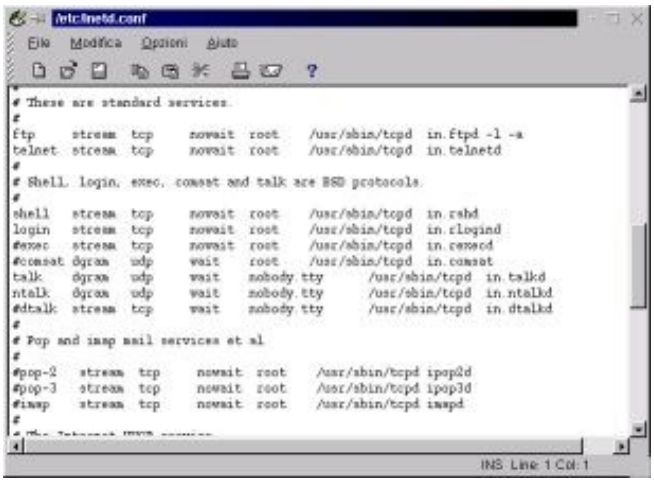

Figura 18−5. Il file *inetd.conf* ha bisogno di una regolata.

Trasformate in commento tutto il commentabile, soprattutto ftp, telnet, shell, login e finger; potete lasciare talk e ntalk, se pensate vi possano servire. Come promemoria di cosa avete disattivato, usate *due* simboli di cancelletto per distinguere quello che avete disattivato voi da quello che era già disattivato in partenza.

Per attivare le modifiche, salvate il file e poi date il comando **killall −HUP inetd**. Questo obbliga Linux a rileggere il file *inetd.conf* modificato ed attivarne immediatamente le impostazioni. Se in futuro volete riattivare un servizio, togliete i simboli di cancelletto dalla riga che lo definisce e ridate il comando **killall −HUP inetd**.

Da questo momento in poi, nessuno potrà attivare dall'esterno i servizi che avete disattivato. Ad esempio, chi dovesse tentare di fare telnet verso la vostra macchina dopo queste modifiche otterrebbe per tutta risposta, invece della richiesta di login, un secco *Connessione rifiutata*, per cui non avrà neppure occasione di tentare di indovinare nome di login e password.

Il buttafuori digitale

Nella directory */etc/* ci sono altri due file molto utili se volete consentire l'accesso dall'esterno soltanto a determinati utenti: *hosts.allow* e *hosts.deny*. Questi due file decidono quali indirizzi IP possono accedere al vostro computer e quali no, e che tipo di accesso possono avere.

La configurazione di questi due file è complessa e articolata, come descritto nelle relative pagine man, ma non è indispensabile fare cose ultrasofisticate. Il modo più pratico e semplice di impostare questo livello di sicurezza è scrivere questa riga in *hosts.deny*:

```
ALL : ALL
```

Traduzione: è vietato l'accesso, con qualsiasi servizio, a chiunque, a meno che il suo indirizzo IP sia specificato esplicitamente in *hosts.allow*. Il primo *ALL* ("tutti" in inglese) specifica i tipi di servizi vietati (tutti, appunto), il secondo indica quali indirizzi IP verranno rifiutati (tutti).

Una volta eseguita questa modifica, avete chiuso completamente le saracinesche. Non importa chi vi chiama, dalla rete locale o da Internet: la sua chiamata verrà respinta.

Se volete concedere l'accesso a un utente specifico (ad esempio una macchina della rete locale o un utente Internet di cui vi fidate ciecamente), potete modificare il file *hosts.allow* scrivendo una serie di righe, una per ciascun indirizzo IP che

volete autorizzare. Per ogni indirizzo IP autorizzato potete inoltre specificare quali servizi concedergli.

Le righe di *hosts.allow* sono simili a quelle di *hosts.deny*. Per prima cosa si specifica il nome del servizio da concedere (per concedere tutti i servizi si scrive *ALL*), poi si scrive un carattere "due punti" di separazione, e infine si scrive l'indirizzo IP da autorizzare. Ad esempio:

```
ALL : 192.168.1.25
```

autorizza solo ed esclusivamente la macchina della rete locale che ha l'indirizzo IP *192.168.1.25* ad accedere alla macchina Linux e a usarne tutti i servizi, sempre che quei servizi non siano stati disattivati in *inetd.conf* (per la distribuzione 6.2) o in *xinetd.d* (per la distribuzione 7.0).

La parete tagliafuoco: firewall con ipchains

La sicurezza non si basa sulla fiducia in un unico strumento, ma sulla stratificazione di più strumenti di protezione. Per un ladro è più difficile forzare due porte che forzarne una; lo stesso vale per l'informatica. È possibile che un intruso particolarmente abile riesca a scavalcare una delle vostre difese, ma non gli servirà a molto se poi se ne troverà davanti un'altra ancora intatta.

Inoltre può sempre capitarvi un momento di distrazione, per cui uno dei vostri meccanismi di protezione rimane disattivato perché l'avete rimosso per manutenzione o per qualsiasi altro motivo. Se è il solo che avete, lasciate la macchina totalmente indifesa; se è soltanto uno dei tanti, la sicurezza è momentaneamente indebolita ma non compromessa.

È per questo che nonostante le procedure di blindatura che ho già descritto siano di per sé sufficienti a bloccare le più comuni intrusioni, vi accenno anche *ipchains*, che è uno dei sistemi di sicurezza più quotati in ambiente Linux. Il programma è installato automaticamente da Red Hat Linux 6.2, per cui dovrebbe essere già presente sul vostro computer, ma in ogni caso lo potete trovare presso http://www.rustcorp.com/linux/ipchains.

Ipchains è un *firewall*, ossia un programma che fa da barriera (letteralmente, da "parete tagliafuoco") fra voi e Internet a un livello molto fondamentale della comunicazione: il livello dei pacchetti IP, che sono le particelle elementari che trasmettono le informazioni su Internet. Quando inviate o trasmettete qualsiasi cosa via Internet, viene convertita in pacchetti IP per la trasmissione e riconvertita all'arrivo. Ipchains decide quali pacchetti possono uscire dal vostro computer, quali possono transitarvi e quali possono entrarvi.

Le decisioni di ipchains si basano su una serie di regole la cui esatta impostazione è piuttosto complessa e varia a seconda della vostra specifica situazione, ma rispetta questo principio generale:

- Ci sono tre flussi di dati fondamentali, o "catene" (*chains*): in ingresso (da Internet verso il vostro computer), in uscita (dal vostro computer a Internet) e in transito (da Internet, passando per il vostro computer, verso altre macchine della rete locale o di Internet).
- Per ciascuno di questi tre flussi potete definire cosa fare dei relativi pacchetti IP in base al tipo di pacchetto e alla sua provenienza e destinazione: ad esempio accettarli (con il parametro *ACCEPT*) o rifiutarli (con *DENY*).

Affinché ipchains possa funzionare, è necessario che sia attivato: in linuxconf, nella sezione *Controllo*, trovate *Verifica dello stato dei servizi*. Scegliete *ipchains* e attivate *Automatic* (per attivarlo automaticamente ad ogni avvio di Linux) e *Start* (per avviarlo subito). Salvate le modifiche e uscite da linuxconf.

Fatto questo, potete eseguire qualche piccola prova per familiarizzare con ipchains. Tanto per cominciare, andate come *root* in una console o in una finestra di terminale e digitate **ipchains −L**. Otterrete una risposta di questo tipo:

```
Chain input (policy ACCEPT):

Chain forward (policy ACCEPT):

Chain output (policy ACCEPT):
```

Questo significa che i pacchetti IP vengono accettati tutti, in ingresso come in uscita come in transito, a prescindere dalla loro destinazione e dalla loro origine. In altre parole, il firewall è attivo ma non blocca assolutamente nulla. Avete messo una guardia alla porta, ma non le avete detto chi lasciar passare e chi no, per cui la guardia lascia passare tutti.

In queste condizioni, potete eseguire il comando **ping 127.0.0.1**, che in pratica dice alla vostra macchina Linux di contattare se stessa usando i protocolli Internet. Contattare se stessi è una prassi normale per verificare il funzionamento del software di rete.

Il comando **ping** genera un flusso di pacchetti IP che "esce" dal vostro computer, passa attraverso i protocolli di rete e "rientra" sul computer medesimo. Siccome ipchains accetta tutto per ora, il risultato del comando **ping** è quello normale: i pacchetti trasmessi arrivano a destinazione.

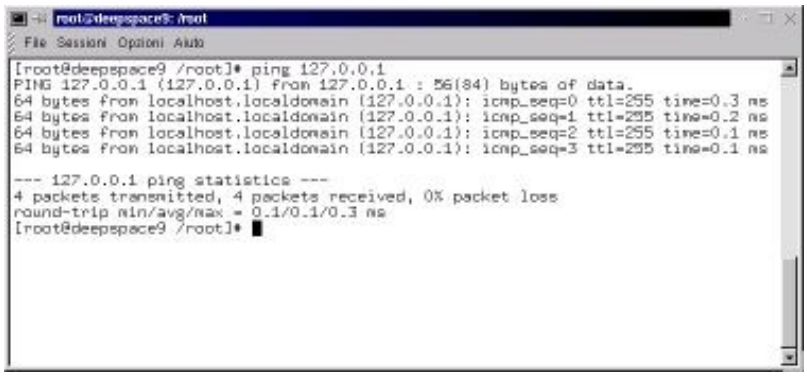

Figura 18−6. Ipchains è attivo, ma lascia passare tutto.

Se però adesso date il comando **ipchains −P input DENY**, tutti i pacchetti in ingresso vengono ignorati totalmente, come se non fossero mai arrivati. Facendo di nuovo **ping 127.0.0.1**, i pacchetti "escono" regolarmente, ma non riescono più a "rientrare", perché c'è il firewall che li blocca, anzi li disintegra all'arrivo.

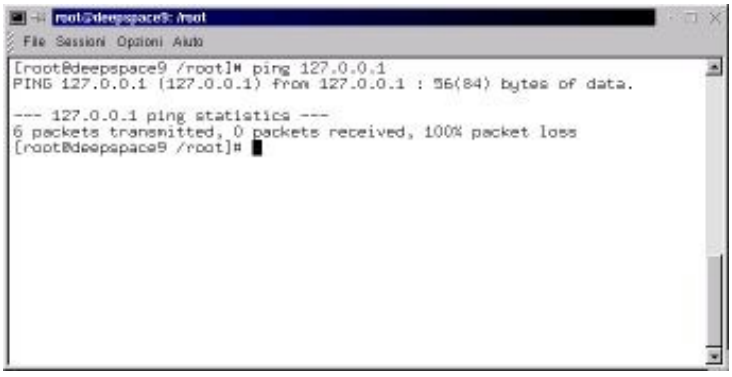

Figura 18−7. Ipchains ha chiuso i boccaporti e non passa più nulla.

Chiaramente questo esempio è molto brutale, perché taglia completamente le comunicazioni, ma si possono dare vari parametri al comando **ipchains** per ottenere filtraggi molto più mirati. Tipicamente, si inizia bloccando tutto il traffico in

ingresso e in uscita; poi si sblocca soltanto quello del tipo desiderato. Ad esempio:

```
ipchains −P input DENY

ipchains −P output DENY

ipchains −A input −i eth0 −j ACCEPT

ipchains −A output −i eth0 −j ACCEPT
```

blocca tutto e poi sblocca esclusivamente il traffico che entra ed esce dalla scheda di rete (*eth0*). Il risultato è che se fate **ping 127.0.0.1**, i vostri pacchetti verranno respinti alla partenza. Se invece digitate **ping** seguito dall'indirizzo IP di un computer collegato alla vostra macchina Linux tramite la scheda di rete, i pacchetti usciranno ed entreranno liberamente.

Una volta che avete preso dimestichezza con la caterva di opzioni di ipchains, potete definire un insieme di regole più complesso e salvarlo in un file da eseguire automaticamente a ogni avvio di Linux. Ipchains consente ad esempio di accettare soltanto i pacchetti provenienti da indirizzi IP fidati e di ignorare i rimanenti.

Uno dei trucchetti preferiti di Odo è dire a ipchains di rifiutare i pacchetti che arrivano dagli indirizzi IP dei siti pubblicitari, come Doubleclick: in questo modo, durante la navigazione nel Web i *banner* pubblicitari non vengono neppure scaricati e quindi l'uso di Internet diventa nettamente più veloce.

Sostenete *Da Windows a Linux*!

Questo libro è distribuito **gratuitamente**, ma le **donazioni** sono sempre ben accette, sia tramite **PayPal,** sia tramite il collaudato sistema della **banconota in una busta**. Se volete dettagli e istruzioni su come procedere, le trovate presso **http://www.attivissimo.net/donazioni/donazioni.htm**.

Grazie!