

Settima dispensa: la sicurezza

[(c)2002 – Jean François Panico]

Sicurezza di Rete

La sicurezza di rete diventa sempre più importante perché il tempo di connessione ad Internet è sempre maggiore. Compromettere la sicurezza di rete è spesso molto più facile che compromettere la sicurezza fisica o locale ed è anche molto più comune.

Esiste una serie di buoni strumenti per aiutare nella sicurezza di rete e molti nuovi vengono inclusi nelle distribuzioni Linux.

Sniffer di Pacchetti

Uno dei modi più comuni con cui gli intrusori entrano in molti sistemi della vostra rete è l'uso di uno sniffer di pacchetti su un host già compromesso. Questo "sniffer" aspetta sulla porta Ethernet dati come passwd, login e su nel flusso dei dati e quindi registra il traffico successivo. In questo modo chi lo usa ottiene le password di sistemi a cui non hanno neppure tentato un attacco. Le password in chiaro sono molto vulnerabili a questo tipo di attacco.

Esempio: L'host A è stato compromesso. L'attaccante installa uno sniffer. Lo sniffer intercetta l'amministratore mentre fa un login dall'host B al C. Ottiene la password personale dell'amministratore. Poi, l'amministratore usa su per risolvere un problema. Ora si conosce anche la password di root per l'host B. Più tardi l'amministratore lascia che dal suo account qualcuno usi telnet per connettersi all'host Z. Ora l'attaccante ha il login e la password per l'host Z.

Oggi l'attaccante non ha neanche più bisogno di compromettere un sistema per usare questa tecnica: potrebbe semplicemente portare un portatile o un PC nell'edificio e connettersi alla vostra rete.

Usare ssh o altri metodi di crittografia delle password blocca questo attacco. Anche cose come APOP per gli account POP lo impediscono (I normali login POP sono molto vulnerabili a questo attacco, come ogni cosa che mandi password in chiaro su una rete).

Servizi di sistema e tcp_wrappers

Prima di mettere un sistema Linux su QUALSIASI rete la prima cosa da sapere è quali servizi volete offrire. I servizi che non volete devono essere disabilitati, così da avere una cosa in meno di cui preoccuparsi e un possibile buco in meno per un intrusore.

Ci sono molti modi per disabilitare i servizi sotto Linux. Potete leggere il vostro /etc/inetd.conf e vedere quali servizi vengono offerti dal vostro inetd. Potete disabilitare tutti quelli che non vi servono commentandoli (# all'inizio della linea), e quindi mandando al processo inetd un SIGHUP.

Potreste rimuovere (o commentare) servizi nel vostro /etc/services. Questo impedirà l'uso del servizio anche da client locali (cioè se rimuovete ftp e provate a connettervi con ftp ad un host remoto da quella macchina otterrete solo un messaggio di "servizio sconosciuto"). In genere il gioco non vale la candela, visto che non dà ulteriori garanzie.

Se qualcuno volesse usare ftp anche se l'avete commentato, potrebbe farsi un proprio client che usi la porta FTP e funzionerebbe benone.

Alcuni servizi che dovrete lasciare disponibili sono:

- ftp
- telnet (o ssh)
- mail, come pop-3 o imap
- identd

Se sapete che non vi serve un pacchetto potete anche cancellarlo del tutto. `rpm -e nome_pacchetto` nella distribuzione RedHat cancella un pacchetto intero. Nella Debian `dpkg --remove` fa lo stesso.

Inoltre, dovrete davvero evitare che le utility rsh/rlogin/rcp, inclusi login (usato da rlogin), shell (usato da rcp) ed exec (usato da rsh) siano eseguite da `/etc/inetd.conf`. Questi protocolli sono molto insicuri e sono stati l'origine di exploit in passato.

Dovreste controllare `/etc/rc.d/rc(0-9).d` (sulla Red Hat; `/etc/rc(0-9).d` sulla Debian), e vedere se vengono avviati server che non sono necessari. I file in quelle directory sono link simbolici ai file nella directory `/etc/rc.d/init.d` (sulla Red Hat; `/etc/init.d` sulla Debian). Rinominare i file nella directory `init.d` blocca tutti i link simbolici che puntano a quel file. Se volete solo disabilitare un servizio per un particolare runlevel, rinominate il giusto link simbolico sostituendo la S maiuscola con una minuscola, così:

```
root# cd /etc/rc6.d
root# mv S45dhcpd s45dhcpd
```

Se avete file `rc rc` in stile BSD, controllate in `/etc/rc*` se ci sono programmi che non servono.

Con molte distribuzioni Linux viene distribuito un `tcp_wrapper` che "incapsula" tutti i vostri servizi TCP. Un `tcp_wrapper(tcpd)` viene invocato da `inetd` al posto del vero server. Quindi `tcpd` controlla l'host che sta richiedendo il servizio ed esegue il server o nega l'accesso all'host. `tcpd` permette di bloccare l'accesso ai vostri servizi TCP. dovrete creare un file `/etc/hosts.allow` e aggiungervi solo gli host che devono avere accesso ai servizi della macchina.

Se avete una connessione telefonica casalinga dovrete negarli TUTTI. Inoltre `tcpd` segna nei log i tentativi falliti di accedere ai servizi, per avvertirvi se siete sotto attacco. Se aggiungete nuovi servizi dovrete configurarli per usare i `tcp_wrapper` se usano TCP. Per esempio, un normale utente telefonico può impedire ad altri di connettersi alla propria macchina, conservando l'accesso alla posta e ad Internet. Per farlo, potreste aggiungere le linee seguenti al vostro `/etc/hosts.allow`:

```
ALL: 127.
```

E ovviamente `/etc/hosts.deny` dovrebbe contenere:

```
ALL: ALL
```

che bloccherà connessioni esterne alla macchina, ma permetterà la connessione a server su Internet.

Ricordatevi che i `tcp_wrapper` proteggono solo i servizi eseguiti da `inetd`, e pochi altri. Ci potrebbero benissimo essere altri servizi in esecuzione sulla vostra macchina. Potete usare `netstat -ta` per avere una lista di tutti i servizi offerti dalla vostra macchina.

8.3 Verificare i vostri DNS

Tenere aggiornate le informazioni dei DNS su tutti gli host della vostra rete aiuta ad aumentare la sicurezza. Se un host non autorizzato si connette alla rete, potete riconoscerlo dalla sua mancata presenza sul DNS. Molti servizi possono essere configurati per negare l'accesso ad host che non sono elencati dal DNS.

8.4 identd

`identd` è un piccolo programma che in genere è eseguito dal vostro `inetd`. Tiene nota di quale utente sta usando quale servizio e quindi fa rapporto a chi lo richiede.

Molte persone non capiscono l'utilità di `identd` e quindi lo disabilitano o bloccano tutte le richieste provenienti dall'esterno. `identd` non è al servizio di siti remoti. Non c'è modo di saper se i dati che ricevete da un `identd` remoto siano corretti o no. Non c'è autenticazione nelle richieste ad `identd`.

Perché eseguirlo allora? Perché aiuta voi, ed è un'informazione in più quando indagate. Se il vostro `identd` è integro, sapete che rivela ad altri l'username o l'uid di chi usa servizi TCP. Se l'amministratore di una rete remota viene a dire che un certo utente ha provato ad intromettersi nella sua rete, potrete facilmente prendere provvedimenti contro l'utente. Se non aveste eseguito `identd`, avreste dovuto leggere log su log, capire chi era nel sistema alla tal ora e in generale sprecare molto tempo a trovare l'utente.

L'`identd` distribuito con molte distribuzioni si può configurare più di quanto molti pensino. Potete disabilitarlo per utenti specifici, (con un file `.noident`), potete avere i log di tutte le richieste a `identd` (È raccomandato), potete persino far sì che `identd` risponda con l'uid di un utente o persino con `NO-USER`.

8.5 SATAN, ISS, e altri scanner di rete

C'è una serie di differenti pacchetti software che fanno scansioni di porte e servizi su macchine o reti intere. SATAN, ISS, SAINT e Nessus sono alcuni dei più conosciuti. Questo software si connette con la macchina bersaglio (o tutte le macchine bersaglio su una rete) su tutte le porte possibili e tentano di capire che servizio è attivo. Basandosi su queste informazioni si capisce se la macchina è vulnerabile ad un particolare exploit.

SATAN (Security Administrator's Tool for Analyzing Networks) è un port scanner con un'interfaccia web. Può essere configurato per eseguire controlli leggeri, medi o pesanti su una macchina o una rete. È una buona idea usare SATAN sulla vostra rete e sistemare i problemi che trova. Assicuratevi di avere la copia di SATAN da metalab o da un sito FTP o web affidabile. È stata distribuita in rete una copia trojan di SATAN. <http://www.trouble.org/~zen/satan/satan.html>. Notate che SATAN non è stato aggiornato da molto tempo, ed altri strumenti potrebbero avere risultati migliori.

ISS (Internet Security Scanner) è un altro port scanner. È più veloce di Satan, quindi potrebbe essere migliore per grandi reti. Comunque Satan in genere fornisce più informazioni.

Abacus è una suite di strumenti che fornisce sicurezza agli host e rilevamento delle intrusioni. Leggete la home page sul web per ulteriori informazioni.

<http://www.psonian.com/abacus/>

SAINT è una versione aggiornata di SATAN. È basata sul web ed ha molti più test aggiornati di SATAN. Potete saperne di più presso: <http://www.wwdsi.com/~saint>

Nessus è uno scanner di sicurezza libero. Ha una interfaccia grafica GTK per semplicità d'uso. Inoltre è basato su una struttura a plug-in per aggiungere nuovi test. Per ulteriori informazioni, date un'occhiata a: <http://www.nessus.org>

Rilevare Scansioni delle Porte

Esistono strumenti progettati per avvisarvi di scansioni da parte di SATAN, ISS ed altri software di scansione. Comunque se usate molto i tcp_wrapper e leggete spesso i vostri log dovrete notare certe scansioni. Anche al settaggio inferiore SATAN lascia tracce nei log di un sistema RedHat "di serie".

Esistono anche port scanner "silenziosi". Un pacchetto con il bit TCP ACK attivo (come si fa per le connessioni stabilite) probabilmente passerebbe un firewall che filtra i pacchetti. Il pacchetto RST in risposta da una porta che *non aveva comunicazioni in corso* viene preso come una prova di vita su quella porta. Non penso che i tcp_wrapper lo rilevino.

8.6 sendmail, qmail e MTA (Agenti di Trasporto di Posta)

Uno dei servizi più importanti che potete fornire è il server di posta. Sfortunatamente, è anche uno dei più vulnerabili agli attacchi, a causa del numero di compiti che esegue e dei privilegi che di solito richiede.

Se state usando sendmail è molto importante tenerlo aggiornato. sendmail ha una lunga, lunga storia di exploit di sicurezza. Assicuratevi di eseguire sempre l'ultima versione da: <http://www.sendmail.org>.

Ricordatevi che sendmail non deve per forza essere in esecuzione per spedire posta. Se siete un utente casalingo potete disabilitare del tutto sendmail e usare semplicemente il vostro client di posta per spedire. Potreste anche togliere l'opzione "-bd" da file di avvio di sendmail, disabilitando l'arrivo di richieste di posta. In altre parole, potete eseguire sendmail dal vostro script di avvio usando il seguente comando:

```
# /usr/lib/sendmail -q15m
```

In questo modo sendmail riprocescherà ogni 15 minuti i messaggi nella coda di stampa che non erano stati precedentemente consegnati.

Molti amministratori non usano sendmail, e al suo posto scelgono uno degli altri MTA. Potreste passare a qmail. qmail è stato progettato da zero tenendo a mente la sicurezza. È veloce, stabile e sicuro. Qmail si trova presso <http://www.qmail.org>

In diretta competizione con qmail si pone "postfix", scritto da Wietse Venema, l'autore di tcp_wrapper ed altri strumenti di sicurezza. Precedentemente intitolato vmailer, e sponsorizzato da IBM, anche questo è un MTA fatto da zero per la sicurezza. Troverete altre informazioni su postfix presso <http://www.postfix.org>

8.7 Attacchi di Denial of Service (Negazione di un Servizio)

Un "Denial of Service" (DoS) è un attacco con cui un aggressore tenta di rendere una risorsa troppo occupata per rispondere a richieste legittime o di negare a utenti legittimi l'accesso ad una macchina.

Questi attacchi sono molto aumentati negli ultimi anni. Sotto sono elencati alcuni dei più comuni o recenti. Notate però che ne nascono in continuazione, quindi questi sono solo esempi. Leggete le liste di sicurezza di Linux e le liste di bugtraq per informazioni aggiornate.

- **SYN Flooding** - Il SYN flooding ("Inondazione di SYN") è un attacco DoS di rete. Sfrutta un buco nel modo in cui sono create le connessioni TCP. Gli ultimi kernel di Linux (2.0.30 e seguenti) hanno diverse opzioni configurabili per evitare che attacchi del genere neghino l'accesso alle vostre macchine. Vedi [Sicurezza del Kernel](#) a proposito delle opzioni adeguate.
- **Il Bug "FOOF" nei Pentium** - Si è scoperto recentemente che una serie di codici assembly mandati ad un Pentium originale Intel riavvierebbero la macchina. Questo bug affligge tutte le macchine Pentium (non i cloni, i Pentium Pro o i PII), a prescindere dal sistema operativo. I kernel Linux 2.0.32 e successivi contengono un rimedio che impedisce alla macchina di bloccarsi. Il kernel 2.0.33 ha una versione migliore rispetto al 2.0.32. Se usate un Pentium, aggiornate subito il kernel!
- **Ping Flooding** - Il ping flooding ("Inondazione di ping") è un attacco DoS basato sulla forza bruta. L'aggressore manda un'inondazione di pacchetti ICMP alla vostra macchina. Se lo fa da un host con un'ampiezza di banda maggiore della vostra, la vostra macchina non potrà mandare niente sulla rete. Un variazione di questo attacco, chiamato "smurfing", manda ad un host pacchetti ICMP con il *vostro* IP, permettendo loro di attaccarvi in modo quasi anonimo. Potete trovare altre informazioni circa lo "smurf" presso <http://www.quadrunner.com/~chuegen/smurf.txt>

Se venite attaccati in questo modo, usate uno strumento come tcpdump per determinare da dove provengono i pacchetti (o da dove sembrano venire), quindi contattate il vostro provider con queste informazioni. I ping flood possono essere fermati facilmente all'altezza del router o usando un firewall.

- **Ping della Morte** - Il Ping della Morte manda pacchetti ICMP ECHO REQUEST che sono troppo grandi per entrare nelle strutture dati del kernel che li dovrebbero contenere. Poiché mandare un solo grande ping (65,510 byte) causa il blocco o il crash di molti sistemi, questo problema fu subito soprannominato "Ping della Morte". Il fatto è stato risolto da tempo, e non è più preoccupante.
- **Teardrop / New Tear** - Uno dei più recenti exploit coinvolge un bug presente nel codice di frammentazione IP sulle piattaforme Linux e Windows. È stato risolto nel kernel 2.0.33 e non richiede la selezione di alcuna opzione di compilazione. Linux non sembra essere vulnerabile al nuovo exploit "newtear".

Potete trovare il codice della maggior parte degli exploit e una più approfondita descrizione del loro funzionamento presso <http://www.rootshell.com> usando il loro motore di ricerca.

8.8 Sicurezza del NFS (Network File System).

NFS è un protocollo di condivisione di file molto diffuso. Permette a server che eseguano nfsd e mountd di "esportare" interi filesystem verso altre macchine usando il supporto per il

filesystem NFS compilato nel kernel (o qualche altro client se non sono macchine Linux). mountd tiene traccia dei filesystem montati in /etc/mntab, e li mostra con showmount.

Molti siti usano NFS per fornire le home directory agli utenti di modo che abbiano i loro file da qualunque macchina si colleghino.

È possibile avere un po' di sicurezza quando si esportano filesystem. Potete far mappare a nfsd l'utente root remoto (uid=0) sull'utente nobody, negando l'accesso totale ai filesystem esportati. Comunque, visto che i singoli utenti hanno accesso ai propri file (o almeno a quelli con la stessa uid), l'utente root remoto può fare un login o su con il loro account ed avere accesso totale ai loro file. Questo è solo un piccolo ostacolo per un aggressore che ha i privilegi per montare i filesystem remoti.

Se dovete usare NFS, assicuratevi di esportare solo verso quelle macchine che lo richiedono. Non esportate mai la vostra intera directory root; esportate solo il necessario.

Leggete il NFS HOWTO per ulteriori informazioni su NFS, disponibile presso <http://metalab.unc.edu/mdw/HOWTO/NFS-HOWTO.html>

8.9 NIS (Network Information Service) (già YP).

Network Information service (servizio di informazione di rete) è un modo di distribuire informazioni ad un gruppo di macchine. Il master NIS tiene le tabelle di informazioni e le converte in file mappa di NIS. Queste mappe vengono distribuite nella rete, permettendo ai client di ottenere informazioni di login, password, home directory e shell (tutte le informazioni che in genere stanno in un normale /etc/passwd). Questo permette agli utenti di cambiare la loro password una volta per tutte le macchine sul dominio NIS.

NIS non è affatto sicuro. Non ha mai voluto esserlo. Doveva solo essere comodo ed utile. Chiunque possa indovinare il nome del vostro dominio NIS (ovunque sia nella rete) può ottenere una copia del file delle password ed usare Crack o John the Ripper contro le password. Se dovete usare NIS siate consapevoli dei pericoli.

Esiste un sostituto molto sicuro di NIS, chiamato NIS+. Controllate il NIS HOWTO: <http://metalab.unc.edu/mdw/HOWTO/NIS-HOWTO.html>

8.10 Firewall

I Firewall sono un mezzo per controllare quali informazioni vengono lasciate entrare ed uscire dalla vostra rete locale. Tipicamente l'host firewall è connesso ad Internet e alla LAN locale, ed è l'unico accesso ad Internet dalla LAN; in questo modo controlla cosa entra ed esce.

Ci sono molti tipi di firewall e metodi di impostarli. Le macchine Linux sono ottimi firewall. Il codice del firewall può essere compilato all'interno dei kernel 2.0 e superiori. Gli strumenti utente ipfwadm per i kernel 2.0 e ipchains per i kernel 2.2, vi permettono di cambiare al volo i tipi di traffico di rete permessi.

I firewall sono un'utilissima ed importante tecnica per la sicurezza di rete. Comunque, non pensate mai che solo perché avete un firewall non sia necessaria la sicurezza delle macchine che copre. Sarebbe un errore fatale. Controllate l'ottimo Firewall-HOWTO presso l'archivio metalab per avere più informazioni sui firewall e Linux. <http://metalab.unc.edu/mdw/HOWTO/Firewall-HOWTO.html>

Si trovano altre informazioni anche nell'IP-Masquerade mini-howto:

<http://metalab.unc.edu/mdw/HOWTO/mini/IP-Masquerade.html>

Altre informazioni su ipfwadm (lo strumento per cambiare impostazioni al firewall) si trovano presso: <http://www.xos.nl/linux/ipfwadm/>

Se non avete esperienza con i firewall e volete metterne su uno per un piano di sicurezza che non sia superficiale, leggere "Firewalls" di O'Reilly and Associates o qualche altro documento online sui firewall è obbligatorio. Troverete altre informazioni su <http://www.ora.com>. Il National Institute of Standards and Technology (Istituto Nazionale degli Standard e della Tecnologia) ha scritto un eccellente documento sui firewall. Anche se datato 1995, è sempre abbastanza buono. Potete trovarlo anche <http://csrc.nist.gov/nistpubs/800-10/main.html>.

- Il progetto Freefire -- una lista di strumenti firewall liberi, disponibili presso http://sites.inka.de/sites/linga/freefire-1/index_en.html
- SunWorld Firewall Design -- scritto dagli autori del libro della O'Reilly, dà una introduzione di base ai differenti tipi di firewall. È disponibile presso <http://www.sunworld.com/swol-01-1996/swol-01-firewall.html>
- Mason - il costruttore automatico di firewall per Linux. È uno script di firewall che impara cosa vi serve mentre lo fate. Altre informazioni presso: <http://www.pobox.com/~wstearns/mason/>

8.11 IP Chains - Firewall per Linux Kernel 2.2.x

IP Firewalling Chains è un aggiornamento dal codice di firewalling del kernel 2.0 al 2.2. Ha molte più caratteristiche delle versioni precedenti, inclusi:

- Manipolazioni dei pacchetti più flessibili.
- Accounting più complesso.
- Sono istantanei i semplici cambiamenti di impostazioni.
- I frammenti possono essere esplicitamente bloccati, rifiutati ecc.
- I pacchetti sospetti vengono segnati in un log.
- Può gestire protocolli non ICMP/TCP/UDP.

Se state usando ipfwadm con il vostro kernel 2.0, sono disponibili degli script per convertire il formato di ipfwadm nel formato che usa ipchains.

Assicuratevi di leggere l'IP Chains HOWTO per altre informazioni. È disponibile presso <http://www.rustcorp.com/linux/ipchains/HOWTO.html>

8.12 VPN - Virtual Private Networks (Reti Private Virtuali)

Le VPN sono un modo per stabilire una rete "virtuale" su una rete esistente. Questa rete virtuale è spesso crittata e passa il traffico solo a e da entità conosciute. Le VPN sono spesso usate per connettere attraverso Internet qualcuno che lavora a casa a un rete interna di una compagnia.

Se eseguite un firewall/masquerading con Linux dovete passare pacchetti di MS PPTP (un prodotto VPN punto-a-punto della Microsoft), c'è una patch per il kernel di Linux fatta apposta. Leggete: ip-masq-vpn.

Esistono diverse soluzioni VPN per Linux:

- vpnd. Leggete <http://sunsite.auc.dk/vpnd/>.
- Free S/Wan, disponibile presso <http://www.xs4all.nl/~freeswan/>
- ssh può essere usato per costruire una VPN. Leggete il VPN mini-howto per altre informazioni.
- vps (virtual private server) presso <http://www.strongcrypto.com>.

Controllate anche la sezione su IPSEC per altre bibliografie e informazioni

9. Preparazione della Sicurezza (prima di entrare in rete)

Bene: avete controllato il sistema, è sicuro per quanto possibile e siete pronti a metterlo in rete. Ci sono alcune cose che dovrete fare ora per prepararvi ad un'intrusione, in modo da poter mettere fuori gioco velocemente l'aggressore e tornare alla piena funzionalità.

9.1 Fate un backup completo della macchina.

La discussione dei metodi di backup va oltre gli scopi di questo documento, ma vanno spese alcune parole su backup e sicurezza:

Se avete meno di 650mb di dati da salvare su una partizione, un CD-R è un'ottima strada (perché difficile da manomettere e molto durevole). Nastri e altri media riscrivibili dovrebbero essere protetti dalla scrittura non appena il backup è completo e quindi verificati per evitare la manomissione. Assicuratevi di lasciare i backup in un'area sicura e off-line. Un buon backup vi darà un buon punto di riferimento da cui ripristinare il sistema.

9.2 Scegliere una Buona Tabella di Backup

Un ciclo di sei nastri è facile da mantenere. Prevede quattro nastri per la settimana, uno per i Venerdì pari e uno per quelli dispari. Eseguite un backup incrementale ogni giorno, e un backup completo sul nastro del Venerdì. Potreste fare un backup completo anche per dei particolari cambiamenti importanti.

9.3 Fate un Backup dei Vostri Database di RPM o Debian

Nel caso di un'intrusione, potete usare il vostro database di pacchetti come usereste tripwire, ma solo se siete sicuri che non è stato modificato. Dovreste copiare il database RPM in un floppy e tenerlo sempre off-line. Probabilmente la Debian ha qualcosa di simile.

I file `/var/lib/rpm/fileindex.rpm` e `/var/lib/rpm/packages.rpm` probabilmente non entreranno in un solo floppy, ma se compressi dovrebbero entrare in un floppy ciascuno.

Ora, se il vostro sistema viene compromesso potete usare il comando:

```
root# rpm -Va
```

per verificare ogni file sul sistema. Leggete la pagina man di rpm, perché esistono alcune opzioni che possono essere usate per avere un output più: conciso. Ricordate che dovete essere sicuri che anche l'eseguibile di RPM non sia stato compromesso.

Questo significa che ogni volta che viene aggiunto al sistema un RPM, il database dovrà essere ri-archiviato, voi decidere i vantaggi contro gli svantaggi.