Introduzione a Linux

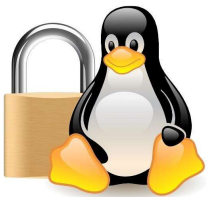
Lezione 9
Sicurezza in Linux

Ruggero Donida Labati

Laboratorio di Sistemi Operativi
Università degli Studi di Milano
Dipartimento di Informatica
A.A. 2022/2023

Panoramica della lezione

- Verranno introdotti alcuni concetti relativi alla sicurezza in ambiente Linux
- Saranno presentati alcune norme di sicurezza utili
- Saranno presentati alcuni strumenti utili per mantenere sicuro il sistema



Sommario (1/2)

1. Introduzione alla sicurezza in Linux
   - Buone norme
   - Caratteristiche sicure di Linux
2. Gestione delle password
3. Panoramica su IPTables
   - Introduzione
   - Firewall
   - NAT
   - GUI per IPTables

Sommario (2/2)

4. Antivirus
   - Perchè usare un antivirus?
   - ClamAV
   - RootkitHunter
5. Sicurezza del file system
   - Permessi cartella personale
   - Crittazione dati personali
6. Posta elettronica sicura
7. Esercizi

1. Introduzione alla sicurezza in Linux

1. Caratteristiche sicure di Linux
2. Buone norme per la sicurezza

Caratteristiche sicure di Linux (1/3)

- Rigida e complessa gestione dei permessi
- Ogni utente, e quindi ogni programma eseguito da tale utente, può fare con un file solo ciò che è consentito in base ai permessi che possiede
- I programmi utente sono separati da quelli di amministrazione
- I programmi per essere eseguiti devono avere lo speciale attributo di eseguibili

Caratteristiche sicure di Linux (2/3)

- I programmi utente possono agire solo sulla Home di quell'utente, non sui file di amministratore né su quelli di altri utenti
- Un malware che agisce a livello utente non può creare danni al sistema, ma infettare solo i file appartenenti a quel determinato utente
  - I programmi non sono mai installati nella directory Home dell'utente

Caratteristiche sicure di Linux (3/3)

- Linux usa software opensource
  - Le vulnerabilità possono essere trovate più facilmente
  - Le vulnerabilità possono essere corrette più facilmente

Buone norme per la sicurezza (1/4)

- La sicurezza di una macchina è una combinazione di fattori e non è stabile nel tempo
  - Va monitorata nel tempo
  - Il fattore umano è determinante
- I sistemi Linux sono più sicuri rispetto ad altri sistemi operativi più diffusi
- Strumenti adeguati e norme corrette sono comunque necessarie

Buone norme per la sicurezza (2/4)

- Log-off
  - Sessione
  - Facebook
  - Ecc.
- Usare una password lunga e non facilmente individuabile
  - Ma non attaccarla con un post-it sotto lo schermo
- Aggiornare regolarmente
  - Le vulnerabilità vengono corrette
  - Un sistema non aggiornato è insicuro

Buone norme per la sicurezza (3/4)

- Usare un antivirus
  - Anche se i virus sono per Windows, si evita la propagazione
- Installare la cartella */home* in una partizione separata
  - Sarà possibile reinstallare il sistema senza perdere i dati
- Disabilitare i servizi non necessari
  - Es. HTTP, FTP, Telnet

Buone norme per la sicurezza (4/4)

- Disabilitare l'utente 'root' per l'accesso tramite SSH
  - Modificare il file */etc/ssh/sshd_config*
  - *PermitRootLogin no*
- Disabilitare i permessi di superuser (sudo) a utenti non amministratori
  - Modificare il file */etc/sudoers* tramite *visudo*

2. Gestione delle password

1. Norme per una password robusta
2. Software per la generazione di password

Norme per una password robusta (1/2)

- Sarebbe ideale avere password diverse per ogni situazione
  - Se una password è compromessa, il danno è limitato
- Risulterebbe molto difficile ricordarle tutte
- Un buon compromesso è una password unica, ma robusta

Norme per una password robusta (2/2)

- Non inferiore agli 8 caratteri
- Non contenente il proprio nome utente, vero nome o il nome dell'organizzazione
- Non contenente una parola intera contenuta in un dizionario
- Dovrebbe contenere 3 dei seguenti tipi di carattere
  - Lettere minuscole (a, b, c, ecc.)
  - Lettere maiuscole (A, B, C, ecc.)
  - Numeri (0, 1, 2, ecc.)
  - Caratteri speciali (@, %, !, ecc.)

Software per la generazione di password (1/2)

- Esistono software per la generazione automatica di password robuste
  - Automated Password Generator (APG)
    - *sudo apt-get install apg*

Software per la generazione di password (2/2)

- Generazione di password ‘‘pronunciabili’’
  - *apg*
- Generazione di password con caratteri casuali
  - *apg -a 1*
- *Password casuale basata su input, con 63 caratteri*
  - *apg -s -a 1 -m 63 -n 4*

3. Panoramica su IPTables

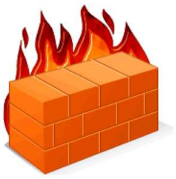
1. Introduzione a IPTables
2. Firewall con IPTables
3. NAT con IPTables
4. GUI per IPTables

Introduzione a IPTables (1/2)

- Linux include un meccanismo per il filtraggio delle informazioni di rete a livello di kernel
  - NetFilter
- La maggior parte delle distribuzioni include un appplicativo per la sua configurazione
  - IPTables

Introduzione a IPTables (2/2)

- IPTables permette la configurazione di diverse funzionalità
  - Firewall
  - NAT
- Verranno presentate velocemente le varie funzionalità



Firewall con IPTables (1/3)

- Ci sono tre insiemi di regole principali (Chain)
  - *Input* (pacchetti in ingresso)
  - *Output* (pacchetti in uscita)
  - *Forward* (pacchetti in transito)

- Visualizzare la configurazione attuale e la policy di default
  - *iptables -L*
  - *Chain INPUT (policy ACCEPT)*
    target prot opt source destination

Firewall con IPTables (2/3)

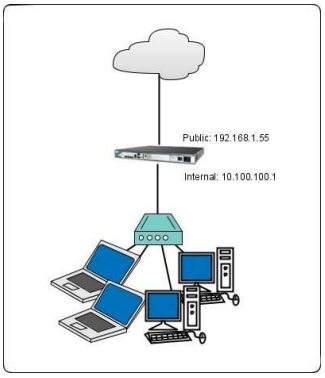
- Una buona regola per un firewall è impostare la policy di default a Drop (blocca tutto)
  - *iptables -P INPUT DROP*
  - Analogamente per Output e Forward

Firewall con IPTables (3/3)

- Alcune regole utili
  - Consentire il traffico interno (interfaccia di loopback)
    - *iptables -A INPUT -i lo -j ACCEPT*
  - Consentire il traffico in ingresso richiesto da noi
    - *iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT*
  - Consentire l'ingresso su porte specifiche (per esempio, la porta 22 se abbiamo configurato un server SSH)
    - *iptables -A INPUT -p tcp --dport 22 -j ACCEPT*

NAT con IPTables (1/4)

- È possibile utilizzare una macchina Linux come gateway tra una rete privata e l'esterno



NAT con IPTables (2/4)

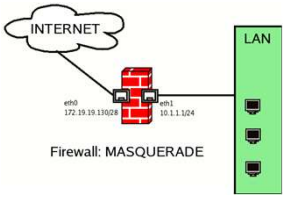
- Una delle operazioni da compiere è configurare il NAT
  - **N**etwork **A**ddress **T**ranslation
  - Più macchine con IP privato possono uscire su internet con lo stesso IP pubblico
  - Tipicamente effettuato dai router casalinghi
- La macchina necessita di due interfacce di rete
  - Esempio:
    - eth1 (rete interna)
    - eth0 (IP pubblico)

NAT con IPTables (3/4)

- Comando per modificare l'IP in uscita dei pacchetti con l'IP pubblico (e rimodificarlo nell'IP privato in ingresso)
  - *iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE*
- Inoltrare i pacchetti in transito dall'interfaccia interna all'interfaccia esterna
  - *iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT*

NAT con IPTables (4/4)

- Inoltrare i pacchetti in transito dall'interfaccia esterna all'interfaccia interna, solo se appartenenti a connessioni iniziate dall'interno
  - *iptables -A FORWARD -i eth0 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT*



GUI per IPTables

- Esistono alcune GUI per configurare IPTables in modo più intuitivo
  - **G**ui for **U**ncomplicated **F**ire**W**all (GUFW)
    - *sudo ufw enable*
    - *sudo apt-get install gufw*
  - Firewall Builder
    - *sudo apt-get install fwbuilder*
  - Firestarter
    - *sudo apt-get install firestarter*

4. Antivirus

1. Perchè usare un antivirus?
2. ClamAV
3. RootkitHunter

Perchè usare un antivirus?

- Una macchina Linux in teoria non ha bisogno di antivirus
- Esistono alcuni casi però in cui un antivirus è consigliabile
  - Server di posta a cui si collegano client Windows
  - Si condividono e scambiano file con utenti Windows
  - Dual-boot sul sistema ma senza un antivirus su Windows
  - Si usa spesso Wine e programmi per Windows

ClamAV (1/2)

- ClamAV è un antivirus utile in ambienti misti
  - Macchine con installati sia Linux che Windows
  - Server di scambio file con Windows
  - Server di posta
- Installazione da linea di comando
  - *sudo apt-get install clamav-daemon*
- Esistono anche interfacce grafiche
  - *sudo apt-get install clamtk*

ClamAV (2/2)

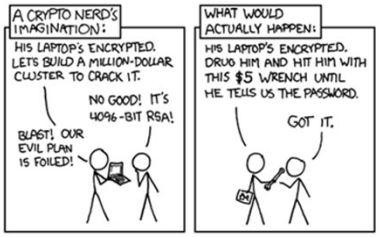
- Integrazione con nautilus
  - *sudo apt-get install nautilus-clamscan*
- Aggiornamento
  - *sudo freshclam*
- Scansione di tutti i file e rimozione dei file infetti
  - *clamscan -r / --remove*

RootkitHunter

- Antivirus per sistemi Linux
- Installazione da linea di comando
  - *sudo apt-get install rkhunter*
- Aggiornamento
  - *sudo rkhunter -update*
- Scansione del sistema
  - *sudo rkhunter -c*

5. Sicurezza del file system

1. Permessi della cartella personale
2. Crittazione dei dati personali



Permessi della cartella personale

- È utile impostare i permessi per la cartella */home*
- Per esempio, per fare in modo che solo l'utente proprietario possa modificarli
  - *chmod 0700 /home/<username>*

Crittazione dei dati personali (1/2)

- Linux mette a disposizione gli strumenti per la crittografia dei dati
  - I dati sono protetti anche se viene fatto l'accesso da altri sistemi operativi
  - I dati sono protetti anche in caso di furto del dispositivo di archiviazione
- Installare il software da linea di comando
  - *sudo apt-get install ecryptfs-utils*

Crittazione dei dati personali (2/2)

- Configurazione
  - *ecryptfs-setup-private*
- I dati sono crittati spostandoli nella cartella nascosta '*Private*'
  - *sudo mount -t ecryptfs /home/<user>/Private*
  - *sudo mv <file> /home/<user>/Private*
- Smontando la cartella, i dati sono illeggibili
  - *sudo umount /home/<user>/Private*

6. Posta elettronica sicura

- Pretty Good Privacy (**PGP**)

Pretty Good Privacy (PGP) (1/2)

- I sistemi basati su Pretty Good Privacy (PGP) permettono lo scambio di messaggi utilizzando una combinazione di crittografia asimmetrica
  - Coppia di chiavi, pubblica e privata
  - Trasmissione cifrata di messaggi anche su canali non sicuri
- Le chiavi possono essere create e gestite a linea di comando o tramite interfacce grafiche
  - Es. Seahorse

Pretty Good Privacy (PGP) (2/2)

- Avviando Seahorse è possible scegliere il tipo di chiavi da creare
  - Le chiavi PGP permettono di inviare email e file in modo sicuro
- Il plugin *enigmail* per thunderbird permette di usare le chiavi PGP

In sintesi

1. Introduzione alla sicurezza in Linux
2. Gestione delle password
3. Panoramica su IPTables
4. Antivirus
5. Sicurezza del file system
6. Posta elettronica sicura

7. Esercizi (1/3)

- Generate una password robusta
  - Riuscereste a ricordarla?
  - Esistono altri software per la generazione di password?
- Cercate i vostri dettagli di login in */ect/passwd*

7. Esercizi (2/3)

- Configurate IPTables per bloccare tutto il traffico di rete
- Configurate IPTables per lasciare passare solo il traffico HTTP
- Eseguite le stesse operazioni utilizzando Firewall Builder

7. Esercizi (3/3)

- Impostate i permessi per la cartella personale in modo che solo un determinato utente possa accedervi
- Installate e configurate *ecryptfs*
  - Provate ad leggere i dati crittati
- (*Per chi ha voglia a casa*) Installate e configurate ClamAV