Esercizio 2 - Server Linux

Perché è stato necessario eseguire ps come root (premettendo il comando con sudo)?

Perché senza privilegi di root, l'utente potrebbe visualizzare solo i processi che ha avviato personalmente mentre con l'abilitazione a **superuser** visualizza informazioni dettagliate su tutti i processi.

Come viene rappresentata la gerarchia dei processi da ps?

```
  503     503     503 ?        00:00:00     at-spi-bus-laun
  509     503     503 ?        00:00:00       dbus-broker-lau
  510     503     503 ?        00:00:00         dbus-broker
  520     520     520 ?        00:00:01     at-spi2-registr
  534     534     534 ?        00:00:00     gpg-agent
  553     553     553 ?        00:00:00     dconf-service
  601     601     601 ?        00:00:10     xfce4-notifyd
  526     526     526 ?        00:00:00   ssh-agent
  622     622     622 ?        00:00:00   upowerd
  668     665     665 ?        00:00:00   VBoxClient
  673     665     665 ?        00:00:00     VBoxClient
  677     676     676 ?        00:00:00   VBoxClient
  679     676     676 ?        00:00:04     VBoxClient
  689     687     687 ?        00:00:00   VBoxClient
  692     687     687 ?        00:00:01     VBoxClient
  774     773     773 ?        00:00:00   VBoxClient
  775     773     773 ?        00:00:00     VBoxClient
 1007    1007    1007 ?        00:00:00   nginx
 1008    1007    1007 ?        00:00:00     nginx
```

Viene rappresentata "a scaletta", i processi figli sono indentati sotto al processo padre.

Qual è il significato delle opzioni -t, -u, -n, -a e -p in netstat?

```
SYNOPSIS
       netstat [address family options] [--tcp|-t] [--udp|-u] [--udplite|-U]
       [--sctp|-S] [--raw|-w] [--l2cap|-2] [--rfcomm|-f] [--listening|-l]
       [--all|-a] [--numeric|-n] [--numeric-hosts] [--numeric-ports] [--nu-
       meric-users] [--symbolic|-N] [--extend|-e[--extend|-e]] [--timers|-o]
       [--program|-p] [--verbose|-v] [--continuous|-c] [--wide|-W]
```

-t -> Mostra solo le connessioni TCP (Transmission Control Protocol).

-u -> Mostra solo le connessioni UDP (User Datagram Protocol).

```
--numeric, -n
    Show  numerical  addresses instead of trying to determine symbolic host,
    port or user names.
```

-n -> Visualizza indirizzi e numeri di porta in formato numerico anziché in nomi host, porte e nomi utente.

```
 -a, --all
     Show both listening and non-listening sockets.   With  the  --interfaces
     option, show interfaces that are not up
```

-a -> Mostra tutte le socket, sia in ascolto che quelle non in ascolto, ovvero le connessioni stabilite o in attesa).

```
-p, --program
    Show  the  PID  and name of the program to which each socket belongs.  A
    hyphen is shown if the socket belongs to the kernel (e.g. a kernel  ser-
    vice,  or  the process has exited but the socket hasn't finished closing
    yet).
```

-p -> Mostra il PID (ID di Processo) e il nome del programma proprietario della socket. Un trattino (-) viene mostrato se il socket appartiene al kernel (per esempio un servizio kernel, o il processo è terminato ma la socket non ha completato ancora la chiusura).

L'ordine delle opzioni è importante per netstat?

No, non è importante e possono essere utilizzate sia in blocco che singolarmente.

```
[analyst@secOps ~]$ sudo netstat -tunap
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:6633            0.0.0.0:*               LISTEN
364/python3.9
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
1007/nginx: master
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
373/sshd: /usr/bin/
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
449/vsftpd
tcp6       0      0 :::22                   :::*                    LISTEN
373/sshd: /usr/bin/
udp        0      0 10.0.2.15:68            0.0.0.0:*
281/systemd-network
```

Basandosi sull'output di netstat mostrato al punto (d), qual è il protocollo di Livello 4, lo stato della connessione e il PID del processo in esecuzione sulla porta 80?

- Protocollo di Livello 4: TCP
- Stato della connessione: LISTEN
- PID del processo: 1007/nginx: master

Sebbene i numeri di porta siano solo una convenzione, puoi indovinare che tipo di servizio è in esecuzione sulla porta 80 TCP?

Di solito la porta 80 è la standard per il server web (http)

```
[analyst@secOps ~]$ sudo ps -elf | grep 395
           [sudo] password for analyst:
           1 S root       395     1  0  80   0 -  1829     19:33 ?        00:00:00 nginx: master process /usr/bin/nginx
           5 S http       396   395  0  80   0 -  1866     19:33 ?        00:00:00 nginx: worker process
           0 S analyst   3789  1872  0  80   0 -  1190     19:53 pts/0    00:00:00 grep 395
```

Il processo PID 395 è nginx. Come si potrebbe concludere questo dall'output sopra?

Osservando la prima riga possiamo concludere che il PID 395 è nginx perché viene indicato come processo master.

Cos'è nginx? Qual è la sua funzione?

Nginx è un Server Web open source ad alte prestazioni noto per la sua architettura asincrona basata su eventi, che gli permette di gestire un numero elevato di connessioni simultanee con un utilizzo minimo di memoria.

Funzioni di NGINX:
Server Web Statico: Serve file statici come HTML, CSS, immagini e JavaScript con grande velocità ed efficienza.

Reverse Proxy: Agisce da intermediario tra i client e i server applicativi di backend, inoltrando le richieste.

Load Balancer (Bilanciatore di Carico): Distribuisce il traffico in entrata su più server per prevenire il sovraccarico e garantire alta disponibilità e scalabilità.

Cache HTTP: Memorizza i contenuti richiesti di frequente per ridurre i tempi di risposta e alleggerire il carico sui server di backend.

La seconda riga mostra che il processo 396 è di proprietà di un utente chiamato http e ha il processo numero 395 come processo genitore. Cosa significa? È un comportamento comune?

Il processo worker viene fatto partire con l'utente http per sicurezza, con privilegi limitati per leggere i file del sito web e scrivere nei file di log; non può accedere a file di sistema critici, modificare configurazioni di altri utenti o prendere il controllo del sistema, garantendo che il processo master e il sistema operativo rimangano protetti in caso di attacco.

Perché l'ultima riga mostra `grep 395`?

Perché è il processo utilizzato per filtrare l'output.
Il comando ps -elf | grep 395:

- Il comando **ps -elf** elenca tutti i processi attivi.
- La **pipe (|)** invia questo elenco al comando **grep**.
- Il comando **grep 395** cerca le righe contenenti la stringa "395".

Poiché l'utilità **grep** è un programma in esecuzione proprio in quel momento, il comando ps la cattura e la elenca nell'output come il processo più recente in esecuzione, con il comando grep 395 visualizzato come descrizione del processo.

Perché l'errore è stato inviato come pagina web?
perché il server nginx la interpreta come un tentativo di inviare una richiesta http e risponderà di conseguenza

Usa Telnet per connetterti alla porta 68. Cosa succede? Spiega.

```
[analyst@secOps ~]$ telnet 127.0.0.1 68
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
```

Quando ho provato a collegarmi con Telnet alla porta 68 su localhost, la connessione è stata rifiutata con il messaggio "Unable to connect to remote host: Connection refused". Questo accade perché la porta 68 non è usata da un servizio TCP in ascolto: è riservata al protocollo DHCP client, che funziona su UDP, non su TCP. Telnet invece tenta una connessione TCP, quindi non trova alcun processo che accetti la connessione e riceve un rifiuto.

Domande di Riflessione

1. Quali sono i vantaggi dell'uso di netstat?

I principali vantaggi dell'uso di netstat sono:

- Diagnostica di Rete: Visualizza rapidamente tutte le connessioni di rete attive (TCP e UDP) e le porte in ascolto (LISTEN) sul sistema.
- Identificazione dei Servizi: Mappa le porte aperte al PID (Process ID) e al nome del programma (p. es., Nginx) responsabile, essenziale per capire quali servizi sono in esecuzione.
- Sicurezza e Troubleshooting: Permette di rilevare servizi non autorizzati e aiuta a diagnosticare problemi di connettività o conflitti di porta.

2. Quali sono i vantaggi dell'uso di Telnet? È sicuro?

Trasmissione in Chiaro (Unencrypted): La ragione principale per cui non è sicuro è che telnet trasmette tutti i dati, incluse le credenziali di accesso (username e password), completamente in testo non cifrato sulla rete. Chiunque sia in grado di intercettare il traffico (ad esempio, tramite sniffing) può leggere l'intera sessione.

Alternativa Sicura: Per l'accesso remoto a un server, telnet è stato completamente sostituito da SSH (Secure Shell). SSH svolge la stessa funzione di terminale remoto, ma cripta (cifra) l'intera sessione di comunicazione, rendendola sicura da intercettazioni.

In sintesi, no, Telnet non è sicuro. Va usato solo come strumento diagnostico occasionale per testare l'apertura delle porte, ma mai per l'accesso remoto o la trasmissione di dati sensibili.