Esercizio 2: Server Linux

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

è stato necessario perchè ps richiede di far vedere i processi, se viene eseguito tramite utente basico si riescono vedere i processi di quel singolo utente. se si fa sudo si riescono a vedere tutti i processi anche quelli amministrativi.

2. Come viene rappresentata la gerarchia dei processi da `ps`?

ci sono i processi che partono da 0 che sarebbero i processi del kernel, dopo a susseguirsi abbiamo processo 1 che è per (system/init) comandati dal utente:root. dopo abbiamo i vari processi che prima erano un massimo di 32768 ora invece sono anche di pi.
da questa informazioni il kernel associa grazie a un gerarchia i vari pid per ogni processo.

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

- `-a` mostra tutte le connessioni e le porte in ascolto
- `-n` mostra indirizzi e porte in formato numerico, non risolve i nomi
- `-t` (TCP)
- `-u` (udp)
- `-p` (pid)

  L'ordine delle opzioni non è importante.

4. 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: **395** (`nginx: master`)

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

La porta 80 TCP è convenzionalmente usata per HTTP.
Quindi è molto probabile che sia un web server.
Vista la distro, ipotizzo nginx.

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

Si conclude perché l'output di `netstat` con l'opzione `-p` mostra direttamente il nome del processo associato al PID.
In alternativa si può confermare con systemctl status nginx

7. Cos'è nginx? Qual è la sua funzione?

Nginx è un web server che può fare anche da reverse proxy.
È molto usato perché leggero.
Protegge e gestisce il traffico.

8. 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?

Sì, è normale.
In Linux un processo "padre" può creare "figli" con la funzione `fork()` seguita da `exec()`.
Ogni figlio ha un PID diverso, ma eredita le caratteristiche del padre come i file desriptor.
Il padre resta attivo tramite il richiamo della funzione waitpid(). per qualunque esigenza abbia il"figlio" parlerà direttamente con il kernel. in questo caso abbiamo che il padre "root395" ha un figlio che è un http 396.

9. Perché l'ultima riga mostra `grep 395`?

Perché anche `grep` è un processo vero e proprio.
essendo che si richiede di fare un filtro, il kernel lo vede come un processo ed essendo un processo gli associa un pid per riconoscerlo.

10. Perché l’errore è stato inviato come pagina web?

Perché quando un server web non capisce una richiesta, restituisce un codice di errore HTTP (es. 404, 500) insieme a una pagina che spiega l’errore.
in cui comunica come lui è stato costruito, cosi da poter dare un indizio all’utente per capire come deve interagire con il server web davanti.

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

Risultato: connessione rifiutata.
Inizialmente sembrava un problema del servizio, ma poi ho scoperto che DHCP usa UDP, non TCP.
Telnet funziona solo con TCP: siccome la porta 68 ascolta in UDP, non ci sarà mai handshake.
Per questo la connessione viene sempre rifiutata.

12. Domande di riflessione

1. **Quali sono i vantaggi dell’uso di netstat?**
    - Permette di vedere connessioni, porte aperte, processi associati.
    - Utile per debug di rete e sicurezza.
    - Anche se è “vecchio”, resta intuitivo.
2. **Quali sono i vantaggi dell’uso di Telnet? È sicuro?**
    - Vantaggi: semplice, diretto, rapido per testare connessioni TCP.
    - Svantaggi: è **insicuro** (trasmette in chiaro, nessuna cifratura).
    - Oggi è sostituito da strumenti più moderni ss/nc ecc, essendo più personalizzabile e sicuro”essendo che vengono patchati in confronto a telnet e netstat”.