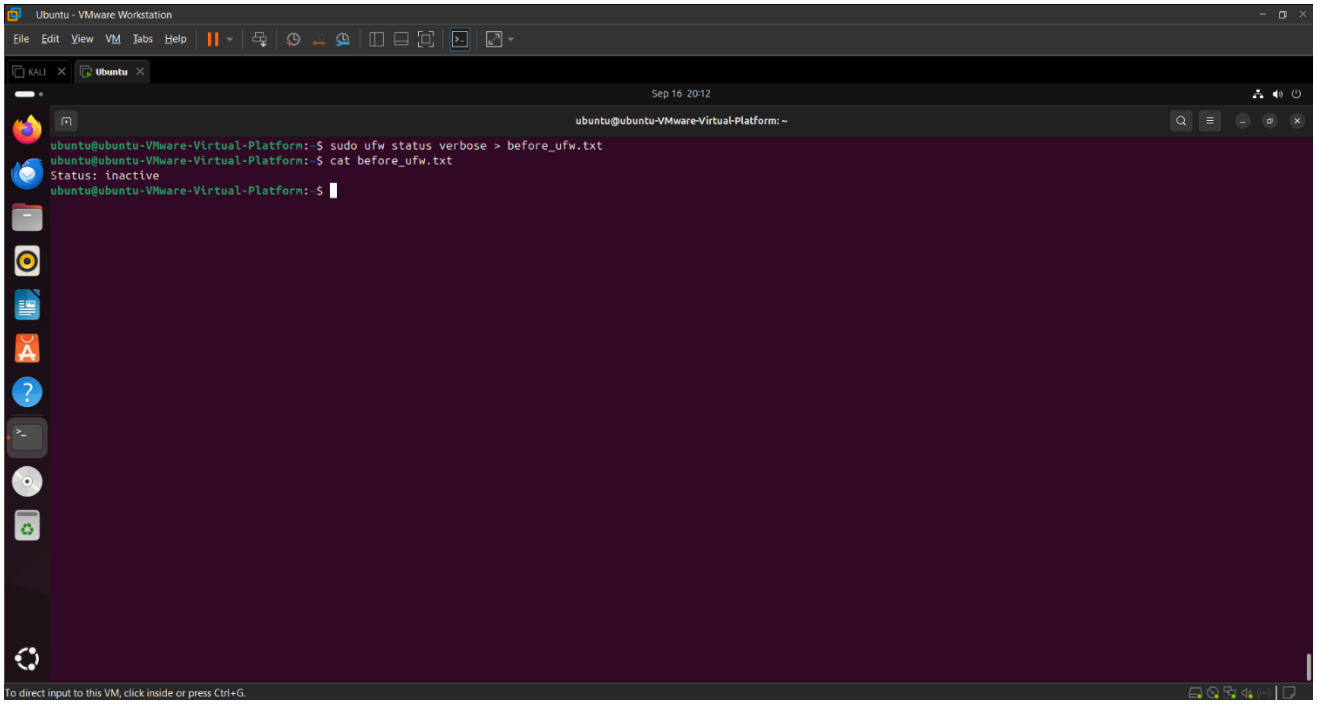
Linux Server Hardening

Objective

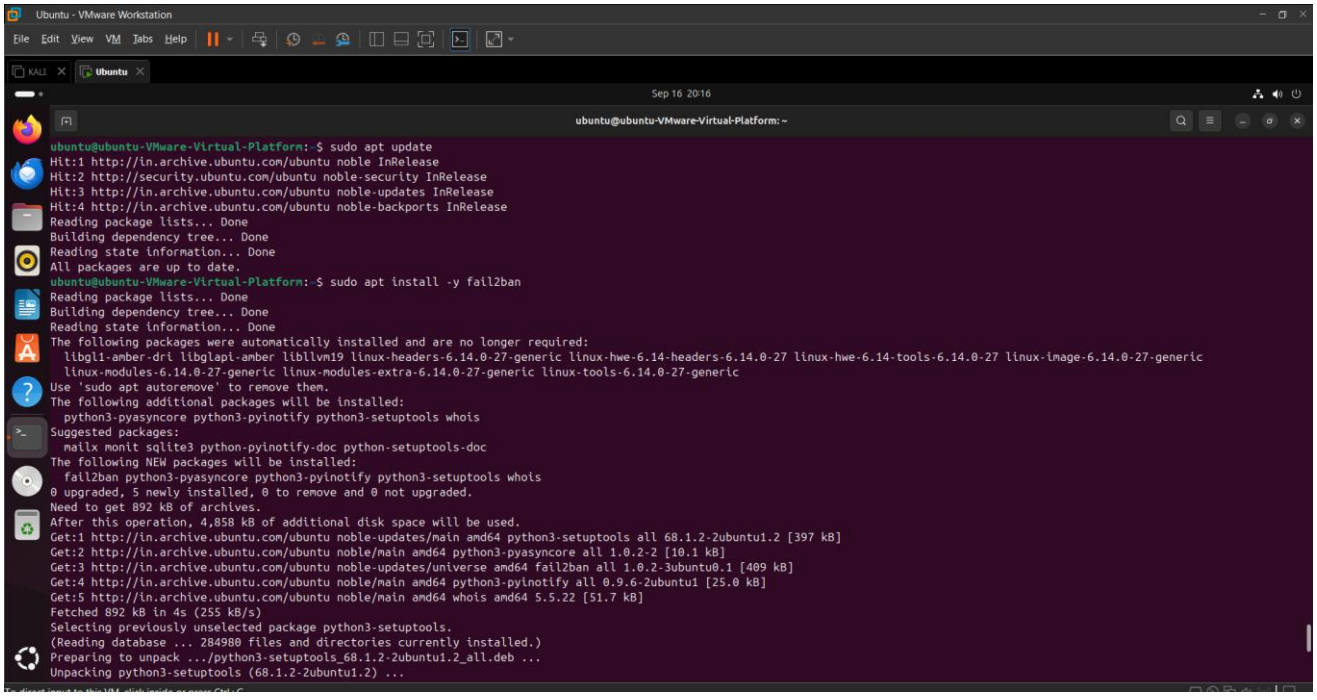
Capture and analyze live network traffic to identify credentials or suspicious activity. Apply Linux server hardening techniques using Ubuntu, UFW, Fail2ban, and SSH.

Before State

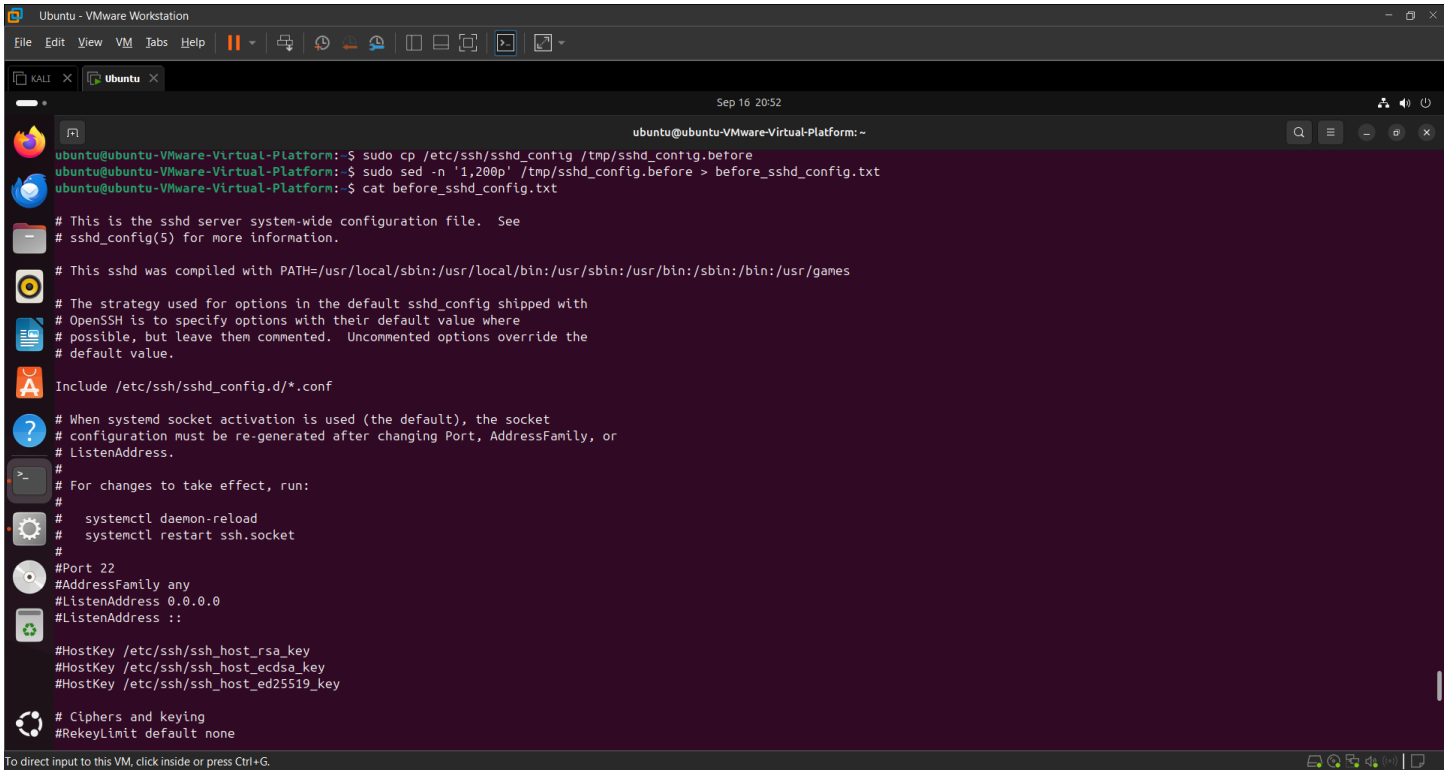
- Firewall (UFW): Inactive



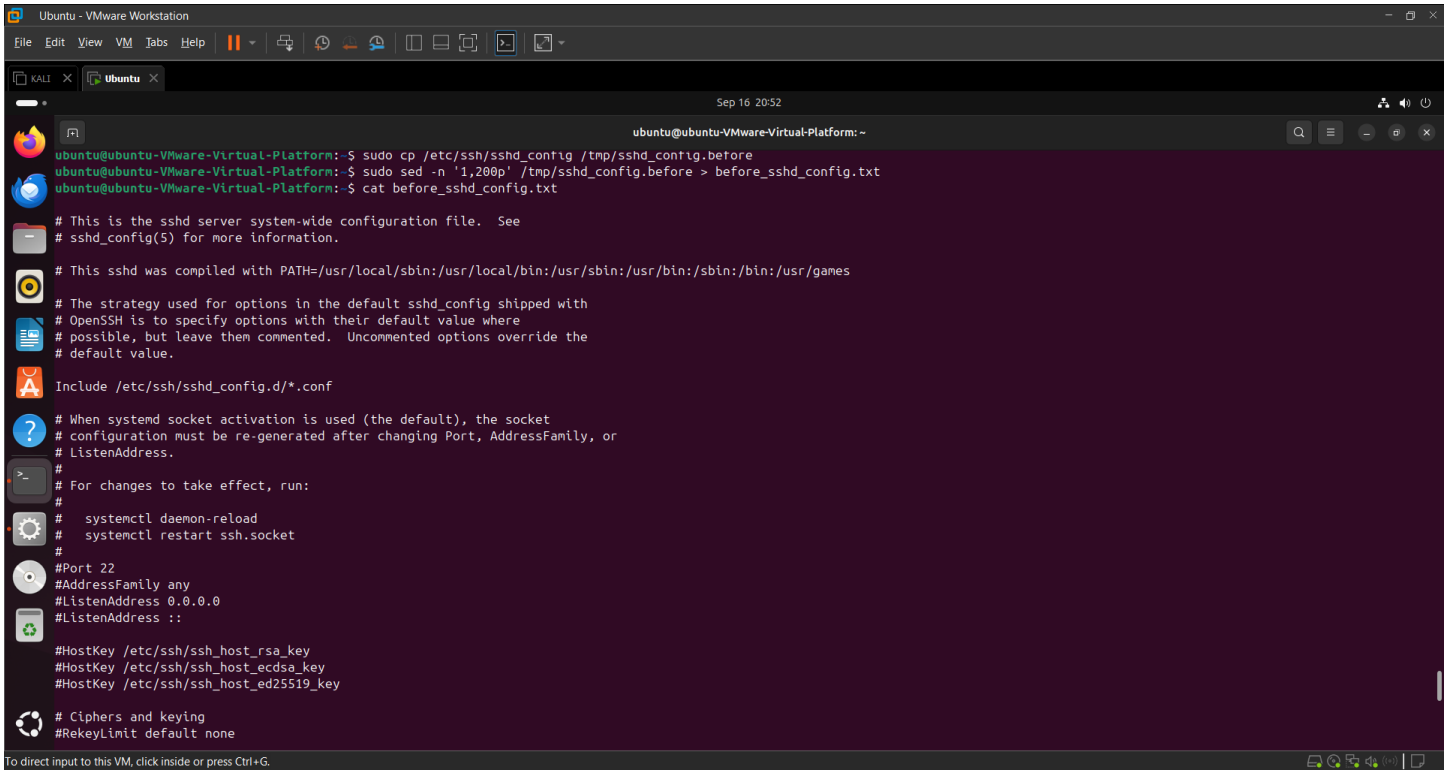
- Fail2ban: Not installed ("Unit fail2ban.service could not be found")



- SSH configuration: Root login allowed, password authentication enabled



- Open Ports: 22 (SSH), 80 (HTTP), 3306 (MySQL – exposed)



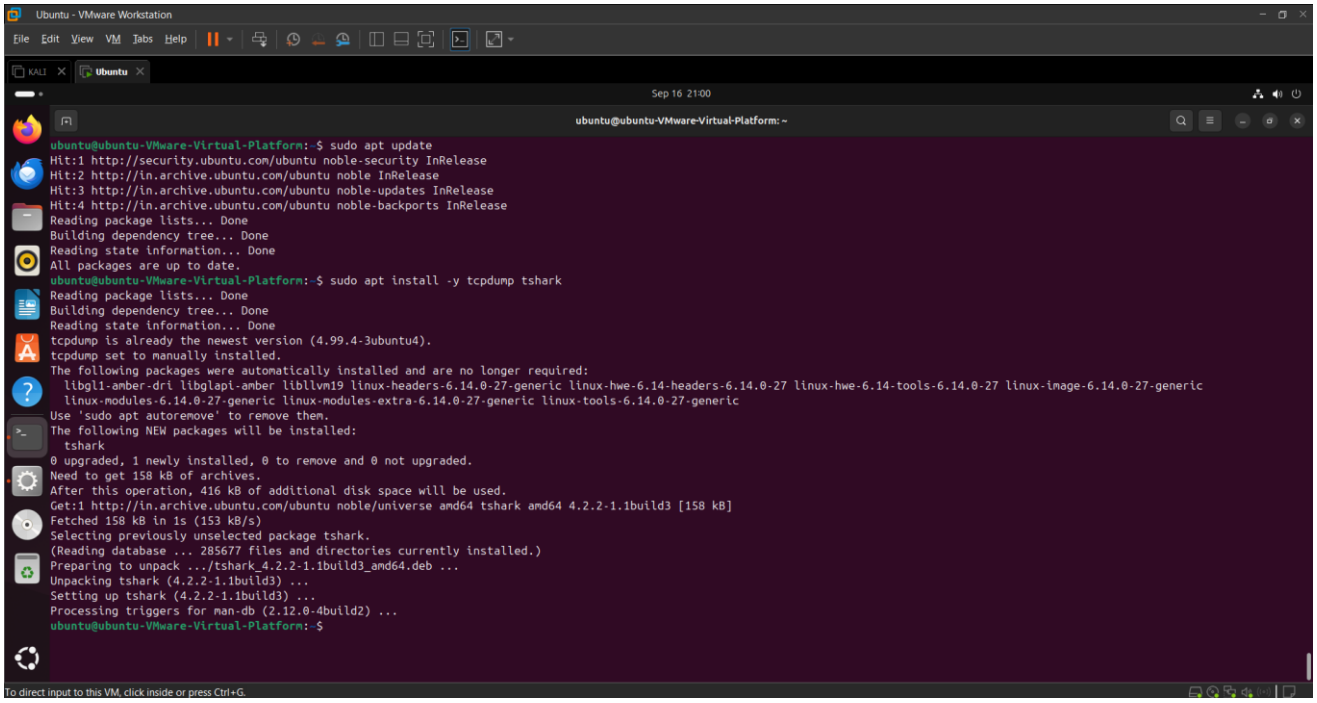
Live capture — safe, targeted capturing:

Important: Capturing everything can expose sensitive data. Only capture what you are authorized to. Use filters to limit scope to suspicious protocols or hosts.

Update and install the tcpdump and tshark by running below commands

-sudo apt update

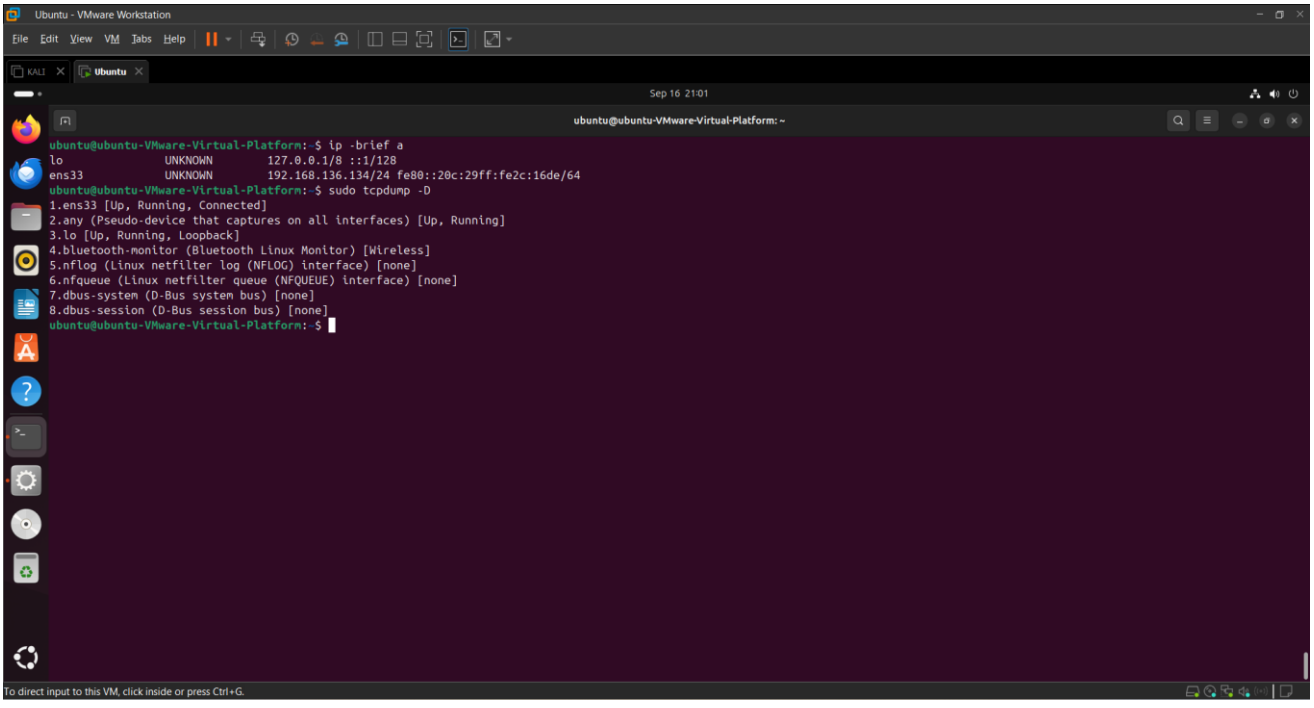
-sudo apt install -y tcpdump tshark



To List network interfaces commands used are :

-ip -brief a

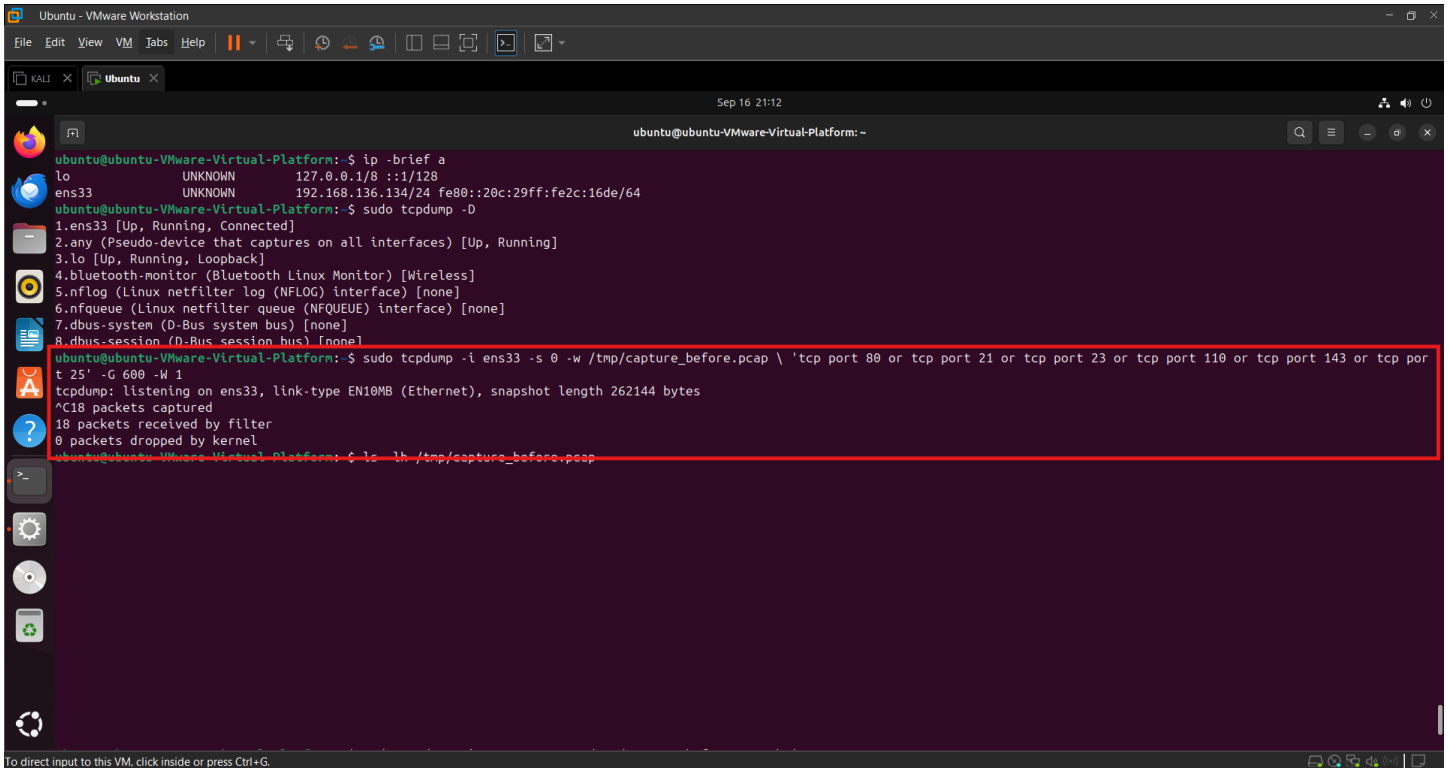
-sudo tcpdump -D



Capture common cleartext authentication protocols (FTP, Telnet, POP3, IMAP, SMTP) for 10 minutes by using below command:

replace ens33 with your interface from tcpdump -D

-sudo tcpdump -i ens33 -s 0 -w /tmp/capture_before.pcap \ 'tcp port 80 or tcp port 21 or tcp port 23 or tcp port 110 or tcp port 143 or tcp port 25' -G 600 -W 1



Notes:

- -s 0 captures full packet.
- -w writes pcap for later analysis.
- Use -G with -W to rotate files by seconds if long run needed.
- It will listen for 10 minutes (-G 600).
- It will write all captured packets that match your filter into /tmp/capture_before.pcap
- If there’s no traffic on those ports (80, 21, 23, 110, 143, 25), the file might remain very small or even empty.

Verify capture file by using this below command:

ls -lh /tmp/capture_before.pcap