

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

The screenshot shows a VMware Workstation window titled 'Ubuntu - VMware Workstation'. Inside, a virtual machine named 'Ubuntu' is running. The terminal window shows the following commands and output:

```
ubuntu@ubuntu-VMware-Virtual-Platform:~$ sudo ufw status verbose > before_ufw.txt
ubuntu@ubuntu-VMware-Virtual-Platform:~$ cat before_ufw.txt
Status: inactive
ubuntu@ubuntu-VMware-Virtual-Platform:~$
```

The terminal window title is 'ubuntu@ubuntu-VMware-Virtual-Platform: ~'. The VMware interface shows the 'Ubuntu' VM is running, and the host is 'KALI'.

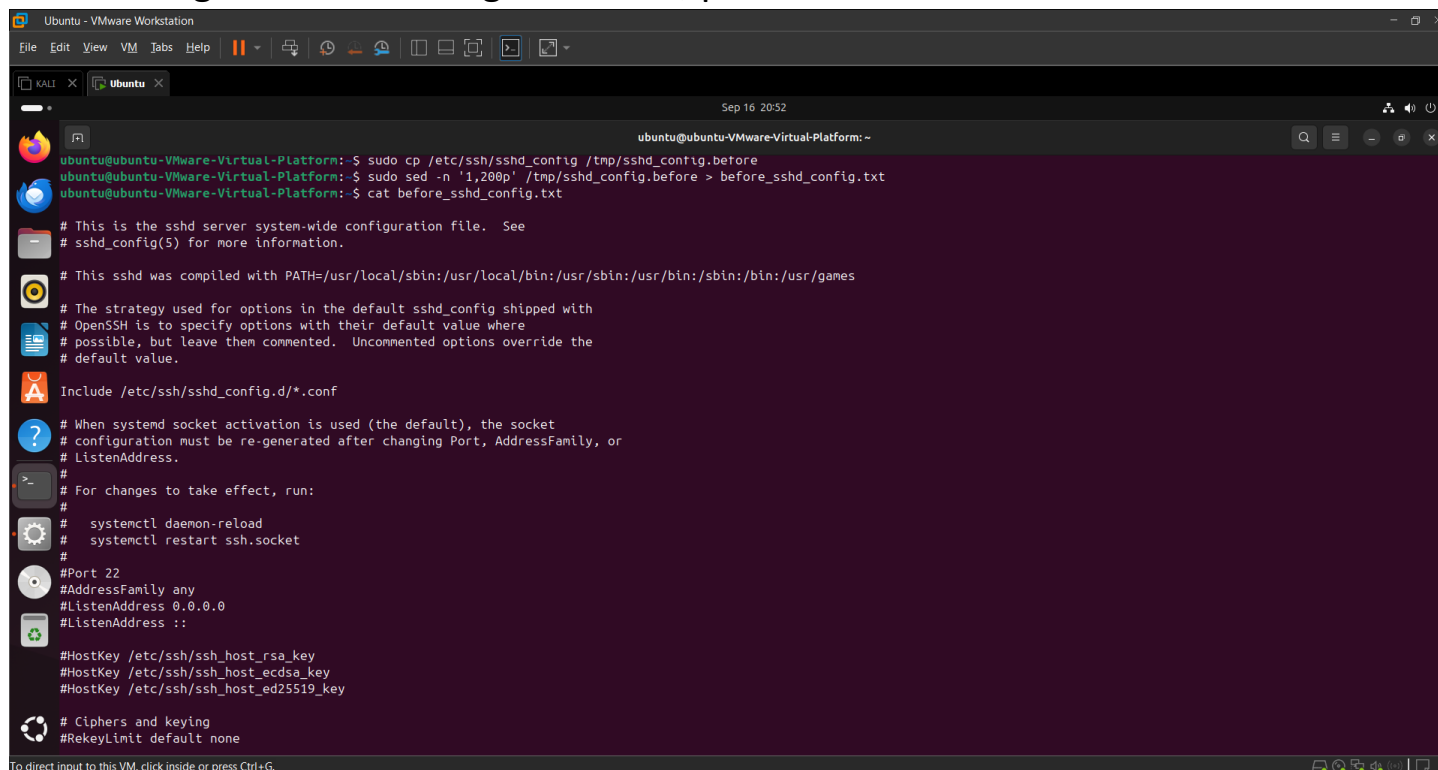
- Fail2ban: Not installed ("Unit fail2ban.service could not be found")

```

ubuntu@ubuntu-Virtual-Platform: ~
File Edit View VM Tabs Help
KALI x Ubuntu x
Sep 16 2016
ubuntu@ubuntu-Virtual-Platform: ~
ubuntu@ubuntu-Virtual-Platform:~$ sudo apt update
Hit:1 http://in.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:4 http://in.archive.ubuntu.com/ubuntu noble-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
ubuntu@ubuntu-Virtual-Platform:~$ sudo apt install -y fail2ban
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libgl1-amd64-dri libglapi-amd64 libllvm19 linux-headers-6.14.0-27-generic linux-hwe-6.14-headers-6.14.0-27 linux-hwe-6.14-tools-6.14.0-27 linux-image-6.14.0-27-generic
  linux-modules-6.14.0-27-generic linux-modules-extra-6.14.0-27-generic linux-tools-6.14.0-27-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  python3-pyasyncore python3-pyinotify python3-setuptools whois
Suggested packages:
  mailx monit sqlite3 python-pyinotify-doc python-setuptools-doc
The following NEW packages will be installed:
  fail2ban python3-pyasyncore python3-pyinotify python3-setuptools whois
0 upgraded, 5 newly installed, 0 to remove and 0 not upgraded.
Need to get 892 kB of archives.
After this operation, 4,859 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu noble-updates/main amd64 python3-setuptools all 68.1.2-2ubuntu1.2 [397 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu noble/main amd64 python3-pyasyncore all 1.0.2-2 [10.1 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu noble-updates/universe amd64 fail2ban all 1.0.2-3ubuntu0.1 [409 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu noble/main amd64 python3-pyinotify all 0.9.6-2ubuntu1 [25.0 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu noble/main amd64 whois amd64 5.5.22 [51.7 kB]
Fetched 892 kB in 4s (255 kB/s)
Selecting previously unselected package python3-setuptools.
(Reading database ... 284980 files and directories currently installed.)
Preparing to unpack .../python3-setuptools_68.1.2-2ubuntu1.2_all.deb ...
Unpacking python3-setuptools (68.1.2-2ubuntu1.2) ...

```

- SSH configuration: Root login allowed, password authentication enabled



The screenshot shows a terminal window titled 'Ubuntu - VMware Workstation' with a sub-tab 'Ubuntu'. The terminal displays the following commands and output:

```
ubuntu@ubuntu-VMware-Virtual-Platform:~$ sudo cp /etc/ssh/sshd_config /tmp/sshd_config.before
ubuntu@ubuntu-VMware-Virtual-Platform:~$ sudo sed -n '1,200p' /tmp/sshd_config.before > before_sshd_config.txt
ubuntu@ubuntu-VMware-Virtual-Platform:~$ cat before_sshd_config.txt
```

The output of the `cat` command shows the contents of the `/etc/ssh/sshd_config` file, including comments and configuration options:

```
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

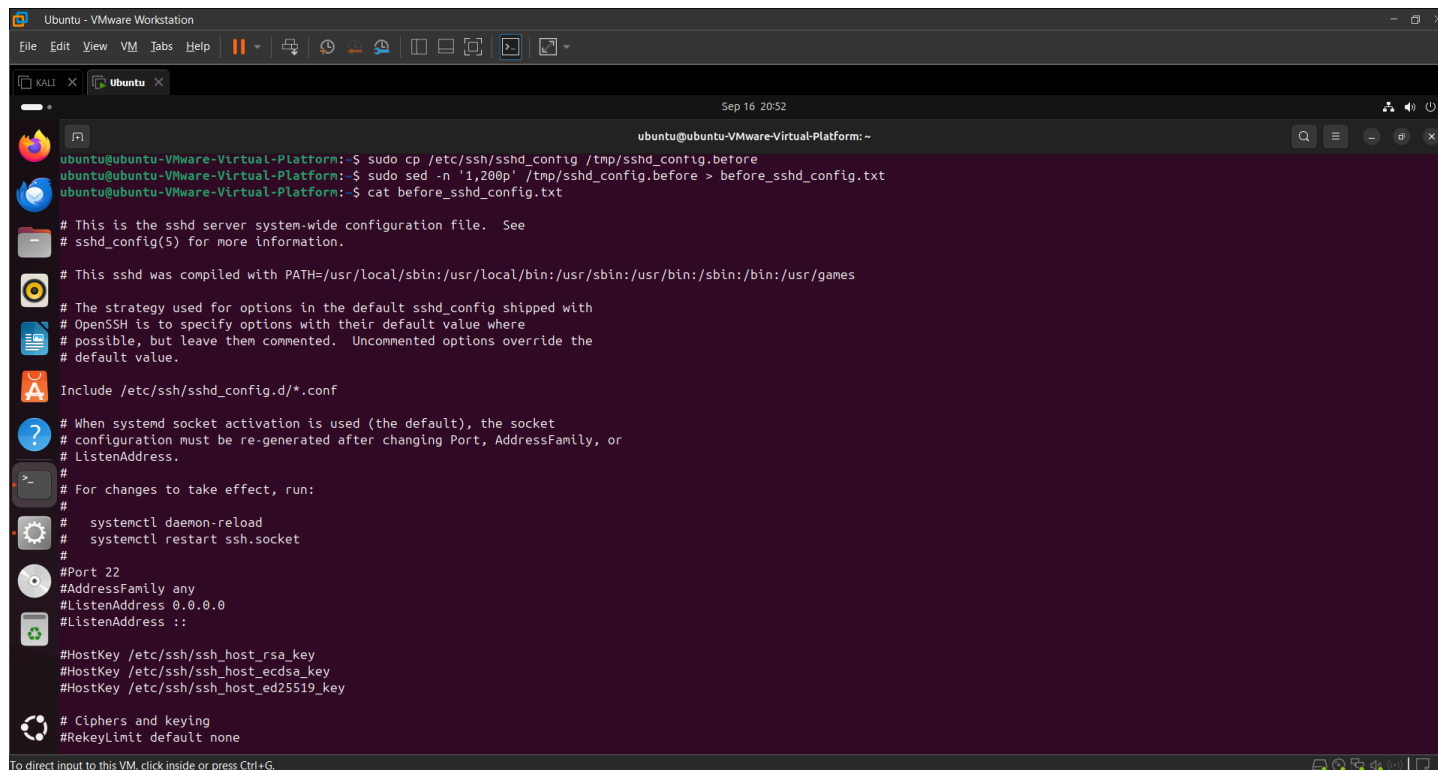
Include /etc/ssh/sshd_config.d/*.conf

# When systemd socket activation is used (the default), the socket
# configuration must be re-generated after changing Port, AddressFamily, or
# ListenAddress.
#
# For changes to take effect, run:
#
#   systemctl daemon-reload
#   systemctl restart ssh.socket
#
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none
```

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



This screenshot is identical to the one above, showing the same terminal window with the same commands and output for the SSH configuration process.

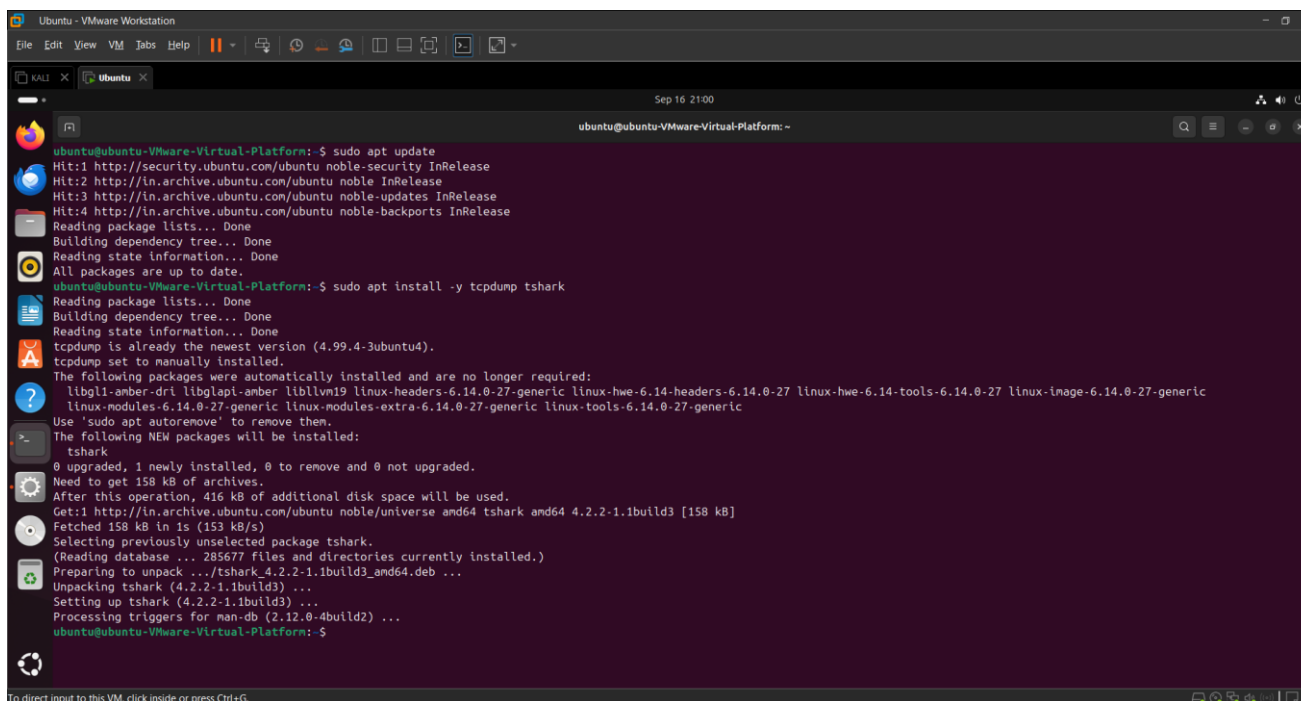
Live capture — safe, targeted capturing:

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

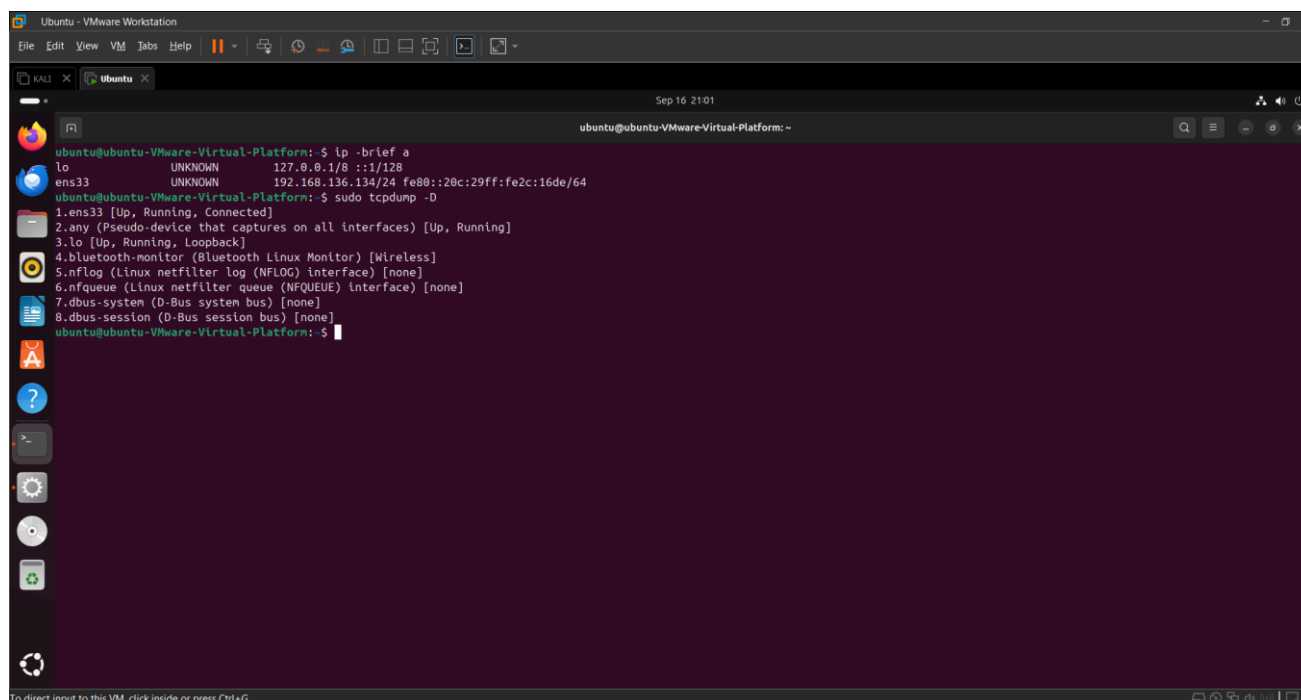


```
ubuntu@ubuntu-VMware-Virtual-Platform:~$ sudo apt update
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://in.archive.ubuntu.com/ubuntu noble InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:4 http://in.archive.ubuntu.com/ubuntu noble-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
ubuntu@ubuntu-VMware-Virtual-Platform:~$ sudo apt install -y tcpdump tshark
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
tcpdump is already the newest version (4.99.4-3ubuntu4).
tcpdump set to manually installed.
The following packages were automatically installed and are no longer required:
  libgl1-amd64 libglapi-amd64 libllvm19 linux-headers-6.14.0-27-generic linux-hwe-6.14-headers-6.14.0-27-generic linux-hwe-6.14-tools-6.14.0-27-generic linux-image-6.14.0-27-generic
  linux-modules-6.14.0-27-generic linux-modules-extra-6.14.0-27-generic linux-tools-6.14.0-27-generic
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  tshark
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 158 kB of archives.
After this operation, 416 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 tshark amd64 4.2.2-1.1build3 [158 kB]
Fetched 158 kB in 1s (153 kB/s)
Selecting previously unselected package tshark.
(Reading database ... 285677 files and directories currently installed.)
Preparing to unpack .../tshark_4.2.2-1.1build3_amd64.deb ...
Unpacking tshark (4.2.2-1.1build3) ...
Setting up tshark (4.2.2-1.1build3) ...
Processing triggers for man-db (2.12.0-4build2) ...
ubuntu@ubuntu-VMware-Virtual-Platform:~$
```

To List network interfaces commands used are :

-ip -brief a

-sudo tcpdump -D

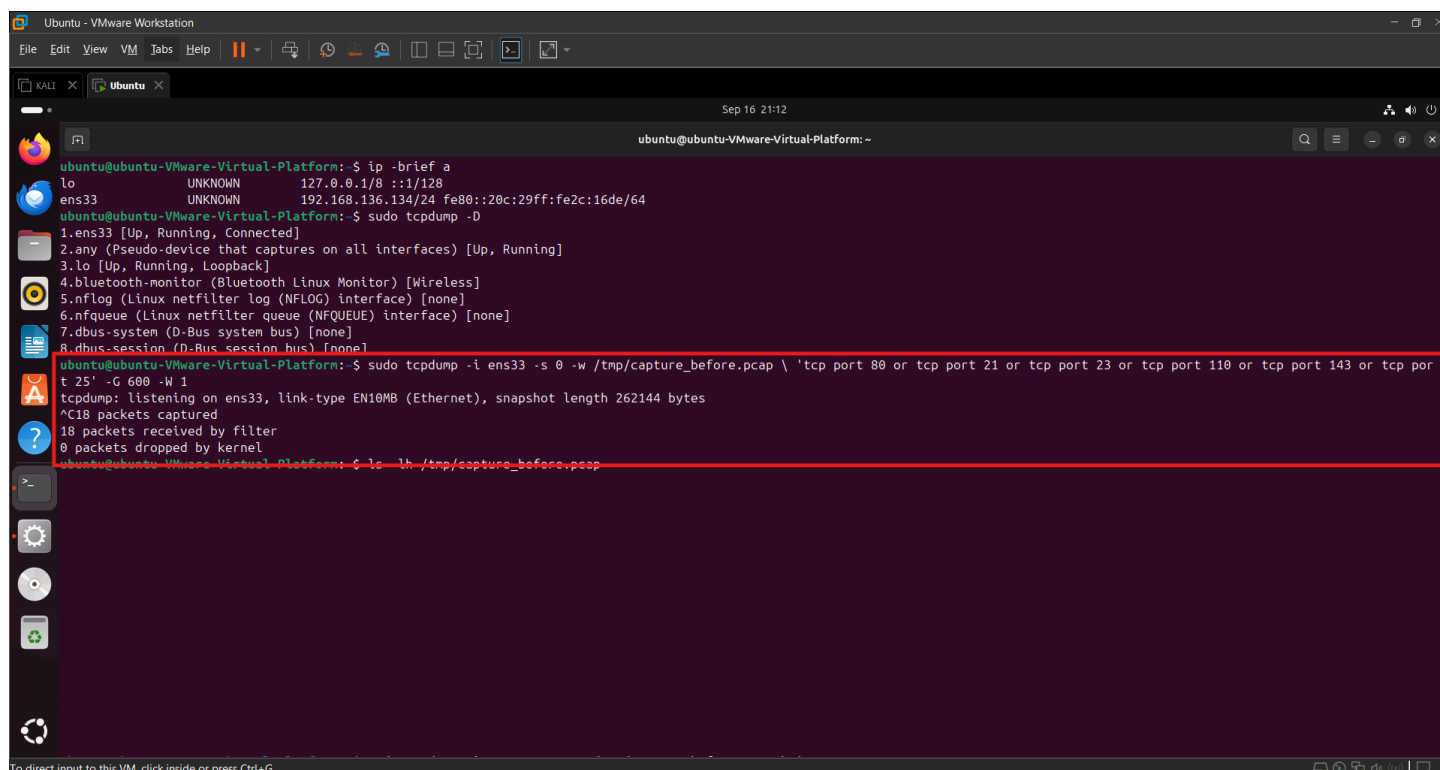


```
ubuntu@ubuntu-VMware-Virtual-Platform:~$ ip -brief a
lo UNKNOWN 127.0.0.1/8 ::1/128
ens33 UNKNOWN 192.168.136.134/24 fe80::20c:29ff:fe2c:16de/64
ubuntu@ubuntu-VMware-Virtual-Platform:~$ sudo tcpdump -D
1.ens33 [Up, Running, Connected]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth-monitor (Bluetooth Linux Monitor) [Wireless]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
7.dbus-system (D-Bus system bus) [none]
8.dbus-session (D-Bus session bus) [none]
ubuntu@ubuntu-VMware-Virtual-Platform:~$
```

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



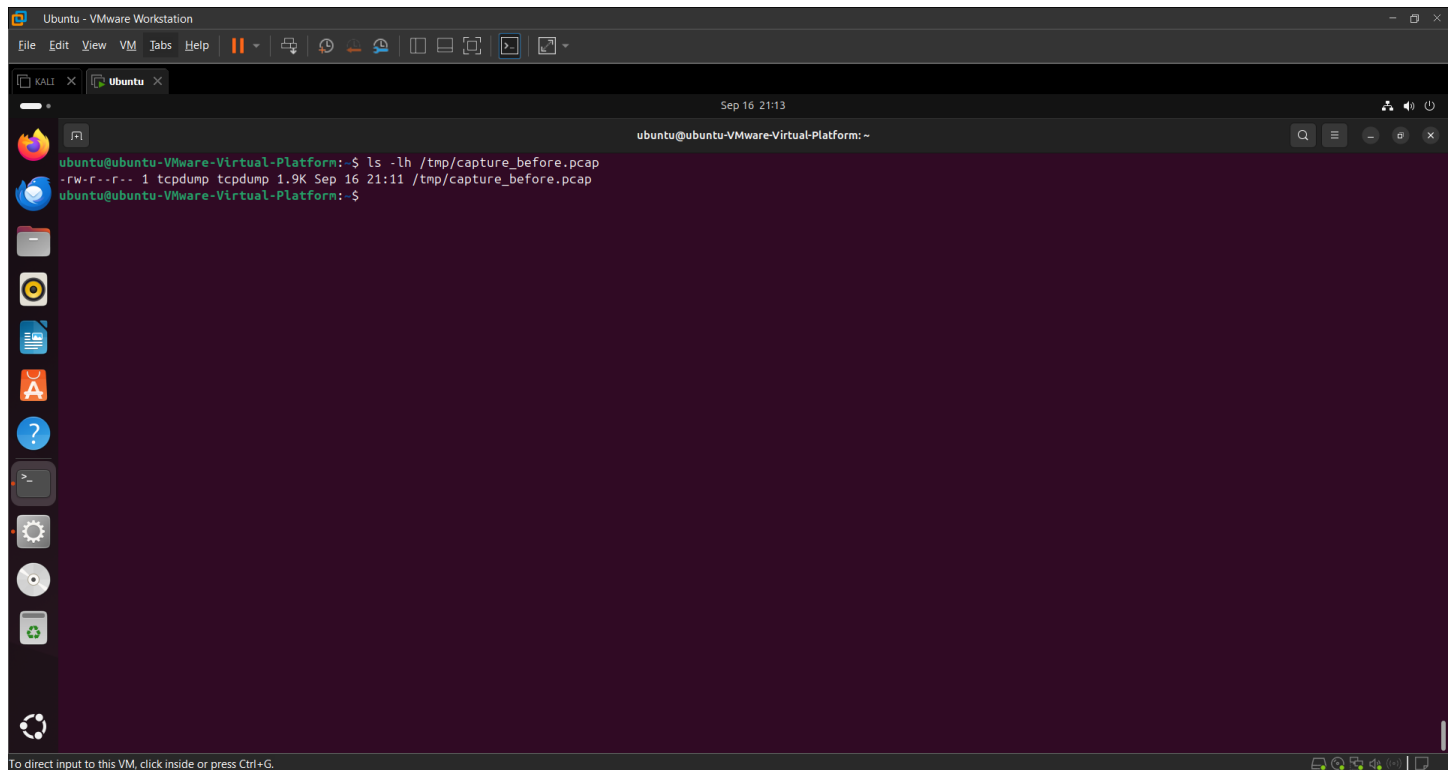
```
ubuntu@ubuntu-VMware-Virtual-Platform:~$ ip -brief a
lo                UNKNOWN    127.0.0.1/8 ::1/128
ens33             UNKNOWN    192.168.136.134/24 fe80::20c:29ff:fe2c:16de/64
ubuntu@ubuntu-VMware-Virtual-Platform:~$ sudo tcpdump -D
1.ens33 [Up, Running, Connected]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth-monitor (Bluetooth Linux Monitor) [Wireless]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
7.dbus-system (D-Bus system bus) [none]
8.dbus-session (D-Bus session bus) [none]
ubuntu@ubuntu-VMware-Virtual-Platform:~$ 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
tcpdump: listening on ens33, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C18 packets captured
18 packets received by filter
0 packets dropped by kernel
ubuntu@ubuntu-VMware-Virtual-Platform:~$ ls -lh /tmp/capture_before.pcap
```

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
```



The screenshot shows a VMware Workstation window titled "Ubuntu - VMware Workstation". Inside the window, there is a terminal window titled "ubuntu@ubuntu-VMware-Virtual-Platform: ~". The terminal shows the following command and output:

```
ubuntu@ubuntu-VMware-Virtual-Platform:~$ ls -lh /tmp/capture_before.pcap
-rw-r--r-- 1 tcpdump tcpdump 1.9K Sep 16 21:11 /tmp/capture_before.pcap
ubuntu@ubuntu-VMware-Virtual-Platform:~$
```

The terminal window has a dark purple background. The VMware Workstation window has a menu bar with "File", "Edit", "View", "VM", "Tools", and "Help". The status bar at the bottom of the VMware window says "To direct input to this VM, click inside or press Ctrl+G."