

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 Kali Linux virtual machine environment. The main window is titled 'Ubuntu' and displays a terminal session. The terminal prompt is 'ubuntu@ubuntu-VMware-Virtual-Platform: ~'. The user has entered the command 'sudo ufw status verbose' and the output is 'Status: inactive'. The terminal also shows the command 'cat before_ufw.txt' being executed. The VMware interface includes a top menu bar with 'File', 'Edit', 'View', 'VM', 'Tabs', and 'Help'. The left sidebar shows the 'Ubuntu' VM is running. The bottom status bar indicates 'To direct input to this VM, click inside or press Ctrl+G.'

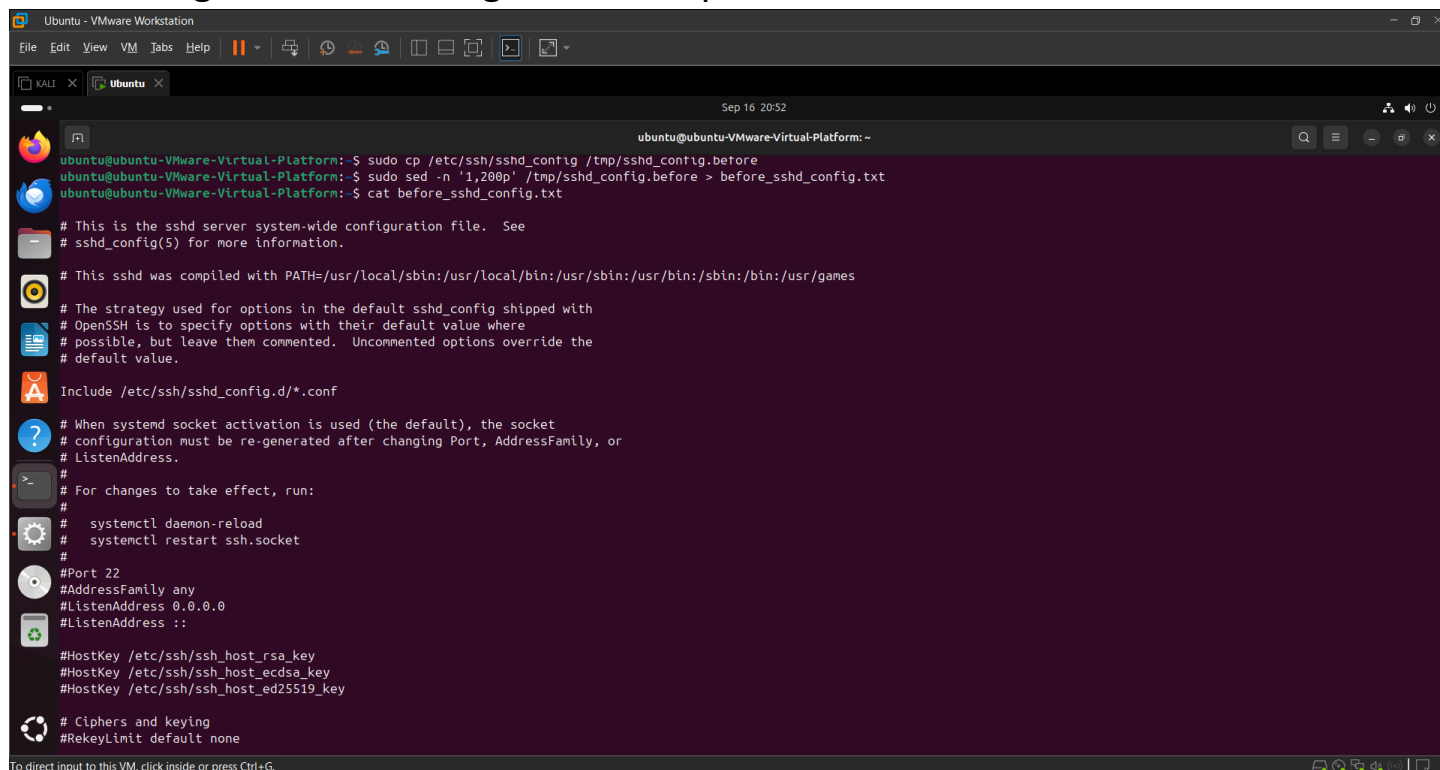
- Fail2ban: Not installed ("Unit fail2ban.service could not be found")

```

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 will be automatically installed and are no longer required:
  libgl1-amd64-dri liblapack amd64 liblapack-dev liblapack90 linux-hwe-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-window '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

# 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.

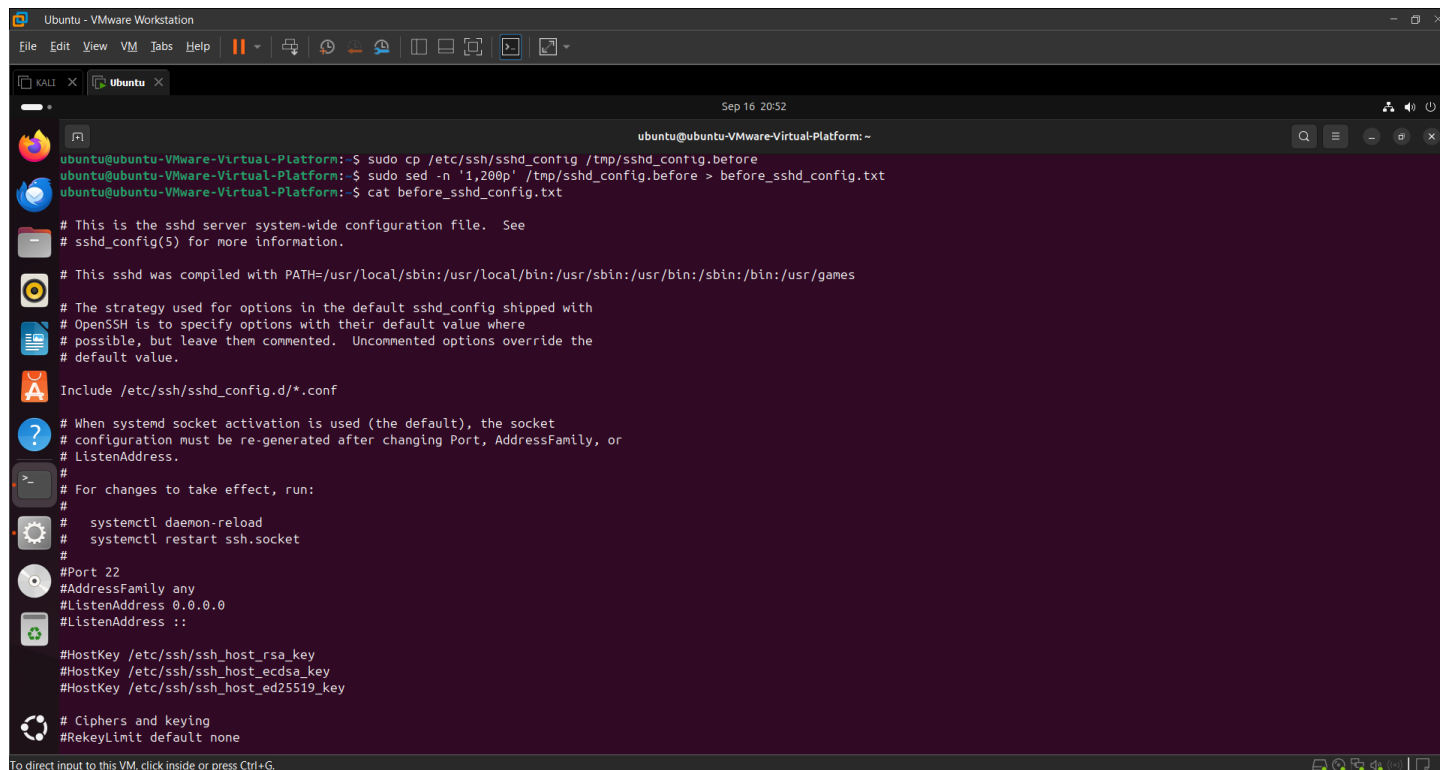
Include /etc/ssh/sshd_config.d/*.conf

# 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 commands and output for SSH configuration.

Legal / Ethical reminder

Only capture and analyze traffic on systems/networks you own or for which you have written permission. Finding credentials on other people's networks without permission is illegal and unethical.

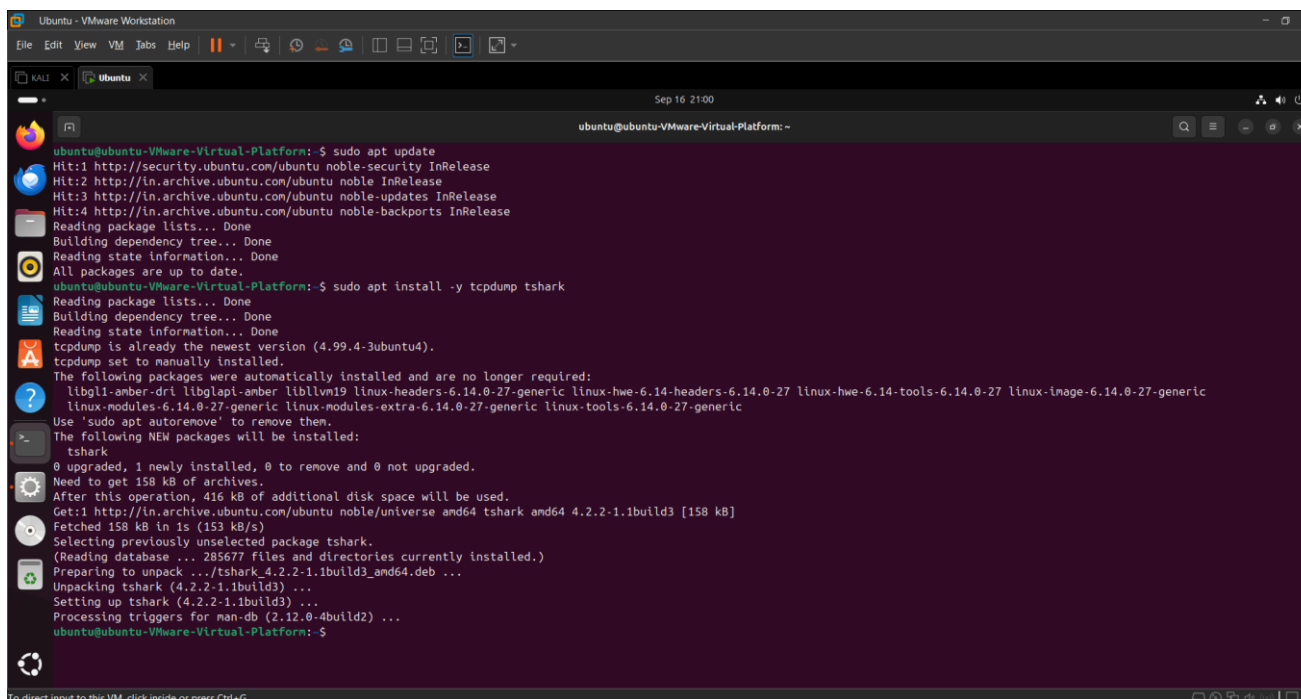
Live capture — safe, targeted capturing:

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

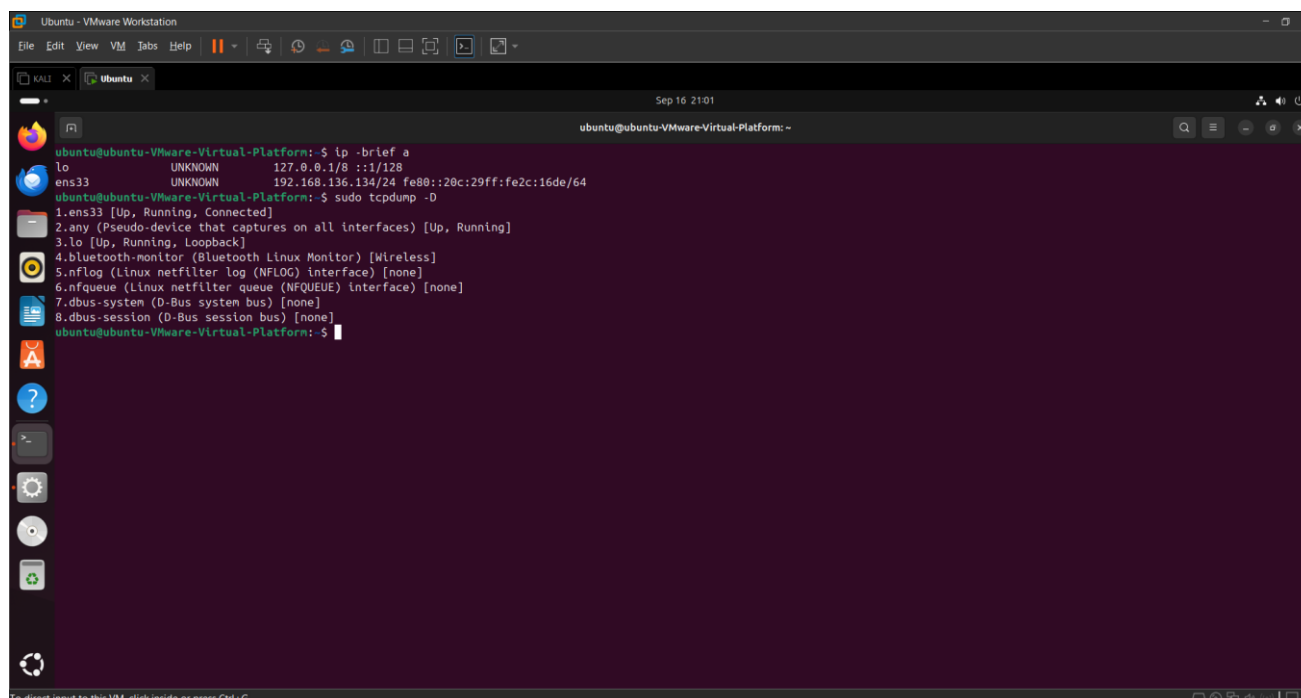


```
ubuntu@ubuntu-VMware-Virtual-Platform:~$ sudo apt update
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://in.archive.ubuntu.com/ubuntu noble InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:4 http://in.archive.ubuntu.com/ubuntu noble-backports 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 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 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

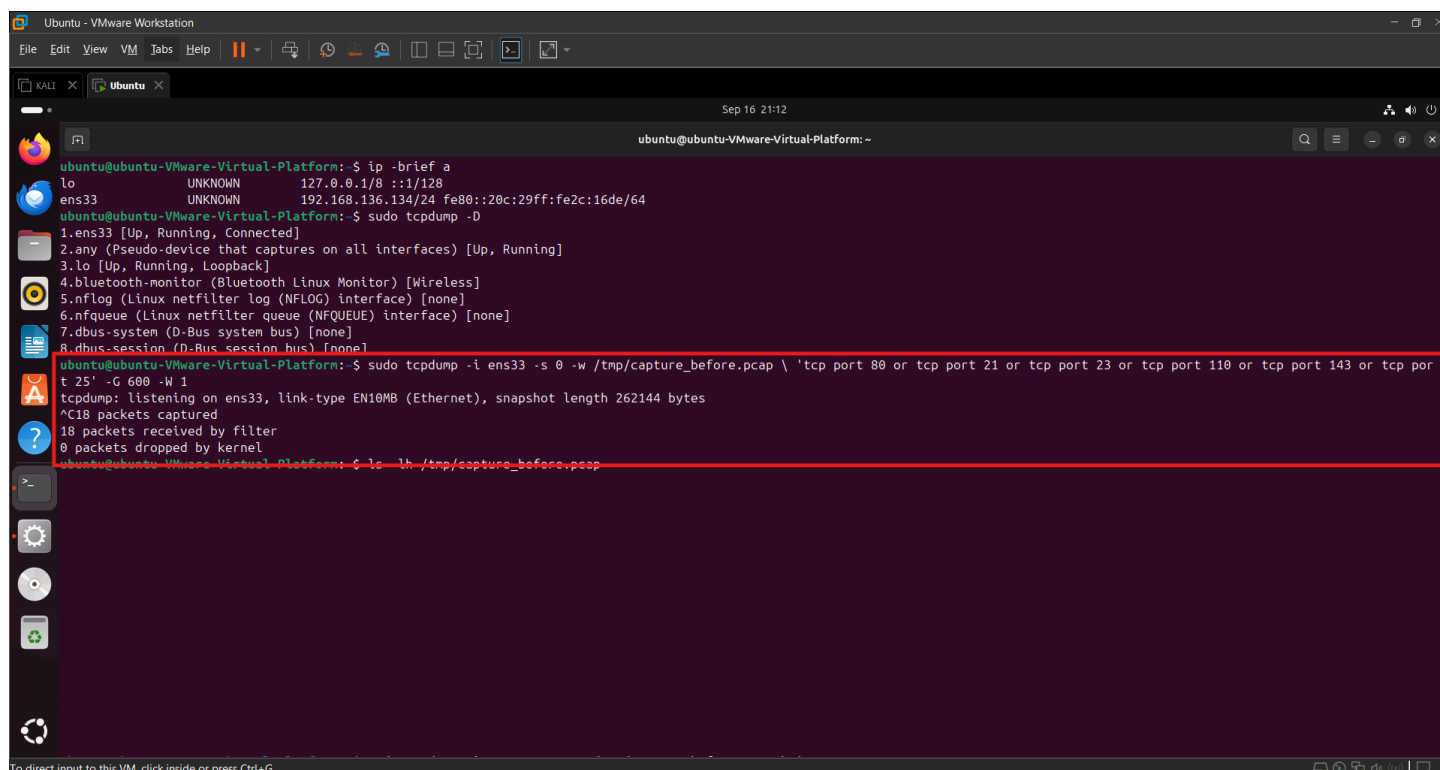


```
ubuntu@ubuntu-VMware-Virtual-Platform:~$ ip -brief a
lo          UNKNOWN    127.0.0.1/8 ::1/128
ens33       UNKNOWN    192.168.136.134/24 fe80::20c:29ff:fe2c:16de/64
ubuntu@ubuntu-VMware-Virtual-Platform:~$ sudo tcpdump -D
1.ens33 [Up, Running, Connected]
2.any (Pseudo-device that captures on all 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]

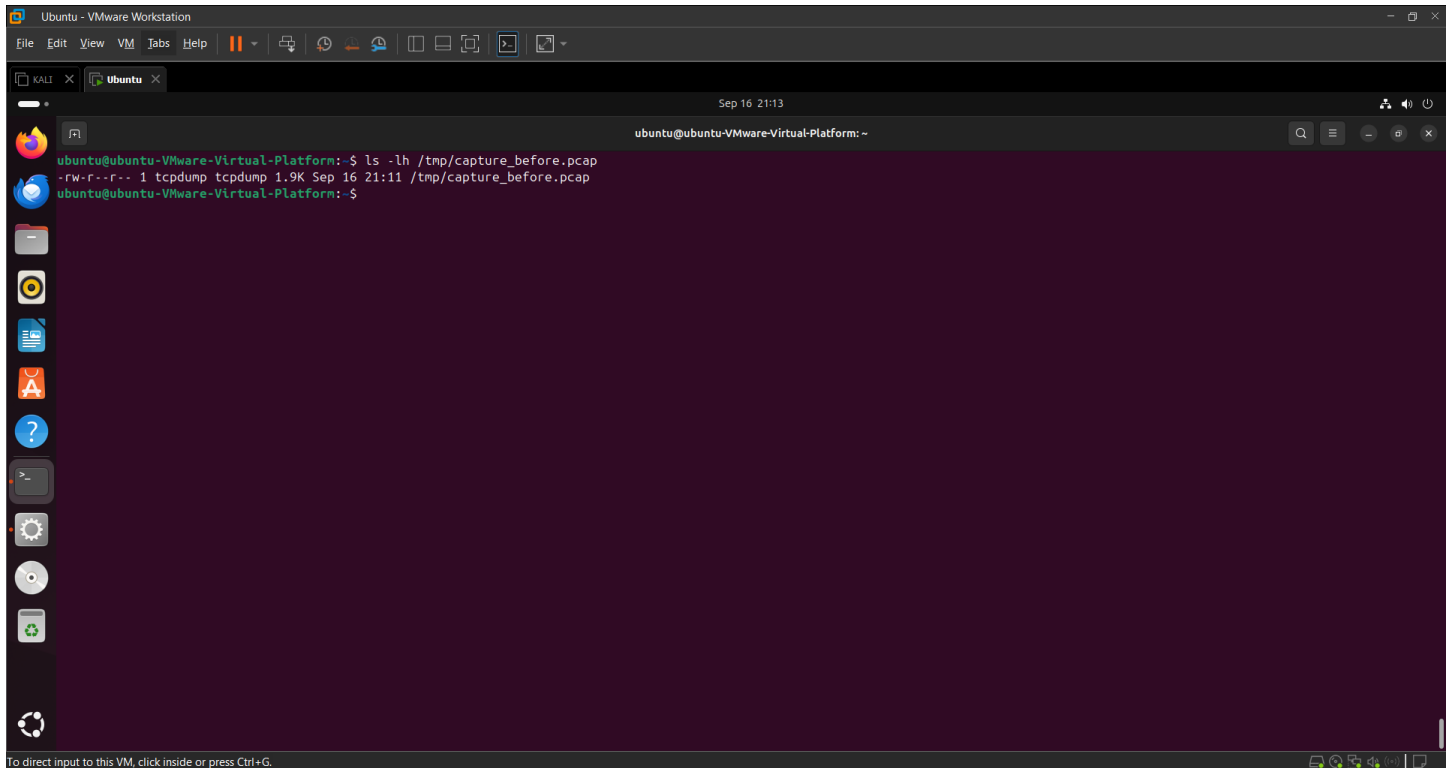
ubuntu@ubuntu-VMware-Virtual-Platform:~$ sudo tcpdump -i ens33 -s 0 -w /tmp/capture_before.pcap \ 'tcp port 80 or tcp port 21 or tcp port 23 or tcp port 110 or tcp port 143 or tcp port 25' -G 600 -W 1
tcpdump: listening on ens33, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C18 packets 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

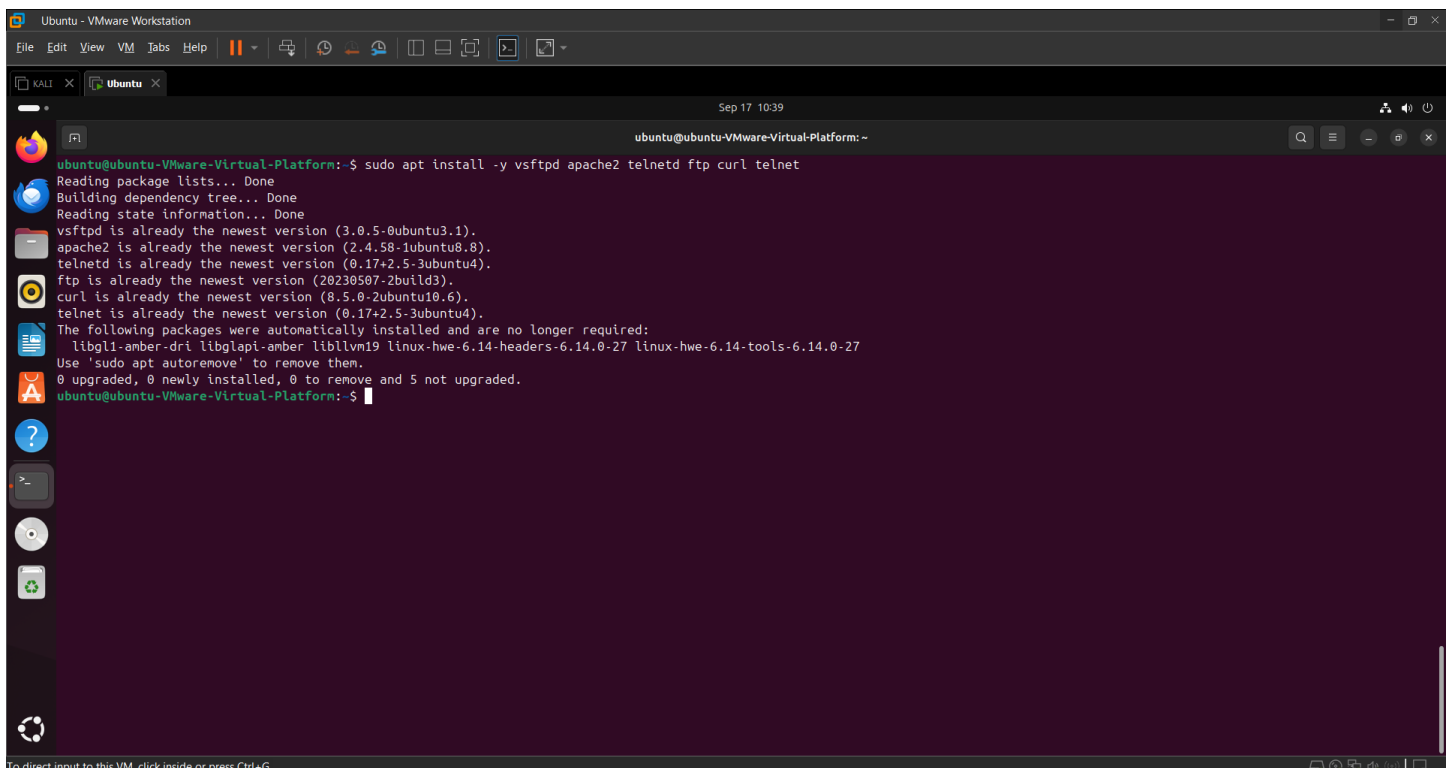


```
ubuntu@ubuntu-VMware-Virtual-Platform:~$ ls -lh /tmp/capture_before.pcap
-rw-r--r-- 1 tcpdump tcpdump 1.9K Sep 16 21:11 /tmp/capture_before.pcap
ubuntu@ubuntu-VMware-Virtual-Platform:~$
```

Install basic servers & clients by below commands

-sudo apt update

-sudo apt install -y vsftpd apache2 telnetd ftp curl telnet



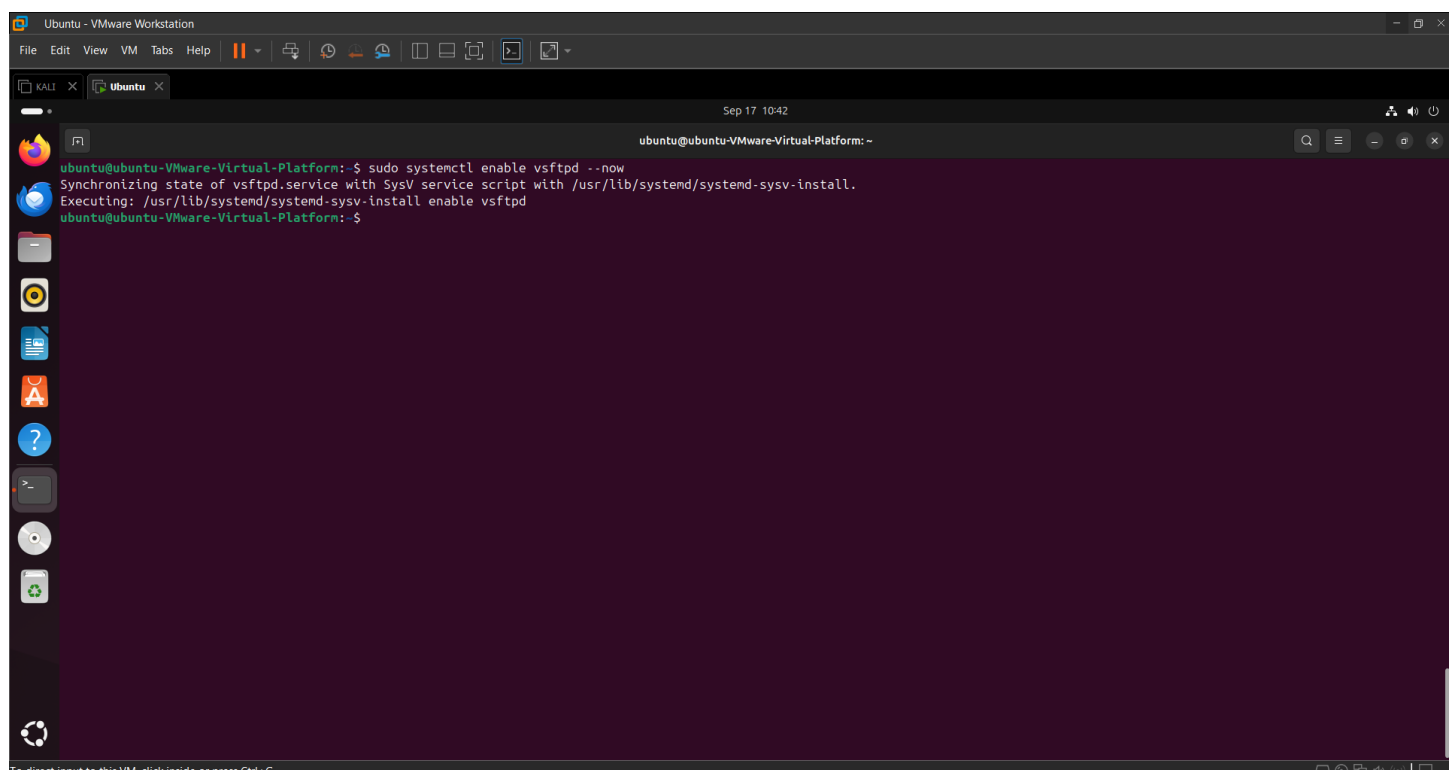
```
ubuntu@ubuntu-VMware-Virtual-Platform:~$ sudo apt install -y vsftpd apache2 telnetd ftp curl telnet
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
vsftpd is already the newest version (3.0.5-0ubuntu3.1).
apache2 is already the newest version (2.4.58-1ubuntu8.8).
telnetd is already the newest version (0.17+2.5-3ubuntu4).
ftp is already the newest version (20230507-2build3).
curl is already the newest version (8.5.0-2ubuntu10.6).
telnet is already the newest version (0.17+2.5-3ubuntu4).
The following packages were automatically installed and are no longer required:
  libgl1-amd64-dri libglapi-amd64 libllvm19 linux-hwe-6.14-headers-6.14.0-27 linux-hwe-6.14-tools-6.14.0-27
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 5 not upgraded.
ubuntu@ubuntu-VMware-Virtual-Platform:~$
```

This gives:

- **vsftpd** → FTP server
- **apache2** → HTTP server
- **telnetd** → Telnet server
- **ftp, curl, telnet** → clients to test

now start FTP (vsftpd) service by default, it allows anonymous or local logins. You can test with your Ubuntu username/password. Use this command:

`-sudo systemctl enable vsftpd --now`



```
ubuntu@ubuntu-VMware-Virtual-Platform:~$ sudo systemctl enable vsftpd --now
Synchronizing state of vsftpd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable vsftpd
ubuntu@ubuntu-VMware-Virtual-Platform:~$
```

Start Telnet service

`-sudo systemctl enable inetd --now`

`-sudo systemctl start telnetd`

Start Apache (HTTP)

`-sudo systemctl enable apache2 --now`

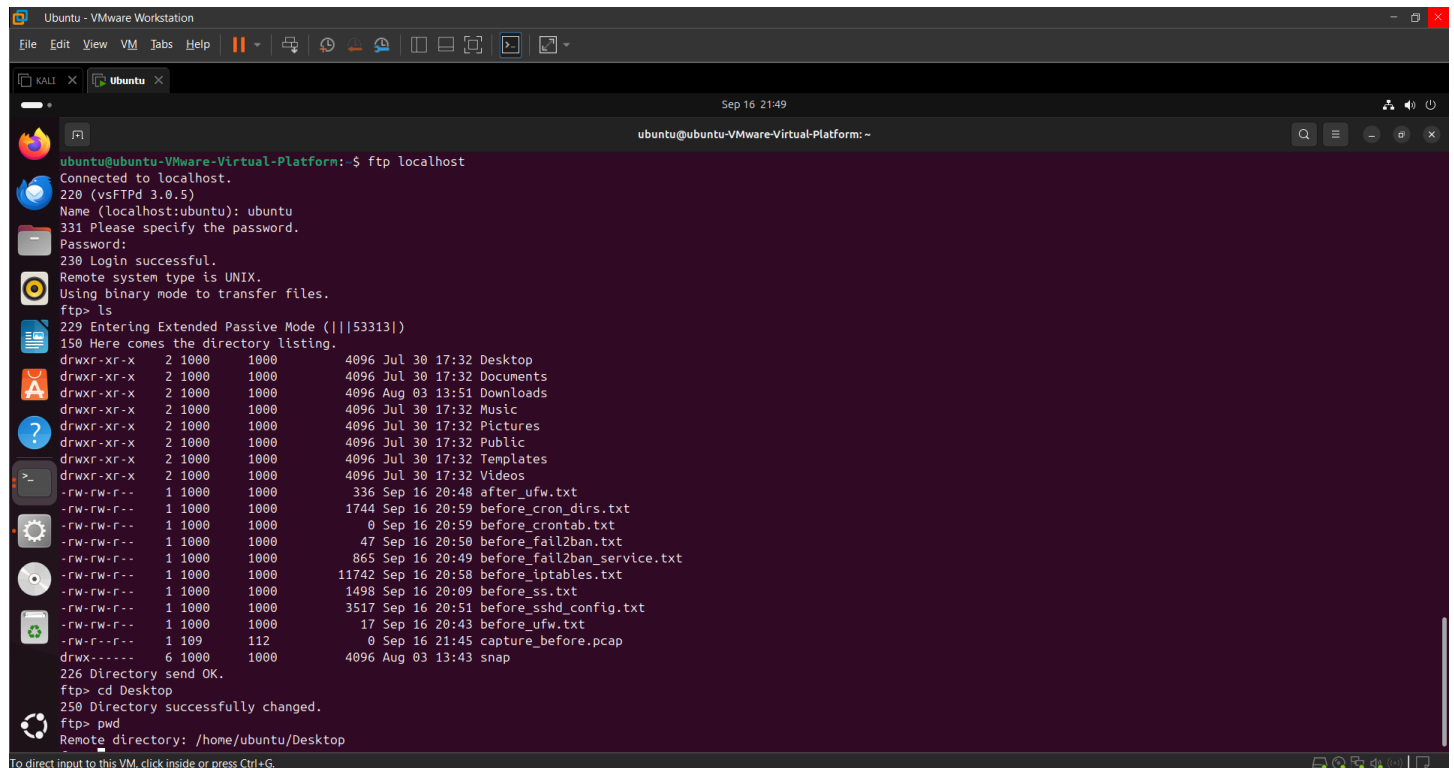
Generate traffic with credentials

FTP test From the same VM or another machine:

-ftp (IP of ubuntu)

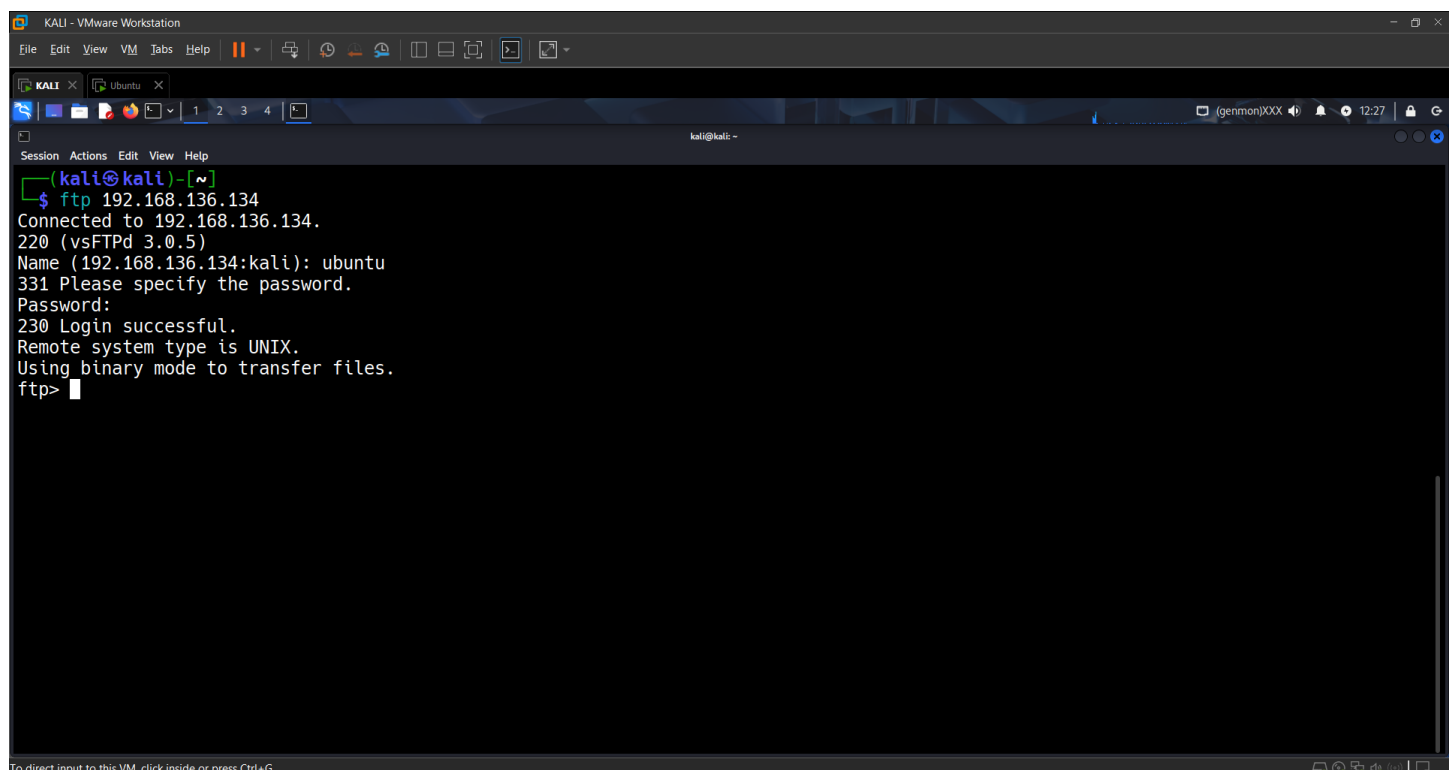
Enter username (your ubuntu username)

Enter password (your ubuntu password)



```
Ubuntu - VMware Workstation
File Edit View VM Tabs Help
KALI x Ubuntu x
Sep 16 21:49
ubuntu@ubuntu-VMware-Virtual-Platform: ~
ftp localhost
Connected to localhost.
220 (vsFTPd 3.0.5)
Name (localhost:ubuntu): ubuntu
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||53313|)
150 Here comes the directory listing.
drwxr-xr-x  2 1000    1000    4096 Jul 30 17:32 Desktop
drwxr-xr-x  2 1000    1000    4096 Jul 30 17:32 Documents
drwxr-xr-x  2 1000    1000    4096 Aug 03 13:51 Downloads
drwxr-xr-x  2 1000    1000    4096 Jul 30 17:32 Music
drwxr-xr-x  2 1000    1000    4096 Jul 30 17:32 Pictures
drwxr-xr-x  2 1000    1000    4096 Jul 30 17:32 Public
drwxr-xr-x  2 1000    1000    4096 Jul 30 17:32 Templates
drwxr-xr-x  2 1000    1000    4096 Jul 30 17:32 Videos
-rw-rw-r--  1 1000    1000    336 Sep 16 20:48 after_ufw.txt
-rw-rw-r--  1 1000    1000    1744 Sep 16 20:59 before_cron_dirs.txt
-rw-rw-r--  1 1000    1000     0 Sep 16 20:59 before_crontab.txt
-rw-rw-r--  1 1000    1000     47 Sep 16 20:50 before_fail2ban.txt
-rw-rw-r--  1 1000    1000    865 Sep 16 20:49 before_fail2ban_service.txt
-rw-rw-r--  1 1000    1000   11742 Sep 16 20:58 before_iptables.txt
-rw-rw-r--  1 1000    1000   1498 Sep 16 20:09 before_ss.txt
-rw-rw-r--  1 1000    1000   3517 Sep 16 20:51 before_sshd_config.txt
-rw-rw-r--  1 1000    1000    17 Sep 16 20:43 before_ufw.txt
-rw-rw-r--  1 109     112     0 Sep 16 21:45 capture_before.pcap
drwx----- 6 1000    1000    4096 Aug 03 13:43 snap
226 Directory send OK.
ftp> cd Desktop
250 Directory successfully changed.
ftp> pwd
Remote directory: /home/ubuntu/Desktop
```

Other machine – Kali Linux

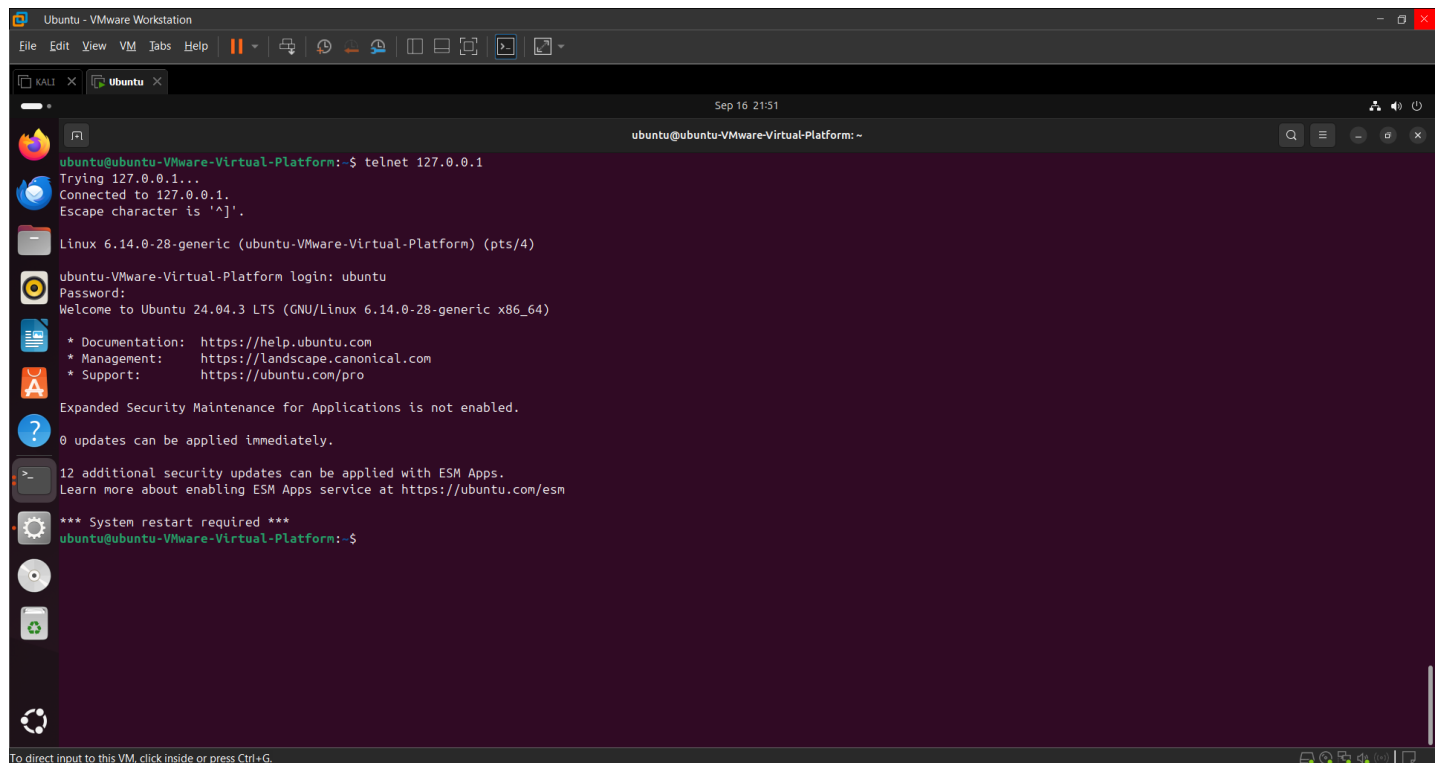


```
KALI - VMware Workstation
File Edit View VM Tabs Help
KALI x Ubuntu x
Session Actions Edit View Help
(kali@kali)~$ ftp 192.168.136.134
Connected to 192.168.136.134.
220 (vsFTPd 3.0.5)
Name (192.168.136.134:kali): ubuntu
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Telnet test From the same VM

-telnet 127.0.0.1

Login with your ubuntu username & password



```
ubuntu@ubuntu-VMware-Virtual-Platform:~$ telnet 127.0.0.1
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^A'.

Linux 6.14.0-28-generic (ubuntu-VMware-Virtual-Platform) (pts/4)
ubuntu-VMware-Virtual-Platform login: ubuntu
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-28-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

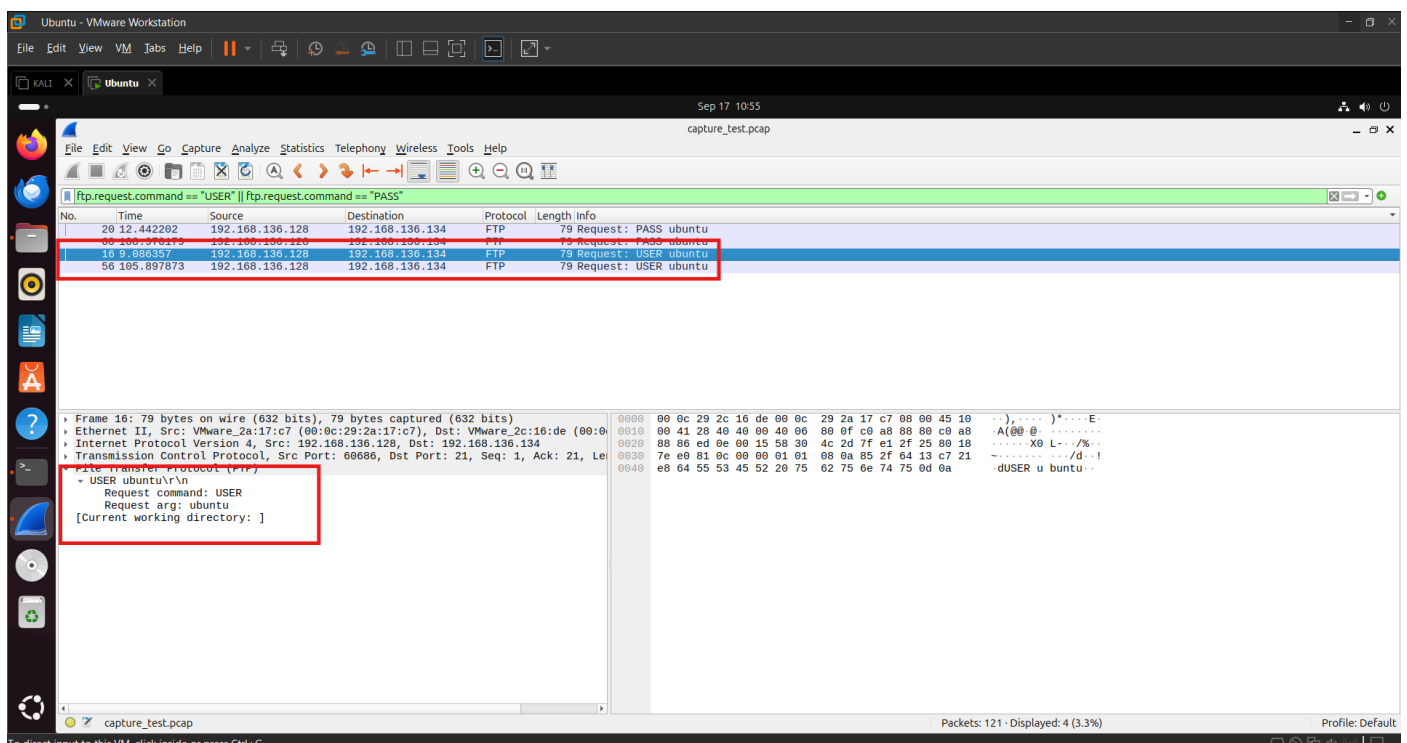
12 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

*** System restart required ***
ubuntu@ubuntu-VMware-Virtual-Platform:~$
```

Analyse the Captured traffic in Wireshark

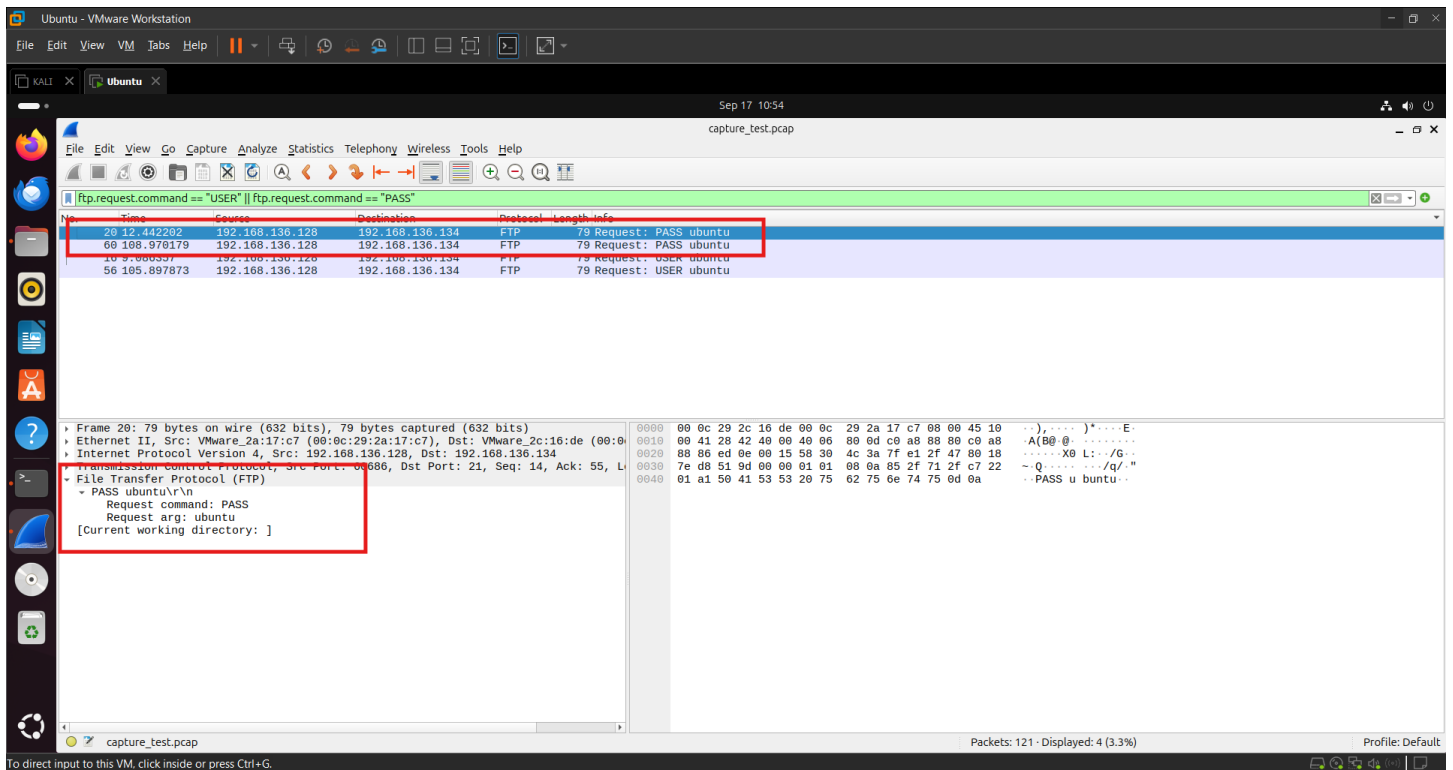
Open /tmp/capture_test.pcap in Wireshark and use filters:

- FTP:
ftp.request.command == "USER" || ftp.request.command == "PASS"



No.	Time	Source	Destination	Protocol	Length	Info
20	12.442282	192.168.136.128	192.168.136.134	FTP	79	Request: PASS ubuntu
60	100.570279	192.168.136.128	192.168.136.134	FTP	79	Request: PASS ubuntu
16	9.088357	192.168.136.128	192.168.136.134	FTP	79	Request: USER ubuntu
56	105.897873	192.168.136.128	192.168.136.134	FTP	79	Request: USER ubuntu

Frame 16: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
Ethernet II, Src: VMware_2a:17:c7 (08:0c:29:2a:17:c7), Dst: VMware_2c:16:de (08:0c:29:2c:16:de)
Internet Protocol Version 4, Src: 192.168.136.128, Dst: 192.168.136.134
Transmission Control Protocol, Src Port: 60806, Dst Port: 21, Seq: 1, Ack: 21, Len: 79
File Transfer Protocol (FTP)
USER ubuntu\r\n
Request command: USER
Request arg: ubuntu
[Current working directory:]



Here we can see the user name and password in plain text.

- **Telnet:**
telnet
→ Right-click a packet → **Follow** → **TCP Stream**. You'll see your username/password typed.
- **HTTP:**
http.authorization
→ Look for Authorization: Basic ... → Base64 decode to get username:password.

Deliverables for report

- **Before:** Show tcpdump running (listening on ens33...)
- **After:** Show .pcap analysis in Wireshark with highlighted credentials
- **Commands used** (services installed, tcpdump, test logins)