

Lab 8 Assignment

1. Use the ping command to test the connectivity to a remote server (e.g., example.com).

```
kali@kali: ~  
File Actions Edit View Help  
└─$ ping google.com  
  
PING google.com (142.250.183.142) 56(84) bytes of data.  
64 bytes from bom07s31-in-f14.1e100.net (142.250.183.142): icmp_seq=1 ttl=128 time=35.9 ms  
64 bytes from bom07s31-in-f14.1e100.net (142.250.183.142): icmp_seq=2 ttl=128 time=27.6 ms  
64 bytes from bom07s31-in-f14.1e100.net (142.250.183.142): icmp_seq=3 ttl=128 time=27.3 ms  
64 bytes from bom07s31-in-f14.1e100.net (142.250.183.142): icmp_seq=4 ttl=128 time=27.0 ms  
64 bytes from bom07s31-in-f14.1e100.net (142.250.183.142): icmp_seq=5 ttl=128 time=27.4 ms  
64 bytes from bom07s31-in-f14.1e100.net (142.250.183.142): icmp_seq=6 ttl=128 time=27.5 ms  
64 bytes from bom07s31-in-f14.1e100.net (142.250.183.142): icmp_seq=7 ttl=128 time=27.7 ms  
64 bytes from bom07s31-in-f14.1e100.net (142.250.183.142): icmp_seq=8 ttl=128 time=29.4 ms  
64 bytes from bom07s31-in-f14.1e100.net (142.250.183.142): icmp_seq=9 ttl=128 time=44.3 ms  
64 bytes from bom07s31-in-f14.1e100.net (142.250.183.142): icmp_seq=10 ttl=128 time=26.7 ms  
64 bytes from bom07s31-in-f14.1e100.net (142.250.183.142): icmp_seq=11 ttl=128 time=35.8 ms  
64 bytes from bom07s31-in-f14.1e100.net (142.250.183.142): icmp_seq=12 ttl=128 time=30.1 ms  
64 bytes from bom07s31-in-f14.1e100.net (142.250.183.142): icmp_seq=13 ttl=128 time=30.6 ms  
64 bytes from bom07s31-in-f14.1e100.net (142.250.183.142): icmp_seq=14 ttl=128 time=28.1 ms  
64 bytes from bom07s31-in-f14.1e100.net (142.250.183.142): icmp_seq=15 ttl=128 time=35.4 ms  
64 bytes from bom07s31-in-f14.1e100.net (142.250.183.142): icmp_seq=16 ttl=128 time=27.5 ms  
64 bytes from bom07s31-in-f14.1e100.net (142.250.183.142): icmp_seq=17 ttl=128 time=34.7 ms  
64 bytes from bom07s31-in-f14.1e100.net (142.250.183.142): icmp_seq=18 ttl=128 time=26.6 ms  
64 bytes from bom07s31-in-f14.1e100.net (142.250.183.142): icmp_seq=19 ttl=128 time=125 ms  
64 bytes from bom07s31-in-f14.1e100.net (142.250.183.142): icmp_seq=20 ttl=128 time=26.8 ms  
64 bytes from bom07s31-in-f14.1e100.net (142.250.183.142): icmp_seq=21 ttl=128 time=32.8 ms  
^C  
— google.com ping statistics —  
21 packets transmitted, 21 received, 0% packet loss, time 23128ms  
rtt min/avg/max/mdev = 26.579/34.966/125.299/20.678 ms  
  
(kali@kali)-[~]  
└─$
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

2. Write a script to measure the round-trip time for each packet and analyze the results.

```
Open [v] [i] rtt.sh  
~/Desktop/CYS/Los_8  
1 #!/bin/bash  
2  
3 # URL or IP address to ping  
4 url="www.google.com"  
5  
6 # Ping the server and display RTT for each packet  
7 ping -c 5 $url  
8
```

```
(kali@kali)-[~/Desktop/CYS/Los_8]  
└─$ ./rtt.sh  
  
PING www.google.com (142.250.196.68) 56(84) bytes of data.  
64 bytes from maa03s46-in-f4.1e100.net (142.250.196.68): icmp_seq=1 ttl=128 time=100 ms  
64 bytes from maa03s46-in-f4.1e100.net (142.250.196.68): icmp_seq=2 ttl=128 time=120 ms  
64 bytes from maa03s46-in-f4.1e100.net (142.250.196.68): icmp_seq=3 ttl=128 time=143 ms  
64 bytes from maa03s46-in-f4.1e100.net (142.250.196.68): icmp_seq=4 ttl=128 time=164 ms  
64 bytes from maa03s46-in-f4.1e100.net (142.250.196.68): icmp_seq=5 ttl=128 time=84.5 ms  
  
— www.google.com ping statistics —  
5 packets transmitted, 5 received, 0% packet loss, time 4006ms  
rtt min/avg/max/mdev = 84.475/122.269/164.218/28.642 ms
```

3. Use the traceroute to trace the route packets take to a destination

```
(kali㉿kali)-[~/Desktop/CYS/Los_8]
$ traceroute google.com
traceroute to google.com (142.250.183.142), 30 hops max, 60 byte packets
 1  192.168.80.2 (192.168.80.2)  0.861 ms  0.752 ms  0.706 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * ^C

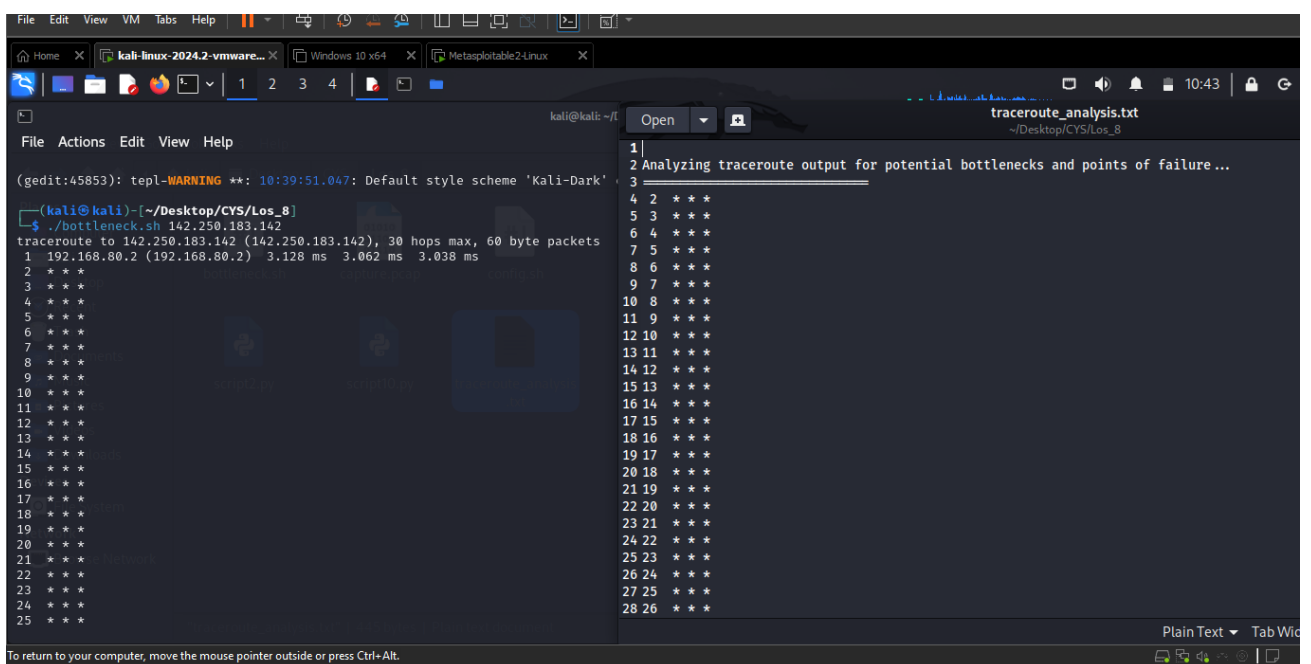
(kali㉿kali)-[~/Desktop/CYS/Los_8]
$
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

4. Analyze the output to identify any potential bottlenecks or points of failure in the route.

```
Open  bottlenecks.sh
~/Desktop/CYS/Los_8

1 #!/bin/bash
2
3 # Check if the user provided a target
4 if [ $# -eq 0 ]; then
5     echo "Usage: $0 <hostname_or_IP>"
6     exit 1
7 fi
8
9 TARGET=$1
10 REPORT_FILE="traceroute_analysis.txt"
11
12 # Run traceroute and save the output
13 traceroute_output=$(traceroute $TARGET)
14
15 # Print the output to the console
16 echo "$traceroute_output"
17
18 # Analyze the output
19 echo -e "\nAnalyzing traceroute output for potential bottlenecks and points of failure..." > $REPORT_FILE
20 echo "===== " >> $REPORT_FILE
21
22 # Look for timeouts (indicated by '*' characters)
23 echo "$traceroute_output" | grep -E '\s*[0-9]+\s+\*\s+\*\s+\*' >> $REPORT_FILE
24
25 # Check for high latency
26 echo -e "\nPotential high latency hops (over 100 ms):" >> $REPORT_FILE
27 echo "$traceroute_output" | awk '{ for (i=1; i<NF; i++) if ($i ~ /^[0-9]+ms/ && $i+0 > 100) print $i; }' >> $REPORT_FILE
28
```



5. Use the nslookup command to find the IP address of a given domain (e.g., example.com).

```
(kali㉿kali)-[~/Desktop/CYS/Los_8]
$ nslookup google.com
Server:          192.168.80.2
Address:         192.168.80.2#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.183.14
Name:   google.com
Address: 2404:6800:4009:820::200e
```

6. Use the netstat command to view active connections and listening ports on your machine.

```
(kali㉿kali)-[~/Desktop/CYS/Los_8]
$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 192.168.80.129:bootpc   192.168.80.254:bootps   ESTABLISHED
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State       I-Node   Path
unix   3      [ ]         STREAM     CONNECTED   7825
unix   2      [ ]         DGRAM      CONNECTED   789
unix   3      [ ]         STREAM     CONNECTED   9064    @/tmp/.X11-unix/X0
unix   3      [ ]         STREAM     CONNECTED   7153
unix   3      [ ]         STREAM     CONNECTED   4895    /run/systemd/journal/stdout
unix   3      [ ]         STREAM     CONNECTED   7971    /run/dbus/system_bus_socket
unix   3      [ ]         STREAM     CONNECTED   7967    /run/user/1000/bus
unix   3      [ ]         STREAM     CONNECTED   9008
unix   3      [ ]         STREAM     CONNECTED   8764    @/tmp/.X11-unix/X0
unix   3      [ ]         STREAM     CONNECTED   10491   /run/user/1000/at-spi/bus_0
unix   3      [ ]         STREAM     CONNECTED   7961
unix   3      [ ]         STREAM     CONNECTED   9863    /run/user/1000/at-spi/bus_0
unix   3      [ ]         DGRAM      CONNECTED   7038
unix   3      [ ]         STREAM     CONNECTED   8948
unix   3      [ ]         STREAM     CONNECTED   7359    /run/dbus/system_bus_socket
unix   3      [ ]         STREAM     CONNECTED   7979
unix   3      [ ]         STREAM     CONNECTED   9823
unix   3      [ ]         STREAM     CONNECTED   7343
unix   3      [ ]         STREAM     CONNECTED   31044   /run/dbus/system_bus_socket
unix   3      [ ]         STREAM     CONNECTED   7742
unix   3      [ ]         STREAM     CONNECTED   7984    /run/user/1000/bus

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
```

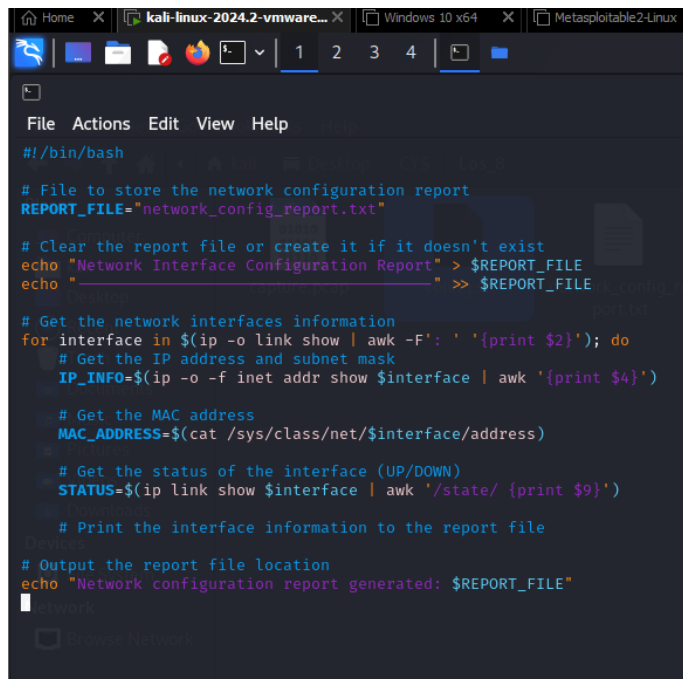
7. Use the ifconfig (Linux) or ip a command to display network interface configurations.

```
(kali㉿kali)-[~/Desktop/CYS/Los_8]
$ ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.80.129 netmask 255.255.255.0 broadcast 192.168.80.255
    inet6 fe80::148c:9f84:c60c:2043 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:b8:05:77 txqueuelen 1000 (Ethernet)
    RX packets 563 bytes 38562 (37.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 328 bytes 26540 (25.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kali)-[~/Desktop/CYS/Los_8]
$
```

8. Write a script to report document the configuration of each interface, noting the IP address, subnet mask, and any other relevant information.



```
#!/bin/bash

# File to store the network configuration report
REPORT_FILE="network_config_report.txt"

# Clear the report file or create it if it doesn't exist
echo "Network Interface Configuration Report" > $REPORT_FILE
echo "_____ " >> $REPORT_FILE

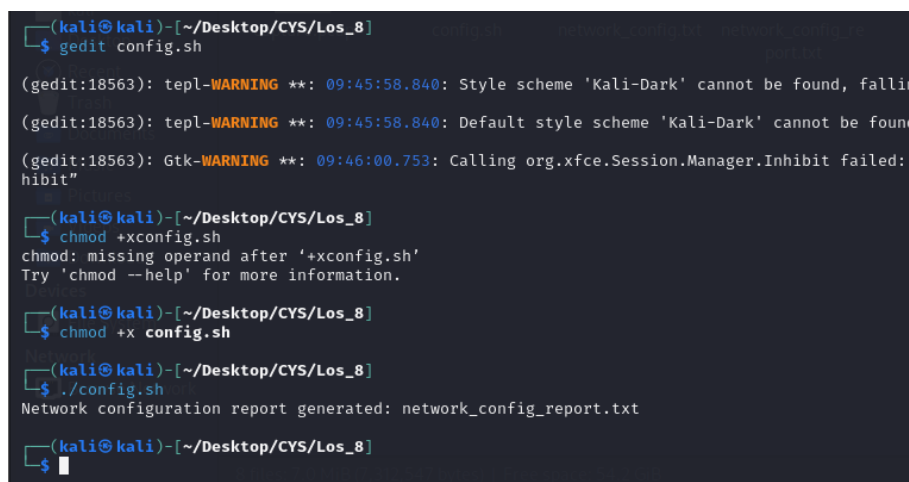
# Get the network interfaces information
for interface in $(ip -o link show | awk -F': ' '{print $2}'); do
    # Get the IP address and subnet mask
    IP_INFO=$(ip -o -f inet addr show $interface | awk '{print $4}')

    # Get the MAC address
    MAC_ADDRESS=$(cat /sys/class/net/$interface/address)

    # Get the status of the interface (UP/DOWN)
    STATUS=$(ip link show $interface | awk '/state/ {print $9}')

    # Print the interface information to the report file
    echo "Interface: $interface" >> $REPORT_FILE
    echo "IP Address/Subnet Mask: $IP_INFO" >> $REPORT_FILE
    echo "MAC Address: $MAC_ADDRESS" >> $REPORT_FILE
    echo "Status: $STATUS" >> $REPORT_FILE
    echo "_____ " >> $REPORT_FILE
done

# Output the report file location
echo "Network configuration report generated: $REPORT_FILE"
```



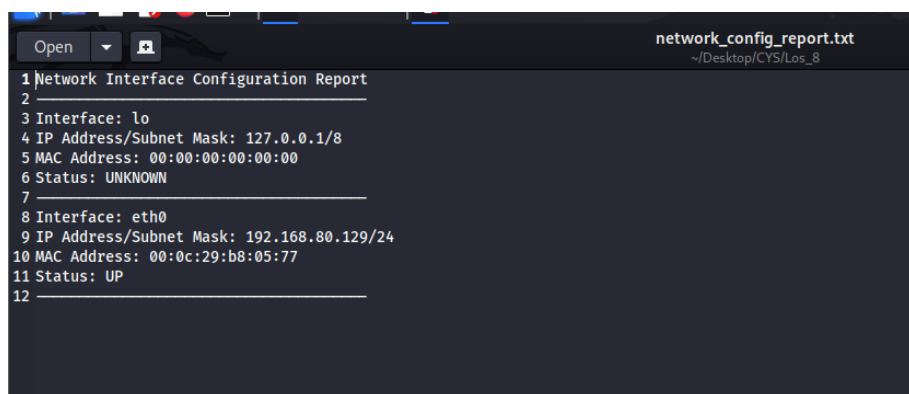
```
(kali@kali)~[~/Desktop/CYS/Los_8]
$ gedit config.sh

(gedit:18563): tepl-WARNING **: 09:45:58.840: Style scheme 'Kali-Dark' cannot be found, falling back to 'Adwaita'
(gedit:18563): tepl-WARNING **: 09:45:58.840: Default style scheme 'Kali-Dark' cannot be found, falling back to 'Adwaita'
(gedit:18563): Gtk-WARNING **: 09:46:00.753: Calling org.xfce.Session.Manager.Inhibit failed: Inhibit failed

(kali@kali)~[~/Desktop/CYS/Los_8]
$ chmod +x config.sh
chmod: missing operand after '+xconfig.sh'
Try 'chmod --help' for more information.

(kali@kali)~[~/Desktop/CYS/Los_8]
$ ./config.sh
Network configuration report generated: network_config_report.txt

(kali@kali)~[~/Desktop/CYS/Los_8]
$
```



```
network_config_report.txt
~/Desktop/CYS/Los_8

1 Network Interface Configuration Report
2 _____
3 Interface: lo
4 IP Address/Subnet Mask: 127.0.0.1/8
5 MAC Address: 00:00:00:00:00:00
6 Status: UNKNOWN
7 _____
8 Interface: eth0
9 IP Address/Subnet Mask: 192.168.80.129/24
10 MAC Address: 00:0c:29:b8:05:77
11 Status: UP
12 _____
```

9. Perform a basic network scan using nmap on your local network to identify active devices and open ports.

```
File Actions Edit View Help
(kali@kali)-[~]
$ nmap 192.168.80.133
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-23 09:52 EDT
Nmap scan report for 192.168.80.133
Host is up (0.0024s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:14:72:41 (VMware)
```

10. Create a report summarizing the devices found, their IP addresses, and the services running on the open ports.

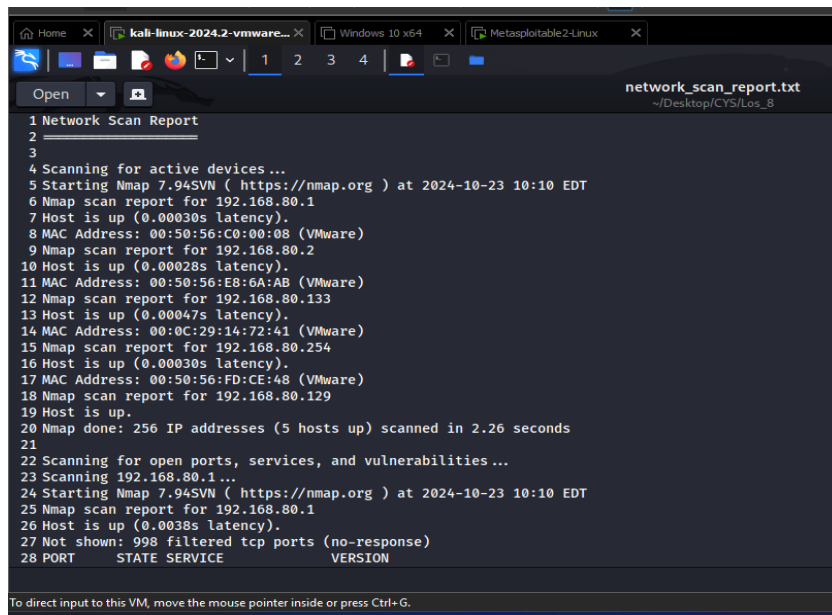
```
File Actions Edit View Help
Shell No. 1
# Clear the report file or create it if it doesn't exist
echo "Network Scan Report" > $REPORT_FILE
echo " " >> $REPORT_FILE
echo >> $REPORT_FILE

# Define the subnet to scan (update this with your local subnet)
SUBNET="192.168.80.0/24"

# Scan for active devices
echo "Scanning for active devices..." >> $REPORT_FILE
nmap -sP $SUBNET >> $REPORT_FILE
echo >> $REPORT_FILE

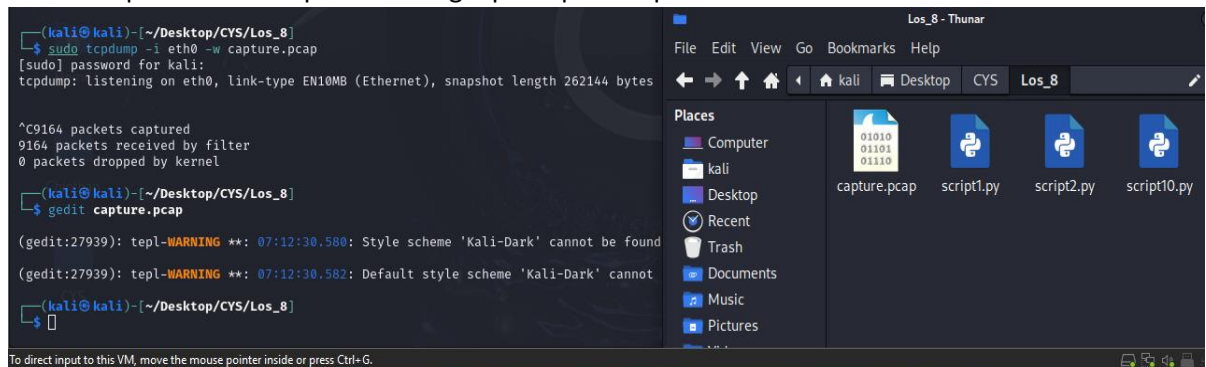
# Scan for open ports, services, and vulnerabilities on each active device
echo "Scanning for open ports, services, and vulnerabilities..." >> $REPORT_FILE
for ip in $(nmap -sP $SUBNET | grep "Nmap scan report" | awk '{print $5}'); do
    echo "Scanning $ip..." >> $REPORT_FILE
    nmap -sV --script=vuln $ip >> $REPORT_FILE # Added --script=vuln to check for vulnerabilities
done
echo >> $REPORT_FILE

# Output the report file location
echo "Network scan report generated: $REPORT_FILE"
```



```
1 Network Scan Report
2
3
4 Scanning for active devices...
5 Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-23 10:10 EDT
6 Nmap scan report for 192.168.80.1
7 Host is up (0.00030s latency).
8 MAC Address: 00:50:56:C0:00:08 (VMware)
9 Nmap scan report for 192.168.80.2
10 Host is up (0.00028s latency).
11 MAC Address: 00:50:56:E8:6A:AB (VMware)
12 Nmap scan report for 192.168.80.133
13 Host is up (0.00047s latency).
14 MAC Address: 00:0C:29:14:72:41 (VMware)
15 Nmap scan report for 192.168.80.254
16 Host is up (0.00030s latency).
17 MAC Address: 00:50:56:FD:CE:48 (VMware)
18 Nmap scan report for 192.168.80.129
19 Host is up.
20 Nmap done: 256 IP addresses (5 hosts up) scanned in 2.26 seconds
21
22 Scanning for open ports, services, and vulnerabilities...
23 Scanning 192.168.80.1...
24 Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-23 10:10 EDT
25 Nmap scan report for 192.168.80.1
26 Host is up (0.0038s latency).
27 Not shown: 998 filtered tcp ports (no-response)
28 PORT      STATE SERVICE      VERSION
```

11. Capture network packets using tcpdump on a specific interface.



```
(kali@kali)-[~/Desktop/CYS/Los_8]
$ sudo tcpdump -i eth0 -w capture.pcap
[sudo] password for kali:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes

^C9164 packets captured
9164 packets received by filter
0 packets dropped by kernel

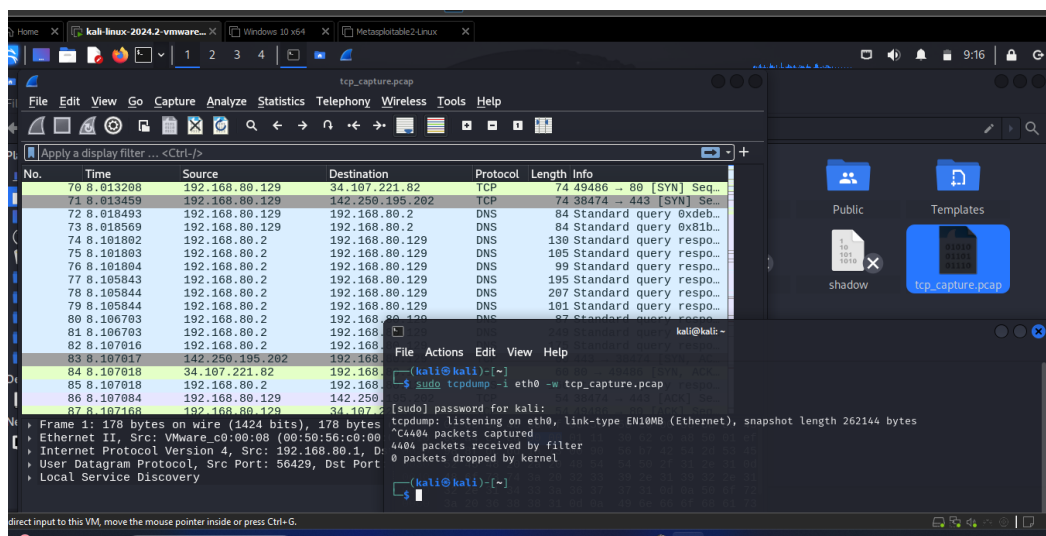
(kali@kali)-[~/Desktop/CYS/Los_8]
$ gedit capture.pcap

(gedit:27939): tepl-WARNING **: 07:12:30.580: Style scheme 'Kali-Dark' cannot be found
(gedit:27939): tepl-WARNING **: 07:12:30.582: Default style scheme 'Kali-Dark' cannot be found

(kali@kali)-[~/Desktop/CYS/Los_8]
$
```

12. Analyze the captured packets for specific protocols (like HTTP or DNS) and summarize your findings.

HTTP



No.	Time	Source	Destination	Protocol	Length	Info
70	8.013208	192.168.80.129	34.107.221.82	TCP	74	49486 → 80 [SYN] Seq...
71	8.013459	192.168.80.129	142.250.195.202	TCP	74	38474 → 443 [SYN] Seq...
72	8.018493	192.168.80.129	192.168.80.2	DNS	84	Standard query 0xdeb...
73	8.018509	192.168.80.129	192.168.80.2	DNS	84	Standard query 0x81b...
74	8.101802	192.168.80.2	192.168.80.129	DNS	130	Standard query respo...
75	8.101803	192.168.80.2	192.168.80.129	DNS	105	Standard query respo...
76	8.101804	192.168.80.2	192.168.80.129	DNS	99	Standard query respo...
77	8.105843	192.168.80.2	192.168.80.129	DNS	195	Standard query respo...
78	8.105844	192.168.80.2	192.168.80.129	DNS	207	Standard query respo...
79	8.105844	192.168.80.2	192.168.80.129	DNS	101	Standard query respo...
80	8.106703	192.168.80.2	192.168.80.129	DNS	...	Standard query respo...
81	8.106703	192.168.80.2	192.168.80.129	DNS	...	Standard query respo...
82	8.107016	192.168.80.2	192.168.80.129	DNS	...	Standard query respo...
83	8.107017	142.250.195.202	192.168.80.129	TCP	...	Standard query respo...
84	8.107018	34.107.221.82	192.168.80.129	TCP	...	Standard query respo...
85	8.107018	192.168.80.2	192.168.80.129	DNS	...	Standard query respo...
86	8.107084	192.168.80.129	142.250.195.202	TCP	...	Standard query respo...
87	8.107168	192.168.80.129	34.107.221.82	TCP	...	Standard query respo...


```
tcpdump: tcp_port.pcap: No such file or directory

(kali@kali)-[~]
└─$ sudo tcpdump -r tcp_capture.pcap 'tcp port 80'

reading from file tcp_capture.pcap, link-type EN10MB (Ethernet), snapshot length 262144
09:14:52.560540 IP 192.168.80.129.49486 > 82.221.107.34.bc.googleusercontent.com.http: Flags [S], seq 590906825, win 64240, options [mss 1460,sackOK,TS val 3327382941 ecr 0,nop,wscale 7], length 0
09:14:52.654350 IP 82.221.107.34.bc.googleusercontent.com.http > 192.168.80.129.49486: Flags [S.], seq 402069437, ack 590906826, win 64240, options [mss 1460], length 0
09:14:52.654500 IP 192.168.80.129.49486 > 82.221.107.34.bc.googleusercontent.com.http: Flags [.], ack 1, win 64240, length 0
09:14:52.662915 IP 192.168.80.129.49486 > 82.221.107.34.bc.googleusercontent.com.http: Flags [P.], seq 1:296, ack 1, win 64240, length 295: HTTP: GET /success.txt?ip=192.168.80.129.49486
09:14:52.663105 IP 82.221.107.34.bc.googleusercontent.com.http > 192.168.80.129.49486: Flags [.], ack 296, win 64240, length 0
09:14:52.753527 IP 82.221.107.34.bc.googleusercontent.com.http > 192.168.80.129.49486: Flags [P.], seq 1:217, ack 296, win 64240, length 216: HTTP: HTTP/1.1 200 OK
09:14:52.753663 IP 192.168.80.129.49486 > 82.221.107.34.bc.googleusercontent.com.http: Flags [.], ack 217, win 64024, length 0
09:14:52.856970 IP 192.168.80.129.37740 > maa05s18-in-f3.1e100.net.http: Flags [S], seq 11783, ack 414, win 64240, options [mss 1460,sackOK,TS val 2506784695 ecr 0,nop,wscale 7], length 0
09:14:52.958381 IP maa05s18-in-f3.1e100.net.http > 192.168.80.129.37740: Flags [S.], seq 1105988361, ack 2147931798, win 64240, options [mss 1460], length 0
09:14:52.958492 IP 192.168.80.129.37740 > maa05s18-in-f3.1e100.net.http: Flags [.], ack 1, win 64240, length 0
09:14:52.964109 IP 192.168.80.129.37740 > maa05s18-in-f3.1e100.net.http: Flags [P.], seq 1:414, ack 1, win 64240, length 413: HTTP: POST /wr2 HTTP/1.1
09:14:52.964524 IP maa05s18-in-f3.1e100.net.http > 192.168.80.129.37740: Flags [.], ack 414, win 64240, length 0
09:14:53.064596 IP maa05s18-in-f3.1e100.net.http > 192.168.80.129.37740: Flags [P.], seq 1:783, ack 414, win 64240, length 782: HTTP: HTTP/1.1 200 OK
09:14:53.064639 IP 192.168.80.129.37740 > maa05s18-in-f3.1e100.net.http: Flags [.], ack 703, win 63538, length 0
09:14:58.451091 IP 192.168.80.129.59046 > maa03s28-in-f3.1e100.net.http: Flags [S], seq 1771388804, win 64240, options [mss 1460,sackOK,TS val 210962708 ecr 0,nop,wscale 7], length 0
09:14:58.640346 IP maa03s28-in-f3.1e100.net.http > 192.168.80.129.59046: Flags [S.], seq 789403874, ack 1771388805, win 64240, options [mss 1460], length 0
09:14:58.640610 IP 192.168.80.129.59046 > maa03s28-in-f3.1e100.net.http: Flags [.], ack 1, win 64240, length 0
09:14:58.640874 IP 192.168.80.129.59046 > maa03s28-in-f3.1e100.net.http: Flags [P.], seq 1:413, ack 1, win 64240, length 412: HTTP: POST /wr2 HTTP/1.1
09:14:58.641214 IP maa03s28-in-f3.1e100.net.http > 192.168.80.129.59046: Flags [.], ack 413, win 64240, length 0
09:14:58.906955 IP maa03s28-in-f3.1e100.net.http > 192.168.80.129.59046: Flags [P.], seq 1:702, ack 413, win 64240, length 701: HTTP: HTTP/1.1 200 OK

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

DNS

```
(kali@kali)-[~]
└─$ sudo tcpdump -r tcp_capture.pcap 'udp port 53'

reading from file tcp_capture.pcap, link-type EN10MB (Ethernet), snapshot length 262144
09:14:51.269287 IP 192.168.80.129.41607 > 192.168.80.2.domain: 58055+ A? contile.services.mozilla.com. (46)
09:14:51.269321 IP 192.168.80.129.41607 > 192.168.80.2.domain: 48835+ AAAA? contile.services.mozilla.com. (46)
09:14:51.422586 IP 192.168.80.2.domain > 192.168.80.129.41607: 58055 1/0/0 A 34.117.188.166 (62)
09:14:51.783990 IP 192.168.80.129.41448 > 192.168.80.2.domain: 57318+ A? content-signature-2.cdn.mozilla.net. (53)
09:14:51.783994 IP 192.168.80.129.41448 > 192.168.80.2.domain: 53728+ AAAA? content-signature-2.cdn.mozilla.net. (53)
09:14:52.028217 IP 192.168.80.2.domain > 192.168.80.129.41448: 57318 3/0/0 CNAME content-signature-chains.prod.autograph.services.mozaws.net., CNAME prod.content-signature-chains.prod.webservices.mozgcp.net., A 34.160.144.191 (207)
09:14:52.028571 IP 192.168.80.2.domain > 192.168.80.129.41448: 53728 3/0/0 CNAME content-signature-chains.prod.autograph.services.mozaws.net., CNAME prod.content-signature-chains.prod.webservices.mozgcp.net., AAAA 2600:1901:0:92a9:: (219)
09:14:52.255441 IP 192.168.80.129.50869 > 192.168.80.2.domain: 5207+ A? safebrowsing.googleapis.com. (45)
09:14:52.255493 IP 192.168.80.129.50869 > 192.168.80.2.domain: 34137+ AAAA? safebrowsing.googleapis.com. (45)
09:14:52.274471 IP 192.168.80.129.49345 > 192.168.80.2.domain: 16885+ A? example.org. (29)
09:14:52.274673 IP 192.168.80.129.47934 > 192.168.80.2.domain: 8745+ A? example.org. (29)
09:14:52.274717 IP 192.168.80.129.47934 > 192.168.80.2.domain: 22568+ AAAA? example.org. (29)
09:14:52.274902 IP 192.168.80.129.49627 > 192.168.80.2.domain: 21462+ A? ipv4only.arpa. (31)
09:14:52.274929 IP 192.168.80.129.49627 > 192.168.80.2.domain: 18377+ AAAA? ipv4only.arpa. (31)
09:14:52.277226 IP 192.168.80.129.58979 > 192.168.80.2.domain: 25080+ A? detectportal.firefox.com. (42)
09:14:52.277305 IP 192.168.80.129.58979 > 192.168.80.2.domain: 43515+ AAAA? detectportal.firefox.com. (42)
09:14:52.282841 IP 192.168.80.129.50523 > 192.168.80.2.domain: 15915+ A? detectportal.firefox.com. (42)
09:14:52.300290 IP 192.168.80.129.41896 > 192.168.80.2.domain: 47723+ A? r10.o.lencr.org. (33)
09:14:52.300347 IP 192.168.80.129.41896 > 192.168.80.2.domain: 65381+ AAAA? r10.o.lencr.org. (33)
09:14:52.311208 IP 192.168.80.2.domain > 192.168.80.129.50869: 5207 1/0/0 A 142.250.195.202 (61)
09:14:52.311289 IP 192.168.80.2.domain > 192.168.80.129.50869: 34137 1/0/0 AAAA 2600:1901:0:92a9::200a (73)
09:14:52.311668 IP 192.168.80.129.60351 > 192.168.80.2.domain: 55690+ A? safebrowsing.googleapis.com. (45)
09:14:52.311707 IP 192.168.80.129.60351 > 192.168.80.2.domain: 395+ AAAA? safebrowsing.googleapis.com. (45)
09:14:52.447092 IP 192.168.80.129.47934 > 192.168.80.2.domain: 8745 1/0/0 A 93.184.215.14 (45)

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

13. Use the whois command to gather registration information about a domain.

```
(kali@newhostname)-[~]
└─$ whois example.com

Domain Name: EXAMPLE.COM
Registry Domain ID: 2336799_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.iana.org
Registrar URL: http://res-dom.iana.org
Updated Date: 2024-08-14T07:01:34Z
Creation Date: 1995-08-14T04:00:00Z
Registry Expiry Date: 2025-08-13T04:00:00Z
Registrar: RESERVED-Internet Assigned Numbers Authority
Registrar IANA ID: 376
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: A.IANA-SERVERS.NET
Name Server: B.IANA-SERVERS.NET
DNSSEC: signedDelegation
DNSSEC DS Data: 370 13 2 BE74359954660069D5C63D200C39F5603827D7DD02B56F120EE9F3A8676427C
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-10-23T13:07:56Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
```

14. Use the hostname command to display and change the hostname of your machine.

```
(kali㉿kali)-[~]  
$ hostname  
kali  
  
(kali㉿kali)-[~]  
$ sudo hostname newhostname  
[sudo] password for kali:  
  
(kali㉿kali)-[~]  
$ hostname  
newhostname  
  
(kali㉿kali)-[~]  
$
```

15. Use the finger command to gather information about users on a system.

```
(kali㉿kali)-[~/Desktop/CYS/Los_8]  
$ finger -l kali  
Login: kali Name:  
Directory: /home/kali Shell: /usr/bin/zsh  
On since Mon Oct 21 06:20 (EDT) on tty7 from :0  
58 minutes 43 seconds idle  
No mail.  
No Plan.  
  
(kali㉿kali)-[~/Desktop/CYS/Los_8]  
$
```

16. Use the who command to see who is currently logged into the system and the last command to view the login history.

```
File Actions Edit View Help  
  
(kali㉿kali)-[~/Desktop/CYS/Los_8]  
$ who  
kali tty7 2024-10-21 06:20 (:0)
```