EC-Council

codered
FROM EC-COUNCIL

CHAPTER 17

NETWORK TRAFFIC MONITORING

CERTIFIED CYBERSECURITY TECHNICIAN

INDEX

Chapter 17:
Network Traffic Monitoring

SCENARIO

Network monitoring helps security professionals identify possible issues before they affect business continuity. If an issue occurs in the network, the root cause can be determined easily through network monitoring. Subsequently, using network automation tools, the problem can be fixed automatically. Networking monitoring not only prevents outages but also provides visibility to potential issues. Continuous network monitoring minimizes downtime and increases the performance of the network.

Even when security tools are in place, attackers can find ways to bypass such security mechanisms to enter the network. Security tools generally use signature-based detection techniques, and it is difficult to identify continuously changing attack signatures/patterns. These tools are not designed to identify behavioural anomalies and are unable to detect attackers' activities that are initiated before and during attacks.

Network monitoring tools provide the first level of security and help identify anomalous conditions in the network, that indicate attacker activity.

OBJECTIVE

The objective of this lab is to provide expert knowledge in network traffic monitoring. This includes knowledge of the following tasks:

- Intercepting network traffic using various tools such as Wireshark and tcpdump
- Exploring various filters in Wireshark
- Analyzing and examining various network packet headers in Linux using tools such as tcpdump
- Performing scan on network to identify machines in the local network

OVERVIEW OF NETWORK TRAFFIC MONITORING

Network monitoring is a retrospective security approach that involves monitoring a network for abnormal activities, performance issues, bandwidth issues, etc. It is an integral part of network security and is a demanding task within the network security operations of organizations. Continuous network traffic monitoring and analysis are critical for effective threat detection.

A proper analysis of log data enables actionable information to be identified, which helps the security professional in detecting and monitoring potential security breaches, internal misuse of information, operational issues, and other long-term issues. It also helps validate whether the end-user has followed all documented protocols to detect fraudulent activities and policy violations. It is also useful for internal investigations, security auditing and forensic analysis, determination of operational trends, and implementation of baselines.

LAB TASKS

Cyber security professional or a security professional use numerous tools and techniques to monitor network traffic. The recommended labs that will assist you in learning various aspects of network traffic monitoring include the following:

01 **Intercept Network Traffic using Wireshark and tcpdump**

02 **Apply Various Filters in Wireshark**

03 **Analyze and Examine Various Network Packet Headers in Linux using tcpdump**

04 **Scan Network to Identify Hosts in the Local Network**

Note: Turn on PfSense Firewall virtual machine and keep it running throughout the lab exercises.

EXERCISE 1: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND tcpdump

Network traffic monitoring is the process of capturing network traffic and inspecting it closely to determine what is happening on the network.

LAB SCENARIO

A security professional must have the required knowledge to intercept and interpret network traffic using various packet sniffing tools. The captured traffic can be used to identify malicious or suspicious packets hiding within traffic.

OBJECTIVE

This lab will demonstrate how to capture network traffic using Wireshark and tcpdump.

OVERVIEW OF TROJAN

The network monitoring process involves sniffing the traffic flowing through the network. For this purpose, network packets must be captured, and a signature analysis must be conducted to identify any malicious activity. Security professionals should constantly strive to maintain smooth network operation by monitoring network traffic. If the network goes down even for a small period, productivity within a company may decline. To be proactive rather than reactive, the traffic movement and performance must be monitored to ensure that no security breach occurs within the network.

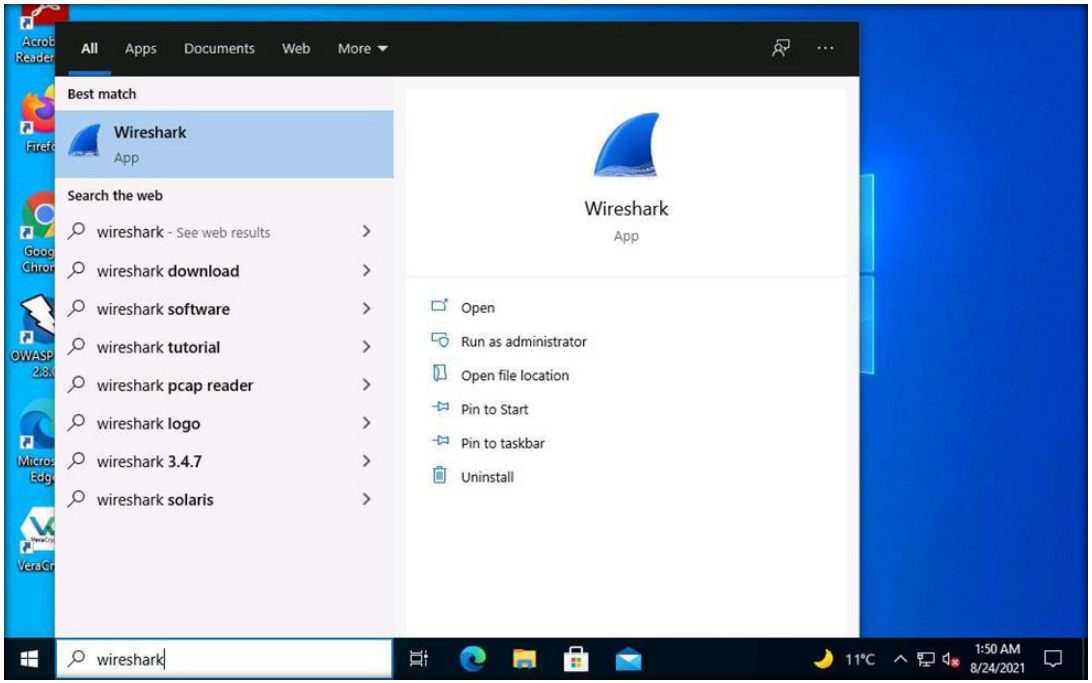
Note: Ensure that the PfSense Firewall virtual machine is running.

1. Turn on Admin Machine-1, Web Server and Attacker Machine-2 virtual machines.
2. Log in with the credentials Admin and admin@123.

Note: If the network screen appears, click Yes.

3. Click on Type here to search field at the bottom right of the Desktop, type wireshark and select Wireshark from the results. The Wireshark app will appear. Click to open the Wireshark.

EXERCISE 1: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



4. The main window of Wireshark appears.

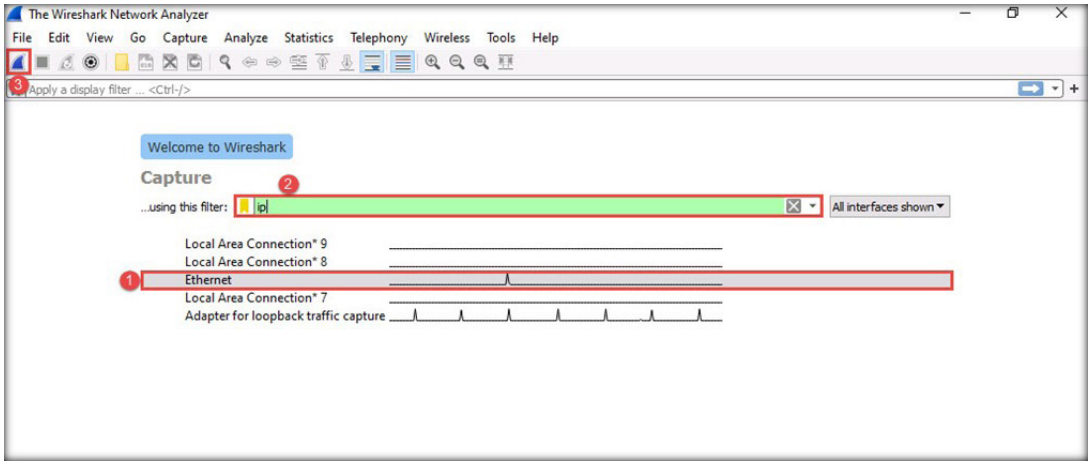
Note: If Software Update Window appears, click on Skip this version.

5. Next, you need to select the interface of which you want Wireshark to capture traffic. To begin packet capture, select the Ethernet interface from the list and in the Enter a captured filter... field, enter ip.

Note: The ip filter captures only IPv4 traffic not IPv6.

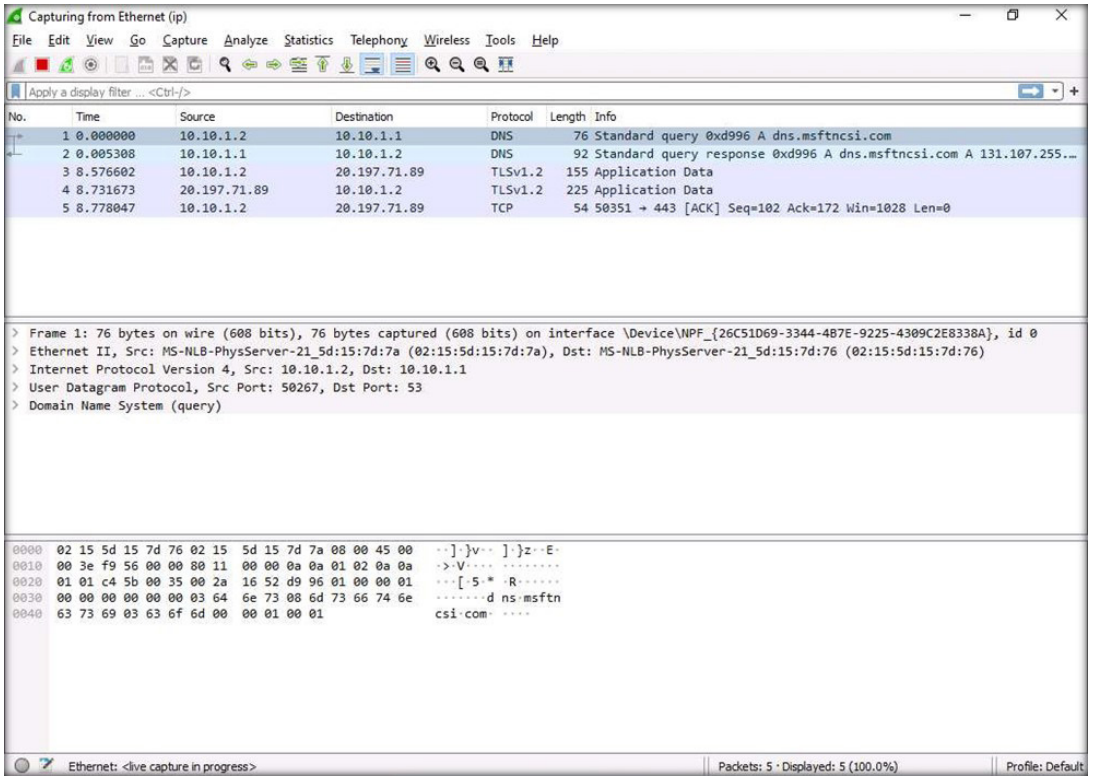
6. Now, to begin packet capturing, click Start capturing packets icon (blue color shark fin icon) from the tool bar.

EXERCISE 1: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



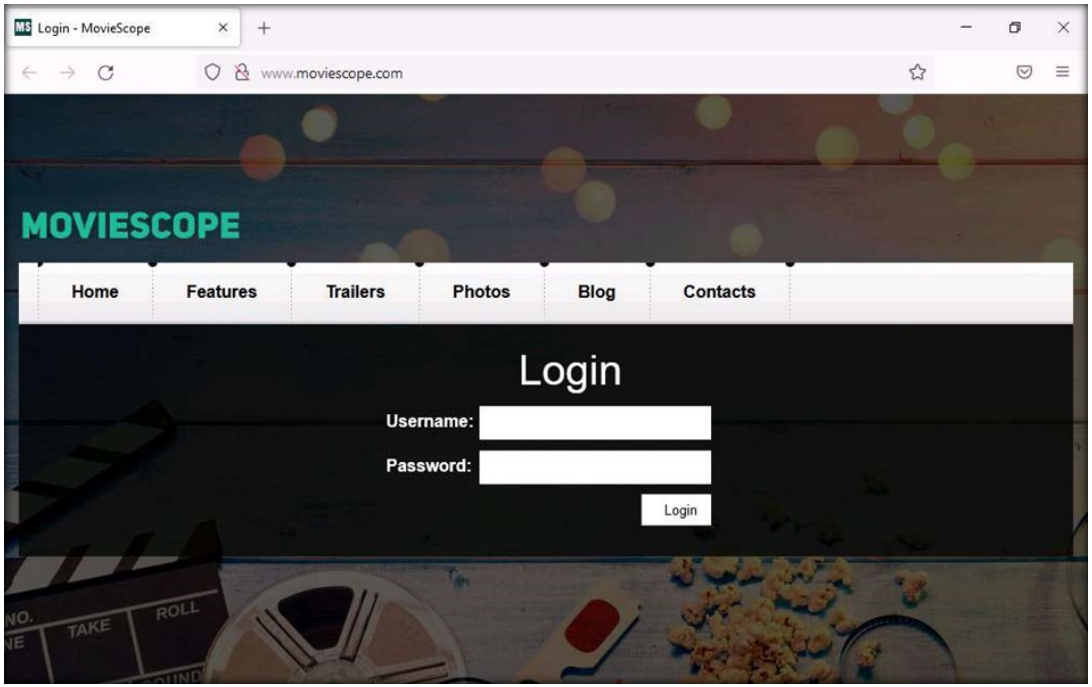
7. Wireshark begins to capture the traffic of the selected interface, as shown in the screenshot below.

EXERCISE 1: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



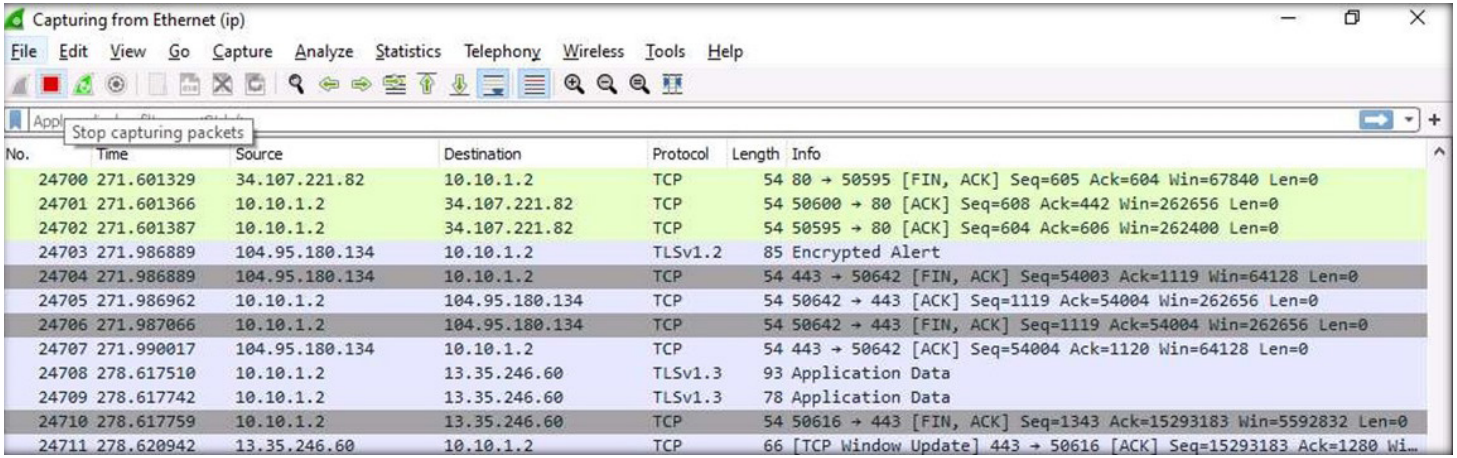
8. Minimize the Wireshark window.
9. Open any web browser (here, Mozilla Firefox) and type http://www.moviescope.com in the url field and press Enter.

EXERCISE 1: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



10. Now, switch back to the Wireshark window and click Stop capturing packets icon (red square icon) from the tool bar to stop capturing packets.

EXERCISE 1: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



11. From the captured packets, select any DNS frame (they are light blue in colour), and observe the packet content displayed in the middle section, as shown in the screenshot below.

Note: Frame: Displays details regarding captured bytes.

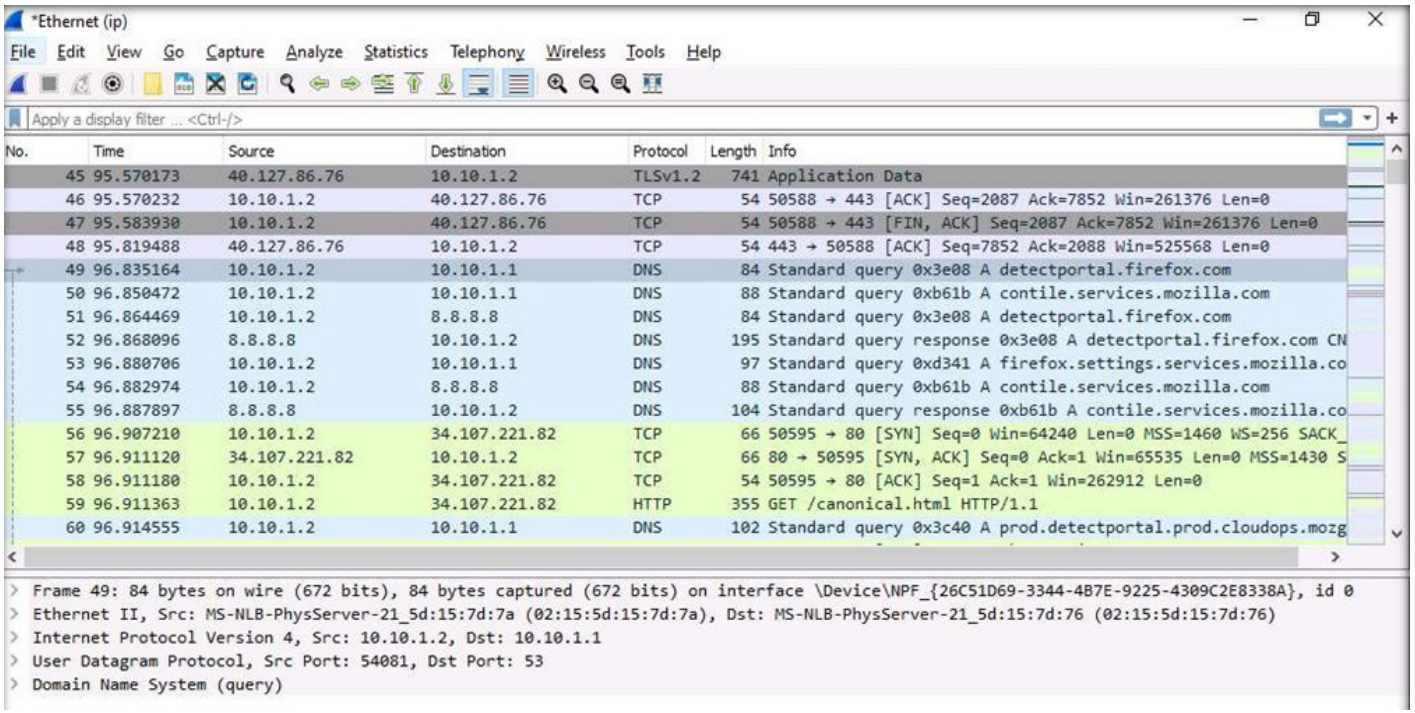
• Ethernet II: Displays details such as destination and source MAC addresses and type of network protocol used in the captured packet such as IPv4.

• Internet Protocol Version 4: Displays details such as source and destination IP addresses.

• User Datagram Protocol: Displays source and destination ports, length of the frame and checksum values.

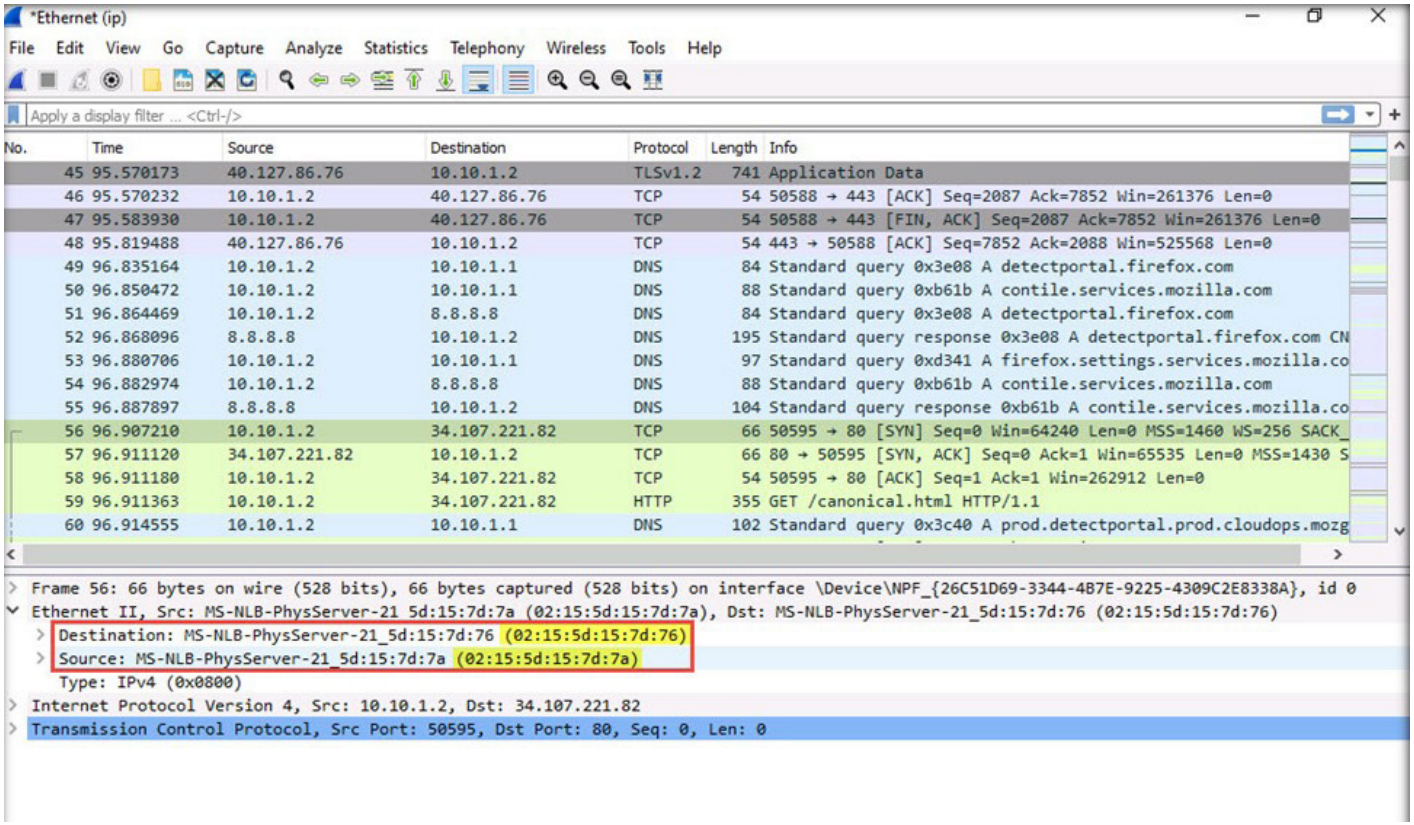
• Domain Name System: Refers to the application protocol, there are two types of frame query and response.

EXERCISE 1: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



12. Now, select first TCP packet (with light green color), to observe the packet content.
13. In the middle section, you can observe source and destination MAC addresses under Ethernet II, as shown in the screenshot below.

EXERCISE 1: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP

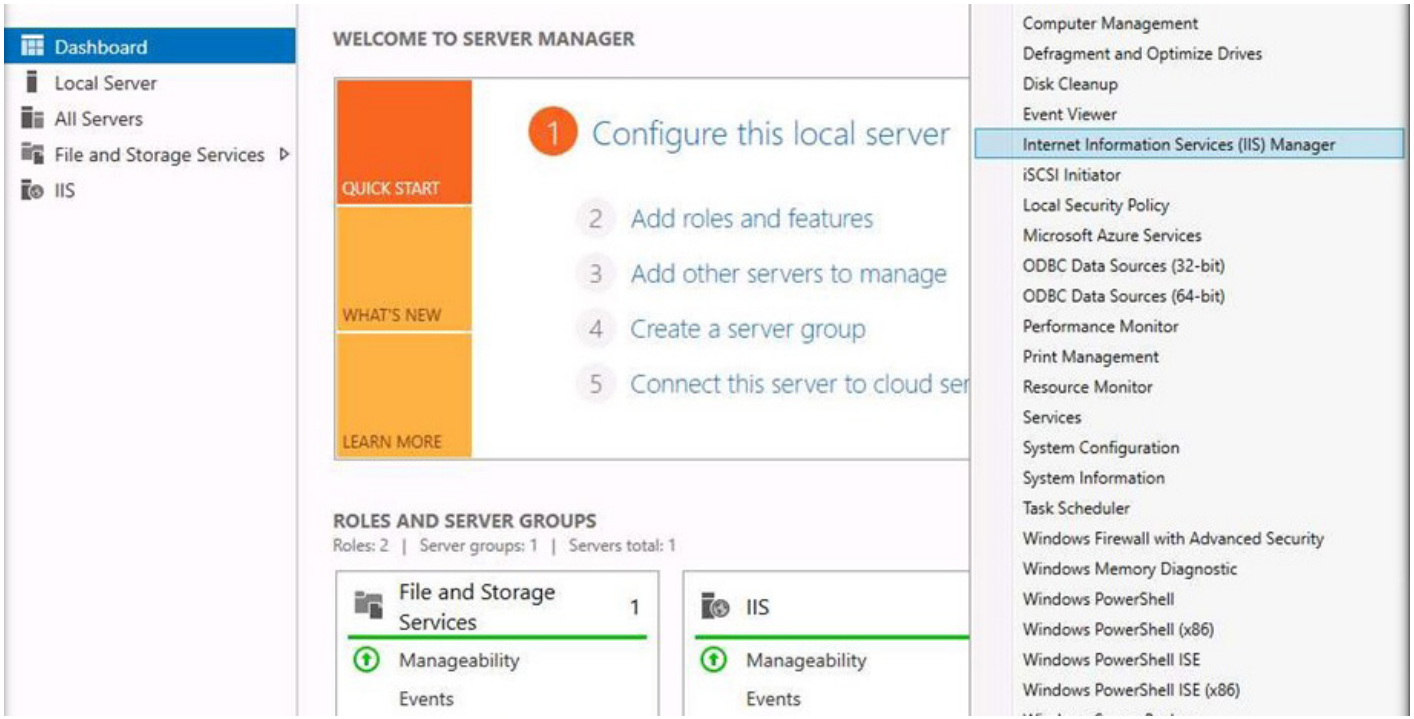


14. Similarly, you can view all the other information under different sections such as Frame, Internet Protocol Version 4, Transmission Control Protocol.
15. Close all open windows.
16. Now, we will use tcpdump tool to intercept HTTP traffic.
17. Switch to the Web Server virtual machine.
18. Log in with the credentials Administrator and admin@123.

Note: The network screen appears, click Yes.

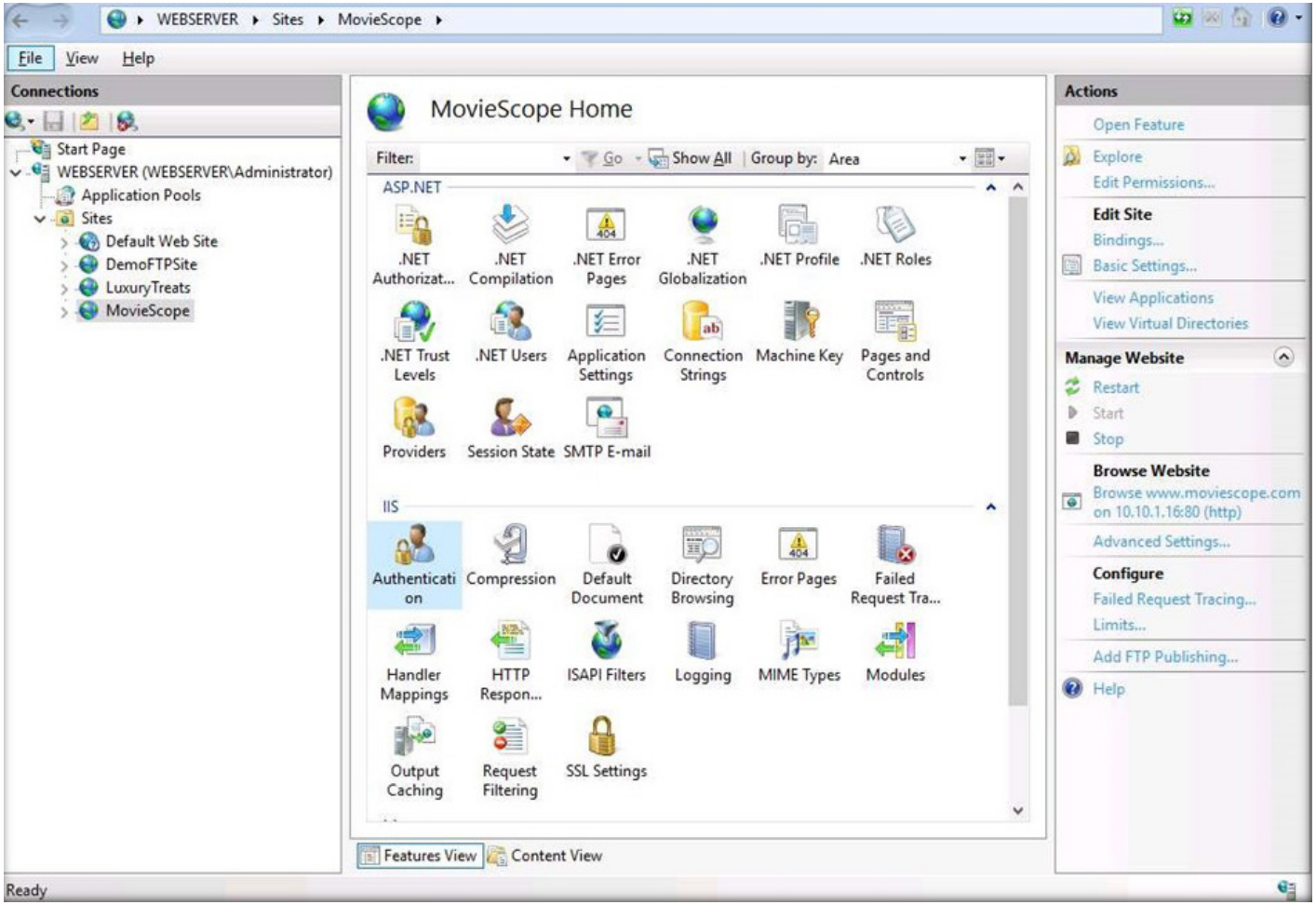
19. Click Start icon from the lower-left corner of the Desktop and from the options, select Server Manager.
20. The Server Manager window appears. Click Tools and select Internet Information Services (IIS) Manager option.

EXERCISE 1: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



21. The Internet Information Services (IIS) Manager window appears; expand WEBSERVER (WEBSERVER\Administrator) node and Sites node under the Connections section from the left-hand pane. Select MovieScope site.
22. From the middle-pane, double-click on Authentication applet under IIS section.

EXERCISE 1: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP

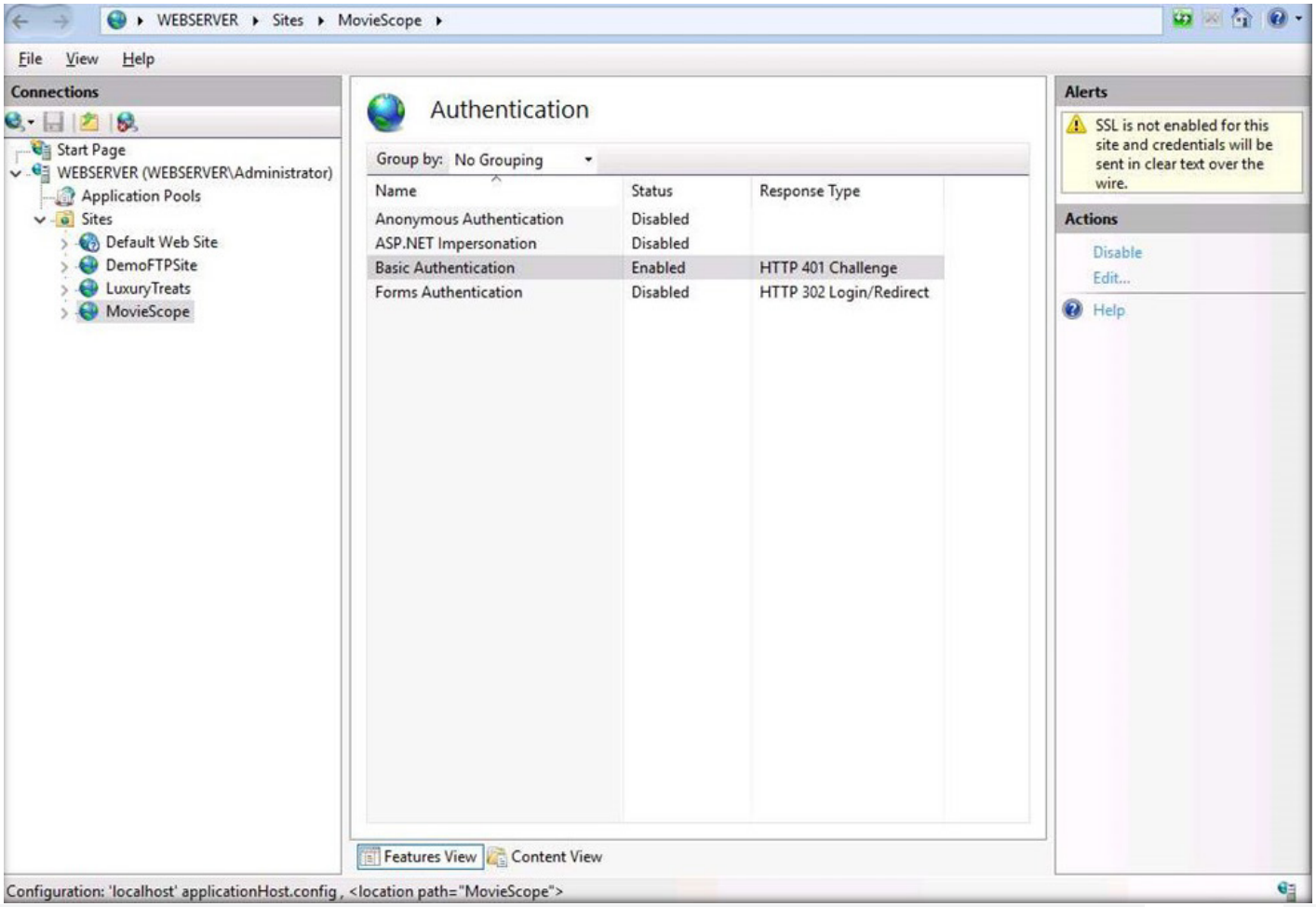


23. Authentication wizard appears, select Anonymous Authentication and click Disable from the right-pane under Actions section.

24. Similarly, select Basic Authentication and click Enable from the right-pane under Actions section.

Note: For demonstration purposes, here, we are using Basic authentication mechanism where plaintext credentials are used to authenticate and access the website which is not a safe practice. In real practice, it is advised to use Windows authentication which is considerably more secure than basic authentication.

EXERCISE 1: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



25. Switch to the Attacker Machine-2 virtual machine.
26. In the login page, the attacker username will be selected by default. Enter password as toor in the Password field and press Enter to log in to the machine.

Note: If a Parrot Updater pop-up appears at the top-right corner of Desktop, ignore and close it.

Note: If a Question pop-up window appears asking you to update the machine, click No to close the window.

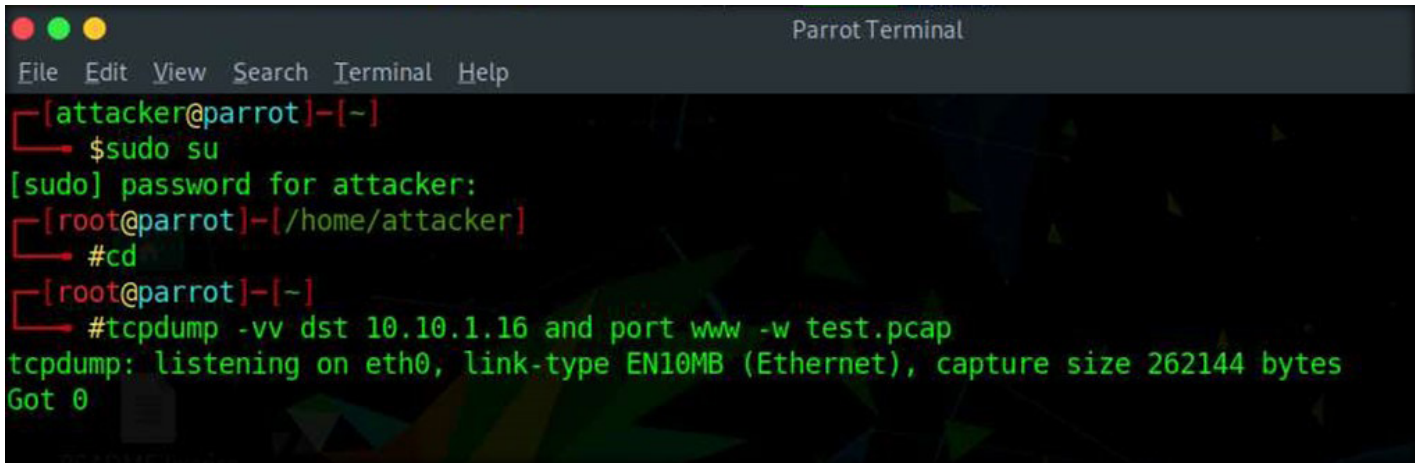
27. Click the MATE Terminal icon at the top of the Desktop window to open a Terminal window.
28. A Parrot Terminal window appears. In the terminal window, type sudo su and press Enter to run the programs as a root user.
29. In the [sudo] password for attacker field, type toor as a password and press Enter.

Note: The password that you type will not be visible.

30. Now, type cd and press Enter to jump to the root directory.
31. In the Terminal window, type tcpdump -vv dst 10.10.1.16 and port www -w test.pcap and press Enter to capture HTTP traffic of the target machine Web Server (10.10.1.16).

Note: --vv: Indicate a verbose output, dst: Indicate the destination, -w: To write raw packets to a file (here, test.pcap)

32. The tcpdump starts listening on eth0 interface to capture HTTP packets, as shown in the screenshot below.

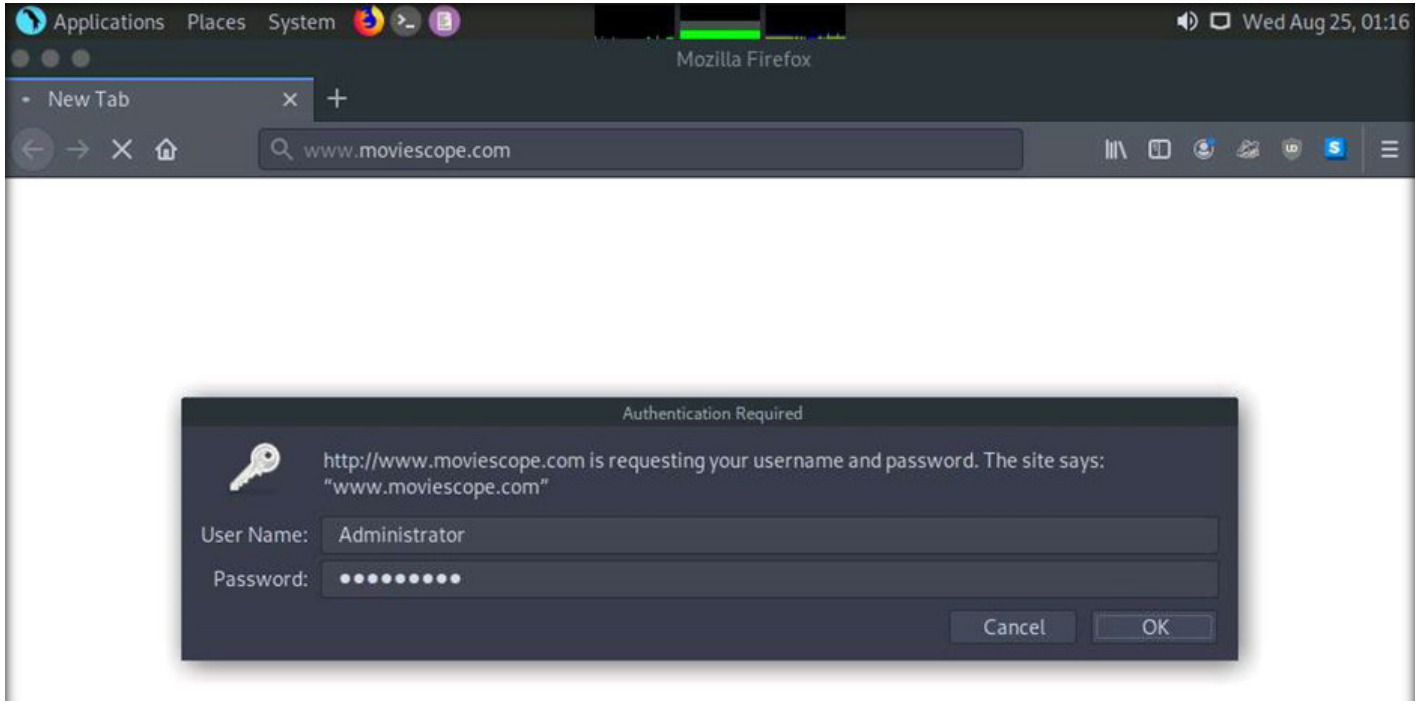


EXERCISE 1: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP

33. Click the Firefox icon from the top section of Desktop to launch the Mozilla Firefox browser.
34. The Mozilla Firefox window appears; type http://www.moviescope.com into the address bar and press Enter.
35. Authentication Required pop-up appears; type Administrator and admin@123 as User Name and Password and click OK.

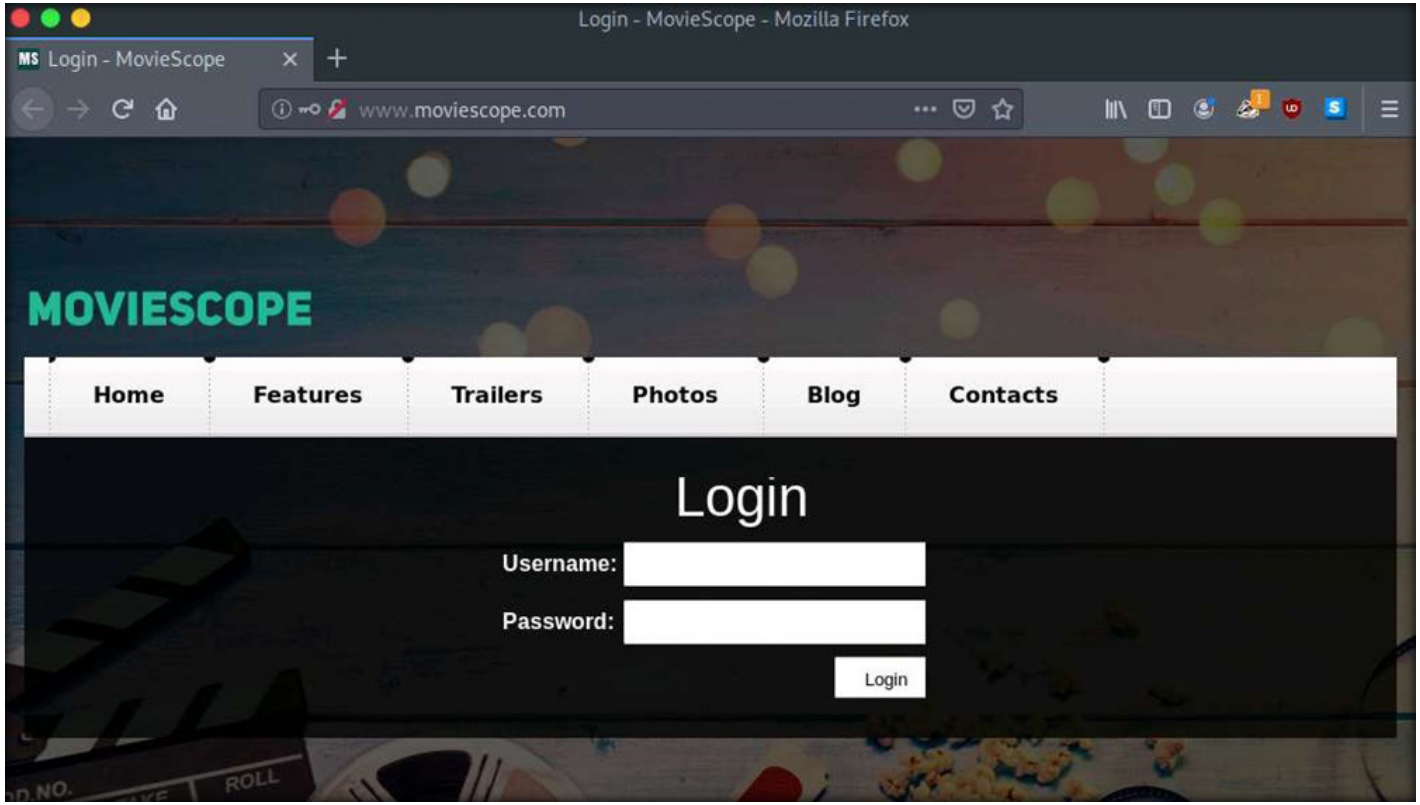
Note: If Would you like Firefox to save this login for moviescope.com? pop-up appears, click Don't Save.

EXERCISE 1: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



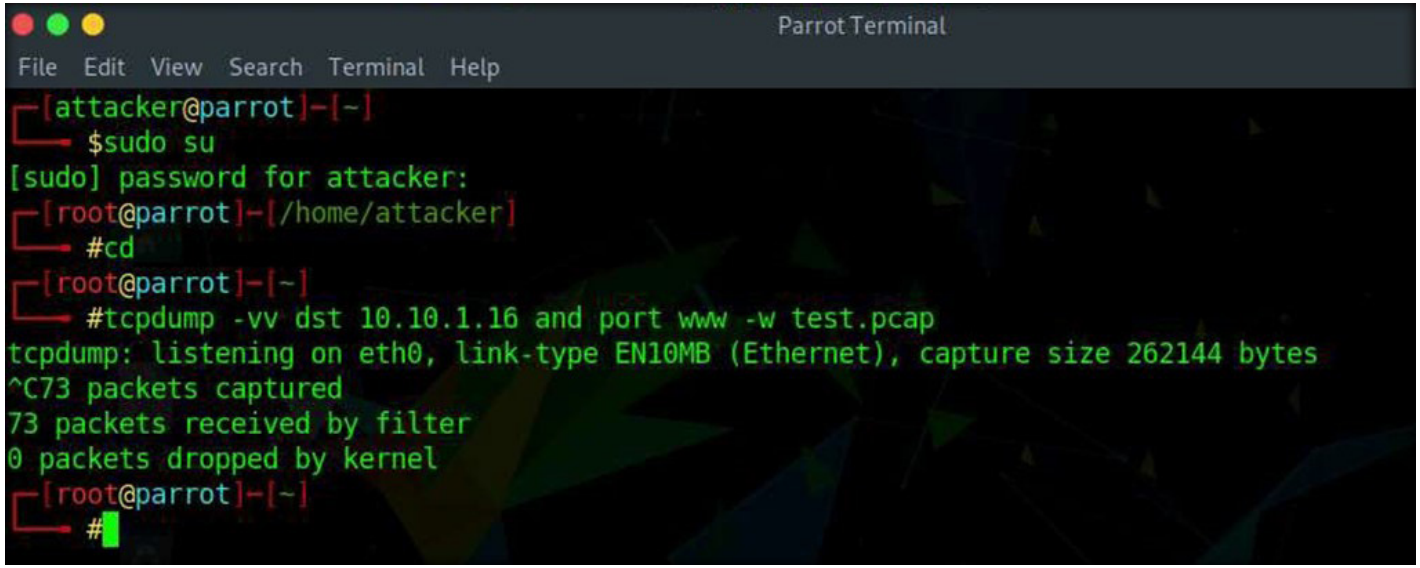
36. You have now logged successfully to access the website, as shown in the screenshot below.

EXERCISE 1: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



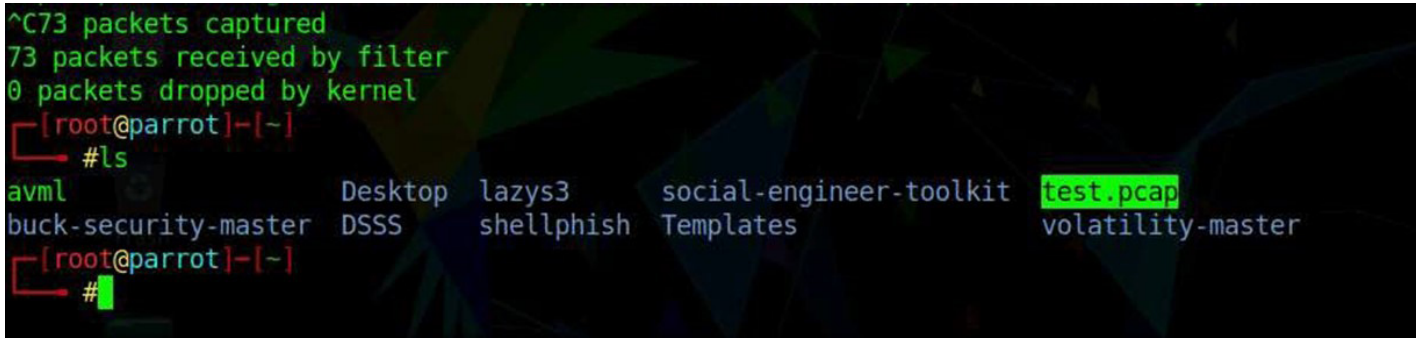
37. Switch to terminal window and press Ctrl+C to terminate intercepting network traffic.

EXERCISE 1: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



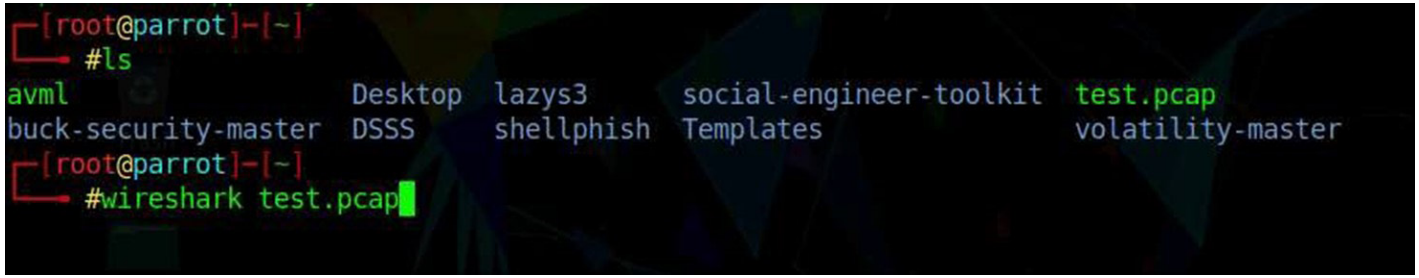
38. Type ls and press Enter.
39. You can observe a file name test.pcap has been created in the /root directory.

EXERCISE 1: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



40. Now, type wireshark test.pcap and press Enter to open the file using Wireshark.

EXERCISE 1: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP

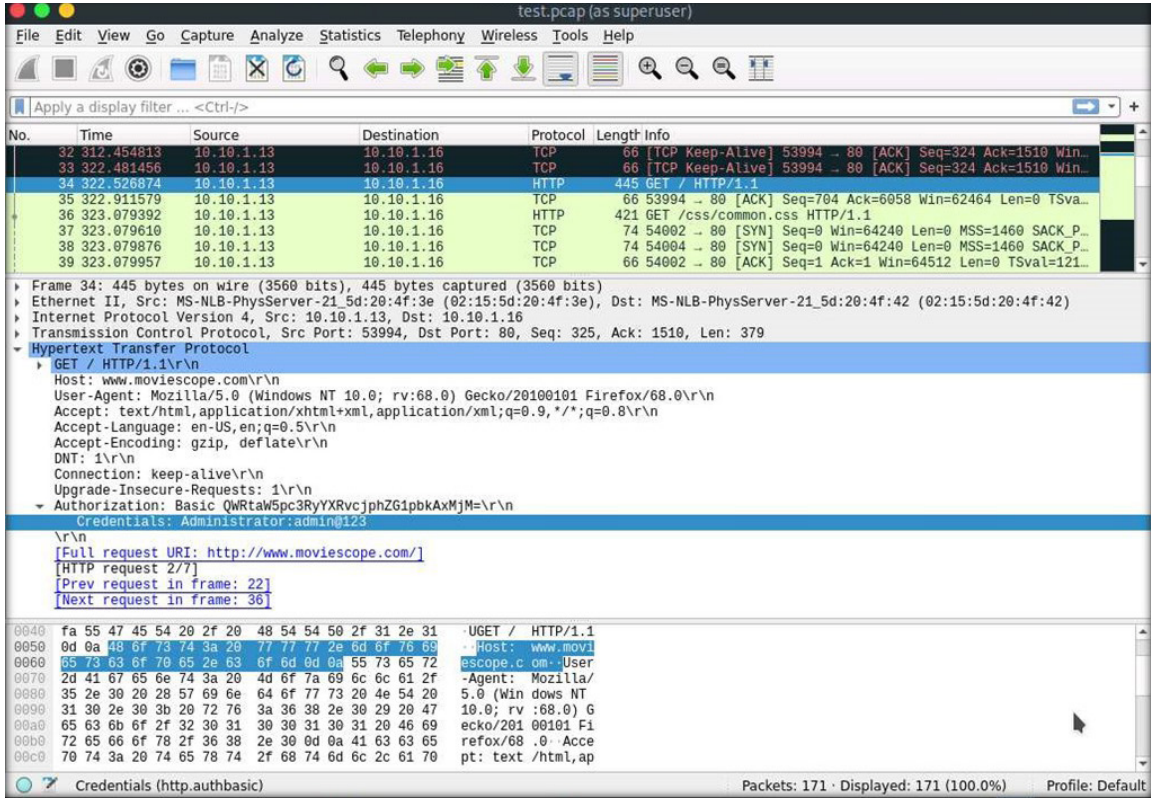


41. Click to select any HTTP message with GET request.
42. From the middle-pane, expand Hypertext Transfer Protocol node. Under Hypertext Transfer Protocol node, expand Authorization node.

Note: If you do not see Authorization node in the first block of HTTP packets then select HTTP GET packet from a different block of HTTP packets.

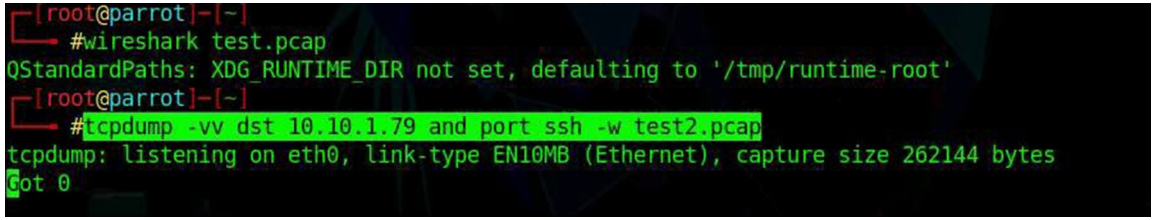
43. You can observe that the credentials are displayed because the HTTP packets are unencrypted which makes them vulnerable to packet sniffing. Close the Wireshark window.

EXERCISE 1: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



44. Now, in a similar way, we will intercept SSH traffic and observe the packet content.
45. In the terminal window, type tcpdump -vv dst 10.10.1.79 and port ssh -w test2.pcap and press Enter to capture SSH traffic to the target machine Admin Machine-2 (10.10.1.79).
46. The tcpdump starts listening on eth0 interface to capture SSH traffic, as shown in the screenshot below.

EXERCISE 1: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



47. Now, click the MATE Terminal icon at the top of the Desktop window to open another Terminal window.
48. A Parrot Terminal window appears. In the terminal window, type sudo su and press Enter to run the programs as a root user.
49. In the [sudo] password for attacker field, type toor as a password and press Enter.

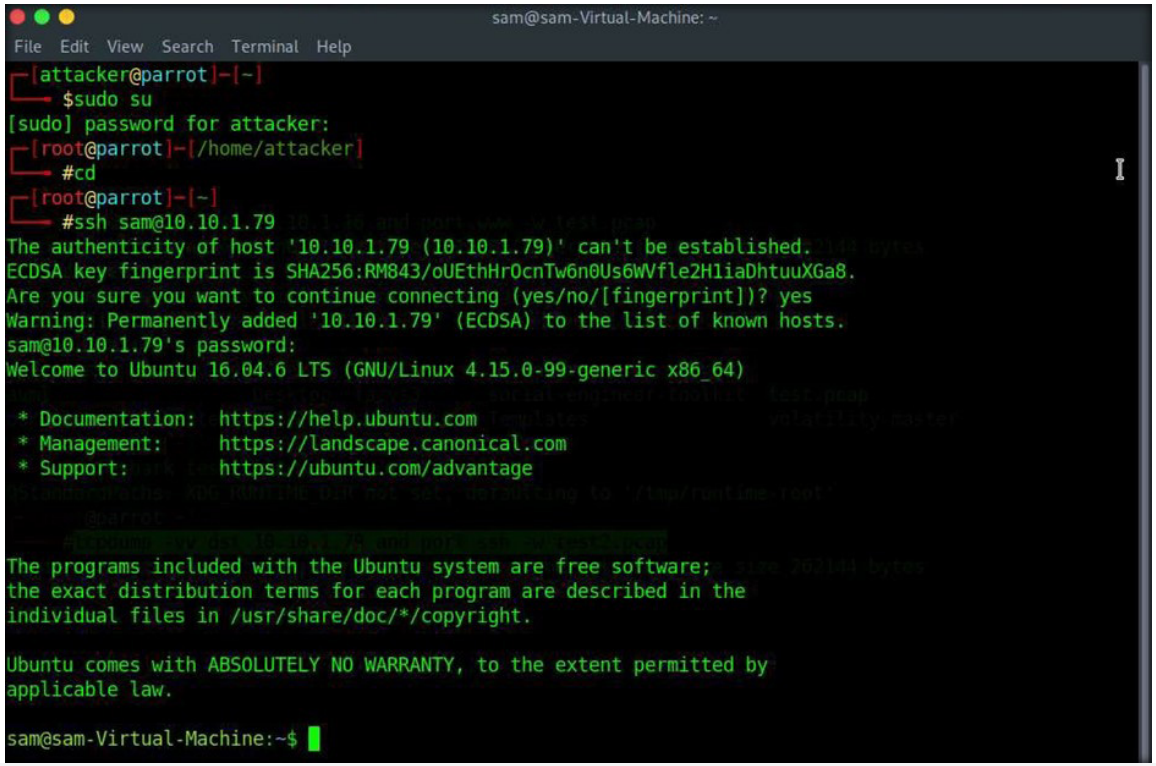
Note: The password that you type will not be visible.

50. Now, type cd and press Enter to jump to the root directory.
51. Type ssh sam@10.10.1.79 and press Enter to establish SSH connection with Admin Machine-2.

Note: If connection attempt prompt appears, type yes and press Enter.

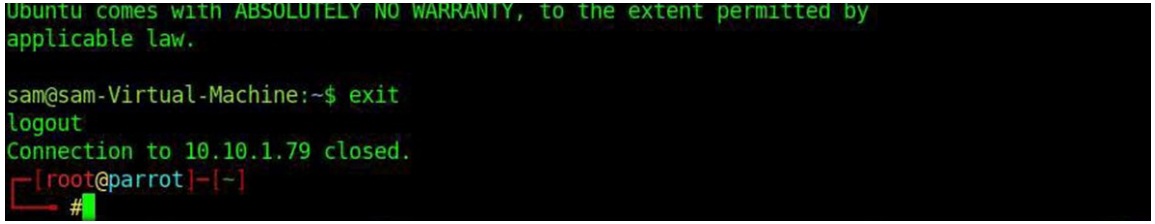
52. In the password field, type admin@123 and press Enter.
53. You can observe that a remote connection has been established, as shown in the screenshot below.

EXERCISE 1: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



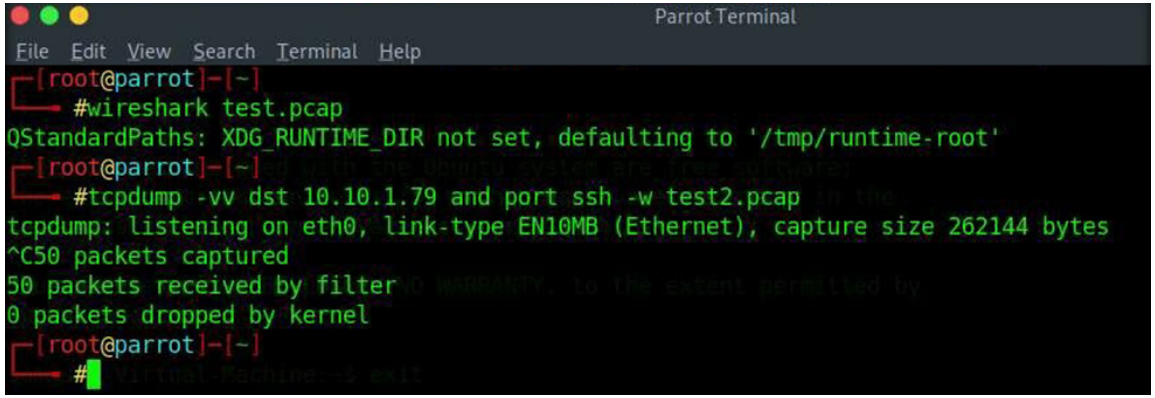
54. Type exit and press Enter to terminate the connection.

EXERCISE 1: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



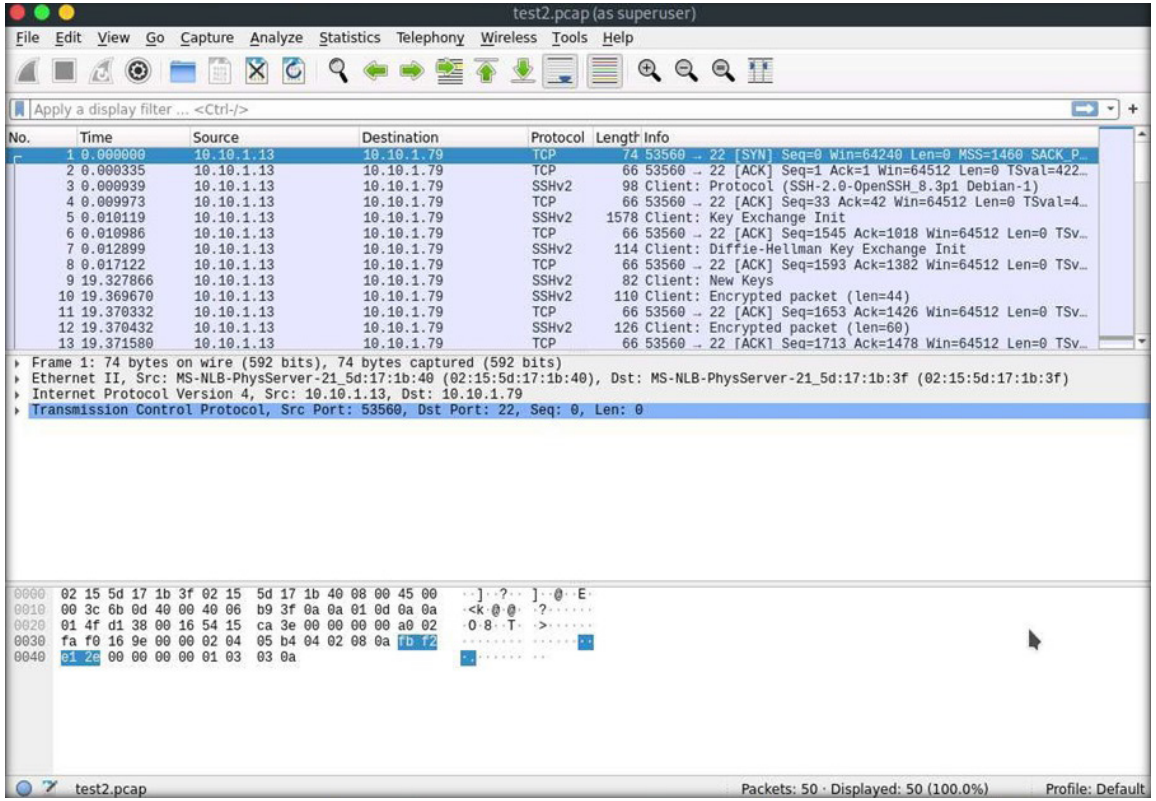
55. Now, switch back to the previous terminal window and press Ctrl+C to terminate packet capturing by tcpdump.

EXERCISE 1: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



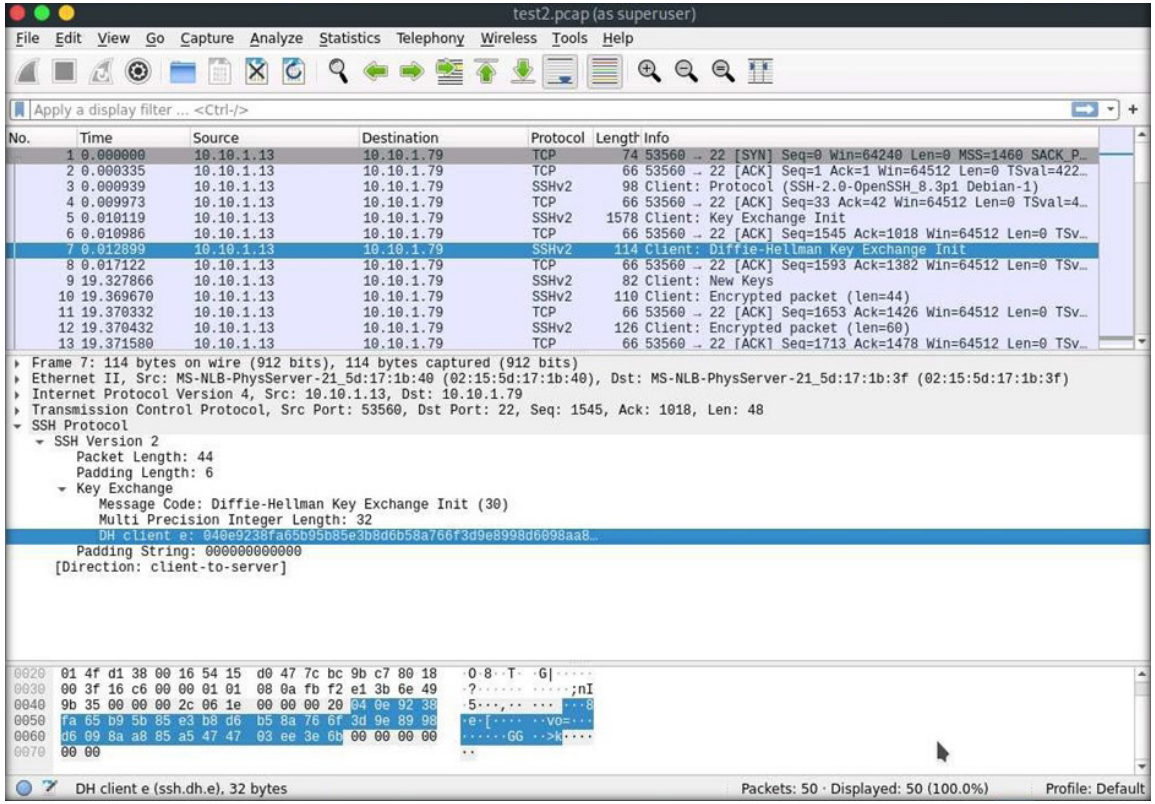
56. Type wireshark test2.pcap and press Enter to open the captured packet file using Wireshark.
57. The Wireshark window appears, displaying captured packets, as shown in the screenshot below.

EXERCISE 1: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



58. Click to select SSHv2 protocol packet with Info as Client: Diffie-Hellman Key Exchange Init.
59. In the middle-pane expand SSH Protocol node. Under SSH Protocol node, expand SSH Version 2 node and Key Exchange node.
60. You can observe that the captured password is in encrypted form, as shown in DH client e option.

EXERCISE 1: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



61. This concludes the demonstration showing how to intercept network traffic using various packet sniffing tools.
62. Close all open windows.
63. Turn off the Attacker Machine-2 virtual machine.

EXERCISE 1:
INTERCEPT
NETWORK TRAFFIC
USING WIRESHARK
AND TCPDUMP

EXERCISE 2: **APPLY VARIOUS FILTERS IN WIRESHARK**

Wireshark provides numerous filters that can be applied to obtain only the required packets.

LAB SCENARIO

Wireshark filters traffic flowing through the entire network. This traffic contains various kinds of data packets associated with various protocols flowing between the source and destination. Therefore, searching for a specific packet, port, or an IP address manually is extremely difficult. In such cases, applying Wireshark filters helps a security professional track down a huge amount of traffic and discover the intended packets. A security professional must have a good knowledge of various Wireshark filters that help you narrow down the traffic and obtain the desired result.

OBJECTIVE

This lab will help you become familiar with various Wireshark filters.

OVERVIEW OF TROJAN

Wireshark has various filters that help you filter packets containing the following:
- Source IP address
- Destination IP address
- Internet Control Message Protocol (ICMP) traffic etc.

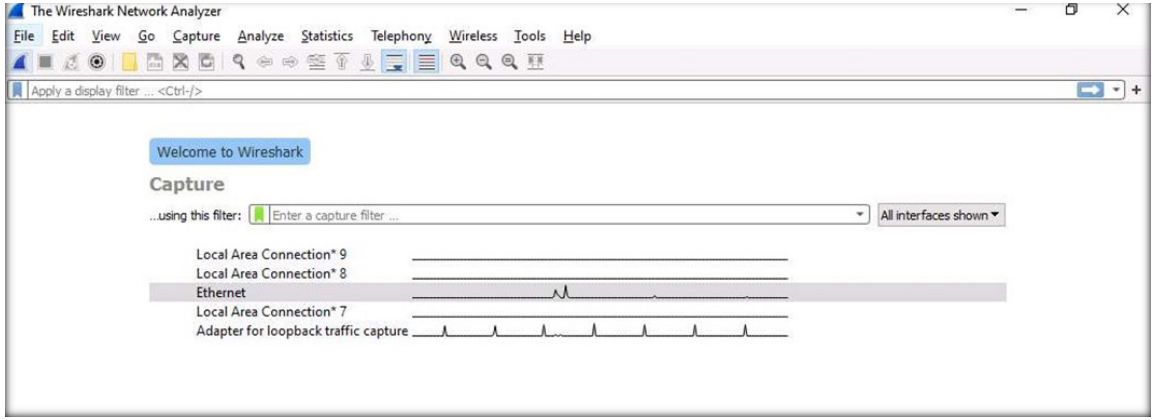
Note: Ensure that Admin Machine-1, Web Server and PfSense Firewall virtual machines are running.

1. In the Admin Machine-1 virtual machine, click Type here to Search field and type Wireshark. Select and open the Wireshark App.
2. The Wireshark main window appears.

Note: If Software Update Window appears, click on Skip this version.

3. Select Ethernet as interface and click the Start capturing packets fin icon to start capturing the network traffic.

EXERCISE 2: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP

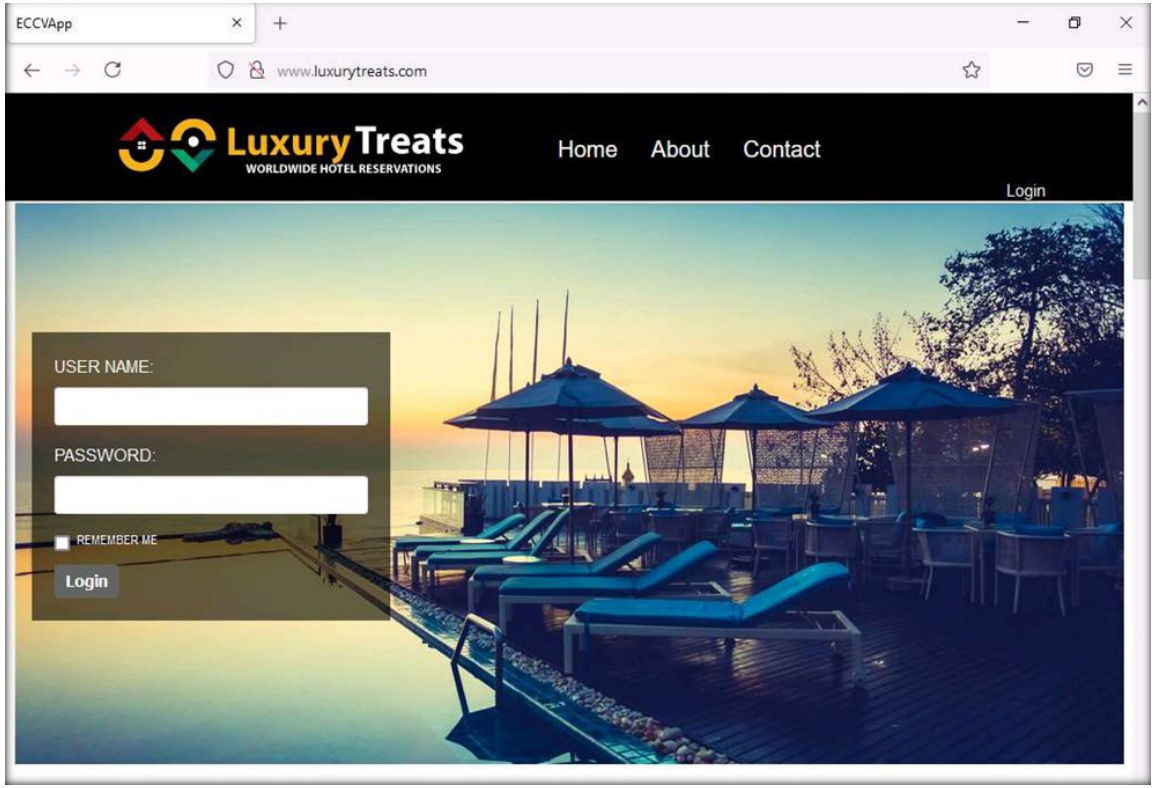


4. Next, in order to generate the network traffic between the local machine and Web Server machines, we will browse the website hosted on Web Server virtual machine.
5. Minimize the Wireshark window.
6. Open any web browser (here, Mozilla Firefox) and type http://www.luxurytreats.com in the url field and press Enter.

Note: If Default Browser pop-up appears, click Not now.

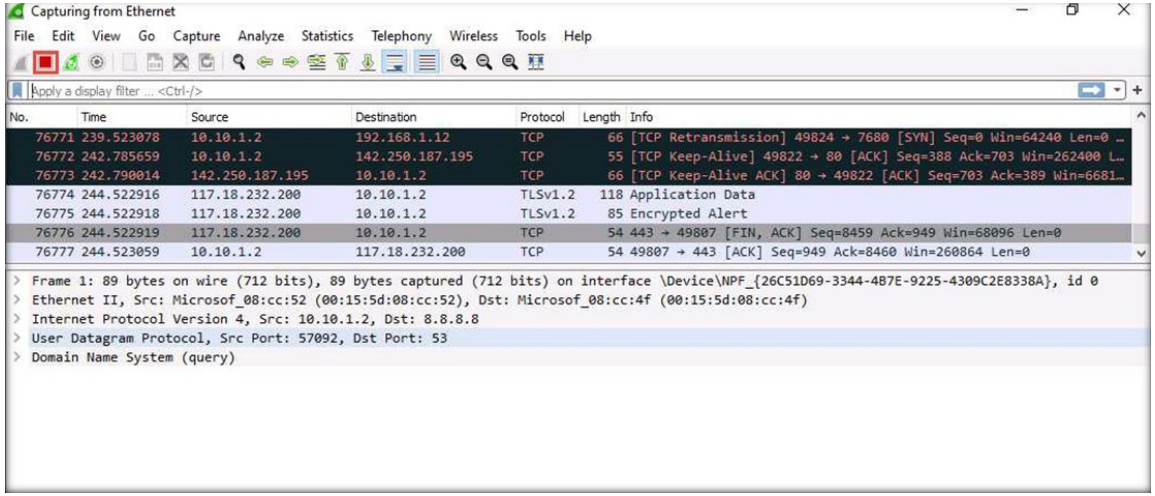
Note: Type the complete URL www.luxurytreats.com or http://www.luxurytreats.com as mentioned in the above instruction. Do not type an incomplete URL such as luxurytreats.com; otherwise, it will redirect you to some external website on the internet.

EXERCISE 2: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



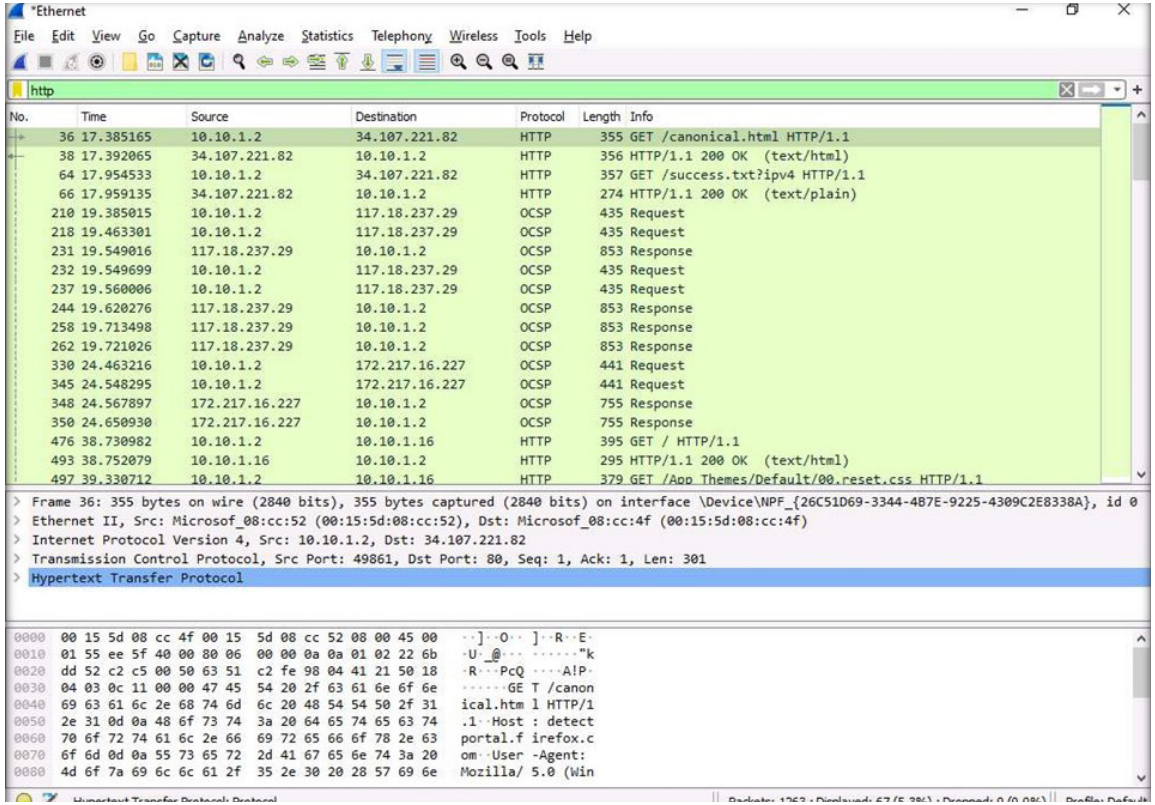
7. Now, navigate back to the Wireshark window and click Stop capturing packets icon (red color icon) in the tool bar (top-left corner) to stop the packet capturing.

EXERCISE 2:
INTERCEPT
NETWORK TRAFFIC
USING WIRESHARK
AND TCPDUMP



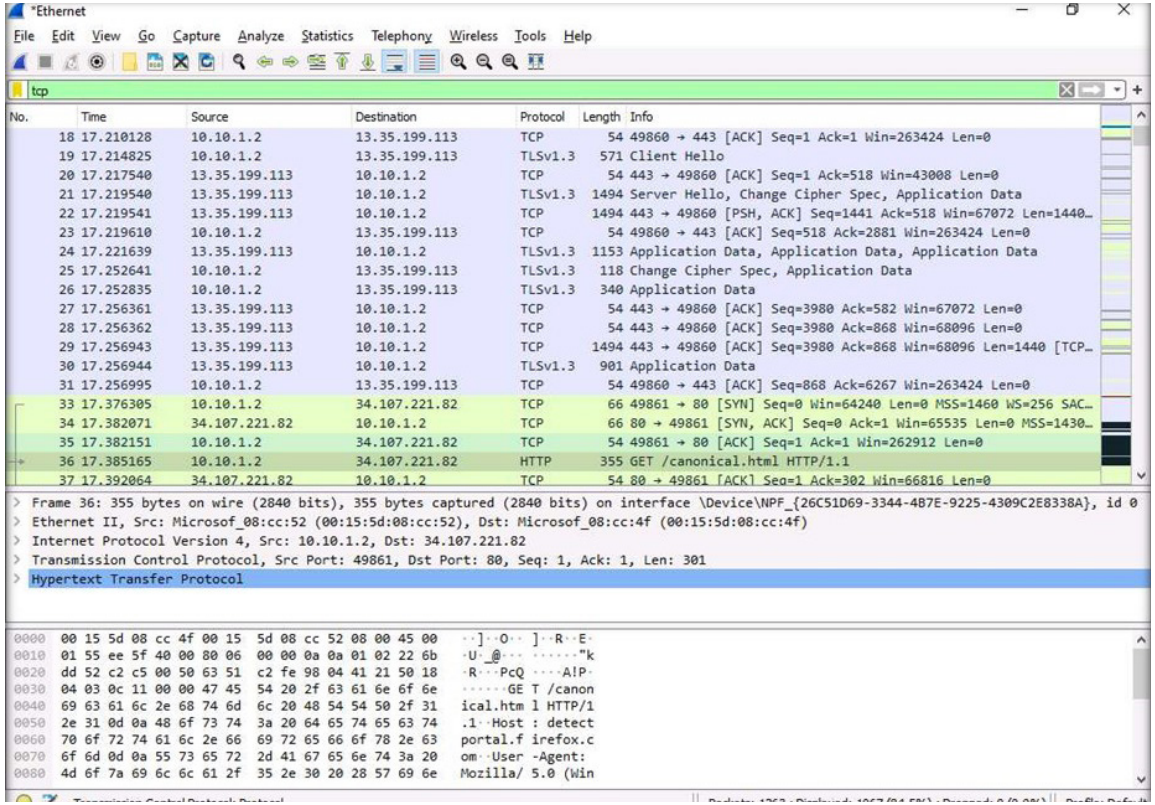
8. The Filter field at the top of the Wireshark main window allows you to apply various filters that help narrow down the traffic including filter traffic by protocol.
9. To view the HTTP-specific traffic flowing in your network, type http in the filter field and press Enter. By applying this filter, Wireshark filters and displays HTTP traffic flowing through the network.

EXERCISE 2: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



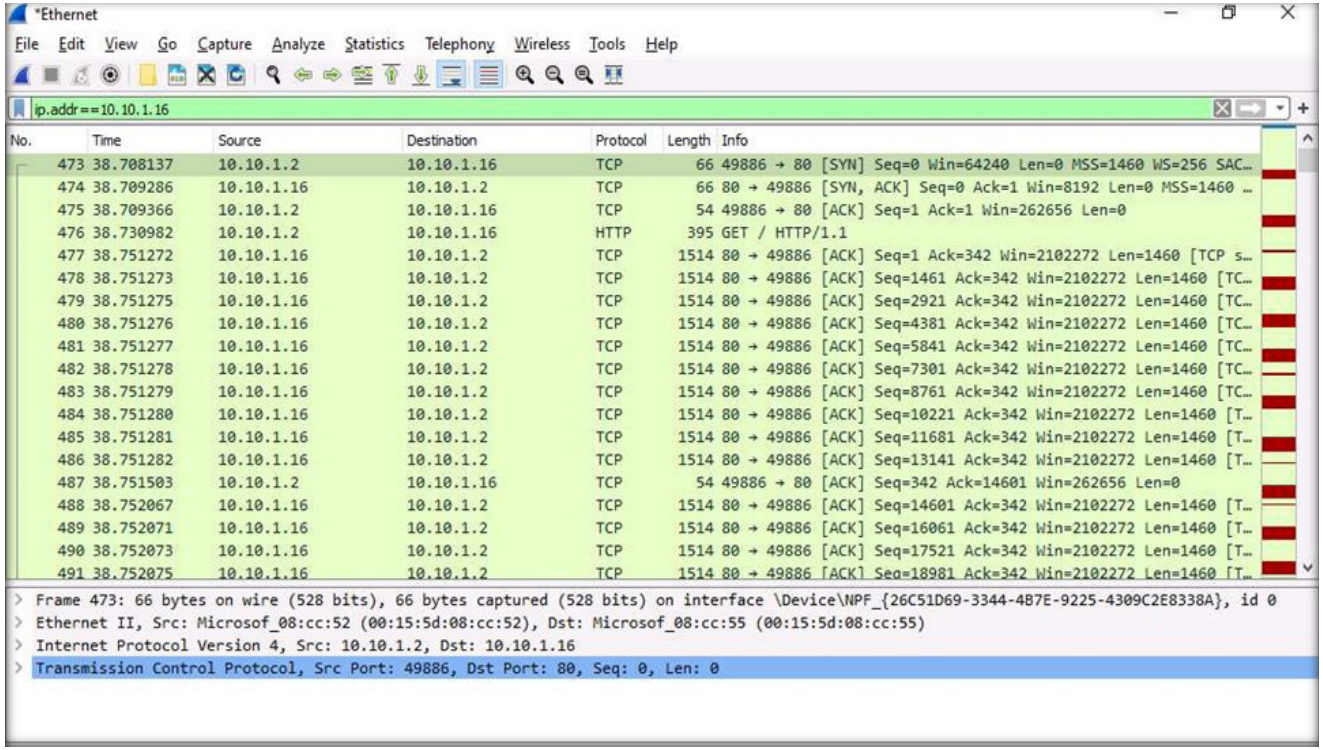
10. To view the TCP-specific traffic flowing in your network, type tcp in the filter field and press Enter. By applying this filter, Wireshark filters TCP traffic flowing through the network and displays.

EXERCISE 2: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



11. You can also filter traffic based on the source and destination IP addresses. To view traffic originating or destined to a specific IP address, apply the filter ip.addr==10.10.1.16 (the Web Server machine in which luxurytreat.com website is hosted (10.10.1.16)).

EXERCISE 2: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP

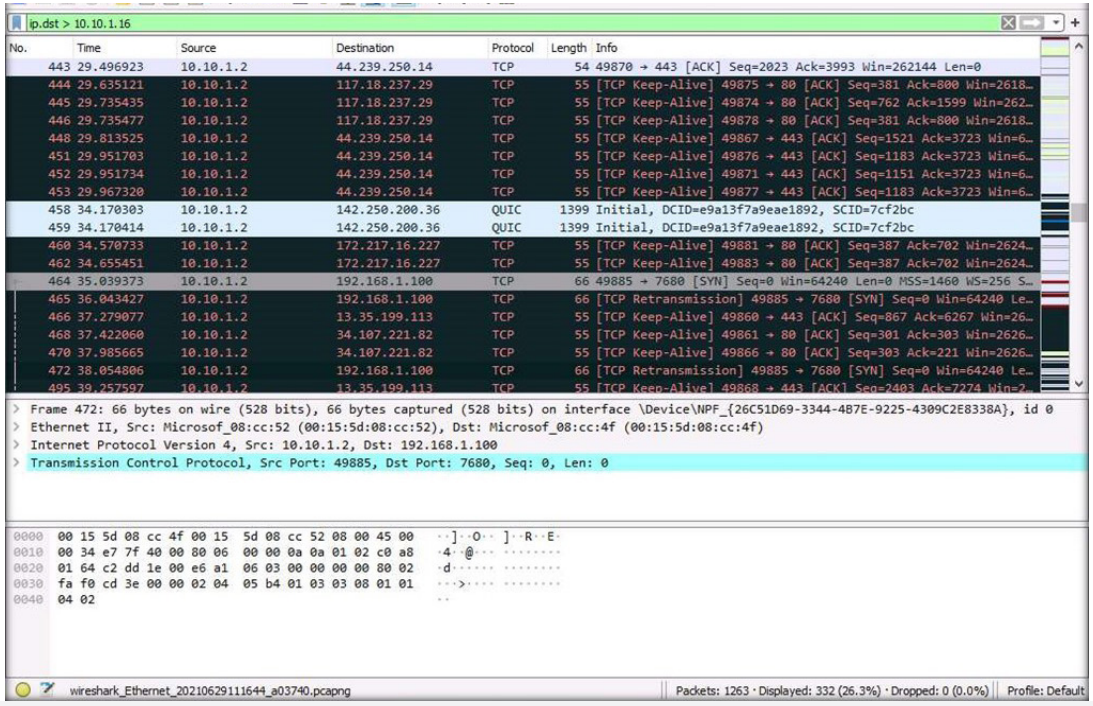


12. You can also use various conditional operators on IP address filtering to filter traffic based on your preference/requirement.

Symbol meaning:

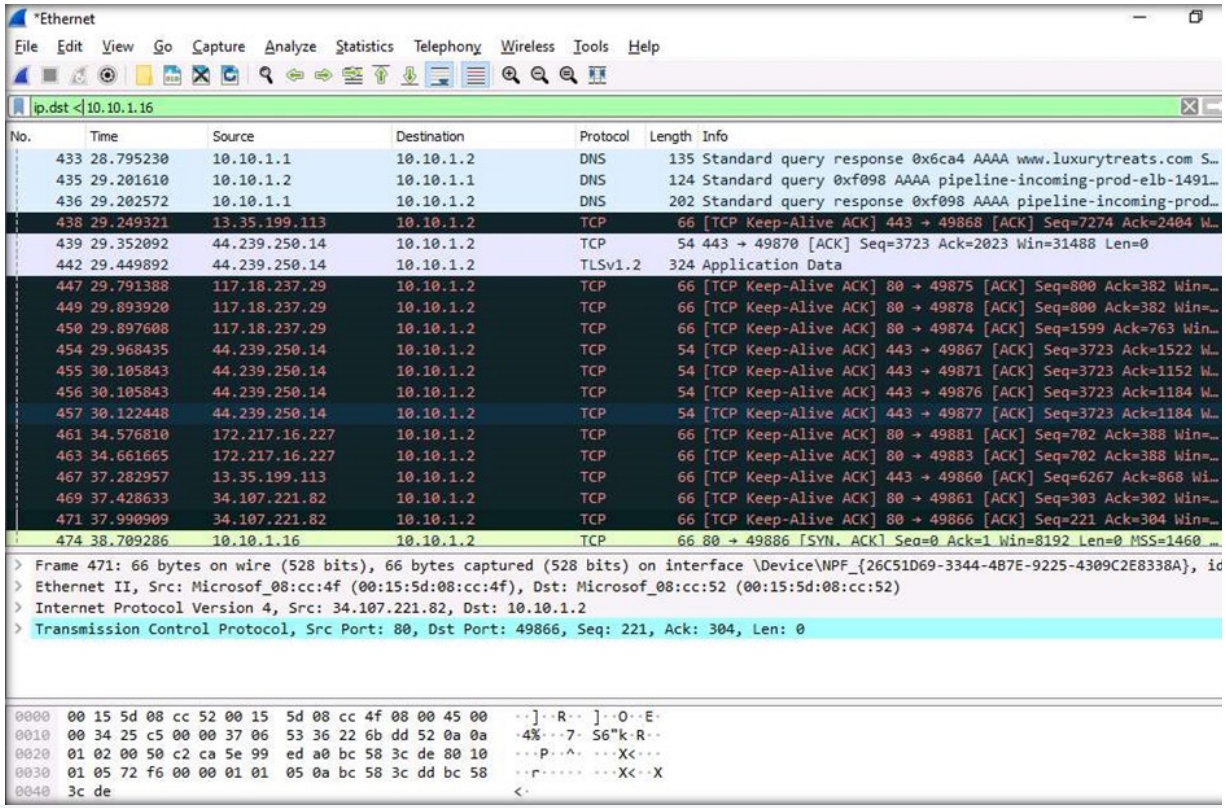
- == Is equal to
- != Not equal to
- \> Is greater than
- < Is lesser than
- \>= Greater than or equal to
- <= Less than or equal to.

13. To view traffic higher than a specific IP address, use the > conditional operator in conjunction with IP address filtering. Apply the filter ip.dst > 10.10.1.16 to find the destination IP addresses greater than the specified IP address.



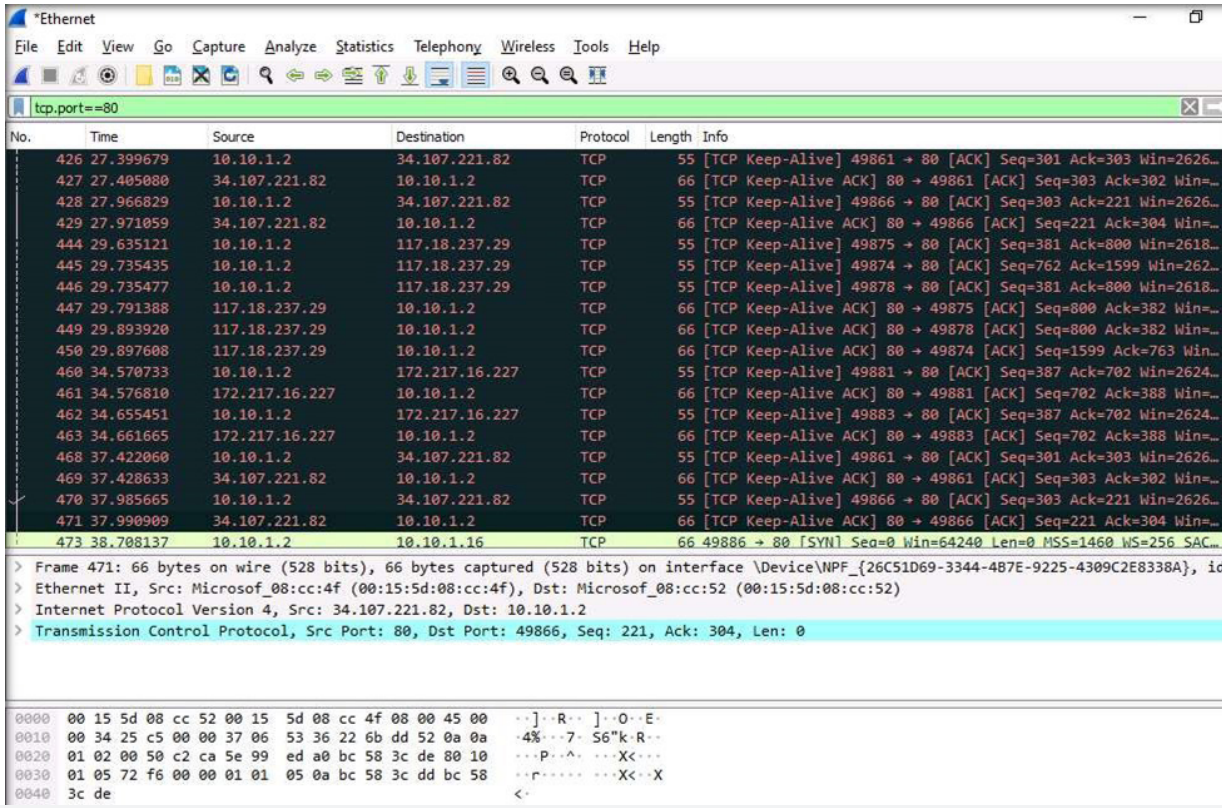
14. To view traffic less than a specific IP address, use the < conditional operator in conjunction with IP address filtering. Apply the filter ip.dst < 10.10.1.16 to find the destination IP addresses less than the specified IP address.

EXERCISE 2: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



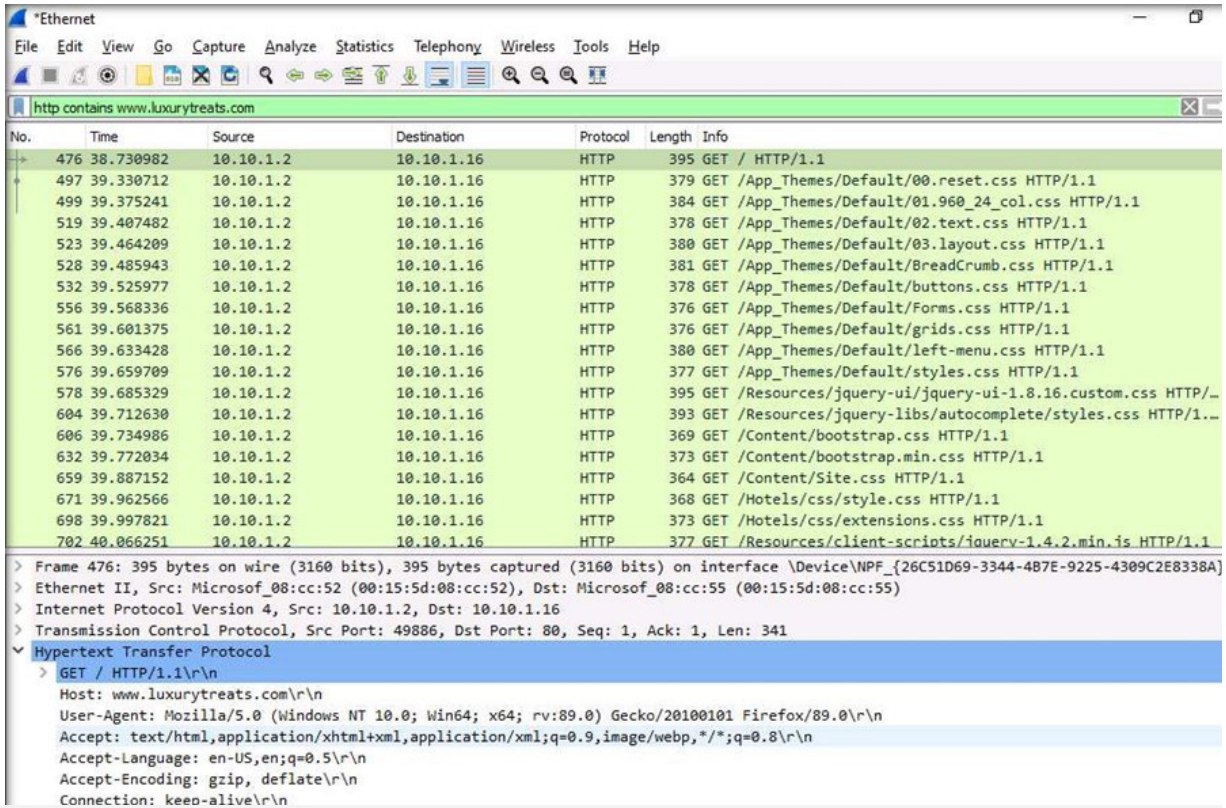
15. You can also filter traffic based on the source and destination ports. To view traffic originating or destined to the TCP port, apply the filter tcp.port==80.

EXERCISE 2: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



16. You can also filter traffic based on a specific string contained in the traffic. Apply the filter http contains www.luxurytreats.com to filter out the traffic that contains the mentioned string.

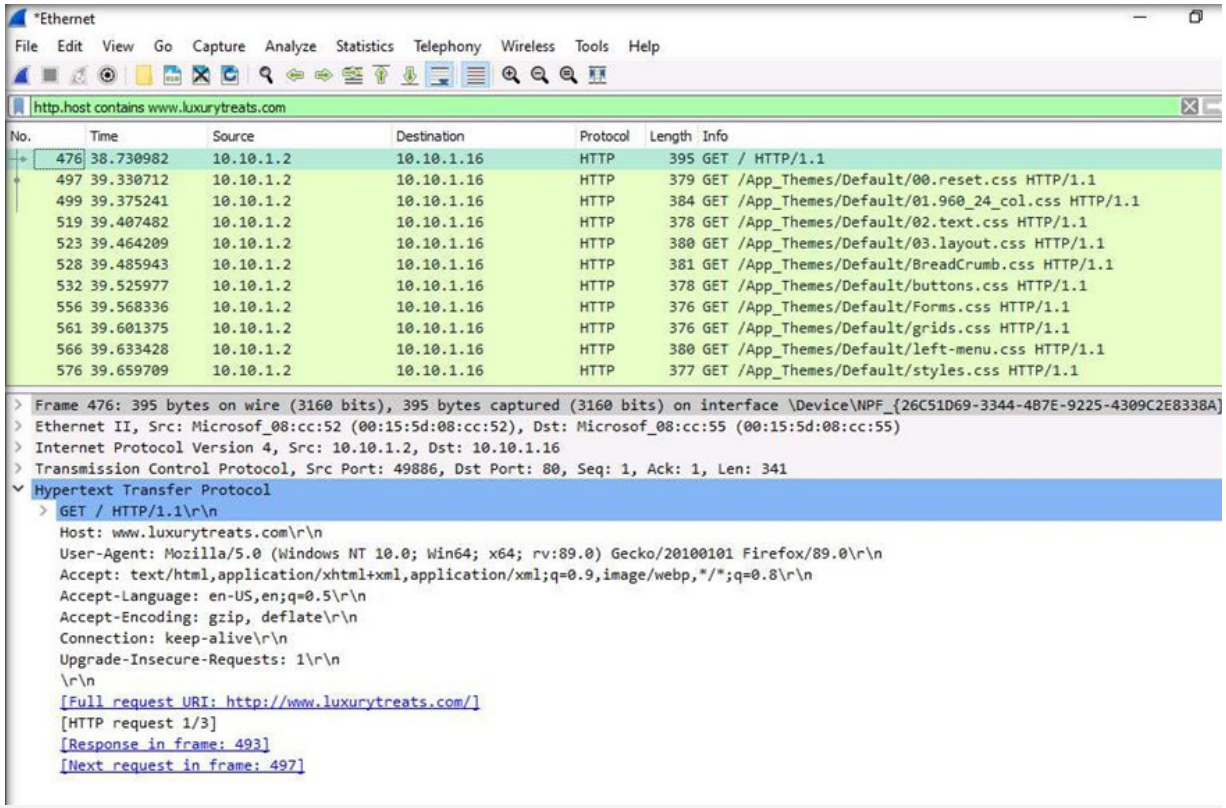
EXERCISE 2: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



Note: This can only be applied to characters and not numerals. It searches for a sequence of characters provided in the filter.

17. To view the HTTP traffic whose request header fields (host) contain a specific string, apply the http.host contains www.luxurytreats.com filter.

EXERCISE 2: INTERCEPT NETWORK TRAFFIC USING WIRESHARK AND TCPDUMP



18. Similarly, you may use various other filters to filter the required traffic.
19. As described above, a security professional can specify one or more conditional and logical operators to find traffic based on their preference/requirement. Thus, Wireshark allows you to use a wide range of filters to filter traffic based on your preference/requirement.
20. This concludes the demonstration showing how to apply various filters using Wireshark.
21. Close all open windows.
22. Turn off the Admin Machine-1 virtual machine.

EXERCISE 2:
INTERCEPT
NETWORK TRAFFIC
USING WIRESHARK
AND TCPDUMP

EXERCISE 3: **ANALYZE AND EXAMINE VARIOUS NETWORK PACKET HEADERS IN LINUX USING tcpdump**

tcpdump is used to analyze TCP/IP and other packets on Linux host machine.

LAB SCENARIO

Each packet in a network contains control information and user data, known as the payload. The control information contains data for delivering the payload, which includes, for example, source and destination IP and MAC addresses and sequencing information. The header part of the packet stores this control information. Hence, the security professional needs to know how to examine the packet headers while examining the data packets.

OBJECTIVE

The objective of this lab is to learn how to inspect TCP/IP and other packet header fields of different network packets.

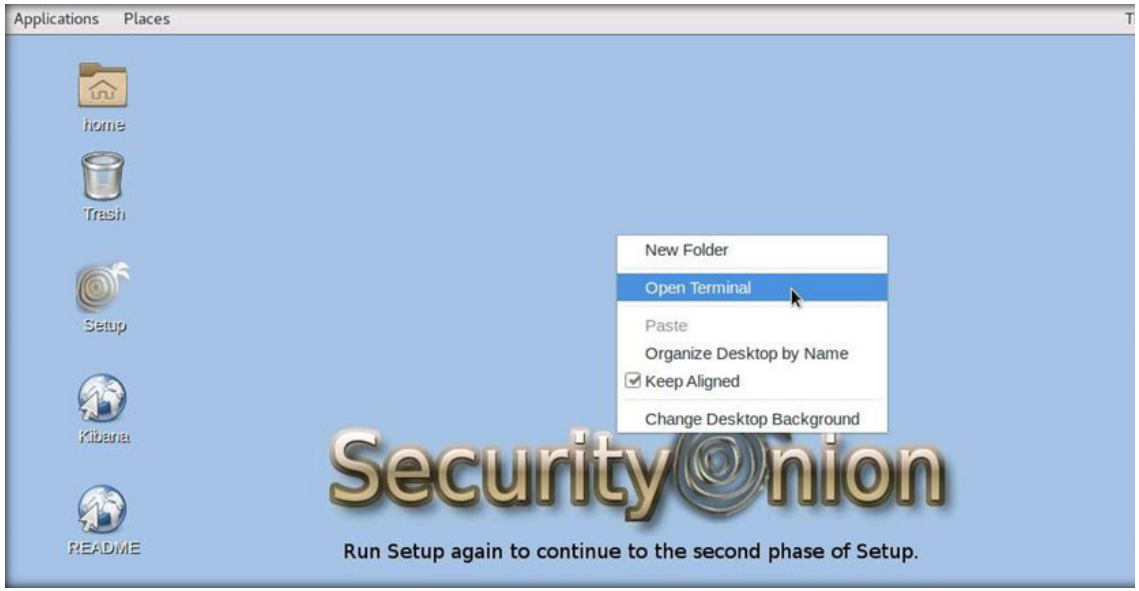
OVERVIEW OF TROJAN

Data packets traversing over a network can be intercepted using packet capture tools such as tcpdump. These captured packets are analyzed to determine whether proper network security policies are being followed.

Note: Ensure that Web Server and PfSense Firewall virtual machines are running.

1. Turn on the Admin Machine-2 virtual machine.
2. Type username as sam and password as admin@123 and click Log In.
3. Open a terminal by right-clicking on Desktop, and then click Open Terminal from the pop-up menu.

EXERCISE 3: ANALYZE AND EXAMINE VARIOUS NETWORK PACKET HEADERS IN LINUX USING TCPDUMP



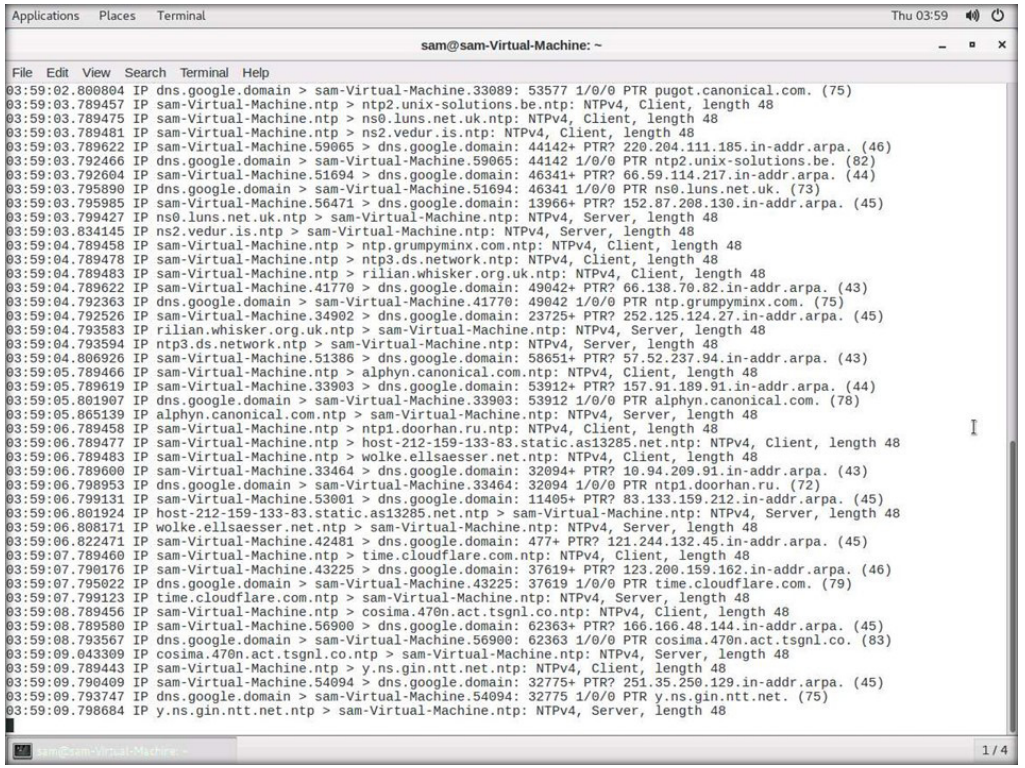
4. The Terminal window will appear. Type sudo tcpdump in Command Prompt and press Enter to capture the network packets of the machine. If you encounter a password prompt, type admin@123.

Note: The password that you type will not be visible.

EXERCISE 3:
ANALYZE AND EXAMINE VARIOUS NETWORK PACKET HEADERS IN LINUX USING TCPDUMP

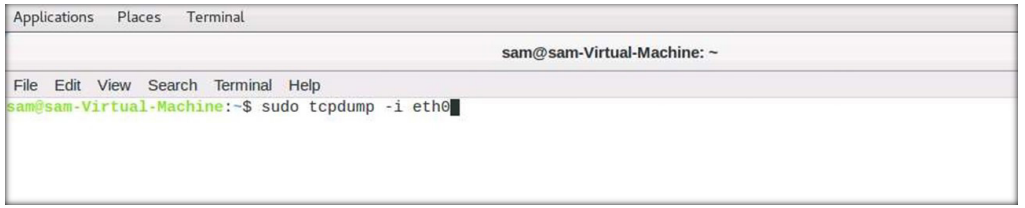
5. The tcpdump command shows the entire payloads captured packet.

EXERCISE 3:
ANALYZE AND EXAMINE VARIOUS NETWORK PACKET HEADERS IN LINUX USING TCPDUMP



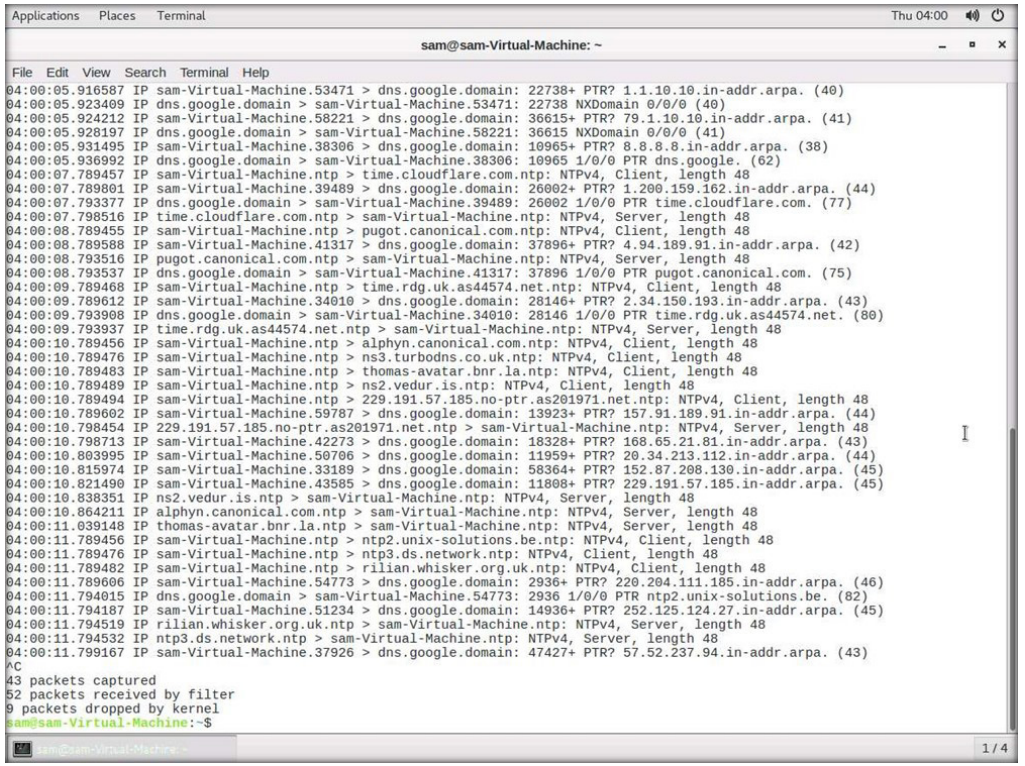
6. Press Ctrl + C to end the packet capture.
7. Type sudo tcpdump -i eth0 in the terminal and press Enter to capture the network packets from the machine's specific interface.

EXERCISE 3:
ANALYZE AND
EXAMINE VARIOUS
NETWORK PACKET
HEADERS IN LINUX
USING TCPDUMP



8. Press Ctrl + C to end the packet capture.

EXERCISE 3:
ANALYZE AND EXAMINE VARIOUS NETWORK PACKET HEADERS IN LINUX USING TCPDUMP

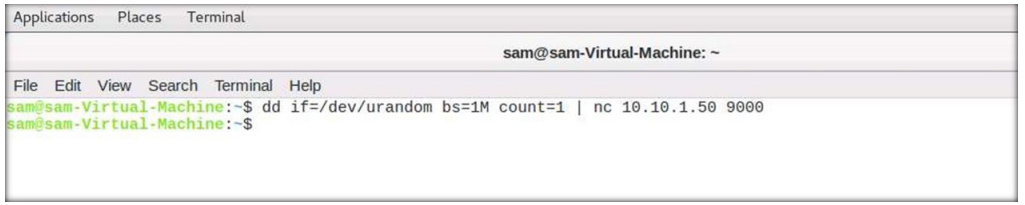


9. Type sudo tcpdump -i eth0 tcp in the terminal and press Enter to capture only the TCP packets from the machine interface.

EXERCISE 3:
ANALYZE AND EXAMINE VARIOUS NETWORK PACKET HEADERS IN LINUX USING TCPDUMP

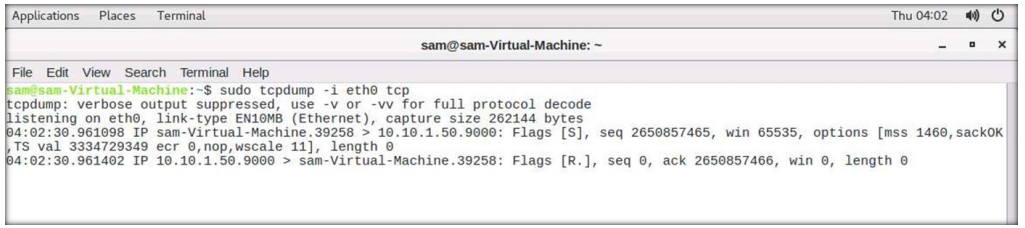
10. Open another terminal and type dd if=/dev/urandom bs=1M count=1 | nc 10.10.1.50 9000 and press Enter; it generates the TCP packets of 1MB and sends them to destination 10.10.1.50.

EXERCISE 3:
ANALYZE AND
EXAMINE VARIOUS
NETWORK PACKET
HEADERS IN LINUX
USING TCPDUMP



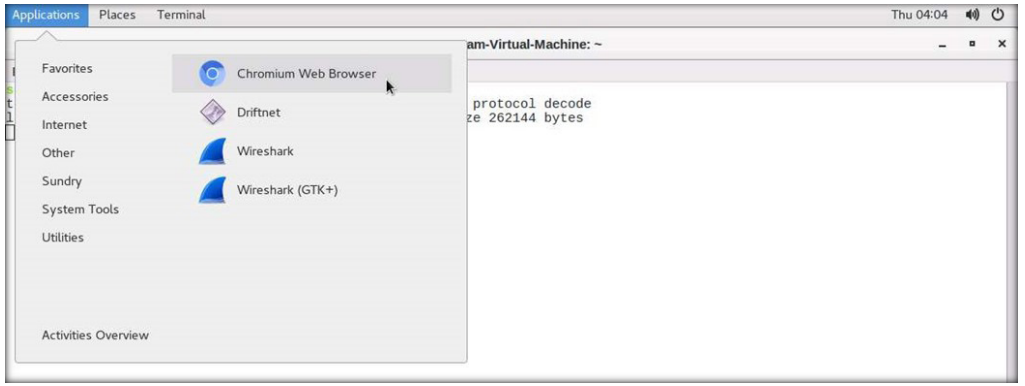
11. Switch back to the first Terminal; here, you can see the traffic captured by the Tcpdump.

EXERCISE 3:
ANALYZE AND
EXAMINE VARIOUS
NETWORK PACKET
HEADERS IN LINUX
USING TCPDUMP



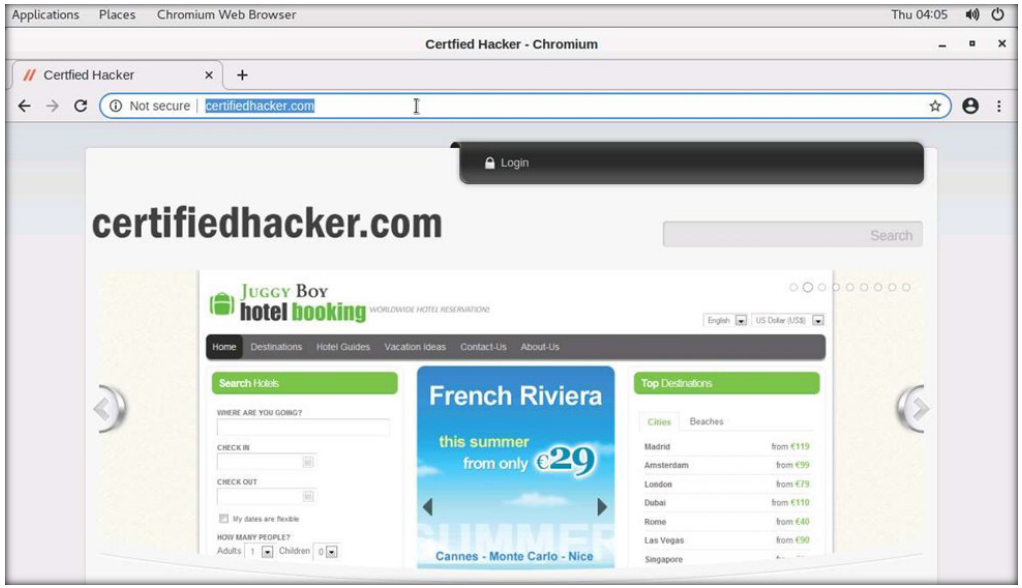
12. Press Ctrl + C to end the packet capture.
13. Type sudo tcpdump -i eth0 port 80 in the terminal and press Enter to capture packets from the specific port on the machine interface.
14. Navigate to Applications Internet and select Chromium Web Browser.

EXERCISE 3:
ANALYZE AND
EXAMINE VARIOUS
NETWORK PACKET
HEADERS IN LINUX
USING TCPDUMP



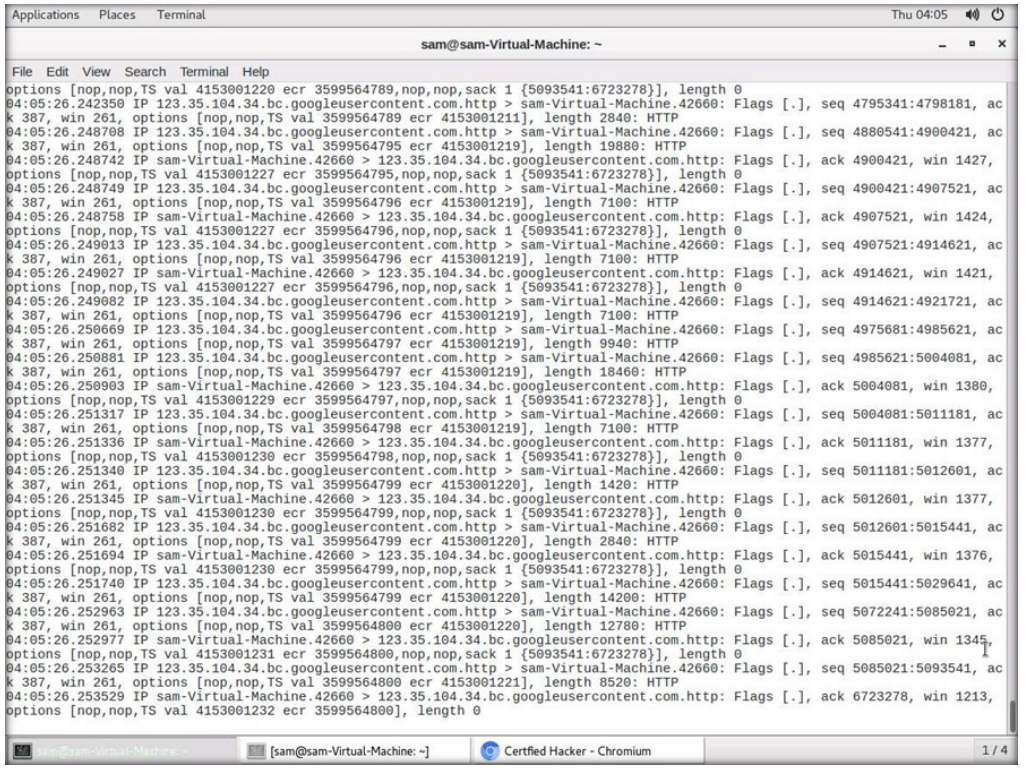
15. The Chromium Web Browser opens. Type http://www.certifiedhacker.com as url and press Enter.

EXERCISE 3:
ANALYZE AND
EXAMINE VARIOUS
NETWORK PACKET
HEADERS IN LINUX
USING TCPDUMP



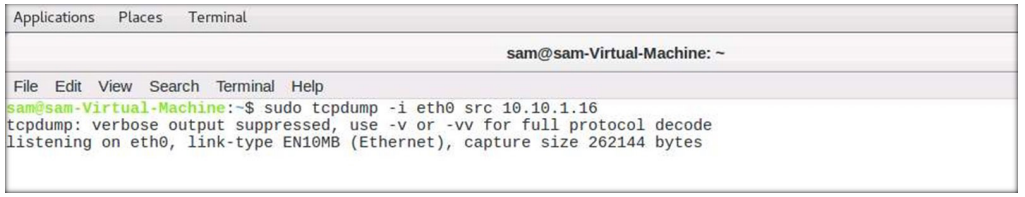
16. Switch back to the opened Terminal; you can observe that the tcpdump is capturing port 80 http traffic.

EXERCISE 3:
ANALYZE AND
EXAMINE VARIOUS
NETWORK PACKET
HEADERS IN LINUX
USING TCPDUMP



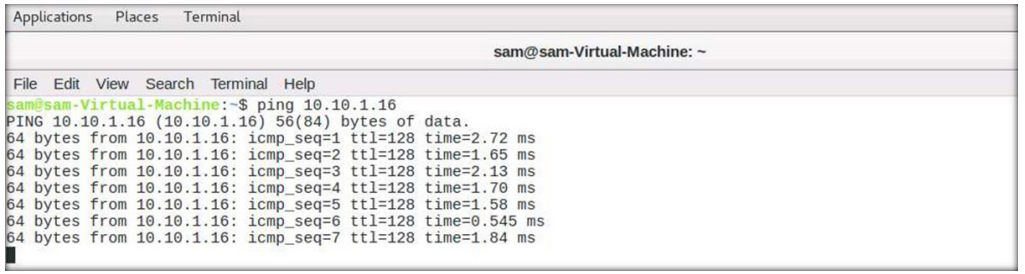
17. Press Ctrl + C to end the packet capture.
18. Now, capture packets from specific source and destination IP.
19. Type sudo tcpdump -i eth0 src 10.10.1.16 in the terminal and press Enter to capture packets from the specific source on the machine interface.

EXERCISE 3:
ANALYZE AND
EXAMINE VARIOUS
NETWORK PACKET
HEADERS IN LINUX
USING TCPDUMP



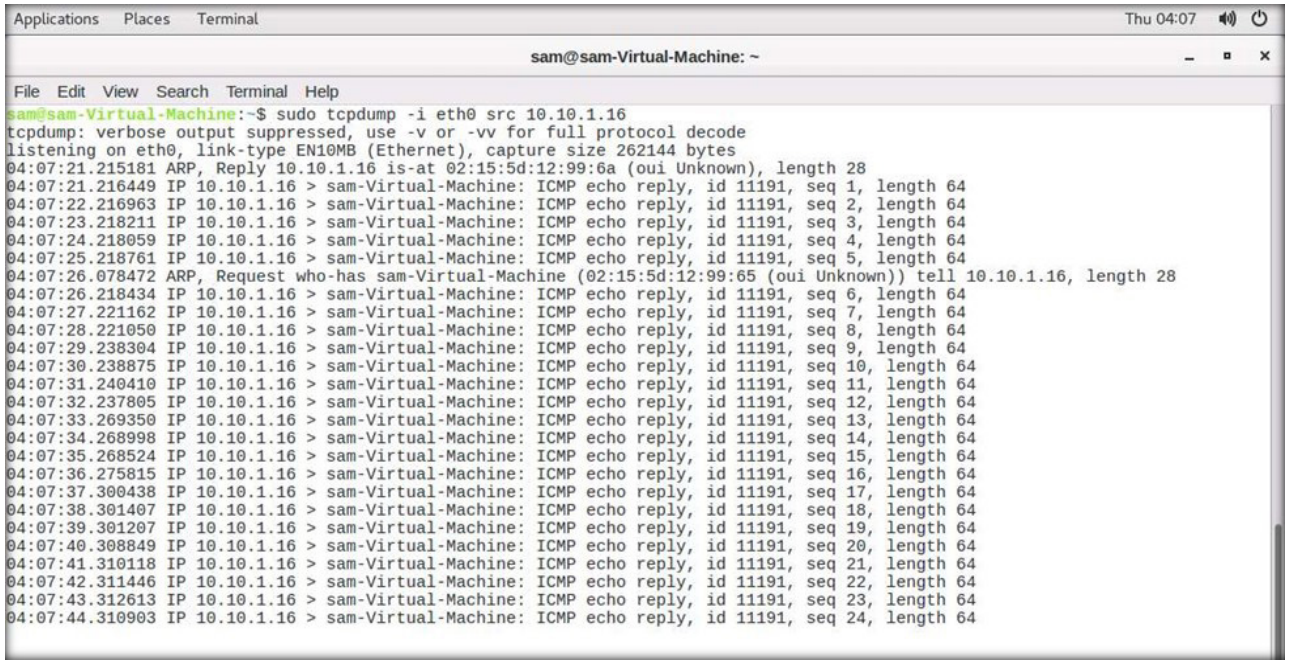
20. Open another Terminal and execute the command ping 10.10.1.16 to communicate with the machine. Leave the terminal open.

EXERCISE 3:
ANALYZE AND
EXAMINE VARIOUS
NETWORK PACKET
HEADERS IN LINUX
USING TCPDUMP



21. Switch back to the first Terminal and observe the captured ICMP packets.

EXERCISE 3:
ANALYZE AND
EXAMINE VARIOUS
NETWORK PACKET
HEADERS IN LINUX
USING TCPDUMP



22. Close the second Terminal and press Ctrl + C in first Terminal to stop the packet capturing.
23. A security professional can use the tcpdump to capture the traffic.
24. This concludes the demonstration showing how to analyze and examine various network packet headers using tcpdump.
25. Close all open windows.

EXERCISE 3:
ANALYZE AND
EXAMINE VARIOUS
NETWORK PACKET
HEADERS IN LINUX
USING TCPDUMP

EXERCISE 4: **SCAN NETWORK TO IDENTIFY HOSTS IN THE LOCAL NETWORK**

Network scanning is the process of gathering additional detailed information about the target by using highly complex and aggressive reconnaissance techniques.

LAB SCENARIO

A security professional must have the required knowledge to perform network scanning to identify active hosts in the entire network. Further, you must scan the machines for open ports and services running on them.

OBJECTIVE

This lab will demonstrate how to use Nmap to perform network scanning.

OVERVIEW NETWORK SCANNING

The purpose of scanning is to discover exploitable communication channels, probe as many listeners as possible, and keep track of the responsive ones.

Types of scanning:

- **Port scanning:** Lists open ports and services
- **Network scanning:** Lists the active hosts and IP addresses
- **Vulnerability scanning:** Shows the presence of known weaknesses

Note: Ensure that Admin Machine-2, Web Server and PfSense Firewall virtual machines are running.

1. Turn on, AD Domain Controller, Attacker Machine-1, Attacker Machine-2, Admin Machine-1, and Android Device virtual machines.
2. Switch to the Attacker Machine-2 virtual machine.
3. In the login page, the attacker username will be selected by default. Enter password as toor in the Password field and press Enter to log in to the machine.

Note: If a Parrot Updater pop-up appears at the top-right corner of Desktop, ignore and close it.

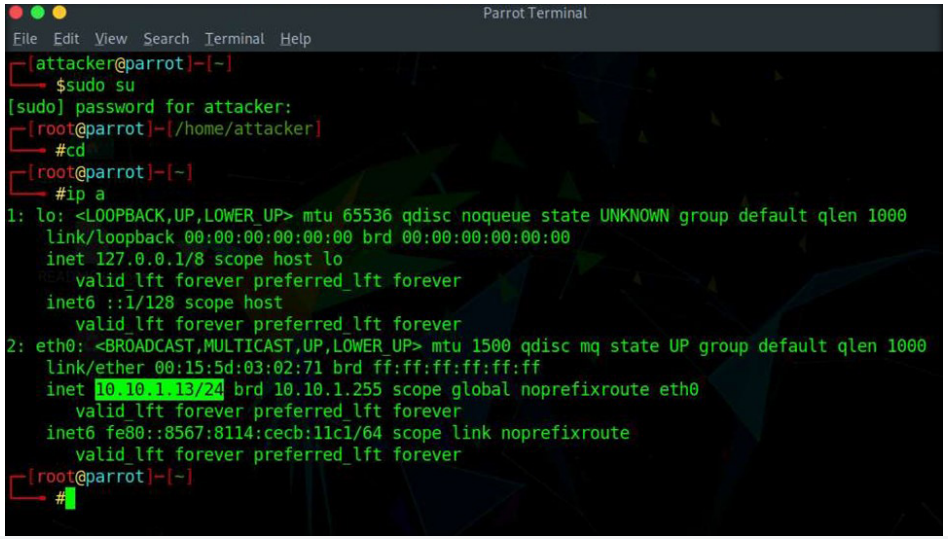
Note: If a Question pop-up window appears asking you to update the machine, click No to close the window.

4. Click the MATE Terminal icon at the top of the Desktop window to open a Terminal window.
5. A Parrot Terminal window appears. In the terminal window, type sudo su and press Enter to run the programs as a root user.
6. In the [sudo] password for attacker field, type toor as a password and press Enter.

Note: The password that you type will not be visible.

7. Now, type cd and press Enter to jump to the root directory.
8. In the Terminal window, type ip a and press Enter to display information related to network configuration.

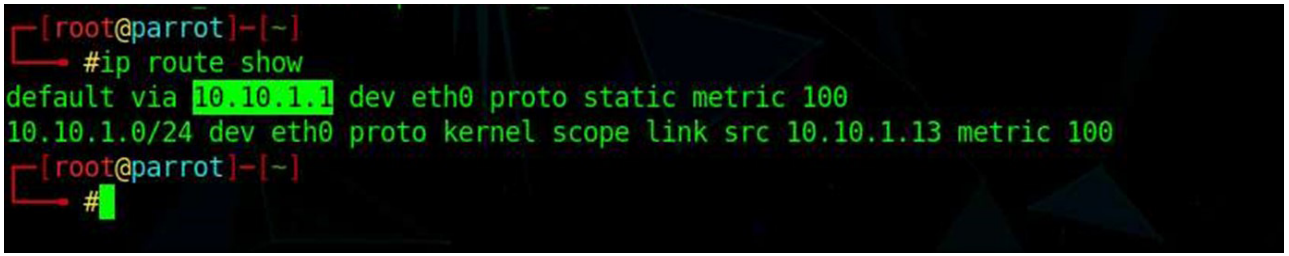
Note: Note down the IP address of the machine, here, 10.10.1.13.



9. Type ip route show and press Enter to display the IP address of the default gateway.

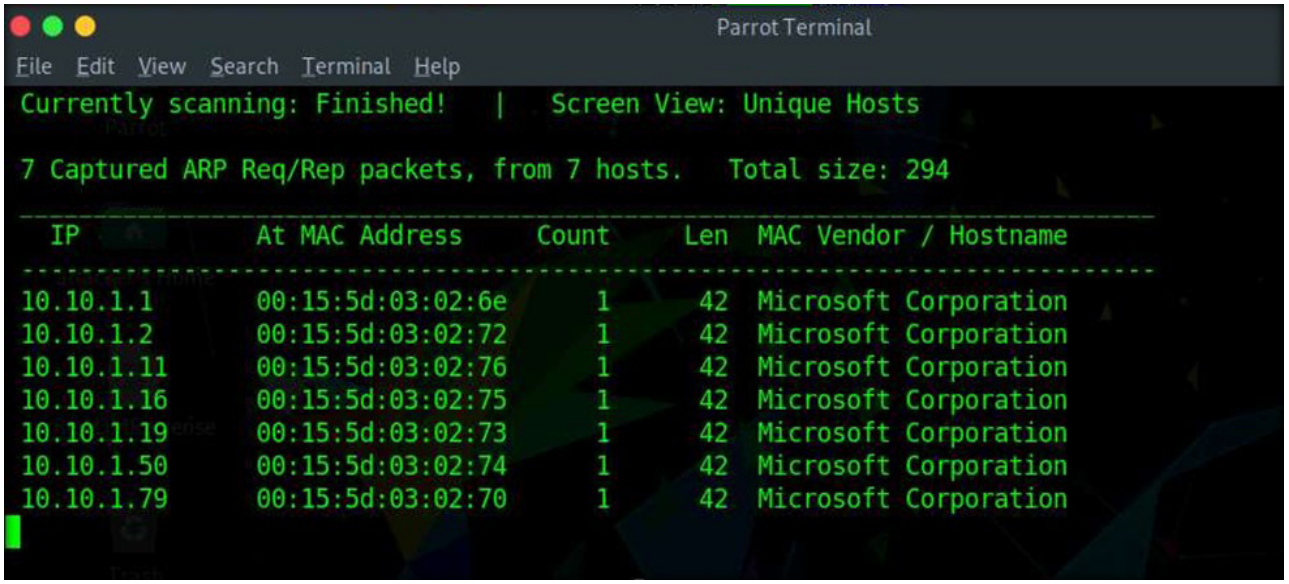
Note: Note down the IP address of the default gateway, here, 10.10.1.1.

EXERCISE 4: SCAN NETWORK TO IDENTIFY HOSTS IN THE LOCAL NETWORK



10. Now, type netdiscover -i eth0 -r 10.10.1.0/24 and press Enter to scan the local network and discover other hosts present in the network.
11. A total of 7 machines will be displayed with details such as MAC Address, Hostname, etc, as shown in the screenshot below.

EXERCISE 4: SCAN NETWORK TO IDENTIFY HOSTS IN THE LOCAL NETWORK

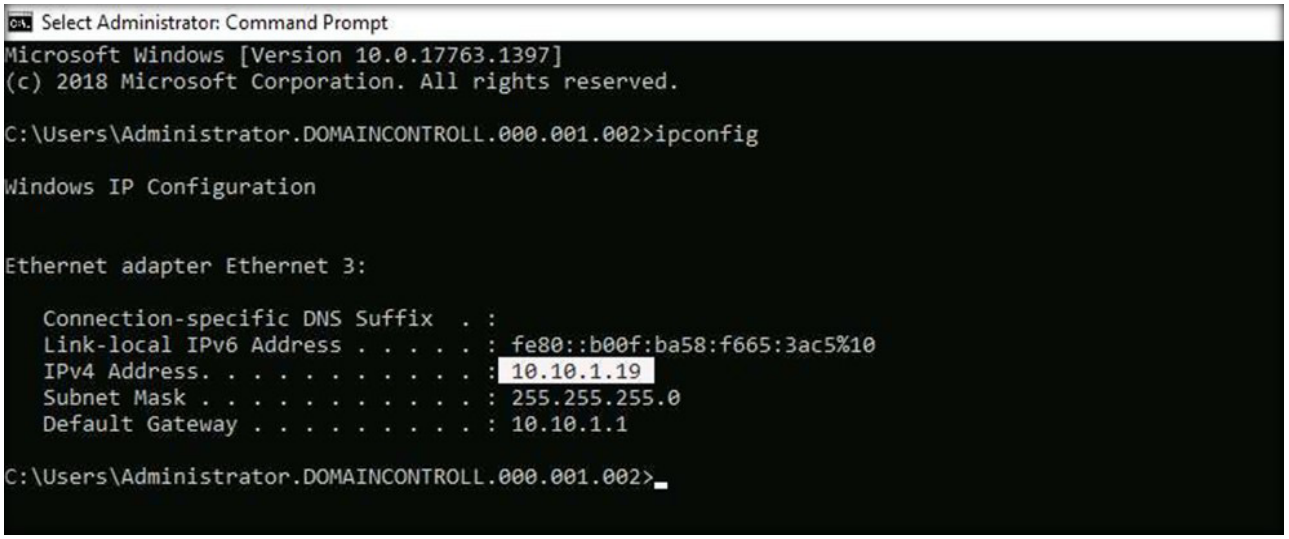


12. Press Ctrl+C to terminate the scan.
13. Switch to the AD Domain Controller virtual machine.
14. Log in with the credentials CCT\Administrator and admin@123.

Note: The network screen appears, click Yes.

15. Click Type here to search icon, type cmd and select Command Prompt from the results.
16. The Command Prompt window appears, type ipconfig and press Enter to display the details related to network configuration.

EXERCISE 4: SCAN NETWORK TO IDENTIFY HOSTS IN THE LOCAL NETWORK



17. Type pathping 10.10.1.13 and press Enter to check the connection between Attacker Machine-2 and AD Domain Controller machine.

Note: It takes a while for the scan to finish.

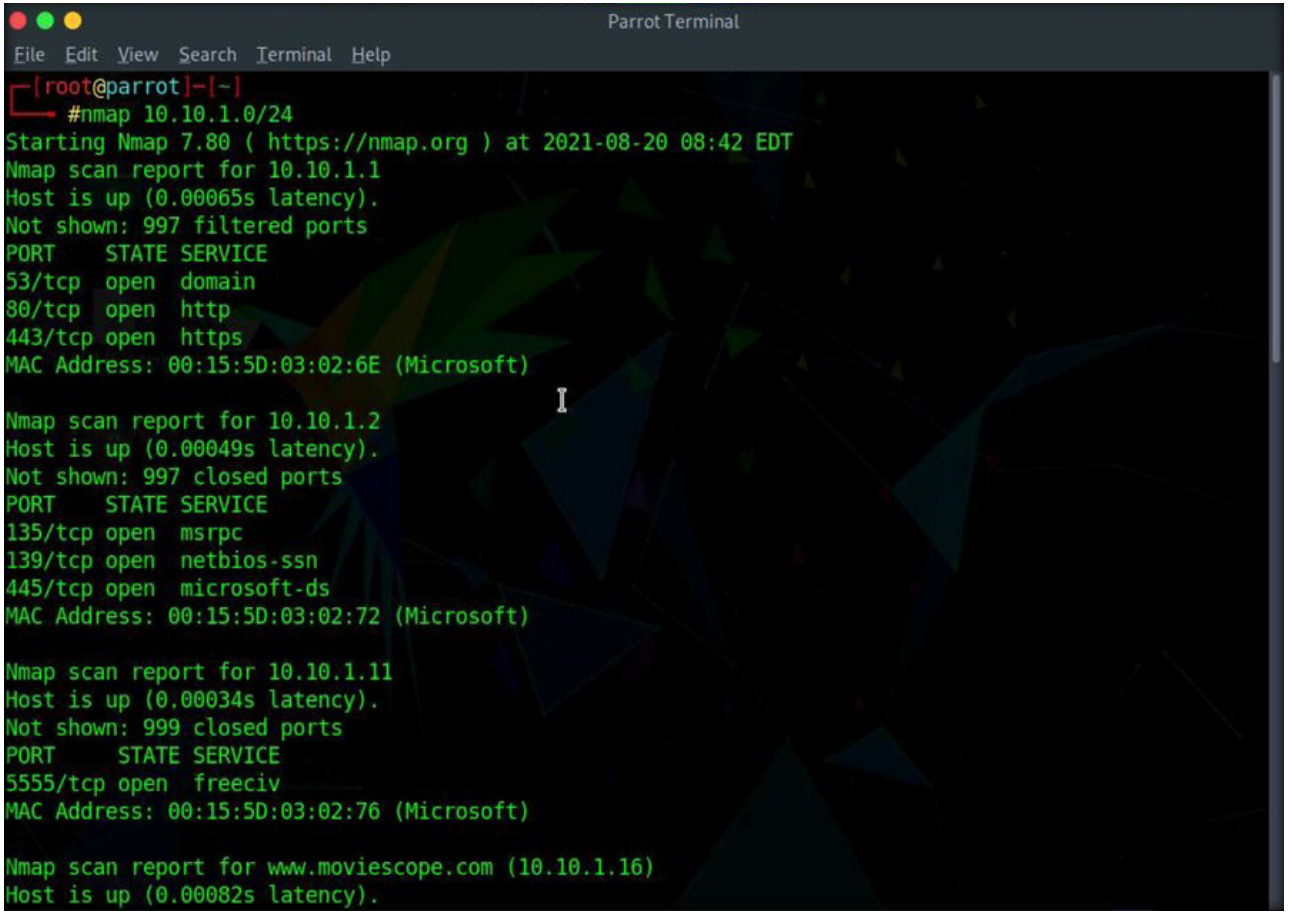
18. From the results, you can observe that Attacker Machine-2 machine is just 1 hop count away from the AD Domain Controller machine with packet lost count being 0 and success rate is 100, as shown in the screenshot below.

EXERCISE 4: SCAN NETWORK TO IDENTIFY HOSTS IN THE LOCAL NETWORK

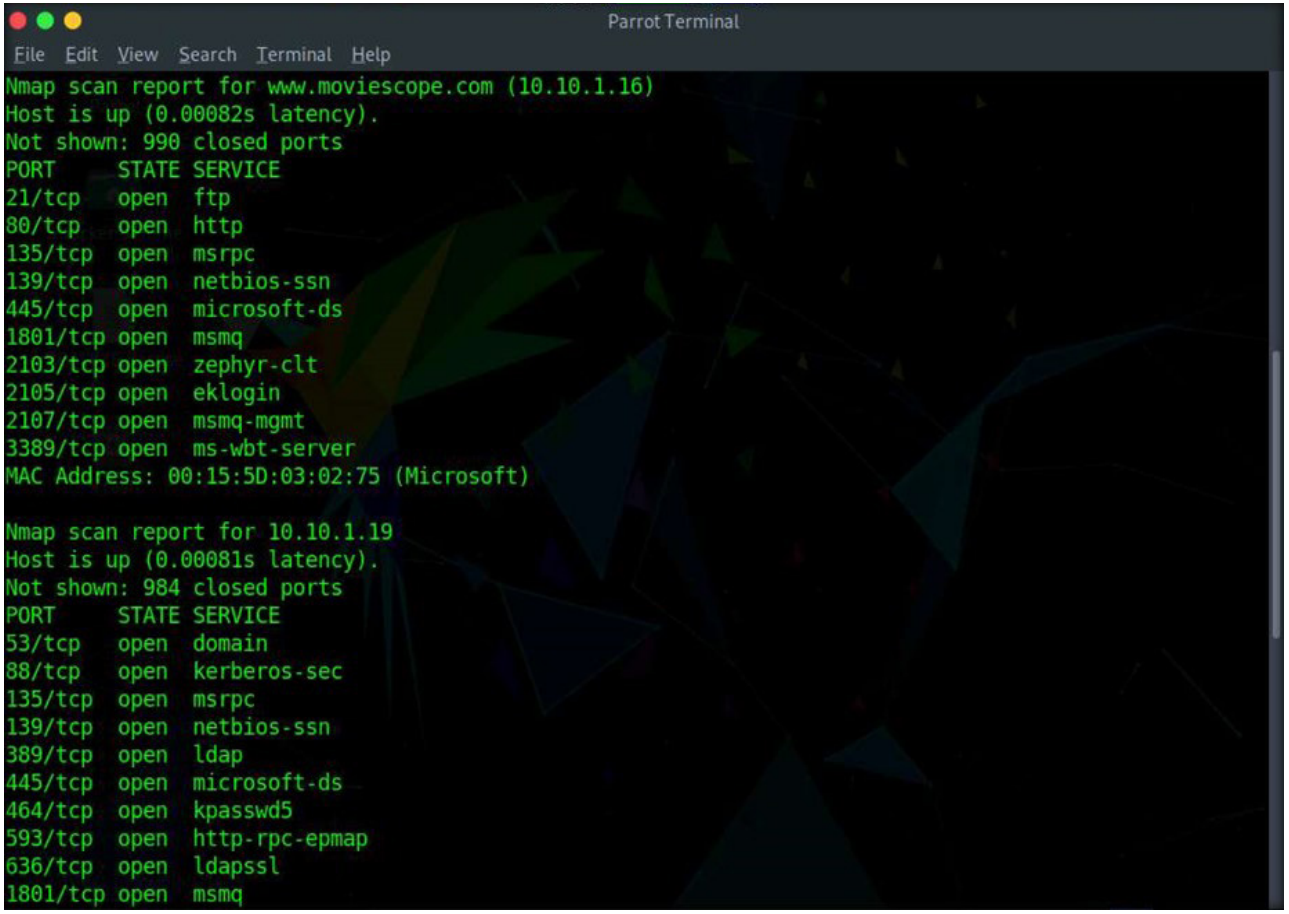
```
C:\Users\Administrator.DOMAINCONTROLL.000.001.002>pathping 10.10.1.13

Tracing route to 10.10.1.13 over a maximum of 30 hops

  0  DomainControll.CCT.com [10.10.1.19]
  1  10.10.1.13

Computing statistics for 25 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           DomainControll.CCT.com [10.10.1.19]
                                    0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%     0/ 100 =  0%  10.10.1.13

Trace complete.

C:\Users\Administrator.DOMAINCONTROLL.000.001.002>
C:\Users\Administrator.DOMAINCONTROLL.000.001.002>
```

19. Now, we will use Nmap to discover hosts in the local network.
20. Switch back to the Attacker Machine-2 virtual machine.
21. In the terminal window, type nmap 10.10.1.0/24 and press Enter to run a basic scan to discover the hosts in the local network.
22. A result appears displaying hosts in the network along with their open ports and service running services, as shown in the screenshot below.

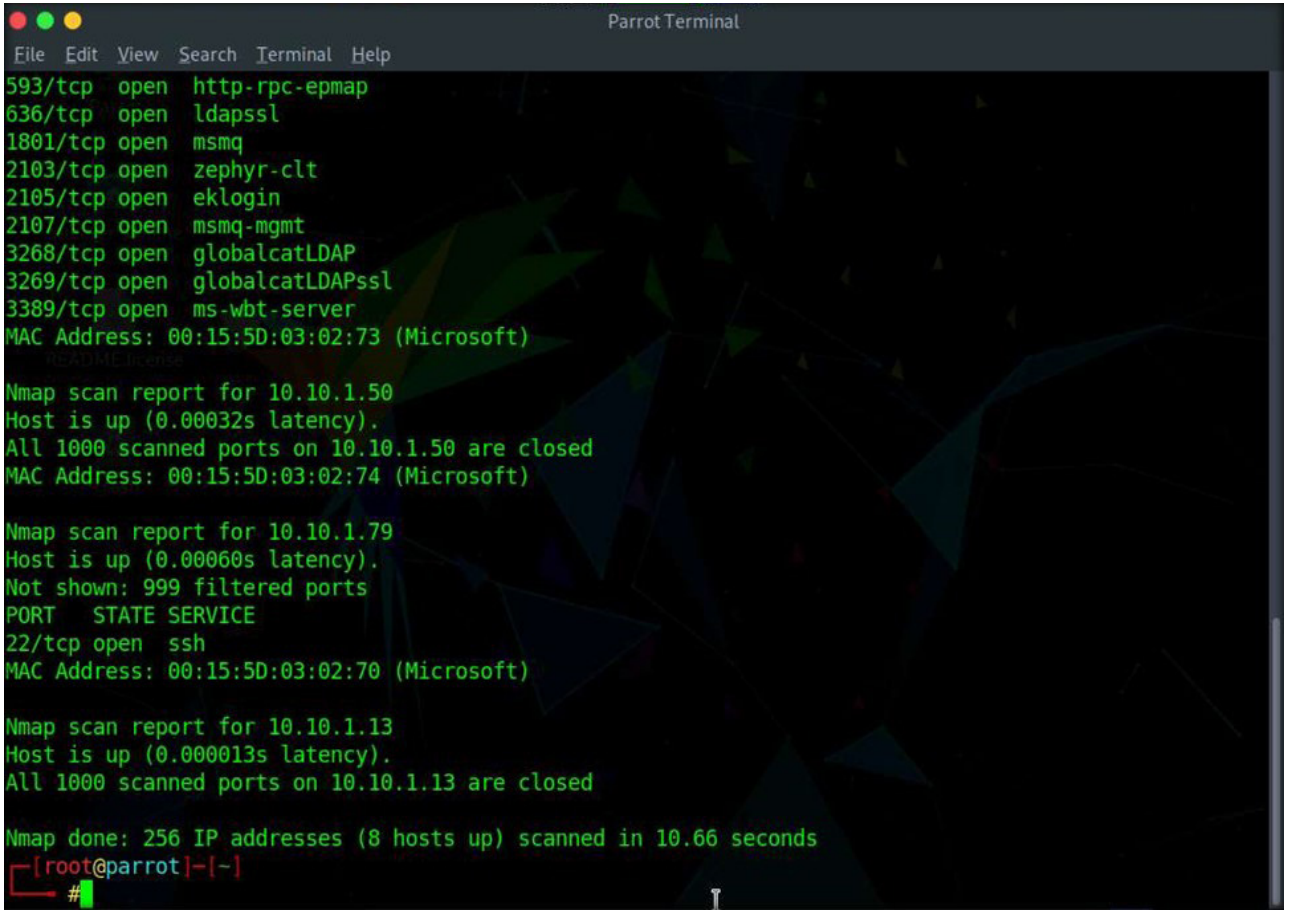
EXERCISE 4: SCAN NETWORK TO IDENTIFY HOSTS IN THE LOCAL NETWORK



EXERCISE 4: SCAN NETWORK TO IDENTIFY HOSTS IN THE LOCAL NETWORK



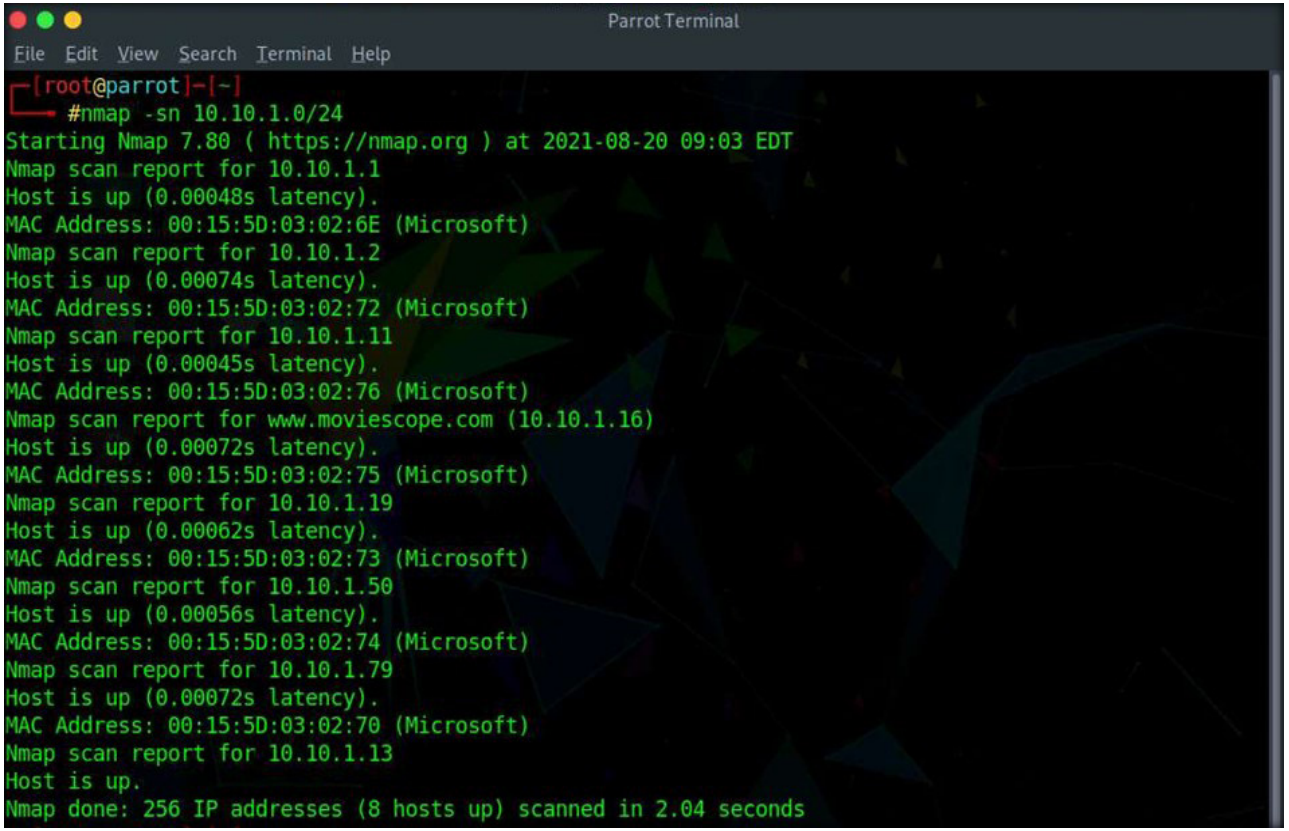
EXERCISE 4: SCAN NETWORK TO IDENTIFY HOSTS IN THE LOCAL NETWORK



23. Type nmap -sn 10.10.1.0/24 and press Enter to scan for active machines in the network.
24. A result appears displaying active hosts in the entire network, as shown in the screenshot below.

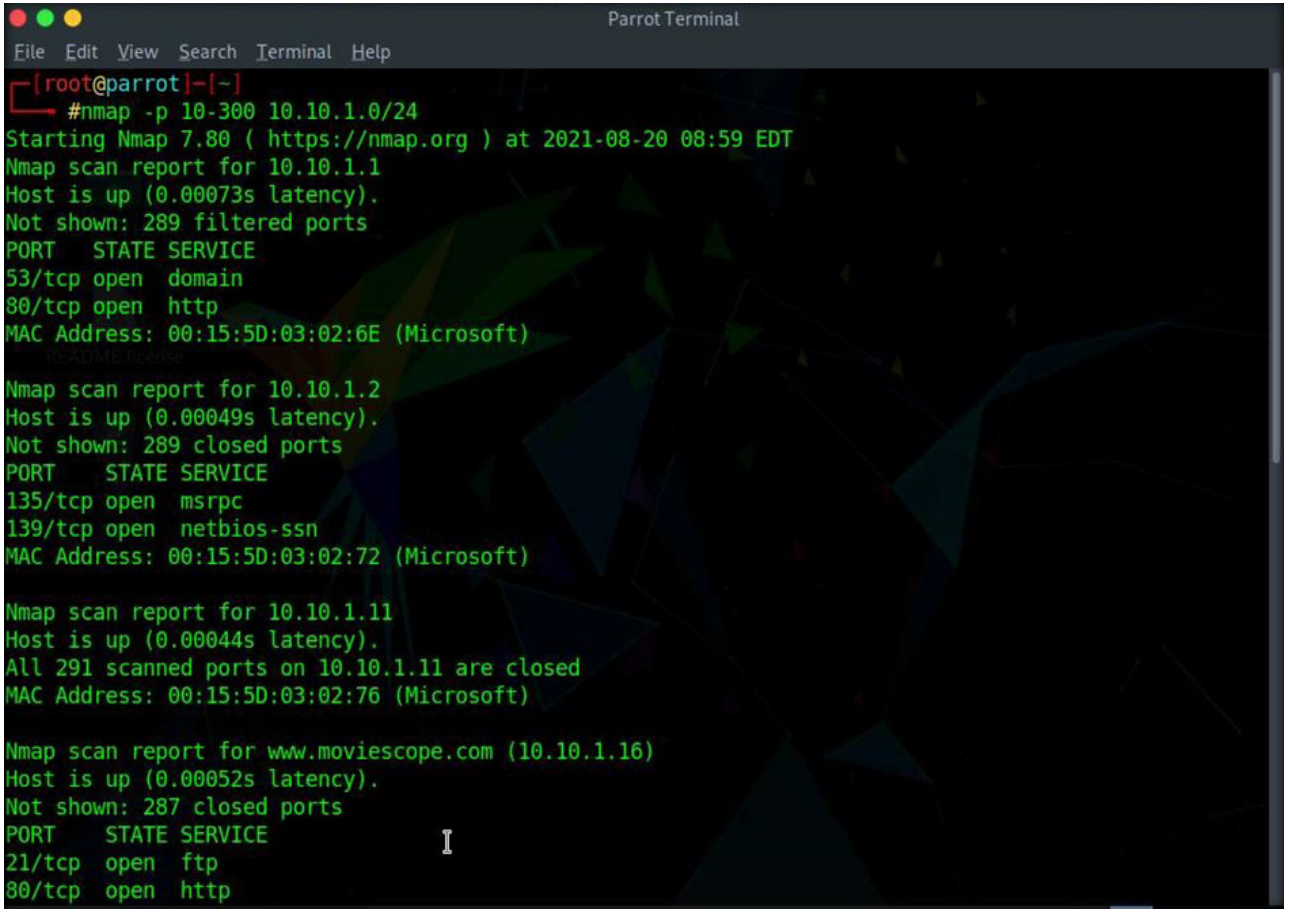
Note: It takes a while for the results to display.

EXERCISE 4: SCAN NETWORK TO IDENTIFY HOSTS IN THE LOCAL NETWORK



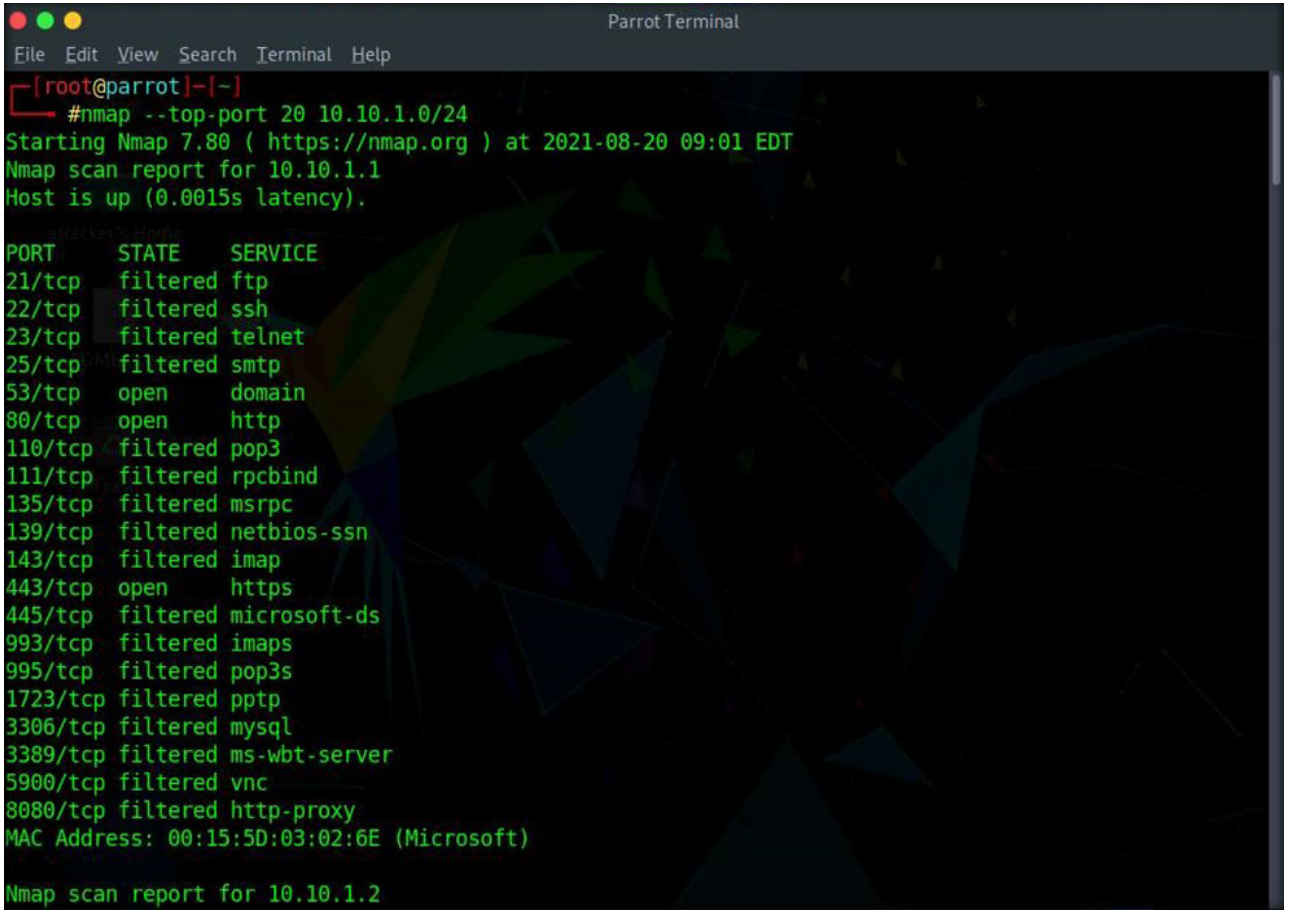
25. Type nmap -p 10-300 10.10.1.0/24 and press Enter to scan the range of ports (10-300) in the entire network.
26. A result appears displaying different machines with open ports along with the services running on them.

EXERCISE 4:
SCAN NETWORK
TO IDENTIFY HOSTS
IN THE LOCAL
NETWORK

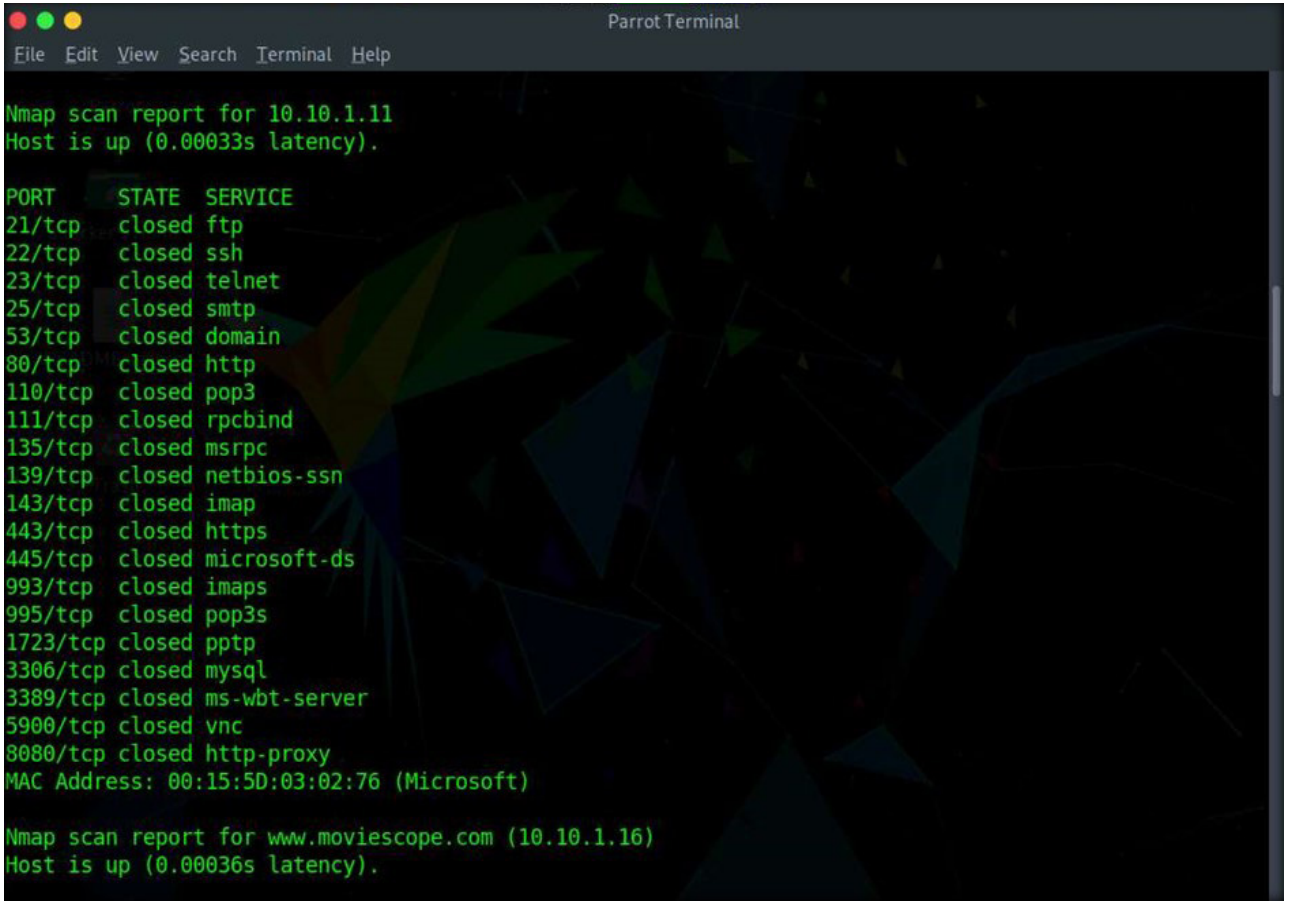


27. Type nmap --top-port 20 10.10.1.0/24 and press Enter to scan for the twenty most common ports.
28. A result appears displaying different top 20 ports along with status as open/close/filtered, as shown in the screenshot below.

EXERCISE 4: SCAN NETWORK TO IDENTIFY HOSTS IN THE LOCAL NETWORK



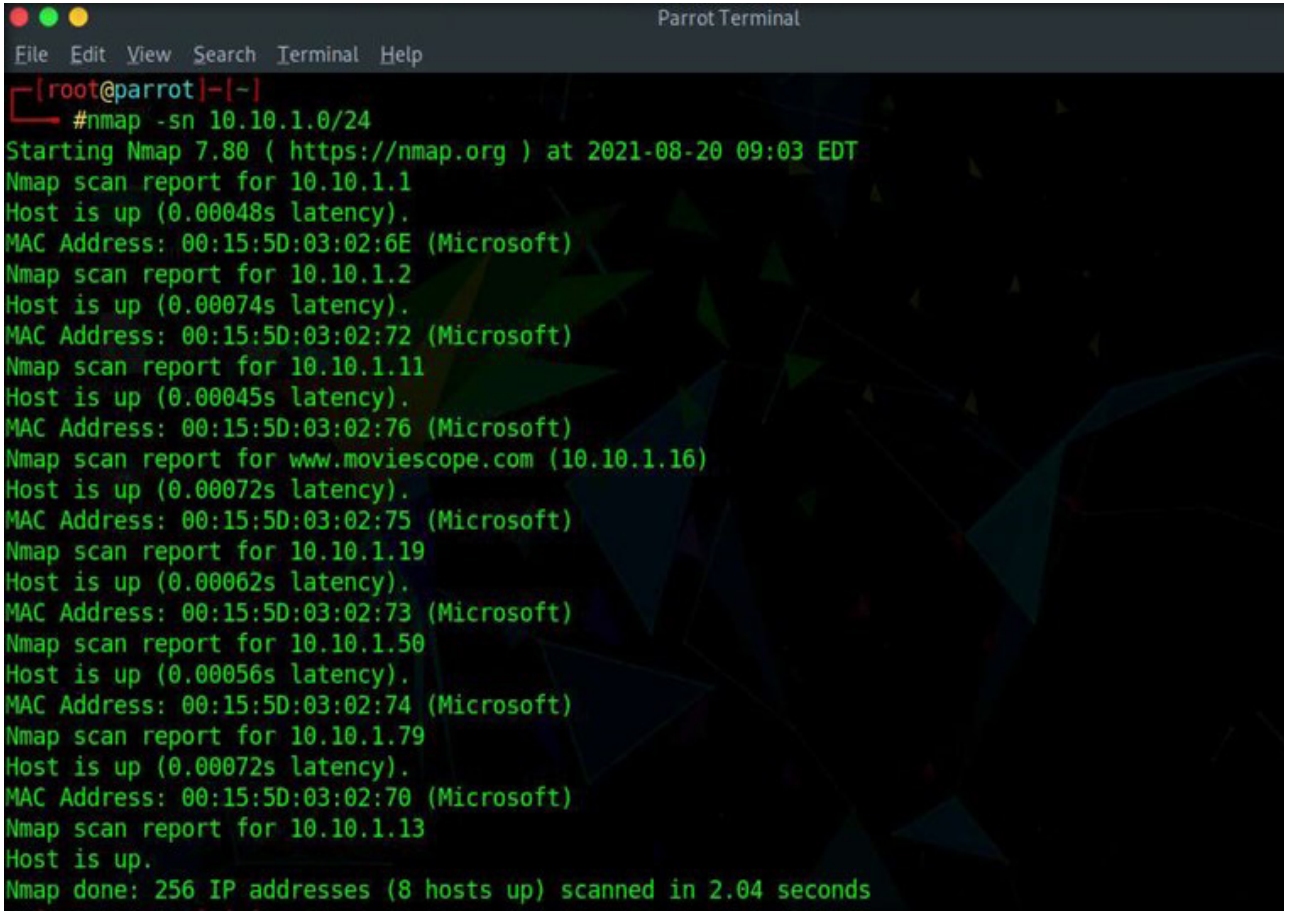
EXERCISE 4: SCAN NETWORK TO IDENTIFY HOSTS IN THE LOCAL NETWORK



29. Type nmap -sn 10.10.1.0/24 and press Enter to scan for the active machines in the network.
30. A result appears displaying active hosts in the entire network, as shown in the screenshot below.

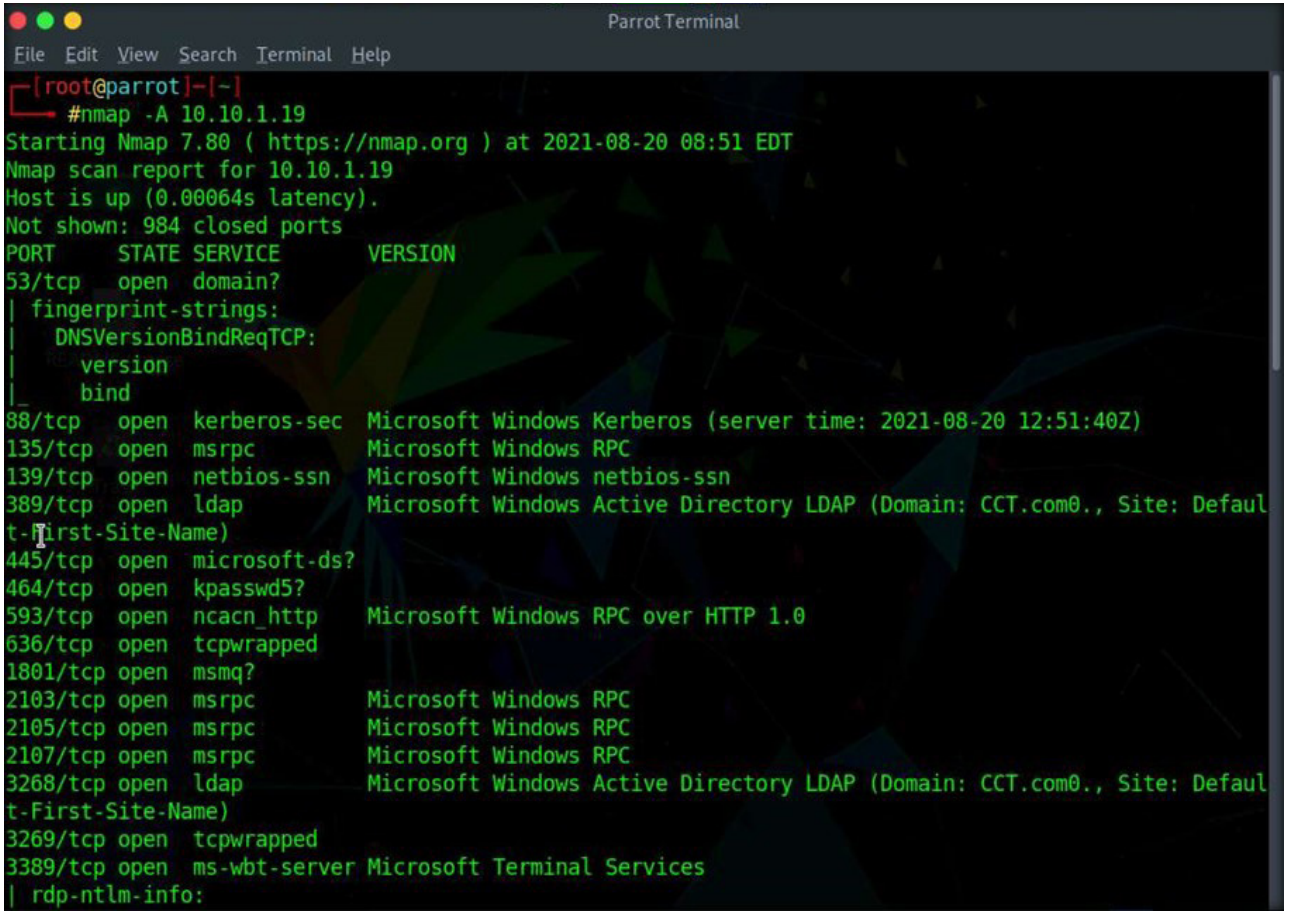
Note: It takes a while for the results to display.

EXERCISE 4: SCAN NETWORK TO IDENTIFY HOSTS IN THE LOCAL NETWORK



31. Now, we will perform a detailed scan on one host (here, AD Domain Controller machine (10.10.1.19)), to do so, type nmap -A 10.10.1.19 and press Enter.
32. Nmap scans the target machine and displays information such as open ports and services, device type, details of OS, etc., as shown in the screenshot below.

EXERCISE 4: SCAN NETWORK TO IDENTIFY HOSTS IN THE LOCAL NETWORK

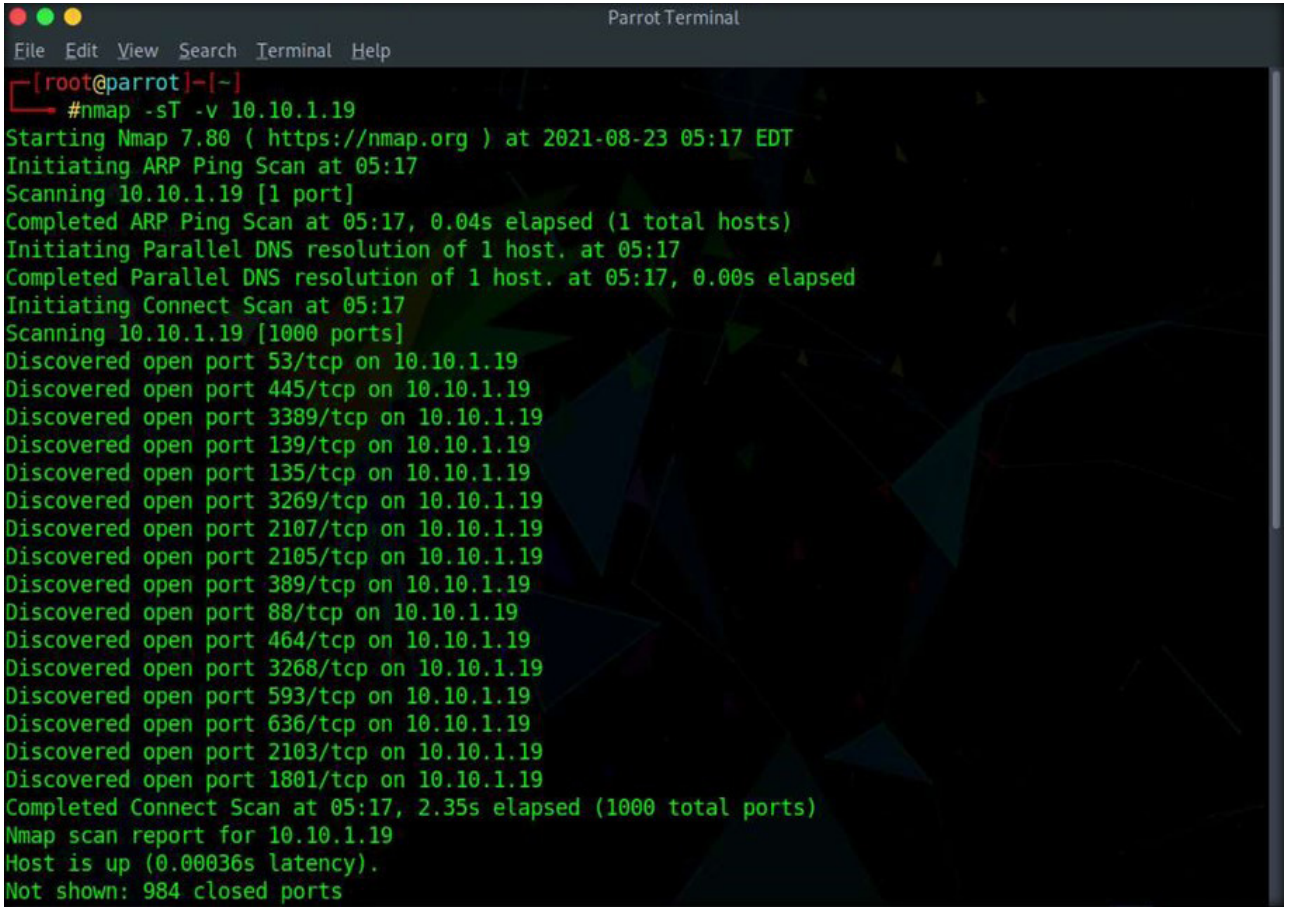


33. In the terminal window, type nmap -sT -v 10.10.1.19 and press Enter.

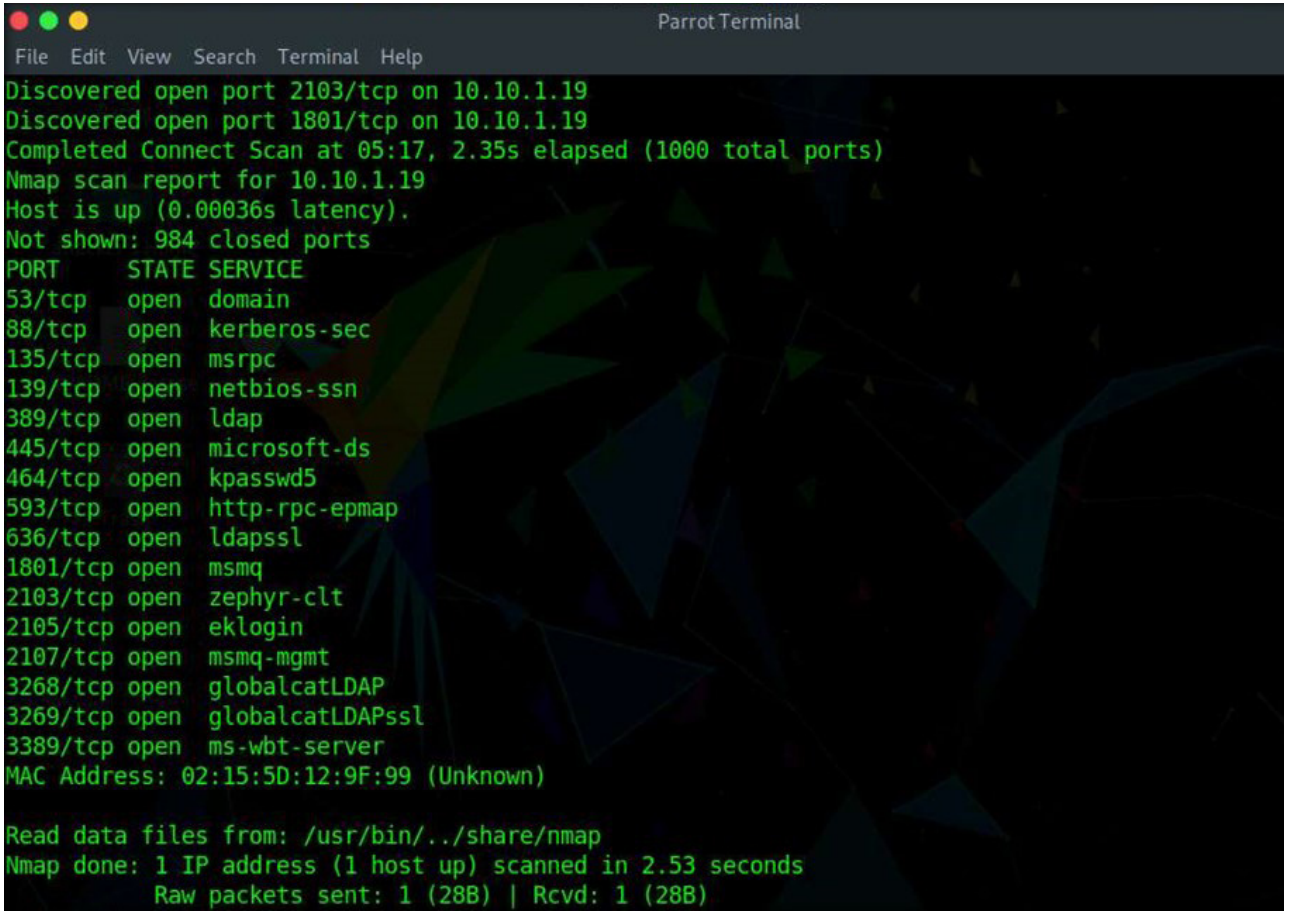
Note: -sT: performs the TCP connect/full open scan and -v: enables the verbose output (include all hosts and ports in the output).

34. The scan results appear, displaying all the open TCP ports and services running on the target machine, as shown in the screenshot below.

EXERCISE 4: SCAN NETWORK TO IDENTIFY HOSTS IN THE LOCAL NETWORK



EXERCISE 4: SCAN NETWORK TO IDENTIFY HOSTS IN THE LOCAL NETWORK



35. This concludes the demonstration showing how to perform network scan using Nmap.
36. Close all open windows.
37. Turn off all the running virtual machines.

EXERCISE 4:
SCAN NETWORK
TO IDENTIFY HOSTS
IN THE LOCAL
NETWORK


EC-Council