INT303: Networking Fundamentals – Lab 1

Lab 1: Understanding Network Layers and TCP/IP Model using OWASP Broken Web Application IP

Objective:

In this lab, you will explore the OSI and TCP/IP models using the IP address of the OWASP Broken Web Application virtual machine. This practical exercise will help you understand how data is transmitted across networks, the key protocols involved, and how to use essential network commands for troubleshooting and analysis.

Lab Exercises:

Exercise 1: Understanding OSI and TCP/IP Models

Task: Review the OSI and TCP/IP models and their layers.

OSI Layers: Physical, Data Link, Network, Transport, Session, Presentation, Application

TCP/IP Layers: Link, Internet, Transport, Application

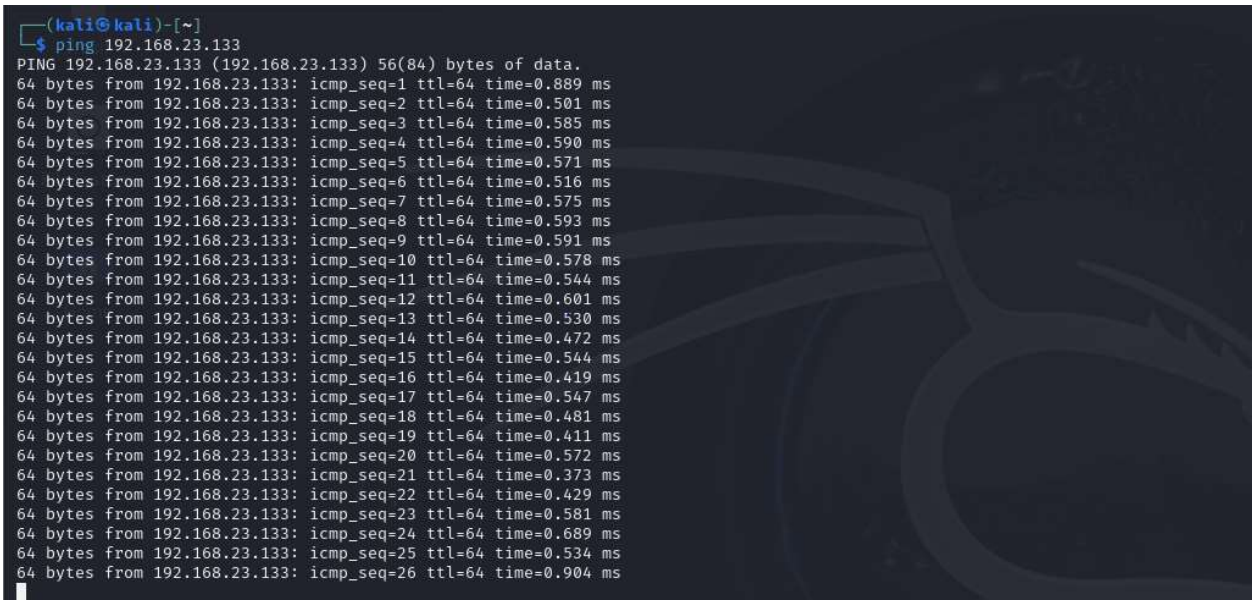
Question:

List the OSI model layers and describe the function of each. Match each OSI layer with its corresponding TCP/IP layer.

Exercise 2: Pinging the OWASP Broken Web Application

Task: Use the ping command to check the reachability of the OWASP Broken Web Application using its IP address.

Command: ping <OWASP_IP> (replace <OWASP_IP> with the actual IP, e.g., ping 192.168.56.101)

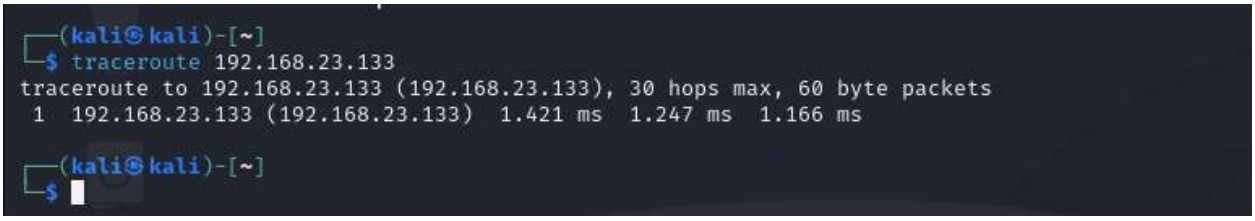


- OSI Layer: The ping command operates at the Network Layer (Layer 3) of the OSI model.
  Process:
- OWASP IP was collected,
- Ping 192.168.23.133 command was run on kali Linux terminal

Exercise 3: Tracing the Path to the OWASP Application

Task: Use the traceroute command to trace the route packets take to reach the OWASP Broken Web Application.

Command: traceroute <OWASP_IP> (e.g., traceroute 192.168.56.101)



- It takes 30 hops maximum to reach the OWASP VM
- Each hop represents a network device along the path, and the round-trip times provide insights into the latency experienced at each hop.

Exercise 4: Viewing Active Connections to OWASP VM

Task: Use netstat to view active network connections between your system and the OWASP application.

Command: netstat -an | grep <OWASP_IP>

Question: What connections do you see? Identify the source and destination IP addresses. Explain how the Transport Layer (TCP/UDP) is involved in this communication.

Exercise 5: TCP vs. UDP

Task: Investigate the difference between TCP and UDP by scanning the OWASP Broken Web Application. Run a TCP scan using nmap.

Command: nmap -sT <OWASP_IP>

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.23.133
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-28 19:43 EST
Nmap scan report for 192.168.23.133
Host is up (0.0031s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
5001/tcp open  commplex-link
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
```

Run a UDP scan.

Command: nmap -sU <OWASP_IP>

```
┌──(root㉿kali)-[~]
└─# nmap -sU 192.168.23.133
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-28 20:01 EST
Stats: 0:10:42 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 64.18% done; ETC: 20:17 (0:05:58 remaining)
Stats: 0:10:43 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 64.28% done; ETC: 20:17 (0:05:57 remaining)
Stats: 0:10:49 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 64.88% done; ETC: 20:17 (0:05:51 remaining)
Stats: 0:10:50 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 64.98% done; ETC: 20:17 (0:05:50 remaining)
Nmap scan report for 192.168.23.133
Host is up (0.0011s latency).
Not shown: 997 closed udp ports (port-unreach)
PORT      STATE         SERVICE
68/udp    open|filtered dhcpc
137/udp   open          netbios-ns
18250/udp open|filtered unknown
MAC Address: 00:0C:29:83:79:69 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1026.93 seconds
```

Question:

What are the key differences between TCP and UDP in terms of reliability and speed?

ANSWER: Using TCP scan is faster within 13.34 seconds while UDP scan is slow in speed and responses within 1026.93 seconds.

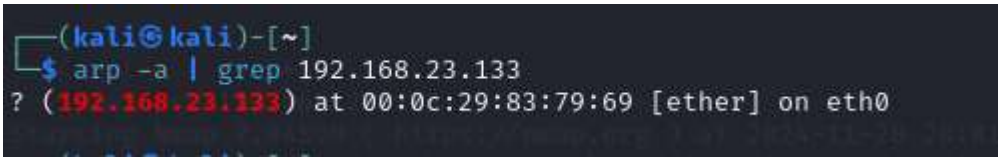
Based on the scan results, list which services on the OWASP application are using TCP and which are using UDP.

TCP SERVICE	**UDP SERVICE**
Ssh	dhcpc
http	Netbios-ns

Netbios-ssn	unknown
Imap	
https	
Microsoft-ds	
Complex-link	
http-proxy	
Blackice-icecap	

Exercise 6: Discovering MAC Addresses with ARP

Task: Use the arp command to view the MAC address of the OWASP Broken Web Application. Command: arp -a | grep <OWASP_IP>



Question:

What is the MAC address associated with the OWASP VM's IP**?**

ANSWER: OWAPS MAC ADD. **00:0c:29:83:79:69**

Explain the significance of ARP in the Data Link Layer and how it contributes to successful communication.

ANSWER:

The Significance of ARP in the Data Link Layer

Address Resolution Protocol (ARP) is a crucial protocol operating within the Data Link Layer of the OSI model. Its primary function is to map logical IP addresses to physical MAC addresses, enabling devices on a network to communicate effectively.

How ARP Works

1. **IP Address to MAC Address Mapping:**
    - When a device wants to send a packet to another device on the same network, it knows the destination's IP address.
    - However, to transmit the packet at the Data Link Layer, it needs the destination's MAC address.
    - ARP is responsible for this translation.
2. **ARP Request:**

    - The sending device broadcasts an ARP request to all devices on the network, asking for the MAC address associated with the destination IP address.

3. **ARP Reply:**
    - The device with the matching IP address receives the request and sends an ARP reply containing its MAC address.

4. **Caching:**
    - The sending device caches the IP-to-MAC address mapping for future reference, reducing the need for repeated ARP requests.

Significance of ARP in Communication

- **Enables Local Network Communication:** ARP ensures that devices on the same network can communicate directly, without relying on routers.
- **Facilitates Packet Forwarding:** Routers use ARP to determine the appropriate interface to forward packets to the next network hop.
- **Supports Network Troubleshooting:** Network administrators can use ARP to diagnose connectivity issues and identify devices on the network.

In Conclusion

ARP plays a vital role in the functioning of local networks. By providing the necessary mapping between logical and physical addresses, it enables seamless communication between devices. A deep understanding of ARP is essential for network engineers and administrators to troubleshoot network problems and optimize network performance.

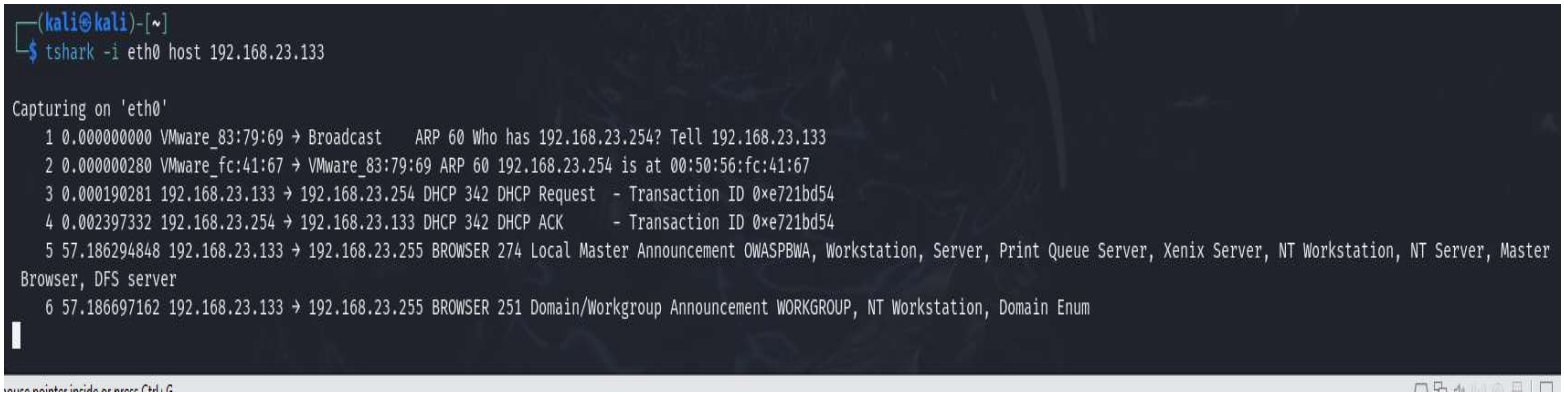
References:

- **Wikipedia:** https://en.wikipedia.org/wiki/Address_Resolution_Protocol
- **GeeksforGeeks:** https://www.geeksforgeeks.org/how-address-resolution-protocol-arp-works/
- **EITCA Academy:** https://eitca.org/cybersecurity/eitc-is-cnf-computer-networking-fundamentals/address-resolution-protocol/introduction-to-arp/examination-review-introduction-to-arp/what-is-the-role-of-arp-in-computer-networking-and-why-is-it-essential-for-communication-between-hosts-on-a-network/

Exercise 7: Capturing Network Traffic with Wireshark

Task: Use Wireshark or tshark to capture network packets between your machine and the OWASP Broken Web Application.

Command: wireshark (to launch the GUI) or tshark -i <interface> host <OWASP_IP>



Question:

Analyze the captured traffic. What protocols are in use?

ANSWER: ARP AND DCHP

INT303: Networking Fundamentals – Lab 2

Lab 2: Exploring Network Interfaces and Packet Transmission Using OWASP Broken Web Application IP

Objective:

In this lab, you will dive deeper into the concept of network interfaces and packet transmission by analyzing the network interface configuration on your system. You will explore how to capture and analyze network packets using various tools and understand the process of packet transmission to and from the OWASP Broken Web Application VM.

Learning Outcomes:

By the end of this lab, students will:

- Understand the role and configuration of network interfaces.
- Use packet capture tools to analyze network traffic and understand how data is

transmitted.

- Gain experience in monitoring and troubleshooting network interfaces and traffic. Materials Needed:
- Linux-based system (Kali, Ubuntu, etc.)
- OWASP Broken Web Application VM (running and reachable on your network)
- IP address of the OWASP Broken Web Application (e.g., 192.168.X.X)
- Wireshark or tshark for packet capture

Lab Exercises:

Exercise 1: Viewing and Configuring Network Interfaces

Task: View your network interfaces using the ifconfig or ip command.

Command: ifconfig or ip addr show

```
┌──(kali㉿kali)-[~]
└─$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:7e:be:78 brd ff:ff:ff:ff:ff:ff
    inet 192.168.23.134/24 brd 192.168.23.255 scope global dynamic noprefixroute eth0
       valid_lft 1285sec preferred_lft 1285sec
    inet6 fe80::5f8:a763:25d6:a1b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Question:

What network interfaces are available on your system?

ANSWER:

Interface 1: lo

- **Type:** Loopback interface
- **IP Address:** 127.0.0.1/8
- **Purpose:** Used for local communication and testing.

Interface 2: eth0

- **Type:** Ethernet interface
- **IP Address:** 192.168.23.134/24
- **Purpose:** Used for communication with other devices on the same network (192.168.23.0/24).

In addition to the IPv4 addresses, both interfaces also have IPv6 addresses:

- **Interface 1 (lo):** ::1/128
- **Interface 2 (eth0):** fe80::5f8:a763:25d6:a1b/64
- **Purpose:** These IPv6 addresses are used for local communication and are not typically used for internet connectivity.

Describe the difference between a loopback interface and an external network interface.

ANSWER:

Here's a breakdown of the key differences between a loopback interface and an external network interface, along with references to support the information:

Loopback Interface

- **Purpose:** Primarily used for local communication within a device.
- **IP Address:** 127.0.0.1 (IPv4) or ::1 (IPv6)
- **Physical Connection:** Doesn't require a physical network connection.
- **Security:** Highly secure as it's isolated from external networks.
- **Reliability:** Always available and unaffected by network outages.
- **Common Uses:**
    - Testing network configurations
    - Running local services and applications
    - Identifying a device's hostname or IP address

External Network Interface

- **Purpose:** Used for communication with other devices on a network.
- **IP Address:** Assigned dynamically (DHCP) or statically configured.
- **Physical Connection:** Requires a physical network connection (e.g., Ethernet cable, Wi-Fi).
- **Security:** Can be vulnerable to external threats if not properly configured.
- **Reliability:** Depends on the physical connection and network infrastructure.
- **Common Uses:**
    - Accessing the internet
    - Connecting to other devices on a local network
    - Remote access to the device

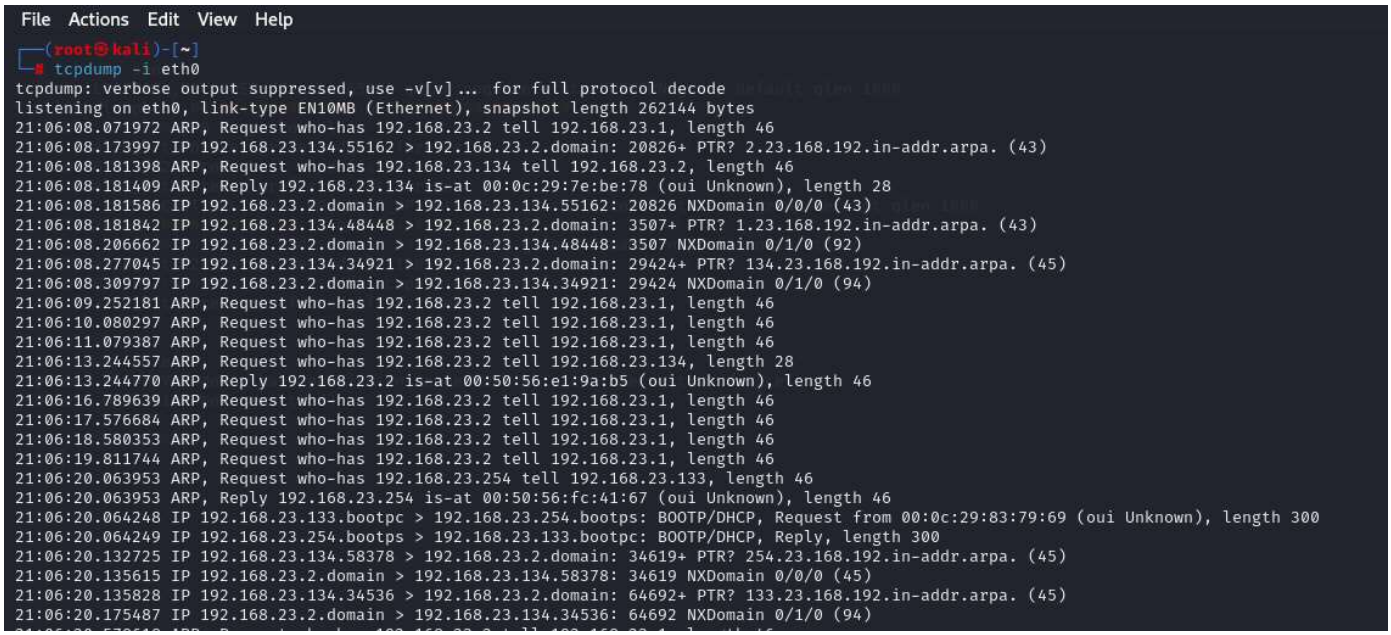
References:

- **GeeksforGeeks:**
    - Loopback Address: https://www.geeksforgeeks.org/local-broadcast-and-loopback-address/
- **Hostwinds:**
    - What is a Loopback Address?: https://www.geeksforgeeks.org/what-is-a-loopback-address/

Exercise 2: Capturing Packets on a Specific Interface

Task: Use tcpdump or tshark to capture packets on your primary network interface.

Command: tcpdump -i <interface> (e.g., tcpdump -i eth0) or tshark -i <interface>

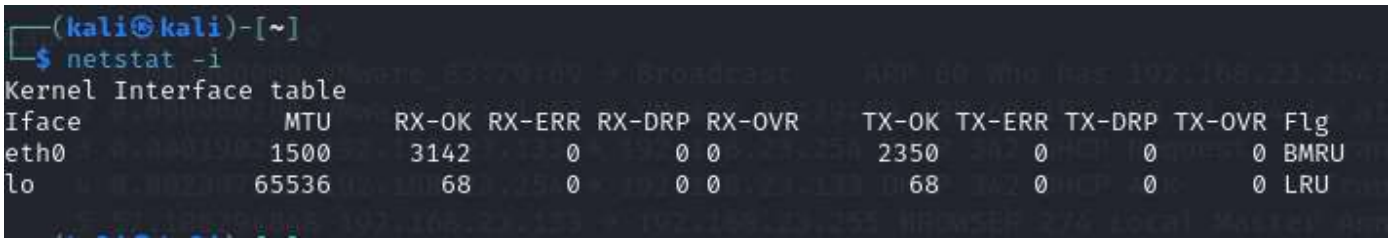


Question: What kind of packets are being captured? Are there any packets related to communication with the OWASP Broken Web Application VM? Describe the role of this network interface in transmitting and receiving packets.

Exercise 3: Examining Network Statistics

Task: Use the netstat or ss command to view current network statistics and connections.

Command: netstat -i or ss -s



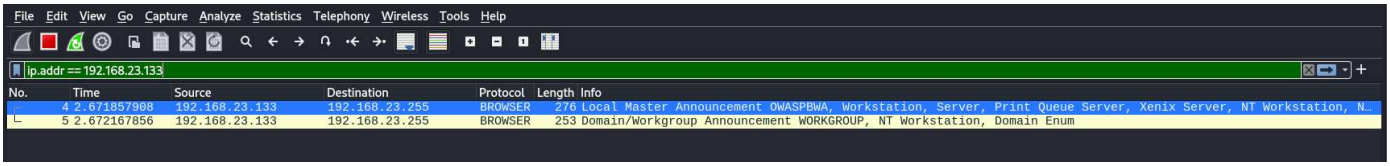
```
┌──(kali㉿kali)-[~]
└─$ ss -s
Total: 507
TCP:   0 (estab 0, closed 0, orphaned 0, timewait 0)

Transport Total     IP        IPv6
RAW       1         0         1
UDP       1         1         0
TCP       0         0         0
INET      2         1         1
FRAG      0         0         0
```

Question: What is the current status of your network interfaces? What active connections are visible? Explain the significance of these statistics in monitoring network performance.

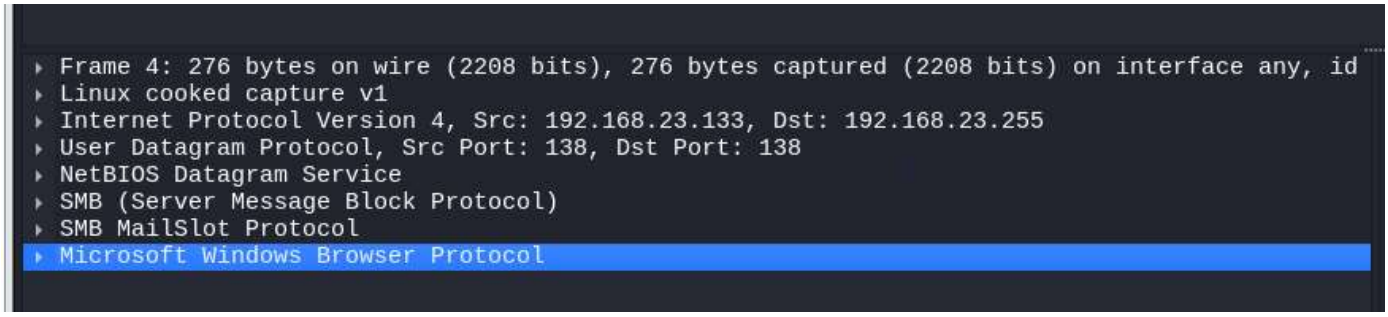
Exercise 4: Monitoring Network Traffic with Wireshark

Task: Use Wireshark to monitor network traffic on your primary interface and filter traffic going to and from the OWASP Broken Web Application VM.

Command: Open Wireshark, choose your network interface, and set the filter to ip.addr == <OWASP_IP> (replace <OWASP_IP> with the actual IP, e.g., 192.168.56.101)



Question: Analyze the packets going to and from the OWASP VM. What types of protocols are in use? Can you identify any key packet details such as source/destination IP addresses, port numbers, and flags? How does the TCP/IP model apply to the data captured?



ANSWER:

Frame 4: 276 bytes on wire (2208 bits), 276 bytes captured (2208 bits) on interface any, id 0

Linux cooked capture v1

Internet Protocol Version 4, Src: 192.168.23.133, Dst: 192.168.23.255

User Datagram Protocol, Src Port: 138, Dst Port: 138

NetBIOS Datagram Service

SMB (Server Message Block Protocol)

SMB Mail Slot Protocol

Microsoft Windows Browser Protocol

Exercise 5: Packet Transmission Analysis

Task: Perform a ping or TCP connection request to the OWASP Broken Web Application IP and capture the packet details using tcpdump or Wireshark.

Command: ping <OWASP_IP> or telnet <OWASP_IP> 80 (to initiate a simple connection) Capture the traffic using tcpdump -i <interface> host <OWASP_IP>, or set the appropriate filter in Wireshark.

Question: What do you observe during the packet transmission process? Describe the handshake process or the round-trip of the packets for ping or TCP connection. Which layers of the OSI and TCP/IP models are involved in this transmission?

Exercise 6: Troubleshooting Network Interface Issues

Task: Simulate a network interface failure by disabling and then re-enabling an interface. Observe how this affects network connectivity to the OWASP Broken Web Application VM.

Command: sudo ifconfig <interface> down and sudo ifconfig <interface> up (or use ip commands)

Question: What happens when you disable the network interface? How does your system respond when the interface is re-enabled? Explain how network administrators can use this knowledge for troubleshooting connectivity issues.

Exercise 7: Bandwidth Monitoring

Task: Use the iftop or nload command to monitor the bandwidth usage on your system while interacting with the OWASP Broken Web Application VM.

Command: sudo iftop -i <interface> or nload <interface> Question: What is the current bandwidth usage while communicating with the OWASP VM? Identify the impact of network traffic on your interface. Is there any traffic congestion? How does this help in monitoring network performance?

Exercise 8: Advanced Packet Capture Filters

Task: Create custom filters in Wireshark or tcpdump to capture only specific types of traffic, such as TCP or HTTP traffic, between your system and the OWASP VM.

Example Filter for HTTP Traffic: tcp port 80 and ip.addr == <OWASP_IP> Question: What is the significance of filtering specific traffic? How can advanced filters help network engineers diagnose and resolve issues?

Submission Requirements:

Submit a report detailing the output of each exercise.

Include screenshots for critical steps such as packet captures and bandwidth monitoring.

Provide explanations for each observed behavior, particularly focusing on the significance of network interfaces and packet transmission.

INT303: Networking Fundamentals – Lab 3

Lab 3: TCP/IP Protocol Stack and Packet Inspection Using OWASP Broken Web Application IP

Objective:

In this lab, students will delve into the Transmission Control Protocol/Internet Protocol (TCP/IP) stack, dissecting and inspecting the various layers involved in packet transmission. Students will focus on understanding how data travels across a network, analyzing packets, and troubleshooting issues related to the TCP/IP model.

Learning Outcomes:

By the end of this lab, students will:

- Understand the fundamentals of the TCP/IP model.
- Be able to analyze packets at different layers (Application, Transport, Network, and Link).
- Gain hands-on experience in dissecting TCP/IP traffic using packet inspection tools.
- Learn how to apply practical troubleshooting techniques based on TCP/IP behavior. Materials Needed:
- Linux-based system (Kali, Ubuntu, etc.)
- OWASP Broken Web Application VM (running and reachable on your network)
- IP address of the OWASP Broken Web Application (e.g., 192.168.X.X)
- Wireshark or tshark for packet capture and analysis

Lab Exercises:

Exercise 1: Understanding the TCP/IP Model

Task: Briefly review the layers of the TCP/IP model (Application, Transport, Network, and Link layers). Understand the purpose and function of each layer in data transmission.

Question:

Explain the differences between the TCP/IP and OSI models.

Which layers of the TCP/IP model correspond to specific OSI layers?

ANSWER:

TCP/IP vs. OSI Model

The TCP/IP and OSI models are two fundamental frameworks used to understand how networks function. While both serve the same purpose, they differ in their structure and approach.

OSI Model

- Open Systems Interconnection (OSI) Model is a conceptual framework that divides network communication into seven distinct layers.
- It provides a clear and comprehensive view of how data is transmitted across a network, from the physical layer to the application layer.
- Each layer has specific functions and interacts with the adjacent layers.

TCP/IP Model

- Transmission Control Protocol/Internet Protocol (TCP/IP) Model is a more practical implementation of network communication, focusing on the protocols used on the internet.
- It has four layers, which are directly related to the protocols that handle data transmission.

Layer Correspondence

Here's how the layers of the TCP/IP model correspond to the OSI model:

OSI Layer	TCP/IP Layer
Application	Application
Presentation	Application
Session	Application
Transport	Transport
Network	Internet
Data Link	Network Interface
Physical	Network Interface

Key Differences

- Number of Layers: OSI has seven layers, while TCP/IP has four.
- Practical vs. Theoretical: OSI is more theoretical, while TCP/IP is more practical and directly reflects real-world protocols.
- Protocol Independence: OSI is protocol-independent, while TCP/IP is protocol-specific.

Reference:

- GeeksforGeeks: https://www.geeksforgeeks.org/difference-between-osi-model-and-tcp-ip-model/

Exercise 2: Capturing and Analyzing TCP Packets

Task: Initiate a connection to the OWASP Broken Web Application VM via HTTP or SSH. Capture TCP packets related to this connection using tcpdump or Wireshark.

Command: tcpdump -i <interface> tcp and host <OWASP_IP> or set a filter in Wireshark.

Example: tcpdump -i eth0 tcp and host 192.168.56.101

Question: What happens during the TCP handshake (SYN, SYN-ACK, ACK)? Identify and describe the flags used in TCP communication (SYN, ACK, FIN, etc.). How does the TCP connection maintain reliability during transmission?

Exercise 3: Investigating IP Packets (Network Layer)

Task: Capture and analyze the IP packets from your connection to the OWASP Broken Web Application.

Command: Use Wireshark or tcpdump with the filter ip.addr == <OWASP_IP> to capture IP packets.

Question: What fields can you see in the IP packet header (e.g., Source IP, Destination IP, TTL, etc.)?

What is the significance of each of these fields? How does IP routing work in this scenario? Are there any hops between your system and the OWASP VM?

Exercise 4: Application Layer Analysis (HTTP/SSH Traffic)

Task: If you're using HTTP, filter the packets to capture only HTTP traffic using Wireshark or tcpdump. If you're using SSH, capture and analyze the encrypted traffic.

Command for HTTP traffic: tcpdump -i <interface> port 80 and host <OWASP_IP>

Command for SSH traffic: tcpdump -i <interface> port 22 and host <OWASP_IP> Question: Analyze the HTTP packets. What information is available in the HTTP request and response? For SSH traffic, what is the significance of encrypted packets? Can you analyze the payload? How does the application layer play a role in data exchange between your system and the

OWASP VM?

Exercise 5: Error Handling in TCP/IP Transmission

Task: Simulate packet loss or network issues by introducing a delay or stopping the network connection momentarily. Capture how TCP/IP handles this issue.

Command: Temporarily disable your network interface using ifconfig <interface> down and then re-enable it.

Question:

What happens when packets are dropped or delayed? How does TCP ensure data reliability in the presence of errors?

How do retransmissions and sequence numbers work in TCP to maintain a proper data flow?

Exercise 6: ICMP and Ping Inspection (Network Layer)

Task: Send a series of ping commands to the OWASP Broken Web Application VM and capture the ICMP packets.

Command: ping <OWASP_IP> and use Wireshark or tcpdump to capture ICMP packets with the filter icmp.

Question:

What are the key fields in an ICMP packet (e.g., Type, Code, Checksum)? How does ICMP assist in diagnosing network connectivity issues?

What is the significance of TTL in both ICMP packets and general IP packets?

Exercise 7: Analyzing UDP Packets (Transport Layer)

Task: If available, generate some UDP traffic to the OWASP VM by using a simple application or UDP-based service. Capture and analyze the UDP packets.

Command: tcpdump -i <interface> udp and host <OWASP_IP> Question:

Compare UDP with TCP. What are the major differences in packet structure and behavior? Why does UDP not ensure reliability, and in what scenarios would you prefer UDP over TCP? How does UDP manage data transmission without the need for acknowledgments or

retransmissions?

Exercise 8: OS Detection via Nmap (Network and Transport Layers)

Task: Use nmap to perform OS detection on the OWASP Broken Web Application VM, analyzing how nmap identifies the operating system based on packet behavior.

Command: nmap -O <OWASP_IP>

Question:

How does nmap detect the OS based on the captured packets?

What packet characteristics (TTL, window size, etc.) help in identifying the OS?

Explain why OS detection can be an important step in network analysis and vulnerability assessment.

ANSWER:

How nmap Detects OS Based on Packet Characteristics

nmap, a powerful network scanning tool, leverages a technique called TCP/IP stack fingerprinting to identify the operating system of a target host. By sending carefully crafted packets and analyzing the responses, nmap can deduce specific characteristics of the target's operating system.

Key Packet Characteristics for OS Detection:

- **TTL (Time to Live):** This field indicates the maximum number of hops a packet can traverse before being discarded. Different operating systems have distinct default TTL values.
- **Window Size:** The window size determines the amount of data a TCP receiver can accept at a given time. OSes often have specific window size behaviors.
- **TCP Timestamps:** Timestamps added to TCP packets can reveal information about the system clock and timing mechanisms, which can vary between OSes.
- **IP ID Sequence:** The IP ID field is incremented for each packet sent. The sequence of IP IDs can provide clues about the OS's packet generation and handling.
- **TCP Options:** TCP options like timestamps, window scaling, and selective acknowledgments can be used to differentiate between OSes.

Importance of OS Detection in Network Analysis and Vulnerability Assessment

OS detection is a crucial step in network analysis and vulnerability assessment for several reasons:

1. **Targeted Attacks:** Knowing the target's OS allows attackers to tailor their attacks to specific vulnerabilities and exploits associated with that OS.
2. **Risk Assessment:** By identifying the OS, security professionals can assess the potential risks and prioritize security measures accordingly.
3. **Vulnerability Scanning:** Vulnerability scanners can focus on known vulnerabilities that affect the identified OS, improving the efficiency of the scanning process.
4. **Network Mapping:** Understanding the OS distribution within a network can help in network mapping and planning.
5. **Incident Response:** During incident response, knowing the OS of compromised systems can aid in investigation and remediation efforts.

REFERENCES

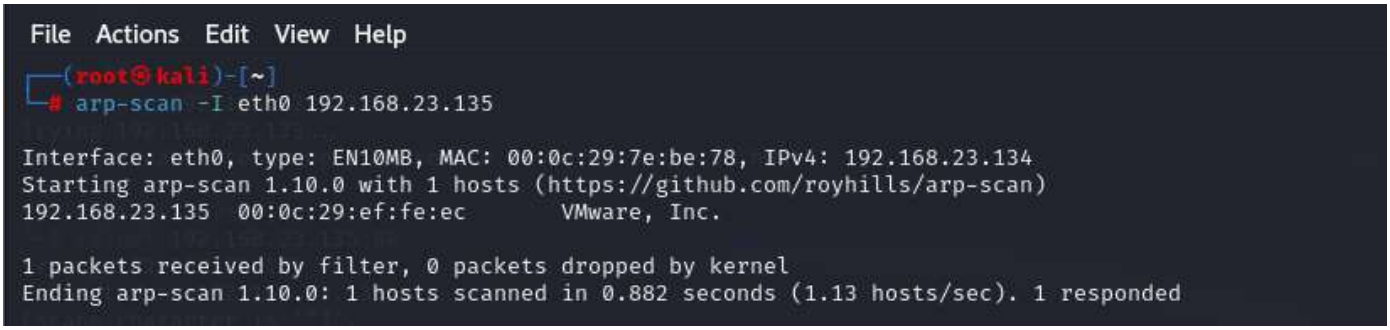
https://nmap.org/book/man-os-detection.html#:~:text=One%20of%20Nmap's%20best%2Dknown,using%20TCP%2FIP%20stack%20fingerprinting.

https://nmap.org/book/osdetect.html#:~:text=Fortunately%2C%20Nmap%20includes%20a%20huge,a%20selection%20of%20TCP%2FIP

Exercise 9: Analyzing ARP Traffic (Link Layer)

Task: Use arp-scan or tcpdump to capture ARP traffic in your local network, focusing on communication with the OWASP VM.

Command: arp-scan -I <interface> <OWASP_IP>



Question:

What information can you gather from ARP packets (e.g., MAC addresses)? How does the ARP protocol function at the link layer? What role does ARP play in the communication between your system and the OWASP VM?

Exercise 10: Troubleshooting Network Connectivity Using TCP/IP Knowledge

Task: Simulate a common network issue (e.g., incorrect subnet mask, gateway misconfiguration) and troubleshoot the issue using your understanding of the TCP/IP stack.

Question:

What is the issue you simulated, and how did it affect network communication?

How did you diagnose and resolve the issue using packet inspection and knowledge of the TCP/IP layers?

What tools and techniques would you recommend for real-world network troubleshooting?

Submission Requirements:

Submit a report that includes packet captures, command outputs, and explanations for each exercise.

Include screenshots and highlight key details in the packet captures.

Provide in-depth analysis of TCP/IP behavior observed during the lab.

Reflection:

Through this lab, students will gain practical experience in dissecting and troubleshooting network traffic using the TCP/IP stack. Understanding how data flows across the network at various layers will help in mastering network fundamentals and preparing for real-world challenges in network administration and cybersecurity.