**OLOLADE ADESHEWA SHOMALA**

**INT303: Networking Fundamentals**

**LAB 1**

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

**OSI Model Layers and Their Functions**

1. **Physical Layer**:
   * **Function**: This layer is responsible for the physical connection between devices. It deals with the transmission and reception of raw bit streams over a physical medium (e.g., cables, switches).
   * **Corresponding TCP/IP Layer**: Link Layer
2. **Data Link Layer**:
   * **Function**: This layer provides node-to-node data transfer and handles error correction from the physical layer. It ensures that data is transferred correctly between adjacent network nodes.
   * **Corresponding TCP/IP Layer**: Link Layer
3. **Network Layer**:
   * **Function**: This layer is responsible for packet forwarding, including routing through different routers. It determines the best path to send data from source to destination.
   * **Corresponding TCP/IP Layer**: Internet Layer
4. **Transport Layer**:
   * **Function**: This layer provides reliable data transfer services to the upper layers. It ensures complete data transfer and manages error detection and recovery (e.g., TCP, UDP).
   * **Corresponding TCP/IP Layer**: Transport Layer
5. **Session Layer**:
   * **Function**: This layer manages sessions between applications. It establishes, maintains, and terminates connections between applications.
   * **Corresponding TCP/IP Layer**: Application Layer
6. **Presentation Layer**:
   * **Function**: This layer translates data between the application layer and the network. It handles data encryption, compression, and translation (e.g., converting data formats).
   * **Corresponding TCP/IP Layer**: Application Layer
7. **Application Layer**:
   * **Function**: This layer provides network services directly to end-user applications. It includes protocols used by applications to communicate over the network (e.g., HTTP, FTP, SMTP).
   * **Corresponding TCP/IP Layer**: Application Layer

**Matching OSI Layers with TCP/IP Layers**

| **OSI Model Layer** | **TCP/IP Model Layer** |
| --- | --- |
| Physical | Link |
| Data Link | Link |
| Network | Internet |
| Transport | Transport |
| Session | Application |
| Presentation | Application |
| Application | Application |

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.

**What Happens When You Ping the OWASP Application?**

When you ping the OWASP application, your system sends ICMP (Internet Control Message Protocol) Echo Request packets to the IP address of the OWASP VM. The OWASP VM responds with ICMP Echo Reply packets. This process helps determine if the OWASP VM is reachable and measures the round-trip time for the packets.

**Breakdown of the Ping Output**

plaintext

64 bytes from 10.0.2.15: icmp\_seq=1432 ttl=64 time=0.75 ms

* **64 bytes**: This indicates the size of the ICMP Echo Reply packet received from the OWASP VM.
* **from 10.0.2.15**: This is the IP address of the OWASP VM that responded to the ping.
* **icmp\_seq=1432**: This is the sequence number of the ICMP Echo Request packet. It helps in identifying the order of packets.
* **ttl=64**: TTL stands for Time To Live. It indicates the maximum number of hops (routers) the packet can pass through before being discarded. A TTL of 64 is typical for many systems.
* **time=0.75 ms**: This is the round-trip time it took for the packet to travel from your system to the OWASP VM and back. It is measured in milliseconds.

**Which OSI Layer Does the Ping Command Operate In?**

The ping command operates at the Network layer (Layer 3) of the OSI model. It uses the ICMP protocol, which is part of the Network layer, to send and receive Echo Request and Echo Reply messages.

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 (e.g., traceroute 192.168.56.101) Question: How many hops did it take to reach the OWASP VM? Describe the significance of each hop and what role traceroute plays in network troubleshooting. Answer: It took 1 hop to reach the OWASP VM.

Significance of Each Hop

- Hop 1: This is the first and only router or gateway that your packet encounters. Since it took only 1 hop, it means that your system is directly connected to the OWASP VM without any intermediate routers.

Role of `traceroute` in Network Troubleshooting

-Identifying Path: `traceroute` helps identify the path that packets take to reach the destination. This is useful for understanding the network topology.

- Diagnosing Issue: By analyzing the hops, you can identify where delays or packet loss occur. This helps in diagnosing network issues and pinpointing problematic routers or network segments.

- Measuring Latency: The time taken for each hop (in milliseconds) helps measure the latency at each stage of the path. High latency at a particular hop can indicate congestion or issues with that router.

OSI Layer

The `traceroute` command operates at the Network layer (Layer 3) of the OSI model. It uses the ICMP protocol, which is part of the Network layer, to send and receive packets.

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 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.

udp 0 0 10.0.2.15:bootpc 10.0.2.2:bootps ESTABLISHED

* **udp**: This indicates that the connection is using the UDP (User Datagram Protocol).
* **0 0**: These columns show the amount of data in the send and receive queues, respectively.
* **10.0.2.15:bootpc**: This is the source IP address and port. 10.0.2.15 is your system's IP address, and bootpc (port 68) is typically used for DHCP client communication.
* **10.0.2.2:bootps**: This is the destination IP address and port. 10.0.2.2 is the IP address of the DHCP server, and bootps (port 67) is used for DHCP server communication.
* **ESTABLISHED**: This indicates that the connection is active and established.

**Significance of Each Part**

* **Source IP and Port**: 10.0.2.15:bootpc indicates that your system (with IP 10.0.2.15) is using port 68 (DHCP client port) to communicate.
* **Destination IP and Port**: 10.0.2.2:bootps indicates that the destination is the DHCP server (with IP 10.0.2.2) using port 67 (DHCP server port).
* **ESTABLISHED**: This shows that there is an active communication session between your system and the DHCP server.

**Role of the Transport Layer (UDP)**

* **UDP (User Datagram Protocol)**: UDP is a connectionless protocol that operates at the Transport layer (Layer 4) of the OSI model. Unlike TCP, UDP does not establish a connection before sending data and does not guarantee delivery, order, or error checking. It is used for applications that require fast, efficient transmission, such as DHCP, DNS, and streaming services.

**How UDP is Involved in This Communication**

* **DHCP Communication**: The connection shown in your netstat output is related to DHCP (Dynamic Host Configuration Protocol). DHCP uses UDP to assign IP addresses to devices on a network. The DHCP client (your system) sends requests to the DHCP server to obtain an IP address and other network configuration details.
* **Efficiency**: UDP is chosen for DHCP because it is faster and requires fewer resources than TCP. Since DHCP messages are small and the protocol can handle occasional packet loss, the reliability features of TCP are not necessary.

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 Run a UDP scan. Command: nmap -sU Question: What are the key differences between TCP and UDP in terms of reliability and speed? Based on the scan results, list which services on the OWASP application are using TCP and which are using UDP

### Answer: Key Differences Between TCP and UDP

1. **Reliability**:
   * **TCP (Transmission Control Protocol)**: TCP is a connection-oriented protocol that ensures reliable data transfer. It establishes a connection through a three-way handshake (SYN, SYN-ACK, ACK), maintains the connection, and ensures data integrity through error checking and retransmission of lost packets.
   * **UDP (User Datagram Protocol)**: UDP is a connectionless protocol that does not guarantee delivery, order, or error checking. It is faster and more efficient for applications that can tolerate some data loss, such as streaming or gaming.
2. **Speed**:
   * **TCP**: Due to its connection-oriented nature and error-checking mechanisms, TCP is generally slower than UDP. However, it provides reliable and ordered delivery of data.
   * **UDP**: UDP is faster than TCP because it does not establish a connection or perform error checking. It is suitable for applications that require low latency and can tolerate some data loss.

### Scan Results Interpretation

* **TCP Scan (**nmap -sT**)**:
  + **Result**: All 1000 scanned TCP ports are closed (connection refused).
  + **Interpretation**: There are no services running on the OWASP VM that are listening on the default 1000 TCP ports scanned by nmap.
* **UDP Scan (**nmap -sU**)**:
  + **Result**: All 1000 scanned UDP ports are closed (port unreachable).
  + **Interpretation**: There are no services running on the OWASP VM that are listening on the default 1000 UDP ports scanned by nmap.

### Conclusion

* **TCP Services**: None of the default 1000 TCP ports are open on the OWASP VM.
* **UDP Services**: None of the default 1000 UDP ports are open on the OWASP VM.

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

### Question

1. **What is the MAC address associated with the OWASP VM’s IP?**
   * **Answer**: The MAC address associated with the OWASP VM’s IP (10.0.2.15) is 08:00:27:4e:66:a1.
2. **Explain the significance of ARP in the Data Link Layer and how it contributes to successful communication.**
   * **Answer**: ARP (Address Resolution Protocol) operates at the Data Link Layer (Layer 2) of the OSI model. Its primary function is to map IP addresses (Layer 3) to MAC addresses (Layer 2). When a device wants to communicate with another device on the same local network, it needs to know the MAC address of the destination device. ARP helps achieve this by broadcasting an ARP request packet to all devices on the network, asking for the MAC address associated with a specific IP address. The device with the matching IP address responds with its MAC address. This mapping is then stored in the ARP cache for future use, allowing efficient and successful communication between devices on the 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 host <OWASP\_IP>

### Analyzing the Captured Traffic

#### Question 1: What protocols are in use?

* **Answer**: The captured traffic may include various protocols such as:
  + **TCP**: Transmission Control Protocol for reliable communication.
  + **UDP**: User Datagram Protocol for connectionless communication.
  + **HTTP/HTTPS**: Hypertext Transfer Protocol (Secure) for web traffic.
  + **DNS**: Domain Name System for resolving domain names.
  + **ICMP**: Internet Control Message Protocol for network diagnostics (e.g., ping).

#### Question 2: Can you identify the handshake process or other significant events in the captured packets?

* **Answer**: Yes, you can identify significant events such as:
  + **TCP Handshake**: The three-way handshake process (SYN, SYN-ACK, ACK) used to establish a TCP connection.
  + **HTTP Requests and Responses**: The exchange of HTTP GET, POST requests, and corresponding responses.
  + **DNS Queries and Responses**: The process of resolving domain names to IP addresses.
  + **ICMP Echo Requests and Replies**: The ping process to check the reachability of the OWASP VM.

### Example Analysis

1. **TCP Handshake**:
   * **SYN**: Your machine sends a SYN packet to the OWASP VM to initiate a connection.
   * **SYN-ACK**: The OWASP VM responds with a SYN-ACK packet to acknowledge the connection request.
   * **ACK**: Your machine sends an ACK packet to establish the connection.
2. **HTTP Request**:
   * **GET Request**: Your machine sends an HTTP GET request to the OWASP VM to retrieve a web page.
   * **HTTP Response**: The OWASP VM responds with the requested web page.
3. **DNS Query**:
   * **Query**: Your machine sends a DNS query to resolve a domain name.
   * **Response**: The DNS server responds with the IP address of the domain.
4. **ICMP Ping**:
   * **Echo Request**: Your machine sends an ICMP Echo Request to the OWASP VM.
   * **Echo Reply**: The OWASP VM responds with an ICMP Echo Reply.

