INT303: Networking Fundamentals – Lab2

**Question**

1. **What network interfaces are available on your system?**
   * **Answer**: The available network interfaces on your system might include eth0 (Ethernet), wlan0 (Wi-Fi), and lo (loopback).
2. **Identify the IP address assigned to each interface.**
   * **Answer**: In the example output:
     + eth0 has the IP address 192.168.1.100.
     + lo (loopback) has the IP address 127.0.0.1.
3. **Describe the difference between a loopback interface and an external network interface.**
   * **Answer**:
     + **Loopback Interface**: The loopback interface (lo) is a virtual network interface used for internal communication within the host. It is assigned the IP address 127.0.0.1 and is used to test network applications without sending packets over the physical network.
     + **External Network Interface**: External network interfaces, such as eth0 (Ethernet) or wlan0 (Wi-Fi), are physical or wireless interfaces used to connect the host to external networks. These interfaces are assigned IP addresses that allow communication with other devices on the network.

### Exercise 2: Question

1. **What kind of packets are being captured?**
   * **Answer**: The captured packets can include various types such as:
     + **TCP Packets**: Used for reliable communication between devices.
     + **UDP Packets**: Used for connectionless communication.
     + **ICMP Packets**: Used for network diagnostics (e.g., ping).
     + **ARP Packets**: Used for mapping IP addresses to MAC addresses.
     + **HTTP/HTTPS Packets**: Used for web traffic.
     + **DNS Packets**: Used for resolving domain names.
2. **Are there any packets related to communication with the OWASP Broken Web Application VM?**
   * **Answer**: To identify packets related to communication with the OWASP VM, look for packets with the IP address of the OWASP VM (10.0.2.15). You can filter the captured packets using the IP address to see if there are any communications between your system and the OWASP VM.
3. **Describe the role of this network interface in transmitting and receiving packets.**
   * **Answer**: The network interface (e.g., eth0) is responsible for transmitting and receiving packets between your system and other devices on the network. It operates at the Data Link Layer (Layer 2) of the OSI model and handles the physical transmission of data over the network medium (e.g., Ethernet cables, Wi-Fi). The interface ensures that packets are correctly formatted, addressed, and transmitted to the appropriate destination. It also receives incoming packets, processes them, and passes them up to the higher layers of the OSI model for further handling.

### Exercise 3: Current Status of Network Interfaces

**Interface: eth0**

* **MTU**: 1500
* **RX-OK**: 26 (Received packets without errors)
* **RX-ERR**: 0 (Received packets with errors)
* **RX-DRP**: 0 (Dropped received packets)
* **RX-OVR**: 0 (Overruns in received packets)
* **TX-OK**: 66 (Transmitted packets without errors)
* **TX-ERR**: 0 (Transmitted packets with errors)
* **TX-DRP**: 0 (Dropped transmitted packets)
* **TX-OVR**: 0 (Overruns in transmitted packets)
* **Flags**: BMRU (Broadcast, Multicast, Running, Up)

**Interface: lo (Loopback)**

* **MTU**: 65536
* **RX-OK**: 7170 (Received packets without errors)
* **RX-ERR**: 0 (Received packets with errors)
* **RX-DRP**: 0 (Dropped received packets)
* **RX-OVR**: 0 (Overruns in received packets)
* **TX-OK**: 7170 (Transmitted packets without errors)
* **TX-ERR**: 0 (Transmitted packets with errors)
* **TX-DRP**: 0 (Dropped transmitted packets)
* **TX-OVR**: 0 (Overruns in transmitted packets)
* **Flags**: LRU (Loopback, Running, Up)

**Current Network Statistics and Connections**

**Active UNIX Domain Sockets**

The output shows active UNIX domain sockets, which are used for inter-process communication (IPC) on the same host. Here are the details:

* **unix 3**: This indicates a UNIX domain socket with 3 references.
* **unix 2**: This indicates a UNIX domain socket with 2 references.
* **stream Dgram connected**: This indicates a connected stream or datagram socket.
* **run/user/1000/bus/**: This is a path to a UNIX domain socket used for IPC.
* **run/user/1000/pulse/native**: This is a path to a UNIX domain socket used by the PulseAudio sound server.
* **run/dbus/socket**: This is a path to a UNIX domain socket used by the D-Bus message bus system.

**Significance of Network Statistics in Monitoring Network Performance**

1. **Packet Counts**: The number of packets transmitted and received helps gauge network activity and performance.
2. **Errors and Drops**: Monitoring errors and dropped packets is crucial for identifying potential issues with the network interface or physical connections.
3. **Active Connections**: Understanding the number of active connections provides insight into network usage and potential congestion.
4. **Protocol Distribution**: Knowing the distribution of TCP, UDP, and other protocols helps in identifying the types of traffic on the network.
5. **Performance Monitoring**: Regularly monitoring these statistics helps in early detection of network issues, ensuring timely troubleshooting and maintenance.

#### Exercise 4: Monitoring Network Traffic with Wireshark **Question 1: What types of protocols are in use?**

* **Answer**: The captured traffic includes 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 any key packet details such as source/destination IP addresses, port numbers, and flags?**

* **Answer**: Yes, i can identify key packet details such as:
  + **Source IP Address**: The IP address of the device sending the packet.
  + **Destination IP Address**: The IP address of the device receiving the packet.
  + **Port Numbers**: The source and destination port numbers used for communication (e.g., 80 for HTTP, 443 for HTTPS, 22 for SSH).
  + **Flags**: TCP flags such as SYN, ACK, FIN, and RST, which indicate the state of the TCP connection.

**Question 3: How does the TCP/IP model apply to the data captured?**

* **Answer**: The TCP/IP model applies to the data captured as follows:
  + **Application Layer**: This layer includes protocols like HTTP, HTTPS, and DNS, which are used for specific applications and services.
  + **Transport Layer**: This layer includes TCP and UDP, which are responsible for data transfer and communication between devices.
  + **Internet Layer**: This layer includes IP, which is responsible for addressing and routing packets between devices.
  + **Link Layer**: This layer includes protocols like Ethernet, which are responsible for the physical transmission of data over the network medium.

### Exercise 5:

### Question

1. **What do you observe during the packet transmission process?**
   * **Answer**: During the packet transmission process, i observed the exchange of packets between my system and the OWASP VM. For a ping, ICMP Echo Request and Echo Reply packets. For a TCP connection, TCP handshake process (SYN, SYN-ACK, ACK) followed by data packets and possibly a connection termination process (FIN, ACK).
2. **Describe the handshake process or the round-trip of the packets for ping or TCP connection.**
   * **Answer**:
     + **Ping (ICMP)**: The ping command sends ICMP Echo Request packets to 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.
     + **TCP Handshake**: The TCP connection process involves a three-way handshake:
       1. **SYN**: The system sends a SYN packet to the OWASP VM to initiate a connection.
       2. **SYN-ACK**: The OWASP VM responds with a SYN-ACK packet to acknowledge the connection request.
       3. **ACK**: The system sends an ACK packet to establish the connection.
     + After the handshake, data packets are exchanged, and the connection is eventually terminated with a FIN-ACK sequence.
3. **Which layers of the OSI and TCP/IP models are involved in this transmission?**
   * **Answer**: The layers involved in this transmission are:
     + **OSI Model**:
       1. **Application Layer**: For protocols like HTTP (when using telnet).
       2. **Transport Layer**: For TCP and UDP communication.
       3. **Network Layer**: For IP addressing and routing.
       4. **Data Link Layer**: For MAC addressing and frame transmission.
     + **TCP/IP Model**:
       1. **Application Layer**: For application-specific protocols.
       2. **Transport Layer**: For TCP and UDP communication.
       3. **Internet Layer**: For IP addressing and routing.
       4. **Link Layer**: For MAC addressing and frame transmission

Exercise 6: Troubleshooting Network Interface Issues

### Question

1. **What happens when you disable the network interface?**
   * **Answer**: When you disable the network interface, all network connectivity through that interface is lost. This means that any ongoing connections will be interrupted, and you will not be able to communicate with the OWASP Broken Web Application VM or any other network resources.
2. **How does your system respond when the interface is re-enabled?**
   * **Answer**: When you re-enable the network interface, the system will attempt to re-establish network connectivity. This includes re-acquiring an IP address (if using DHCP) and re-establishing any previously interrupted connections. You should be able to communicate with the OWASP Broken Web Application VM again once the interface is up and running.
3. **Explain how network administrators can use this knowledge for troubleshooting connectivity issues.**
   * **Answer**: Network administrators can use this knowledge to troubleshoot connectivity issues by:
     + **Isolating Problems**: Disabling and re-enabling network interfaces can help isolate whether connectivity issues are related to the interface itself or other network components.
     + **Resetting Connections**: This process can reset network connections and clear any temporary issues that might be affecting connectivity.
     + **Testing Configuration Changes**: Administrators can test the effects of configuration changes by disabling and re-enabling interfaces to ensure that changes are applied correctly.
     + **Diagnosing Hardware Issues**: If re-enabling the interface does not restore connectivity, it may indicate a hardware issue with the network interface card (NIC) or physical connections.

### Exercise 7:

### Question

1. **What is the current bandwidth usage while communicating with the OWASP VM?**
   * **Answer**: The current bandwidth usage is displayed in the iftop or nload interface. There is real-time data on the amount of bandwidth being used for incoming and outgoing traffic.
2. **Identify the impact of network traffic on your interface. Is there any traffic congestion?**
   * **Answer**: By monitoring the bandwidth usage, you can identify the impact of network traffic on your interface. High bandwidth usage may indicate heavy traffic, which could lead to congestion. If you notice that the bandwidth usage is consistently high and the network performance is degraded, it may suggest traffic congestion.
3. **How does this help in monitoring network performance?**
   * **Answer**: Monitoring bandwidth usage helps in several ways:
     + **Identifying Bottlenecks**: By observing bandwidth usage, you can identify network bottlenecks and take steps to alleviate them.
     + **Optimizing Performance**: Understanding how bandwidth is being used allows you to optimize network performance by managing traffic and prioritizing critical applications.
     + **Troubleshooting Issues**: Bandwidth monitoring can help diagnose network issues by revealing patterns of high usage or congestion that may be causing performance problems.
     + **Capacity Planning**: Regular monitoring helps in planning for future network capacity needs by providing insights into usage trends and growth.

### Exercise 8:

### Question

1. **What is the significance of filtering specific traffic?**
   * **Answer**: Filtering specific traffic allows you to focus on the packets that are most relevant to your analysis. This is particularly useful in environments with high traffic volumes, as it helps reduce the amount of data you need to sift through. By capturing only the traffic of interest, you can more easily identify patterns, diagnose issues, and understand the behavior of specific protocols or applications.
2. **How can advanced filters help network engineers diagnose and resolve issues?**
   * **Answer**: Advanced filters help network engineers in several ways:
     + **Targeted Analysis**: By filtering for specific types of traffic, engineers can zero in on the packets that are relevant to the issue at hand. This makes it easier to identify anomalies, performance bottlenecks, or security threats.
     + **Efficiency**: Filtering reduces the amount of data captured, making it more manageable and quicker to analyze. This is especially important in large networks where capturing all traffic would be impractical.
     + **Troubleshooting**: Filters can help isolate problems by focusing on specific protocols, ports, or IP addresses. For example, if there is an issue with HTTP traffic, filtering for TCP port 80 traffic can help pinpoint the problem.
     + **Security**: Advanced filters can be used to monitor for suspicious activity, such as unusual traffic patterns or unauthorized access attempts. This helps in identifying and mitigating security threats.