Fundamentals of Data Communications

Lab 9

Security

University of Colorado Boulder

Department of Computer Science

Network Engineering

Professor Levi Perigo, Ph.D.

# Summary

This lab is intended to be an overview of security policy and troubleshooting measures that need to be implemented in a production environment.

The questions in the lab are intentionally vague. The purpose of this is for you not only to research, investigate, and learn the technologies, but also become proficient at interpreting both non-technical and technical questions. Being able to research and discover answers on your own will be critical as you progress in your career.

# Objective 1: Apache (90 points)

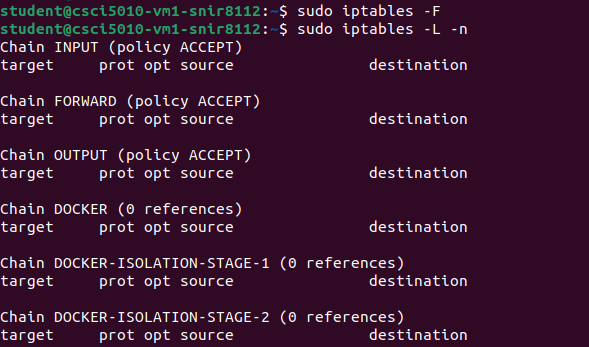
**Note:**

* **Install Apache on VM1 provided.**
* **Install NMAP on VM2 provided.**
* **IP address in range of 10.X.X.X is connected between the VM’s i.e., adapter ENS160 is connected between VM1 and VM2. Make use of this IP everywhere.**

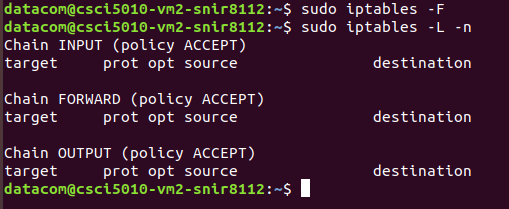
1. Flush the firewall rules on VM1 and VM2. What is the command used? Paste screenshots. **[10 points]**

I used iptables -F command to flush all the firewall rules.

**VM1:**

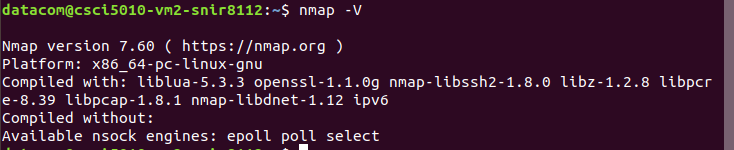
****

**VM2:**

****

1. Install NMAP on VM2. How will you check the version of NMAP installed? Paste screenshots **[5 points]**

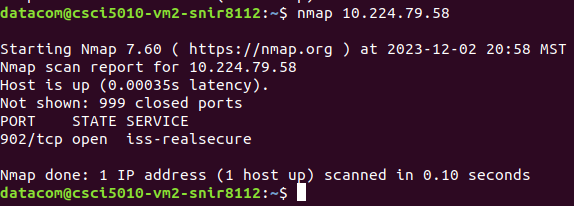
nmap -V or nmap –version will show the version of NMAP.

****

1. What is NMAP used for? List two uses. **[5 points]**

Nmap, which stands for Network Mapper, is a powerful open-source tool for network exploration and security auditing.

1. Nmap can be used to discover hosts on a network and identify the active devices. It can perform host discovery by sending packets to a range of IP addresses and analyzing the responses. This helps administrators to understand the structure of their network, identify live hosts, and determine which services are running on those hosts.
2. Nmap is frequently used to conduct security audits and vulnerability assessments on networks. It can scan for open ports, detect running services, and gather information about the versions of software running on the target systems. By identifying open ports and services, administrators can assess potential security risks and take necessary measures to secure their systems.
3. Scan Datacom VM1 from VM2 using NMAP and explain the output. **[15 points]**

****

I executed the 'nmap' command with the specified IP address, 10.224.79.58, corresponding to VM1. The initial output indicated that the scan was initiated for the target IP, and the report displayed details for that specific address. The scan determined that the host (VM1) is responsive, with a latency of 0.00035 seconds, signifying the time it took for VM2 to reach VM1.

Following this, the report noted that there were 999 closed ports, indicating that these ports did not respond during the scan and are considered closed.

In the subsequent section of the report, it highlighted that port 902/tcp on VM1 is open, suggesting that a service or application is actively using this port.

1. Install and initialize an Apache server on VM1. Mention the steps followed. **[15 points]**

I ran the following commands:

sudo apt update

sudo apt install apache2 : To install Apache2 on VM1

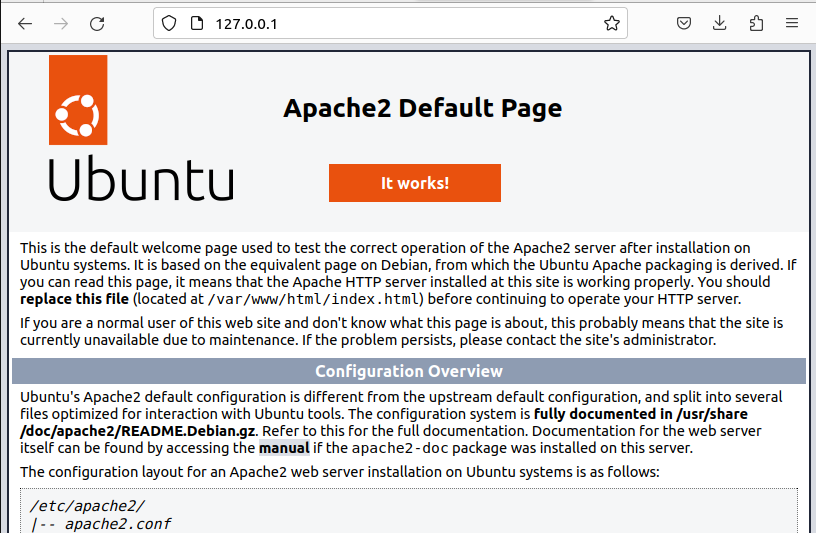
sudo systemctl start apache2: To start the apache2 service on port 80

sudo systemctl enable apache2: To make the apache2 service reboot-persistent

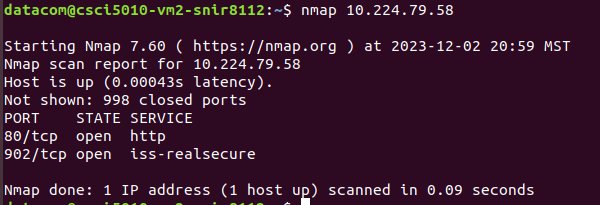
sudo systemctl status apache2: To check the status as “active(running)”

Since our firewall does not have any block rules, it will allow all outbound traffic by default, hence I did not configure any firewall rules.

Typed 127.0.0.1 on my VM1 browser, and voila! I got the Apache2 default page.

****

1. Scan Datacom VM1 again using NMAP. Do you notice any difference? Why or why not? **[10 points]**

****

Yes, I see TCP port 80 open on VM1. This is a result of our installation of apache2 and starting/enabling the service. Apache2 functions as a web server and operates on port 80.

1. Explain the different port states available in NMAP? Explain. **[20 points]**

Nmap provides several distinct port states to describe the status of a particular port on a target system. Each port state conveys specific information about the accessibility and responsiveness of the corresponding network service.

1. **Open:** The target system actively accepts connections on the specified port. The service associated with this port is running and accessible.
2. **Closed:** The target system actively rejects connections on the specified port. The service associated with this port is not running, or it may be behind a firewall that actively denies access.
3. **Filtered:** Nmap cannot determine whether the port is open or closed. The port may be protected by a firewall that prevents Nmap from determining its state. It could also indicate that the target system is not responding to the probes.
4. **Unfiltered:** Nmap can confirm that the port is open or closed but cannot determine the exact state. This state usually occurs when Nmap is unable to reliably identify whether the port is open or closed due to factors like packet filtering or lack of response.
5. **Open|Filtered:** Nmap is unable to determine whether the port is open or filtered. Similar to the "Filtered" state, but Nmap specifically indicates the uncertainty between an open or filtered condition.
6. **Closed|Filtered:** Nmap is unable to determine whether the port is closed or filtered. Similar to the "Filtered" state, but Nmap specifically indicates the uncertainty between a closed or filtered condition.
7. **Unspecified|Filtered:** Nmap cannot determine whether the port is open, closed, or filtered. The port's state cannot be accurately determined due to various factors, and Nmap cannot specify the exact condition.

**References for Objective 1:   
Apache:**

To install, on terminal run **“sudo apt install apache2”** and check the status by **“sudo systemctl status apache2”  
nmap:**

<https://phoenixnap.com/kb/how-to-install-nmap-ubuntu>

<https://phoenixnap.com/kb/nmap-scan-open-ports>

# Objective 2: Threat detection and Mitigation (90 points)

**Note:**

**Install HPING3 on VM2.**

**Add firewall rule on VM1.**

1. What is hping? What are the different applications? **[10 points]**

hping is a command-line-oriented TCP/IP packet assembler/analyzer. It's a tool used for network testing, analysis, and penetration testing. hping allows users to construct TCP, UDP, ICMP, and RAW-IP packets and send them to a target host. Here are some of its main applications:

1. **Packet Crafting and Sending**: hping enables users to craft and send custom packets to a target host. This is particularly useful for testing and analyzing network behavior and security.
2. **Network Scanning**: hping can be used for network scanning to discover hosts and open ports. It sends various types of packets to a range of IP addresses and ports to gather information about the network.
3. **Firewall Testing**: Security professionals often use hping to test the effectiveness of firewalls. By sending crafted packets, users can evaluate how well a firewall filters or allows specific types of traffic.
4. **Route Testing**: hping can be employed to test and analyze network routes. It helps in understanding the path that packets take between the source and destination, revealing potential issues or inefficiencies.
5. **Denial-of-Service (DoS) Attacks Simulation**: While it's crucial to use Hping responsibly, security professionals sometimes leverage it to simulate certain types of Denial-of-Service attacks. This helps organizations identify and mitigate vulnerabilities in their systems.
6. **Fragmentation Testing**: hping allows users to test how different operating systems and firewalls handle fragmented packets. This can be essential for understanding potential security weaknesses related to packet fragmentation.
7. **Firewall Evasion Techniques**: Security experts may use hping to test and demonstrate techniques for evading firewall detection. Understanding potential evasion methods can be essential for improving firewall configurations.
8. **Advanced Ping and Traceroute:** hping can perform advanced ping and traceroute operations, providing more flexibility and customization compared to traditional tools.
9. Install hping3 on VM2. Mention the steps followed. **[5 points]**

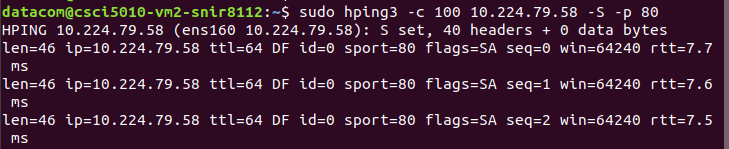
sudo apt update

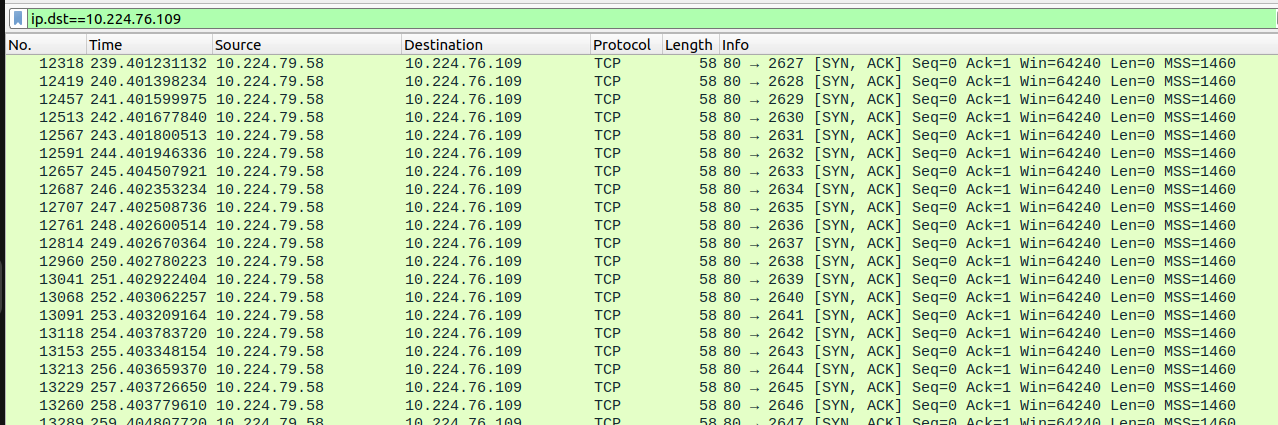
sudo apt install hping3

hping3 --version

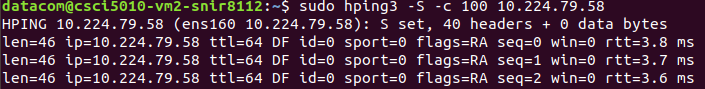
1. Monitor the adapter on VM1 that connects to VM2 and analyze the packets received using Wireshark to detect attacks.
2. Send 100 TCP SYN packets to VM1. Paste the screenshot of the output and the command used. **[15 points]**

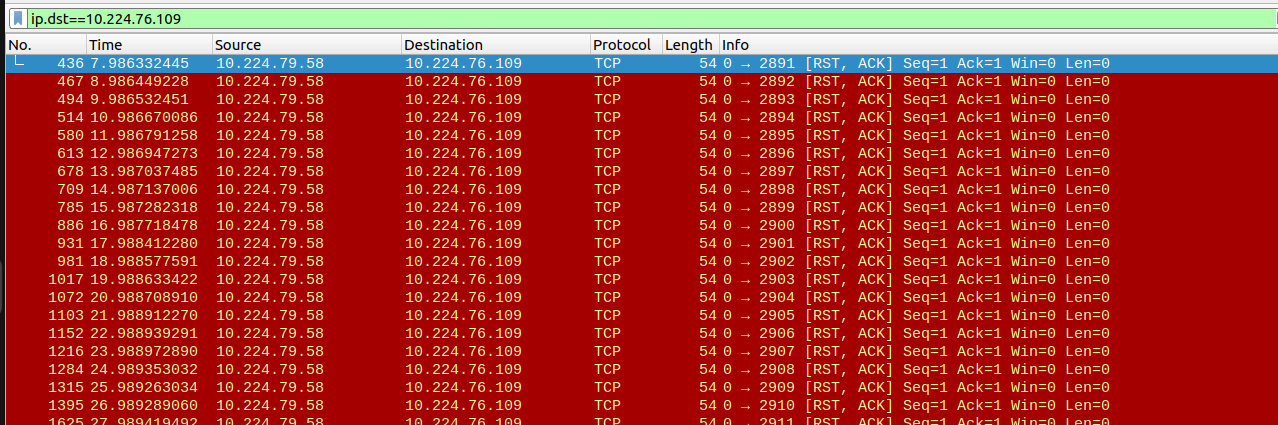
I used hping3 to send 100 SYN packets to VM1. One observation is that when I mention the port number (in this case port 80), I get an SA flag. This is because port 80 is open.

****

****

In contrast to sending it to the default port (without mentioning the port number), which is 0 and I get an RST flag.

****

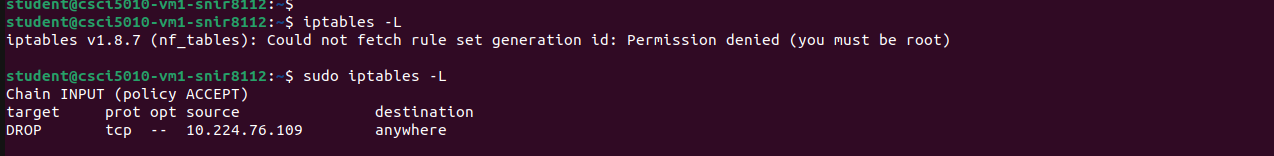
****

1. Identify the malicious traffic (in this case the hping3 generated traffic) and install a firewall rule to block the incoming packets. Paste the screenshots of the iptables rules and Wireshark capture. **[40 points]**

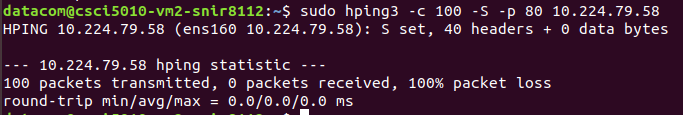
**Method 1: Blocking the IP address completely**

I blocked VM2 IP address using this command:

| sudo iptables -A INPUT -p tcp -s 10.224.76.109 -j DROP |
| --- |

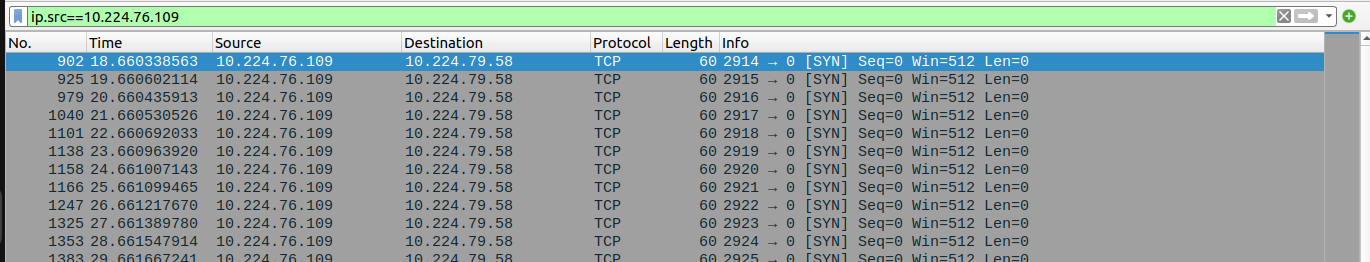


Post this, VM2 is unable to send any TCP SYN packets to VM1.

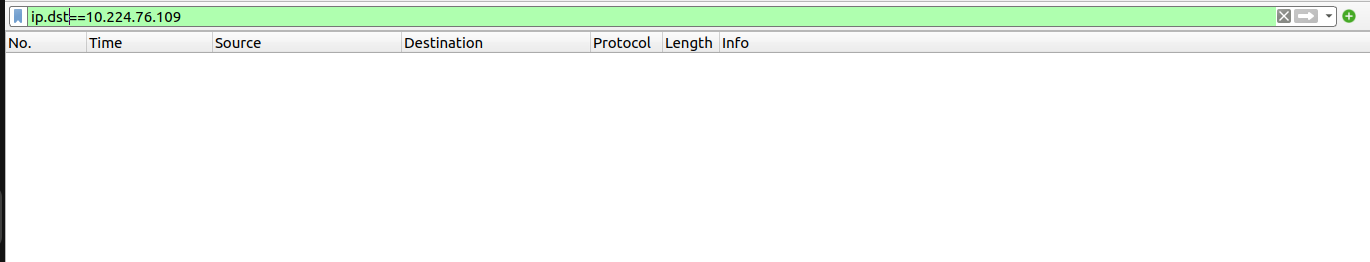


**Wireshark output**

When I filter with ip.src=VM2\_IP, I can see that all the TCP packets are gray in color, which means that the TCP packets are malformed or incomplete. If the SYN packet is incomplete or malformed, VM1 will not respond with a standard SYN/ACK.



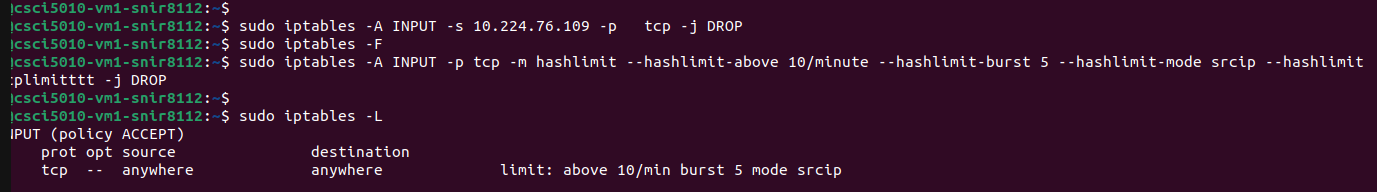
To confirm this, I filtered with ip.dst=VM2\_IP and the output was empty.



Hence, all the TCP packets were blocked by VM1.

**Method 2: Rate Limiting**

However, if I have rate limiting in place (*say, VM2 can only send 10 SYN packets a minute*), this would still allow communication between VM2 and VM1, but we can limit the number of SYN packets are being sent to VM1 to avoid congestion.



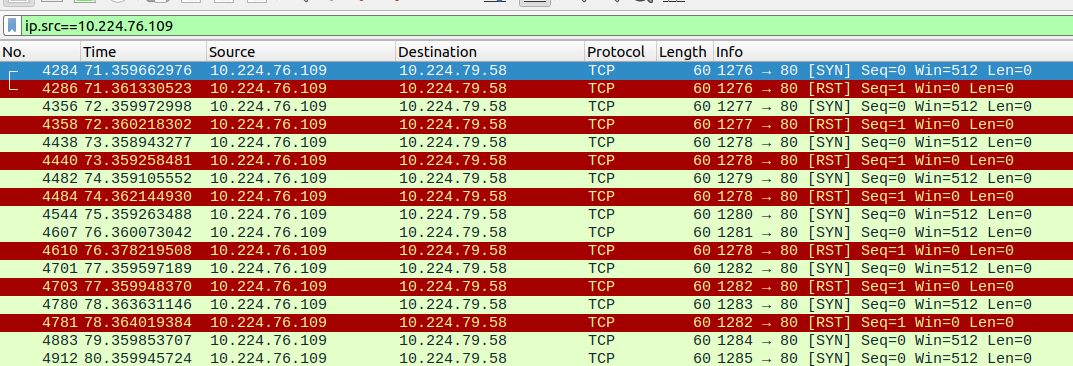
*–hashlimit-above* sets the threshold. Here, I set 10 SYN packets/min

*–hashlimit-mode srcip* limits based on source IP address

​​ *–hashlimit-burst* parameter determines how many packets are allowed to arrive in quick succession before the rate limit is applied.

This rule will drop incoming TCP SYN packets if the rate from a source IP exceeds 10 per minute, allowing for an initial burst of up to 5 packets.

On checking the wireshark capture:



Since the limiting is set, some of the TCP SYN packets are denied and some of the TCP SYN packets are acknowledged.

1. Once the rule is in place, repeat Q3 and Q4. Do you see the packets from VM2 now? Why or why not? **[10 points]**

Without any rate limiting in place, I do not see any packets from VM2. This was because we have a firewall rule in place that blocks all TCP packets sent from VM2 to VM1 in the above step.

However, with rate limiting in place, some of the TCP packets were acknowledged, and some sent RST flag. This was because I had set a rate limiting policy which states that anything above 10 SYN packets a minute should be dropped.

1. How do you check the firewall rules are effectively in place? Paste the command used. **[10 points]**

I used sudo **iptables -L -n** to check if the firewall rules are effectively in place

****

**References for Objective 2:**

**HPING3**: <https://techyrick.com/hping3-full-tutorial-for-dummies-to-pro/>

**Add rule using Iptables**: <https://upcloud.com/resources/tutorials/configure-iptables-ubuntu>

# Report Questions: (105)

1. What is an intrusion detection system? **[10 points]**

An Intrusion Detection System (IDS) is a security technology designed to monitor and analyze network or system activities for signs of unauthorized access, malicious activities, or security policy violations. The primary purpose of an IDS is to detect and respond to potential security threats in real-time or near real-time.

There are two main types of Intrusion Detection Systems:

* **Network-based Intrusion Detection System (NIDS):**

Functionality: Monitors network traffic and analyzes packets to identify suspicious patterns or signatures.

Deployment: Positioned at key points within a network, such as at network boundaries or critical segments.

Detection Techniques: Signature-based detection (matching patterns against a database of known attack signatures) and anomaly-based detection (identifying deviations from normal network behavior).

* **Host-based Intrusion Detection System (HIDS):**

Functionality: Monitors activities on individual hosts or devices, including file integrity, system logs, and application behavior.

Deployment: Installed on individual computers or servers.

Detection Techniques: Focuses on activities at the host level, detecting unusual behavior or changes in system files, configurations, or user activities.

Key features and functions of Intrusion Detection Systems include:

* IDS systems generate alerts or notifications when potentially malicious activities are detected. These alerts are then reviewed by security personnel for further investigation.
* IDS systems maintain logs of detected events, which can be useful for forensic analysis, compliance reporting, and ongoing security monitoring.
* IDS systems operate in real-time or near real-time, allowing for quick detection and response to security incidents.

1. Explain the below terms: **[15 points]**
2. Man-in-middle attack

A Man-in-the-Middle attack occurs when an unauthorized third party intercepts and potentially alters the communication between two parties without their knowledge. The attacker positions themselves between the communicating entities, allowing them to eavesdrop on the communication, capture sensitive information, or inject malicious content into the data stream. The goals of a MitM attack may include unauthorized access to confidential information, session hijacking, identity theft, or the manipulation of communication.

1. Fabrication/Masquerade attack

In a Fabrication or Masquerade attack, an attacker impersonates a legitimate user, system, or service to gain unauthorized access or deceive others. The attacker pretends to be someone or something they are not, often using stolen credentials or deceptive techniques to appear as a trusted entity. The primary objective is to trick systems, users, or other entities into granting access or privileges, leading to potential unauthorized activities.

1. DDoS

DDoS is a type of cyber attack where multiple compromised computers are used to flood a target system, service, or network with excessive traffic, rendering it unavailable to users. The attacker controls a network of compromised devices, often referred to as a botnet, to generate a massive volume of requests or traffic, overwhelming the target's resources and causing service disruption. DDoS attacks aim to disrupt the availability of online services, websites, or networks, causing inconvenience, financial losses, or reputational damage for the target.

1. Mentions three tools or methods that can be used to detect and prevent the above-mentioned attacks **[10 points]**

**Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):**

* For MitM attacks: IDS can detect unusual patterns in network traffic, such as unexpected changes in data flow or unauthorized interception attempts. IPS can block or alert on suspicious activities related to communication interception.
* For Fabrication/Masquerade attacks: IDS examines login patterns, user behavior, and system access to identify anomalies that may indicate unauthorized access or masquerading. IPS can prevent access by blocking suspicious credentials or activities.
* For DDoS attacks: IDS monitors network traffic for sudden spikes in volume or unusual patterns indicative of a DDoS attack. IPS can employ rate limiting, traffic filtering, or redirection to mitigate the impact of DDoS attacks.

**Network Encryption:** Use encryption protocols such as SSL/TLS for securing communication channels between entities to protect against MitM attacks.

* For MitM attacks: Encryption helps prevent eavesdropping and tampering by ensuring that only authorized parties can decrypt and access the transmitted data.

**Firewalls with Advanced Threat Protection**: Firewalls monitor and control incoming and outgoing network traffic based on predetermined security rules. Advanced Threat Protection features enhance the firewall's capabilities to detect and prevent sophisticated attacks.

* For Fabrication/Masquerade attacks: Firewalls can enforce access controls and inspect traffic for anomalies, blocking unauthorized access attempts or suspicious behavior.
* For DDoS attacks: Firewalls equipped with DDoS mitigation features can identify and filter out malicious traffic, preventing it from overwhelming the target's resources.

1. Explain any four types of DoS attacks and how do you prevent them? **[40 points]**

Denial of Service (DoS) attacks aim to disrupt the availability of a service, network, or system, making it inaccessible to its intended users. Here are four types of DoS attacks and preventive measures for each:

1. **TCP/IP Flooding (SYN/ACK Flood) Attack:**

Description: Attackers flood the target system with a high volume of TCP connection requests (SYN packets) without completing the handshake, overwhelming the system's resources and preventing legitimate connections.

Prevention:

SYN Cookies: Use SYN cookies to validate incoming connection requests without allocating significant resources until the connection is established.

Rate Limiting: Implement rate-limiting mechanisms to control the rate of incoming connection requests from a single source, preventing rapid flooding.

1. **UDP Flooding (UDP Flood) Attack:**

Description: Attackers flood the target with a large number of UDP packets, causing resource exhaustion and disrupting normal service.

Prevention:

Stateful Firewalls: Use stateful firewalls to inspect and filter incoming UDP packets, allowing only legitimate and expected traffic.

Rate Limiting: Set rate limits for incoming UDP traffic to prevent overwhelming the system with an excessive number of packets.

1. **HTTP/S Flooding (HTTP/S Flood) Attack:**

Description: Attackers flood a web server with a high volume of HTTP or HTTPS requests, consuming server resources and making the website unavailable.

Prevention:

Web Application Firewalls (WAF): Deploy WAFs to filter and block malicious HTTP/S traffic, identifying and blocking common attack patterns.

Load Balancers: Use load balancers to distribute incoming traffic across multiple servers, preventing a single server from becoming a bottleneck.

1. **Ping Flood (Ping of Death) Attack:**

Description: Attackers flood the target with a large number of ICMP Echo Request (ping) packets, causing resource exhaustion and disrupting normal network operation.

Prevention:

ICMP Rate Limiting: Implement rate limiting for incoming ICMP traffic to prevent excessive ping requests.

Firewalls: Configure firewalls to filter out and block ICMP traffic that exceeds acceptable thresholds.

1. What is cryptography? Explain symmetric and asymmetric keys **[15 points]**

Cryptography is the science and practice of securing communication and information through the use of codes and ciphers. It involves the application of mathematical algorithms to transform data into a format that is unintelligible without the appropriate key. The primary goals of cryptography include confidentiality (ensuring only authorized parties can access the information), integrity (ensuring the data has not been altered), authentication (verifying the identity of communicating parties), and non-repudiation (ensuring that a sender cannot deny sending a message).

**Symmetric keys:** In symmetric key cryptography, a single key is used for both encryption and decryption. The same secret key is shared between the communicating parties. The sender uses the shared key to encrypt the plaintext, transforming it into ciphertext. The recipient uses the same shared key to decrypt the received ciphertext and recover the original plaintext.

**Asymmetric keys:** Asymmetric key cryptography uses a pair of public and private keys for encryption and decryption. Each user has a public key that is shared openly and a private key kept secret. The sender uses the recipient's public key to encrypt the message. The recipient uses their private key to decrypt the received ciphertext.

1. Explain the below network setting attachments in Virtual-Box: **[15 points]**
2. NAT

NAT is a networking mode where VirtualBox acts as an intermediary between the guest VM (Virtual Machine) and the external network. The host system's IP address is used for outgoing connections, and VirtualBox performs translation to allow communication with external networks. By default, the VM is assigned an IP address within a private network range, and the host system performs network address translation for outgoing traffic.

1. Bridged Network

In bridged networking, the guest VM appears as a separate device on the external network. It gets its own IP address from the same network as the host, making the VM directly accessible from other devices on the external network. The VM is assigned an IP address from the external network's DHCP server or can be configured with a static IP.

1. Host-only adapter

Host-only networking creates a private network that includes the host system and all guest VMs, allowing communication only within this isolated network. VMs on the same host-only network can communicate with each other using private IP addresses assigned by VirtualBox.

# Total Score = \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_285\_\_