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.

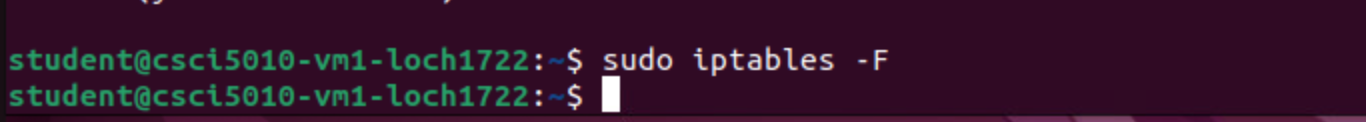
The questions in the lab are intentionally vague. The purpose of this is for you not only to research, investigate, and learn the technologies, but also become proficient at interpreting both non-technical and technical questions. Being able to research and discover answers on your own will be critical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



A screenshot of a computer

Description automatically generated

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

A screenshot of a computer program

Description automatically generated

1. What is NMAP used for? List two uses. **[5 points]**
   1. NMAP can scan for vulnerabilities on a network.
   2. NMAP can monitor host or service uptime.
2. Scan Datacom VM1 from VM2 using NMAP and explain the output. **[15 points]**A screenshot of a computer program

   Description automatically generated
   1. I did a NMAP of VM1s IP interface that is connected to the same network as VM2. The results show that all ports on VM1 are closed and it also shows that the host is up. I assume it did some sort of ping to show if it was up or not seeing that the latency is shown.
3. Install and initialize an Apache server on VM1. Mention the steps followed. **[15 points]**
4. In the terminal of VM1, type the command: sudo apt-get install apache2.
5. Type the command: sudo systemctl start apache2
6. To check if it is running, type: sudo systemctl status apache2
7. The apache2 server is now initialized.
8. Scan Datacom VM1 again using NMAP. Do you notice any difference? Why or why not? **[10 points]**
   1. I do notice one difference. There is now a port that is open on port 80. I think this is because apache2 is a service that hosts your own web server on your machine. Being that I started apache2 on VM1, that makes sense.
9. Explain the different port states available in NMAP? Explain. **[20 points]**
   1. Open: The port is open and listening for traffic
   2. Closed: There is no active service listening on the port
   3. Filtered: Cannot determine whether port is opened or closed.
   4. Unfiltered: Port is accessible, but cannot determine whether it is open or closed.
   5. Open|filtered: Unbale to determine whether the port is open or filtered.
   6. Closed|filtered: Unable to determine whether the port is closed or filtered.
   7. Unspecified: Could not determine the status of the port for several reasons.

**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]**
   1. Hping is a packet generator security testing tool
   2. Applications:
      1. Firewall Testing
      2. Advanced port scanning
      3. Network testing
2. Install hping3 on VM2. Mention the steps followed. **[5 points]**
   1. Type: sudo apt-get install hping3
3. Monitor the adapter on VM1 that connects to VM2 and analyze the packets received using Wireshark to detect attacks.
4. Send 100 TCP SYN packets to VM1. Paste the screenshot of the output and the command used. **[15 points]**

A screenshot of a computer program

Description automatically generated

(The rest of the pings sent aren’t shown as that would take many screenshots, but sequence goes to 100)

Sudo hping3 -S 10.224.79.42 -p 80 -c 100

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]**

A screenshot of a computer

Description automatically generated

This Wireshark capture shows the SYN packets sent to VM1 by VM2 using hping.

A screenshot of a computer program

Description automatically generated

Rules show above

A screenshot of a computer

Description automatically generated

I ran the hping command on VM2 once again and here is the wireshark capture from VM1.

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]**

I do see the packets incoming from VM2, but now we are not sending a response. We only see the SYN packets but VM1 is not sending back SYN-ACK packets.

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

Sudo iptables -L –line-numbers

This is how I saw which firewall rules are in place and by what order they get put 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]**
   1. An IDS is a system that detects any security vulnerabilities on a target device. It is a passive device that is placed out of band of the network and notifies when there is a vulnerability.
2. Explain the below terms: **[15 points]**
3. Man-in-middle attack
   1. When a third-party intercepts information from two host communicating with each other without the hosts knowing of the fact. The attacker can manipulate data or just listen on what the hosts are doing.
4. Fabrication/Masquerade attack
   1. This is when an attacker impersonates someone or provides a false identity to get information from someone. For example, someone could impersonate a CEO of a company and try to communicate with one of the employees to get sensitive information.
5. DDoS
   1. A distributed denial of service or DDOS is when an attacker sends an overwhelming amount of traffic to a device to crash the target device. This could be done by getting access to a large amount of devices that can then ping a target and overwhelm it with requests.
6. Mentions three tools or methods that can be used to detect and prevent the above-mentioned attacks **[10 points]**
   1. An IDS would be a great way to prevent these attacks by analyzing patterns and malicious traffic.
   2. A firewall with specific rules of what traffic can flow on the network would also be a great prevention of these attacks. You could set rules that only allow for certain traffic to come in and prevent malicious traffic trying to enter.
   3. If these attackers were trying to intercept wireless traffic like the MITM attack, implementing a strong WPA3 password would prevent attackers like this from accessing the wireless network in the first place.
7. Explain any four types of DoS attacks and how do you prevent them? **[40 points]**
   1. HTTP flood attack
      1. Where an attacker sends an overwhelming amount of HTTP requests to a target website
      2. Prevention:
         1. Implement a web application firewall that can look for abnormal patterns and limit the rate of incoming HTTP requests as to not overwhelm the server
   2. Ping flood attack
      1. This type of DoS involves sending a large amount of ICMP requests to a target to crash it.
      2. Prevention
         1. Implementing an IDS and rate limiting will mitigate this type of attack.
   3. UDP amplification attack
      1. This is where an attacker spoofs the IP of a target device and sends a bunch of UDP packets to amplification targets. The targets then respond with a huge response of UDP packets and overwhelm the target.
      2. Prevention:
         1. Implement packet filtering on the network to not allow packets incoming from vulnerable sources.
   4. SYN/ACK flood attack
      1. The attacker sends a large amount of SYN packets to a target without the goal of sending back an ACK, in which this crashes the target device.
      2. Prevention:
         1. Add cookies to the SYN packet so when sending SYN packets to the client, it can verify via the cookie that it is coming from a legit source.
8. What is cryptography? Explain symmetric and asymmetric keys **[15 points]**
   1. Cryptography is the process of encoding a message so that only the receiver can decipher and read your message.
   2. Symmetric keys
      1. When sending an encoded message, symmetric keys are used both for encryption and decryption.
   3. Asymmetric keys
      1. For asyemmtric keys, there is a pair of keys: a public and private key. The public key is widely known and is used to decrypt the message, while the private key is kept secret and can decrypt that message.
9. Explain the below network setting attachments in Virtual-Box: **[15 points]**
10. NAT
    1. NAT or network address translation in this scenario allows for the VM in Virtual Box to connect to external networks via the hosts IP address. The host acts as a router, and the VM is allowed to access external resources from there.
11. Bridged Network
    1. A bridged network allows for the VM to have its own unique IP address on the same network as the host, and acts like a totally separate machine on the network.
12. Host-only adapter
    1. The host-only adapter setting sets the VM and host to its own detached network. Only the host and the VM can communicate with each other in this scenario.

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