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]**
2. Install NMAP on VM2. How will you check the version of NMAP installed? Paste screenshots **[5 points]**
3. What is NMAP used for? List two uses. **[5 points]**
4. Scan Datacom VM1 from VM2 using NMAP and explain the output. **[15 points]**
5. Install and initialize an Apache server on VM1. Mention the steps followed. **[15 points]**
6. Scan Datacom VM1 again using NMAP. Do you notice any difference? Why or why not? **[10 points]**
7. Explain the different port states available in NMAP? Explain. **[20 points]**

**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]**
2. Install hping3 on VM2. Mention the steps followed. **[5 points]**
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]**
5. 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]**
6. Once the rule is in place, repeat Q3 and Q4. Do you see the packets from VM2 now? Why or why not? **[10 points]**
7. How do you check the firewall rules are effectively in place? Paste the command used. **[10 points]**

**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]**
2. Explain the below terms: **[15 points]**
3. Man-in-middle attack
4. Fabrication/Masquerade attack
5. DDoS
6. Mentions three tools or methods that can be used to detect and prevent the above-mentioned attacks **[10 points]**
7. Explain any four types of DoS attacks and how do you prevent them? **[40 points]**
8. What is cryptography? Explain symmetric and asymmetric keys **[15 points]**
9. Explain the below network setting attachments in Virtual-Box: **[15 points]**
10. NAT
11. Bridged Network
12. Host-only adapter

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