**Lab 6**

**Firewall**

**Outcome**: Introduction to Firewalls

**Objectives**:

1. Allow and Block ports using the basic firewall in a Linux platform.

2. Use Nmap as a vulnerability scanner

**Task 1: Allow and Block ports using the basic firewall in a Linux platform.**

In this task you will be using the basic firewall setting present in Alpine Docker container to Allow and Deny traffic to different ports. For this purpose, you will require, two Docker containers.

1. Install Alpine Docker container:
   1. Open a first terminal (terminal 1) and run the following command:



* 1. Open a second terminal (terminal 2) and run the following command:



1. In Terminal 1, Type the below command:



Write down the IP address of your Docker container on terminal 1.

1. In Terminal 2, Type the below command:



Write down the IP address of your docker container on terminal2.

1. In Terminal1, execute the following commands. **Explain each command**



1. Write an additional rule that prevents the creation of DNS connections that use port 53 and UDP protocol. **Provide a screenshot.**
2. Type the below command, **explain it**



1. Use the following command to view the rules added to the firewall, **Provide a screenshot.**:



* **Which protocol uses port 80?**
* **Which protocol uses port 22?**
* **Which protocol uses port 25?**

1. Now switch to terminal 2. and Run the command:



1. Use the below command to scan the specified IP Address using the Nmap application, **Provide a screenshot of the output.**



# What is nmap? What is it used for?

* **What is the output displayed?**
* **Explain the difference between filtered ports and closed ports?**
* **Why is the HTTP port filtered while SSH and SMTP ports are closed?**

1. Switch to terminal 1 and run the following command to start ssh service on Terminal1.



1. Switch back to Ttrminal2 and run the following command to scan Terminal 1 container again



# − how is the output different from the nmap scan in step 7 (the first Nmap scan)?

1. Go back to terminal 1 and type the following commands to reset the firewall. **Why have we repeated this command 5 times?**

INPUT 1

1. Type the following command, **what does the below command do?**



1. Use the below command to confirm the changes. **Provide a screenshot.**



1. Now switch to terminal2 and type:



# − Provide a screenshot of the output What is your observation? And how does it vary from step 7 (the first nmap scan)?

**Task 2: Vulnerability assessment**

# We can extend the use of Nmap as vulnerability scanner by using NSE (Nmap Scripting Engine) scripts. We will use Vulscan which is a module that enhances nmap to a vulnerability scanner. It includes the following databases:

# scipvuldb.csv - https://vuldb.com

# cve.csv - https://cve.mitre.org

# securityfocus.csv - https://www.securityfocus.com/bid/

# xforce.csv - https://exchange.xforce.ibmcloud.com/

# expliotdb.csv - https://www.exploit-db.com

# openvas.csv - http://www.openvas.org

# securitytracker.csv - https://www.securitytracker.com

# osvdb.csv - http://www.osvdb.org

# On terminal 2, run the following commands:

# 

# Select any of the reported vulnerability, and describe it (description, impact, affected versions, solution)