EN4720: Security in Cyber-Physical Systems
Exercise — Infrastructure Security

Name: Thalagala B. P.
Index No: 180631J

June 15, 2023

This is an individual exercise!
Due Date: 20 June 2023 by 11.59 PM

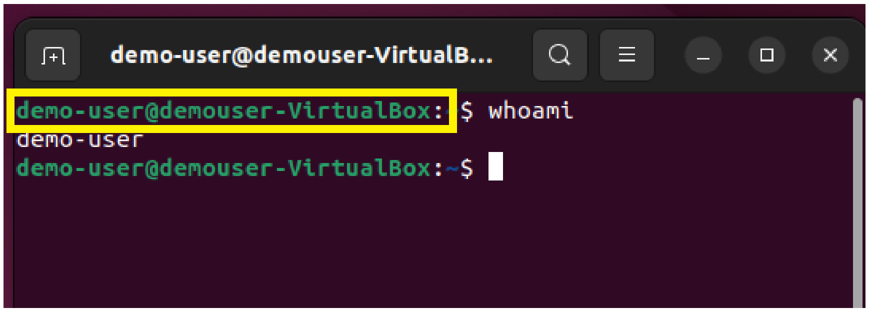
This exercise has to be carried out using a Linux-based PC/virtual machine. Read all the instructions and questions before attempting the exercise. Add answers under each question and submit the resulting PDF.

Section 1

In this section, you will implement Firewall rules using **iptables** and **ufw** Linux commands. Moreover, you will scan network ports of a remote device using **nmap** Linux command.

For all the questions in this section, add a screenshot of the terminal (including all the commands you ran to perform the task) unless specified otherwise. The evaluator should be able to see each step that you followed to perform each task. In all screenshots, the areas marked (which are unique to your terminal display) in Figure 1 (the sample answer to Question 1) must be visible.

1. View the currently logged in user.



```
demo-user@demouser-VirtualBox:~$ whoami
demo-user
demo-user@demouser-VirtualBox:~$
```

Figure 1: Sample Terminal Output

Creating Firewall Rules with iptables

2. Use `dpkg -l | grep iptables` command to check whether iptables is installed on your system. If it does not existing in your system, install it by running `sudo apt-get install iptables`.

   Your answer here

3. Check all available iptables rules in your system using the command `/sbin/iptables -n -L` .

   Your answer here

4. Save all available iptables rules to a file named **iptablesRule.v4** using `iptables-save` command.

   Your answer here

5. Flush all the iptables rules that exist in your system and set a default policy to drop packets.

   Your answer here

6. Set iptables rules to permit input and output DNS traffic in your system.

   Your answer here

7. Add iptables rules to accept local network incoming and outgoing traffic from the network 192.168.1.0/24.

   Your answer here

8. Configure iptables rules to allow all HTTP traffic.

   Your answer here

9. View all iptables rules in your system and save them to a file **iptablesRuleNew.v4**.

Your answer here

10. Create a file called **iptablesCommands.sh** and put all commands you ran from steps 4, 5 and 6 in the file. After creating the file, flush your iptables commands again and run **iptablesCommands.sh** file. View the iptables rules now and compare with the previous result.

    Your answer here

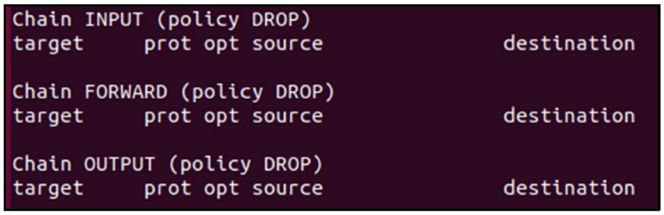
11. Finally, flush your iptables rules again. But this time, load the saved iptables rules from the file **iptablesRuleNew.v4** using `iptables-restore` command. View the iptables rules and compare them with the ones you have in step 8.

    Your answer here

Creating Firewall Rules with UFW

The scenario comprises of two virtual machines (VM1 IP - 192.168.46.140 and VM2 IP - 192.168.46.141) running on a host (HOST IP - 192.168.46.1) machine. VM1 is an Ubuntu virtual machine that has a firewall implemented/configured.

The current firewall ruleset is as below.



```
Chain INPUT (policy DROP)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
```

All chain policies are set to drop traffic. To implement base rules, you can use the following commands:

- Delete any current rules associated with UFW using `sudo ufw reset`
- Disable UFW using `sudo ufw disable`
- Flush all iptables rules using `sudo iptables -F`
- Enable UFW using `sudo ufw enable`
- Deny outgoing traffic using `sudo ufw default deny outgoing`

12. Implement the following network administration in VM1:

    - Access to VM1 from VM2 must only be allowed over FTP and Telnet.
    - Access to VM1 from HOST must only be allowed over SSH
    - Allow all outgoing traffic from VM1 with the exception of access to HTTP websites

    In this task, you are asked to implement UFW rules on the ubuntu machine. You can pretend that VM2 and HOST exist in your network. List the commands you used to achieve the above. Add a screenshot of the terminal output after running the command `sudo ufw status numbered`.

    If the firewall is physically implemented, you could have tested the connections using PuTTY or the command line.

    Your answer here

Scan systems with NMAP

In this section, you will scan for the Ports of a remote host. You will need to have two devices connected to the same local network to perform this task.

13. View ip addresses of both devices using `hostname -I` command.

    Your answer here

14. Scan one host from the other host for TCP and UDP ports using `nmap` command.

    Your answer here

Section 2

15. Briefly explain VLANs, VPNs, DMZs and Network Segmentation concepts outlining their similarities and differences.

    Your answer here

16. Perform a comparison between IPsec and SSL.

Table 1: Comparison of IPsec and SSL

IPsec	**SSL**
Your answer here	Your answer here
Your answer here	Your answer here

17. Explain the differences between an IDS, an IPS, and a firewall?

    Your answer here

18. What is the difference between anomaly detection and signature or heuristic-based intrusion detection?

    Your answer here