VICTORIA UNIVERSITY OF WELLINGTON
TE HERENGA WAKA

CYBR371: System and Network Security
2024– T1

Arman Khouzani, Mohammad Nekooei

Lab 4: Packet Filtering Firewall

Submission Deadline: ***23:59:00 (NZST) on Sunday, 12 May 2024***

Question:	1	2	3	4	5	6	7	8	9	Total
Points:	4	4	4	6	6	4	4	4	4	40
Score:										

1 pfSense Firewall

Complete the following labs on **`netlab`** (access them through **`Nuku`**, under **`modules`**) and answer the questions accordingly:

- **Configuring a Network-Based Firewall**

Q.1. [4 points] Explain why the **`ping`** command in "Step 23" of "Section 1" of the lab fails. [100 words max]

Q.2. [4 points] Compare the screenshot in "Step 1" of "Section 2.1" of the lab with the screenshot in "Step 1" of "Section 2.2". Identify the difference, and then, explain why we see this difference. [100 words max]

Q.3. [4 points] In "Step 5" of Section 2.2 of the lab, explain why we do not see the SSH service.

Q.4. [6 points] Is **`pfsense`** a stateful or stateless firewall? Demonstrate the statefullless or the statelessness of **`pfsense`** firewall using the lab "Configuring a Network-Based Firewall". You may include a screenshot. [250 Words Max]

2 Walking on Firewalls!

- **Testing Firewall Rules with Firewalking**

Q.5. [6 points] What is Firewalking (the technique and/or the tool) and how can it be used in an attack process against a potential target? [250 Words Max]

3 Packet Filtering by `iptables`

Complete the following lab on **`netlab`** and answer the questions accordingly:

- **Configuring a Packet Filtering Firewall**

Q.6. [4 points] We have the following rule in our iptables on the server (`192.168.1.1`). The client (`192.168.1.78`) however fails to initiate an SSH connection. Explain why this is the case.

```
sudo iptables -A INPUT -p tcp -s 192.168.1.78 -d 192.168.1.1
    --dport 22 -i "enp0s3" --j ACCEPT
sudo iptables -A OUTPUT -p tcp -s 192.168.1.78 --sport 22
    -d 192.168.1.1 --dport 22 ACCEPT
sudo iptables -P INPUT DENY
sudo iptables -P OUTPUT DENY
```

Q.7. [4 points] Our server is running a Telnet service listening on port 23. We would like to stop any new Telnet connections from a client with the IP address of `10.0.2.5`. Is the following a good rule to block the Client? Explain.

```
sudo iptables -A INPUT -s 10.0.2.5 -p tcp --sport 23 -j DROP
```

Q.8. [4 points] Write a rule to drop all the new and established outgoing SSH service requests received on your primary interface (eth0) which has a source MAC address of `30:65:EC:22:14:D1`.

Q.9. [4 points] Write a rule to drop any incoming packets with "`INVALID`" state.