Lab 1: Virtualised Infrastructures

A Challenge

Our challenge is to set up MyBank Incorp, where each of you will be allocated a network and hosts to configure and get online (Figure 1). You have a pfSense firewall, a Ubuntu (Private) host, a Windows (DMZ) host, a Metasploitable (DMZ) host, a Kali (DMZ) host and a Kali (Public) host to achieve your objectives.

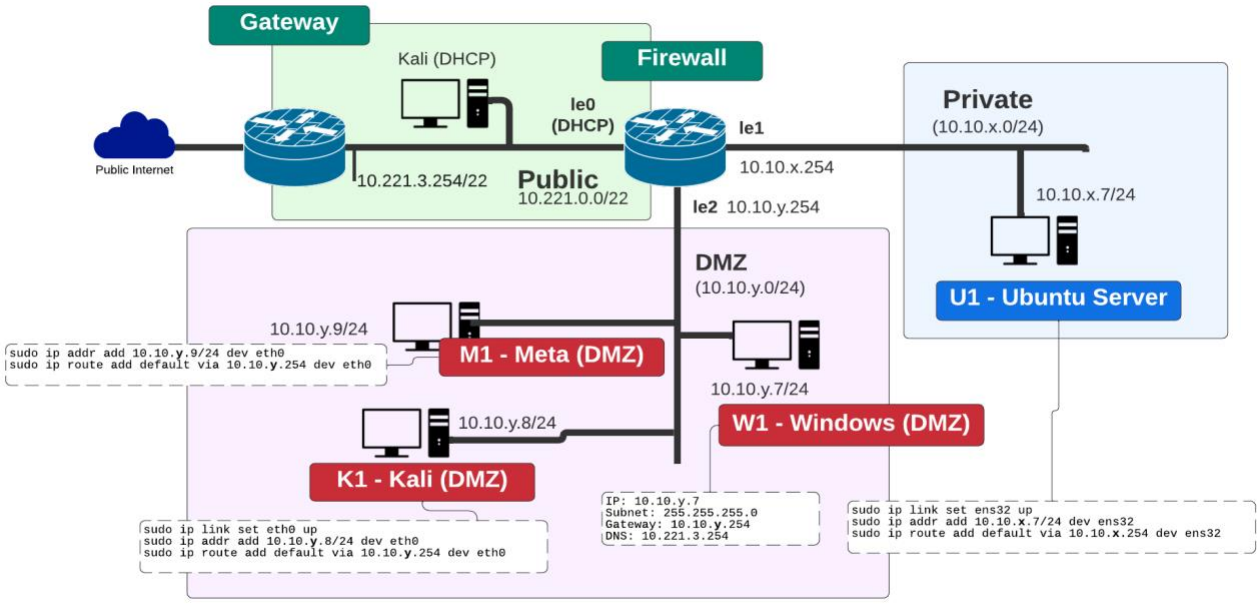

Figure 1: My Bank architecture

B Quick guide

For Ubuntu configuration, for 10.10.x.7:

```
sudo ip link set ens160 up
sudo ip addr add 10.10.x.7/24 dev ens160
sudo ip route add default via 10.10.x.254 dev ens32
nano /etc/resolv.conf and change "nameserver 146.176.1.5"
```

C Setting up the network

In this lab, we will connect our firewall to the main gateway and be able to complete the challenges in Table 1. You will be given two things:

Group Number:

Your networks will be: 10.10.x.0/24 10.10.y.0/24

Demo: here

D Initial Firewall Creation

Power up your Pfsense firewall and the rest of the hosts (do not power up the Vyatta firewall). Select the Pfsense firewall terminal Do not set VLANs, and enable the interfaces of:

- vmx0. WAN.
- vmx1. Private.
- vmx2. DMZ

Let the firewall boot up, and then select (2) Setup IP Interface(s), and set the LAN interface to have an IP address of 10.10.x.254/24.

Now we will configure the hosts to sit on the Private and DMZ networks.

E Ubuntu setup

Set up the Ubuntu host to have an IP address of 10.10.x.7/24 (for the ens160 network adaptor) with a default gateway of your firewall port (10.10.x.254/24).

```
sudo ip link set ens160 up
sudo ip addr add 10.10.x.7/24 dev ens160
sudo ip route add default via 10.10.x.254 dev ens160
```

Next setup the nameserver on the Ubuntu host by editing the /etc/resolv.config and adding a nameserver of 146.176.1.6:

```
sudo nano /etc/resolv.conf
```

then add:

```
nameserver 146.176.1.5
```

1. Can you ping the default gateway?	Yes/No
2. Can you ping the main gateway (10.221.3.254)?	Yes/No
3. Can you ping the 8.8.8.8?	Yes/No
4. Can you ping the google.com?	Yes/No
5. Run "nslookup google.com". What IP address does it give?	
6. Open a browser and navigate to google.com. Can you access the site?	Yes/No

If any of these answers is No, you need to debug your network and find the problem. By default, all traffic is allowed to flow from the Private network to the other network, so we do not have to enable any firewall rules. If (1) does not ping, you have a basic connectivity problem and need to check your network adaptor on Ubuntu for its IP address and subnet mask. If (2) doesn't work, you have a problem with your default gateway on Ubuntu, so check that the default gateway of Ubuntu is set of the LAN port of the firewall. If (3) doesn't work, you have a general problem with your firewall, so check the details on the pfSense firewall. If (4) doesn't work, but (3) does, you have a problem with your DNS service, so check the DNS details on the Ubuntu host.

F Windows 7 host setup

On the Windows 7 server, modify the static address on the network interface with:

```
IP: 10.10.y.7
Subnet mask: 255.255.255.0
Gateway: 10.10.y.254
DNS: 146.176.1.5
```

1. Can you ping the default gateway?	Yes/No

The answer to this should be No, as we have not setup the firewall yet for this network port. Also, the firewall will block the traffic by default until we enable it with firewall rules.

G Firewall setup

We will now configure of the firewall. For this, log into the firewall from the Ubuntu host on the Private zone by opening a browser and entering:

```
http://10.10.x.254
```

The username for pfSense is admin and the password is pfsense.

Next, navigate to the Interfaces menu item and then set up the required IP on the DMZ (10.10.y.254/24) and subnet mask. Note that by default the DMZ is named with the OPT network name.

1. Go to the pfSense terminal, and check that the right address is set for DMX2 (10.10.y.254/24). Is it correct?	Yes/No
2. Go to the Windows 7 server. Can you ping the default gateway (10.10.y.254/24)?	Yes/No

The answer to this should still be No, as the firewall will block the traffic by default until we enable it with firewall rules.

Now go to the Rules menu option, and add a rule that will allow ICMP traffic on the DMZ network.

1. Can you ping the default gateway (10.10.y.254)?	Yes/No
2. Can you ping the main gateway (10.221.3.254)?	Yes/No
3. Can you ping the 8.8.8.8?	Yes/No
3. Can you ping the google.com	Yes/No

The answer to the first three should now be Yes, but the last one should be No, as the firewall will be blocking DNS traffic. For this we need to enable Port 53 UDP traffic from the DMZ. As we did before, go and enable this rule on the firewall, and commit it.

1. Can you ping the default gateway?	Yes/No
2. Can you ping the main gateway (10.221.3.254)?	Yes/No
3. Can you ping the 8.8.8.8?	Yes/No
4. Can you ping the google.com?	Yes/No

5. Run "nslookup google.com". What IP address does it give?	
6. Open a browser and navigate to google.com. Can you access the site?	Yes/No

The answers to the first five should be Yes, but the last one will be No, as we have not enabled HTTPS (Port 443) on the DMZ.

Now, set a rule to allow traffic from Port 443 on the DMZ.

1. Can you ping the default gateway (10.10.y.254)?	Yes/No
2. Can you ping the main gateway (10.221.3.254)?	Yes/No
3. Can you ping the 8.8.8.8?	Yes/No
4. Can you ping the google.com?	Yes/No
5. Run "nslookup google.com". What IP address does it give?	
6. Open a browser and navigate to google.com. Can you access the site?	Yes/No

The answer to each of these should be Yes.

H Kali host setup

Now we will setup the Kali host on the DMZ. Set up the Kali host to connect to 10.10.y.8/24 with a default gateway of your firewall port (10.10.y.254/24).

```
sudo ip link set eth0 up
sudo ip addr add 10.10.y.8/24 dev eth0
sudo ip route add default via 10.10.y.254 dev eth0
```

Next setup the nameserver on the Kali host by editing the /etc/resolv.config and adding a nameserver:

```
sudo nano /etc/resolv.conf
```

then add:

```
nameserver 10.221.3.254
```

1. Can you ping the default gateway (10.10.y.254)?	Yes/No
2. Can you ping the Windows 7 (10.10.y.7)?	Yes/No
3. Can you ping the main gateway (10.221.3.254)?	Yes/No
4. Can you ping the 8.8.8.8?	Yes/No
5. Can you ping the google.com?	Yes/No
6. Run "nslookup google.com". What IP address does it give?	
7. Open a browser and navigate to google.com. Can you access the site?	Yes/No

The answer to these should be Yes. If not, you will have to check your configuration.

I Metasploitable host setup

Next setup your Metasploitable host on the DMZ (User: msfadmin, Password: napier123). Set up the Metasploitable host to connect to 10.10.y.9/24 with a default gateway of your firewall port (10.10.y.254/24).

```
sudo ip addr add 10.10.y.9/24 dev eth0
sudo ip route add default via 10.10.y.254 dev eth0
```

1. Can you ping the default gateway (10.10.y.254)?	Yes/No
2. Can you ping the Windows 7 (10.10.y.7)?	Yes/No
3. Can you ping the Kali DMZ (10.10.y.8)?	Yes/No
4. Can you ping the main gateway (10.221.3.254)?	Yes/No
5. Can you ping the 8.8.8.8?	Yes/No
6. Can you ping the google.com?	Yes/No

The answer to these should be Yes. If not, you will have to check your configuration.

J Kali (Public) host setup

On the Kali public host, verify that it can ping the default gateway (10.221.3.254), 8.8.8.8 and also google.com?

1. What is the IP address of your Kali (Public) host?	
2. Can you ping 10.221.3.254?	[Yes/No]
3. Can you ping 8.8.8.8?	[Yes/No]
4. Can you ping Google.com?	[Yes/No]
5. Can you access Google.com from a browser?	[Yes/No]

The answer to these should be Yes.

K Final check of connectivity

Go back to your Windows 7 host, and check that you can ping all of the hosts on the network.

1. Can you ping all the hosts and the firewall ports?	Yes/No

Go back to your Ubuntu host, and check that you can ping all of the hosts on the network.

1. Can you ping all the hosts and the firewall ports?	Yes/No

L Running NMAP to discover services

From Ubuntu, run nmap and discover the services that are running on Windows 7.

1. Do you get a range of services shown?	Yes/No

2. Name three services that are running on Windows 7?	

You should get a range of services here, as the firewall will be open from the Private network to the DMZ.

From Windows 7, run nmap and discover the services that are running on Ubuntu.

1. Do you get a range of services shown?	Yes/No

You should not get a range of services here, as the firewall will be closed from the DMZ network to the Private network (apart from HTTPS - which we enabled earlier.

From Windows 7, run nmap and discover the services that are running on Ubuntu.

1. Do you get a range of services shown?	Yes/No

Go to the firewall, and enable all the TCP and UDP ports from the DMZ to the Private network.

From Windows 7, run nmap and discover the services that are running on Ubuntu.

1. Do you get a range of services shown?	Yes/No
2. Name three services that are running on Ubuntu?	

You should now get a range of services shown.

From Windows 7, run nmap and discover the services that are running on Metasploitable.

1. Do you get a range of services shown?	Yes/No
2. Name three services that are running on Metasploitable?	

You should now get a range of services shown.

M Final connectivity

From Ubuntu, open up a browser, and connect to the Web server on Windows 7.

1. Can you view the Web server?	Yes/No

From Windows 7, open up a browser, and connect to the Web server on Ubuntu.

1. Can you view the Web server?	Yes/No

From Windows 7, open up a browser, and connect to the Web server on Metasploitable.

1. Can you view the Web server?	Yes/No

Appendix

User logins:

Ubuntu:- User: napier, Password: napier123
Kali:- User: root, Password: toor
Windows:- User: Administrator, Password: napier123
pfsense:- User: admin, Password: pfsense
Metasploitable:- User: msfadmin, Password: napier123