Lab 2: Creating Secure Architectures

A Challenge

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

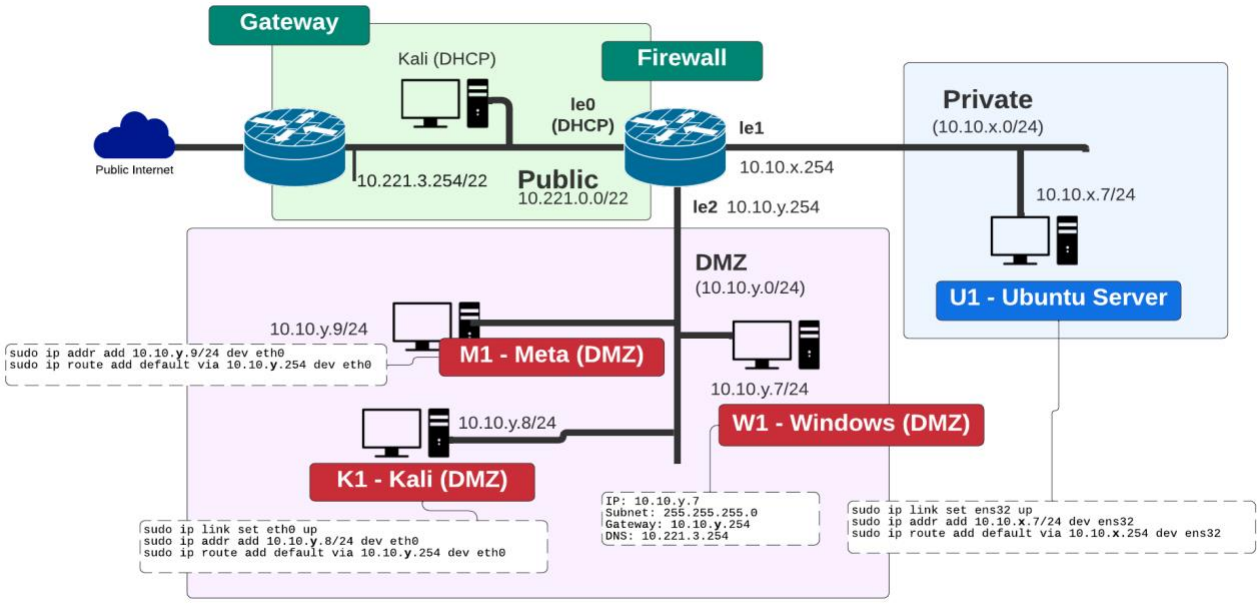

Figure 1: My Bank architecture

A Setting up the network

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

Your networks will be: 10.10.*x*.0/24 10.10.*y*.0/24 Demo: https://youtu.be/g7dzDM4aU0k

Setup the network as you did in Lab 1, but remove any firewall rules that you have on the DMZ port of the firewall.

B Investigate NAT

Now we will investigate NAT on the device.

Run packet capture on the firewall, and then ping from both the Windows host and the Ubuntu host. Stop the trace.

Which IP address appears in the pings?

Why is it just a single address?

Now we will investigate the routing table on the firewall.

On the firewall, investigate the firewall, and identify how the device makes decisions on the routing of data packets. What is the default gateway?

Now we will investigate the Metasploitable host.

Run NMAP from Windows to Metasploit. Which services are enabled:

[ftp][ssh][telnet][smtp][domain][http][vnc]

Run NMAP from Ubuntu to Metasploit. Which services are enabled:

[ftp][ssh][telnet][smtp][domain][http][vnc]

Now we will investigate the Metasploitable host for Telnet:

From Windows run Wireshark and capture packets. Now log into Metasploitable using telnet:

```
telnet 10.10.y.9
```

Can you log into each into Metasploit: [Yes/No]

Stop Wireshark and examine the data packets. Can you find the Telnet login session, and can you discover the password used? [Yes/No]

From Ubuntu run Wireshark and capture packets. Now log into Metasploitable using telnet:

```
telnet 10.10.y.9
```

Can you log into each into Metasploit: [Yes/No]

Stop Wireshark and examine the data packets. Can you find the Telnet login session, and can you discover the password used? [Yes/No]

Note: login for Telnet in Metasploitable is User: msfadmin, Password: napier123

Now we will investigate the Metasploitable host for Telnet:

From Windows, run Wireshark and capture packets. Now log into Metasploitable using SSH:

```
ssh 10.10.y.9 -l msfadmin
```

Can you log into each into Metasploit: [Yes/No]

Stop Wireshark, and examine the data packets. Can you find the Telnet login, and can you discover the password used? [Yes/No]

From Ubuntu run Wireshark and capture packets. Now log into Metasploitable using SSH:

```
ssh 10.10.y.9 -l msfadmin
```

Can you log into each into Metasploit: [Yes/No]

Stop Wireshark and examine the data packets. Can you find the SSH login session, and can you discover the password used? [Yes/No]

Note: in Wireshark, use tcp.port==23 as a filter for Telnet and use tcp.prt==22 as a filter for SSH.

C NMAP

Run Wireshark on both hosts. Now run NMAP from the Ubuntu host to the Windows host, and from the Windows host to the Ubuntu host.

What IP addresses are used in the source addresses of the scan?

Which services have been identified from the Ubuntu host to the Windows host?

Which services have been identified from the Windows host to the Ubuntu host?

Why are these different in their scope? Where is the blocking happening?

Now enable **http (Port 80), https (Port 443), and ftp (Port 21)** from the DMZ to the Private network.

Re-do NMAP. How are the scans different?

Can you now access the Web server from the Ubuntu host to the Windows host?

Can you now access the Web server from the Windows host to the Ubuntu host?

Access Google.com from the Ubuntu host and also the Windows host.

Can you access it? If not, on the firewall, **enable UDP/TCP DNS** (Port 53) from the DMZ and also from the Private network. Add logging on the rule.

Can you now access Google.com from the Ubuntu host and also from the Windows host?

On the firewall, examine the log and view the accesses for a DNS lookup on Google.com. Which addresses are present?

D Identifying Services

Within a network infrastructure we have services which run on hosts. These services provide a given functionality, such as for sending/receiving email, file storage, and so on.

From → To	Command	Observation
DMZ	On your Windows host, run the command: `netstat –a` and outline some of the services which are running on your host (define the port number and the name of the service and only pick off the LISTENING status on the port).	Outline some of the services which are running on your host (define the port number and the name of the service):
LAN	For the Ubuntu Virtual Machine, and run the command: `netstat –l`	Outline some of the services which are running on your host (define the port number and the name of the service):
DMZ	Next we will determine if these services are working. There should be a Web server working on each of the virtual machines (Ubuntu and Windows 7), so from the Windows host and using a Web browser, access the home page: `http://10.10.x.7`	Is the service working: [Yes] [No]
LAN	From Ubuntu, access the Web server at: `http://10.10.y.7`	Is the service working: [Yes] [No]
LAN	Next we will determine if these services are working using a command line. From your UBUNTU host, undertake the following: `telnet 10.10.y.7 80` then enter: `GET /`	Outline the message that is returned:
DMZ	Repeat the previous example from the WINDOWS host: `telnet 10.10.x.7 80`	
DMZ	There should be an FTP server working on Ubuntu and Windows 7. From WINDOWS, access the FTP server on the UBUNTU server: `telnet 10.10.x.7 21`	Outline the messages that you received:

	then enter:
	
	`USER napier`
	`PASS napier123`
	`PWD`
	`QUIT`
		What happens to each of these when you try with an incorrect username and password:
		
		Which status code is used for each command that you enter:

LAN	From UBUNTU access the WINDOWS host with
	
	`telnet 10.10.x.7 21`
	
	then enter:
	
	`USER napier`
	`PASS napier123`
	`PWD`
	`QUIT`
		Outline the messages that you received:
		
		What happens to each of these when you try with an incorrect username and password:
		
		Which status code is used for each command that you enter:

DMZ	On the UBUNTU instance you will see that the **VNC** service is running. From your WINDOWS host, access the VNC service using a VNC client, and see what happens (and the password for vnc is "napier"). Note: you may have to open up the DMZ for Port 5900.	What does this service do:

E Enumeration – Host scan

Nmap is one of the most popular network scanning tools. It is widely available, for Windows and Ubuntu/Unix platforms, and has both a Command Line Interface (CLI) and a Graphical User Interface (GUI).

From → To	Command	Observation
LAN to WAN	**`sudo nmap –sP –r 10.221.0.0/24`**	Which hosts are on-line:
LAN to DMZ	**`sudo nmap –sP –r 10.10.y.0/24`**	Which hosts are on-line:
DMZ to LAN	**`nmap –sP –r 10.10.x.0/24`**	Which hosts are on-line:
LAN to DMZ	Run Wireshark on host in LAN, and run: **`sudo nmap –sP –r 10.10.y.0/24`**	Which transport layer protocol does NMAP use to discover the host: [ICMP] or [ARP]
LAN to LAN	Run Wireshark on host in LAN, and run: **`sudo nmap –sP –r 10.10.x.0/24`**	Which transport layer protocol does NMAP use to discover the host: [ICMP] or [ARP]

F Enumeration - Operating System Fingerprinting

Enumeration is the gathering of information about target hosts. After discovering live target systems, we want to identify which machines are running which OSs. A useful feature of **nmap**, is determining the operating system of hosts on the network. It performs active OS fingerprinting by sending packets to the target system.

From → To	Command	Observation
LAN to DMZ	Perform an OS Fingerprint Scan on some of the hosts discovered on the network, using a command such as: `sudo nmap –O 10.10.y.0/24`	Which operating systems does it return:
DMZ to LAN	Perform an OS Fingerprint Scan on some of the hosts discovered on the network, using a command such as: `nmap –O 10.10.x.0/24`	Which operating systems does it return:

I Enumeration – Application Fingerprinting

Application Fingerprinting or **Banner Grabbing** covers techniques to enumerate OSs and Applications running on target hosts. An attacker or security tester would be specifically looking for versions of applications and operating systems which have vulnerabilities. **Nmap** can be used to check applications and versions for network services running on the target for the open ports it finds during a port scan.

From → To	Command	Observation
LAN to DMZ	Perform an application and version scan for networked services: `sudo nmap –sS 10.10.y.7/24`	Which services are running on the Windows host:
DMZ to LAN	Perform an application and version scan for networked services: `nmap –sS 10.10.x.7/24`	Which services are running on the Linux host:
LAN to DMZ	Scan the Web server in the DMZ for its version: `sudo nmap –sV 10.10.y.7/24 –p 80`	Which Web server type is being used:

DMZ to LAN	Scan the Web server in the LAN for its version: `nmap -sV 10.10.x.7/24 -p 80`	Which Web server type is being used:

Telnet is another tool commonly used for banner grabbing. Once open ports have been found using a scanner, Telnet can be used to connect to a service and return its banner.

From → To	Command	Observation

DMZ to LAN	Connect to port 80, with:
	`telnet 10.10.x.7 80`
	
	and then send the HTTP `OPTIONS` command to the web server:
	`OPTIONS / HTTP/1.0`
		What is returned and how can this be used to fingerprint the WebServer?
		
		Which WebServer is running and which version?

DMZ to LAN	Similarly, other HTTP commands such as HEAD (get a HTML page header) and GET (get the whole HTML page) can be used to footprint a web server. Try the following and observe:
	
	`HEAD / HTTP/1.0`
	`GET / HTTP/1.0`
		What do you observe from using these HTTP requests:

G Brute Force

For this part of the lab, we will crack the username and password on the FTP login on Metasploitable. We will Hydra on Kali (DMZ), where you create a user file and password file with the following lists:

list_user:
administrator
admin
root
msfadmin
guest

list_password:
adminpass
password
Password
123456
napier123
pa$$word

Next, start Wireshark on Kali (DMZ), and then run Hydra with these usernames and passwords:

```
# hydra -L list_user -P list_password 10.10.y.9 ftp
```

From this determine one of the usernames and passwords.

Stop Wireshark and find the hydra trace. What do you observe from the trace:

What is the FTP status code for an incorrect login:

What is the FTP status code for a correct login:

Now write a Snort rule to detect an incorrect login on FTP (and thus detect a possible Hydra scan on the server). Hint, you need to detect "530" in the Port 21 connection.

Which rule have you used:

Rerun Hydra and start Snort to detect incorrect logins. Did it detect the scan? [Yes/No]

Next, run Hydra and crack the username and the password for the Web server. With these usernames and passwords we will target the DVWA site. First access the Web server from:

`http://20.20.21.9/dvwa/login.php`

Next, start Wireshark on Kali (DMZ), and then run Hydra to try a range of logins:

```
# hydra -L list_user -P list_password 10.10.y.9 http-post-form
'/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed'
```

From this determine one of the usernames and passwords.

Stop Wireshark and find the hydra trace. What do you observe from the trace:

What is the HTTP status code for an incorrect login:

What is the HTTP status code for a correct login:

Now access the Mutillidae site on Metasploit:

```
http://10.10.y.9/mutillidae
```

Now we will attack the Mutillidae site:

```
# hydra -L list_user -P list_password 10.10.y.9 http-post-form
'/mutillidae/index.php?page=login.php:username=^USER^&password=^PASS^&login-php-
submit-button=Login:Not Logged In'
```

From this determine one of the usernames and passwords.

H NAT and 1:1 mappings

No other group can access any of your hosts, as you are behind NAT. Now we need to setup a 1:1 mapping and a virtual IP address (with Proxy ARP) to map an internal address to an external one. First, we need to find an IP address from the 10.221.0.0/22 network **which is not being used**, and then we will use this to allow other group's access to the hosts in the DMZ (Figure 2).

Demo: https://youtu.be/1wn2io8EWvs

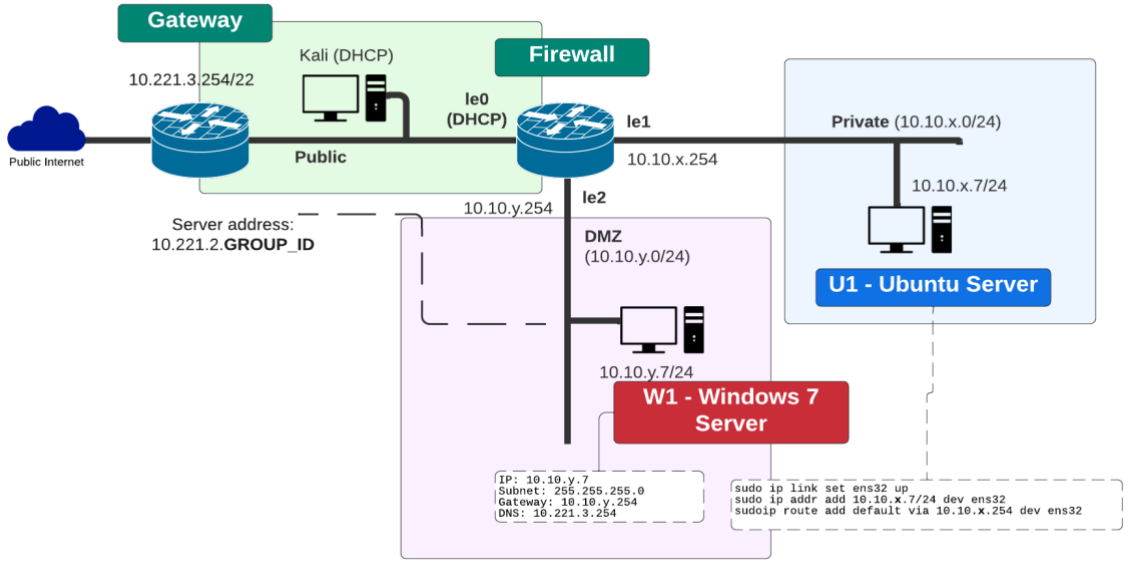

Figure 2: Setup 1:1 NAT for mapping of servers

Run NMAP from the Private network with: **nmap –sP 10.221.0.0/24**

Which hosts are on-line?

Now pick an address which is (where GROUP ID is your ID number):

10.221.2.[GROUP ID]

Now, on the firewall, setup a 1:1 mapping of the External IP address that you have selected and the Internal IP address on the DMZ (Figure 3).

Next, setup a Virtual IP address (with Proxy ARP) for the external address you have selected, which will advertise the IP address (Figure 4).

Now from the WAN interface, ping the host in the DMZ. Can you ping it?

Finally ask, someone in another group to ping your host in the DMZ. Can they ping it?

Now get them to access the Web server on your host.

Finally get them to NMAP your host? What can you observe from the NMAP?

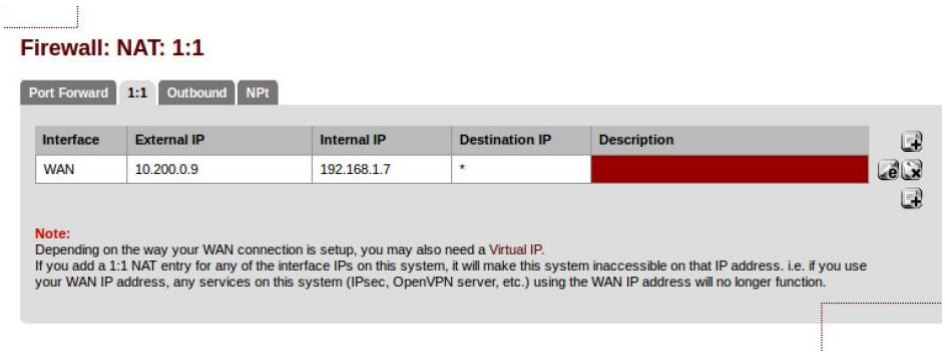

Figure 3: 1:1 NAT settings

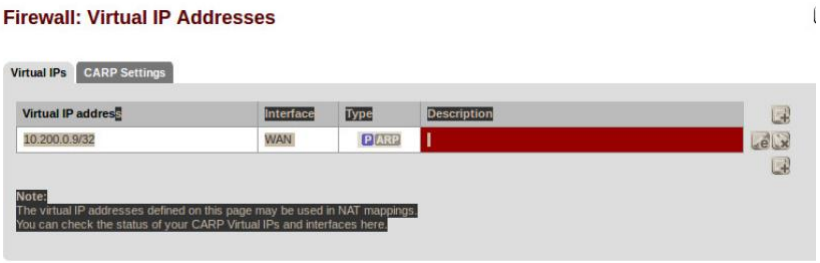

Figure 4: Virtual IP addresses

I Connecting to another network

Now, wait for other teams to finish (or use the Test setup). You should have ready:

- A forward-facing Web and FTP site ready to connect from outside your network.

NMAP their server, and then make sure you can connect to the service. Now get them to block your specific source (just one address), and recheck that you cannot connect. Finally change your IP address, and re-do the NMAP, and make sure you can connect.

Please note some of the information related to their server. What information can you determine? Can you determine the MAC address of their server?

Software Tutorial

Complete the software tutorial at:

`http://asecuritysite.com/csn09112/software02`

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