

OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

---

## Assignment #3 Sword vs. Shield

---

Sahmer Ismael

01219271

## TASK A

1. Use Nmap to profile the basic information about the subnet topology (including open ports information, operation systems, etc.) You need to get the service and backend software information associated with each opening port in each VM.

```
root@CS2APenTest: # nmap 192.168.10.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2024-02-25 04:19 EST
Nmap scan report for 192.168.10.2
Host is up (0.0046s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 192.168.10.10
Host is up (0.012s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp

Nmap scan report for 192.168.10.11
Host is up (0.0070s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrcp
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49154/tcp open  unknown

Nmap done: 230 IP addresses (3 hosts up) scanned in 17.44 seconds
root@CS2APenTest: #
```

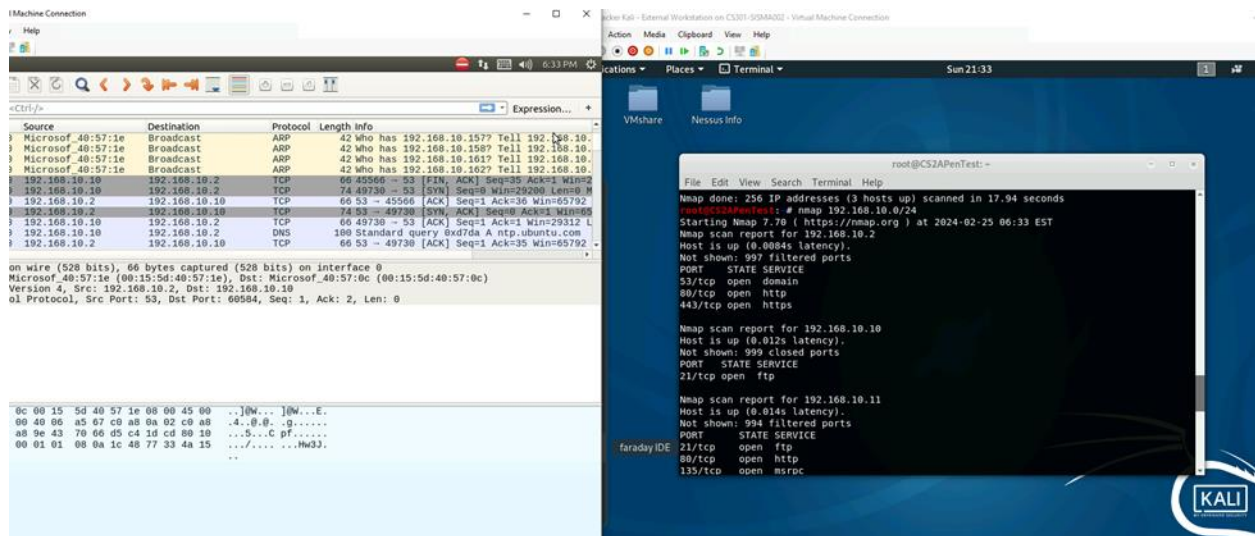
```
root@CS2APenTest: # nmap -sV 192.168.10.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2024-02-25 04:26 EST
Nmap scan report for 192.168.10.2
Host is up (0.0040s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE      VERSION
53/tcp    open  tcpwrapped
80/tcp    open  http         nginx
443/tcp   open  ssl/http     nginx

Nmap scan report for 192.168.10.10
Host is up (0.019s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.3
Service Info: OS: Unix

Nmap scan report for 192.168.10.11
Host is up (0.0078s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
80/tcp    open  http         Microsoft IIS httpd 7.5
135/tcp   open  msrcp        Microsoft Windows RPC
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp  open  ms-wbt-server?
49154/tcp open  msrcp        Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 256 IP addresses (3 hosts up) scanned in 99.82 seconds
root@CS2APenTest: #
```



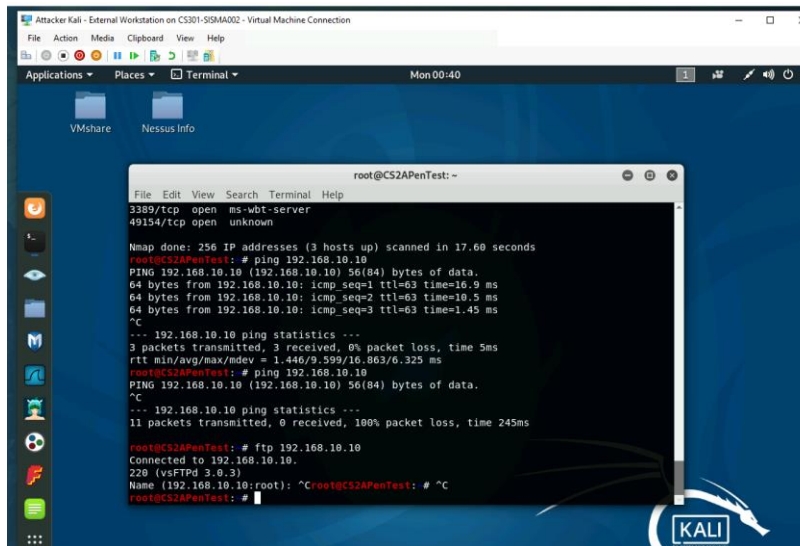
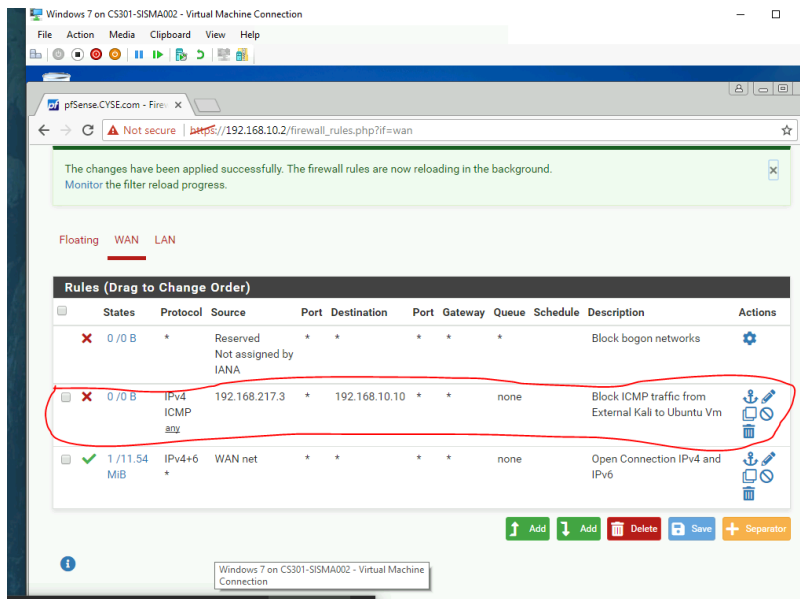


**Description:** From what I have gathered from the screenshot, is that after running the scan from the External Kali VM, using the command of 192.168.10.0/24 to scan the whole subnet. I was able to locate, the traffic from the Ubuntu VM, and was able to Identify that the Nmap scan was trying to communicate with different ports within the Subnet, and it was displaying a bunch of different source packets, that were running in the background of the scan. One of the protocols that the screenshot, displayed from the scan, is the ARP protocol, which is used to determine which IP addresses are in use within the local network. This message was broadcasted throughout the server, to display who has the 192.168.10.157, and to tell the designated Ip address, which was in this case, IP address 192.168.10.2, about it. Furthermore, the screenshot, displays that Nmap was completing the TCP handshake process, which it was trying to find out about the TCP ports that where in the network, to communicate with. I also examined the protocol Hierarchy statistics tool in Wireshark, and was able to identify, the different types of packets that where going, through the Wireshark tool, and the percentage of the packets being successful.

**Task B: Shield – Protect your network with firewall (10 + 10+ 20 + 20 = 60 points)**

**1. Configure the pfSense firewall rule to block the ICMP traffic from External Kali to Ubuntu VM.**

Rule#	Interface	Action	Source IP	Destination IP	Protocol (port # if applicable)
1	WAN	Block	192.168.217.3	192.168.10.10	ICMP

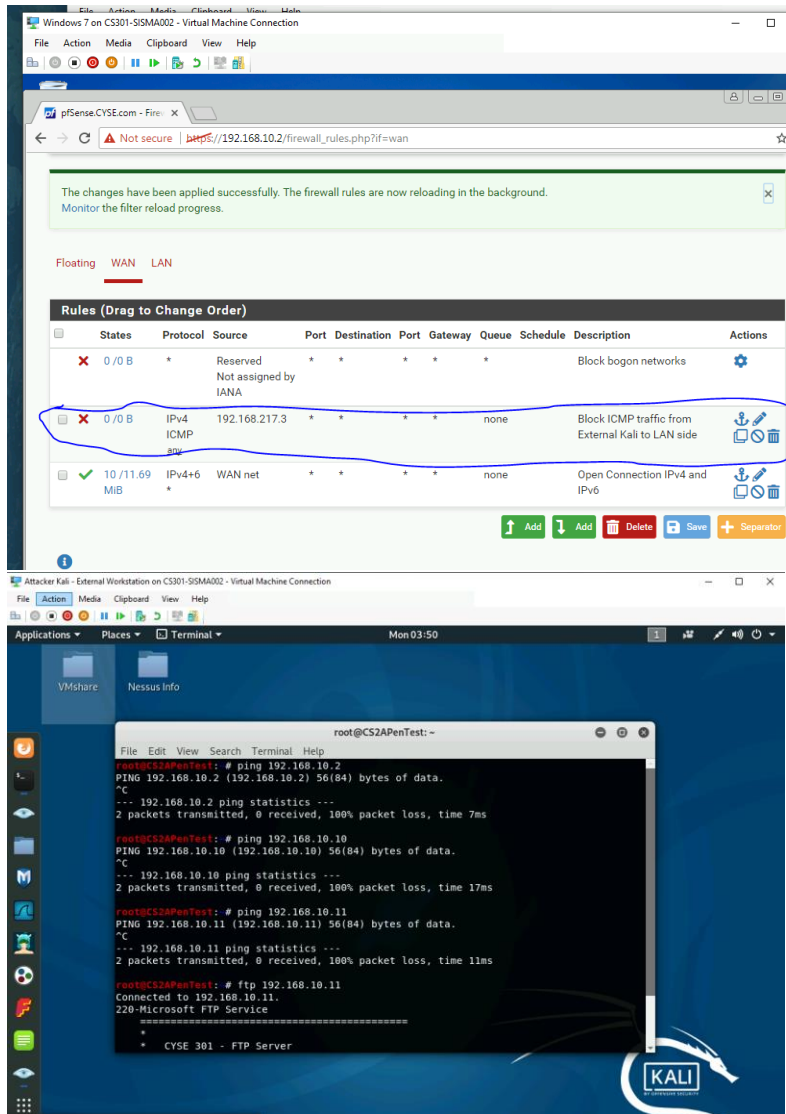


**Description:** from the screenshots above, I blocked the ICMP traffic, from external Kali to Ubuntu Vm. I showed, before the rule, they were connected, and then after, I showed the ICMP traffic being blocked, after the rule was set. I also accessed FTP packets, to make certain that the rule only blocked ICMP traffic.

2. Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if applicable)

1	WAN	Block	192.168.217.3	LAN Side	ICMP
---	-----	-------	---------------	----------	------



**Description:** I displayed, me blocking the ICMP traffic, from external Kali to the LAN side, and tested it. Furthermore I also tested the firewall rule, by using FTP, to show only ICMP was blocked.

3. Clear the previous firewall policies and configure the pfSense firewall to block ALL traffic from External Kali to the LAN side, except for the FTP protocol towards Windows Server 2008.

Rule#	Interface	Action	Source IP	Destination IP	Protocol
1	WAN	pass	192.168.217.3	192.168.10.11	TCP

2	WAN	Block	192.168.217.3	Any	Any
---	-----	-------	---------------	-----	-----

The top screenshot shows the pfSense web interface. A notification at the top states: "The firewall rule configuration has been changed. The changes must be applied for them to take effect." Below this, the "Rules (Drag to Change Order)" table is visible. The table has columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. The rules are as follows:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	
0/3 KIB	IPv4 TCP	192.168.217.3	*	192.168.10.11	21 (FTP)	*	none		Pass FTP protocol towards window server 2008	
0/16 KIB	IPv4 *	192.168.217.3	*	*	*	*	none		Block all traffic from external Kali to LAN side	
1/11.89 MIB	IPv4+6	WAN net	*	*	*	*	none		Open Connection IPv4 and IPv6	

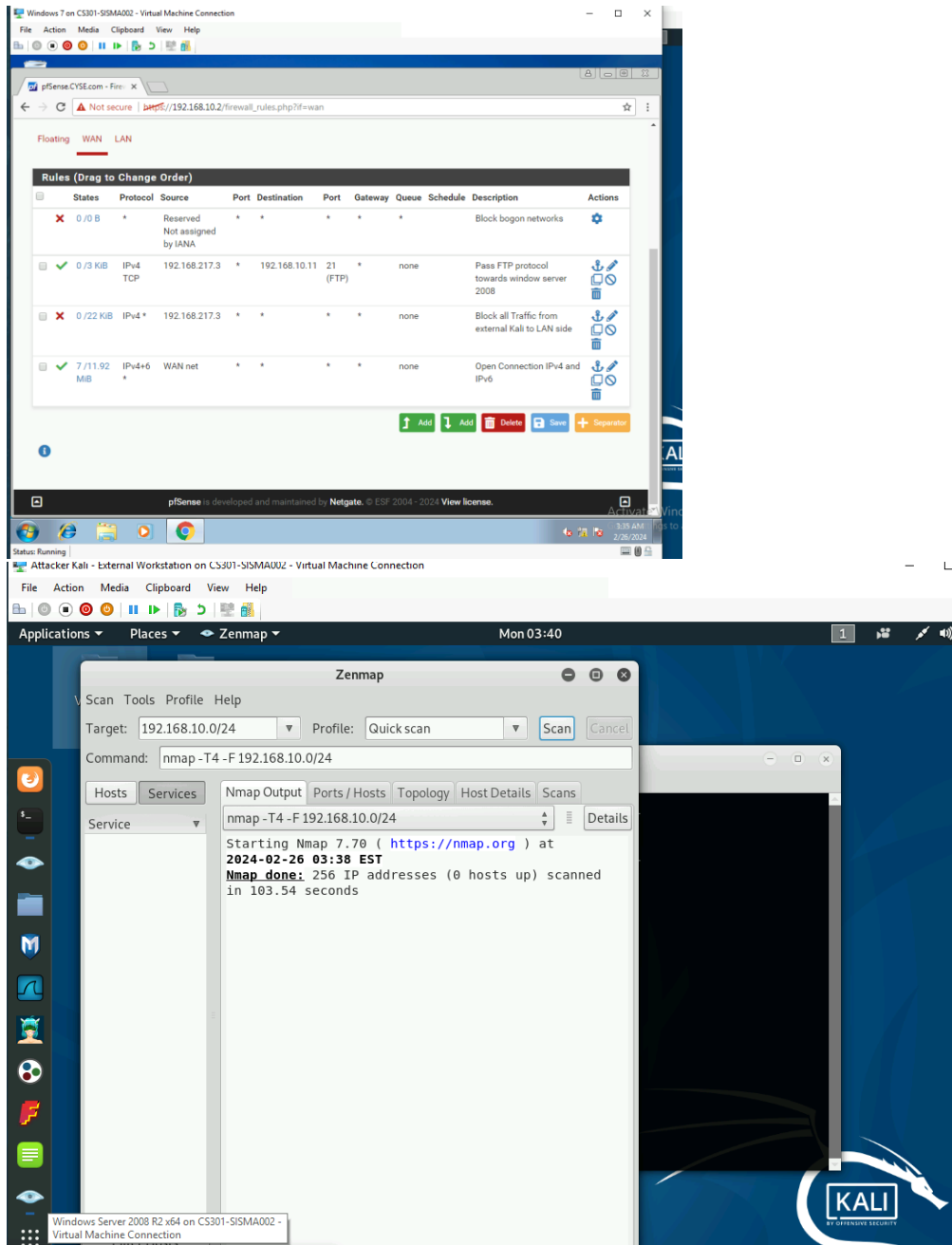
The bottom screenshot shows a terminal window on a Kali Linux machine. It displays the output of an FTP connection to 192.168.10.11. The output shows that the connection is successful and that the user is now accessing the FTP service on Windows 2008 R2 for CISE301.

The top screenshot shows the pfSense web interface, identical to the one above. The "Rules (Drag to Change Order)" table is the same, but the rule "Block all traffic from external Kali to LAN side" is now highlighted with a red circle.

The bottom screenshot shows a terminal window on a Kali Linux machine. It displays the output of ping tests to 192.168.10.2, 192.168.10.10, and 192.168.10.11. The output shows that the ping tests are successful and that the user is now accessing the FTP service on Windows 2008 R2 for CISE301.

**Description:** The first set of screenshots, for question 3 display, FTP only passing, through the windows server 2008, and the firewall rule that was used. The second set of pictures for question 3, displays that all the VMS are completely blocked besides, the FTP on windows server.

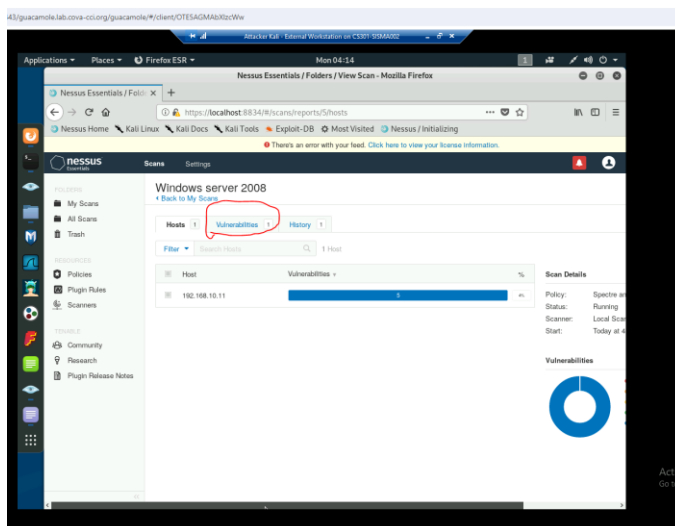
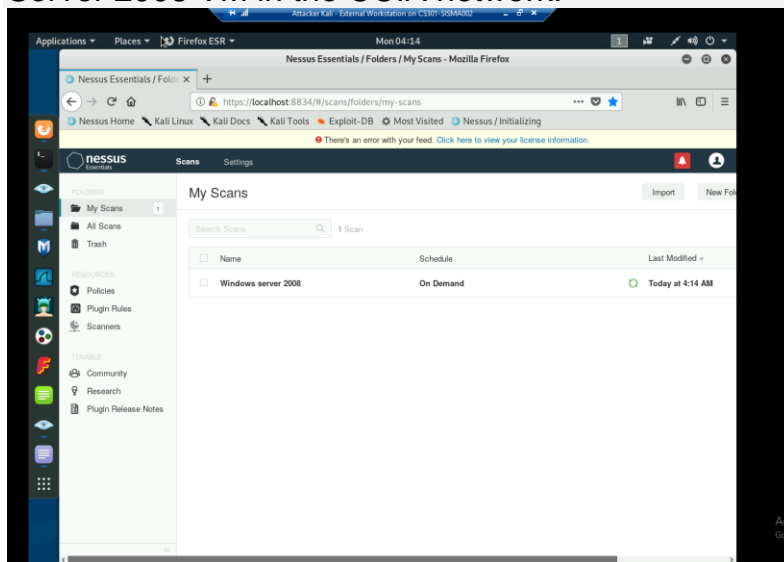
4. Keep the firewall policies you created in Task B.3 and repeat Task A.1. What's the difference?





**Description:** After keeping the same rules on PF sense, from the previous step, and applying a quick scan to Zen map/Nmap, it seems that the subnet topology which include, the port information, operating system, and backend software where all down, due to the firewall rules blocking all traffic, and information from the kali VM.

Extra credit (15 points): Use NESSUS to enumerate the security vulnerabilities of Microsoft Windows Server 2008 VM in the CCIA network.



**Description:** After going through Nessus from external Kali, I initiated a scan to target windows server 2008, which I inputted the Ip address. After that, the website scanned the server, which it found 1

vulnerability in the system. I only scanned the system for a couple, mins and many vuilerabilites occurred.