Old Dominion University

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

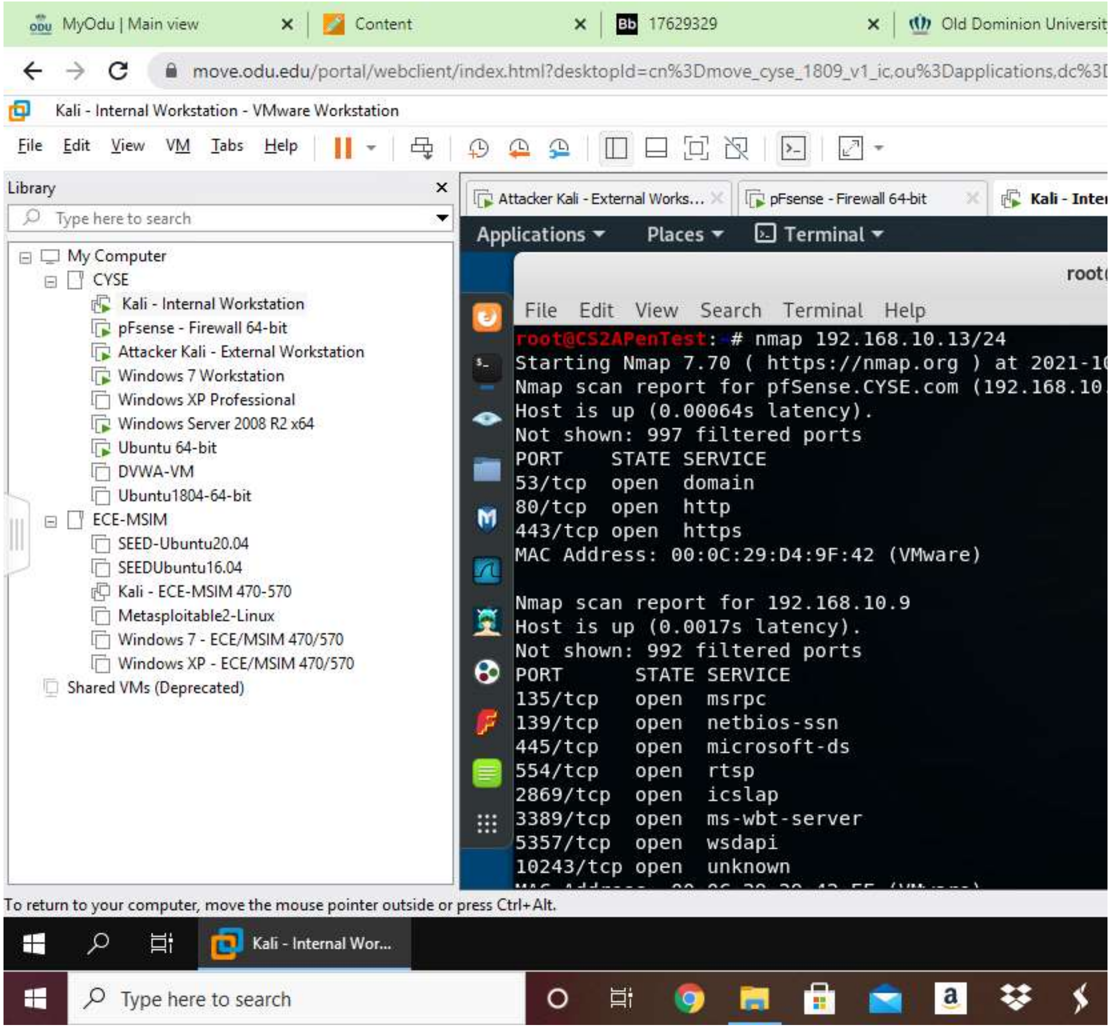
Assignment 2.3: Network Scanning

Jordan Sustarsic

Task A:

- (10 points) Run a simple scan from Internal Kali to obtain the basic information for all subnet hosts (including open ports information, MAC address, operation systems, etc.)

I used the command: “nmap 192.168.10.13/24” to complete this step


MyOdu | Main view
Content
17629329
Old Dominion Universit
move.odu.edu/portal/webclient/index.html?desktopId=cn%3Dmove_cyse_1809_v1_ic,ou%3Dapplications,dc%3D
Kali - Internal Workstation - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
CYSE
Kali - Internal Workstation
pFsense - Firewall 64-bit
Attacker Kali - External Workstation
Windows 7 Workstation
Windows XP Professional
Windows Server 2008 R2 x64
Ubuntu 64-bit
DVWA-VM
Ubuntu1804-64-bit
ECE-MSIM
SEED-Ubuntu20.04
SEEDUbuntu16.04
Kali - ECE-MSIM 470-570
Metasploitable2-Linux
Windows 7 - ECE/MSIM 470/570
Windows XP - ECE/MSIM 470/570
Shared VMs (Deprecated)
Attacker Kali - External Works...
pFsense - Firewall 64-bit
Kali - Inter
Applications
Places
Terminal
root(
File Edit View Search Terminal Help
Kali - Internal Wor...
Type here to search

```
root@CS2APenTest:~# nmap 192.168.10.13/24
Starting Nmap 7.70 ( https://nmap.org ) at 2021-1
Nmap scan report for pfSense.CYSE.com (192.168.10
Host is up (0.00064s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
MAC Address: 00:0C:29:D4:9F:42 (VMware)

Nmap scan report for 192.168.10.9
Host is up (0.0017s latency).
Not shown: 992 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
10243/tcp open  unknown
```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

- (40 points) Run an intensive scan from Internal Kali to obtain detailed information for all subnet hosts. Complete the first FIVE columns of the following table based on the information you observed. You need to create a table for the following VMs:

I will be using the cammands: "nmap 192.168.10.13/24", "nmap -O", and "nmap -v –script vuln" to complete this step

- pFsense

IP Address	Mac Address	OS Guessed	Open Ports	Service and Version	Safe or Not

192.168.10.2	00:0C:29:D4:9F:42	• Comau embedded; • FreeBSD 10.X; • OpenBSD 4.X	• 53, • 80, • 443	• Tcpwrapped • http-nginx • ssl/http-nginx	Yes

- Windows 7

IP Address	Mac Address	OS Guessed	Open Ports	Service and Version	Safe or Not
192.168.10.9	00:0C:29:29:42:EF	Microsoft Windows 2008 |8.1|7|Phone|Vista	• 135, • 139, • 445, • 554, • 2869, • 5357, • 10243	• msrcp-windowsRPC; • netbios ssn-windows netbios ssn; • Microsoft ds-windows 7; • Rtsp; • http-HTTPAPI httpd 2.0; • tcpwrapped; • http-HTTPAPI httpd 2.0; • http-HTTPAPI httpd 2.0;	No

- Unbuntu 64-bit

IP Address	Mac Address	OS Guessed	Open Ports	Service and Version	Safe or Not
192.168.10.10	00:0C:29:22:3C:09	Linux 4.X	21	ftp-vsftpd 3.0.3	Yes

- Windows Server 2008

IP Address	Mac Address	OS Guessed	Open Ports	Service and Version	Safe or Not
192.168.10.11	00:0C:29:1B:11:7C	Microsoft Windows 2008 |8.1|7|Phone|Vista	• 21, • 80, • 135, • 445, • 49154	• ftp-ftpd • http-IIS httpd 7.5 • msrpc-Windows RPC • Microsoft ds-2012 microsoft ds • Msrpc-windows RPC	No

- (10 points) Run Wireshark on Ubuntu VM while Internal Kali is scanning the network. Discuss the traffic pattern you observed

When scanning with nmap a lot of TCP traffic is generated from scanning all the various hosts and ports associated with them.

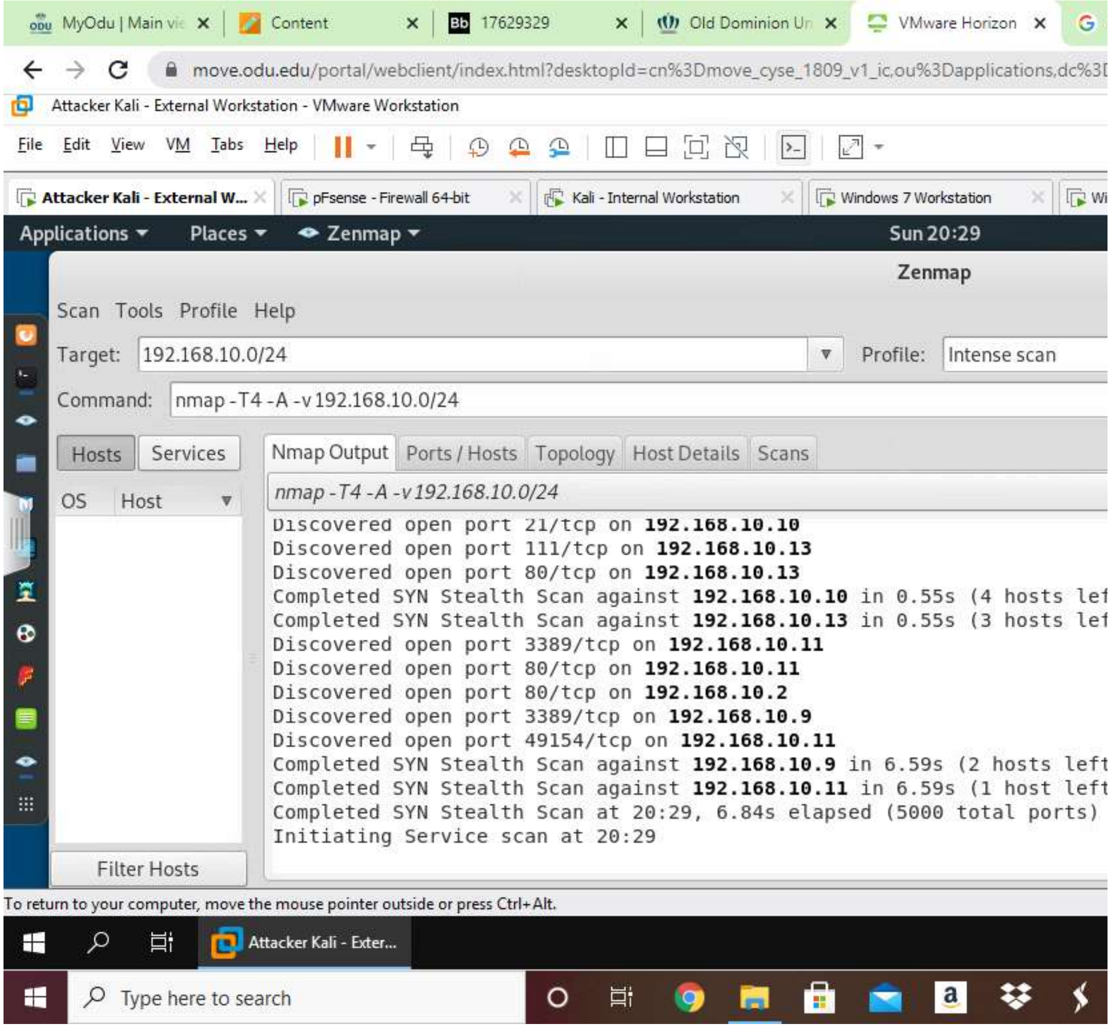
- (10 points) Google the service behind each opening port number you found in step 2. Then complete the last column of the table. If you consider a specific port is unsafe, please discuss the possible risks of opening that port.

  - In windows 7, port 135, service msrpc: There is a remote code vulnerability. This allows attackers to run code of their choosing with system privileges on a server.

  - In windows 2008 server, port 135 and 49154, service msrpc: There is a remote code vulnerability. This allows attackers to run code of their choosing with system privileges on a server.

Task B:

- (10 points) Use Zenmap to run an intensive scan from External Kali to obtain detailed information for all subnet hosts.



MyOdu | Main vie
Content
17629329
Old Dominion Un
VMware Horizon
move.odu.edu/portal/webclient/index.html?desktopId=cn%3Dmove_cyse_1809_v1_ic,ou%3Dapplications,dc%3D
Attacker Kali - External Workstation - VMware Workstation
File Edit View VM Tabs Help
Attacker Kali - External W...
pFsense - Firewall 64-bit
Kali - Internal Workstation
Windows 7 Workstation
Applications
Places
Zenmap
Sun 20:29
Zenmap
Scan Tools Profile Help
Hosts Services
OS Host
Nmap Output Ports / Hosts Topology Host Details Scans
Filter Hosts
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
Attacker Kali - Exter...
Type here to search

Target: 192.168.10.0/24

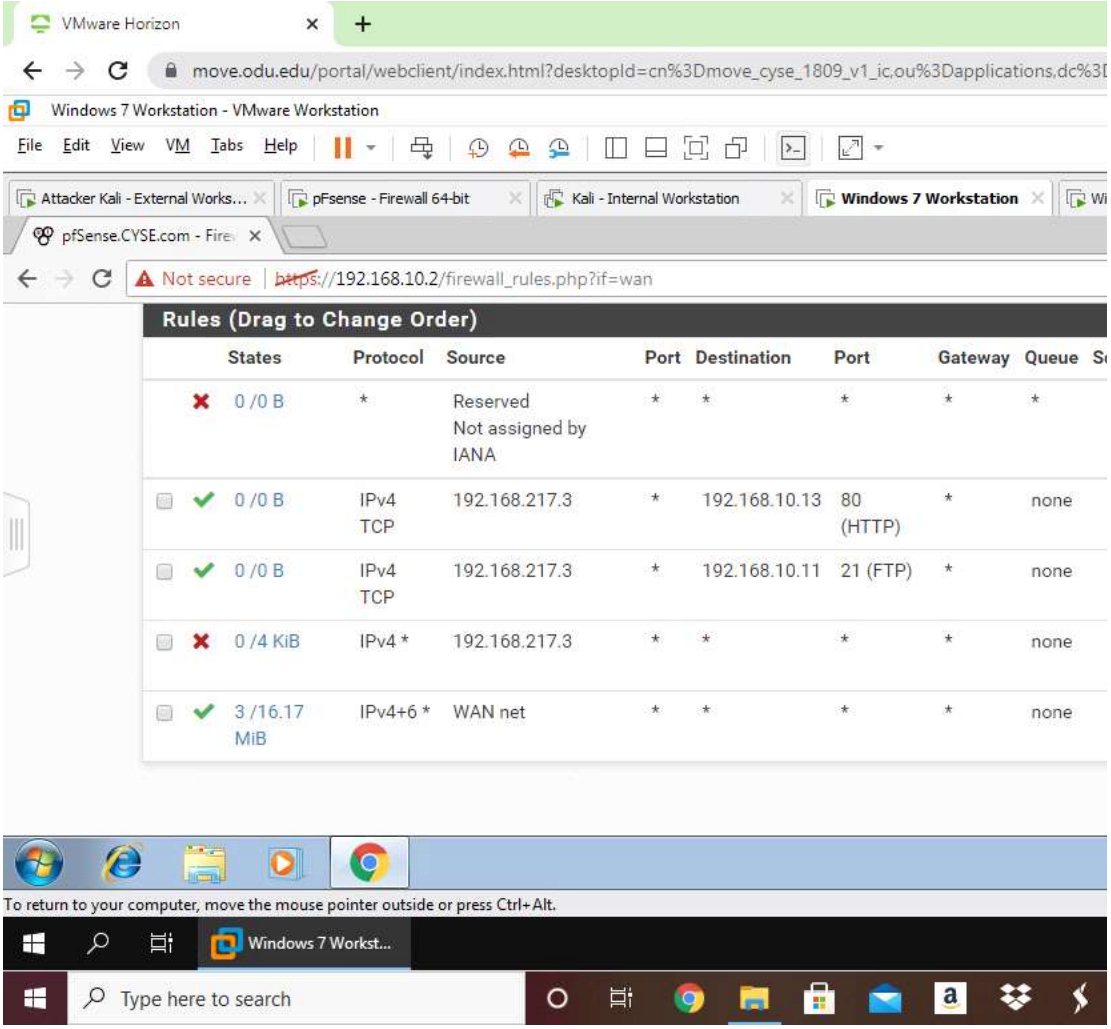
Profile: Intense scan

Command: nmap -T4 -A -v 192.168.10.0/24

```
nmap -T4 -A -v 192.168.10.0/24
Discovered open port 21/tcp on 192.168.10.10
Discovered open port 111/tcp on 192.168.10.13
Discovered open port 80/tcp on 192.168.10.13
Completed SYN Stealth Scan against 192.168.10.10 in 0.55s (4 hosts lef
Completed SYN Stealth Scan against 192.168.10.13 in 0.55s (3 hosts lef
Discovered open port 3389/tcp on 192.168.10.11
Discovered open port 80/tcp on 192.168.10.11
Discovered open port 80/tcp on 192.168.10.2
Discovered open port 3389/tcp on 192.168.10.9
Discovered open port 49154/tcp on 192.168.10.11
Completed SYN Stealth Scan against 192.168.10.9 in 6.59s (2 hosts left
Completed SYN Stealth Scan against 192.168.10.11 in 6.59s (1 host left
Completed SYN Stealth Scan at 20:29, 6.84s elapsed (5000 total ports)
Initiating Service scan at 20:29
```

- (10 points) Re-Scan the network after you apply the firewall policy created in assignment M 2.2, Task 4. Analyze and summarize the differences between two scan results.

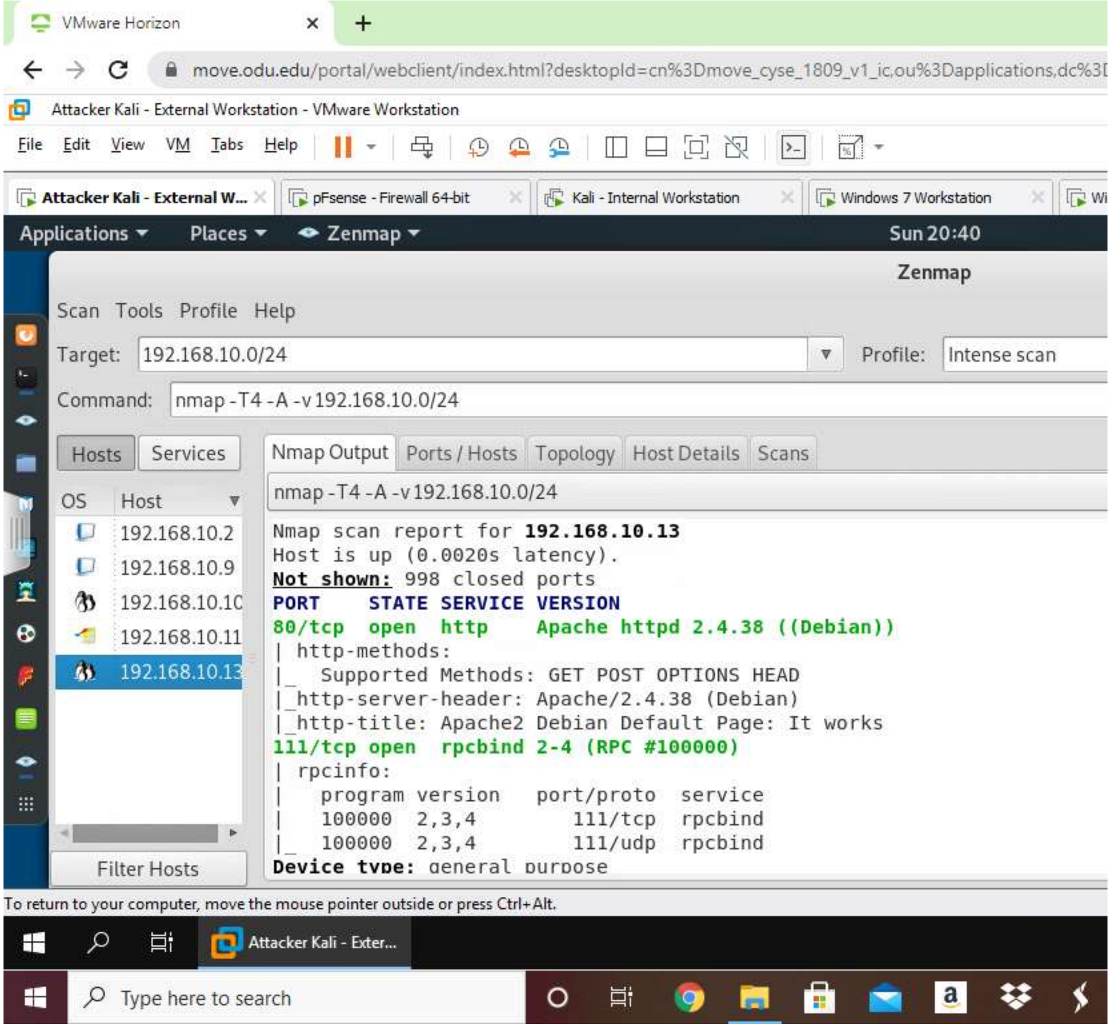
pFsense rule table showing the rules have been implemented


VMware Horizon
move.odu.edu/portal/webclient/index.html?desktopId=cn%3Dmove_cyse_1809_v1_ic,ou%3Dapplications,dc%3D
Windows 7 Workstation - VMware Workstation
File Edit View VM Tabs Help
Attacker Kali - External Works...
pFsense - Firewall 64-bit
Kali - Internal Workstation
Windows 7 Workstation
pfSense.CYSE.com - Fire
Not secure
https://192.168.10.2/firewall_rules.php?if=wan
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
Windows 7 Workst...
Type here to search

Rules (Drag to Change Order)

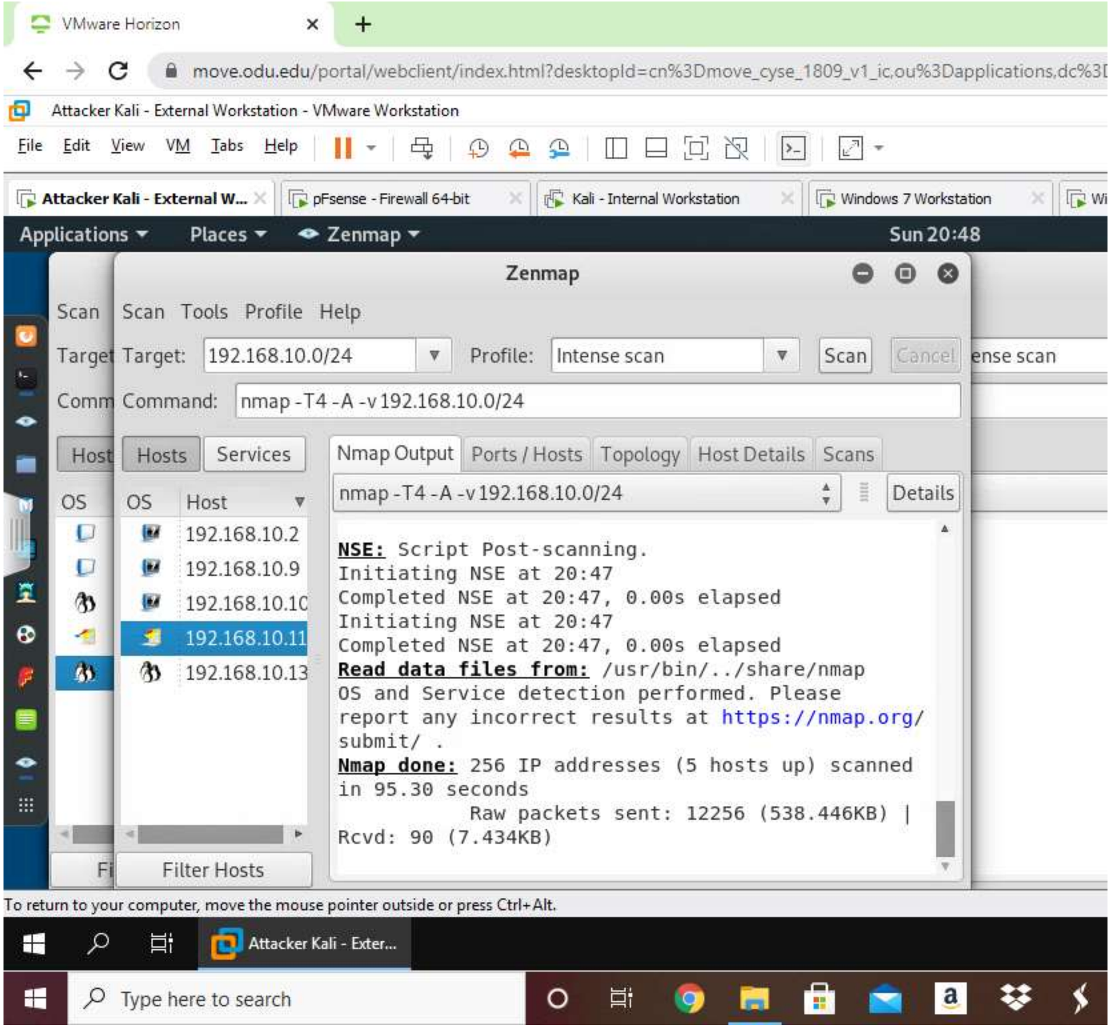
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	S
	✗	0 /0 B	*	Reserved Not assigned by IANA	*	*	*	*	*	
□	✓	0 /0 B	IPv4 TCP	192.168.217.3	*	192.168.10.13	80 (HTTP)	*	none	
□	✓	0 /0 B	IPv4 TCP	192.168.217.3	*	192.168.10.11	21 (FTP)	*	none	
□	✗	0 /4 KiB	IPv4 *	192.168.217.3	*	*	*	*	none	
□	✓	3 /16.17 MiB	IPv4+6 *	WAN net	*	*	*	*	none	

Zenmap can for subnet before the firewall rules


VMware Horizon
move.odu.edu/portal/webclient/index.html?desktopId=cn%3Dmove_cyse_1809_v1_ic,ou%3Dapplications,dc%3I
Attacker Kali - External Workstation - VMware Workstation
File Edit View VM Tabs Help
Attacker Kali - External W...
pFsense - Firewall 64-bit
Kali - Internal Workstation
Windows 7 Workstation
Applications
Places
Zenmap
Sun 20:40
Zenmap
Scan Tools Profile Help
Target: 192.168.10.0/24
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.10.0/24
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
192.168.10.2
192.168.10.9
192.168.10.10
192.168.10.11
192.168.10.13
Filter Hosts
nmap -T4 -A -v 192.168.10.0/24
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
Attacker Kali - Exter...
Type here to search

```
Nmap scan report for 192.168.10.13
Host is up (0.0020s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE VERSION
80/tcp  open  http    Apache httpd 2.4.38 ((Debian))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Apache2 Debian Default Page: It works
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|_  100000  2,3,4        111/udp  rpcbind
Device type: general purpose
```

Zenmap scan after the rules have been implemented


VMware Horizon
move.odu.edu/portal/webclient/index.html?desktopId=cn%3Dmove_cyse_1809_v1_ic,ou%3Dapplications,dc%3D
Attacker Kali - External Workstation - VMware Workstation
File Edit View VM Tabs Help
Attacker Kali - External W...
pFsense - Firewall 64-bit
Kali - Internal Workstation
Windows 7 Workstation
Applications
Places
Zenmap
Sun 20:48
Zenmap
Scan Tools Profile Help
Scan
Cancel
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Details
OS
Host
Filter Hosts
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
Attacker Kali - Exter...
Type here to search

Target: 192.168.10.0/24

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.10.0/24

```
192.168.10.2
192.168.10.9
192.168.10.10
192.168.10.11
192.168.10.13
```

```
nmap -T4 -A -v 192.168.10.0/24

NSE: Script Post-scanning.
Initiating NSE at 20:47
Completed NSE at 20:47, 0.00s elapsed
Initiating NSE at 20:47
Completed NSE at 20:47, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please
report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned
in 95.30 seconds
           Raw packets sent: 12256 (538.446KB) |
Rcvd: 90 (7.434KB)
```

- When running the scan before the rules you can see all the hosts and their open ports.

- When you run the scan after the rules, you can see all the hosts, but you can only see two ports out of all 5 hosts. One of the ports is port 80 on internal kali. This port is the http port for the apache server. The second port is port 21 on Windows server 2008. This port is the ftp port. As stated in the rules we can only send http traffic to internal kali and ftp traffic to windows server 2008.