CYSE 301: Cybersecurity Technique and Operations

Assignment 3: Sword vs. Shield

In this assignment, you will act as an attacker to identify the vulnerabilities in the LAN network and a defender to apply proper countermeasures. You need to provide a screenshot for each task below.

Task A: Sword - Network Scanning (20+ 20 = 40 points)

Power on the listed VMs and complete the following steps from the External Kali (you can use either nmap or zenmap to complete the assignment)

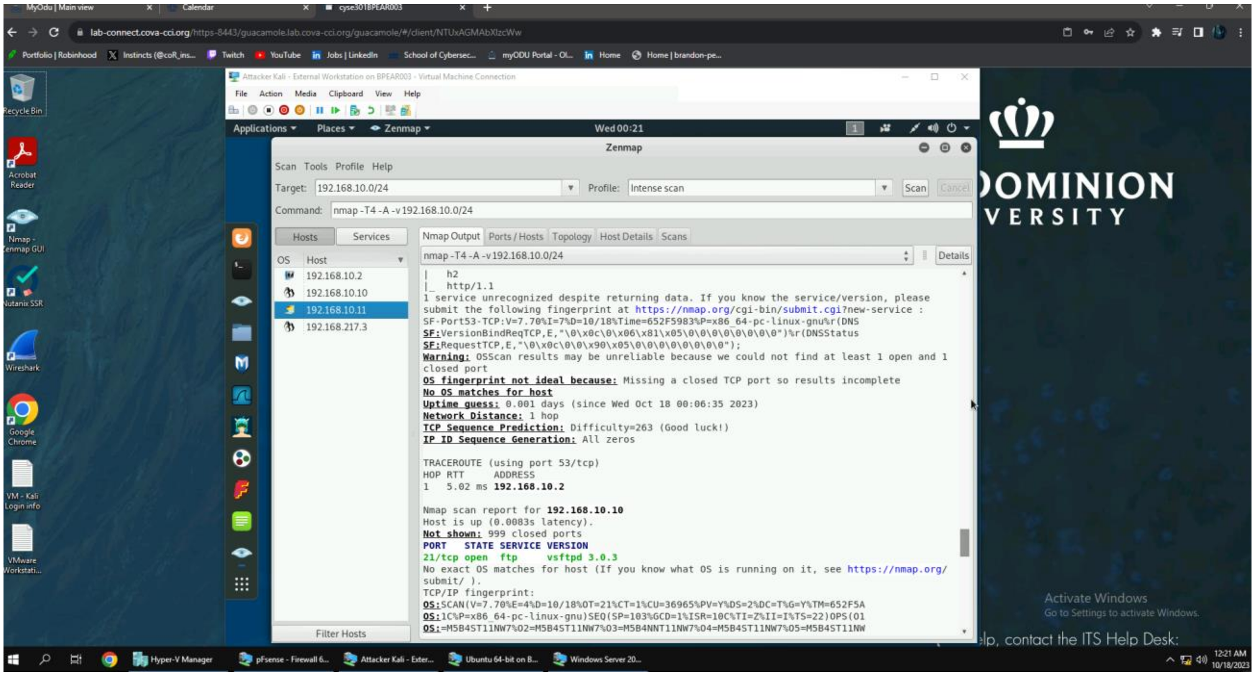
- External Kali
- pfSense
- Ubuntu
- Windows Server 2008

Make sure you didn't add/delete any firewall policy before continuing.

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.

Ubuntu 192.168.10.10 is running on Linux

192.168.1.0.11 is running on Microsoft 2008


Attacker Kali - External Workstation on BPEAR003 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Zenmap
Wed 00:21
Zenmap
Scan Tools Profile Help
Scan Cancel
Hosts Services
OS Host
Nmap Output Ports / Hosts Topology Host Details Scans
Details
Filter Hosts
Activate Windows
Go to Settings to activate Windows.
Hyper-V Manager
pfSense - Firewall 6...
Attacker Kali - Exter...
Ubuntu 64-bit on B...
Windows Server 20...

Target: 192.168.10.0/24

Profile: Intense scan

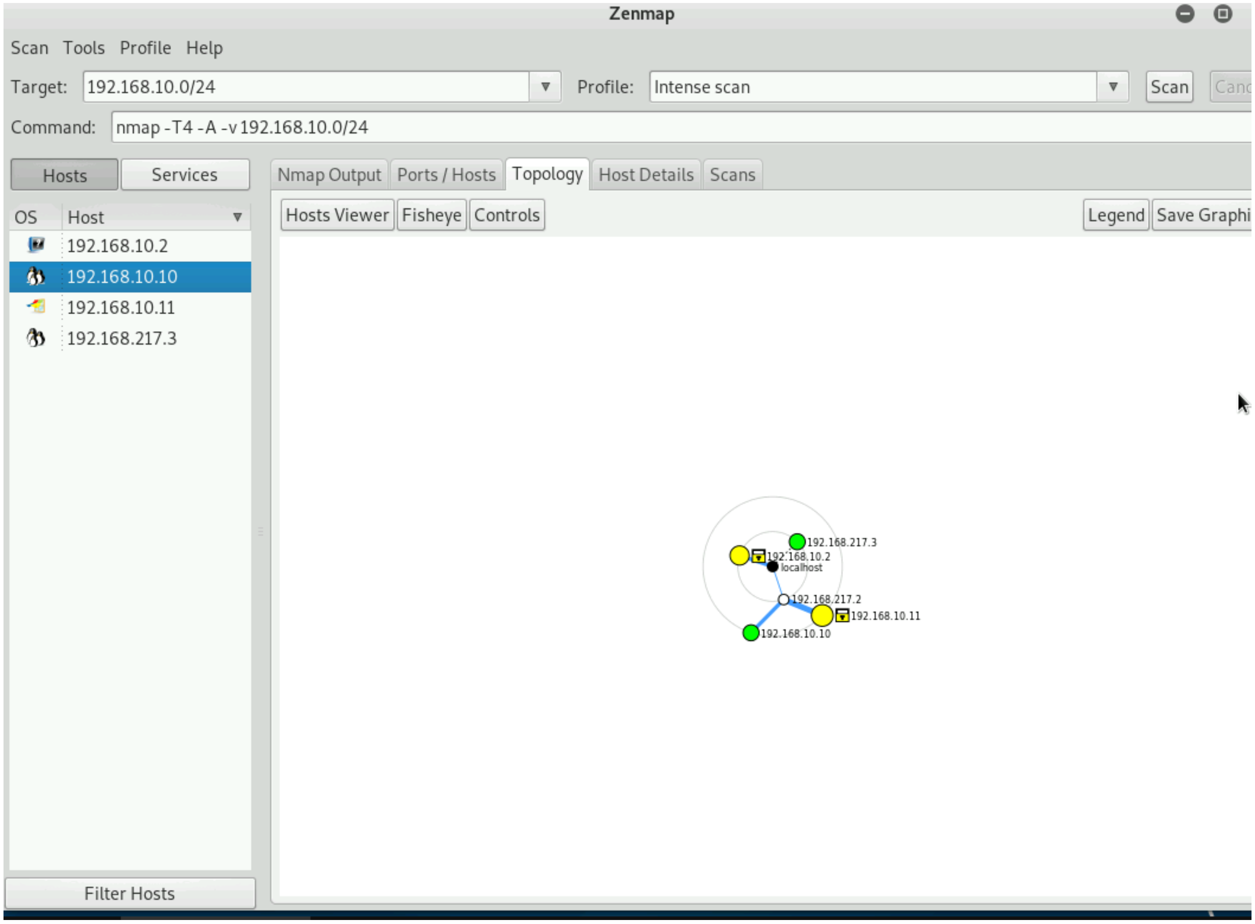
Command: nmap -T4 -A -v 192.168.10.0/24

192.168.10.2
192.168.10.10
192.168.10.11
192.168.217.3

```
|   h2
|_  http/1.1
1 service unrecognized despite returning data. If you know the service/version, please
submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.70%I=7%D=10/18%Time=652F5983%P=x86_64-pc-linux-gnu%r(DNS
SF:VersionBindReqTCP,E,"\0\x0c\0\x06\x81\x05\0\0\0\0\0\0\0\0")%r(DNSStatus
SF:RequestTCP,E,"\0\x0c\0\0\x90\x05\0\0\0\0\0\0\0\0");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Uptime guess: 0.001 days (since Wed Oct 18 00:06:35 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 53/tcp)
HOP RTT     ADDRESS
1   5.02 ms 192.168.10.2

Nmap scan report for 192.168.10.10
Host is up (0.0083s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/
submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=10/18%OT=21%CT=1%CU=36965%PV=Y%DS=2%DC=T%G=Y%TM=652F5A
OS:1C%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10C%TI=Z%II=I%TS=22)OPS(O1
OS:=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW
```

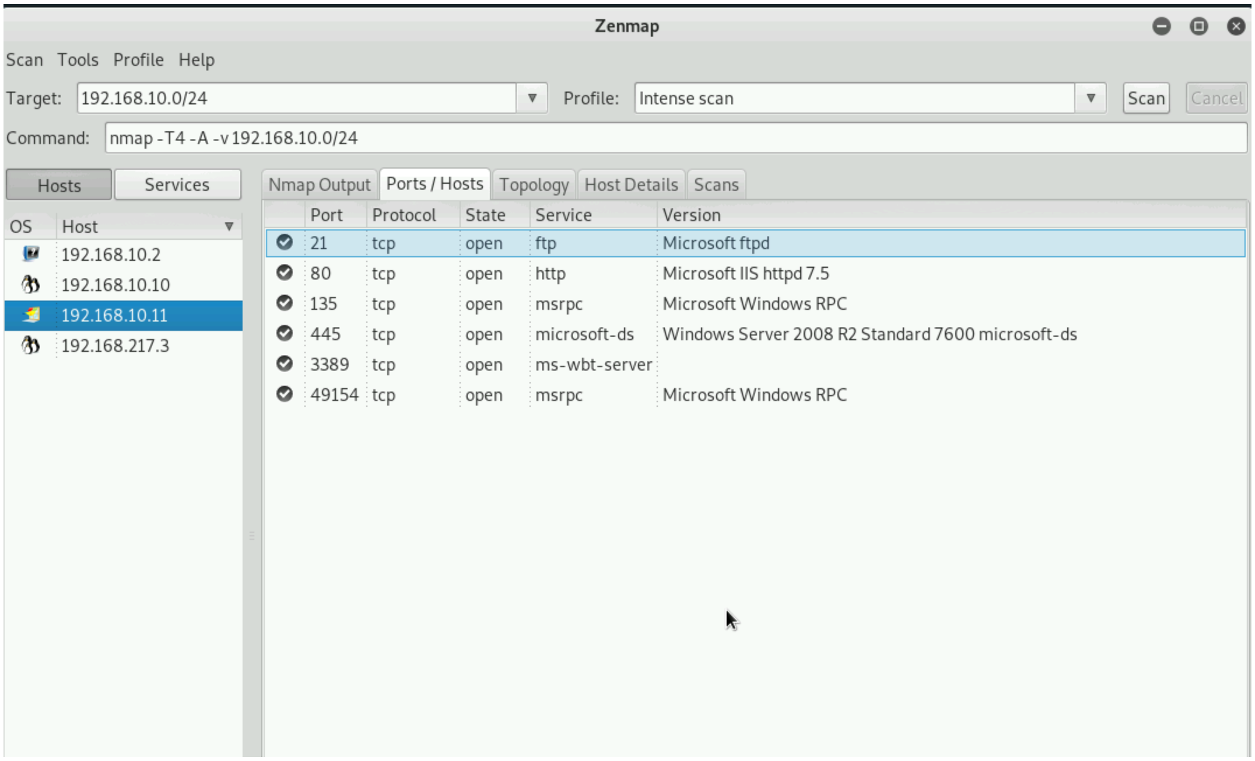


Target: 192.168.10.0/24

Profile: Intense scan

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

OS	Host
	192.168.10.2
	192.168.10.10
	192.168.10.11
	192.168.217.3



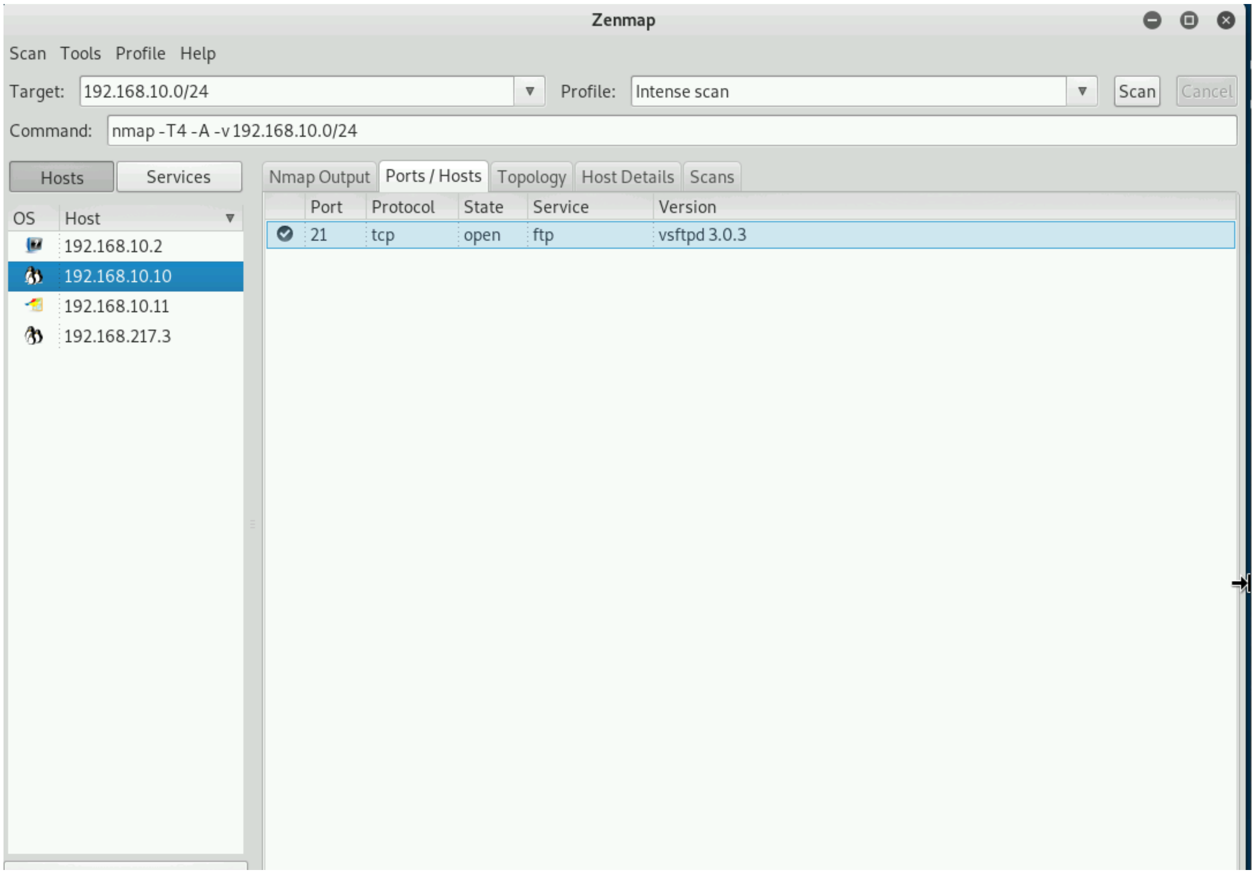
Target: 192.168.10.0/24

Profile: Intense scan

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

OS	Host
	192.168.10.2
	192.168.10.10
	192.168.10.11
	192.168.217.3

	Port	Protocol	State	Service	Version
✓	21	tcp	open	ftp	Microsoft ftpd
✓	80	tcp	open	http	Microsoft IIS httpd 7.5
✓	135	tcp	open	msrpc	Microsoft Windows RPC
✓	445	tcp	open	microsoft-ds	Windows Server 2008 R2 Standard 7600 microsoft-ds
✓	3389	tcp	open	ms-wbt-server	
✓	49154	tcp	open	msrpc	Microsoft Windows RPC



Target: 192.168.10.0/24

Profile: Intense scan

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

OS	Host
	192.168.10.2
	192.168.10.10
	192.168.10.11
	192.168.217.3

	Port	Protocol	State	Service	Version
✓	21	tcp	open	ftp	vsftpd 3.0.3

2. Run Wireshark in Ubuntu VM while External Kali is scanning the network. Discuss the traffic pattern you observed. What do you find? **Please write a 200-word essay to discuss your findings.**

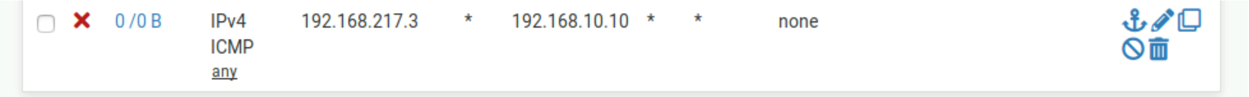
The main communication that can be seen is between 192.168.10.10 and 192.168.10.2. The Protocols that have been seen on the network are DNS, TCP, and ARP. 192.168.10.2 source port was 53 while the port for 192.168.10.10 often varied from 38000 to 59000.

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

In order to receive full credits, you need to fill the table (add more rows if needed), implement the firewall rule(s), show me the screenshot of your firewall table, and verify the results.

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 appliable)
3	WAN	block	192.168.217.3	192.168.10.10	IPv4 ICMP



□	✗	0 /0 B	IPv4 ICMP any	192.168.217.3	*	192.168.10.10	*	*	none

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 appliable)
2	WAN	block	192.168.217.3	*	IPv4 ICMP

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 (port # if appliable)
2	LAN	block	192.168.10.9	192.168.217.3	IPv4 TCP port 21 (ftp)
3	LAN	pass	192.168.10.11	192.168.217.3	IPv4 TCP 21 (Ftp)

4. Keep the firewall policies you created in Task B.3 and repeat Task A.1. What's the difference? The FTP files are no longer being transferred.

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