



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Advanced Cybersecurity (ACCB6000)

Scanning Networks



Objectives

In continuation to our earlier lectures, this tutorial helps in providing you an overview of tools used to scan networks.

ETHICAL STATEMENT

The tools and techniques you are exposed to' in this lab is to work only on a virtual machine environment and the purpose is entirely to demonstrate various types of cyber-attacks. Experimentation with these tools, techniques, and resources is at the discretion of the instructor and institution. If you as a student consider using attack tools for educational purposes on an outside environment, you should contact me prior to any experimentation.

Note: Unauthorized access to data, computer, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator's motivations. It is the learner's responsibility, as the user of this material, to be cognizant of and compliant with computer use laws.

Part 1: Use HPING Version 3 to send ICMP/TCP/UPD Packets and analyse the target replies.
--

Part 2: Use MegaPing to identify live hosts and open ports of the Target.

Part 3: Use NetScanTools Pro to initiate various Scans
--

Part 4: Explore various network scanning Techniques

<i>This activity will continue...</i>

ICONS Used in this document:



Find out the outcome/ Answers/ Solution



Do research and complete the task. Need referencing/ in-text citations.
Shall be included as a part of your coursework.



Record your Reflection

Why to use these tools? These tools are used to scan the networks and identify hosts, ports, and services. It is one of the components of intelligence gathering that can be used by attackers to gather information and create a profile of their targets



You need Windows Server 2016, Server 2012, Windows 10, Windows 8 and Kali Linux to complete this activity.

Part 1: Use HPING Version 3 to send ICMP/TCP/UDP Packets and analyse the target replies.

Target Machine: Windows 10

Attacker Machine: Kali Linux

Use Wireshark in the Target Machine to capture the packets and observe

Task 1 (Commands):

1. Install HPING

Sudo apt-get install hping3

```
└─# apt install hping3
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  dbus dbus-bin dbus-daemon dbus-session-bus-common dbus-system-bus-common libdbus-1-3 libexpat1 libpcap0.8 libtcl8.6
Suggested packages:
  default-dbus-session-bus | dbus-session-bus tcl8.6
The following NEW packages will be installed:
  dbus dbus-bin dbus-daemon dbus-session-bus-common dbus-system-bus-common hping3 libdbus-1-3 libexpat1 libpcap0.8
  libtcl8.6
0 upgraded, 10 newly installed, 0 to remove and 93 not upgraded.
Need to get 106 kB/2,258 kB of archives.
After this operation, 7,062 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://kali.download/kali kali-rolling/main amd64 libexpat1 amd64 2.4.3-3 [106 kB]
Fetched 106 kB in 0s (250 kB/s)
Selecting previously unselected package libdbus-1-3:amd64.
(Reading database ... 17135 files and directories currently installed.)
Preparing to unpack .../0-libdbus-1-3_1.12.20-3_amd64.deb ...
Unpacking libdbus-1-3:amd64 (1.12.20-3) ...
Selecting previously unselected package dbus-bin.
Preparing to unpack .../1-dbus-bin_1.12.20-3_amd64.deb ...
Unpacking dbus-bin (1.12.20-3) ...
Selecting previously unselected package dbus-session-bus-common.
Preparing to unpack .../2-dbus-session-bus-common_1.12.20-3_all.deb ...
Unpacking dbus-session-bus-common (1.12.20-3) ...
Selecting previously unselected package libexpat1:amd64.
Preparing to unpack .../3-libexpat1_2.4.3-3_amd64.deb ...
Unpacking libexpat1:amd64 (2.4.3-3) ...
Selecting previously unselected package dbus-daemon.
Preparing to unpack .../4-dbus-daemon_1.12.20-3_amd64.deb ...
Unpacking dbus-daemon (1.12.20-3) ...
Selecting previously unselected package dbus-system-bus-common.
Preparing to unpack .../5-dbus-system-bus-common_1.12.20-3_all.deb ...
Unpacking dbus-system-bus-common (1.12.20-3) ...
Selecting previously unselected package dbus.
Preparing to unpack .../6-dbus_1.12.20-3_amd64.deb ...
Unpacking dbus (1.12.20-3) ...
Selecting previously unselected package libpcap0.8:amd64.
Preparing to unpack .../7-libpcap0.8_1.10.1-4_amd64.deb ...
Unpacking libpcap0.8:amd64 (1.10.1-4) ...
Selecting previously unselected package libtcl8.6:amd64.
Preparing to unpack .../8-libtcl8.6_8.6.12+dfsg-1_amd64.deb ...
Unpacking libtcl8.6:amd64 (8.6.12+dfsg-1) ...
Selecting previously unselected package hping3.
Preparing to unpack .../9-hping3_3.a2.ds2-10_amd64.deb ...
Unpacking hping3 (3.a2.ds2-10) ...
Setting up libexpat1:amd64 (2.4.3-3) ...
Setting up libdbus-1-3:amd64 (1.12.20-3) ...
Setting up libtcl8.6:amd64 (8.6.12+dfsg-1) ...
Setting up dbus-session-bus-common (1.12.20-3) ...
Setting up dbus-system-bus-common (1.12.20-3) ...
Setting up dbus-bin (1.12.20-3) ...
Setting up dbus-daemon (1.12.20-3) ...
Setting up libpcap0.8:amd64 (1.10.1-4) ...
Setting up dbus (1.12.20-3) ...
invoke-rc.d: could not determine current runlevel
Setting up hping3 (3.a2.ds2-10) ...
Processing triggers for libc-bin (2.32-4) ...
```

```
hping3 --help
```

2. ICMP Scanning

```
hping3 -1 "Target"
```

#in my case it is 192.168.1.27



What is the other method to send an ICMP packet?

3. Sending SYN Packet

```
hping3 -S "Target"
```

4. ACK Scanning on port 80

```
hping3 -A "Target" -p 80
```

5. Sending Fin Packet

```
hping3 -F "Target"
```

6. Sending Syn Packet to a port

```
hping3 -S "Target" -p 80
```

#here -S is syn and -p is port

What are the other TCP flags? List out the commands to send other TCP flags, execute the commands and capture the outputs. Write a brief note to reflect your understanding on using HPING to send TCP flags. Include what is the purpose, what intelligence did you gather etc



7. Scanning entire subnet

```
hping3 -1 192.168.1.x --rand-dest -I eth0
```

Based on your observation and research done so far with HPING tool, what is your understanding about the usage of this tool? Could you list out the pros and cons of using this tool?



Task 2 (Execute): #in my case it is 10.10.10.10

1. Send 5 packets to the target and receive response.

```
Hping3 -c 5 10.10.10.10
```

2. Send a SYN flag targeting ports 1 to 5000

```
Hping3 --scan 1-5000 -S 10.10.10.10
```

3. Send UDP Packets by crafting them with data size 600 on the Target

```
Hping3 10.10.10.10 -udp -rand-source -data 600
```

By sending this UDP packet, what did you observe at the Target machine?
Demonstrate the steps of Observation here.



Launch Wireshark in the Target Machine

4. **Send a TCP SYN Scan request to the Target through port 80 with 3 counts of packet** (*Refer to the above commands to execute this task*)

```
Hping3 -S 10.10.10.10 -p 80 -c 3
```

Document the Outcome

5. **Observe the TCP Packets in the Target using Wireshark.** Could you locate the TCP Packets?



Start a new Wireshark capture in the Target Machine

6. **Flood the Target with TCP packets**

```
Hping3 10.10.10.10 --flood
```

Document the Outcome

7. **Observe the flooding TCP Packets in the Target machine using Wireshark.** Could you look at the information of TCP packets transmitted to and from attacker machine?



Record your Reflection.



End of Task 1 (Commands), you did an Observation and Research on HPING Tool. After your Task 2 (Execute), could you able to extend your thoughts? (Like re-write/ add more thoughts/ clarity to your understanding)

List/demonstrate other tools which could be used for doing similar attacks. Compare and Contrast.

Part 2: Use MegaPing to identify live hosts and open ports of the Target..

Machine: Windows Servers 2016, 2012: Windows Client 10, 8, 7, XP: Kali, Ubuntu
(If you don't have any of the above machines, still you shall work on this activity.)

1. Download MegaPing.
2. Do an Internet Search about MegaPing. What is this tool for? Which website did you download MegaPing? Why?
3. Install MegaPing in Windows 2016.
4. Scan your Lab Network. (Look for Information like Active Host Machines, Ports, System info, DNS list host, DNS Lookup name, Network Time Synchronizer, Resources etc.



MegaPing
visit <http://www.magnetosoft.com> for sales and support.

File Created: 02/21/22 05:39:22

Address	Name	Status
192.168.1.1	3	Alive
192.168.1.2	F [redacted]	Unique
192.168.1.3	Workstation Service	Unique
192.168.1.4	Domain Name	Group
192.168.1.5	P0-4E-0B-C3-CD-1C	
192.168.1.6	WORKGROUP	
192.168.1.7	0	
192.168.1.8	0	
192.168.1.9	0	
192.168.1.10	0	
192.168.1.11	0	
192.168.1.12	0	
192.168.1.13	0	
192.168.1.14	0	
192.168.1.15	0	
192.168.1.16	0	
192.168.1.17	0	
192.168.1.18	0	
192.168.1.19	0	
192.168.1.20	0	
192.168.1.21	0	

Access is denied.
Access is denied.

Traceroute

Destination: 192.168.1.51

Destination Address List

Host

Results

Hop	Time	Name	Details
1	0.00	[192.168.1.1]	Complete.
2	0.00	Request Timed Out	02/21/22 05:46:11
3	0.00	Request Timed Out	02/21/22 05:46:15
4	0.00	Request Timed Out	02/21/22 05:46:17
5	0.00	Request Timed Out	02/21/22 05:46:19
6	0.00	Request Timed Out	02/21/22 05:46:21
7	0.00	Request Timed Out	02/21/22 05:46:23
8	0.00	Request Timed Out	02/21/22 05:46:25
9	0.00	Request Timed Out	02/21/22 05:46:27
10	0.00	Request Timed Out	02/21/22 05:46:29
11	0.00	Request Timed Out	02/21/22 05:46:31
12	0.00	Request Timed Out	02/21/22 05:46:33
13	0.00	Request Timed Out	02/21/22 05:46:35
14	0.00	Request Timed Out	02/21/22 05:46:37
15	0.00	Request Timed Out	02/21/22 05:46:39
16	0.00	Request Timed Out	02/21/22 05:46:41
17	0.00	Request Timed Out	02/21/22 05:46:43
18	0.00	Request Timed Out	02/21/22 05:46:45
19	0.00	Request Timed Out	02/21/22 05:46:47
20	0.00	Request Timed Out	02/21/22 05:46:49
21	0.00	Request Timed Out	02/21/22 05:46:51

Traceroute

Destination: 192.168.1.51

Destination Address List

Host

Results

Hop	Time	Name	Details
1	0.00	[192.168.1.1]	Complete.
2	65	192.168.1.51	02/21/22 05:50:25
3	65	192.168.1.51	02/21/22 05:50:25

Traceroute

Destination: 192.168.1.51

Destination Address List

Host

Results

Name	Details
192.168.1.51	Request Failed
Error: 10061	No connection could be made because the target machine actively refused it.
Local Time:	02/21/22 05:51:25

Security Scanner

Select: Host: 192.168.1.151

Status: Completed 1 address in 415 secs

Address	Name	Status
192.168.1.151	192.168.1.151	Alive
NetBIOS Names	6	Unique
Adapter Address	WORKGROUP	Group
Domain	<Information Not Available>	Access is denied.
SNMP	0	Access is denied.
Shared Resources	0	Access is denied.
Sessions	0	Access is denied.
Printers	0	Access is denied.
Installed Programs	3	Access is denied.
Modems	loc-srv	Risk: Low
TCP Ports	netbios-ssn	Risk: Elevated
	microsoft-ds	Risk: Low

Security Scanner

Select: Host: 192.168.1.151

Status: Completed Querying Modems on 192.168.1.151 TCP Ports: 69 %

Address	Name	Status
192.168.1.151	192.168.1.151	Alive
NetBIOS Names	6	Unique
Adapter Address	WORKGROUP	Group
Domain	<Information Not Available>	Access is denied.
SNMP	0	Access is denied.
Shared Resources	0	Access is denied.
Sessions	0	Access is denied.
Printers	0	Access is denied.
Installed Programs	3	Access is denied.
Modems	loc-srv	Risk: Low
	netbios-ssn	Risk: Elevated
	microsoft-ds	Risk: Low

5. Based on your research earlier at Step 2, you might have known that MegaPing tool could look for potential vulnerabilities within your network. Did you manage to discover any vulnerabilities in your network?



6. Report

MegaPing

visit <http://www.magnetsoft.com> for sales and support.

File Created: 02/21/22 05:56:17

Address	Name	Status
192.168.1.51	192.168.1.51	Alive
NetBIOS Names	6	Unique
Adapter Address	WORKGROUP	Group
Domain	<Information Not Available>	Access is denied.
SNMP	0	Access is denied.
Shared Resources	0	Access is denied.
Sessions	0	Access is denied.
Printers	0	Access is denied.
Installed Programs	3	Access is denied.
Modems	loc-srv	Risk: Low
	netbios-ssn	Risk: Elevated
	microsoft-ds	Risk: Low

Part 3: Use NetScanTools Pro to initiate various Scans (not limited to ARP Ping Scan, DHCP Server Discovery, Ping Scan, Port Scan etc).

Note: NetScanTools Pro is one of the handy tools which could be used for various scanning and enumeration process.

Machine: Windows Servers 2016, 2012: Windows Client 10, 8, 7, XP (If you don't have any of the above machines, still you shall work on this activity.)

- 1. Download NetScanTools Pro.**
- 2. Based on our Lectures this week, (I have discussed about various scans and enumeration methods for which NetScanTools Pro could be used) could you list out the various functions of this tool?**

- 3. Install NetScanTools Pro in Windows 2016.**

*Note that, using this tool, you can do an Active operation by sending packets to the target to receive responses. **USE ONLY IN LAB ENVIRONMENT***

- 4. Scan your Lab Network. (Use Manual Tools to scan range of ports, Hostnames, IP Addresses, MAC Addresses, DHCP Servers etc).**
 - a. Use utilities like ARP Ping Tool: ARP ping will send ARP packets to the target to find the response time. As discussed in the lecture, using response time, we could gather more information.
 - b. Use utilities like ARP Scan Tool: ARP scan will send ARP packets to the range of IPs to rapidly sweep the subnet for devices that are connected.
 - c. Similarly, use many utilities available in the tool and discover information about your network.

ARP

ARP Cache

ARP Ping

ARP Scan (MAC Scan)

Cache Forensics

Connection Monitor

Country to IP or ASN

DHCP Server Discovery

DNS Tools - Core

DNS Tools - Advanced

DNS Tools - Batch Queries

DNS Traffic Monitor

Duplicate IP Scanner

Subnet: 192.168.1.1/24

Target IPv4 Address: 192.168.1.51

Send Arp

Stop

Number to Send: 16

Cycle Time (ms): 1000

Show Timing Chart

Send Broadcast ARP, then Unicast ARP

Send Broadcast ARP Only

Search for Duplicate IP Addresses

Jump To Duplicate IP Scanner

Duplicates Source IP Address

0.0.0.0

Interface IP Address

Jump To Automated

Reports

Add to Favorites

IPv4

IPv6

Index	IP Address	MAC Address	Response Time (sec)	Type
0	192.168.1.51	A4...	0.003800	Broadcast
1	192.168.1.51	A4...	0.017100	Unicast
2	192.168.1.51	A4...	0.004900	Unicast
3	192.168.1.51	A4...	0.094600	Unicast
4	192.168.1.51	A4...	0.001000	Unicast
5	192.168.1.51	A4...	0.001200	Unicast
6	192.168.1.51	A4...	0.004400	Unicast
7	192.168.1.51	A4...	0.004400	Unicast
8	192.168.1.51	A4...	0.001200	Unicast
9	192.168.1.51	A4...	0.005000	Unicast
10	192.168.1.51	A4...	0.001300	Unicast
11	192.168.1.51	A4...	0.004000	Unicast
12	192.168.1.51	A4...	0.090600	Unicast
13	192.168.1.51	A4...	0.005000	Unicast
14	192.168.1.51	A4...	0.019200	Unicast
15	192.168.1.51	A4...	0.000900	Unicast

Welcome

Automated Tools

Manual Tools (all)

ARP

ARP Cache

ARP Ping

ARP Scan (MAC Scan)

Cache Forensics

Connection Monitor

Country to IP or ASN

DHCP Server Discovery

DNS Tools - Core

DNS Tools - Advanced

Use this tool to find all active IPv4 devices on your subnet.

Network Interface: Wi-Fi (192.168.1.57) - TP-LINK Wireless USB Adapter

Starting IPv4 Address: 192.168.1.1

Ending IPv4 Address: 192.168.1.60

Do Arp Scan

Stop

Scan Delay Time (ms): 10

Packets sent per IP: 3

Resolve IPs

Include Local I/F Info

Defaults

Jump To Dupe IP Scan

ARP Scanner Response Summary

1: Response, 6

2: +Other Local I/F, 1

3: No Response, 54

IPv4 Address	MAC Address	I/F Manufacturer	Hos...	Notes or Comments
192.168.1.1	44-AD-...			ttr...
192.168.1.1	B8-5F-...			?
192.168.1.1	10-7B-...	AS...		?
192.168.1.1	D4-63-...	...		ality ... ?
192.168.1.1	F0-6E-...	Micr...		
192.168.1.1	A4-17-...	...		ion ... Eli...
192.168.1.1	98-DE-...	...		hos...

Target Hostname or IPv4 Address

Network Interface

192.168.1.1

X

Wi-Fi (192.168.1.57) - [REDACTED]

Add Note

Jump To Automated

Reports

Add to Favorites

Completed.

Analyze Target

Stop

Settings

Start Time: Mon, 21 Feb 2022 06:21:09

Target: 192.168.1.1 [192.168.1.1]

Hops: 1

TargetReached? Yes

Possible Operating System(s):

Windows 7 - 32 or 64 bit

5. Based on your usage of this tool, and earlier tools within your lab network, what are the additional details you gathered after using this tool?



6. Report

NetScanTools® Pro v11 ✱ Reports Created with DEMO v11.11 Buy from: www.netscantools.com				
Report created with NetScanTools Pro v11 DEMO. Purchase NetScanTools Pro at www.netscantools.com				
Test Results Report				
Report Print Date and Time: 02/21/22 06:35:29				
Results Database: demo				
Analyst:				
Title:				
Organization:				
Target: Multiple targets.				
All tests in the database for the above target are shown.				
Test: ARP D				
Input: 192.168.1.1				
Reference: 1645424				
Results:				
Index	IP Address	MAC Address	Response Time (sec)	Type
0	192.168.1.1	A4:57:45:00:00:00	0.003800	Broadcast
1	192.168.1.2	A4:57:45:00:00:00	0.017100	Unicast
2	192.168.1.3	A4:57:45:00:00:00	0.004900	Unicast
3	192.168.1.4	A4:57:45:00:00:00	0.094600	Unicast
4	192.168.1.5	A4:57:45:00:00:00	0.001000	Unicast
5	192.168.1.6	A4:57:45:00:00:00	0.001200	Unicast
6	192.168.1.7	A4:57:45:00:00:00	0.004400	Unicast
7	192.168.1.8	A4:57:45:00:00:00	0.004400	Unicast
8	192.168.1.9	A4:57:45:00:00:00	0.001200	Unicast
9	192.168.1.10	A4:57:45:00:00:00	0.005000	Unicast
10	192.168.1.11	A4:57:45:00:00:00	0.001300	Unicast
11	192.168.1.12	A4:57:45:00:00:00	0.004000	Unicast
12	192.168.1.13	A4:57:45:00:00:00	0.090600	Unicast

Part 4: Explore various network scanning Techniques

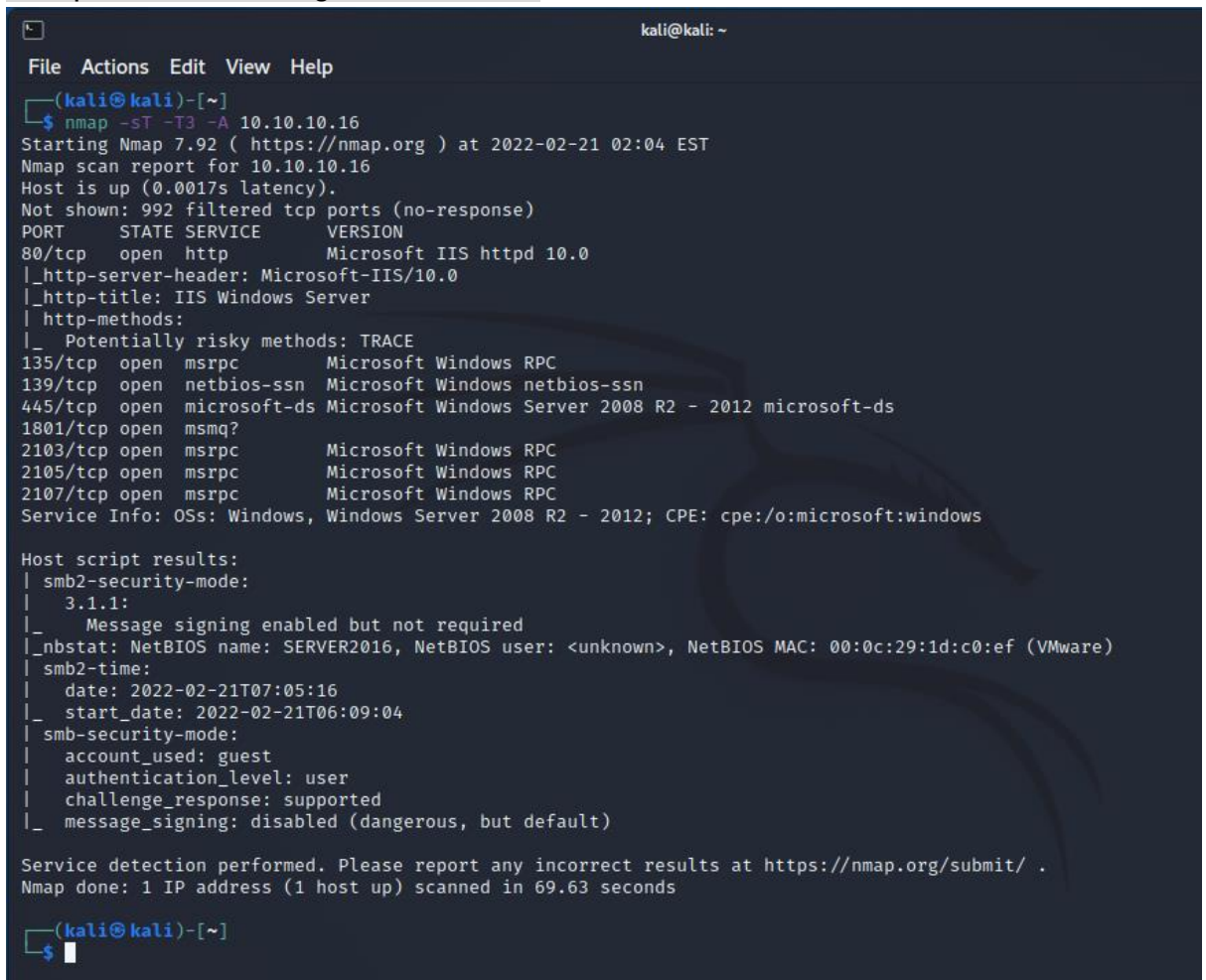
Machine: Windows Servers 2016, 2012: Kali Linux (If you don't have any of the above machines, still you shall work on this activity).

Use Nmap to do a TCP Connect scan, Xmas Scan, ACK Flag scan, UDP Scan and IDLE Scan.

Task

1. Login to Win Server 2012, Win Server 2016 & Kali Linux
2. Perform a TCP Connect Scan on Win Server 2016. (Refer to TCP Connect Scan during our Lecture)

Nmap -St -T3 -A <Target IP Address>



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -sT -T3 -A 10.10.10.16  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-21 02:04 EST  
Nmap scan report for 10.10.10.16  
Host is up (0.0017s latency).  
Not shown: 992 filtered tcp ports (no-response)  
PORT      STATE SERVICE      VERSION  
80/tcp    open  http         Microsoft IIS httpd 10.0  
|_ http-server-header: Microsoft-IIS/10.0  
|_ http-title: IIS Windows Server  
|_ http-methods:  
|_ Potentially risky methods: TRACE  
135/tcp   open  msrpc        Microsoft Windows RPC  
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn  
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds  
1801/tcp  open  msmq?          
2103/tcp  open  msrpc        Microsoft Windows RPC  
2105/tcp  open  msrpc        Microsoft Windows RPC  
2107/tcp  open  msrpc        Microsoft Windows RPC  
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows  
  
Host script results:  
| smb2-security-mode:  
|   3.1.1:  
|_   Message signing enabled but not required  
|_ nbstat: NetBIOS name: SERVER2016, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:1d:c0:ef (VMware)  
| smb2-time:  
|   date: 2022-02-21T07:05:16  
|   start_date: 2022-02-21T06:09:04  
| smb-security-mode:  
|   account_used: guest  
|   authentication_level: user  
|   challenge_response: supported  
|_   message_signing: disabled (dangerous, but default)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 69.63 seconds  
(kali@kali)-[~]  
$
```

From the above screenshot, you might notice that the result gives you all open ports, OS Fingerprinting results, nbstat, smb details etc.

3. Perform a Xmas Scan on Win Server 2016. (Refer to Xmas Scan during our Lecture). Note that we are sending a TCP Frame to the target with PSH, URG & FIN flags set.

```

# nmap -sA -v -T4 10.10.10.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-21 02:18 EST
Initiating ARP Ping Scan at 02:18
Scanning 10.10.10.16 [1 port]
Completed ARP Ping Scan at 02:18, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:18
Completed Parallel DNS resolution of 1 host. at 02:18, 0.02s elapsed
Initiating ACK Scan at 02:18
Scanning 10.10.10.16 [1000 ports]
Completed ACK Scan at 02:18, 2.56s elapsed (1000 total ports)
Nmap scan report for 10.10.10.16
Host is up (0.00048s latency).
All 1000 scanned ports on 10.10.10.16 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 00:0C:29:1D:C0:EF (VMware)

Read data files from: /usr/bin/../../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.80 seconds
Raw packets sent: 1148 (45.908KB) | Rcvd: 1001 (40.028KB)

```

We are initiating ACK Scan to display the port. Could you observe that the ports are in ignored states.

- ✓ Why?
- ✓ Is it because of Firewall? Is our Firewall Off or On? Try the viceversa.



Maybe, Yes!!! Initially, we might have turned the Firewall Off. Turn them On and execute Xmas scan with aggressive timing. Here the timing is -T4. Again, Turn them Off and execute the same.

```

(kali@kali)-[~]
$ nmap -sX -T4 10.10.10.16
You requested a scan type which requires root privileges.
QUITTING!

(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# nmap -sX -T4 10.10.10.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-21 02:11 EST
Nmap scan report for 10.10.10.16
Host is up (0.00034s latency).
All 1000 scanned ports on 10.10.10.16 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:1D:C0:EF (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds

(root@kali)-[/home/kali]
# nmap -sX -T4 10.10.10.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-21 02:12 EST
Nmap scan report for 10.10.10.16
Host is up (0.00049s latency).
All 1000 scanned ports on 10.10.10.16 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:0C:29:1D:C0:EF (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.66 seconds

```

Can you identify the difference between firewall status? With reference to our lecture, ACK probe could be sent with random sequence number on the target.

If there is an response saying unfiltered, then it means the port is closed. If there is no response, then the port is filtered.

In all my scans, the ports are in ignored states. Could you able to find out a way to identify the status of the ports? Do some research.



4. Perform UDP Scan on Win Server 2016. (Refer to UDP Scan during our Lecture).

Lets find out the UDP ports on the target. I used -T5 to send packets quicker which waits only for 0.3 seconds for the response.

```
(root@kali)~/home/kali
# nmap -sU -T5 10.10.10.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-21 02:21 EST
Warning: 10.10.10.16 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.10.16
Host is up (0.00046s latency).
Not shown: 988 open|filtered udp ports (no-response)
PORT      STATE SERVICE
19/udp    closed chargen
137/udp    open  netbios-ns
161/udp    open  snmp
3389/udp   closed ms-wbt-server
18543/udp  closed unknown
19315/udp  closed keyshadow
21902/udp  closed unknown
26407/udp  closed unknown
38498/udp  closed unknown
41058/udp  closed unknown
41896/udp  closed unknown
49503/udp  closed unknown
MAC Address: 00:0C:29:1D:C0:EF (VMware)

Nmap done: 1 IP address (1 host up) scanned in 10.14 seconds
```

Lets now do a Zombie scan. Two choices for us to test. One make Win Server 2016 as Zombie and target Windows 10 and other vice versa.

```
(root@kali)~/home/kali
# nmap -Pn -p 80 -sI 10.10.10.16 10.10.10.10
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-21 02:22 EST
Idle scan using zombie 10.10.10.16 (10.10.10.16:80); Class: Incremental
Even though your Zombie (10.10.10.16; 10.10.10.16) appears to be vulnerable to IP ID sequence prediction (class: Incremental), our attempts have failed. This generally means that either the Zombie uses a separate IP ID base for each host (like Solaris), or because you cannot spoof IP packets (perhaps your ISP has enabled egress filtering to prevent IP spoofing), or may be the target network recognizes the packet source as bogus and drops them
QUITTING!
```

```
(root@kali)~/home/kali
# nmap -Pn -p 80 -sI 10.10.10.10 10.10.10.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-21 02:23 EST
Idle scan using zombie 10.10.10.10 (10.10.10.10:80); Class: Incremental
Nmap scan report for 10.10.10.16
Host is up (0.0068s latency).

PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:1D:C0:EF (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.08 seconds
```

Observe the output. Why is the difference?



5. Perform Ping sweep Scan on Target Network. (Refer to Ping Sweep Scan during our Lecture).

```
(root@kali)~[/home/kali]
# nmap -SP 10.10.10.*
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-21 02:23 EST
Nmap scan report for 10.10.10.1
Host is up (0.00088s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 10.10.10.2
Host is up (0.00034s latency).
MAC Address: 00:50:56:F4:76:12 (VMware)
Nmap scan report for 10.10.10.10
Host is up (0.00028s latency).
MAC Address: 00:0C:29:60:3C:DA (VMware)
Nmap scan report for 10.10.10.16
Host is up (0.00034s latency).
MAC Address: 00:0C:29:1D:C0:EF (VMware)
Nmap scan report for 10.10.10.254
Host is up (0.00044s latency).
MAC Address: 00:50:56:E9:75:26 (VMware)
Nmap scan report for 10.10.10.11
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.17 seconds
(root@kali)~[/home/kali]
```

Observe the output.



After using various tools so far, what are the details you have gathered?
Document them. Include your previous activity information too.



/* THIS ACTIVITY WILL CONTINUE */