



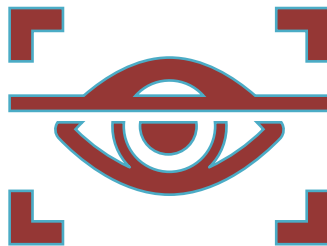
PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Advanced Cybersecurity (ACCB6000)

Scanning your Network



Objectives

Note 1: To proceed with Activity 3, completion of Activity 1 and 2 are required, which includes the following tasks:

- Testing the existing network
- Installing a security operating system
- Gathering Information about your network

The objectives of this activity must be fully achieved by completing all assigned tasks and demonstrating them during the scheduled session.

Recommendation: It is advised to complete the activities outlined in this document between Week 3 and Week 4.

1. Understand multiple ways to Gather Information both Actively and Passively.
2. Scan your Network using Tools to identify the Services and its possible vulnerabilities.

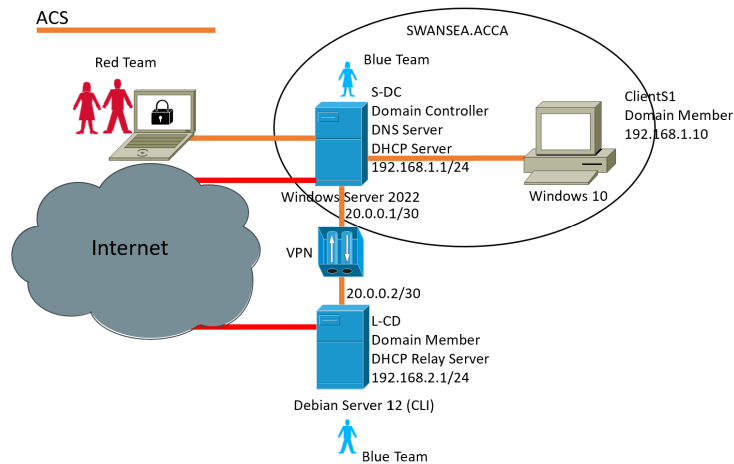
Optional Changes: Considering the number of Virtual Machines, you might ignore ClientL1 in your Activities. For Testing Purposes from a Client Machine, use ClientS1. However, if you wish to include ClientL1 in your Topology/ Testing, you are more than welcome.

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 get approval from your lecturer 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.

Lab Topology



PART 1: Scan a Network

Prior to start this activity, it is always recommended to capture a snapshot of the current VM state to back up your configurations using “Snapshot”.

“SWANSEA.ACCA” - Network

Scan and Enumerate the SWANSEA.ACCA network from Kali, targeting S-DC and L-CD.

This tutorial assumes Kali is on 192.168.1.0/24 with 192.168.1.2 as IP Address and can route via 20.0.0.0/30.

What is the Objective?

Scan and Identify any internal/external vulnerable services (DNS, DHCP, IIS) within the Network.

Here, we use NMAP. Refer to <https://nmap.org/book/port-scanning-options.html> for more information.

1. Scan the Network:

(Note: The Commands are given as Examples. Feel free to modify the commands based on your understanding)

Ping Scan

```
sudo nmap -sn 192.168.0.0/16
```

This is a ping scan (-sn) that disables port scanning and just checks if hosts respond to ICMP echo (ping) or other probes.

It's quick for discovering live hosts.

```
(securityadmin@seclogin)-[~]
└─$ sudo nmap -sn 192.168.0.0/16
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-19 20:05 BST
Nmap scan report for 192.168.1.1
Host is up (0.00044s latency).
MAC Address: 08:00:27:10:8C:B0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.2
Host is up.
Nmap scan report for 192.168.2.1
Host is up (0.0011s latency).
```

UDP Scan

```
sudo nmap -sU -p- 192.168.1.1
```

This is a udp scan Performs a UDP port scan to identify open UDP ports.

Version Detection

```
sudo nmap -sV -p 1-1024 192.168.1.1
```

Enables service version detection on specified ports.

OS Detection

```
sudo nmap -O 192.168.1.1
```

Performs OS detection by fingerprinting the target's operating system.

Aggressive Scan

```
sudo nmap -A 192.168.1.1
```

Aggressive scan combining OS detection, version scanning, script scanning, and traceroute.

Timing to Aggressive Level

```
sudo nmap -T4 -p- 192.168.1.1
```

Adjusts timing to aggressive level (T4) for faster scanning.

"full" or "connect" scan

(completes the entire TCP 3-way handshake to check port status. It's straightforward but not stealthy, as it mimics a real connection attempt)

```
sudo nmap -sT -p- 192.168.1.1 (repeat for other IPs).
```

"half-open" or "stealth" scan

it's the default Nmap TCP scan for root users. Nmap sends a SYN packet (as if starting a connection).

If the port is open, the target responds with SYN-ACK;

Nmap then sends RST to abort (no full handshake).

If closed, target sends RST. No response = filtered.

```
sudo nmap -sS -p- 192.168.1.1 (repeat for others).
```

XMAS Scan

An "inverse" or non-standard TCP flag scan

`sudo nmap -sX -p- 192.168.1.1` (repeat for others).

On Linux (Debian), you might see more "open|filtered" results; on Windows, it may mark everything as closed.

Note differences on Windows vs. Debian. Why might this scan fail on certain OSes?

SYN/FIN Scan (TCP FIN Scan)

Another inverse flag scan using the FIN flag, often grouped with SYN but distinct—here, it refers to FIN scan, sometimes combined in discussions with SYN for contrast.

`sudo nmap -sF -p- 192.168.1.1` (repeat for others).

Run and compare to XMAS. How does the single FIN flag change results vs. multiple flags?

ACK Scan

A scan focused on mapping firewall rules rather than port states directly.

`sudo nmap -sA -p- 192.168.1.1` (repeat for others).

Use this after a SYN scan. Which ports appear filtered? Discuss firewall implications.

Inverse TCP Flag Scan (TCP Null Scan)

A broad term for scans using invalid or no flags (inverse to normal TCP), often referring to Null scan (-sN), but encompassing FIN/XMAS too—here,

`sudo nmap -sN -p- 192.168.1.1` (repeat for others).

Compare to other inverse scans (XMAS, FIN). Why are these called "inverse"?

Outputs

`sudo nmap -oN scan_results.txt 192.168.1.1`

Outputs scan results to a normal (human-readable) file.

To help you Understand further – Discuss with your Class:
Can you Identify the Scans below? What scans are done below?

```
(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
```

a.

```
(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
```

b.

```
(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!
```

c.

```
(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
```

d.

```
(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
```

e.

Observe the output. What scans are these?

1. ?
2. ?
3. ?
4. ?
5. ?

2. Enumerate using Nmap and Net Use

[Using this technique, we could gather User names, User groups, List of Computers, OS, Ports, Names, Network resources, Services, Policies and Passwords]

Task

Open Nmap in Kali Linux

By default, you could see an Intense scan profile present. Do various scans on the target OS. Refer to our lecture sessions to use various nmap commands.

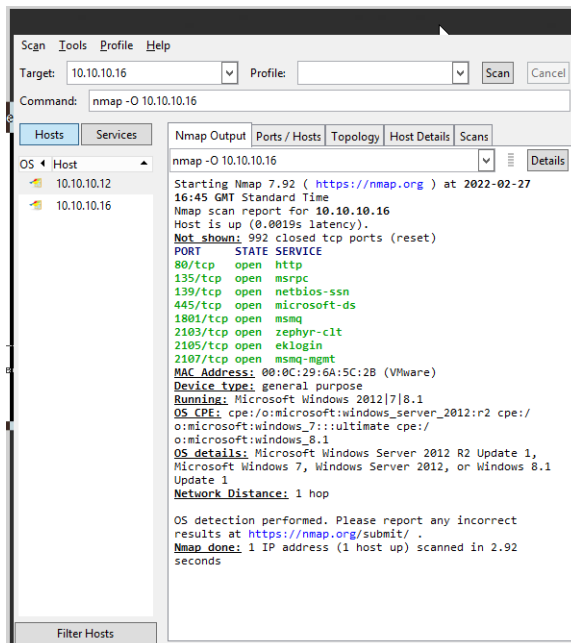
Based on the earlier activities, we have managed to find our Users, Host Names, Live Hosts, List of Machines in the Target Network etc. Now, let us focus on gathering ports open, their services and shared resources.

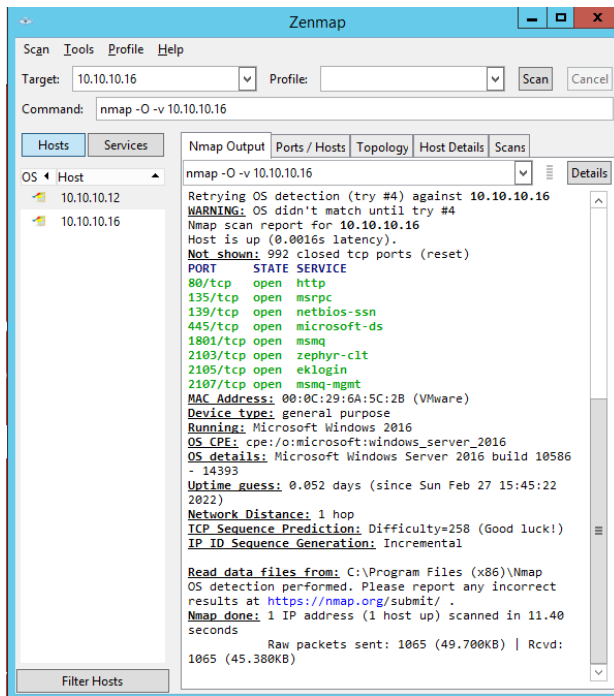
Issue the nmap command to find out the operating system. Which command would you use?

Nmap -O <Target> (Used to Fingerprint the OS of a host – Detect Operating System)

Nmap -O -v <Target> (Used to Fingerprint the OS of a host – Detect Operating System)

what is the difference between the above two commands?





From the above output/ or from your output gathered in Kali Linux (Attacker), what is your finding? Did you notice Ports 80, 135, 139, 445, 1801 etc are open and 139 is using netbios service?

Let us use NBTSTAT:

- What is NBTSTAT?
- Which OS does NBTSTAT work?
- How do you find similar information using only Kali Linux?

NBTSTAT command to look at NETBIOS related information. NBTSTAT is a diagnostic tool for NetBIOS over TCP/IP. It's primary objective is to troubleshoot NetBIOS name resolution problems. (Wikipedia)

```
C:\Users\Administrator>nbtstat -A 10.10.10.16
```

```
Ethernet0:
```

```
Node IpAddress: [10.10.10.12] Scope Id: []
```

```
NetBIOS Remote Machine Name Table
```

Name	Type	Status
SERVER2016	<00> UNIQUE	Registered
WORKGROUP	<00> GROUP	Registered
SERVER2016	<20> UNIQUE	Registered

```
MAC Address = 00-0C-29-6A-5C-2B
```

```
C:\Users\Administrator>nbtstat -A 10.10.10.12
```

```
Ethernet0:
```

```
Node IpAddress: [10.10.10.12] Scope Id: []
```

```
NetBIOS Remote Machine Name Table
```

Name	Type	Status
SERVER2012	<00> UNIQUE	Registered
WORKGROUP	<00> GROUP	Registered
SERVER2012	<20> UNIQUE	Registered

```
MAC Address = 00-0C-29-6C-7C-49
```

Now use net use command to view the created shared folders from your hosts.

```
C:\Users\Administrator>net use
New connections will be remembered.
```

Status	Local	Remote	Network
	Z:	\\vmware-host\Shared Folders	UMware Shared Folders

```
The command completed successfully.
```

Do research on net use. Know what is the purpose of net use command? Which OS versions is that supported etc.?

Execute further more commands (not limited to)***nmap -sP 10.0.0.0/24***

```
(kali㉿kali)-[~]
$ nmap -sP 10.10.10.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-27 12:23 EST
Nmap scan report for 10.10.10.2
Host is up (0.00093s latency).
Nmap scan report for 10.10.10.11
Host is up (0.0020s latency).
Nmap scan report for 10.10.10.12
Host is up (0.0039s latency).
Nmap scan report for 10.10.10.16
Host is up (0.0019s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.53 seconds
```

Nmap -sS 10.10.10.12

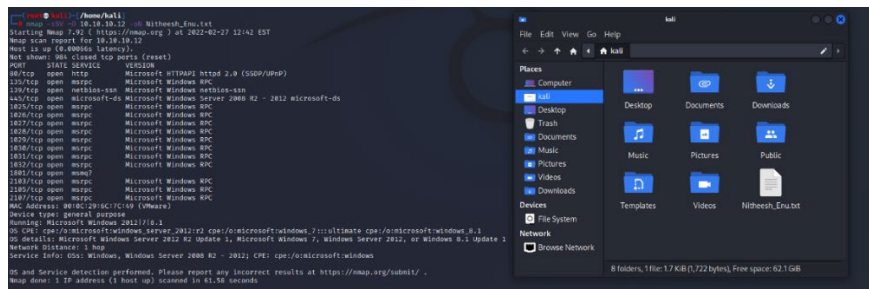
```
~# nmap -sS 10.10.10.12
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-27 12:29 EST
Nmap scan report for 10.10.10.12
Host is up (0.00049s latency).
Not shown: 984 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1025/tcp   open  NFS-or-IIS
1026/tcp   open  LSA-or-nterm
1027/tcp   open  IIS
1028/tcp   open  unknown
1029/tcp   open  ms-lsa
1030/tcp   open  iad1
1031/tcp   open  iad2
1032/tcp   open  iad3
1801/tcp   open  msmq
2103/tcp   open  zephyr-clt
2105/tcp   open  eklogin
2107/tcp   open  msmq-mgmt
```

nmap -ssV -O 10.10.10.12

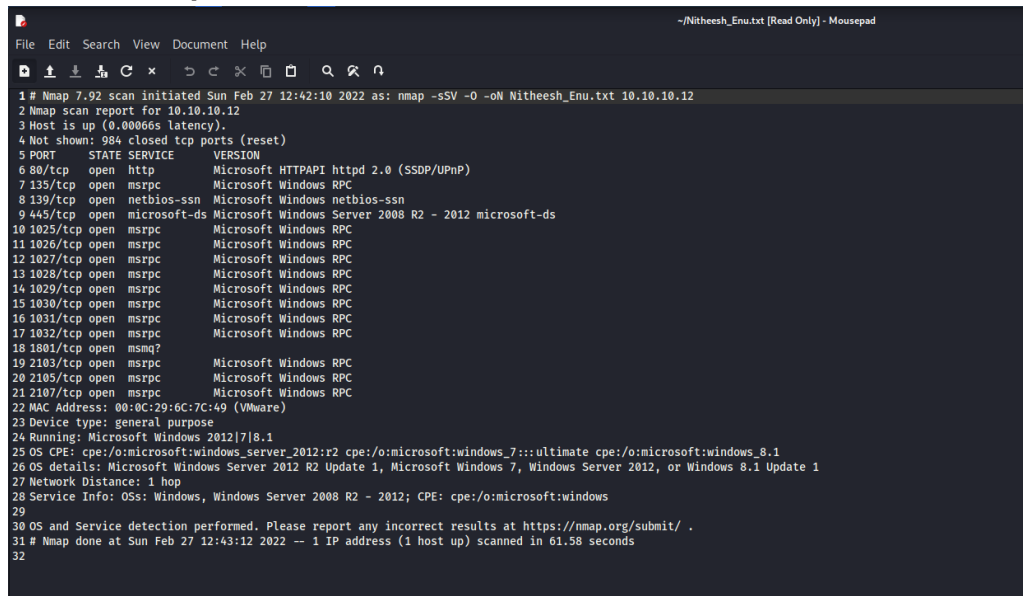
```
(root㉿kali)-[/home/kali]
# nmap -ssV -O 10.10.10.12
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-27 12:36 EST
Nmap scan report for 10.10.10.12
Host is up (0.00047s latency).
Not shown: 984 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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
1025/tcp   open  msrpc        Microsoft Windows RPC
1026/tcp   open  msrpc        Microsoft Windows RPC
1027/tcp   open  msrpc        Microsoft Windows RPC
1028/tcp   open  msrpc        Microsoft Windows RPC
1029/tcp   open  msrpc        Microsoft Windows RPC
1030/tcp   open  msrpc        Microsoft Windows RPC
1031/tcp   open  msrpc        Microsoft Windows RPC
1032/tcp   open  msrpc        Microsoft Windows RPC
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
MAC Address: 00:0C:29:6C:7C:49 (VMware)
Device type: general purpose
Running: Microsoft Windows 2012|7|8.1
OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_7:::
ultimate cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Server 2012 R2 Update 1, Microsoft Windows 7, W
indows Server 2012, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:micros
oft:windows

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 79.12 seconds
```

Save this report to a txt file with your name. What command do you use to save?



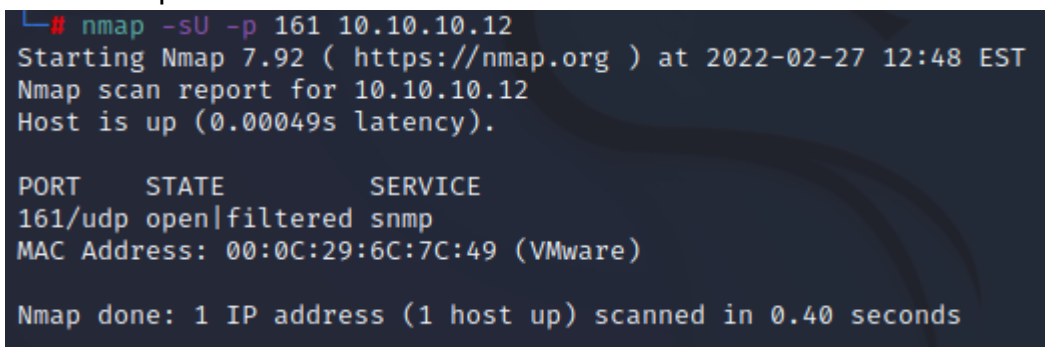
Save the Report



SNMP

Which is the default port for SNMP?

Check the port status.



From the above output, knowing that SNMP Service is running in port 161 and the status is open, execute a script to extract the SNMP Community string from the target machine.

```
# nmap -sU -p 161 --script=snmp-brute 10.10.10.12
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-27 13:22 EST
Nmap scan report for 10.10.10.12
Host is up (0.00042s latency).

PORT      STATE      SERVICE
161/udp    open|filtered snmp
MAC Address: 00:0C:29:6C:7C:49 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.78 seconds
```

```
(root@kali)~[/home/kali]
# nmap -sU -p 161 --script=snmp-brute 10.10.10.12
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-27 13:24 EST
Nmap scan report for 10.10.10.12
Host is up (0.00056s latency).

PORT      STATE SERVICE
161/udp    open  snmp
| snmp-brute:
|_ public - Valid credentials
MAC Address: 00:0C:29:6C:7C:49 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.79 seconds
```

Above two commands are same but outputs are different. Could you justify why the outputs are different? What actions was taken before executing the command second time?

With valid credentials, let us perform SNMP enumeration on the target machine.

Open MSFCONSOLE

```
(root@kali)~[/home/kali]
msfconsole

METASPLOIT CYBER MISSILE COMMAND V5

#####
# WAVE 5 ##### SCORE 11337 ##### HIGH FFFFFFFF #
#####
https://metasploit.com

+-- metasploit v6.1.29-dev
+-- --[ 2198 exploits - 1164 auxiliary - 408 post
+-- --[ 596 payloads - 45 encoders - 11 nops
+-- --[ 9 evasion

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true
```

Know about MSF console. Do research on Metasploit. A very useful tool in Kali Linux. Refer to Metasploit.com, Github for references.

Use `auxiliary/scanner/snmp/snmp_login`. Setg RHOSTS <target>. Exploit

```
msf6 > use auxiliary/scanner/snmp/snmp_login
msf6 auxiliary(scanner/snmp/snmp_login) > setg RHOSTS 10.10.10.12
RHOSTS => 10.10.10.12
msf6 auxiliary(scanner/snmp/snmp_login) > exploit

[!] No active DB -- Credential data will not be saved!
[+] 10.10.10.12:161 - Login Successful: public (Access level: read-only); Proof (sysDescr.0): Hardware: Intel64
  Family 6 Model 158 Stepping 9 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 9600 Multiprocessor Free
  )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Did you notice that the target has a read-only community string? This is the vulnerability via SNMP which could be used to exploit the target. *(If you don't understand SNMP Community String – refer to our lectures and do research)*

Use Enumeration to exploit further.

```
msf6 auxiliary(scanner/snmp/snmp_login) > use auxiliary/scanner/snmp/snmp_enum
msf6 auxiliary(scanner/snmp/snmp_enum) > exploit

[+] 10.10.10.12, Connected.

[*] System information:

Host IP           : 10.10.10.12
Hostname          : Server2012.accb.com
Description       : Hardware: Intel64 Family 6 Model 158 Stepping 9 AT/AT COMPATIBLE - Software: Wi
ndows Version 6.3 (Build 9600 Multiprocessor Free)
Contact           : -
Location          : -
Uptime snmp       : 00:23:23.07
Uptime system     : 00:22:46.53
System date       : 2022-2-27 18:33:18.3

[*] User accounts:

["Guest"]
["krbtgt"]
["Administrator"]

[*] Network information:

IP forwarding enabled : no
Default TTL           : 128
TCP segments received : 9320
TCP segments sent     : 9312
TCP segments retrans  : 8
Input datagrams       : 405
```

After enumerating the target on SNMP, what information did you gather?

In similar method, could you try to enumerate LDAP on an ADDS and modify domain user accounts?

3. Reflect on the above activities

- Understanding on all the activities
- Understanding about various tools used
- New/ Similar tools you identified and used
- Rate yourself: How confident are you to do footprinting and reconnaissance activity ethically?
- Any other Troubleshooting Steps, you need to share?

Reference:

https://www.youtube.com/playlist?list=PLddfEpDxAoTt8mx4VcThYm_hSDid1WjZd