



LAB MANUAL ON A PRACTICAL APPROACH TO NETWORK MONITORING



ESTABLISHMENT OF ADVANCED LABORATORY FOR CYBER SECURITY TRAINING TO
TECHNICAL TEACHERS
DEPARTMENT OF INFORMATION MANAGEMENT AND EMERGING ENGINEERING
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
GOVERNMENT OF INDIA

Principal Investigator: Prof. Maitreyee Dutta

Co Investigator: Prof. Shyam Sundar Pattnaik

PREPARED BY:

Prof. Maitreyee Dutta and Ms. Shweta Sharma (Technical Assistant)

Table of Contents

INTRODUCTION TO NMAP	2
FEATURES OF NMAP.....	3
SCANNING	4
HOW TO OPEN NMAP	5
STEP 1: FIND LIVE MACHINES.....	6
STEP 2: DISCOVER OPEN PORTS	7
a) TCP Connect Scan [-sT]	9
b) SYN Stealth Scan [-sS]	10
c) UDP Scan [-sU]	12
d) Idle Scan [-sI]	13
<i>Idle scan of an open port:.....</i>	<i>13</i>
<i>Idle scan of a closed port:.....</i>	<i>14</i>
<i>Idle scan of a filtered port:.....</i>	<i>14</i>
STEP 3: SCANNING BEYOND FIREWALL	16
STEP 4: IDENTIFY VULNERABILITIES.....	20
COUNTERMEASURES	23
REFERENCES.....	23

MANUAL-1:

**A Practical
Approach to
Network
Monitoring**

INTRODUCTION TO NMAP

- Nmap ("Network Mapper") is an open source tool [1] that is freely available for network discovery and vulnerability scanning.
- Nmap tool helps network administrators in identifying the devices running on the systems, discovering the accessible hosts and their services such as finding open ports and detecting security risks.
- Nmap utilizes IP packets to determine the available hosts on the network, the services provided by them, operating systems on which they are running as well as other characteristics such as packet filters/firewalls.
- Nmap sends the special crafted packets to the target hosts and received responses are analyzed by it.
- The output from Nmap is a list of scanned targets, with additional information such as port number and protocol, service name, and state(open, filtered, closed, or unfiltered).
 - Open state signifies that an application on the target machine is listening for connections on that port.
 - Filtered state implies that firewall is blocking the port and restricting Nmap to check whether it is open or closed.

- Closed ports could open up at any time and have no application listening on them.

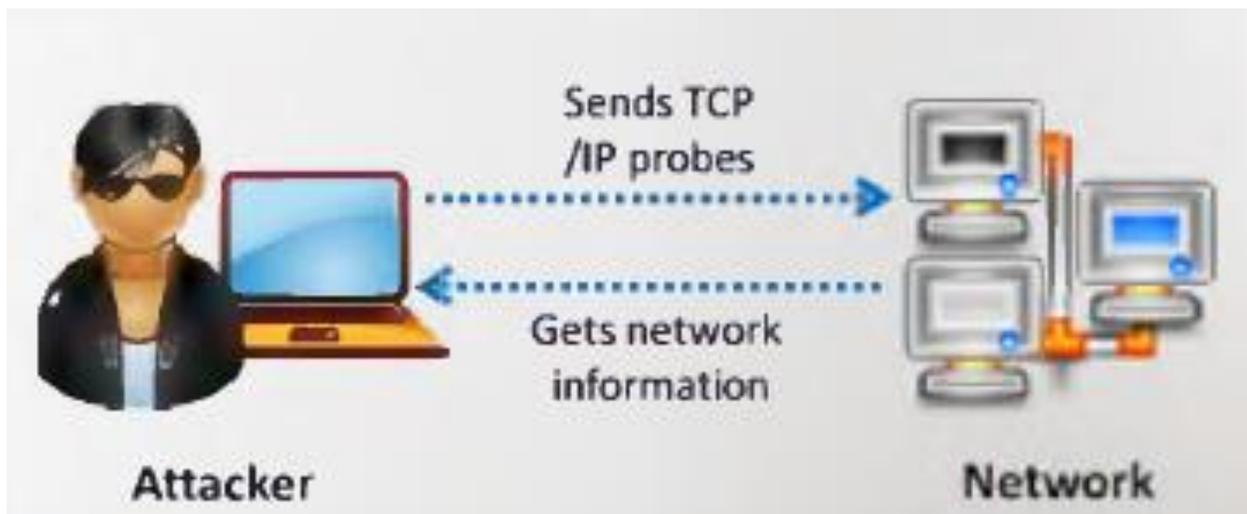


FEATURES OF NMAP

- **HOST DISCOVERY:** To identify hosts on a network. For example, listening the hosts that acknowledges to crafted TCP and/or ICMP requests or the specific port open.
- **PORT SCANNING:** To identify open ports on target hosts.
- **VERSION DETECTION:** To identify application name and version number by examining network services on remote devices
- **OS DETECTION:** To identify the operating system and hardware characteristics of network devices.

SCANNING

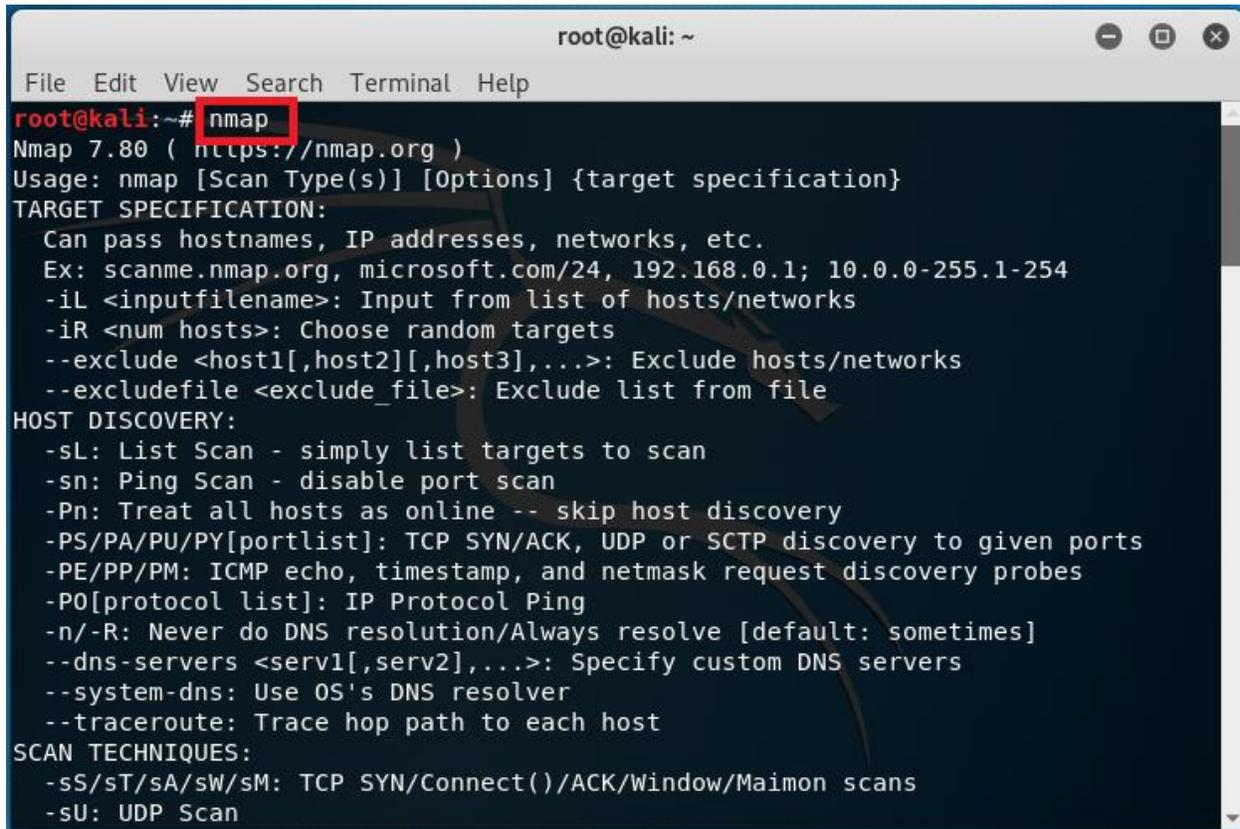
- Scanning is an active mode of information gathering.
- It refers to a set of procedures for identifying machines, open ports, and services running in network.
- The purpose is to find exploitable communication channels by discovering live machines, IP addresses, open ports, and services.
- It also identifies operating system, system architectures, and various vulnerabilities associated with it.



- The NMAP tool performs following steps of scanning:
 - Step 1: Find live machines
 - Step 2: Discover open ports
 - Step 3: Scanning beyond IDS
 - Step 4: Identify vulnerabilities

HOW TO OPEN NMAP

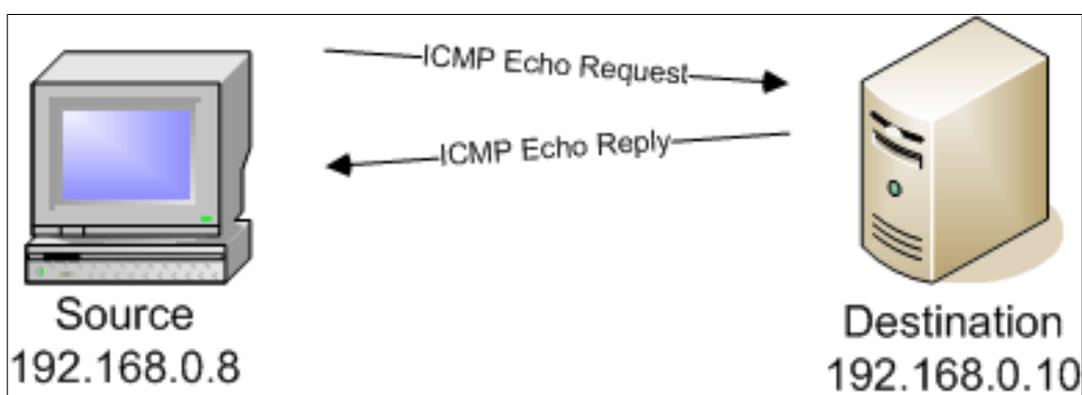
Open the Terminal in Kali Linux OS and type *nmap*.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap  
Nmap 7.80 ( https://nmap.org )  
Usage: nmap [Scan Type(s)] [Options] {target specification}  
TARGET SPECIFICATION:  
  Can pass hostnames, IP addresses, networks, etc.  
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254  
  -iL <inputfilename>: Input from list of hosts/networks  
  -iR <num hosts>: Choose random targets  
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks  
  --excludefile <exclude_file>: Exclude list from file  
HOST DISCOVERY:  
  -sL: List Scan - simply list targets to scan  
  -sn: Ping Scan - disable port scan  
  -Pn: Treat all hosts as online -- skip host discovery  
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports  
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes  
  -PO[protocol list]: IP Protocol Ping  
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]  
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers  
  --system-dns: Use OS's DNS resolver  
  --traceroute: Trace hop path to each host  
SCAN TECHNIQUES:  
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans  
  -sU: UDP Scan
```

STEP 1: FIND LIVE MACHINES

Introduction: Ping Sweep/Scan (-sP) is used to find live machines from a range of IP addresses. It sends ICMP echo request to multiple machines. In case of ping request, a single packet (56 bytes data + 08 byte header) is sent. It also determines round trip time.



Command:

```
nmap -sP <target>
```

For example:

```
nmap -sP 172.16.4.1-254
```

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sP 172.16.4.51  
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-10 01:57 EDT  
Nmap scan report for 172.16.4.51  
Host is up (0.00041s latency).  
Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds  
root@kali:~#
```

STEP 2: DISCOVER OPEN PORTS

Introduction: In computer networking, a port is a communication endpoint. For example, Server Message Block (SMB) is a network file sharing protocol used by Windows machine for file and printer sharing. It operates on TCP port number 138 and 445.

Attackers can exploit the vulnerabilities associated with SMB protocol if these ports are open. Microsoft released a patch for SMB v1 vulnerability but most of the users installed pirated version of operating system which will never be updated.

Command:

```
nmap -p <port> -v <target>
```

(-v is the verbose output to display extended information)

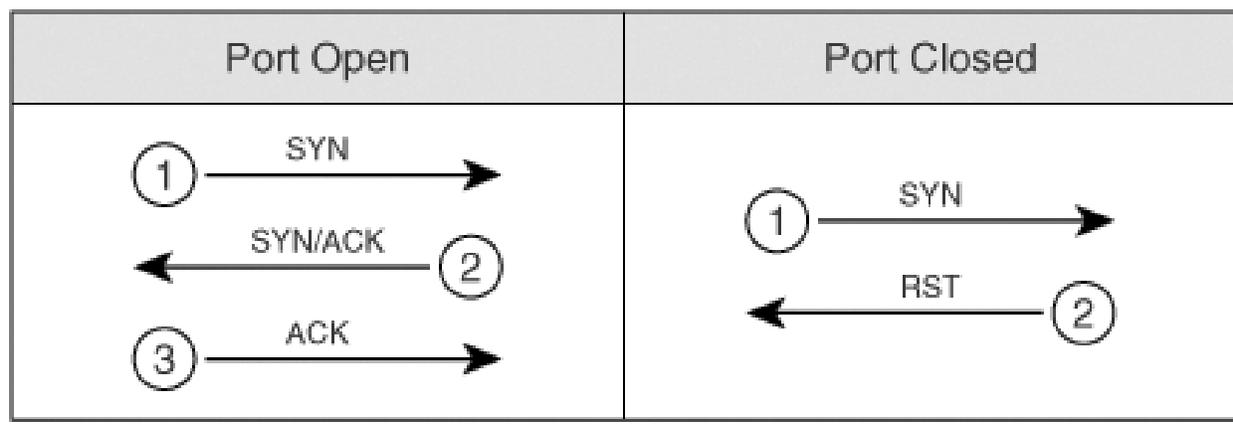
For example:

```
nmap -p 1-65535 -v 172.16.4.51
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -p 1-65535 -v 172.16.4.51
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-10 02:02 EDT
Initiating Ping Scan at 02:02
Scanning 172.16.4.51 [4 ports]
Completed Ping Scan at 02:02, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:02
Completed Parallel DNS resolution of 1 host. at 02:02, 0.01s elapsed
Initiating SYN Stealth Scan at 02:02
Scanning 172.16.4.51 [65535 ports]
Discovered open port 139/tcp on 172.16.4.51
Discovered open port 445/tcp on 172.16.4.51
Discovered open port 135/tcp on 172.16.4.51
Discovered open port 49154/tcp on 172.16.4.51
Discovered open port 49155/tcp on 172.16.4.51
Discovered open port 9012/tcp on 172.16.4.51
Discovered open port 2869/tcp on 172.16.4.51
Discovered open port 49156/tcp on 172.16.4.51
SYN Stealth Scan Timing: About 19.65% done; ETC: 02:05 (0:02:07 remaining)
Discovered open port 5357/tcp on 172.16.4.51
Discovered open port 55163/tcp on 172.16.4.51
SYN Stealth Scan Timing: About 46.93% done; ETC: 02:04 (0:01:09 remaining)
Discovered open port 5700/tcp on 172.16.4.51
Increasing send delay for 172.16.4.51 from 0 to 5 due to 32 out of 106 dropped p
robes since last increase.
```

a) TCP Connect Scan [-sT]

Introduction: TCP Connect scan detects open ports by three way handshake. It is also referred as FULL OPEN Scan.

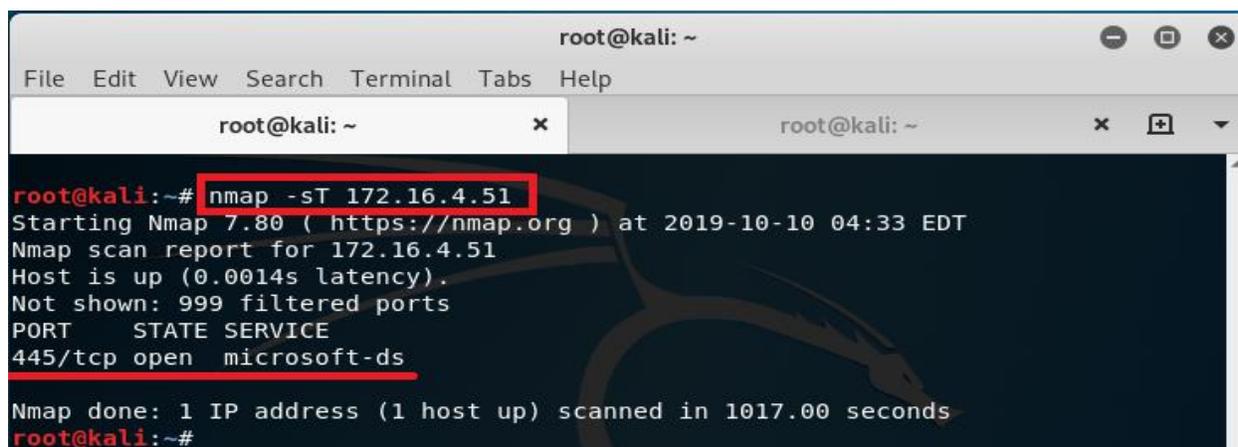


Command:

```
nmap -sT <target>
```

For example:

```
nmap -sT 172.16.4.51
```

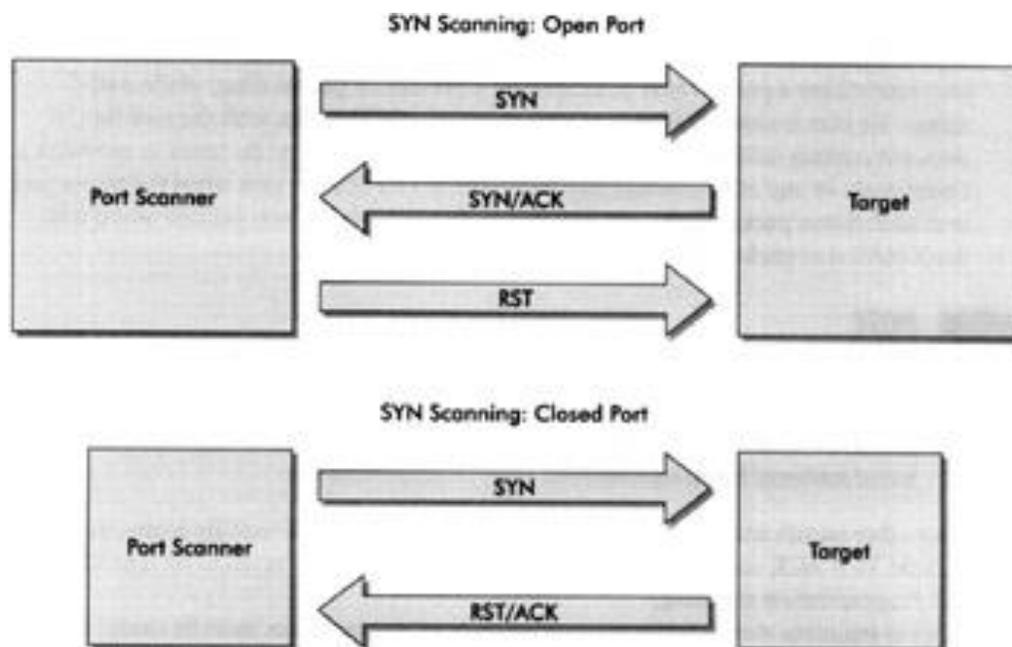


```
root@kali: ~  
File Edit View Search Terminal Tabs Help  
root@kali: ~ x root@kali: ~ x + v  
root@kali:~# nmap -sT 172.16.4.51  
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-10 04:33 EDT  
Nmap scan report for 172.16.4.51  
Host is up (0.0014s latency).  
Not shown: 999 filtered ports  
PORT      STATE SERVICE  
445/tcp  open  microsoft-ds  
Nmap done: 1 IP address (1 host up) scanned in 1017.00 seconds  
root@kali:~#
```

b) SYN Stealth Scan [-sS]

Introduction: It is based upon TCP handshake. It is also referred as HALF OPEN Scan. In this type of scan, Nmap sends SYN packet:

- If port is open - it responds with ACK.
- If port is closed - it responds with RST.
- If port is filtered - it simply drops SYN packet.



Command:

```
nmap -sS -A -O <target> -p <port>
```

(where -A is Aggressive scan, -O is operating system)

For example:

```
nmap -sS -A -O 172.16.4.51 -p 445
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sS -A -O 172.16.4.51 -p 445
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-10 05:28 EDT
Nmap scan report for 172.16.4.51
Host is up (0.00031s latency).

PORT      STATE SERVICE          VERSION
445/tcp   open  microsoft-ds    Windows 8 Pro with Media Center 9200 microsoft-ds (workgroup: WORKGROUP)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows XP|7|2012
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
OS details: Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012
Network Distance: 2 hops
Service Info: Host: SHWETA; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: mean: -53m45s, deviation: 3h10m30s, median: 56m13s
|_ nbstat: NetBIOS name: SHWETA, NetBIOS user: <unknown>, NetBIOS MAC: 04-17-56-56-12-7E (Dell)
|_ smb-os-discovery:
|   OS: Windows 8 Pro with Media Center 9200 (Windows 8 Pro with Media Center 6.2)
|   OS CPE: cpe:/o:microsoft:windows_8::-
|   Computer name: Shweta
|   NetBIOS computer name: SHWETA\x00
|   Workgroup: WORKGROUP\x00
|_ System time: 2019-10-10T15:55:21+05:30
|_ smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
```

c) UDP Scan [-sU]

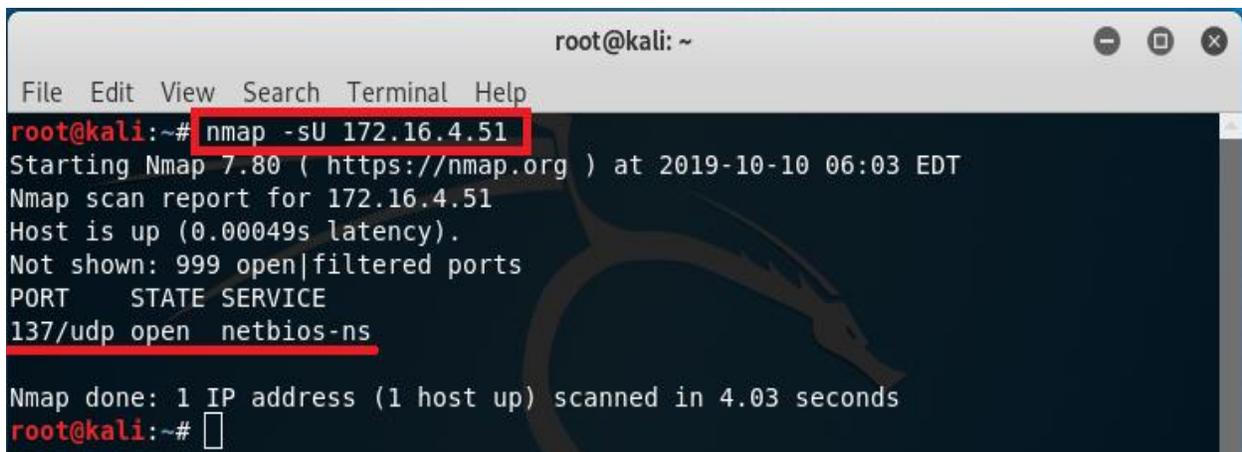
Introduction: This type of scan is used to scan UDP ports. Nmap sends the 0 byte UDP packets. If source receives an ICMP Port Unreachable message, then the Port is closed.

Command:

```
nmap -sU <target>
```

For example:

```
nmap -sU 172.16.4.51
```



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sU 172.16.4.51  
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-10 06:03 EDT  
Nmap scan report for 172.16.4.51  
Host is up (0.00049s latency).  
Not shown: 999 open|filtered ports  
PORT      STATE SERVICE  
137/udp  open  netbios-ns  
Nmap done: 1 IP address (1 host up) scanned in 4.03 seconds  
root@kali:~#
```

d) Idle Scan [-sI]

Introduction: An idle scan contains three steps that are repeatedly followed for each of the port:

- Step 1: Probe the zombie's IP ID and record it.
- Step 2: Forge a SYN packet from the zombie and send it to the desired port on the target. Depending on the port state, the target's reaction may or may not cause the zombie's IP ID to be incremented.
- Step 3: Probe the zombie's IP ID again. The target port state is then determined by comparing this new IP ID with the previous recorded step.

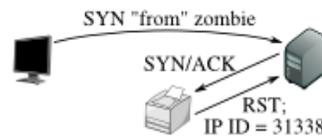
Idle scan of an open port:

Step 1: Probe the zombie's IP ID.



The attacker sends a SYN/ACK to the zombie. The zombie, not expecting the SYN/ACK, sends back a RST, disclosing its IP ID.

Step 2: Forge a SYN packet from the zombie.



The target sends a SYN/ACK in response to the SYN that appears to come from the zombie. The zombie, not expecting it, sends back a RST, incrementing its IP ID in the process.

Step 3: Probe the zombie's IP ID again.



The zombie's IP ID has increased by 2 since step 1, so the port is open!

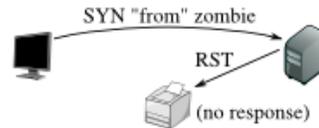
Idle scan of a closed port:

Step 1: Probe the zombie's IP ID.



The attacker sends a SYN/ACK to the zombie. The zombie, not expecting the SYN/ACK, sends back a RST, disclosing its IP ID. This step is always the same.

Step 2: Forge a SYN packet from the zombie.



The target sends a RST (the port is closed) in response to the SYN that appears to come from the zombie. The zombie ignores the unsolicited RST, leaving its IP ID unchanged.

Step 3: Probe the zombie's IP ID again.



The zombie's IP ID has increased by only 1 since step 1, so the port is not open.

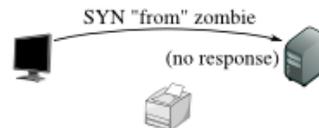
Idle scan of a filtered port:

Step 1: Probe the zombie's IP ID.



Just as in the other two cases, the attacker sends a SYN/ACK to the zombie. The zombie discloses its IP ID.

Step 2: Forge a SYN packet from the zombie.



The target, obstinately filtering its port, ignores the SYN that appears to come from the zombie. The zombie, unaware that anything has happened, does not increment its IP ID.

Step 3: Probe the zombie's IP ID again.



The zombie's IP ID has increased by only 1 since step 1, so the port is not open. From the attacker's point of view this filtered port is indistinguishable from a closed port.

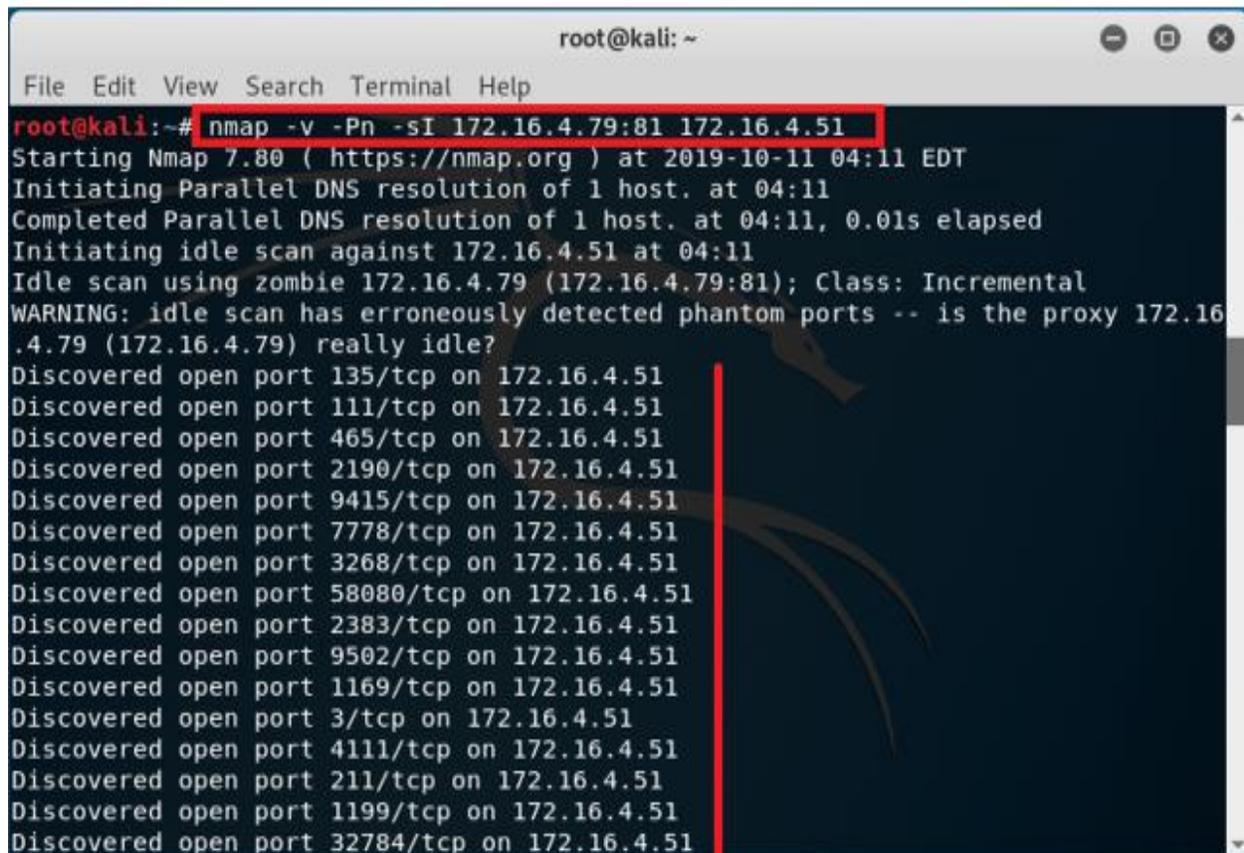
Command:

```
nmap -V -Pn -sl <zombie-address> :<port no.> <victim's address>
```

(By default port no. is 80)

For example:

```
nmap -v -Pn -sI 172.16.4.79:81 172.16.4.51
```

A terminal window titled 'root@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The command 'nmap -v -Pn -sI 172.16.4.79:81 172.16.4.51' is entered and highlighted with a red box. The output shows the start of an idle scan using the proxy 172.16.4.79:81 against the target 172.16.4.51. A warning message states: 'WARNING: idle scan has erroneously detected phantom ports -- is the proxy 172.16.4.79 (172.16.4.79) really idle?'. Below this, a list of discovered open ports on the target is shown, including 135/tcp, 111/tcp, 465/tcp, 2190/tcp, 9415/tcp, 7778/tcp, 3268/tcp, 58080/tcp, 2383/tcp, 9502/tcp, 1169/tcp, 3/tcp, 4111/tcp, 211/tcp, 1199/tcp, and 32784/tcp. A vertical red line is present in the terminal output.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -v -Pn -sI 172.16.4.79:81 172.16.4.51
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-11 04:11 EDT
Initiating Parallel DNS resolution of 1 host. at 04:11
Completed Parallel DNS resolution of 1 host. at 04:11, 0.01s elapsed
Initiating idle scan against 172.16.4.51 at 04:11
Idle scan using zombie 172.16.4.79 (172.16.4.79:81); Class: Incremental
WARNING: idle scan has erroneously detected phantom ports -- is the proxy 172.16
.4.79 (172.16.4.79) really idle?
Discovered open port 135/tcp on 172.16.4.51
Discovered open port 111/tcp on 172.16.4.51
Discovered open port 465/tcp on 172.16.4.51
Discovered open port 2190/tcp on 172.16.4.51
Discovered open port 9415/tcp on 172.16.4.51
Discovered open port 7778/tcp on 172.16.4.51
Discovered open port 3268/tcp on 172.16.4.51
Discovered open port 58080/tcp on 172.16.4.51
Discovered open port 2383/tcp on 172.16.4.51
Discovered open port 9502/tcp on 172.16.4.51
Discovered open port 1169/tcp on 172.16.4.51
Discovered open port 3/tcp on 172.16.4.51
Discovered open port 4111/tcp on 172.16.4.51
Discovered open port 211/tcp on 172.16.4.51
Discovered open port 1199/tcp on 172.16.4.51
Discovered open port 32784/tcp on 172.16.4.51
```

STEP 3: SCANNING BEYOND FIREWALL

Introduction: Nmap provides feature to control time options—[-T]. The timings are: Paranoid [-T0], Sneaky [-T1], Polite [-T2], Normal [-T3], Aggressive [-T4], and Insane [-T5].

Where -T0 implies 5 minutes wait between each packet to send that make it almost impossible for firewall to detect.

Similarly,

-T1 implies 4 minutes wait between each packet to send.

-T2 implies 3 minutes wait between each packet to send.

-T3 implies 2 minutes wait between each packet to send.

-T4 implies 1 minutes wait between each packet to send.

-T5 implies no wait between each packet to send.

Command:

```
nmap -T[0-5] [target]
```

For example:

```
nmap -T5 172.16.4.51
```

```
nmap -T4 172.16.4.51
```

nmap -T3 172.16.4.51

nmap -T2 172.16.4.51

nmap -T1 172.16.4.51

nmap -T0 172.16.4.51

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -T5 172.16.4.51  
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-14 07:20 EDT  
Nmap scan report for 172.16.4.51  
Host is up (0.00100s latency).  
Not shown: 995 filtered ports  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
554/tcp   open  rtsp  
49153/tcp open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 3.34 seconds
```

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -T4 172.16.4.51  
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-03 23:01 EST  
Nmap scan report for 172.16.4.51  
Host is up (0.050s latency).  
Not shown: 996 filtered ports  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
2869/tcp  open  icslap  
  
Nmap done: 1 IP address (1 host up) scanned in 47.64 seconds  
root@kali:~#
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -T3 172.16.4.51
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-03 23:00 EST
Nmap scan report for 172.16.4.51
Host is up (0.019s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 49.59 seconds
root@kali:~#
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -T2 172.16.4.51
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-30 01:39 EDT
Nmap scan report for 172.16.4.51
Host is up (0.0011s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2869/tcp  open  icslap
5357/tcp  open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 894.79 seconds
root@kali:~#
```

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -T1 172.16.4.51  
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-15 00:50 EDT  
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 172.16.4.51, 16) => Network is unreachable  
Offending packet: TCP 192.168.209.128:58931 > 172.16.4.51:1071 S ttl=54 id=922 iplen=44 seq=3267213583 win=1024 <mss 1460>  
Nmap scan report for 172.16.4.51  
Host is up (0.0017s latency).  
Not shown: 969 closed ports  
PORT      STATE      SERVICE  
33/tcp    filtered  dsp  
135/tcp   open       msrpc  
139/tcp   open       netbios-ssn  
445/tcp   open       microsoft-ds  
514/tcp   filtered  shell  
554/tcp   open       rtsp  
1071/tcp  filtered  bsquare-voip  
1086/tcp  filtered  cplscrambler-lg  
1328/tcp  filtered  ewart  
1755/tcp  filtered  wms  
1805/tcp  filtered  enl-name  
2144/tcp  filtered  lv-ffx  
2869/tcp  open       icslap  
3006/tcp  filtered  deslogind
```

```
root@kali: ~  
File Edit View Search Terminal Help  
1805/tcp  filtered  enl-name  
2144/tcp  filtered  lv-ffx  
2869/tcp  open       icslap  
3006/tcp  filtered  deslogind  
3071/tcp  filtered  csd-mgmt-port  
5718/tcp  filtered  dpm  
5801/tcp  filtered  vnc-http-1  
5877/tcp  filtered  unknown  
7106/tcp  filtered  unknown  
8031/tcp  filtered  unknown  
8651/tcp  filtered  unknown  
10004/tcp filtered  emcirmirccd  
10243/tcp open       unknown  
32784/tcp filtered  unknown  
33899/tcp filtered  unknown  
42510/tcp filtered  caerpc  
49152/tcp open       unknown  
49153/tcp open       unknown  
49154/tcp open       unknown  
49156/tcp open       unknown  
49167/tcp filtered  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 7040.01 seconds  
root@kali:~#
```

STEP 4: IDENTIFY VULNERABILITIES

Introduction: After finding the open ports and services running on it, this step identifies the vulnerabilities associated with the open ports. For example, vulnerabilities associated with the open ports of Simple Network Management Protocol (SNMP) and Server Message Block (SMB) protocols.

Simple Network Management Protocol (SNMP) is built in to virtually every network device. Network management programs (such as HP OpenView and LANDesk) use SNMP for remote network host management. Unfortunately, SNMP also presents security vulnerabilities.

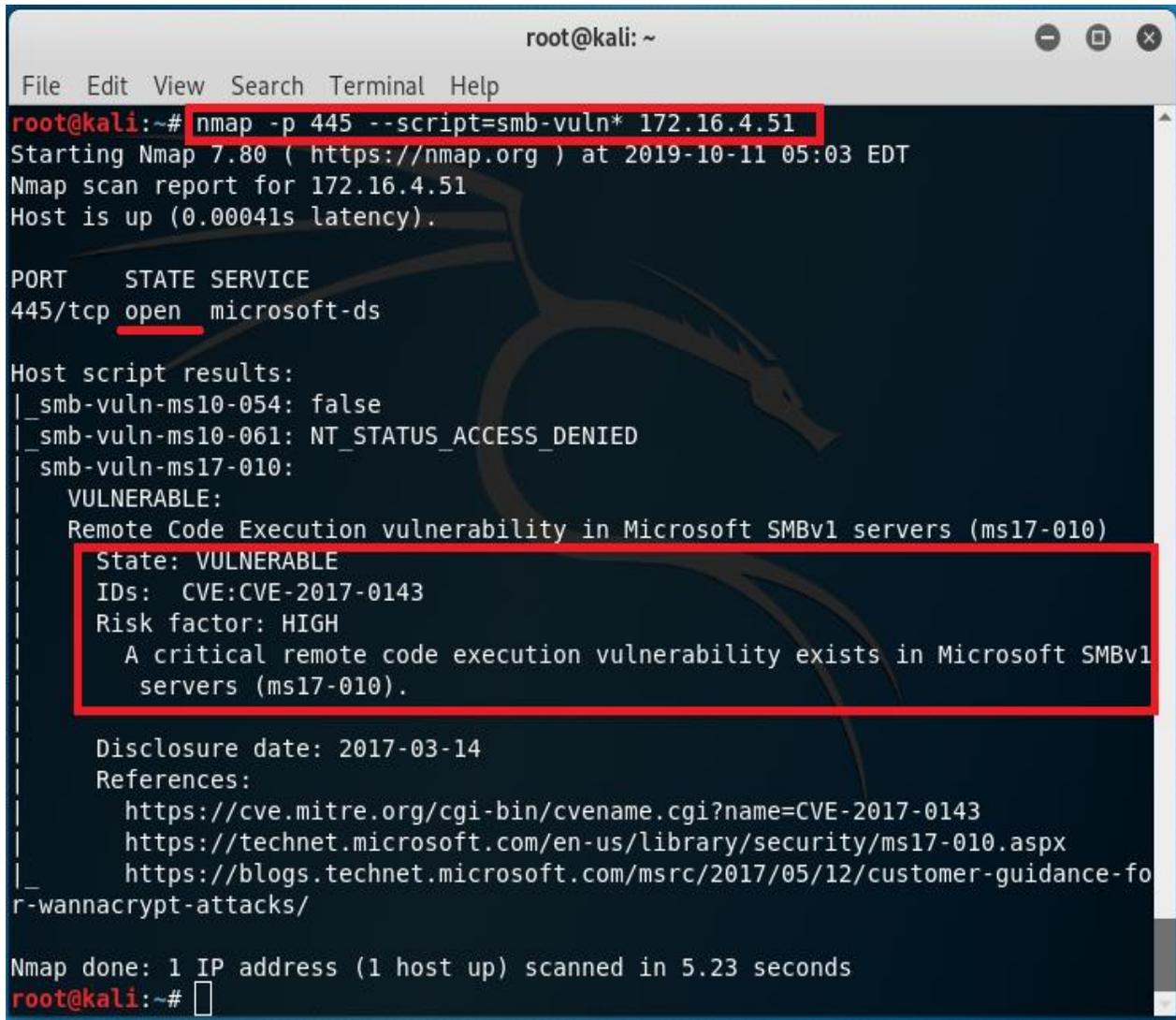
If SNMP is compromised, an attacker can collect information of network such as ARP tables, usernames, and TCP connections to perform various attacks. If SNMP shows up in port scans, then a hacker will try to hack the system.

Command:

```
nmap -p 445 --script=smb-vuln* <target>
```

For example:

```
nmap -p 445 --script=smb-vuln* 172.16.4.51
```



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -p 445 --script=smb-vuln* 172.16.4.51
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-11 05:03 EDT
Nmap scan report for 172.16.4.51
Host is up (0.00041s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|   State: VULNERABLE
|   IDs: CVE:CVE-2017-0143
|   Risk factor: HIGH
|   A critical remote code execution vulnerability exists in Microsoft SMBv1
|   servers (ms17-010).
|
|   Disclosure date: 2017-03-14
|   References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-fo
r-wannacrypt-attacks/

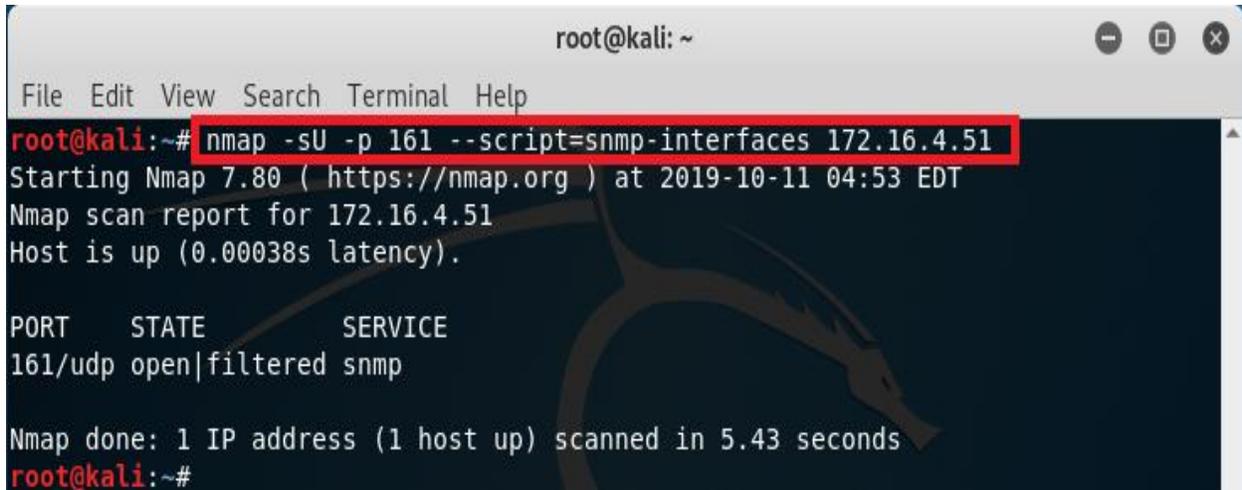
Nmap done: 1 IP address (1 host up) scanned in 5.23 seconds
root@kali:~#
```

Command:

`nmap -sU -p 161 --script=snmp-interfaces <target>`

For example:

`nmap -sU -p 161 --script=snmp-interfaces 172.16.4.51`



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sU -p 161 --script=snmp-interfaces 172.16.4.51  
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-11 04:53 EDT  
Nmap scan report for 172.16.4.51  
Host is up (0.00038s latency).  
  
PORT      STATE      SERVICE  
161/udp   open|filtered snmp  
  
Nmap done: 1 IP address (1 host up) scanned in 5.43 seconds  
root@kali:~#
```

COUNTERMEASURES

The following countermeasures must be followed:

- Always disable SNMP and SMB on hosts if not using it for a particular period of time.
- Block the SNMP ports (UDP ports 161 and 162) and SMB ports (TCP port 139 and 445) at the network perimeter.
- Change the default SNMP community read string from public and the default community write string from private to another long and complex value that's virtually impossible to guess.
- There's technically a "U" that's part of the solution: upgrade. Upgrading systems (at least the ones you can) to SNMP version 3 and SMB version 2 can resolve many of the well-known SNMP and SMB security weaknesses.

REFERENCES

- [1] O. S. Limited, "Nmap Package Description," 2020. <https://tools.kali.org/information-gathering/nmap> (accessed Jan. 20, 2020).