Department of Information Technology

Academic Year: 2022-23 **Semester: V**
Class / Branch: TE IT Subject: Security Lab (SL)
Subject Lab Incharge: Prof. Apeksha Mohite

Experiment No. 04

1. **Aim:** To use nmap for network discovery and security auditing.
2. **Software Required** : Ubuntu 14.04 OS, nmap
3. **Theory :**

Nmap (Network Mapper) is a security scanner originally written by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich) used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses. Unlike many simple port scanners that just send packets at some predefined constant rate, Nmap accounts for the network conditions (latency fluctuations, network congestion, the target interference with the scan)during the run. Also, owing to the large and active user community providing feedback and contributing to its features, Nmap has been able to extend its discovery capabilities beyond simply figuring out whether a host is up or down and which ports are open and closed; it can determinethe operating system of the target, names and versions of the listening services, estimated uptime, type of device, and presence of a firewall.

Nmap features include:

• Host Discovery – Identifying hosts on a network. For example, listing the hosts which respond to pings or have a particular port open.

• Port Scanning – Enumerating the open ports on one or more target hosts.

• Version Detection – Interrogating listening network services listening on remote devices to determine the application name and version number.

• OS Detection – Remotely determining the operating system and some hardware characteristics of network devices.

Basic commands working in Nmap:

• For target specifications: nmap <target‘s URL or IP with spaces between them>

• For OS detection: nmap -O <target-host's URL or IP>

• For version detection: nmap -sV <target-host's URL or IP>

SYN scan is the default and most popular scan option for good reasons. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls. It is also relatively unobtrusive and stealthy since it never completes TCP connections.

Installation Steps:

sudo apt-get install nmap

```
root@apsit-HP-Notebook:/# sudo apt-get install nmap
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  liblinear3 lua-lpeg ndiff python-bs4 python-chardet python-html5lib
  python-lxml python-pkg-resources
Suggested packages:
  liblinear-tools liblinear-dev python-genshi python-lxml-dbg python-lxml-doc
  python-setuptools
The following NEW packages will be installed:
  liblinear3 lua-lpeg ndiff nmap python-bs4 python-chardet python-html5lib
  python-lxml python-pkg-resources
0 upgraded, 9 newly installed, 0 to remove and 314 not upgraded.
```

How to Use Nmap Effectively

The usage of Nmap depends on the target machine because there is a difference between simple (basic) scanning and advance scanning. There is need to use some advanced techniques to bypass the firewall and intrusion detection/preventative software to get the right result. Below are the examples of some basic commands and their usage.

To scan a single system, then following command-line can be used:

nmap -sP 192.168.43.32

```
root@apsit-HP-Notebook:/# nmap -sP 192.168.43.32

Starting Nmap 7.01 ( https://nmap.org ) at 2018-09-20 10:55 IST
Nmap scan report for apsit-Satellite-C660 (192.168.43.32)
Host is up (0.030s latency).
MAC Address: B4:74:9F:11:98:28 (Askey Computer)
Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
root@apsit-HP-Notebook:/#
```

To scan the entire subnet, then the command is

nmap target/subnetmask

nmap -sP 192.168.43.32/24

```
root@apsit-HP-Notebook:/# nmap -sP 192.168.43.32/24

Starting Nmap 7.01 ( https://nmap.org ) at 2018-09-20 10:58 IST
Nmap scan report for 192.168.43.1
Host is up (0.027s latency).
MAC Address: 0A:25:25:C3:05:56 (Unknown)
Nmap scan report for apsit-Satellite-C660 (192.168.43.32)
Host is up (0.12s latency).
MAC Address: B4:74:9F:11:98:28 (Askey Computer)
Nmap scan report for apsit-HP-Notebook (192.168.43.169)
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.75 seconds
root@apsit-HP-Notebook:/#
```

To scan a multiple targets, all you need to do is to separate each target via space:

nmap target target1 target2

nmap -sP 192.168.43.32 192.168.43.169

```
root@apsit-HP-Notebook:/# nmap -sP 192.168.43.32 192.168.43.169

Starting Nmap 7.01 ( https://nmap.org ) at 2018-09-20 10:59 IST
Nmap scan report for apsit-Satellite-C660 (192.168.43.32)
Host is up (0.0071s latency).
MAC Address: B4:74:9F:11:98:28 (Askey Computer)
Nmap scan report for apsit-HP-Notebook (192.168.43.169)
Host is up.
Nmap done: 2 IP addresses (2 hosts up) scanned in 0.35 seconds
root@apsit-HP-Notebook:/#
```

To see the list of all the hosts that are being scanned, then use the command with an -sL parameter:

nmap -sL target/cdir

nmap -sL 192.168.43.32 192.168.43.169

```
root@apsit-HP-Notebook:/# nmap -sL 192.168.43.32 192.168.43.169

Starting Nmap 7.01 ( https://nmap.org ) at 2018-09-20 11:02 IST
Nmap scan report for apsit-Satellite-C660 (192.168.43.32)
Nmap scan report for apsit-HP-Notebook (192.168.43.169)
Nmap done: 2 IP addresses (0 hosts up) scanned in 0.05 seconds
root@apsit-HP-Notebook:/#
```

```
Starting Nmap 7.01 ( https://nmap.org ) at 2018-09-20 11:06 IST

root@apsit-HP-Notebook:/# nmap -sL 192.168.43.255/24 -exclude 192.168.43.32

Starting Nmap 7.01 ( https://nmap.org ) at 2018-09-20 11:06 IST
Nmap scan report for 192.168.43.0
Nmap scan report for 192.168.43.1
Nmap scan report for 192.168.43.2
Nmap sc
Nmap sc
Nmap sc
Nmap scan report for 192.168.43.26
Nmap scan report for 192.168.43.27
Nmap scan report for 192.168.43.28
Nmap scan report for 192.168.43.29
Nmap scan report for 192.168.43.30
Nmap scan report for 192.168.43.31
Nmap scan report for 192.168.43.33
Nmap scan report for 192.168.43.34
Nmap scan report for 192.168.43.35
Nmap scan report for 192.168.43.36
Nmap scan report for 192.168.43.37
Nmap scan report for 192.168.43.38
```

To scan the entire subnet but not a specific IP addresses because it might be dangerous for us. In this scenario, use the Nmap command with the excluding parameter:

IP address 192.168.43.32 is excluded in nmap scan.

To scan a specific port on the target machines (for example, To scan the HTTP, FTP, and Telnet port only on the target computer), then the Nmap command with the relevant parameter can be used. Following command-line **scan the target for port number 80,21 and 23.**

nmap -p 80,21,23 192.168.43.32

```
root@apsit-HP-Notebook:/# nmap -p 80,21,23 192.168.43.32

Starting Nmap 7.01 ( https://nmap.org ) at 2018-09-20 11:18 IST
Nmap scan report for apsit-Satellite-C660 (192.168.43.32)
Host is up (0.022s latency).
PORT   STATE SERVICE
21/tcp open  ftp
23/tcp open  telnet
80/tcp open  http
MAC Address: B4:74:9F:11:98:28 (Askey Computer)

Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds
root@apsit-HP-Notebook:/#
```

To know the open ports on target system:nmap -open 192.168.43.32

nmap -open 192.168.43.32

```
root@apsit-HP-Notebook:/# nmap -open 192.168.43.32

Starting Nmap 7.01 ( https://nmap.org ) at 2018-09-20 11:20 IST
Nmap scan report for apsit-Satellite-C660 (192.168.43.32)
Host is up (0.013s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
5432/tcp open  postgresql
MAC Address: B4:74:9F:11:98:28 (Askey Computer)

Nmap done: 1 IP address (1 host up) scanned in 3.49 seconds
root@apsit-HP-Notebook:/#
```

Scans the N highest-ratio ports found in nmap-services file:

nmap --top-ports 5 192.168.43.32

```
root@apsit-HP-Notebook:/# nmap --top-ports 5 192.168.43.32

Starting Nmap 7.01 ( https://nmap.org ) at 2018-09-20 13:21 IST
Nmap scan report for apsit-Satellite-C660 (192.168.43.32)
Host is up (0.0080s latency).
PORT    STATE  SERVICE
21/tcp  open   ftp
22/tcp  open   ssh
23/tcp  open   telnet
80/tcp  open   http
443/tcp closed https
MAC Address: B4:74:9F:11:98:28 (Askey Computer)

Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
root@apsit-HP-Notebook:/#
```

Nmap Scanning Techniques

There are so many scanning techniques available on Nmap. Few important and frequently used techniques are discussed.

Table 1: Scanning Techniques

Scanning Technique	Syntax	Use
TCP SYN	-sS	Stealth scan
TCP connect()	-sT	Scan without root privileges
FIN	-sF	Stealth scan
Xmas	-sX	Stealth scan
Null	-sN	Stealth scan
Ping	-sP	Identify live hosts
Version Detection	-sV	Identify services
UDP	-sU	Find UDP services
IP Protocol	-sO	Discover supported protocols
ACK	-sA	Identify firewalls
Window	-sW	Advanced ACK scan
RPC	-sR	Information on RPC services
List	-sL	Dummy for test purposes
Idle	-sI	Scan via third party
FTP Bounce	-b	Historic

Scan Type	Syntax	Example
TCP SYN Scan	-sS	nmap –sS 10.20.3.100
TCP Connect Scan	-sT	nmap –sT 10.20.3.100
Fin Scan	-sF	nmap –sF 10.20.3.100
XMAS Scan	-sX	nmap –sX 10.20.3.100
Null Scan	-sN	nmap –sN 10.20.3.100
Ping Scan	-sP	nmap –sP 10.20.3.100
Version Detection	-sV	nmap –sV 10.20.3.100
UDP Scan	-sU	nmap –sU 10.20.3.100
IP Protocol Scan	-sO	nmap –sO 10.20.3.100
ACK Scan	-sA	nmap –sA 10.20.3.100
Windows Scan	-sW	nmap –sW 10.20.3.100
List Scan	-sL	nmap –sL 10.20.3.100

TCP SYN Scan (-sS)

It is a basic scan, and it is also called half-open scanning because this technique allows Nmap to get information from the remote host without the complete TCP handshake process, Nmap sends SYN packets to the destination, but it does not create any sessions, As a result, the target computer can't create any log of the interaction because no session was initiated, making this feature an advantage of the TCP SYN scan. If there is no scan type mentioned on the command, then TCP SYN scan is used by default, but it requires the root/administrator privileged.

nmap -sS 192.168.43.32

```
root@apsit-HP-Notebook:/# nmap -sS 192.168.43.32

Starting Nmap 7.01 ( https://nmap.org ) at 2018-09-20 11:31 IST
Nmap scan report for apsit-Satellite-C660 (192.168.43.32)
Host is up (0.037s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
5432/tcp open  postgresql
MAC Address: B4:74:9F:11:98:28 (Askey Computer)

Nmap done: 1 IP address (1 host up) scanned in 9.64 seconds
root@apsit-HP-Notebook:/#
```

TCP connect() scan (-sT)

This the default scanning technique used, if and only if the SYN scan is not an option, because the SYN scan requires root privilege. Unlike the TCP SYN scan, it completes the normal TCP three way handshake process and requires the system to call connect(), which is a part of the operating system. This technique is only applicable to find out the TCP ports, not the UDP ports.

nmap -sT 192.168.43.32

```
apsit@apsit-HP-Notebook:~$ nmap -sT 192.168.43.32

Starting Nmap 7.01 ( https://nmap.org ) at 2018-09-20 13:16 IST
Nmap scan report for apsit-Satellite-C660 (192.168.43.32)
Host is up (0.013s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
5432/tcp open  postgresql

Nmap done: 1 IP address (1 host up) scanned in 1.58 seconds
apsit@apsit-HP-Notebook:~$
```

UDP Scan (-sU)

As the name suggests, this technique is used to find an open UDP port of the target machine. It does not require any SYN packet to be sent because it is targeting the UDP ports. Scanning can be made more effective by using -sS along with –sU. UDP scans send the UDP packets to the target machine, and waits for a response—if an error message arrives saying the ICMP is unreachable, then it means that the port is closed; but if it gets an appropriate response, then it

means that the port is open.

nmap -sU 192.168.43.32

FIN Scan (-sF)

Sometimes a normal TCP SYN scan is not the best solution because of the firewall. IDS and IPS scans might be deployed on the target machine, but a firewall will usually block the SYN packets. A FIN scan sends the packet only set with a FIN flag, so it is not required to complete the TCP handshaking. The target computer is not able to create a log of this scan (again, an advantage of FIN).

Version Detection (-sV)

Version detection is the right technique that is used to find out what software version is running on the target computer and on the respective ports. It is unlike the other scanning techniques because it is not used to detect the open ports, but it requires the information from open ports to detect the software version. In the first step of this scan technique, version detection uses the TCP SYN scan to find out which ports are open.

```
root@apsit-HP-Notebook:/# nmap -sV 192.168.43.169

Starting Nmap 7.01 ( https://nmap.org ) at 2018-09-20 13:31 IST
Nmap scan report for apsit-HP-Notebook (192.168.43.169)
Host is up (0.000025s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol
2.0)
23/tcp   open  telnet   Linux telnetd
1433/tcp open  ms-sql-s Microsoft SQL Server
```

Idle Scan (-sI)

Idle scan is an advance scan that provides complete anonymity while scanning. In idle scan, Nmap does not send the packets from your real IP address. Instead of generating the packets from the attacker machine, Nmap uses another host from the target network to send the packets. Let's consider an example to understand the concept of idle scan.

nmap -sI zombie_host target_host

The idle scan technique (as mentioned above) is used to discover the open ports on 192.168.43.32

while it uses the zombie_host (192.168.43.169) to communicate with the target host. So this is an ideal technique to scan a target computer anonymously.

nmap -sI 192.168.43.169 192.168.43.32

```
root@apsit-HP-Notebook:/# nmap -sI 192.168.43.169 192.168.43.32
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP.  On t
he other hand, timing info Nmap gains from pings can allow for faster, more reliab
le scans.

Starting Nmap 7.01 ( https://nmap.org ) at 2018-09-20 18:42 IST
Idle scan using zombie 192.168.43.169 (192.168.43.169:443); Class: Incremental
```

OS Detection by using Nmap

One of the most important feature that Nmap has is the ability to detect remote operating systems and software. It is very helpful during a penetration test to know about the operating system and the software used by the remote computer because you can easily predict the known vulnerabilitiesfrom this information.

Nmap has a database called *nmap-os-db,* the database contains information of more than 2,600 operating systems. Nmap sends TCP and UDP packets to the target machine and then it examines the response by comparing the result with the database. The Nmap operating system discovery technique is slightly slower then the scanning techniques because OS detection involves the process of finding open ports. Nmap OS fingerprinting technique discovers the: •Device type (router, work station, and so on)

•Running (running operating system)

•OS details (the name and the version of OS)

•Network distance (the distance in hops between the target and attacker)

```
root@apsit-HP-Notebook:/# nmap -O 192.168.43.32

Starting Nmap 7.01 ( https://nmap.org ) at 2018-09-20 18:44 IST
Nmap scan report for apsit-Satellite-C660 (192.168.43.32)
Host is up (0.020s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
5432/tcp open  postgresql
MAC Address: B4:74:9F:11:98:28 (Askey Computer)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.0
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/su
```

4. Conclusion: Nmap has ability to cover the very first aspects of penetration testing, which include information gathering and enumeration. It is also powerful utility that can be used as a vulnerability detector or a security scanner.