Acropolis Institute of Technology & Research, Indore

Department of Computer Science & Information Technology

EVALUATION OF INTERNSHIP REPORT

B.Tech: III Year

Project - Nmap Utility Command

Submitted to -
Prof. Nidhi Nigam

Submitted by -
Jessica Chouhan
0827CI201087
CSIT-2

Nmap utility commands

Nmap ("Network Mapper") is a free and open-source utility for network discovery and security auditing. It is a globally recognized tool mostly used by networking experts and penetration testers to find services, hosts, and open ports on a computer network. Network mapper allows its users to discover which devices are running on the network, find vulnerabilities, and detect installed services.

Features of Nmap

1. **Find security issues –** It warns users against external attackers. Nmap scans the server and finds out the path that hackers might use to attack their server.
2. **Identify open ports–** port scanning of target hosts is very easy with the help of Nmap.
3. **Detect Vulnerabilities –** To detect security vulnerabilities in the network, Nmap is the best choice.
4. **Host discovery –** Live hosts in the network can be discovered using Nmap.
5. **OS Version Detection –** Operating system and version detection are also possible through this network mapper.
6. **Provide crucial information** – Nmap also provides additional information such as devices types, reverse DNS (Domain Name System) names, MAC addresses, and IP addresses of all active hosts.

Nmap Commands

1. Scan a Range of IP Address

To scan the entire CIDR(classless inter-domain routing) range of IP addresses, you can use this command.

Command: nmap <IP range>

Output:

```
E:\>nmap 162.16.121.125-135
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-25 14:32 India Standard Time
Nmap scan report for 162.16.121.125
Host is up (0.027s latency).
All 1000 scanned ports on 162.16.121.125 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 162.16.121.126
Host is up (0.033s latency).
All 1000 scanned ports on 162.16.121.126 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 162.16.121.127
Host is up (0.031s latency).
All 1000 scanned ports on 162.16.121.127 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 162.16.121.128
Host is up (0.026s latency).
All 1000 scanned ports on 162.16.121.128 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 162.16.121.129
Host is up (0.025s latency).
All 1000 scanned ports on 162.16.121.129 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 162.16.121.130
Host is up (0.025s latency).
All 1000 scanned ports on 162.16.121.130 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 162.16.121.131
Host is up (0.024s latency).
All 1000 scanned ports on 162.16.121.131 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 162.16.121.132
Host is up (0.023s latency).
All 1000 scanned ports on 162.16.121.132 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 162.16.121.133
Host is up (0.023s latency).
All 1000 scanned ports on 162.16.121.133 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 162.16.121.134
```


```
Nmap scan report for 162.16.121.134
Host is up (0.027s latency).
All 1000 scanned ports on 162.16.121.134 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 162.16.121.135
Host is up (0.026s latency).
All 1000 scanned ports on 162.16.121.135 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 11 IP addresses (11 hosts up) scanned in 27.37 seconds
```


2. Port Scanning

Nmap is the best port scanning tool. Performing port scans will provide you with details about port services and states. It scan a specific port or entire port range.

Command: nmap -p <numeric value> <IP>

Output:

```
E:\>nmap -p 80 192.168.20.128
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-25 11:30 India Standard Time
Nmap scan report for 192.168.20.128
Host is up (0.0030s latency).

PORT   STATE    SERVICE
80/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 0.92 seconds
```

3. Ping Scan Using Nmap

This is one of the most popular and easiest Nmap commands for host detection. If you are interested in knowing which hosts are running in your network, you should use this command. It also provides the option to find out multiple hosts or any specific host. This command returns the IP address and MAC address of available hosts but provides no information about ports.

Command: Nmap -sP <target>

```
E:\> Nmap -sP 192.168.2.1/24
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-25 11:31 India Standard Time
Nmap scan report for 192.168.2.1
Host is up (0.0030s latency).
Nmap scan report for 192.168.2.2
Host is up (0.0065s latency).
Nmap scan report for 192.168.2.3
Host is up (0.0020s latency).
Nmap scan report for 192.168.2.4
Host is up (0.0020s latency).
Nmap scan report for 192.168.2.5
Host is up (0.0010s latency).
Nmap scan report for 192.168.2.6
Host is up (0.013s latency).
Nmap scan report for 192.168.2.7
Host is up (0.012s latency).
```

```
Nmap scan report for 192.168.2.249
Host is up (0.016s latency).
Nmap scan report for 192.168.2.250
Host is up (0.016s latency).
Nmap scan report for 192.168.2.251
Host is up (0.015s latency).
Nmap scan report for 192.168.2.252
Host is up (0.015s latency).
Nmap scan report for 192.168.2.253
Host is up (0.014s latency).
Nmap scan report for 192.168.2.254
Host is up (0.014s latency).
Nmap done: 256 IP addresses (254 hosts up) scanned in 16.81 seconds
```

4. Saving the Nmap Scan Output to a File

Security tool Nmap has become a crucial tool in the cyber security field. And Nmap allows its users to export or save scan results into the text file or XML.

Command: nmap -oN output.txt example.com (This command will export Nmap scan into a text file)

nmap -oX output.xml example.com (This command will save the output of Nmap scanning in XML)

```
E:\>nmap -oN output.txt example.com
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-25 11:34 India Standard Time
Nmap scan report for example.com (93.184.216.34)
Host is up (0.057s latency).
Other addresses for example.com (not scanned): 2606:2800:220:1:248:1893:25c8:1946
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
1119/tcp closed bnetgame
1935/tcp closed rtmp
```

5. Most Popular Ports Scanning

It scan the fixed number of most popular ports.In order to apply this command you have to use the "–top-ports" option with a specific numeric value. This option gives you the ability to scan top ports. However, in Nmap, you also have the option to select the number of top ports to scan. This command allows users to get better and faster results.

Command: nmap –top-ports <numeric value> <IP address/Domain>

Output:

```
E:\>nmap -top-ports 15 196.134.5.67
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-25 11:36 India Standard Time
Nmap scan report for 196.134.5.67
Host is up (0.0029s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
53/tcp   filtered domain
80/tcp   filtered http
110/tcp  filtered pop3
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  filtered imap
443/tcp  filtered https
445/tcp  filtered microsoft-ds
3306/tcp filtered mysql
3389/tcp filtered ms-wbt-server
8080/tcp filtered http-proxy

Nmap done: 1 IP address (1 host up) scanned in 2.34 seconds
```

6. Display Open Ports

It detect open ports.Finding open ports (target ports that respond to UDP/TCP/SCTP requests) can be the first step to protecting and hacking any network. And if you only want to find ports you can connect to, then this command can be really useful to you.

Command: nmap — open<IP address/domain name>

Output:

```
E:\>nmap -open 198.152.45.33
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-25 11:37 India Standard Time
Nmap done: 1 IP address (1 host up) scanned in 4.96 seconds
```

7. Service Version Detection

Nmap has a database of more than 2000 services and associated ports for example– SSH(port 22) and HTTP (port 80). So while doing network inventories if you want to know which versions are running, you can use the Nmap version detection (-sV) command. Knowing the exact version number can be really helpful while finding which exploits your server is vulnerable to.

Command: nmap -sV<IP>

Output: