

Network VAPT

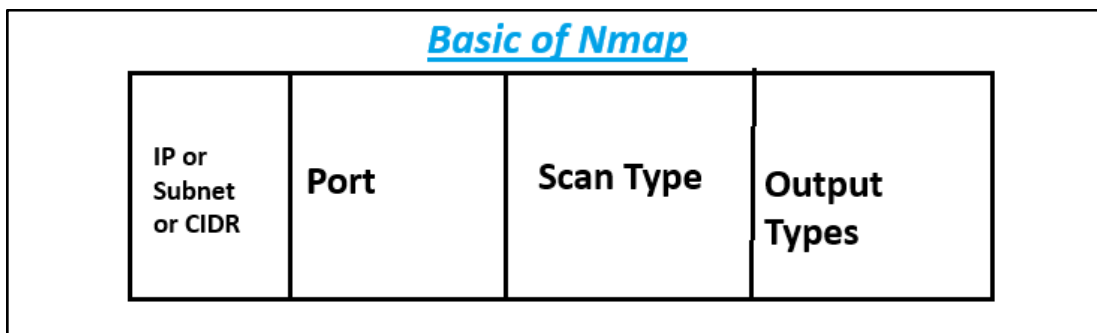
Contents :

- What is Nmap and mention the uses of Nmap?
- Why are Nmap scripts used?
- Practical



Nmap [Network mapper]

- Nmap (Network Mapper) is a [network scanner](#) created by [Gordon Lyon](#)
- Nmap is used to discover hosts and services on a computer network by sending packets and analysing the responses.
- Nmap has become hugely popular, being featured in movies like [The Matrix](#) and the popular series [Mr. Robot](#).
- Basic of nmap used in command line.



Uses of Nmap

- Used to identify the target port is up or not and what are the ports open with respect to that domain or ip address.
- It used various types of **scanning techniques** like TCP connection scan -sS, Tcp SYN scan -SS, XMAS scan -sX, null scan -sN, IDle scan, etc all these scans used for different purposes.

- Nmap has the feature to mention the **scan timing** like T0, T1, T2T5 and also can use the **Host Timeout** option if service is not responding up to a given time period and also there is a **scan delay** means you can mention the timings for sending the next packets.
- Nmap can also detect **application versions** with reasonable accuracy to help detect existing vulnerabilities.
- Nmap can find information about the **operating system** running on devices. It can provide detailed information like OS versions, making it easier to plan additional approaches during penetration testing.
- In Nmap you can use scripts which are called **NSE [Nmap script engine]** . There are various scripts available for different purposes . Path for the script to access - </usr/share/nmap/scripts>
- Nmap has a graphical user interface called **Zenmap**. It helps you develop visual mappings of a network for better usability and reporting.

Basic command for Nmap

A.Target

- | | |
|-------------------------|----------------|
| 1. nmap 1.2.3.4 | //single IP |
| 2. nmap 1.2.3.4/8 | //subnet Range |
| 3. nmap 1.2.3.4-8 | //IP range |
| 4. nmap 1.2.3.4 | //single IP |
| 5. nmap 1.2.3.4 1.3.4.5 | //specific IPs |
| 6. nmap -iL host.txt | //Text file |
| 7. nmap a.com | //domain name |

B.Port

- | | |
|-----------------------------|--|
| 1. nmap 1.2.3.4 -p80 | //single port |
| 2. nmap 1.2.3.4 -p20-30 | //Sequential port |
| 3. nmap 1.2.3.4 -p80,22,111 | //Distributed port |
| 4. nmap 1.2.3.4 -p http | //service specific it'll scan 80, 8080 |

5. nmap 1.2.3.4 -p- //All ports [65535]
6. nmap 1.2.3.4 -p T:22 U:53 //Protocol specific, where T is tcp and U is UDP
7. nmap 1.2.3.4 - - top-ports 10 //Scan only top ports

C. Other command

1. nmap -host-timeout 500ms 1.2.3.4
2. nmap -scan-delay 1s 1.2.3.4
3. nmap 1.2.3.4 -oN 1.txt //it will store output in .txt format
4. nmap 1.2.3.4 -oX 2.txt //store output in .xml format
5. nmap <domainName> -script http-headers //used script for scan
6. nmap -sV 1.2.3.4 //service version
7. nmap -O 1.2.3.4 //OS detection
8. nmap -A 1.2.3.4 //service version+ OS detect + scan + traceroute

Nmap Script usage

- Nmap script used for security auditing and vulnerability scanning and known as nmap script Engine [NSE]
- Used for firewall bypass, FTP Enumeration, DNS Enumeration, Http Enumeration, etc.
- Path to find all these scripts is -
\$ cd /usr/share/nmap/scripts

Practical

Scan the website - <http://testphp.vulnweb.com/>

1. Normal scan with time speed fast for that I mention -T4

```
(kali@kali)~$ nmap testphp.vulnweb.com -T4
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-15 02:59 EST
Stats: 0/0/15 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 79.35% done; ETC: 02:59 (0:00:04 remaining)
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.27s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
N
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
554/tcp   open  rtsp
1723/tcp  open  pptp
Nmap done: 1 IP address (1 host up) scanned in 19.75 seconds
```

2. Get to know what services are the services running.

```
(kali@kali)~$ nmap -host-timeout 500ms testphp.vulnweb.com -sV
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-15 03:01 EST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.22s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Skipping host testphp.vulnweb.com (44.228.249.3) due to host timeout
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.72 seconds
```

References :

- <https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/>
- <https://en.wikipedia.org/wiki/Nmap>
- <https://www.youtube.com/watch?v=DD3LopYcOYI>