Report on

FOOT PRINTING WITH NMAP

AICTE APPROVED SUMMER INTERNSHIP PROGRAM

NAME: Shaurya Damathia

COLLEGE: Thapar Institute of Engineering and Technology, Patiala

COURSE: Cyber Security and Ethical Hacking

INTRODUCTION:

In the realm of cybersecurity, foot printing is a critical process that involves gathering information about a target system to identify potential vulnerabilities. One of the most effective tools for foot printing is NMAP (Network Mapper). This report provides a comprehensive overview of foot printing with NMAP, illustrating its significance, usage, and benefits.

NMAP:

NMAP, abbreviated from Network Mapper, is a robust and freely available tool used for exploring networks and conducting security assessments. Created by Gordon Lyon, it enables users to examine networks, find open ports, identify operating systems, and collect diverse information about network devices.

Important features of NMAP include:

- **Host Discovery**: Identifying active devices on a network.
- **Port Scanning**: Checking for open ports on a target.
- **Service Detection**: Determining the services and applications running on open ports.
- **Operating System Detection**: Recognizing the operating system of a target device.
- **Nmap Scripting Engine (NSE)**: Allowing customized scripts to perform a variety of network tasks and vulnerability detection.

FOOT PRINTING WITH NMAP:

Foot printing is the first step in the ethical hacking process. It involves gathering as much information as possible about the target network. NMAP is particularly useful for this purpose due to its ability to perform detailed scans and provide comprehensive data about network topology and device configurations.

Some of the NMAP commands for footprinting include:

- Scan a list of targets → nmap -iL [list.txt]
- Excluding targets using a list → nmap [targets] -excludefile[list.txt]
- Perform an aggressive scan → nmap -A [target]
- Perform a ping scan only → nmap -sp [target]
- Full TCP connect → sudo nmap -sT -p 80,443 10.7.1.0/24

- Operating System detection → nmap -O [target]
- Service version detection → nmap -sV [target]
- Save output to a text file → nmap -oN [scan.txt] [target]
- Save output to an xml file → nmap -oX [scan.xml] [target]
- Grepable output → nmap -oG [scan.txt] [target]
- Scan a range of hosts → nmap [range of IP addresses]
- Scan an IPv6 address → nmap -6 [target]

EXAMPLES:

➢ Case Study-1:

```
┌──(root㉿kali)-[~]
└─# nmap -oG -  192.168.5.0-255 -p 22 -vv >/home/scan
```

```
File  Edit  Search  View  Document  Help
 1 # Nmap 7.94SVN scan initiated Wed Jul 17 00:19:21 2024 as: nmap -oG - -p 22 -vv 192.168.5.0-255
 2 # Ports scanned: TCP(1;22) UDP(0;) SCTP(0;) PROTOCOLS(0;)
 3 Host: 192.168.5.0 ()    Status: Up
 4 Host: 192.168.5.0 ()    Ports: 22/filtered/tcp//ssh///
 5 Host: 192.168.5.1 ()    Status: Up
 6 Host: 192.168.5.1 ()    Ports: 22/filtered/tcp//ssh///
 7 Host: 192.168.5.2 ()    Status: Up
 8 Host: 192.168.5.2 ()    Ports: 22/filtered/tcp//ssh///
 9 Host: 192.168.5.3 ()    Status: Up
10 Host: 192.168.5.3 ()    Ports: 22/filtered/tcp//ssh///
11 Host: 192.168.5.4 ()    Status: Up
12 Host: 192.168.5.4 ()    Ports: 22/filtered/tcp//ssh///
13 Host: 192.168.5.5 ()    Status: Up
14 Host: 192.168.5.5 ()    Ports: 22/filtered/tcp//ssh///
15 Host: 192.168.5.6 ()    Status: Up
16 Host: 192.168.5.6 ()    Ports: 22/filtered/tcp//ssh///
17 Host: 192.168.5.7 ()    Status: Up
18 Host: 192.168.5.7 ()    Ports: 22/filtered/tcp//ssh///
19 Host: 192.168.5.8 ()    Status: Up
20 Host: 192.168.5.8 ()    Ports: 22/filtered/tcp//ssh///
21 Host: 192.168.5.9 ()    Status: Up
22 Host: 192.168.5.9 ()    Ports: 22/filtered/tcp//ssh///
23 Host: 192.168.5.10 ()   Status: Up
24 Host: 192.168.5.10 ()   Ports: 22/filtered/tcp//ssh///
25 Host: 192.168.5.11 ()   Status: Up
26 Host: 192.168.5.11 ()   Ports: 22/filtered/tcp//ssh///
27 Host: 192.168.5.12 ()   Status: Up
28 Host: 192.168.5.12 ()   Ports: 22/filtered/tcp//ssh///
29 Host: 192.168.5.13 ()   Status: Up
30 Host: 192.168.5.13 ()   Ports: 22/filtered/tcp//ssh///
31 Host: 192.168.5.14 ()   Status: Up
32 Host: 192.168.5.14 ()   Ports: 22/filtered/tcp//ssh///
33 Host: 192.168.5.15 ()   Status: Up
34 Host: 192.168.5.15 ()   Ports: 22/filtered/tcp//ssh///
```

The command nmap -oG - 192.168.5.0-255 -p 22 -vv >/home/scan performs a network scan using Nmap and outputs the results in a specific format to a file.

The command scans the IP range 192.168.5.0 to 192.168.5.255 for open port 22 (SSH), providing detailed output in a grepable format, and saves the results to the file /home/scan.

- **Case Study-2:**

```
┌──(root㉿kali)-[~]
└─# nmap 192.168.5.0-255 -excludefile hostup.txt  -vv
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-17 00:50 IST
```

The command nmap 192.168.5.0-255 --excludefile hostup.txt -vv scans the IP range 192.168.5.0 to 192.168.5.255 with verbose output (-vv), excluding the hosts listed in the file hostup.txt from the scan.

- **Case Study-3:**

```
┌──(root㉿kali)-[~]
└─# nmap -sP Google.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-17 00:55 IST
Nmap scan report for Google.com (142.250.192.206)
Host is up (0.0014s latency).
Other addresses for Google.com (not scanned): 2404:6800:4002:817::200e
rDNS record for 142.250.192.206: del11s12-in-f14.1e100.net
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

The command nmap -sP Google.com performs a ping scan (-sP) on the domain Google.com. This type of scan is used to determine which hosts are up and running by sending ICMP echo requests to the target. It's essentially a way to check the availability of the target without performing a full port scan or gathering detailed information.

- **Case Study-4:**

```
┌──(root㉿kali)-[~]
└─# nmap -sT -p 88,443 scanme.nmap.org -vv
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-17 00:58 IST
Warning: Hostname scanme.nmap.org resolves to 2 IPs. Using 45.33.32.156.
Initiating Ping Scan at 00:58
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 00:58, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:58
Completed Parallel DNS resolution of 1 host. at 00:58, 3.23s elapsed
Initiating Connect Scan at 00:58
Scanning scanme.nmap.org (45.33.32.156) [2 ports]
Completed Connect Scan at 00:58, 1.20s elapsed (2 total ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up, received reset ttl 255 (0.00035s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Scanned at 2024-07-17 00:58:10 IST for 1s

PORT    STATE    SERVICE      REASON
88/tcp  filtered kerberos-sec no-response
443/tcp filtered https        no-response

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 8.90 seconds
           Raw packets sent: 4 (152B) | Rcvd: 1 (40B)
```

The command nmap -sT -p 88,443 scanme.nmap.org -vv performs a TCP connect scan (-sT) on the host scanme.nmap.org, specifically targeting ports 88 and 443. The -vv flag enables very verbose output, providing detailed information about the scan process. This scan method establishes a full TCP connection to the specified ports to determine their status (open, closed, or filtered).

CONCLUSION:

Foot printing is a foundational step in cybersecurity, providing critical information about target systems. NMAP is a powerful tool that enhances the foot printing process through its robust scanning and detection capabilities. It has some limitations like it may trigger security alerts and can be detected by intrusion detection system. Despite its limitations, NMAP remains an invaluable asset for cybersecurity professionals.