UNIVERSITA' DEGLI STUDI DI
NAPOLI FEDERICO II

Scuola Politecnica e delle Scienze di Base
Corso di Laurea Magistrale in Ingegneria Informatica

Elaborato di Network Security

Anno Accademico 2022/2023

Christian Marescalco
matr. M63001367
Antonio Avolio
matr. M63001352

Contents

1 Footprinting **1**

2 Scanning **2**

Chapter 1

Footprinting

The footprinting phase involves gathering information in the network regarding the target,in our case the organization and its members.
In this scenario, the attacker already knows information regarding the company and has managed to connect to the target local network.
Through the ifconfig tool he discovers the subnets to which he is connected: Employee Network, Company Network.
ifconfig screen
Using the nmap tool, the attacker discovers the topology of the various subnets within the organization, identifying the target ip's of the web server and employee computers

```
┌──(root㉿eadc7d2c7274)-[/]
└─# nmap -sn -PE --send-ip 193.20.3.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-03 08:24 UTC
Nmap scan report for 193.20.3.1
Host is up (0.00017s latency).
MAC Address: 02:42:C8:3C:3B:6C (Unknown)
Nmap scan report for eadc7d2c7274 (193.20.3.2)
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 4.83 seconds
```

nmap –sn –PE ––send–ip 193.20.3.0/24

From the top scan of the IP range 193.20.3.0/24 Bob found out one host up at 193.20.3.1 and his MAC Address.

```
┌──(root㉿eadc7d2c7274)-[/]
└─# nmap -sn -PE --send-ip 193.20.1.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-03 08:24 UTC
Nmap scan report for 193.20.1.1
Host is up (0.00012s latency).
MAC Address: 02:42:14:E0:E1:7C (Unknown)
Nmap scan report for c01_generallab_TomPC_1.c01_generallab_EmployeeNetwork (193.20.1.3)
Host is up (0.00019s latency).
MAC Address: 02:42:C1:14:01:03 (Unknown)
Nmap scan report for eadc7d2c7274 (193.20.1.2)
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 4.74 seconds
```

Chapter 2

Scanning

Nmap (Network Mapper) is a versatile and powerful tool with a range of options and features. Here are some of the main options:

- Host Discovery: This option is used to discover hosts on a network. Nmap can identify active hosts, as well as those that are currently offline.
- Port Scanning: Port scanning is one of the most popular features of Nmap. It can be used to identify open ports on a target system, and even detect hidden ports and services.
- Service and Version Detection: This option is used to identify the services and versions of software running on the target system. This information can be useful in identifying vulnerabilities and weaknesses.
- Operating System Detection: Nmap can also be used to identify the operating system running on the target system. This information can be helpful in identifying potential attack vectors.
- Scripting Engine: Nmap has a powerful scripting engine that allows users to write and execute custom scripts. This feature can be used to automate tasks, customize scans, and extend the functionality of Nmap.
- Output Formats: Nmap can generate output in various formats, including XML, HTML, and plain text. This feature can be helpful in generating reports, analyzing results, and sharing information with others.

These are just a few of the main options available in Nmap. Other features include traceroute, firewall detection, and performance tuning options. Nmap is a highly flexible tool that can be customized to suit the needs of the user. It has a number of flags or options that can be used to customize and fine-tune its scanning behavior. Here are some commonly used flag options:

- **-sS**: This flag specifies the type of scan to be performed, in this case a SYN scan.
- **-sT**: This flag specifies a TCP connect scan, where Nmap attempts to establish a full TCP connection with the target ports.

- **-sU**: This flag specifies a UDP scan, where Nmap sends UDP packets to the target ports and listens for responses.
- **-sC**: This flag specifies a scan usiong the default set of scripts. Some of the scripts in this category are considered intrusive.
- **-O**: This flag enables operating system detection, allowing Nmap to identify the operating system running on the target system.
- **-p**: This flag specifies the ports to be scanned, and can take a range of values or a comma-separated list of individual port numbers.
- **-oN**: This flag specifies the output format for Nmap results, in this case, plain text format.
- **-oN**: This option is used to specify the output format of the scan results. For example, the command "nmap -oN output.txt" will save the scan results to a file called "output.txt".

These are just a few examples of the flag options available in Nmap.