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

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 IPs of potential target nodes.

```
┌──(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

```
┌──(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
```

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 its MAC Address. On the other subnet 193.20.1.0/24, there is another host up with the address 193.20.1.2.

Chapter 2

Scanning

In this phase, the attacker explore the entire network perimeter by sending probe packets to endpoints with the goal of identify potential access points in the company systems. 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".

The attacker Bob exploits the following nmap command to discover open services on the target host 193.20.3.1:

```
┌──(root㉿eadc7d2c7274)-[/]
└─# nmap -sS 193.20.3.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-03 08:27 UTC
Nmap scan report for 193.20.3.1
Host is up (0.0000050s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
2222/tcp open  EtherNetIP-1
3306/tcp open  mysql
8080/tcp open  http-proxy
MAC Address: 02:42:C8:3C:3B:6C (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

From the scan report, there are multiple open ports: *http* on 8080, *mysql* on 3306 and *ssh* on 22. The attacker can assume that the target host 193.20.3.1 is a Web Server.
Then, he does the same for the node on the other subnet: (manca screen)

```
┌──(root㉿eadc7d2c7274)-[/]
└─# nmap -sV -sC 193.20.1.3
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-03 08:31 UTC
Nmap scan report for c01_generallab_TomPC_1.c01_generallab_EmployeeNetwork (193.20.1.3)
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 1c412ae17dc9c1ae86957688c863281b (ECDSA)
|_  256 c5a8871aabda48fc1d11e409dc14de73 (ED25519)
MAC Address: 02:42:C1:14:01:03 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.80 seconds
```

From the scan report, there is only an open SSH 22/Tcp port.

Chapter 3

Enumeration

After discovering the potential access points on the hosts, it is necessary to reveal other information regarding the active services on the detected ports. In the enumeration phase, active connections are created towards the target services by using the nmap tool with appropriate flags. This phase is more dangerous and traceable than the previous techniques because it requires an higher level of intrusiveness.
The objective of this phase is the service fingerprinting, i.e. the detection of the specific version and implementation of the service through an analysis of the service behaviour.
The attacker uses the nmap flag -sV, which compares answers obtained with a service fingerprint database, to determine services version on the Web Server:

```
┌──(root㉿eadc7d2c7274)-[/]
└─# nmap -sV 193.20.3.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-03 08:27 UTC
Nmap scan report for 193.20.3.1
Host is up (0.0000060s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
2222/tcp open  ssh     OpenSSH 9.2p1 Debian 2 (protocol 2.0)
3306/tcp open  mysql   MySQL 8.0.32
8080/tcp open  http    Node.js Express framework
MAC Address: 02:42:C8:3C:3B:6C (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.72 seconds
```

The attacker grabs information about the Web Server: it is implemented with NodeJS and has a connection with a mySQL Database. Then, he does the same for the Employee computer:

```
┌──(root㉿eadc7d2c7274)-[/]
└─# nmap -sV -sC 193.20.1.3
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-03 08:31 UTC
Nmap scan report for c01_generallab_TomPC_1.c01_generallab_EmployeeNetwork (193.20.1.3)
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 1c412ae17dc9c1ae86957688c863281b (ECDSA)
|_  256 c5a8871aabda48fc1d11e409dc14de73 (ED25519)
MAC Address: 02:42:C1:14:01:03 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.80 seconds
```

On the other host, nmap determines that: the ssh service is implemented with a specific version of OpenSSH and the OS family is Ubuntu Linux.

Chapter 4

Exploitation

After discovering the potential access points on the hosts, it is necessary to reveal other information regarding the active services on the detected ports. In the enumeration phase, active connections are created towards the target services by using the nmap tool with appropriate flags. This phase is more dangerous and traceable than the previous techniques because it requires an higher level of intrusiveness.
The objective of this phase is the service fingerprinting, i.e. the detection of the specific version and implementation of the service through an analysis of the service behaviour.
The attacker uses the nmap flag -sV, which compares answers obtained with a service fingerprint database, to determine services version on the Web Server:

```
┌──(root㉿eadc7d2c7274)-[/]
└─# nmap -sV 193.20.3.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-03 08:27 UTC
Nmap scan report for 193.20.3.1
Host is up (0.0000060s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
2222/tcp open  ssh     OpenSSH 9.2p1 Debian 2 (protocol 2.0)
3306/tcp open  mysql   MySQL 8.0.32
8080/tcp open  http    Node.js Express framework
MAC Address: 02:42:C8:3C:3B:6C (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.72 seconds
```

The attacker grabs information about the Web Server: it is implemented with NodeJS and has a connection with a mySQL Database. Then, he does the same for the Employee computer:

```
┌──(root㉿eadc7d2c7274)-[/]
└─# nmap -sV -sC 193.20.1.3
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-03 08:31 UTC
Nmap scan report for c01_generallab_TomPC_1.c01_generallab_EmployeeNetwork (193.20.1.3)
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 1c412ae17dc9c1ae86957688c863281b (ECDSA)
|_  256 c5a8871aabda48fc1d11e409dc14de73 (ED25519)
MAC Address: 02:42:C1:14:01:03 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.80 seconds
```

On the other host, nmap determines that: the ssh service is implemented with a specific version of OpenSSH and the OS family is Ubuntu Linux.