Information Gathering - Infra - Lab Scanning and OS Fingerprinting | Sonael de A. Angelos Neto

Introdução

O objetivo deste documento é apresentar uma metodologia para a coleta de informações sobre a infraestrutura de TI do Lab Scanning and OS Fingerprinting da plataforma INE, com o intuito de identificar vulnerabilidades e pontos de ataque.

Metodologia

Para identificar o sistema operacional da máquina que estamos utilizando e sua versão utilizamos o comando `cat /etc/os-release` cuja saída foi:

```
root@INE:~# cat /etc/os-release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2021.4"
VERSION_ID="2021.4"
VERSION_CODENAME="kali-rolling"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
```

Para checar quais interfaces de rede estão ativas no Lab Scanning and OS Fingerprinting, foi utilizado o comando `ifconfig` no terminal do Kali Linux. O resultado foi o seguinte:

```
root@INE:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.1.0.9  netmask 255.255.0.0  broadcast 10.1.255.255
        ether 02:42:0a:01:00:09  txqueuelen 0  (Ethernet)
        RX packets 1445  bytes 150726 (147.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1281  bytes 2794702 (2.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.221.161.2  netmask 255.255.255.0  broadcast 192.221.161.255
        ether 02:42:c0:dd:a1:02  txqueuelen 0  (Ethernet)
        RX packets 17  bytes 1486 (1.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4152  bytes 11920270 (11.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4152  bytes 11920270 (11.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

através desse output, podemos identificar que existem duas interfaces de rede ativas, a `eth0` e a `eth1`. as duas interfaces apresentam endereços IP.

Para esse laboratório, focaremos na interface `eth1`.

• How many machines are there?

Para identificar quantas máquinas estão ativas no Lab Scanning and OS Fingerprinting, utilizamos o comando `nmap -sn 192.221.161.2` (**-sn (No port scan)**) que nos retorna o seguinte resultado:

```
root@INE:~# nmap -sn 192.221.161.2
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-21 05:50 IST
Nmap scan report for INE (192.221.161.2)
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.00 seconds
root@INE:~# nmap -sn 192.221.161.2/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-21 05:50 IST
Nmap scan report for DNS-192-221-161-1.SanJose1.Level3.net (192.221.161.1)
Host is up (0.000097s latency).
MAC Address: 02:42:9B:57:AE:55 (Unknown)
Nmap scan report for pc1.ine.local (192.221.161.3)
Host is up (0.00013s latency).
MAC Address: 02:42:C0:DD:A1:03 (Unknown)
Nmap scan report for pc2.ine.local (192.221.161.4)
Host is up (0.000034s latency).
MAC Address: 02:42:C0:DD:A1:04 (Unknown)
Nmap scan report for pc3.ine.local (192.221.161.5)
Host is up (0.000029s latency).
MAC Address: 02:42:C0:DD:A1:05 (Unknown)
Nmap scan report for pc4.ine.local (192.221.161.6)
Host is up (0.000038s latency).
MAC Address: 02:42:C0:DD:A1:06 (Unknown)
Nmap scan report for INE (192.221.161.2)
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.05 seconds
```

Através do resultado, podemos identificar que existem **6** máquinas ativas nesse lab.

• What ports are open on pc1.ine.local machine?

Para identificar quais portas estão abertas na máquina `pc1.ine.local`, utilizamos o comando `nmap -p- pc1.ine.local`, onde `"-p-"` faz uma varredura nas 65.536 possíveis portas abertas retornando o seguinte resultado:

```
root@INE:~# nmap -p- pc1.ine.local
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-21 06:00 IST
Nmap scan report for pc1.ine.local (192.221.161.3)
Host is up (0.000012s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
MAC Address: 02:42:C0:DD:A1:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds
```

a máquina `pc1.ine.local` possui 3 portas abertas.

Portas	***Serviços***	***Status***
80/tcp	http	open
443/tcp	https	open
3306/tcp	mysql	open

• What OS is running on machine pc1.ine.local machine?

Para identificar qual sistema operacional está sendo executado na máquina `pc1.ine.local`, utilizamos o comando `nmap -O pc1.ine.local`, onde `"-O"` faz uma varredura no sistema operacional da máquina retornando o seguinte resultado:

```
root@INE:~# nmap -O pc1.ine.local
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-21 06:07 IST
Nmap scan report for pc1.ine.local (192.221.161.3)
Host is up (0.000044s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
MAC Address: 02:42:C0:DD:A1:03 (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
```

```
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.82 seconds
```

Através do resultado, podemos identificar que o sistema operacional da máquina `pc1.ine.local` é o `Linux 4.15 - 5.6`.

• What services are running on pc2.ine.local machine?

Primeiramente identificamos quais portas estão abertas na máquina `pc2.ine.local` através do comando `nmap -p- pc2.ine.local`, fazendo uma varredura de todas a portas possíveis abertas, retornando o seguinte resultado:

```
root@INE:~# nmap -p- pc2.ine.local
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-21 06:12 IST
Nmap scan report for pc2.ine.local (192.221.161.4)
Host is up (0.000012s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
27017/tcp open  mongod
MAC Address: 02:42:C0:DD:A1:04 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.48 seconds
```

Através do resultado, podemos identificar que a máquina `pc2.ine.local` possui apenas uma porta aberta, a porta `27017/tcp` que é o serviço `mongod`.

• What is the version of the FTP server running on one of the machines?

Para identificar a versão do serviço `FTP` que está sendo executado em uma das máquinas, utilizamos o comando `nmap -sV -p21 192.221.161.2/24 --open`, onde `"-sV"` faz uma varredura na versão do serviço , `"-p 21"` especifica a porta `21` para que ocorra a varredura, `\24` para que o scan ocorra em todos os 256 host da rede e o `--open` filtra as portas abertas, retornando o seguinte resultado:

```
root@INE:~# nmap -sV -p21 192.221.161.1/24 --open
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-21 06:24 IST
Nmap scan report for pc4.ine.local (192.221.161.6)
Host is up (0.000020s latency).
```

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
MAC Address: 02:42:C0:DD:A1:06 (Unknown)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.61 seconds
```

Através do resultado, podemos identificar que a versão do serviço `FTP` que está sendo executado na máquina `pc4.ine.local` é a `vsftpd 3.0.3`.

• A caching server is also running on one of the machines. What is the domain name of that machine?

Para identificar qual máquina está rodando um servidor de cache, utilizamos o comando `nmap -p- 192.221.161.1,2,3,4,5,6`, fazendo assim uma varredura em todas as portas dos hosts ativos da rede, retornando o seguinte resultado:

```
root@INE:~# nmap -p- 192.221.161.1,2,3,4,5,6
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-21 06:32 IST
Nmap scan report for DNS-192-221-161-1.SanJose1.Level3.net (192.221.161.1)
Host is up (0.0000090s latency).
Not shown: 65530 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    filtered http
443/tcp   filtered https
25555/tcp open     unknown
29999/tcp open     bingbang
MAC Address: 02:42:9B:57:AE:55 (Unknown)

Nmap scan report for pc1.ine.local (192.221.161.3)
Host is up (0.000014s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
MAC Address: 02:42:C0:DD:A1:03 (Unknown)

Nmap scan report for pc2.ine.local (192.221.161.4)
Host is up (0.000013s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
27017/tcp open  mongod
MAC Address: 02:42:C0:DD:A1:04 (Unknown)
```

```
Nmap scan report for pc3.ine.local (192.221.161.5)
Host is up (0.000013s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
11211/tcp open  memcache
MAC Address: 02:42:C0:DD:A1:05 (Unknown)

Nmap scan report for pc4.ine.local (192.221.161.6)
Host is up (0.000014s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 02:42:C0:DD:A1:06 (Unknown)

Nmap scan report for INE (192.221.161.2)
Host is up (0.0000070s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server
5910/tcp  open  cm
45654/tcp open  unknown

Nmap done: 6 IP addresses (6 hosts up) scanned in 8.32 seconds
```

Através do resultado, podemos identificar que a máquina `pc3.ine.local` está rodando um servidor de cache `mencache`, pois a porta `11211/tcp` está aberta.

• A NoSQL database and SQL database services are running on different machines. Can we use Nmap scripts to extract some information from those?

Pelo scan feito anteriormente podemos identificar que a maquina `pc1.ine.local (192.221.161.3)` está rodando o `MYSQL` na porta `3306/tcp` e a maquina `pc2.ine.local (192.221.161.4)` está rodando o `MongoDB` na porta `27017/tcp`.

```
root@INE:~# nmap -p- 192.221.161.3,4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-21 06:43 IST
Nmap scan report for pc1.ine.local (192.221.161.3)
Host is up (0.000012s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
MAC Address: 02:42:C0:DD:A1:03 (Unknown)

Nmap scan report for pc2.ine.local (192.221.161.4)
Host is up (0.000012s latency).
Not shown: 65534 closed tcp ports (reset)
```

```
PORT      STATE SERVICE
27017/tcp open  mongod
MAC Address: 02:42:C0:DD:A1:04 (Unknown)

Nmap done: 2 IP addresses (2 hosts up) scanned in 2.60 seconds
```

Para extrair informações do `MYSQL` podemos utilizar o script `mysql-*` e para extrair informações do `MongoDB` podemos utilizar o script `mongodb-info`.

```
root@INE:~# nmap -p27017 --script=mongodb-info pc2.ine.local | more
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-21 06:48 IST
Nmap scan report for pc2.ine.local (192.221.161.4)
Host is up (0.000083s latency).

PORT      STATE SERVICE
27017/tcp open  mongodb
| mongodb-info:
|   MongoDB Build info
|     versionArray
|       2 = 3
|       1 = 6
|       0 = 3
|       3 = 0
|     debug = false
|     javascriptEngine = mozjs
|     sysInfo = deprecated
|     maxBsonObjectSize = 16777216
|     storageEngines
|       2 = mmapv1
|       1 = ephemeralForTest
|       0 = devnull
|       3 = wiredTiger
|     bits = 64
|     openssl
|       compiled = OpenSSL 1.1.0g  2 Nov 2017
|       running = OpenSSL 1.1.0g  2 Nov 2017
|     buildEnvironment
|       target_os = linux
```

```
root@INE:~# nmap -p3306 --script=mysql-* pc1.ine.local | more
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-21 07:01 IST
Nmap scan report for pc1.ine.local (192.221.161.3)
Host is up (0.000089s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
```

```
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
| mysql-enum:
|   Accounts: No valid accounts found
|   Statistics: Performed 5 guesses in 1 seconds, average tps: 5.0
|_  ERROR: Host 'INE' is blocked because of many connection errors; unblock with
'mysqladmin flush-hosts'
|_mysql-empty-password: Host 'INE' is blocked because of many connection errors;
unblock with 'mysqladmin flush-hosts'
| mysql-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 50009 guesses in 12 seconds, average tps: 4167.4
MAC Address: 02:42:C0:DD:A1:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 12.54 seconds
```

Conclusão

Neste laboratório, aprendemos a utilizar o Nmap para realizar um scan de portas em uma rede, identificar serviços rodando em uma máquina e extrair informações de serviços específicos.