Esercitazione W11D1 Pratica 1

Ilaria Pedrelli

Tecniche di scansione con Nmap

Di seguito le scansioni effettuate su macchina target Metasploitable, inizialmente su reti diverse e successivamente con stessa rete. Durante la scansione su stessa rete ho provveduto anche alla creazione e al salvataggio di Report in vari formati (-oG, -oN, -oX)

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.30.2
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-17 13:35 EST
Nmap scan report for 192.168.30.2
Host is up (0.019s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    open     ssh
23/tcp    open     telnet
25/tcp    open     smtp
53/tcp    open     domain
80/tcp    filtered http
111/tcp   open     rpcbind
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
512/tcp   open     exec
513/tcp   open     login
514/tcp   open     shell
1099/tcp  open     rmiregistry
1524/tcp  open     ingreslock
2049/tcp  open     nfs
2121/tcp  open     ccproxy-ftp
3306/tcp  open     mysql
5432/tcp  open     postgresql
5900/tcp  open     vnc
6000/tcp  open     X11
6667/tcp  open     irc
8009/tcp  open     ajp13
8180/tcp  open     unknown

Nmap done: 1 IP address (1 host up) scanned in 14.82 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.30.2
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-17 13:36 EST
Nmap scan report for 192.168.30.2
Host is up (0.019s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    open     ssh
23/tcp    open     telnet
25/tcp    open     smtp
53/tcp    open     domain
80/tcp    filtered http
111/tcp   open     rpcbind
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
512/tcp   open     exec
513/tcp   open     login
514/tcp   open     shell
1099/tcp  open     rmiregistry
1524/tcp  open     ingreslock
2049/tcp  open     nfs
2121/tcp  open     ccproxy-ftp
3306/tcp  open     mysql
5432/tcp  open     postgresql
5900/tcp  open     vnc
6000/tcp  open     X11
6667/tcp  open     irc
8009/tcp  open     ajp13
8180/tcp  open     unknown

Nmap done: 1 IP address (1 host up) scanned in 14.61 seconds
```

```
┌──(kali㉿kali)-[~]
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O  192.168.50.101 -oN report1O
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-18 10:56 EST
Nmap scan report for 192.168.50.101
Host is up (0.015s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:D3:7B:60 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
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 16.08 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS  192.168.50.101 -oG report1S
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-18 10:58 EST
Nmap scan report for 192.168.50.101
Host is up (0.51s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:D3:7B:60 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 15.40 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.101 -oX report1T
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-18 11:36 EST
Nmap scan report for 192.168.50.101
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:D3:7B:60 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.39 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.101 -oX report1V
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-18 12:06 EST
Nmap scan report for 192.168.50.101
Host is up (0.020s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           vsftpd 2.3.4
22/tcp   open  ssh           OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet?
25/tcp   open  smtp?
53/tcp   open  domain        ISC BIND 9.4.2
80/tcp   open  http          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind       2 (RPC #100000)
139/tcp  open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  java-rmi      GNU Classpath grmiregistry
1524/tcp open  bindshell     Metasploitable root shell
2049/tcp open  nfs           2-4 (RPC #100003)
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql         MySQL (Too many connections)
5432/tcp open  postgresql    PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc           VNC (protocol 3.3)
6000/tcp open  X11           (access denied)
6667/tcp open  irc           UnrealIRCd
8009/tcp open  ajp13         Apache Jserv (Protocol v1.3)
8180/tcp open  http          Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:D3:7B:60 (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, 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 193.82 seconds
```