W11D4

SCANSIONE SERVIZI CON NMAP

La traccia

Tecniche di scansione con Nmap - scansione di un host, senza e con completamento del 3-way handshake

Questo esercizio può essere utile per lo studente per prendere dimestichezza con i vari comandi di nmap.
Poiché su Linux è un potente tool di scansione della rete, si richiede di utilizzare i seguenti comandi e trascrivere i vari risultati su un report:

TCP: #	nmap -sS ip address
scansione completa: #	nmap -sV ip address
output su file: #	nmap -sV -oN file.txt ip address
scansione su porta: #	nmap -sS -p 8080 ip address
scansione tutte le porte: #	nmap -sS -p ip address
scansione UDP: #	nmap -sU -r -v ip address
scansione sistema operativo: #	nmap -O ip address
scansione versione servizi: #	nmap -sV ip address
scansione common 100 ports: #	nmap -F ip address
scansione tramite ARP: #	nmap -PR ip address
scansione tramite PING: #	nmap -sP ip address
scansione senza PING: #	nmap -PN ip address

Tecniche di scansione con Nmap - scansione di un host, senza e con completamento del 3-way handshake

Infine, disegnare 3-4 grafici delle scansioni effettuate, esplicitando le varie fasi di syn, syn/ack ecc.

1) Nmap –sS ipaddress

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.4
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 19:45 EST
Nmap scan report for 192.168.50.4
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:A9:45:82 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds
```

2) Nmap –sV ipaddress

```
└─$ sudo nmap -sV 192.168.50.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 19:47 EST
Nmap scan report for 192.168.50.4
Host is up (0.011s 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      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
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        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
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  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
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:A9:45:82 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:li
ux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.31 seconds
```

3) Nmap –sV –oN file.txt ipaddress

```
└─$ sudo nmap -sV -oN file.txt 192.168.50.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 19:49 EST
Nmap scan report for 192.168.50.4
Host is up (0.00051s 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      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
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        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
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  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
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:A9:45:82 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:lin
ux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.20 seconds
```

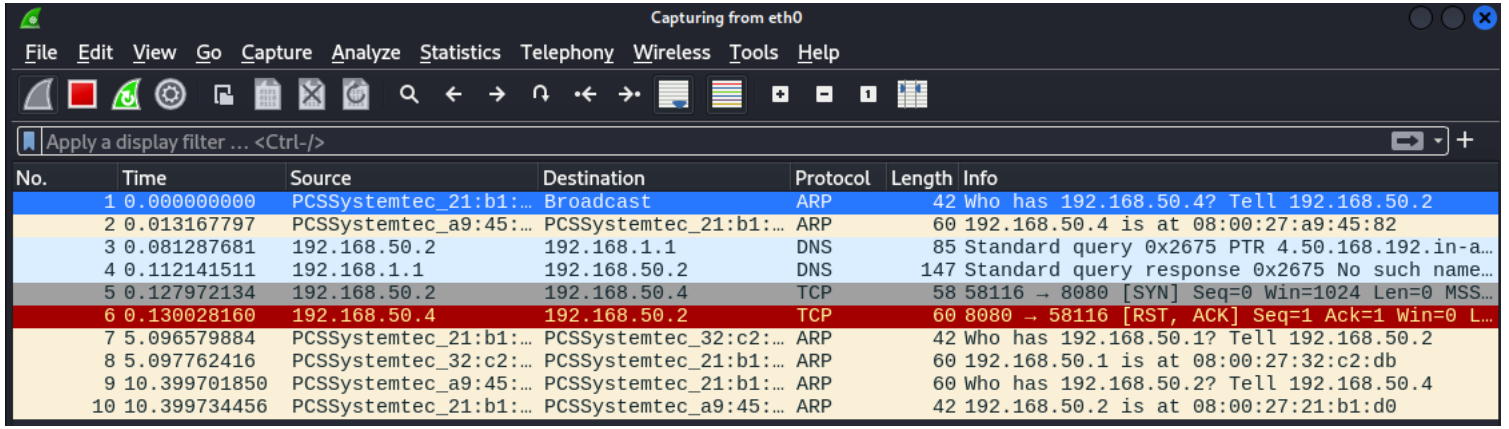
4) Nmap –sS –p 8080 ipaddress

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p 8080 192.168.50.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 19:50 EST
Nmap scan report for 192.168.50.4
Host is up (0.0012s latency).

PORT     STATE  SERVICE
8080/tcp closed http-proxy
MAC Address: 08:00:27:A9:45:82 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

In questo caso non completa la 3 way handshake ma si ferma alla syn.



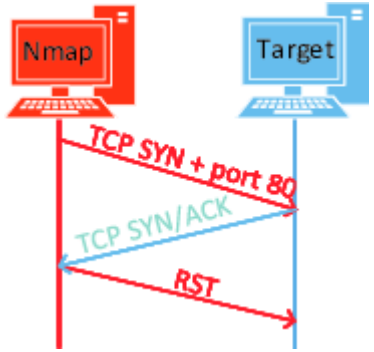
5) Nmap –sU –r -v ipaddress

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU -r -v  192.168.50.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 19:52 EST
Initiating ARP Ping Scan at 19:52
Scanning 192.168.50.4 [1 port]
Completed ARP Ping Scan at 19:52, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:52
Completed Parallel DNS resolution of 1 host. at 19:52, 0.03s elapsed
Initiating UDP Scan at 19:52
Scanning 192.168.50.4 [1000 ports]
Discovered open port 53/udp on 192.168.50.4
Discovered open port 111/udp on 192.168.50.4
Discovered open port 137/udp on 192.168.50.4
Increasing send delay for 192.168.50.4 from 0 to 50 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.50.4 from 50 to 100 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.50.4 from 100 to 200 due to max_successful_tryno increase to 6
Increasing send delay for 192.168.50.4 from 200 to 400 due to max_successful_tryno increase to 7
Increasing send delay for 192.168.50.4 from 400 to 800 due to max_successful_tryno increase to 8
Increasing send delay for 192.168.50.4 from 800 to 1000 due to max_successful_tryno increase to 9
UDP Scan Timing: About 4.21% done; ETC: 20:05 (0:11:46 remaining)
UDP Scan Timing: About 5.55% done; ETC: 20:11 (0:17:17 remaining)
UDP Scan Timing: About 6.62% done; ETC: 20:15 (0:21:24 remaining)
Warning: 192.168.50.4 giving up on port because retransmission cap hit (10).
UDP Scan Timing: About 8.25% done; ETC: 20:18 (0:23:00 remaining)
```

6) Nmap –O ipaddress

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O  192.168.50.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 19:57 EST
Nmap scan report for 192.168.50.4
Host is up (0.0076s 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
```

La syn-ack per questo tipo di scansione funziona come per la SYN(-sS).



tcp.port==41743

No.	Time	Source	Destination	Protocol	Length	Info
2054	7.086210460	192.168.50.2	192.168.50.4	TCP	66	41743 → 21 [SYN, ECE, CWR, Reserved] Seq=0 …
2055	7.087274781	192.168.50.4	192.168.50.2	TCP	66	21 → 41743 [SYN, ACK] Seq=0 Ack=1 Win=5840 …
2056	7.087317201	192.168.50.2	192.168.50.4	TCP	54	41743 → 21 [RST] Seq=1 Win=0 Len=0

7) Nmap –F ipaddress

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -F  192.168.50.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 20:05 EST
Nmap scan report for 192.168.50.4
Host is up (0.0071s latency).
Not shown: 82 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
513/tcp  open  login
514/tcp  open  shell
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
8009/tcp open  ajp13
MAC Address: 08:00:27:A9:45:82 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
```

8) Nmap –PR ipaddress

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -PR  192.168.50.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 20:12 EST
Nmap scan report for 192.168.50.4
Host is up (0.00075s 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:A9:45:82 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds
```

9) Nmap –sP ipaddress

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sP 192.168.50.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 20:17 EST
Nmap scan report for 192.168.50.4
Host is up (0.00075s latency).
MAC Address: 08:00:27:A9:45:82 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

10) Nmap –Pn ipaddress

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -Pn 192.168.50.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 20:19 EST
Nmap scan report for 192.168.50.4
Host is up (0.00051s 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:A9:45:82 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds
```