



W9D1

SCANSIONE DI SERVIZI DI RETE

La traccia

La traccia prevede di svolgere un esercizio di scansione dei servizi di rete:

Vedremo da vicino nmap e i suoi comandi.

Sulle base delle nozioni viste nella lezione teorica eseguiremo diversi tipi di scan sulla macchine metasploitable, come di seguito:

- Scansione TCP sulle porte well-known
- Scansione SYN sulle porte well-known
- Scansione con switch «-A» sulle porte well-known

Evidenziare la differenza tra la scansione completa TCP e la scansione SYN intercettando le richieste inviate dalla macchine sorgente con Wireshark.

Scansione Tcp

In questo caso, durante la scansione TCP delle well-known ports possiamo osservare che nmap completa i 3 passaggi del 3 way handshake.

The image displays two windows from a Kali Linux system. The left window is Wireshark, showing a packet capture for the IP address 192.168.1.11. The right window is a terminal showing the output of an Nmap scan.

Wireshark Packet Capture:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|--------------|--------------|----------|--------|-----------------------------|
| 12 | 10.117584325 | 192.168.1.13 | 192.168.1.11 | TCP | 76 | 51638 → 80 [SYN] Seq= |
| 13 | 10.117881080 | 192.168.1.13 | 192.168.1.11 | TCP | 76 | 34382 → 443 [SYN] Seq= |
| 14 | 10.121634993 | 192.168.1.11 | 192.168.1.13 | TCP | 76 | 80 → 51638 [SYN, ACK] Seq= |
| 15 | 10.121635735 | 192.168.1.11 | 192.168.1.13 | TCP | 62 | 443 → 34382 [RST, ACK] Seq= |
| 16 | 10.121678799 | 192.168.1.13 | 192.168.1.11 | TCP | 68 | 51638 → 80 [ACK] Seq= |
| 17 | 10.122116624 | 192.168.1.13 | 192.168.1.11 | TCP | 68 | 51638 → 80 [RST, ACK] Seq= |
| 20 | 10.146426930 | 192.168.1.13 | 192.168.1.11 | TCP | 76 | 49940 → 113 [SYN] Seq= |
| 21 | 10.146810214 | 192.168.1.13 | 192.168.1.11 | TCP | 76 | 40580 → 135 [SYN] Seq= |
| 22 | 10.147049401 | 192.168.1.11 | 192.168.1.13 | TCP | 62 | 113 → 49940 [RST, ACK] Seq= |
| 23 | 10.147150154 | 192.168.1.13 | 192.168.1.11 | TCP | 76 | 34386 → 443 [SYN] Seq= |
| 24 | 10.147339782 | 192.168.1.11 | 192.168.1.13 | TCP | 62 | 135 → 40580 [RST, ACK] Seq= |
| 25 | 10.147583971 | 192.168.1.11 | 192.168.1.13 | TCP | 62 | 443 → 34386 [RST, ACK] Seq= |
| 26 | 10.147821754 | 192.168.1.13 | 192.168.1.11 | TCP | 76 | 34282 → 23 [SYN] Seq= |
| 27 | 10.148195154 | 192.168.1.13 | 192.168.1.11 | TCP | 76 | 50748 → 53 [SYN] Seq= |
| 28 | 10.148387879 | 192.168.1.11 | 192.168.1.13 | TCP | 76 | 23 → 34282 [SYN, ACK] Seq= |
| 29 | 10.148413451 | 192.168.1.13 | 192.168.1.11 | TCP | 68 | 34282 → 23 [ACK] Seq= |
| 30 | 10.148902981 | 192.168.1.11 | 192.168.1.13 | TCP | 76 | 53 → 50748 [SYN, ACK] Seq= |
| 31 | 10.148990923 | 192.168.1.13 | 192.168.1.11 | TCP | 68 | 50748 → 53 [ACK] Seq= |
| 32 | 10.149276883 | 192.168.1.13 | 192.168.1.11 | TCP | 76 | 45828 → 554 [SYN] Seq= |
| 33 | 10.149521905 | 192.168.1.13 | 192.168.1.11 | TCP | 76 | 58960 → 110 [SYN] Seq= |
| 34 | 10.149710199 | 192.168.1.11 | 192.168.1.13 | TCP | 62 | 554 → 45828 [RST, ACK] Seq= |
| 35 | 10.149959619 | 192.168.1.11 | 192.168.1.13 | TCP | 62 | 110 → 58960 [RST, ACK] Seq= |
| 36 | 10.150277747 | 192.168.1.13 | 192.168.1.11 | TCP | 76 | 51654 → 80 [SYN] Seq= |
| 37 | 10.150520873 | 192.168.1.13 | 192.168.1.11 | TCP | 76 | 36224 → 445 [SYN] Seq= |
| 38 | 10.150733005 | 192.168.1.11 | 192.168.1.13 | TCP | 76 | 80 → 51654 [SYN, ACK] Seq= |

Nmap Scan Output:

```
kali@kali: ~/Downloads
File Actions Edit View Help
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

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds

(kali@kali)-[~/Downloads]
$ nmap -sT -p 0-1023 192.168.1.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-24 07:53 EST
Nmap scan report for 192.168.1.11
Host is up (0.012s latency).
Not shown: 1012 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

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Scansione Syn

In questo caso, durante la scansione SYN delle well-known ports possiamo osservare che nmap NON completa i 3 passaggi del 3 way handshake.

The image shows a network capture in Wireshark and a terminal window. The Wireshark capture is filtered for 'ip.addr == 192.168.1.11' and displays a list of packets. The terminal window shows the execution of an nmap SYN scan on the same IP address.

Wireshark Packet List:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|--------------|--------------|----------|--------|------------------------|
| 11 | 2.312908291 | 192.168.1.13 | 192.168.1.11 | TCP | 60 | 57091 → 199 [SYN] Seq= |
| 12 | 2.313101226 | 192.168.1.13 | 192.168.1.11 | TCP | 60 | 57091 → 587 [SYN] Seq= |
| 13 | 2.313260350 | 192.168.1.13 | 192.168.1.11 | TCP | 60 | 57091 → 993 [SYN] Seq= |
| 14 | 2.313419073 | 192.168.1.13 | 192.168.1.11 | TCP | 60 | 57091 → 110 [SYN] Seq= |
| 15 | 2.313576533 | 192.168.1.13 | 192.168.1.11 | TCP | 60 | 57091 → 80 [SYN] Seq= |
| 16 | 2.313733802 | 192.168.1.13 | 192.168.1.11 | TCP | 60 | 57091 → 995 [SYN] Seq= |
| 17 | 2.313890490 | 192.168.1.13 | 192.168.1.11 | TCP | 60 | 57091 → 445 [SYN] Seq= |
| 18 | 2.314002791 | 192.168.1.13 | 192.168.1.11 | TCP | 60 | 57091 → 53 [SYN] Seq= |
| 19 | 2.314060018 | 192.168.1.13 | 192.168.1.11 | TCP | 60 | 57091 → 143 [SYN] Seq= |
| 20 | 2.314118821 | 192.168.1.13 | 192.168.1.11 | TCP | 60 | 57091 → 135 [SYN] Seq= |
| 21 | 2.320700984 | 192.168.1.11 | 192.168.1.13 | TCP | 62 | 199 → 57091 [RST, ACK] |
| 22 | 2.320701515 | 192.168.1.11 | 192.168.1.13 | TCP | 62 | 587 → 57091 [RST, ACK] |
| 23 | 2.320701715 | 192.168.1.11 | 192.168.1.13 | TCP | 62 | 993 → 57091 [RST, ACK] |
| 24 | 2.320701926 | 192.168.1.11 | 192.168.1.13 | TCP | 62 | 110 → 57091 [RST, ACK] |
| 25 | 2.320702136 | 192.168.1.11 | 192.168.1.13 | TCP | 62 | 80 → 57091 [SYN, ACK] |
| 26 | 2.320702347 | 192.168.1.11 | 192.168.1.13 | TCP | 62 | 995 → 57091 [RST, ACK] |
| 27 | 2.320702548 | 192.168.1.11 | 192.168.1.13 | TCP | 62 | 445 → 57091 [SYN, ACK] |
| 28 | 2.320702758 | 192.168.1.11 | 192.168.1.13 | TCP | 62 | 53 → 57091 [SYN, ACK] |
| 29 | 2.320966645 | 192.168.1.13 | 192.168.1.11 | TCP | 56 | 57091 → 80 [RST] Seq= |
| 30 | 2.321183888 | 192.168.1.13 | 192.168.1.11 | TCP | 56 | 57091 → 445 [RST] Seq= |
| 31 | 2.321232004 | 192.168.1.13 | 192.168.1.11 | TCP | 56 | 57091 → 53 [RST] Seq= |
| 32 | 2.321307075 | 192.168.1.11 | 192.168.1.13 | TCP | 62 | 143 → 57091 [RST, ACK] |
| 33 | 2.321307276 | 192.168.1.11 | 192.168.1.13 | TCP | 62 | 135 → 57091 [RST, ACK] |
| 34 | 2.321463082 | 192.168.1.13 | 192.168.1.11 | TCP | 60 | 57091 → 22 [SYN] Seq= |
| 35 | 2.321519468 | 192.168.1.13 | 192.168.1.11 | TCP | 60 | 57091 → 554 [SYN] Seq= |

Terminal Output:

```
kali@kali: ~/Downloads
File Actions Edit View Help
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
MAC Address: 08:00:27:A9:45:82 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds

(kali@kali)~[~/Downloads]
$ sudo nmap -sS -p 0-1023 192.168.1.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-24 09:50 EST
Nmap scan report for 192.168.1.11
Host is up (0.0040s latency).
Not shown: 1012 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
MAC Address: 08:00:27:A9:45:82 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds

(kali@kali)~[~/Downloads]
```

Scansione -A

In questo caso, durante la scansione -A delle well-known ports possiamo osservare che nmap completa i 3 passaggi del 3 way handshake e aggiunge diverse informazioni.

The image consists of two side-by-side screenshots. The left screenshot shows a Wireshark packet capture of an nmap -A scan. The right screenshot shows the terminal output of the same scan.

Left Screenshot (Wireshark):

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|--------------|--------------|----------|--------|--------------------------------|
| 1 | 0.000000000 | 192.168.1.13 | 192.168.1.11 | TELNET | 72 | Telnet Data ... |
| 2 | 0.000225574 | 192.168.1.13 | 192.168.1.11 | DNS | 100 | Standard query 0x0006 TXT |
| 3 | 0.000412555 | 192.168.1.13 | 192.168.1.11 | HTTP | 86 | GET / HTTP/1.0 |
| 4 | 0.000583266 | 192.168.1.13 | 192.168.1.11 | Portmap | 112 | V104316 proc-0 Call (Reply) |
| 5 | 0.000751984 | 192.168.1.13 | 192.168.1.11 | NBSS | 86 | NBSS Continuation Message |
| 6 | 0.000911317 | 192.168.1.13 | 192.168.1.11 | SMB | 236 | Negotiate Protocol Request |
| 7 | 0.001047191 | 192.168.1.11 | 192.168.1.13 | TCP | 68 | 23 → 37482 [ACK] Seq=1 |
| 8 | 0.001047482 | 192.168.1.11 | 192.168.1.13 | TCP | 68 | 53 → 35090 [ACK] Seq=1 |
| 9 | 0.001036610 | 192.168.1.13 | 192.168.1.11 | Rlogin | 100 | Start Handshake |
| 10 | 0.001319278 | 192.168.1.11 | 192.168.1.13 | TCP | 68 | 80 → 51560 [ACK] Seq=1 |
| 11 | 0.001319488 | 192.168.1.11 | 192.168.1.13 | TCP | 68 | 111 → 46642 [ACK] Seq=1 |
| 12 | 0.001319558 | 192.168.1.11 | 192.168.1.13 | TCP | 68 | 139 → 53602 [ACK] Seq=1 |
| 13 | 0.001590392 | 192.168.1.11 | 192.168.1.13 | TCP | 68 | 445 → 40732 [ACK] Seq=1 |
| 14 | 0.015251008 | 192.168.1.11 | 192.168.1.13 | Portmap | 104 | V104316 proc-0 Reply (Call) |
| 15 | 0.015379127 | 192.168.1.13 | 192.168.1.11 | TCP | 68 | 46642 → 111 [ACK] Seq=45 |
| 16 | 0.015620727 | 192.168.1.13 | 192.168.1.11 | TCP | 68 | 46642 → 111 [FIN, ACK] Seq=45 |
| 17 | 0.016534881 | 192.168.1.11 | 192.168.1.13 | TCP | 68 | 513 → 52246 [ACK] Seq=1 |
| 18 | 0.031651957 | 192.168.1.11 | 192.168.1.13 | TCP | 68 | 111 → 46642 [FIN, ACK] Seq=45 |
| 19 | 0.031700754 | 192.168.1.13 | 192.168.1.11 | TCP | 68 | 46642 → 111 [ACK] Seq=46 |
| 20 | 0.043121850 | 192.168.1.11 | 192.168.1.13 | DNS | 132 | Standard query response 0x0006 |
| 21 | 0.043252626 | 192.168.1.13 | 192.168.1.11 | TCP | 68 | 35090 → 53 [ACK] Seq=33 |
| 22 | 0.043951417 | 192.168.1.13 | 192.168.1.11 | TCP | 68 | 35090 → 53 [FIN, ACK] Seq=33 |
| 23 | 0.044009982 | 192.168.1.11 | 192.168.1.13 | SMB | 169 | Negotiate Protocol Response |
| 24 | 0.044024006 | 192.168.1.13 | 192.168.1.11 | TCP | 68 | 40732 → 445 [ACK] Seq=169 |
| 25 | 0.044106966 | 192.168.1.13 | 192.168.1.11 | TCP | 68 | 40732 → 445 [FIN, ACK] Seq=169 |

Right Screenshot (Terminal):

```
kali@kali: ~/Downloads
$ sudo nmap -A -p 0-1023 192.168.1.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-24 10:05 EST
Nmap scan report for 192.168.1.11
Host is up (0.010s latency).
Not shown: 1012 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_  Connected to 192.168.1.13
|_  Logged in as ftp
|_  TYPE: ASCII
|_  No session bandwidth limit
|_  Session timeout in seconds is 300
|_  Control connection is plain text
|_  Data connections will be plain text
|_ vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_  1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_ssl-date: TLS randomness does not represent time
|_smtp-command: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCED
|_STATUSCODES, 8BITMIME, DSN
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=
```