

UTILIZZO DELLO STRUMENTO NMAP PER EFFETTUARE VARI TIPI DI SCANSIONE SU MACCHINA METASPLOITABLE

Dopo avere avviato entrambe le macchine all'interno della virtual box ed aver configurato la loro connessione su rete interna ho proceduto lanciando una serie di comandi dal terminale di linux kali. Il primo comando di scansione è stato “sudo nmap 192.168.50.101 -sT -p 0-1023” per avviare una scansione TCP sulle porte well-known. La foto qua sotto riporta il risultato di questa scansione:

```
(kali@kali)-[~]
$ sudo nmap 192.168.50.101 -sS -p 0-1023
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 09:07 EST
Nmap scan report for 192.168.50.101
Host is up (0.00036s 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: 08:00:27:2F:16:43 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.41 seconds
```

Successivamente sono andato a fare la scansione SYN sempre limitandola alle porte well-known tramite il comando “sudo nmap 192.168.50.101 -sS -p 0-1023”, ottenendo questo risultato:

```
(kali@kali)-[~]
$ sudo nmap 192.168.50.101 -sT -p 0-1023
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 09:07 EST

zsh: suspended sudo nmap 192.168.50.101 -sT -p 0-1023

(kali@kali)-[~]
$ sudo nmap 192.168.50.101 -sT -p 0-1023
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 09:08 EST
Nmap scan report for 192.168.50.101
Host is up (0.00030s 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
MAC Address: 08:00:27:2F:16:43 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
```

In entrambi i casi le porte della categoria well-known che risultano essere attive sono 12. Andando tramite Wireshark ad intercettare le richieste inviate dalla macchina linux kali possiamo vedere la differenza nei 2 tipi di scansione.

Prendiamo la porta 80 come punto di riferimento: nella scansione SYN se andiamo ad intercettare i pacchetti possiamo vedere come la connessione tra le 2 macchine non viene completata (cerchiato in arancione possiamo vedere RST che chiude la comunicazione). Nella scansione TCP infatti possiamo vedere come la three way handshake viene completata al contrario dell'altra (nel cerchio rosso possiamo vedere come viene completata la sequenza SYN-SYN+ACK-ACK)

No.	Time	Source	Destination	Protocol	Length	Info
44	13.108547941	192.168.50.100	192.168.50.101	TCP		60 52852 → 21 [SYN] Seq=0 Win=0 Len=0 MSS=1460
55	13.108713069	192.168.50.101	192.168.50.100	TCP		62 21 → 52852 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
61	13.108820291	192.168.50.100	192.168.50.101	TCP		56 52852 → 21 [RST] Seq=1 Win=0 Len=0

No.	Time	Source	Destination	Protocol	Length	Info
44	13.083562718	192.168.50.100	192.168.50.101	TCP		76 41840 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1479919181 TSecr=0 WS=128
52	13.084285211	192.168.50.101	192.168.50.100	TCP		76 80 → 41840 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=403911 TSecr=1479919181 WS=64
58	13.084349616	192.168.50.100	192.168.50.101	TCP		68 41840 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1479919182 TSecr=403911

Andando a fare uno scan usando sempre nmap ma con lo switch -A eseguiamo una scansione aggressiva ed avanzata che ci permette di vedere informazioni aggiuntive, come possiamo vedere dall'immagine qui sotto:

```

kali@kali: ~
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 102.87 seconds

(kali@kali)-[~]
$ sudo nmap 192.168.50.101 -A -p 0-1023
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 10:08 EST
Nmap scan report for 192.168.50.101
Host is up (0.00052s latency).
Not shown: 1012 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ ftp-syst:
|_ STAT:
|_ FTP server status:
|_   Connected to 192.168.50.100
|_   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
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
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
|_ sslv2:
|_   SSLv2 supported
|_   ciphers:
|_     SSL2_RC2_128_CBC_WITH_MD5
|_     SSL2_DES_64_CBC_WITH_MD5
|_     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_     SSL2_RC4_128_EXPORT40_WITH_MD5
|_     SSL2_RC4_128_WITH_MD5
|_     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ smtp-comands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, EN
|_ BITIME, DSN
53/tcp    open  domain       ISC BIND 9.4.2
|_ dns-nsid:
|_   bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_ http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_ http-title: Metasploitable2 - Linux

```

La seguente tabella riporta l'analisi della scansione SYN effettuata sulle porte well-know:

SOURCE	DESTINATION	TIPO DI SCAN	SERVIZIO
192.168.50.100:52852	192.168.50.101:21	SYN	ftp
192.168.50.100:52852	192.168.50.101:22	SYN	ssh
192.168.50.100:52852	192.168.50.101:23	SYN	telnet
192.168.50.100:52852	192.168.50.101:25	SYN	smtp
192.168.50.100:52852	192.168.50.101:53	SYN	domain
192.168.50.100:52852	192.168.50.101:80	SYN	http
192.168.50.100:52852	192.168.50.101:111	SYN	rpcbind
192.168.50.100:52852	192.168.50.101:139	SYN	Netbios-ssn
192.168.50.100:52852	192.168.50.101:445	SYN	Microsoft-ds
192.168.50.100:52852	192.168.50.101:512	SYN	exec
192.168.50.100:52852	192.168.50.101:513	SYN	login
192.168.50.100:52852	192.168.50.101:514	SYN	shell

La prossima tabella invece riporta l'analisi della scansione TCP

SOURCE	DESTINATION	TIPO DI SCAN	SERVIZIO
192.168.50.100:59206	192.168.50.101:21	TCP	ftp
192.168.50.100:37338	192.168.50.101:22	TCP	ssh
192.168.50.100:44908	192.168.50.101:23	TCP	telnet
192.168.50.100:37970	192.168.50.101:25	TCP	smtp
192.168.50.100:47332	192.168.50.101:53	TCP	domain
192.168.50.100:41840	192.168.50.101:80	TCP	http
192.168.50.100:37888	192.168.50.101:111	TCP	rpcbind
192.168.50.100:52240	192.168.50.101:139	TCP	Netbios-ssn
192.168.50.100:34548	192.168.50.101:445	TCP	Microsoft-ds
192.168.50.100:47844	192.168.50.101:512	TCP	exec
192.168.50.100:50254	192.168.50.101:513	TCP	login
192.168.50.100:41732	192.168.50.101:514	TCP	shell

I entrambi i tipi di scansione abbiamo visto che le porte well-known aperte sono 12. Se invece andiamo ad eseguire le scansioni SYN e TCP senza limitarci alle porte well-known otteniamo questo risultato:

```
(kali㉿kali)-[~]
$ sudo nmap 192.168.50.101 -sS
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 10:53 EST
Nmap scan report for 192.168.50.101
Host is up (0.00015s 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: 08:00:27:2F:16:43 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.35 seconds

(kali㉿kali)-[~]
$ sudo nmap 192.168.50.101 -sT
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 10:54 EST
Nmap scan report for 192.168.50.101
Host is up (0.00035s 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: 08:00:27:2F:16:43 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
```