


Beatrice Folino

[NMAP SCAN]

EPICODE - CYBERSECURITY CLASS [W9D1 Pratica2]

27 dicembre 2023





L'esercitazione è finalizzata ad acquisire dimestichezza con il tool **nmap** e i suoi comandi effettuando 3 tipi di scansioni (Syn, TCP e -A) da una macchina Kali Linux a una macchina target Metasploitable. Il traffico verrà poi intercettato su Wireshark e analizzato.

SCANSIONE SYN

Effettuiamo una scansione nmap SYN sulle well known ports del sistema target col comando

```
- nmap -sS 192.168.50.101 -p 1-1024
```

Lo switch **-sS** indica che il tipo di scansione è quella SYN. Il sistema prova a contattare tutte le porte del range (indicato da "**-p 1-1024**") inviando un pacchetto SYN. Se la porta è aperta, il metasploitable invierà un pacchetto SYN-ACK. Kali Linux non risponderà a questo pacchetto, non concludendo di fatto la three-way-handshake.

E' una delle scansioni meno rumorose, proprio per via del fatto che non si stabilisce una connessione TCP completa. Per questo motivo le informazioni ottenute dalla scansione sono limitate rispetto a scansioni più aggressive.

Abbiamo scoperto 12 porte aperte. Tra le informazioni ci sono il numero di porta ed il tipo (es. 21/tcp), lo stato (open) e il tipo di servizio della porta (ftp, telnet, http ecc...).



```
(kali@kali)-[~]
$ sudo nmap -sS 192.168.50.101 -p 1-1024
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-31 03:56 EST
Nmap scan report for 192.168.50.101
Host is up (0.00019s 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: 08:00:27:31:C7:7B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.28 seconds
```

Durante la scansione abbiamo intercettato il traffico tramite Wireshark e abbiamo notato che se la porta scansionata è aperta, Metasploitable risponde con un pacchetto SYN/ACK ma Kali non risponde con solito pacchetto ACK.

Nell'immagine: la porta 34 risponde con un pacchetto SYN/ACK. La macchina Kali chiuderà in seguito la connessione inviando un pacchetto TCP con il flag RST (reset) attivo, abbandonando quindi la connessione.

tcp.port == 34						
No.	Time	Source	Destination	Protocol	Length	Info
520	13.110877213	192.168.50.100	192.168.50.101	TCP	58	64743 → 34 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
528	13.110991734	192.168.50.101	192.168.50.100	TCP	60	34 → 64743 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0



SCANSIONE TCP

La scansione “-sT” stabilisce un canale TCP concludendo di fatto la three-way-handshake. E’ una scansione più invasiva.

```
(kali㉿kali)-[~]
$ sudo nmap -sT 192.168.50.101 -p 1-1024
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-31 04:12 EST
Nmap scan report for 192.168.50.101
Host is up (0.00042s 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: 08:00:27:31:C7:7B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
```

Tramite Wireshark possiamo verificare la three-way-handshake applicando un filtro per un porta aperta, ad esempio la 139.

tcp.port == 139						
No.	Time	Source	Destination	Protocol	Length	Info
8	13.072455615	192.168.50.100	192.168.50.101	TCP	74	56688 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=65941106 TSecr=102895
13	13.072849342	192.168.50.101	192.168.50.100	TCP	74	139 → 56688 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=102895 TSecr=65941106
15	13.072855179	192.168.50.100	192.168.50.101	TCP	66	56688 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=65941106 TSecr=102895
30	13.074184779	192.168.50.100	192.168.50.101	TCP	66	56688 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=65941107 TSecr=102895

Dopo aver ricevuto il pacchetto SYN/ACK, Kali invierà il pacchetto ACK e poi chiuderà la connessione inviando un altro pacchetto TCP con il flag RST attivo.

SCANSIONE -A

Questa scansione è molto più rumorosa delle precedenti, ma consente di ottenere molte informazioni sul target (porte aperte, versione dei servizi, sistema operativo target e moltissime altre). Impiega più tempo rispetto ai metodi discussi di sopra.

```
(kali㉿kali)-[~]
$ sudo nmap -A 192.168.50.101 -p 1-1024
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-31 04:22 EST
Nmap scan report for 192.168.50.101
Host is up (0.00030s 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
|_smtp_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
|_ ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_  SSL2_RC4_128_EXPORT40_WITH_MD5
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
111/tcp   open  rpcbind      2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2                111/tcp    rpcbind
```

```

| 100000 2          111/tcp  rpcbind
| 100000 2          111/udp  rpcbind
| 100003 2,3,4      2049/tcp  nfs
| 100003 2,3,4      2049/udp  nfs
| 100005 1,2,3      51246/udp  mountd
| 100005 1,2,3      55522/tcp  mountd
| 100021 1,3,4      41673/udp  nlockmgr
| 100021 1,3,4      54163/tcp  nlockmgr
| 100024 1          42674/tcp  status
|_ 100024 1          57484/udp  status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open  exec        netkit-rsh rexecd
513/tcp open  login?
514/tcp open  shell       Netkit rshd
MAC Address: 08:00:27:31:C7:7B (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
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/
o:linux:linux_kernel

Host script results:
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
|_ clock-skew: mean: 2h29m59s, deviation: 3h32m07s, median: 0s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-12-31T04:23:02-05:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT      ADDRESS
1   0.30 ms  192.168.50.101

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 99.10 seconds

```


Intercettando il traffico su Wireshark si nota come ci sia uno scambio di pacchetti più intenso. Ad esempio, se la scansione della porta 80 in modalità TCP avviene stabilendo un canale TCP con immediato reset della connessione, con la scan aggressiva si richiedono anche le pagine HTML per ottenere maggiori informazioni.

No.	Time	Source	Destination	Protocol	Length	Info
2507	50.778598428	192.168.50.100	192.168.50.101	HTTP	222	OPTIONS / HTTP/1.1
2509	50.778668491	192.168.50.100	192.168.50.101	HTTP	242	GET /nmaplowercheck1704014582 HTTP/1.1
2510	50.778717003	192.168.50.101	192.168.50.100	TCP	66	80 → 36526 [ACK] Seq=1 Ack=153 Win=6912 Len=0 TSval=156711 TSecr=66479375
2511	50.778717107	192.168.50.101	192.168.50.100	TCP	66	80 → 36540 [ACK] Seq=1 Ack=157 Win=6912 Len=0 TSval=156711 TSecr=66479376
2513	50.778756120	192.168.50.100	192.168.50.101	HTTP	227	GET /.git/HEAD HTTP/1.1
2514	50.778762694	192.168.50.100	192.168.50.101	HTTP	684	POST /sdk HTTP/1.1
2515	50.778784742	192.168.50.100	192.168.50.101	HTTP	228	GET /robots.txt HTTP/1.1
2517	50.778814476	192.168.50.100	192.168.50.101	HTTP	84	GET / HTTP/1.0
2518	50.778823038	192.168.50.100	192.168.50.101	HTTP	233	PROPFIND / HTTP/1.1
2519	50.778830765	192.168.50.100	192.168.50.101	HTTP	376	POST / HTTP/1.1 (application/x-www-form-urlencoded)
2521	50.778882780	192.168.50.101	192.168.50.100	TCP	66	80 → 36558 [ACK] Seq=1 Ack=177 Win=6912 Len=0 TSval=156711 TSecr=66479376
2523	50.778926930	192.168.50.101	192.168.50.100	TCP	66	80 → 36568 [ACK] Seq=1 Ack=162 Win=6912 Len=0 TSval=156711 TSecr=66479376
2524	50.778926996	192.168.50.101	192.168.50.100	TCP	66	80 → 36564 [ACK] Seq=1 Ack=619 Win=7040 Len=0 TSval=156711 TSecr=66479376
2525	50.778978563	192.168.50.101	192.168.50.100	TCP	66	80 → 36546 [ACK] Seq=1 Ack=163 Win=6912 Len=0 TSval=156711 TSecr=66479376
2526	50.778978641	192.168.50.101	192.168.50.100	TCP	66	80 → 36492 [ACK] Seq=1 Ack=19 Win=5824 Len=0 TSval=156711 TSecr=66479376
2527	50.778978704	192.168.50.101	192.168.50.100	TCP	66	80 → 36582 [ACK] Seq=1 Ack=168 Win=6912 Len=0 TSval=156711 TSecr=66479376
2528	50.778978762	192.168.50.101	192.168.50.100	TCP	66	80 → 36510 [ACK] Seq=1 Ack=311 Win=6912 Len=0 TSval=156711 TSecr=66479376
2532	50.780088123	192.168.50.101	192.168.50.100	HTTP	558	HTTP/1.1 404 Not Found (text/html)
2533	50.780088254	192.168.50.101	192.168.50.100	TCP	66	80 → 36558 [FIN, ACK] Seq=493 Ack=177 Win=6912 Len=0 TSval=156711 TSecr=66479376
2534	50.780098825	192.168.50.100	192.168.50.101	TCP	66	36558 → 80 [ACK] Seq=177 Ack=493 Win=64128 Len=0 TSval=66479377 TSecr=156711
2535	50.780152889	192.168.50.101	192.168.50.100	HTTP	543	HTTP/1.1 404 Not Found (text/html)

Frame 21: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0	0000 08 00 27 31 c7 7b 08 00 27 cb 7e f5 08 00 45 00
Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: PcsCompu_31:c7:7b (08:00:27:31:c7:7b)	0010 00 28 00 00 40 00 40 06 54 b6 c0 a8 32 64 c0 a8
Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.101	0020 32 65 b1 39 00 50 bf 57 77 16 00 00 00 00 50 04
Transmission Control Protocol, Src Port: 45369, Dst Port: 80, Seq: 1, Len: 0	0030 00 00 e1 ce 00 00