

Esercitazione M3D2

Nmap

Ettore Farris - 23/12/2023

1) Descrizione sintetica dell'esercitazione

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.

2) Svolgimento

- 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-hankshake*. 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...).

```
root@kali: /home/kali/Desktop
File Actions Edit View Help
+
(root@kali)-[/home/kali/Desktop]
# nmap -sS 192.168.50.101 -p 0-1024
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-29 18:50 EST
Nmap scan report for 192.168.50.101
Host is up (0.0011s latency).
Not shown: 1013 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: 08:00:27:2B:56:8F (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 1.03 seconds
```

Nell'immagine: le porte 80 e 139 rispondono 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.

7	0.172974556	192.168.50.100	192.168.50.101	TCP	58 588802 - 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	0.172316544	192.168.50.100	192.168.50.101	TCP	58 588802 - 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	0.172497434	192.168.50.100	192.168.50.101	TCP	58 588802 - 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10	0.172683313	192.168.50.100	192.168.50.101	TCP	58 588802 - 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11	0.172856675	192.168.50.100	192.168.50.101	TCP	58 588802 - 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12	0.173029830	192.168.50.100	192.168.50.101	TCP	58 588802 - 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13	0.173206528	192.168.50.100	192.168.50.101	TCP	58 588802 - 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14	0.173407999	192.168.50.100	192.168.50.101	TCP	58 588802 - 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15	0.173644186	192.168.50.100	192.168.50.101	TCP	58 588802 - 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	0.173869297	192.168.50.100	192.168.50.101	TCP	58 588802 - 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	0.174231389	192.168.50.101	192.168.50.100	TCP	60 111 - 58802 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
18	0.174529979	192.168.50.100	192.168.50.101	TCP	54 588802 - 111 [RST] Seq=1 Win=0 Len=0
19	0.176882934	192.168.50.101	192.168.50.100	TCP	60 80 - 58802 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
20	0.176883480	192.168.50.101	192.168.50.100	TCP	60 139 - 58802 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
21	0.176883607	192.168.50.101	192.168.50.100	TCP	60 25 - 58802 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
22	0.176884004	192.168.50.101	192.168.50.100	TCP	60 110 - 58802 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	0.176884114	192.168.50.101	192.168.50.100	TCP	60 993 - 58802 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	0.176884257	192.168.50.101	192.168.50.100	TCP	60 445 - 58802 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
25	0.177121868	192.168.50.100	192.168.50.101	TCP	54 588802 - 80 [RST] Seq=1 Win=0 Len=0
26	0.177485669	192.168.50.100	192.168.50.101	TCP	54 588802 - 139 [RST] Seq=1 Win=0 Len=0

- **Scansione TCP (-sT)**

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

```
root@kali: /home/kali/Desktop

File Actions Edit View Help

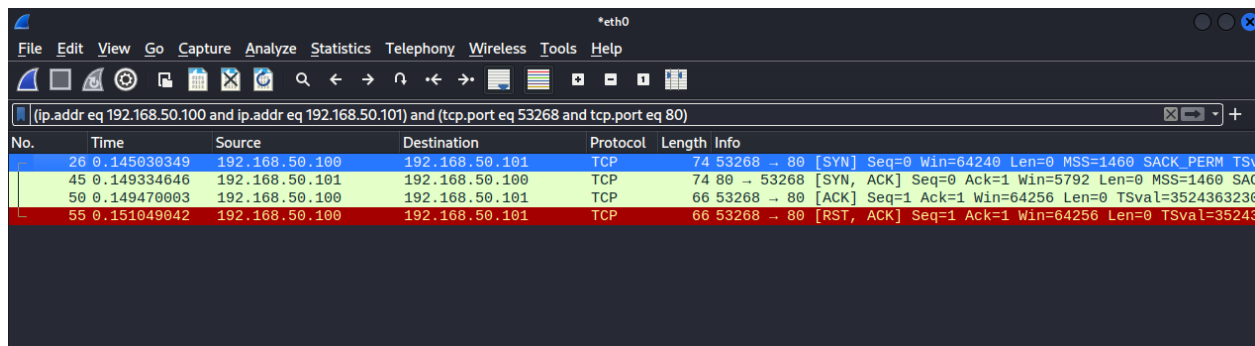
(root@kali)-[/home/kali/Desktop]
# nmap -sT 192.168.50.101 -p 0-1024
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-29 19:21 EST
Nmap scan report for 192.168.50.101
Host is up (0.0060s latency).
Not shown: 1013 closed tcp ports (conn-refused)

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: 08:00:27:2B:56:8F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.05 seconds
```

Tramite Wireshark possiamo verificare la three-way-handshake applicando un filtro per un porta aperta, ad esempio quella 80.



The image shows a Wireshark packet capture window with the filter '(ip.addr eq 192.168.50.100 and ip.addr eq 192.168.50.101) and (tcp.port eq 53268 and tcp.port eq 80)'. The packet list shows four packets:

No.	Time	Source	Destination	Protocol	Length	Info
26	0.145030349	192.168.50.100	192.168.50.101	TCP	74	53268 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS...
45	0.149334646	192.168.50.101	192.168.50.100	TCP	74	80 → 53268 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SAC...
50	0.149470003	192.168.50.100	192.168.50.101	TCP	66	53268 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3524363236...
55	0.151049042	192.168.50.100	192.168.50.101	TCP	66	53268 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=35243...

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.

(Vedi pagine successive)

```

(root@kali)-[/home/kali/Desktop]
# nmap -A 192.168.50.101 -p 1-1024
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-29 19:33 EST
Nmap scan report for 192.168.50.101
Host is up (0.0033s latency).
Not shown: 1012 closed tcp ports (reset)

```

PORT	STATE	SERVICE	VERSION	Source	Destination	Protocol	Length
21/tcp	open	ftp	vsftpd 2.3.4	192.168.50.101	192.168.50.100	FTP	104
_ftp-anon: Anonymous FTP login allowed (FTP code 230)							
_ftp-syst: 1552 73:681784577 192.168.50.100 192.168.50.101 TCP 66							
_STAT: 1553 73:681784577 192.168.50.100 192.168.50.101 TCP 66							
_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							
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)	192.168.50.101	192.168.50.100	TCP	66
_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	192.168.50.101	192.168.50.100	TCP	66
25/tcp	open	smtp	Postfix smtpd	192.168.50.101	192.168.50.100	TCP	66
_ssl-date: 2023-12-23T02:47:33+00:00; -6d21h47m21s from scanner time.							
_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTT							
_LS, ENHANCEDSTATUSCODES, 8BITMIME, DSN							
_ssl-v2:							
_SSLv2 supported							
_ciphers:							
_SSL2_DES_192_EDE3_CBC_WITH_MD5							
_SSL2_RC2_128_CBC_WITH_MD5							
_SSL2_RC2_128_CBC_EXPORT40_WITH_MD5							
_SSL2_DES_64_CBC_WITH_MD5							
_SSL2_RC4_128_EXPORT40_WITH_MD5							
_SSL2_RC4_128_WITH_MD5							
_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrP							
_rovinceName=There is no such thing outside US/countryName=XX							
_Not valid before: 2010-03-17T14:07:45							
_Not valid after: 2010-04-16T14:07:45							
53/tcp	open	domain	ISC BIND 9.4.2	192.168.50.101	192.168.50.100	TCP	66
_dns-nsid:							
_bind.version: 9.4.2							
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)	192.168.50.101	192.168.50.100	TCP	66
_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/udp    rpcbind
|   100003   2,3,4         2049/tcp   nfs
|   100003   2,3,4         2049/udp   nfs
|   100005   1,2,3         38492/tcp  mountd
|   100005   1,2,3         45496/udp  mountd
|   100021   1,3,4         54759/tcp  nlockmgr
|   100021   1,3,4         58945/udp  nlockmgr
|   100024   1             49950/tcp  status
|   100024   1             58725/udp  status
|_ 139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
| 445/tcp open  %b%*U       Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
| 512/tcp open  exec?
| 513/tcp open  login       OpenBSD or Solaris rlogind
| 514/tcp open  tcpwrapped
MAC Address: 08:00:27:2B:56:8F (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:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-12-22T21:47:24-05:00
|_ clock-skew: mean: -6d20h07m20s, deviation: 2h53m12s, median: -6d21h47m21s

TRACEROUTE
HOP RTT ADDRESS
1 3.34 ms 192.168.50.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 76.22 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.

3283	66.857832269	192.168.50.101	192.168.50.100	TCP	66.80 → 52846 [FIN, ACK] Seq=1186 Ack=210 Win=6912 Len=0 TSval=1452857 TSecr=3525154797
3288	66.899049729	192.168.50.100	192.168.50.101	TCP	66.52846 → 80 [ACK] Seq=216 Ack=1107 Win=64128 Len=0 TSval=3525154860 TSecr=1452057
3289	66.943987417	192.168.50.100	192.168.50.101	TCP	66.52846 → 80 [FIN, ACK] Seq=216 Ack=1107 Win=64128 Len=0 TSval=3525154905 TSecr=1452057
3292	66.946228671	192.168.50.101	192.168.50.100	TCP	66.80 → 52846 [ACK] Seq=1107 Ack=217 Win=6912 Len=0 TSval=1452066 TSecr=3525154905
3368	73.397225997	192.168.50.100	192.168.50.101	TCP	74.39986 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3525161358 TSecr=0 WS=128
3369	73.399456341	192.168.50.101	192.168.50.100	TCP	74.80 → 39986 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1452711 TSecr=3525161358 WS=128
3370	73.400752705	192.168.50.100	192.168.50.101	TCP	66.39986 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3525161361 TSecr=1452711
3396	73.439741811	192.168.50.100	192.168.50.101	HTTP	84 GET / HTTP/1.0
3399	73.440880989	192.168.50.101	192.168.50.100	TCP	66.80 → 39986 [ACK] Seq=1 Ack=19 Win=5888 Len=0 TSval=1452715 TSecr=3525161400
3408	73.487809537	192.168.50.101	192.168.50.100	HTTP	1152 HTTP/1.1 200 OK (text/html)
3409	73.487826335	192.168.50.100	192.168.50.101	TCP	66.39986 → 80 [ACK] Seq=19 Ack=1087 Win=64128 Len=0 TSval=3525161449 TSecr=1452720
3437	73.510975734	192.168.50.101	192.168.50.100	TCP	66.80 → 39986 [FIN, ACK] Seq=1087 Ack=19 Win=5888 Len=0 TSval=1452722 TSecr=3525161449
3440	73.531756303	192.168.50.100	192.168.50.101	TCP	66.39986 → 80 [FIN, ACK] Seq=19 Ack=1088 Win=64128 Len=0 TSval=3525161492 TSecr=1452722
3441	73.532245852	192.168.50.100	192.168.50.101	TCP	74.39986 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3525161493 TSecr=0 WS=128
3442	73.532569822	192.168.50.101	192.168.50.100	TCP	66.80 → 39986 [ACK] Seq=1088 Ack=20 Win=5888 Len=0 TSval=1452724 TSecr=3525161492
3443	73.533021163	192.168.50.101	192.168.50.100	TCP	74.80 → 39986 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1452724 TSecr=3525161493 WS=128
3444	73.533138361	192.168.50.100	192.168.50.101	TCP	66.39986 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3525161494 TSecr=1452724
3456	73.540529493	192.168.50.100	192.168.50.101	HTTP	106 GET / HTTP/1.1
3457	73.541116253	192.168.50.101	192.168.50.100	TCP	66.80 → 39986 [ACK] Seq=1 Ack=41 Win=5888 Len=0 TSval=1452725 TSecr=3525161501
3474	73.574795379	192.168.50.101	192.168.50.100	HTTP	1133 HTTP/1.1 200 OK (text/html)