ESERCITAZIONE W9D1(2)

EPICODE

Esercizio
Nmap scan

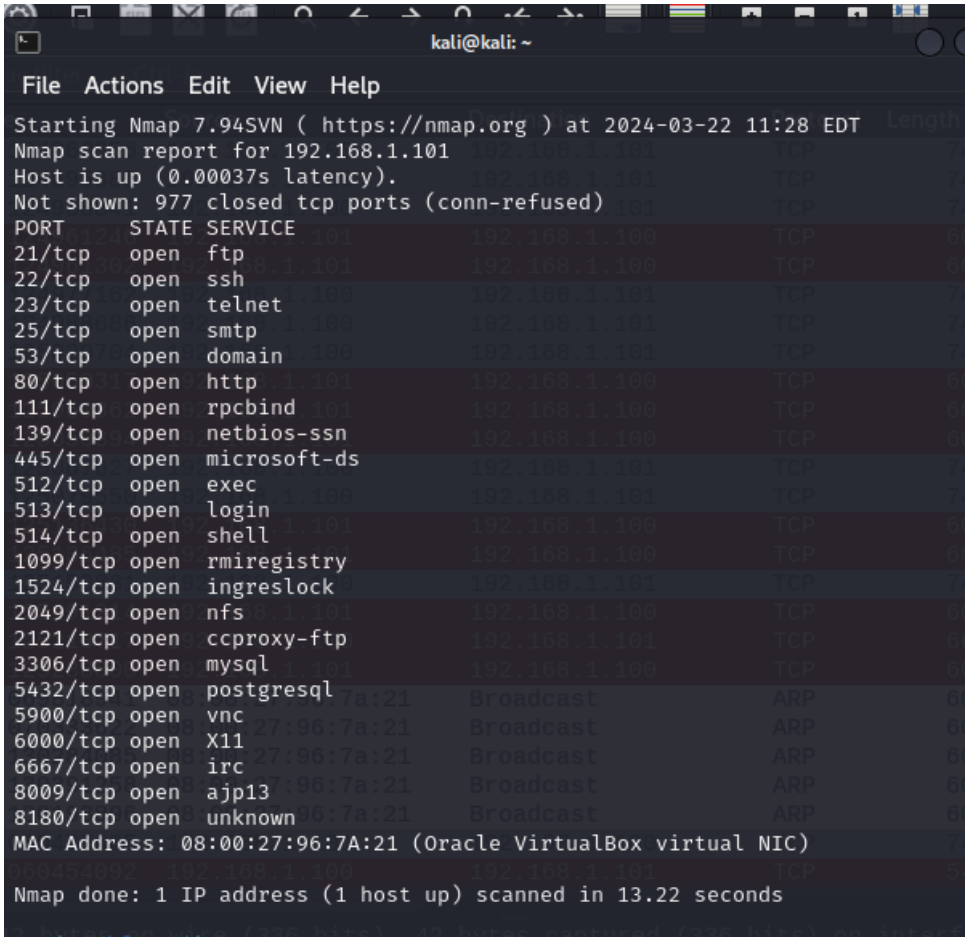
Traccia:

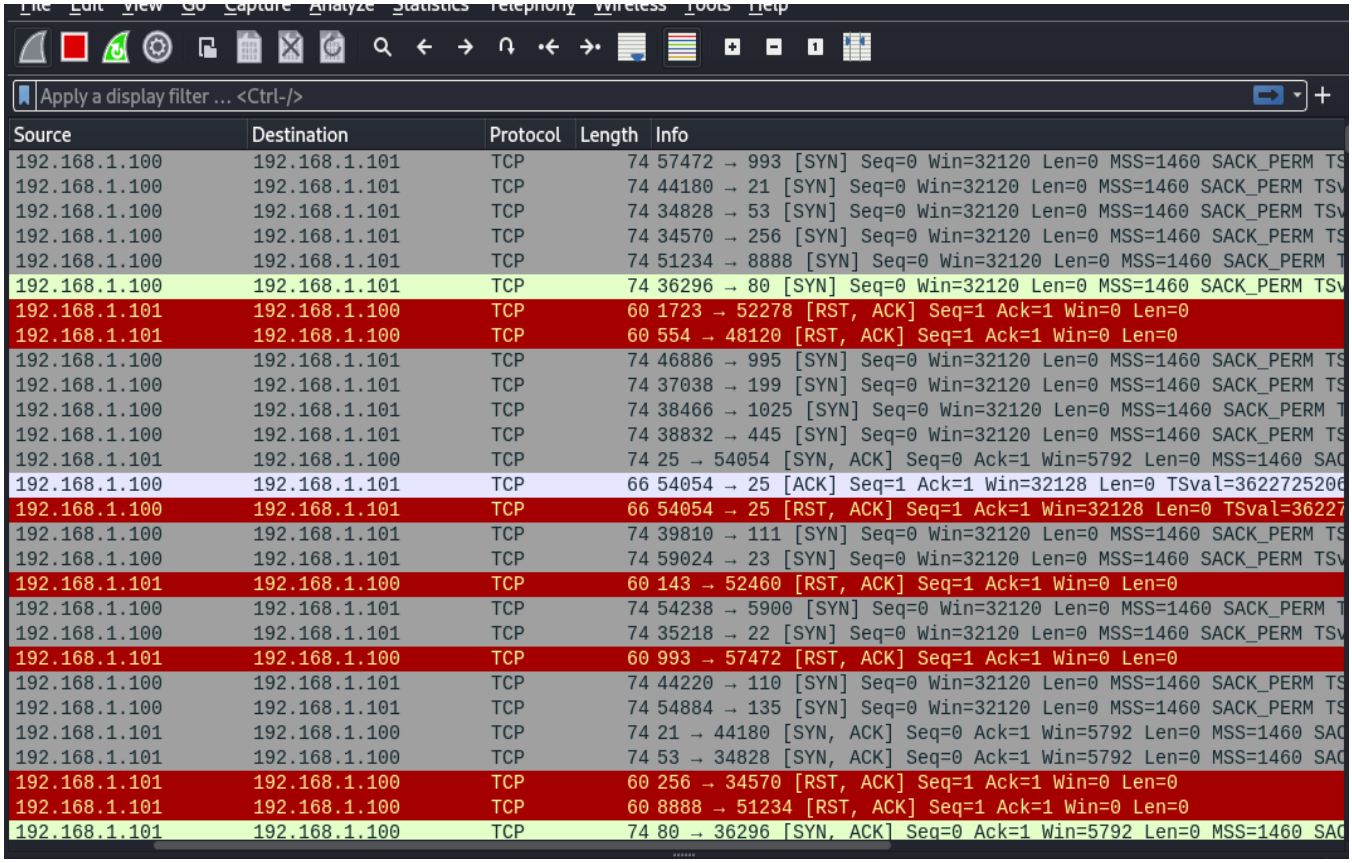
Vedremo da vicino nmap e i suoi comandi.
Sulle base delle nozioni viste nella lezione teorica eseguiremo diversi tipi di scan sulla macchine metasploitable, come di seguito:

- 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



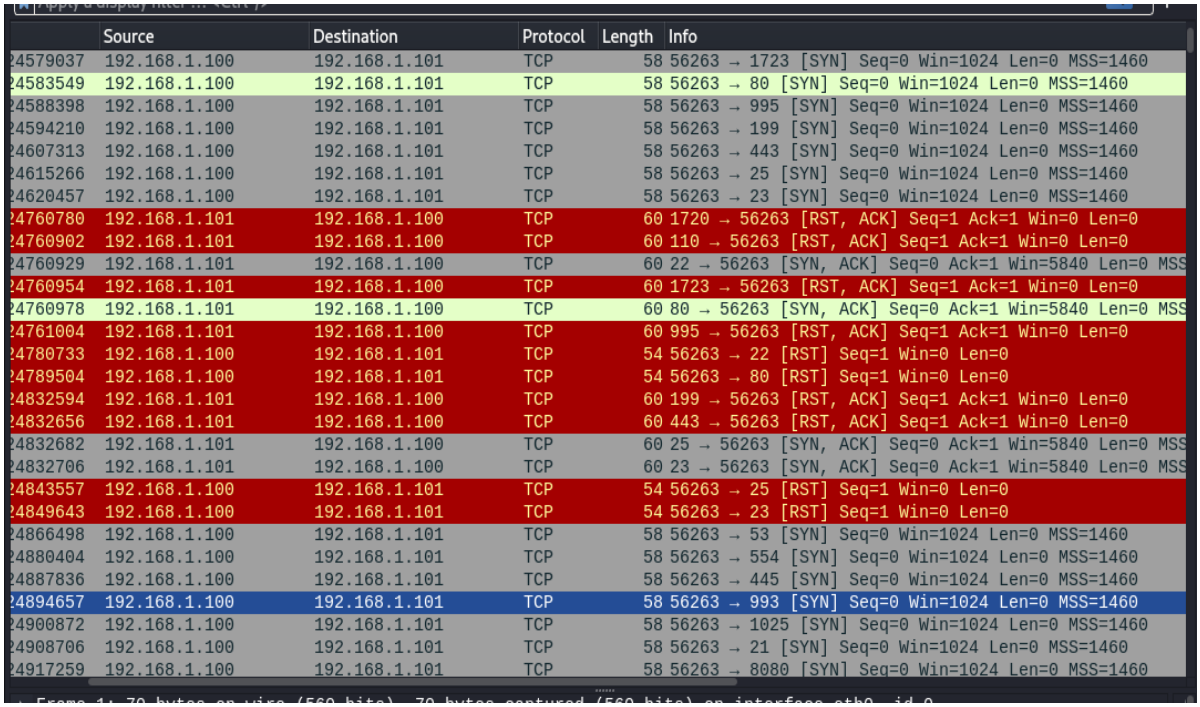


Dalla cattura di wireshark possiamo vedere che il tentativo di 3 way handshake è riuscito solo sulle porte aperte.

SCANSIONE SYN

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-22 11:37 EDT
Nmap scan report for 192.168.1.101
Host is up (0.00013s 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: 08:00:27:96:7A:21 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
```

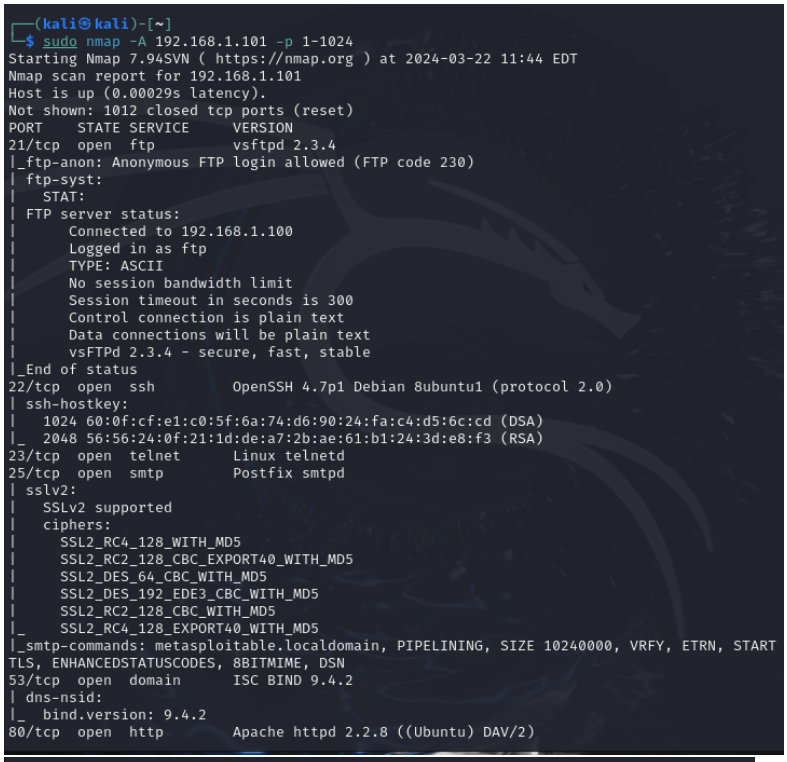


	Source	Destination	Protocol	Length	Info
24579037	192.168.1.100	192.168.1.101	TCP	58	56263 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24583549	192.168.1.100	192.168.1.101	TCP	58	56263 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24588398	192.168.1.100	192.168.1.101	TCP	58	56263 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24594210	192.168.1.100	192.168.1.101	TCP	58	56263 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24607313	192.168.1.100	192.168.1.101	TCP	58	56263 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24615266	192.168.1.100	192.168.1.101	TCP	58	56263 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24620457	192.168.1.100	192.168.1.101	TCP	58	56263 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24760780	192.168.1.101	192.168.1.100	TCP	60	1720 → 56263 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24760902	192.168.1.101	192.168.1.100	TCP	60	110 → 56263 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24760929	192.168.1.101	192.168.1.100	TCP	60	22 → 56263 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS
24760954	192.168.1.101	192.168.1.100	TCP	60	1723 → 56263 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24760978	192.168.1.101	192.168.1.100	TCP	60	80 → 56263 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS
24761004	192.168.1.101	192.168.1.100	TCP	60	995 → 56263 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24780733	192.168.1.100	192.168.1.101	TCP	54	56263 → 22 [RST] Seq=1 Win=0 Len=0
24789504	192.168.1.100	192.168.1.101	TCP	54	56263 → 80 [RST] Seq=1 Win=0 Len=0
24832594	192.168.1.101	192.168.1.100	TCP	60	199 → 56263 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24832656	192.168.1.101	192.168.1.100	TCP	60	443 → 56263 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24832682	192.168.1.101	192.168.1.100	TCP	60	25 → 56263 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS
24832706	192.168.1.101	192.168.1.100	TCP	60	23 → 56263 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS
24843557	192.168.1.100	192.168.1.101	TCP	54	56263 → 25 [RST] Seq=1 Win=0 Len=0
24849643	192.168.1.100	192.168.1.101	TCP	54	56263 → 23 [RST] Seq=1 Win=0 Len=0
24866498	192.168.1.100	192.168.1.101	TCP	58	56263 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24880404	192.168.1.100	192.168.1.101	TCP	58	56263 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24887836	192.168.1.100	192.168.1.101	TCP	58	56263 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24894657	192.168.1.100	192.168.1.101	TCP	58	56263 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24900872	192.168.1.100	192.168.1.101	TCP	58	56263 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24908706	192.168.1.100	192.168.1.101	TCP	58	56263 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24917259	192.168.1.100	192.168.1.101	TCP	58	56263 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Il SYN scan è considerato meno invasivo rispetto allo scan completo (sT) poiché, una volta ricevuto il pacchetto SYN/ACK dalla macchina di

destinazione, Nmap non completa il 3-way-handshake. Invece, dopo aver verificato che la porta è aperta, termina la comunicazione senza creare il canale completo. Questo aiuta a evitare sovraccarichi dovuti alla creazione e al mantenimento di molteplici connessioni.

SCANSIONE CON LO SWITCH -A



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 192.168.1.101 -p 1-1024
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-22 11:44 EDT
Nmap scan report for 192.168.1.101
Host is up (0.00029s 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 192.168.1.100
|      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)
| 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_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, START
TLS, ENHANCEDSTATUSCODES, 8BITMIME, 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)
```

```
File  Actions  Edit  View  Help
|   100021  1,3,4      37798/tcp   nlockmgr
|   100021  1,3,4      59492/udp   nlockmgr
|   100024  1          56814/udp   status
|_  100024  1          57537/tcp   status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn 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: 08:00:27:96:7A:21 (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:linu
x_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-03-22T11:45:20-04:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (
unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 2h00m04s, deviation: 2h49m50s, median: -1s

TRACEROUTE
HOP RTT     ADDRESS
1   0.29 ms 192.168.1.101

OS and Service detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 99.46 seconds
```

Lo switch -A di Nmap consente di ottenere una vasta gamma di informazioni utili sull'indirizzo IP di destinazione, come la versione del sistema operativo e dei servizi attivi sulle porte aperte. Pur essendo uno degli scans più invasivi, poiché invia numerose richieste, fornisce dati preziosi per le fasi successive dell'analisi.