

# NMAP

Nmap è un software open-source ampiamente utilizzato per la scansione di reti e l'analisi della sicurezza.

Nmap, acronimo di Network Mapper, è uno strumento di scansione di rete progettato per esplorare, mappare e analizzare reti informatiche.

**Nmap** può essere utilizzato per **individuare** e **analizzare** le porte aperte su un dispositivo o su una rete. Questo è utile per identificare servizi in esecuzione e potenziali vulnerabilità.

Può tentare di **determinare il sistema operativo** in esecuzione su un dispositivo sulla base delle risposte dei pacchetti di rete. Questo aiuta gli amministratori di sistema a comprendere meglio la loro infrastruttura e a identificare potenziali punti deboli.

E' in grado di rilevare i servizi in esecuzione su una macchina e le versioni di tali servizi. Questo è cruciale per la valutazione della sicurezza e per l'identificazione di software obsoleto o vulnerabile.

Può aiutare a **mappare la topologia di una rete** identificando dispositivi, router e switch. Questo è importante per la pianificazione della sicurezza e per la comprensione della struttura di una rete.

Nmap può essere utilizzato per valutare la sicurezza di una rete identificando potenziali vulnerabilità e punti deboli. Durante i **penetration test** per **identificare possibili vie di accesso** non autorizzate. Come strumento per l'analisi degli incidenti di sicurezza per comprendere meglio l'estensione di una violazione e **identificare dispositivi compromessi** e può essere integrato in sistemi di monitoraggio di rete per rilevare cambiamenti nella topologia di rete e nelle configurazioni dei dispositivi.

# **SVOLGIMENTO DELL'ESERCIZIO**

E' stato richiesto di effettuare tre scansioni

**TCP, SYN e -A**

**TCP -sS** invia solo pacchetti SYN ai dispositivi di destinazione senza completare l'handshake TCP. Con Wireshark si può una serie di pacchetti SYN inviati dalla shell 1 verso la shell di destinazione, non ci saranno pacchetti di risposta SYN/ACK o ACK.

Questa scelta è fatta per essere più furtiva e non lasciare traccia nell'endpoint di destinazione, ma può essere rilevata da sistemi di sicurezza come firewall o IDS che monitorano il traffico di rete.

```
(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.3.245 -p 0-1024
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-20 21:51 CEST
Nmap scan report for 192.168.3.245
Host is up (0.00095s 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: 08:00:27:56:32:EC (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.09 seconds
```

```
192.168.3.245 192.168.3.14 TCP 60 165 → 54109 [RST, ACK] Seq=1
192.168.3.14 192.168.3.245 TCP 58 54109 → 1002 [SYN] Seq=0 Win=
192.168.3.14 192.168.3.245 TCP 58 54109 → 332 [SYN] Seq=0 Win=
192.168.3.245 192.168.3.14 TCP 60 1002 → 54109 [RST, ACK] Seq=1
.14 TCP 60 332 → 54109 [RST, ACK] Seq=1
.245 TCP 58 54109 → 997 [SYN] Seq=0 Win=
.14 TCP 60 997 → 54109 [RST, ACK] Seq=1
.245 TCP 58 54109 → 857 [SYN] Seq=0 Win=
.245 TCP 58 54109 → 780 [SYN] Seq=0 Win=
.245 TCP 58 54109 → 462 [SYN] Seq=0 Win=
.14 TCP 60 857 → 54109 [RST, ACK] Seq=1
.14 TCP 60 780 → 54109 [RST, ACK] Seq=1
Transmission Control Protocol, Src Port: 54109, Dst Port: 332,
Source Port: 54109
Destination Port: 332
[Stream index: 1006]
[Conversation completeness: Incomplete (37)]
...1. .... = RST: Present
...0 .... = FIN: Absent
.... 0... = Data: Absent
.... .1.. = ACK: Present
.....0. = SYN-ACK: Absent
.... ...1 = SYN: Present
[Completeness Flags: R..A.S]
```

**SYN -sT** questo tipo di scansione completa l'handshake TCP, inviando pacchetti SYN, ricevendo pacchetti SYN/ACK e inviando ACK di risposta. Con Wireshark, vedrai il normale flusso di pacchetti TCP per l'inizializzazione di una connessione, inclusi pacchetti SYN, SYN/ACK e ACK. Questo metodo è meno furtivo rispetto alla scansione SYN ma è più affidabile perché completa l'handshake TCP.

```
(kali@kali)-[~]
$ sudo nmap -sT 192.168.3.245 -p 0-1024
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-20 21:56 CEST
Nmap scan report for 192.168.3.245
Host is up (0.0052s 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: 08:00:27:56:32:EC (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.39 seconds
```

```
74 45176 → 53 [SYN] Seq=0 Win=64240 Len=0
74 36520 → 80 [SYN] Seq=0 Win=64240 Len=0
74 53 → 45176 [SYN, ACK] Seq=0 Ack=1 Win=
66 45176 → 53 [ACK] Seq=1 Ack=1 Win=64256
74 44402 → 87 [SYN] Seq=0 Win=64240 Len=0
74 43116 → 88 [SYN] Seq=0 Win=64240 Len=0
74 58044 → 84 [SYN] Seq=0 Win=64240 Len=0
74 36300 → 76 [SYN] Seq=0 Win=64240 Len=0

Flags: 0x012 (SYN, ACK)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
... 0... = Congestion Window Reduced: Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...1 = Acknowledgment: Set
.... ...0 = Push: Not set
.... ....0.. = Reset: Not set
.... ....1. = Syn: Set
.... ....0 = Fin: Not set
[TCP Flags: .....A..S.]

Flags: 0x010 (ACK)
00. .... = Reserved: Not set
..0 .... = Accurate ECN: Not set
.. 0... = Congestion Window Reduced: Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...1 = Acknowledgment: Set
.... ...0 = Push: Not set
.... ....0.. = Reset: Not set
.... ....0. = Syn: Not set
.... ....0 = Fin: Not set
[TCP Flags: .....A....]
```

Questo tipo di scansione è una scansione completa che include rilevamento di servizi, versioni di servizi, rilevamento di sistema operativo.

Con Wireshark si vedono un ampio spettro di pacchetti di rete, inclusi quelli associati a l'handshake TCP, ma anche altri tipi di pacchetti come quelli utilizzati per interrogare i servizi, ottenere informazioni sul sistema operativo.

Questa scansione può generare un traffico di rete significativo poiché esegue molte interrogazioni e analisi per raccogliere informazioni complete sul dispositivo di destinazione.

```
Source Address: 192.168.3.245
Destination Address: 192.168.3.14
Transmission Control Protocol, Src Port: 25, Dst Port: 45738, Seq=
Source Port: 25
Destination Port: 45738
[Stream index: 1127]
▼ [Conversation completeness: Complete, WITH_DATA (31)]
..0. .... = RST: Absent
...1 .... = FIN: Present
.... 1... = Data: Present
.... .1.. = ACK: Present
.... ..1. = SYN-ACK: Present
.... ...1 = SYN: Present
[Completeness Flags: .FDASS]
```

TCP	66 25 → 45738	[ACK]	Seq=56 Ack=23 Win=
TCP	66 80 → 42338	[ACK]	Seq=1088 Ack=20 Win=
TCP	74 80 → 42346	[SYN, ACK]	Seq=0 Ack=1 Win=
TCP	66 42346 → 80	[ACK]	Seq=1 Ack=1 Win=
Portmap	102 V103788859	proc-0	Reply (Call In 3)
TCP	66 858 → 111	[ACK]	Seq=45 Ack=37 Win=
RSTAT	94 V78206688	proc-0	Reply (Call In 3)
TCP	66 521 → 111	[ACK]	Seq=45 Ack=29 Win=
RPC	94	Continuation	
TCP	66 817 → 111	[ACK]	Seq=45 Ack=29 Win=

*Nell'ultima slide si mostra parte della risposta ottenuta da nmap visibile su shell e il grafico excel richiesto dall'esercizio.*



```

kali@kali)-[~]
$ sudo nmap -A 192.168.3.245 -p 0-1024
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-20 21:58 CEST
Nmap scan report for 192.168.3.245
Host is up (0.0019s latency).
Not shown: 1013 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 192.168.3.14
|_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
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=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
|_ssl-date: 2024-04-20T19:57:36+00:00; -1m38s from scanner time.
|_sslv2:
|_SSLv2 supported
|_ciphers:
|_SSL2_RC2_128_CBC_WITH_MD5
|_SSL2_RC4_128_EXPORT40_WITH_MD5
|_SSL2_DES_192_EDE3_CBC_WITH_MD5
|_SSL2_DES_64_CBC_WITH_MD5
|_SSL2_RC4_128_WITH_MD5
|_SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, 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)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

```

Fonte dello Scan	Target dello Scan	Tipo di Scan	Risultati Ottenuti
Kali Linux	192.168.3.245	Nmap -Ss	Trovati 12 servizi attivi sul target 192.168.1.16
Kali Linux	192.168.3.245	Nmap -sT	Trovati 12 servizi attivi sul target 192.168.1.16
Kali Linux	192.168.3.245	Nmap -A	Trovati 12 servizi attivi sul target 192.168.1.16