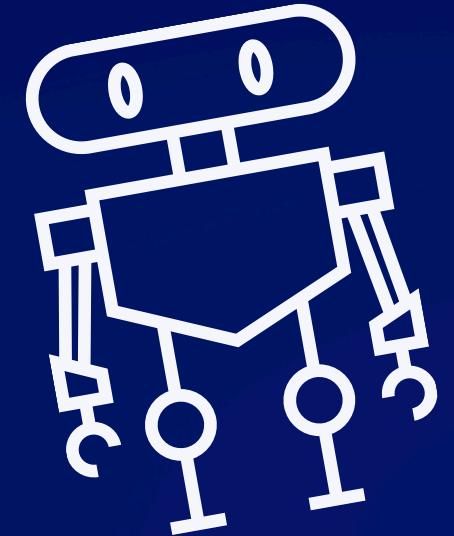
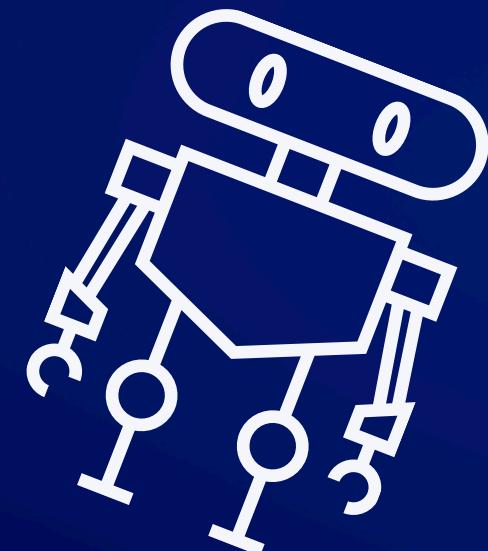




Scansione dei servizi con nmap

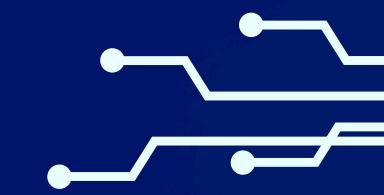
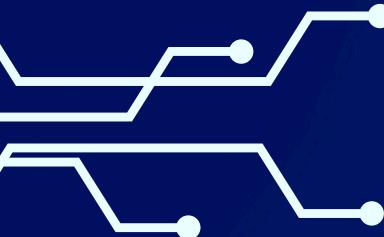
55/L3



Mara Dello Russo



# Cos'è nmap?



Nmap è uno strumento di **scansione di rete** open source utilizzato per scoprire dispositivi connessi a una rete e analizzare i servizi e le porte aperte su di essi. È ampiamente utilizzato dagli ethical hacker per valutare la sicurezza di una rete o per individuare vulnerabilità. Consente di eseguire varie operazioni, come la scansione di porte, la rilevazione di versioni di servizi, la tracciatura del percorso dei pacchetti e molto altro ancora. È uno strumento potente e flessibile che fornisce molte informazioni utili per la gestione e la sicurezza delle reti.

# Digitando nmap da terminale viene mostrato un elenco di tutti gli switch con le relative funzioni:

```
(kali㉿kali)-[~/Desktop] nmap -l
$ nmap
Nmap 7.94SVN ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/-sT/-sA/-sW/-sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/-sF/-sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/-sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
```

```
-sV: Probe open ports to determine service/version info
--version-intensity <level>: Set from 0 (light) to 9 (try all probes)
--version-light: Limit to most likely probes (intensity 2)
--version-all: Try every single probe (intensity 9)
--version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
    directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,... ]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
    <Lua scripts> is a comma-separated list of script-files or
    script-categories.
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
    probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g--source-port <portnum>: Use given port number
  --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
```

```
--ttl <val>: Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIdi3,
    and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --noninteractive: Disable runtime interactions via keyboard
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
```

In rosso gli switch che usiamo nelle slide successive

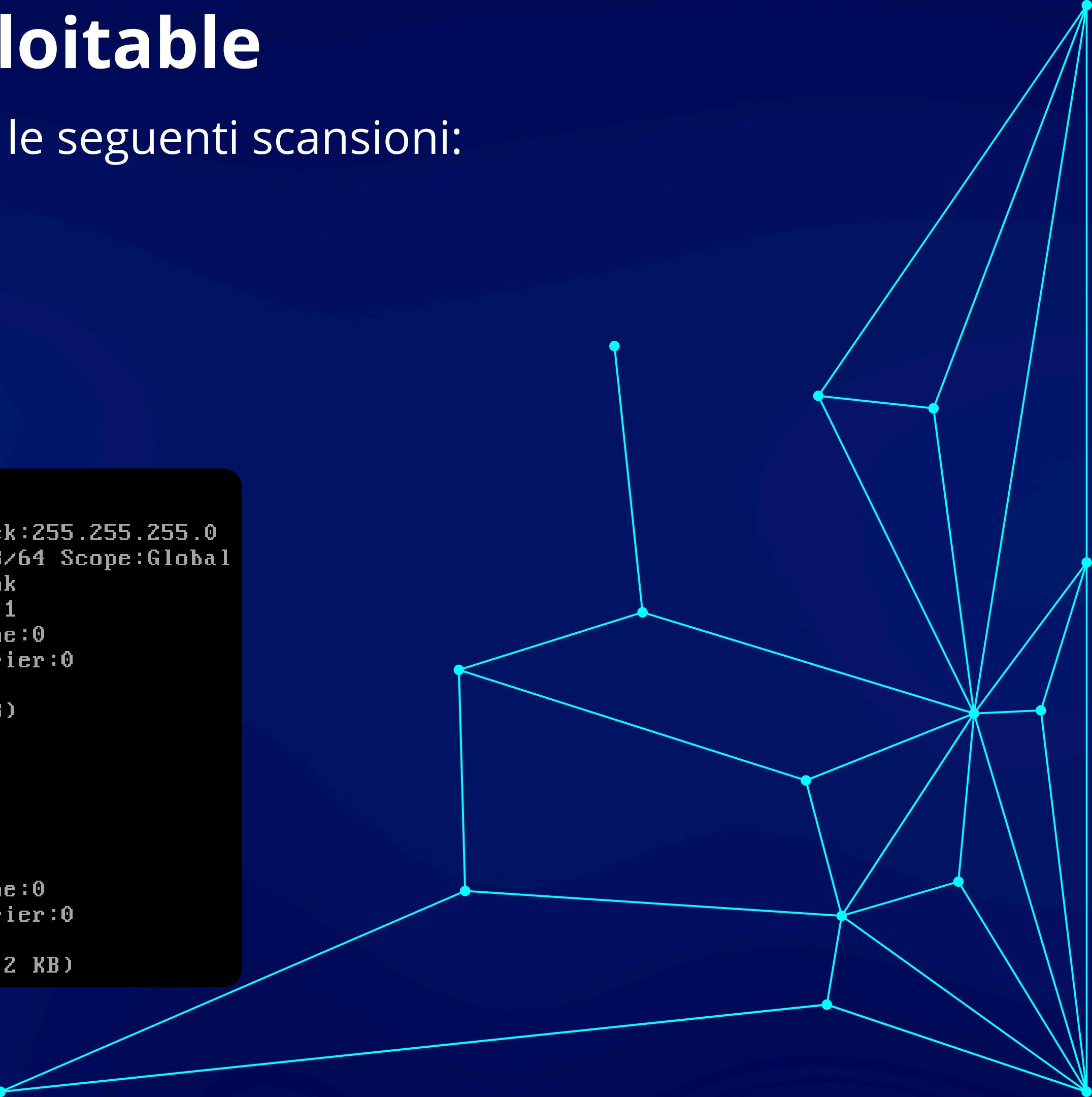
# Nmap su target Metasploitable

Effettueremo sul target Metasploitable le seguenti scansioni:

- 1.OS fingerprint
- 2.Syn Scan
- 3.TCP Connect
- 4.Version Detection

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a4:9f:a8
          inet addr:192.168.1.101  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2a01:e11:3003:d110:a00:27ff:fea4:9fa8/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fea4:9fa8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:714 errors:0 dropped:0 overruns:0 frame:0
          TX packets:487 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:70680 (69.0 KB)  TX bytes:63747 (62.2 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:490 errors:0 dropped:0 overruns:0 frame:0
          TX packets:490 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:207109 (202.2 KB)  TX bytes:207109 (202.2 KB)
```



# OS Fingerprint

La scansione OS fingerprint è una tecnica utilizzata da Nmap per **determinare il sistema operativo** in esecuzione su un determinato host nella rete. Questo processo coinvolge l'analisi delle risposte dei pacchetti inviati all'host in base a determinati criteri come il comportamento della pila TCP/IP, le opzioni IP e altri fattori specifici del sistema operativo.

## nmap -O

```
[root@kali ~]# nmap -O 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 11:04 CEST
Nmap scan report for 192.168.1.101
Host is up (0.0018s latency).
Not shown: 978 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
8180/tcp  open  unknown
MAC Address: 08:00:27:A4:9F:A8 (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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.89 seconds
```

# Syn Scan

Syn scan è una tecnica di scansione delle porte utilizzata da Nmap per determinare quali **porte di un determinato host sono aperte**. Questo tipo di scansione sfrutta il protocollo TCP e invia pacchetti SYN (synchronization) a ciascuna porta del dispositivo di destinazione. L'utilizzo di SYN scan è vantaggioso perché è più **discreto** rispetto ad altre tecniche di scansione delle porte, come le scansioni TCP complete, poiché non completa la connessione TCP, evitando così l'attivazione degli eventi di logging e intrusion detection system. Tuttavia, alcuni sistemi di sicurezza possono ancora rilevare e bloccare tali scansioni in base a modelli di traffico anomalo.

nmap -SS

```
# nmap -sS 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 11:07 CEST
Nmap scan report for 192.168.1.101
Host is up (0.0016s latency).
Not shown: 978 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
8180/tcp  open  unknown
MAC Address: 08:00:27:A4:9F:A8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.06 seconds
```

Il funzionamento del SYN scan è il seguente:

1. L'attaccante (o l'analista di sicurezza) invia un pacchetto **SYN** al dispositivo di destinazione per ogni porta che desidera esaminare.
2. Se la porta è chiusa, il dispositivo di destinazione risponderà con un pacchetto RST (reset), indicando che la porta è chiusa.
3. Se la porta è aperta, il dispositivo di destinazione non risponderà con un pacchetto RST, ma invierà invece un pacchetto di risposta **SYN/ACK** (synchronization/acknowledgment) indicando che la porta è aperta e pronta ad accettare connessioni.
4. Dopo aver ricevuto la risposta SYN/ACK, l'attaccante invierà un pacchetto RST per interrompere la connessione, **evitando così di stabilire una connessione TCP completa**.

# TCP Connect

La scansione TCP connect è una tecnica utilizzata da nmap per determinare lo stato delle porte di un host. Questo tipo di scansione coinvolge l'invio di connessioni TCP complete a ciascuna porta del dispositivo di destinazione per determinare se la porta è aperta, chiusa o filtrata. La scansione TCP è una delle tecniche più comuni utilizzate per la valutazione della sicurezza delle reti, poiché fornisce informazioni dettagliate sullo stato delle porte del dispositivo di destinazione. È più lenta e meno discreta rispetto al SYN scan, poiché richiede l'instaurazione di una connessione TCP completa per ogni porta esaminata.

**nmap -sT**

```
(root㉿kali)-[~/home/kali/Desktop]
# nmap -sT 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 11:09 CEST
Nmap scan report for 192.168.1.101
Host is up (0.0049s latency).
Not shown: 978 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
8180/tcp  open  unknown
MAC Address: 08:00:27:A4:9F:A8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.39 seconds
```

Il funzionamento del TCP Connect scan:

1. L'attaccante (o l'analista di sicurezza) invia un pacchetto **SYN** al dispositivo di destinazione per ogni porta che desidera esaminare.
2. Se la porta è chiusa, il dispositivo di destinazione risponderà con un pacchetto RST (reset), indicando che la porta è chiusa.
3. Se la porta è aperta, il dispositivo di destinazione non risponderà con un pacchetto RST, ma invierà invece un pacchetto di risposta **SYN/ACK** (synchronization/acknowledgment) indicando che la porta è aperta e pronta ad accettare connessioni.
4. Dopo aver ricevuto la risposta SYN/ACK, l'attaccante invierà un pacchetto **ACK** per conferma che l'host mittente ha ricevuto correttamente il pacchetto SYN/ACK del destinatario e accetta la connessione. Una volta che entrambi gli host hanno inviato e ricevuto correttamente i pacchetti SYN e SYN/ACK, **la connessione completa TCP è stabilita**.

# Version Detection

La version detection è una tecnica utilizzata da nmap per identificare le **versioni dei servizi** che operano sulle porte scansionate. Questo è utile perché consente agli amministratori di rete e agli analisti di sicurezza di comprendere esattamente quali servizi e versioni sono in esecuzione su un host, il che può essere cruciale per valutare la sicurezza della rete e individuare eventuali vulnerabilità.

**nmap -sV**

```
(root㉿kali)-[~/home/kali/Desktop]
# nmap -sV 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 11:10 CEST
Stats: 0:01:00 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.45% done; ETC: 11:11 (0:00:03 remaining)
Nmap scan report for 192.168.1.101
Host is up (0.00100s latency).

Not shown: 978 closed tcp ports (reset)

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8180/tcp  open  unknown

MAC Address: 08:00:27:A4:9F:A8 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 191.54 seconds
```

# Nmap su target Windows7

Effettueremo sul target Windows 7 la seguente scansione:

1.OS fingerprint

```
C:\Windows\system32\cmd.exe
C:\Users\admin>ipconfig

Configurazione IP di Windows

Scheda Ethernet Connessione alla rete locale (LAN):

    Suffixo DNS specifico per connessione: . . . . . : 2a01:e11:3003:d110:7d9f:65
    Indirizzo IPv6 . . . . . : . . . . . : 2a01:e11:3003:d110:29:cbc5
68:3ab3:cd67
    Indirizzo IPv6 temporaneo. . . . . : 2a01:e11:3003:d110:29:cbc5
:b718:310b
    Indirizzo IPv6 locale rispetto al collegamento . . . : fe80::7d9f:6568:3ab3:cd67%11
    Indirizzo IPv4. . . . . : 192.168.1.102
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : fe80::3a07:16ff:fe0e:83ef%11
                                192.168.1.1

Scheda Tunnel isatap.<205C26F0-EB66-41FF-A377-515F28681P41>:

    Stato supporto. . . . . : Supporto disconnesso
    Suffixo DNS specifico per connessione:

C:\Users\admin>
```



# OS Fingerprint

La scansione OS fingerprint è una tecnica utilizzata da Nmap per **determinare il sistema operativo** in esecuzione su un determinato host nella rete. Questo processo coinvolge l'analisi delle risposte dei pacchetti inviati all'host in base a determinati criteri come il comportamento della pila TCP/IP, le opzioni IP e altri fattori specifici del sistema operativo.

## nmap -O

```
Home SRT ZIP G...  
└─(kali㉿kali)-[~/Desktop]  
$ sudo nmap -O 192.168.1.102  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 13:23 CEST  
Nmap scan report for 192.168.1.102  
Host is up (0.0022s latency).  
Not shown: 990 closed tcp ports (reset)  
PORT      STATE SERVICE  
135/tcp    open  msrpc  
139/tcp    open  netbios-ssn  
445/tcp    open  microsoft-ds  
5357/tcp   open  wsddapi  
49152/tcp  open  unknown  
49153/tcp  open  unknown  
49154/tcp  open  unknown  
49155/tcp  open  unknown  
49156/tcp  open  unknown  
49157/tcp  open  unknown  
MAC Address: 08:00:27:21:68:86 (Oracle VirtualBox virtual NIC)  
Device type: general purpose  
Running: Microsoft Windows 7|2008|8.1  
OS CPE: cpe:/o:microsoft:windows_7:: - cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008: :sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1  
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or W  
indows 8.1 Update 1  
Network Distance: 1 hop  
  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 1.74 seconds
```

Il termine "unknown", che indica il servizio di alcune porte, si riferisce a una porta su cui non è stato possibile determinare lo stato, perché potrebbe essere in uno stato non supportato da Nmap o perché la risposta è stata ambigua. Per approfondire è possibile fare una scansione con nmap -T0, in modo da impostare il livello di "tempo" (T) a zero nella scansione con Nmap. Questo significa che si sta selezionando la modalità di scansione più lenta e accurata possibile, che potrebbe richiedere molto tempo ma può essere utile quando si desidera minimizzare il rumore di rete o evitare di essere rilevati durante la scansione.

GRAZIE PER  
L'ATTENZIONE

