

## **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.

La scansione dei servizi di rete è il primo passo per capire quali servizi potrebbero essere vulnerabili, ed essere sfruttati successivamente per ottenere accesso alla macchine.

E' molto importante in questa fase essere organizzati e strutturati.

Dunque, per ognuno degli scan effettuati, lo studente è invitato a riprodurre un report Excel / altro (tabella su word ad esempio) che riporti in maniera chiara:

- La fonte dello scan
- Il target dello scan
- Il tipo di scan
- I risultati ottenuti (e.s. trovati 50 servizi attivi sulla macchina)

```

(kali@kali)-[~]
$ sudo nmap -A -p 1-1023 192.168.0.109
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-16 16:54 EDT
Stats: 0:00:14 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.67% done; ETC: 16:54 (0:00:01 remaining)
Nmap scan report for 192.168.0.109 (192.168.0.109)
Host is up (0.0012s latency).
Not shown: 1011 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ ftp-syst: 200 451 553904992 192.168.0.104 255.255.255.255
|_ STAT: 200 451 553904992 192.168.0.104 255.255.255.255
|_ FTP server status: 200 150 148 192.168.0.104 255.255.255.255
|_   Connected to 192.168.0.108 192.168.0.102 255.255.255.255
|_   Logged in as ftp
|_   TYPE: ASCII
|_   No session bandwidth limit (300 bits), 44 byte
|_   Session timeout in seconds is 300
|_   Control connection is plain text (request)
|_   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:el: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-date: 2024-04-16T20:55:52+00:00; -1s from scanner time.
|_ ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=
|_ Not valid before: 2010-03-17T14:07:45
|_ Not valid after: 2010-04-16T14:07:45
|_ smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY
|_ sslv2:
|_   SSLv2 supported
|_   ciphers:
|_     SSL2_DES_64_CBC_WITH_MD5
|_     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_     SSL2_RC4_128_WITH_MD5
|_     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_     SSL2_RC2_128_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

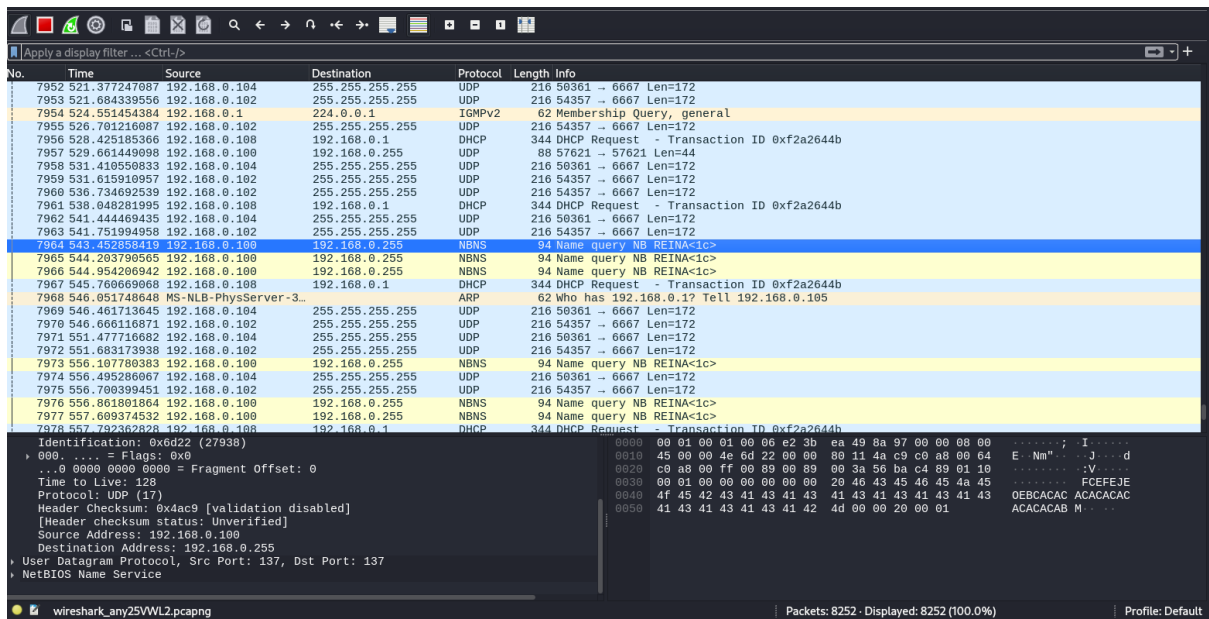
```

```

The Actions Edit View Help
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-title: Metasploitable2 - Linux
|_ http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
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 35000/udp   mountd
|_   100005 1,2,3 51916/tcp   mountd
|_   100021 1,3,4 42181/udp   nlockmgr
|_   100021 1,3,4 57196/tcp   nlockmgr
|_   100024 1 35844/tcp   status
|_   100024 1 42338/udp   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?
513/tcp    open  login         OpenBSD or Solaris rlogind
514/tcp    open  tcpwrapped
MAC Address: 08:00:27:B1:7C:1D (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:
|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ smb-os-discovery:
|_   OS: Unix (Samba 3.0.20-Debian)
|_   Computer name: metasploitable
|_   NetBIOS computer name:
|_   Domain name: localdomain
|_   FQDN: metasploitable.localdomain
|_   System time: 2024-04-16T16:55:43-04:00
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ clock-skew: mean: 1h19m58s, deviation: 2h18m34s, median: -1s
|_ smb-security-mode:
|_   account_used: guest
|_   authentication_level: user
|_   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)

```



## SWITCH -A

Con la scansione con lo switch **-A** fornisce più informazioni sul target.

Rileva le versioni dei servizi in esecuzione sulle porte aperte.

Rileva il sistema operativo e l'hardware del target.

Esegue degli script di Nmap Scripting Engine per avere informazioni su vulnerabilità potenzialmente note.

Esegue il tracciamento dei pacchetti verso il target per determinarne il percorso.

Comando:

```
sudo nmap -A -p 1-1023 [Indirizzo IP]
```

```

└─$ sudo nmap -sT -p 1-1023 192.168.0.109
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-16 16:51 EDT
Nmap scan report for 192.168.0.109 (192.168.0.109)
Host is up (0.0026s latency).
Not shown: 1011 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:B1:7C:1D (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds

```

No.	Time	Source	Destination	Protocol	Length	Info
10	5.784158946	192.168.0.108	192.168.0.109	TCP	76	45966 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1466302670 TSecr=0 WS=128
11	5.784460585	192.168.0.108	192.168.0.109	TCP	76	59798 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1466302671 TSecr=0 WS=128
12	5.784885718	192.168.0.109	192.168.0.108	TCP	62	443 → 45966 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
13	5.784885849	192.168.0.109	192.168.0.108	TCP	62	110 → 59798 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
14	5.785232915	192.168.0.108	192.168.0.109	TCP	76	59632 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1466302671 TSecr=0 WS=128
15	5.785498778	192.168.0.108	192.168.0.109	TCP	76	58034 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1466302672 TSecr=0 WS=128
16	5.785924858	192.168.0.109	192.168.0.108	TCP	62	143 → 59632 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17	5.785924992	192.168.0.109	192.168.0.108	TCP	62	113 → 58034 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
18	5.786266671	192.168.0.108	192.168.0.109	TCP	76	52238 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1466302672 TSecr=0 WS=128
19	5.786678339	192.168.0.108	192.168.0.109	TCP	76	45872 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1466302673 TSecr=0 WS=128
20	5.786992232	192.168.0.109	192.168.0.108	TCP	76	25 → 52238 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1466302673 TSecr=1466..
21	5.786993254	192.168.0.108	192.168.0.109	TCP	68	52238 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1466302673 TSecr=661546
22	5.787848315	192.168.0.109	192.168.0.108	TCP	62	587 → 45872 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	5.787944353	192.168.0.108	192.168.0.109	TCP	76	46594 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1466302674 TSecr=0 WS=128
24	5.788249910	192.168.0.108	192.168.0.109	TCP	76	45532 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1466302674 TSecr=0 WS=128
25	5.788457113	192.168.0.109	192.168.0.108	TCP	76	445 → 46594 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=661546 TSecr=146..
26	5.788465295	192.168.0.108	192.168.0.109	TCP	68	46594 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1466302675 TSecr=661546
27	5.788601926	192.168.0.108	192.168.0.109	TCP	76	48972 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1466302675 TSecr=0 WS=128
28	5.788813185	192.168.0.109	192.168.0.108	TCP	62	554 → 45532 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29	5.789102436	192.168.0.109	192.168.0.108	TCP	76	80 → 48972 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=661546 TSecr=1466..
30	5.789110475	192.168.0.108	192.168.0.109	TCP	68	48972 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1466302675 TSecr=661546
31	5.789480409	192.168.0.108	192.168.0.109	TCP	76	55078 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1466302676 TSecr=0 WS=128
32	5.789931704	192.168.0.109	192.168.0.108	TCP	62	993 → 55078 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	5.710048043	192.168.0.108	192.168.0.109	TCP	68	52238 → 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1466302676 TSecr=661546
34	5.710312339	192.168.0.108	192.168.0.109	TCP	68	46594 → 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1466302677 TSecr=661546
35	5.710605368	192.168.0.108	192.168.0.109	TCP	68	48972 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1466302677 TSecr=661546

Frame 12: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface ar  
Linux cooked capture v1  
Internet Protocol Version 4, Src: 192.168.0.109, Dst: 192.168.0.108  
Transmission Control Protocol, Src Port: 443, Dst Port: 45966, Seq: 1, Ack: 1, Len: 0  
Source Port: 443  
Destination Port: 45966  
[Stream index: 0]  
[Conversation completeness: Incomplete (37)]  
[TCP Segment Len: 0]  
Sequence Number: 1 (relative sequence number)  
Sequence Number (raw): 0  
Next Sequence Number: 1 (relative sequence number)

0000 00 00 00 01 00 06 08 00 27 b1 76 10 00 00 00 00  
0010 45 00 00 28 00 00 40 00 40 06 b8 a6 c9 a8 00 6d E: ( . @ @ . . . m  
0020 c0 a8 00 6c 01 bb b3 8e 00 00 00 00 86 c0 4c 05 .: L . . . . . L .  
0030 50 14 00 00 a5 97 00 00 00 00 00 00 00 00 00 P: . . . . .

## TCP

Con la scansione TCP si posso identificare le porte aperte su un Host di rete.

Mappa le reti per determinare quali servizi sono in esecuzione su quali porte

Identifica potenziali punti di ingresso vulnerabili su una rete o un sistema.

Crea un elenco delle risorse di rete, server e dispositivi e i servizi che offrono.

Rileva la versione dei servizi in esecuzione.

Identifica il sistema operativo e l'hardware.

Comando:

`sudo nmap -sT -p 1-1023 [indirizzo ip]`

```
(kali@kali)-[~]
$ sudo nmap -sS -p 1-1023 192.168.0.109
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-16 16:53 EDT
Nmap scan report for 192.168.0.109 (192.168.0.109)
Host is up (0.00043s latency).
Not shown: 1011 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:B1:7C:1D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.76 seconds
```

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
157	5.744543146	192.168.0.109	192.168.0.108	TCP	62	708 → 33556 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
158	5.744854246	192.168.0.109	192.168.0.108	TCP	62	120 → 51878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
159	5.744950529	192.168.0.108	192.168.0.109	TCP	76	40118 → 413 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1466302711 TSecr=0 WS=128
160	5.745214634	192.168.0.108	192.168.0.109	TCP	76	57070 → 536 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1466302711 TSecr=0 WS=128
161	5.745470314	192.168.0.108	192.168.0.109	TCP	76	56816 → 1014 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1466302712 TSecr=0 WS=128
162	5.745689765	192.168.0.109	192.168.0.108	TCP	62	413 → 40118 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
163	5.745791411	192.168.0.108	192.168.0.109	TCP	76	52652 → 992 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1466302712 TSecr=0 WS=128
164	5.746020052	192.168.0.109	192.168.0.108	TCP	62	536 → 57070 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
165	5.746337685	192.168.0.109	192.168.0.108	TCP	62	1014 → 56816 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
166	5.746357827	192.168.0.108	192.168.0.109	TCP	62	992 → 52652 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
167	5.746430401	192.168.0.109	192.168.0.108	TCP	76	43876 → 050 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1466302713 TSecr=0 WS=128
168	5.746845415	192.168.0.108	192.168.0.109	TCP	68	35726 → 512 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1466302713 TSecr=661548
169	5.747142073	192.168.0.109	192.168.0.108	TCP	62	059 → 43876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
170	5.747481022	192.168.0.108	192.168.0.109	TCP	76	55758 → 797 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1466302714 TSecr=0 WS=128
171	5.747796291	192.168.0.109	192.168.0.108	TCP	62	797 → 55758 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
172	5.747963278	192.168.0.108	192.168.0.109	TCP	76	94516 → 415 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1466302714 TSecr=0 WS=128
173	5.748271671	192.168.0.108	192.168.0.109	TCP	76	34784 → 317 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1466302714 TSecr=0 WS=128
174	5.748782333	192.168.0.109	192.168.0.108	TCP	62	415 → 54516 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
175	5.748783860	192.168.0.109	192.168.0.108	TCP	62	317 → 34784 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
176	5.749760415	192.168.0.108	192.168.0.109	TCP	76	52996 → 867 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1466302716 TSecr=0 WS=128
177	5.750030834	192.168.0.108	192.168.0.109	TCP	76	33888 → 672 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1466302716 TSecr=0 WS=128
178	5.750290222	192.168.0.109	192.168.0.108	TCP	62	867 → 52996 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
179	5.750536323	192.168.0.109	192.168.0.108	TCP	62	672 → 33888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
180	5.750630139	192.168.0.108	192.168.0.109	TCP	76	55554 → 566 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1466302717 TSecr=0 WS=128
181	5.750898526	192.168.0.108	192.168.0.109	TCP	76	51772 → 311 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1466302717 TSecr=0 WS=128
182	5.751108118	192.168.0.109	192.168.0.108	TCP	62	566 → 55554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
183	5.751519008	192.168.0.109	192.168.0.108	TCP	62	311 → 51772 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Frame 168: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface v1

Linux cooked capture v1

Internet Protocol Version 4, Src: 192.168.0.108, Dst: 192.168.0.109

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 52

Identification: 0x6b7e (27518)

010. .... = Flags: 0x2, Don't fragment

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 64

Protocol: TCP (6)

0000 00 0a 00 01 00 00 00 00 27 5d 4b 00 00 00 00 E.....V]K....

0010 45 00 00 34 6b 7e 40 00 40 00 4d 1c c0 a8 00 6c E..4k-@. @M....l

0020 c0 a8 00 6d 8b 8e 02 00 08 7a 29 29 cd 4e 9b 1e ...m.....z)).N..

0030 80 14 01 f6 82 50 00 00 01 01 08 0a 57 66 00 f9 .....P.....Wf..

0040 00 0a 18 2c ....

Frame (frame), 68 bytesPackets: 8201 · Displayed: 8201 (100.0%)Profile: Default

## SYN

Con la scansione SYN si possono identificare rapidamente le porte aperte su un host di rete senza completare l’handshake TCP. E’ una scansione più difficile da rilevare dai sistemi di rilevamento intrusioni o firewall.

La scansione SYN è più veloce rispetto ad altre scansioni perchè non stabilisce una connessione completa.

Non completando l’handshake TCP è meno probabile che venga registrata nei log dei server.

Fornisce risultati affidabili sullo stato delle porte.

Se riceve un pacchetto SYN/ACK significa che la porta è aperta.

Se riceve un pacchetto RST (reset) la porta è chiusa.

Se non riceve risposta la porta potrebbe essere protetta da un firewall.

## Comando:

```
sudo nmap -sS -p 1-1023 [indirizzo ip]
```

## Scansione della domotica collegata:

8358	1169.5717532...	TuyaSmart_c5:8b:ce	ARP	62	Who has 192.168.0.1? Tell 192.168.0.104
8359	1171.0154964...	192.168.0.108	DHCP	344	DHCP Request - Transaction ID 0xf2a2644b
8360	1172.6429885...	192.168.0.104	UDP	216	50361 → 6667 Len=172
8361	1172.8478024...	192.168.0.102	UDP	216	54357 → 6667 Len=172
8362	1177.7503155...	192.168.0.100	UDP	88	57621 → 57621 Len=44
8363	1177.8645892...	192.168.0.102	UDP	216	54357 → 6667 Len=172
8364	1182.8816822...	192.168.0.102	UDP	216	54357 → 6667 Len=172
8365	1187.4280943...	192.168.0.108	DHCP	344	DHCP Request - Transaction ID 0xf2a2644b
8366	1187.6937041...	192.168.0.104	UDP	216	50361 → 6667 Len=172
8367	1188.0003714...	192.168.0.102	UDP	216	54357 → 6667 Len=172
8368	1191.5065237...	AmazonTechno_e6:db:80	ARP	62	Who has 192.168.0.100? Tell 192.168.0.101

## Rilevamento nome utente dell’hardware:

8221	944.650790502	TpLinkTechno_f4:ce:...	ARP	62	Who has 192.168.0.100? Tell 192.168.0.1
8222	944.847830292	192.168.0.100	NBNS	94	Name query NB REINA<1c>
8223	945.599561923	192.168.0.100	NBNS	94	Name query NB REINA<1c>
8224	946.350073772	192.168.0.100	NBNS	94	Name query NB REINA<1c>

## Scansione macchina virtuale:

8171	867.12948573	192.168.0.104	UDP	216	50361 → 6667 Len=172
8172	867.435719949	192.168.0.102	UDP	216	54357 → 6667 Len=172
8173	867.82428696	192.168.0.109	BROWSER	288	Local Master Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Se...
8174	867.824729869	192.168.0.109	BROWSER	259	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum

## Scansione hardware e router:

8344	1147.3542410...	MS-NLB-PhysServer-32_04:80:c3:e3:65	ARP	62	Who has 192.168.0.1? Tell 192.168.0.105
8345	1147.39380558...	PCSystemtec_56:5d:4b	ARP	44	Who has 192.168.0.1? Tell 192.168.0.108
8346	1147.3959964...	TpLinkTechno_f4:ce:10	ARP	62	192.168.0.1 is at 74:da:88:f4:ce:10