

W11D4 – Nicholas Di Angelo -

Quando due dispositivi comunicano tramite il protocollo TCP/IP, si svolge un processo di "handshake" per stabilire una connessione affidabile tra mittente e destinatario. Questo handshake è composto da tre passaggi fondamentali: SYN, SYN/ACK e ACK.

1. **SYN (Synchronization):**

- Il mittente invia un segmento di richiesta di sincronizzazione (SYN) al destinatario per avviare la connessione.
- Questo segmento include un numero di sequenza iniziale (ISN) generato casualmente dal mittente, che serve a numerare i byte dei dati trasmessi durante la connessione.

2. **SYN/ACK (Synchronization/Acknowledgment):**

- Il destinatario riceve il segmento SYN e risponde inviando un segmento di conferma di sincronizzazione e accettazione (SYN/ACK) al mittente.
- Il segmento SYN/ACK include il numero di sequenza iniziale del destinatario (ISN) e conferma l'accettazione della connessione.

3. **ACK (Acknowledgment):**

- Infine, il mittente riceve il segmento SYN/ACK e risponde inviando un segmento di conferma (ACK) al destinatario.
- Questo segmento conferma che il mittente ha ricevuto correttamente il segmento di conferma di sincronizzazione del destinatario.

Una volta completato questo processo di handshake, la connessione è stabilita e i dati possono essere trasmessi in modo affidabile tra il mittente e il destinatario. La numerazione dei byte e la gestione dei pacchetti consentono di garantire l'affidabilità e l'integrità della trasmissione dei dati su Internet.

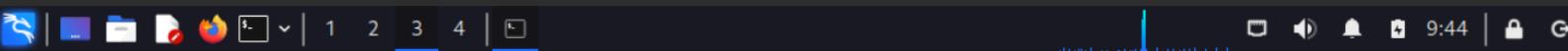
Ecco una relazione sulle diverse modalità di scansione utilizzate con Nmap su un indirizzo IP specifico:

Scansione completa con SYN scan (-sS):

 nmap -sS ip_address

Questa modalità di scansione utilizza il metodo SYN per individuare le porte aperte sulla macchina di destinazione.
È una scansione approfondita che fornisce informazioni dettagliate sulle porte aperte e chiuse.

kali linux 1 [Running]



```
(root@kali)-[~]
# nmap -sS 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 09:44 CEST
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.00047s 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: 08:00:27:24:01:F5 (Oracle VirtualBox virtual NIC)

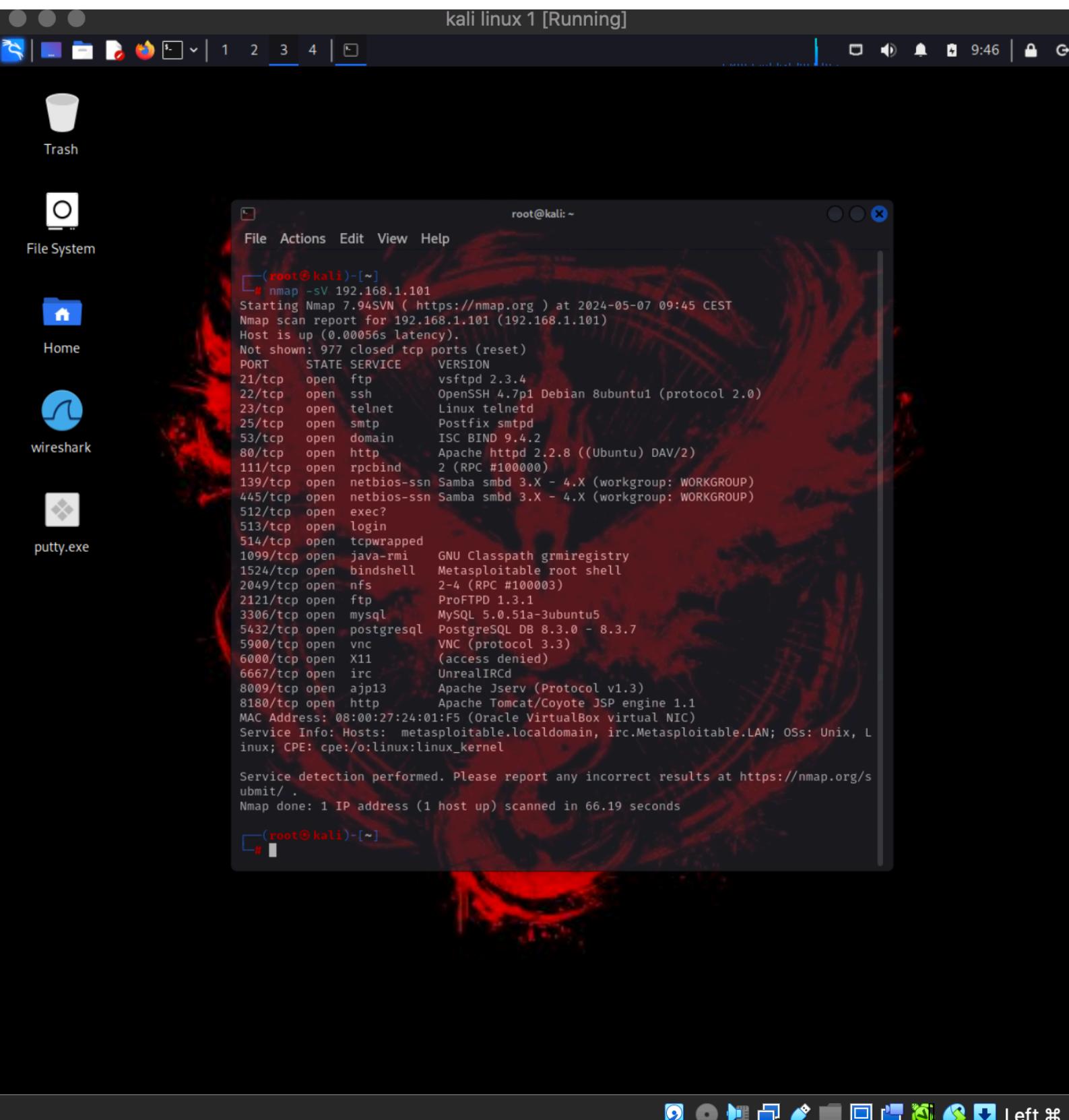
Nmap done: 1 IP address (1 host up) scanned in 0.64 seconds

(root@kali)-[~]
#
```

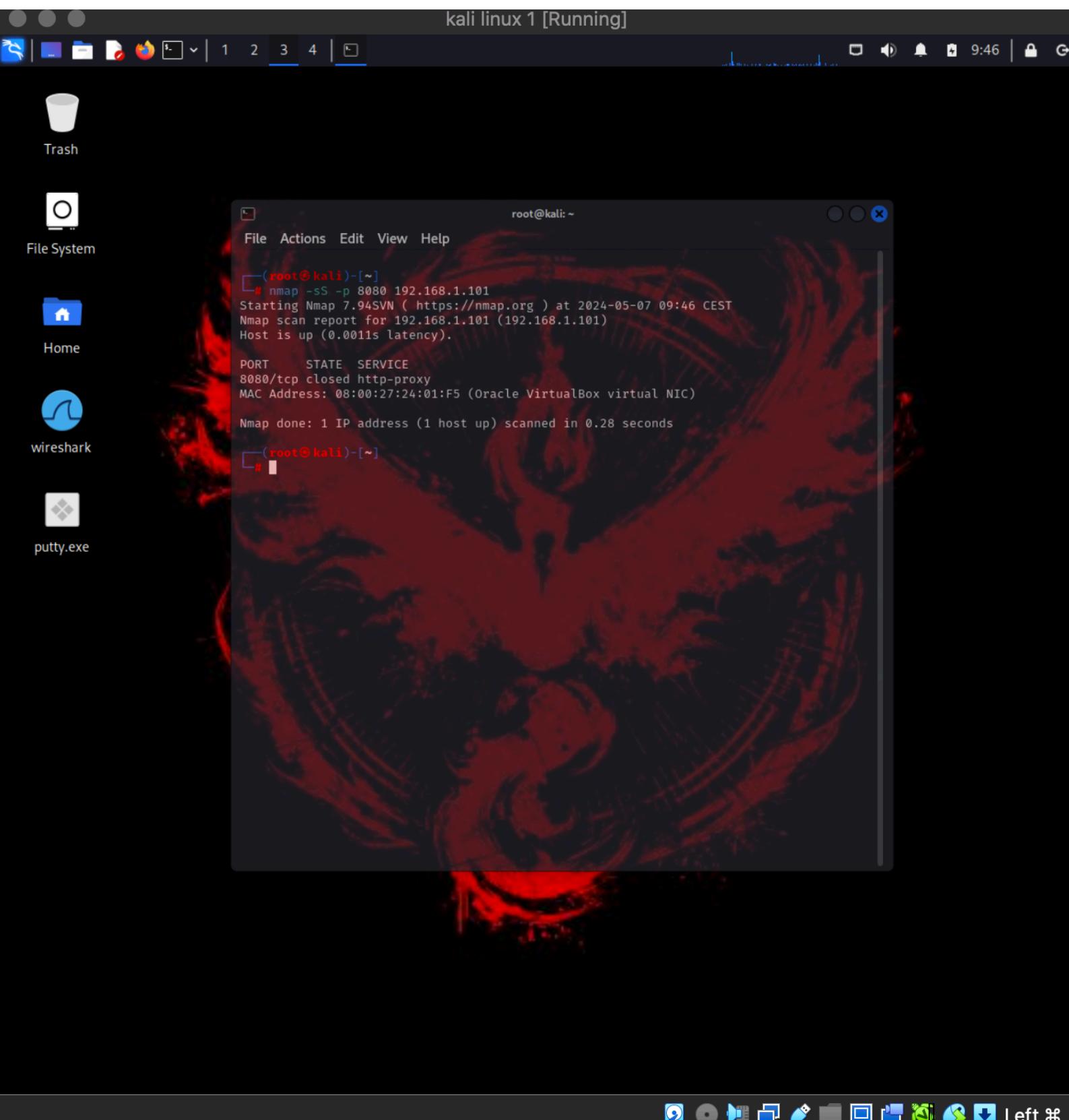


Scansione completa con rilevamento versione e output su file (-sV -oN):
nmap -sV -oN file.txt ip_address

Questa scansione fornisce informazioni sulle versioni dei servizi in esecuzione sulle porte aperte e registra l'output su un file di testo specificato.



Scansione su tutte le porte con SYN scan (-sS -p-):
nmap -sS -p- ip_address
Questo comando esegue una scansione SYN su tutte le porte della macchina di destinazione.

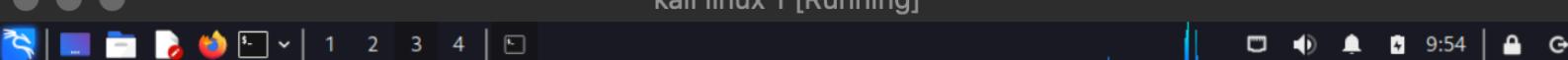


Scansione del sistema operativo (-O):

nmap -O ip_address

Questa scansione tenta di determinare il sistema operativo in esecuzione sulla macchina di destinazione analizzando le risposte ai pacchetti inviati.

kali linux 1 [Running]



Trash



File System



Home



wireshark



putty.exe



Scansione delle 100 porte comuni (scansione rapida) (-F):
nmap -F ip_address

Questa scansione si concentra sulle 100 porte comuni, fornendo un'analisi più rapida delle porte aperte sulla macchina di destinazione.

kali linux 1 [Running]

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "kali linux 1 [Running]". The terminal content displays the output of an Nmap scan:

```
(root@kali)-[~]
# nmap -F 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 09:55 CEST
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.00052s latency).
Not shown: 82 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
513/tcp   open  login
514/tcp   open  shell
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
8009/tcp  open  ajp13
MAC Address: 08:00:27:24:01:F5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

The desktop interface includes a dock with icons for various tools like File System, Home, Wireshark, and Putty.exe. The taskbar at the bottom also has several icons.

Scansione tramite ARP (-PR):

nmap -PR ip_address

Questa modalità di scansione utilizza ARP per individuare i dispositivi presenti nella rete locale.

kali linux 1 [Running]

```
Scansione tramite ARP (-PR):
nmap -PR ip_address
Questa modalità di scansione utilizza ARP per individuare i dispositivi presenti nella rete locale.

kali linux 1 [Running]
Trash
File System
Home
wireshark
putty.exe

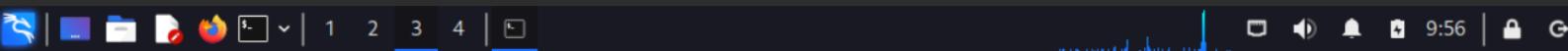
root@kali:[~]
# nmap -PR 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 09:55 CEST
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.00057s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    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: 08:00:27:24:01:F5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds

root@kali:[~]
#
```



kali linux 1 [Running]



Trash



File System



Home



wireshark



putty.exe

```
(root@kali)-[~]
└─# nmap -PN 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 09:56 CEST
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.00046s 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: 08:00:27:24:01:F5 (Oracle VirtualBox virtual NIC)

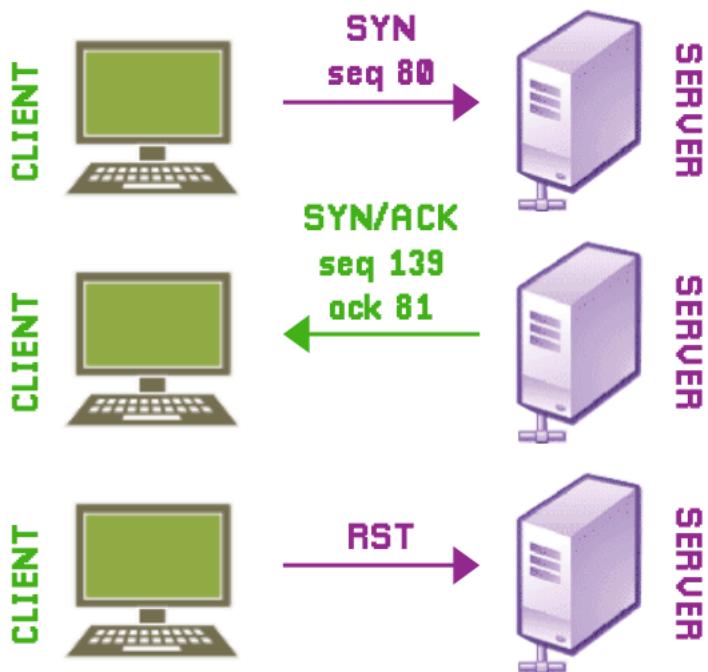
Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds

└─#
```

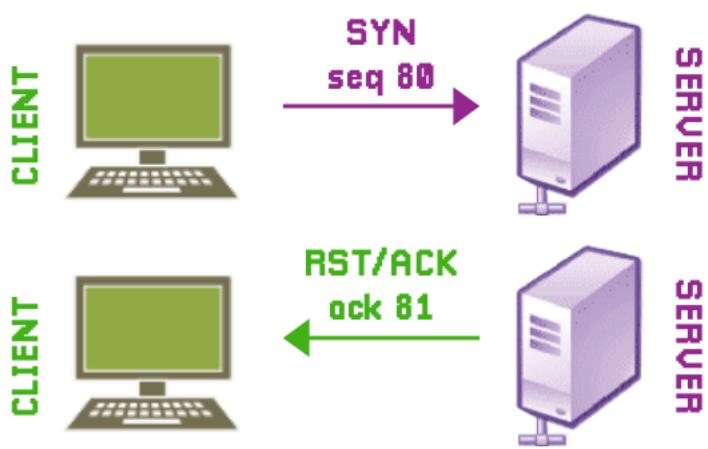


#SCANSIONE DI TIPO SYN (STEALTH) SCAN: `nmap -sS <IP>`
NASCOSTO E POCO INVASIVO, POICHÉ NON COMPLETA MAI LE CONNESSIONI TCP (CASO DI PORTA APERTA / CHIUSA)

PORTA APERTA:
THREE WAY HANDSHAKE
NON COMPLETATO

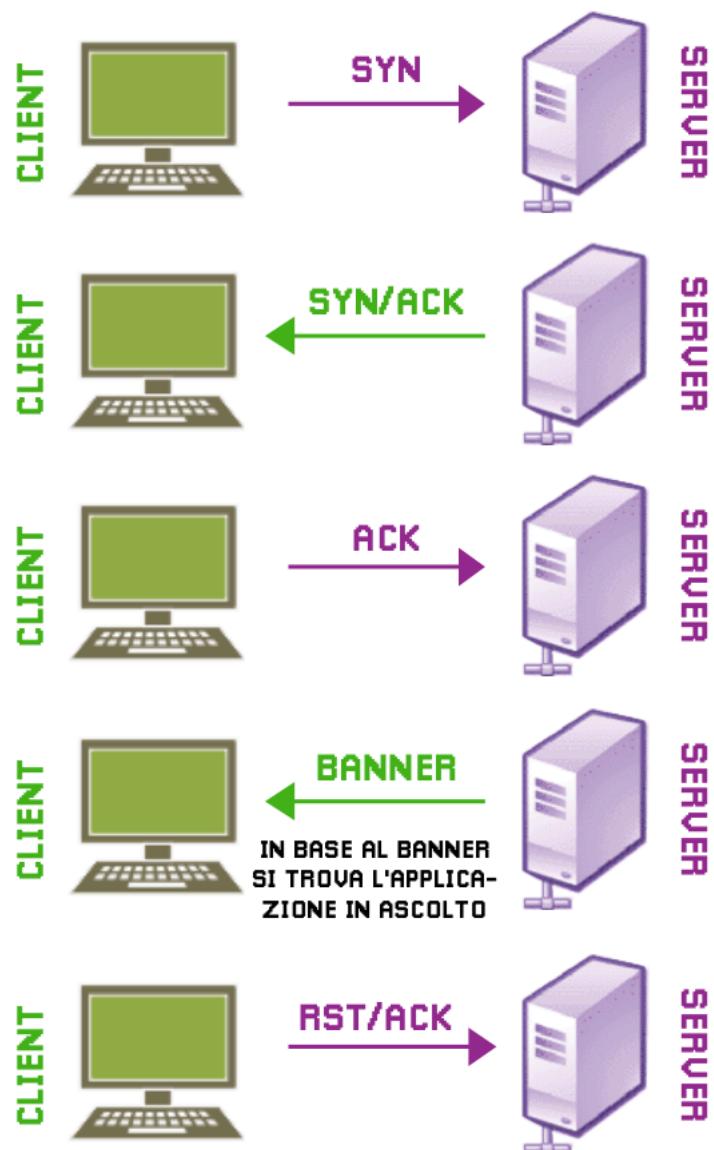


PORTA CHIUSA:
THREE WAY HANDSHAKE
NON COMPLETATO



#SCANSIONE DI TIPO VERSIONE SERVIZI: `nmap -sV <IP>`

SCANSIONE DI TIPO TCP, ABILITA IL VERSION DETECTION COSÌ DA RICONOSCERE VERSIONE E NOME DEL SERVIZIO RPC. È RUMOROSA E GENERA MOLTO TRAFFICO DI RETE



#SCANSIONE DI TIPO UDP: `nmap -sU <IP>`

PIÙ LENTO E PIÙ DIFFICOLTOSO DI QUELLO SU TCP, FUNZIONA INVIANDO PACCHETTI UDP AD OGNI PORTA DI DESTINAZIONE (ALCUNE PORTE COMUNI: 53 E 161)

