

S11L5

## INDICE

-esplorazione comandi powershell (1,2,3,4)

-utilizzo wireshark per esaminare traffico http e https (4,5,6,7)

-bonus 1 (7,8,9)

## ESPLORAZIONE COMANDI POWERSHELL

Apriamo il menu start e apriamo il windows powershell

Come primo comando vediamo dir

Il comando dir visualizza l'elenco dei file e delle cartelle all'interno di una directory specificata (o della directory corrente se non viene indicata alcuna directory). Può essere usato con varie opzioni per personalizzare la visualizzazione.

```
Mode                LastWriteTime         Length Name
-----
d-----          10/12/2024      15:25             .VirtualBox
d-r-----        29/07/2024      19:29             3D Objects
d-r-----        18/10/2024      10:32             Contacts
d-r-----        10/12/2024      15:34             Desktop
d-r-----        30/10/2024      20:22             Documents
d-r-----        12/12/2024      14:02             Downloads
d-r-----        18/10/2024      10:32             Favorites
d-r-----        18/10/2024      10:32             Links
d-r-----        18/10/2024      10:32             Music
dar-----        30/09/2024      12:29             OneDrive
d-r-----        29/10/2024      18:23             Pictures
d-r-----        18/10/2024      10:32             Saved Games
d-r-----        18/10/2024      10:32             Searches
d-r-----        15/11/2024      13:54             Videos
d-----         10/12/2024      15:23             VirtualBox VMs

PS C:\Users\mirko> cd desktop
PS C:\Users\mirko\desktop> cd..
PS C:\Users\mirko> Get-Alias dir

CommandType      Name
-----
Alias             dir -> Get-ChildItem
```

In questo screen vediamo altri comandi ad esempio cd che ci permette di cambiare directory oppure get alias dir, getchilditem

In PowerShell, **dir** è effettivamente un alias per il comando **Get-ChildItem**. Quindi, quando usi **dir** in PowerShell, sta eseguendo il comando **Get-ChildItem**, che elenca i file e le cartelle nella directory corrente o in quella specificata.

Il prossimo comando che andiamo a vedere è netstat -r

Il comando **netstat -r** serve per visualizzare la **tabella di routing** del sistema, che mostra come i pacchetti di rete vengono indirizzati tra le diverse reti e sottoreti a livello di sistema operativo.

La **tabella di routing** contiene informazioni cruciali per il funzionamento della rete, come la destinazione, la rete di gateway, l'interfaccia di rete utilizzata e altre informazioni relative al percorso seguito dai pacchetti.

```
PS C:\Users\mirko> netstat -r
=====
Elenco interfacce
12...0a 00 27 00 00 0c .....VirtualBox Host-Only Ethernet Adapter
15...74 56 3c d9 dc 73 .....Realtek Gaming 2.5GbE Family Controller
1.....Software Loopback Interface 1
=====

IPv4 Tabella route
=====
Route attive:
      Indirizzo rete      Mask      Gateway      Interfaccia  Metrica
      0.0.0.0      0.0.0.0      192.168.178.1      192.168.178.43      35
      127.0.0.0      255.0.0.0      On-link      127.0.0.1      331
      127.0.0.1      255.255.255.255      On-link      127.0.0.1      331
127.255.255.255      255.255.255.255      On-link      127.0.0.1      331
      192.168.56.0      255.255.255.0      On-link      192.168.56.1      281
      192.168.56.1      255.255.255.255      On-link      192.168.56.1      281
      192.168.56.255      255.255.255.255      On-link      192.168.56.1      281
      192.168.178.0      255.255.255.0      On-link      192.168.178.43      291
      192.168.178.43      255.255.255.255      On-link      192.168.178.43      291
      192.168.178.255      255.255.255.255      On-link      192.168.178.43      291
      224.0.0.0      240.0.0.0      On-link      127.0.0.1      331
      224.0.0.0      240.0.0.0      On-link      192.168.56.1      281
      224.0.0.0      240.0.0.0      On-link      192.168.178.43      291
      255.255.255.255      255.255.255.255      On-link      127.0.0.1      331
      255.255.255.255      255.255.255.255      On-link      192.168.56.1      281
      255.255.255.255      255.255.255.255      On-link      192.168.178.43      291
=====
Route permanenti:
```

Per il prossimo comando `netstat -abno` dobbiamo aprire il powershell come amministratore. Il comando `netstat -abno` è una variante avanzata di `netstat`, utilizzato per ottenere informazioni dettagliate sulle connessioni di rete attive e sui processi associati a quelle connessioni in un sistema Windows.

**-a:** Visualizza **tutte** le connessioni e le porte di ascolto (inclusi i collegamenti in entrata e in uscita). Mostra sia le connessioni TCP che UDP.

**-b:** Mostra il **nome del programma** (processo) associato a ciascuna connessione o porta di ascolto. Questo aiuta a identificare quale applicazione o servizio sta utilizzando una specifica connessione di rete.

**-n:** Visualizza gli **indirizzi IP e le porte** numerici anziché i nomi di dominio e i nomi di servizio. Questo è utile per ottenere una visualizzazione più rapida dei dettagli di rete, senza risolvere i nomi.

**-o:** Mostra l'**ID del processo (PID)** che ha aperto la connessione o la porta. Questo consente di associare la connessione di rete a un particolare processo in esecuzione nel sistema

```

Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.

Installa la versione più recente di PowerShell per nuove funzionalità e miglioramenti. https://aka.ms/PSWindows

PS C:\WINDOWS\system32> netstat -abno

Connessioni attive

Proto  Indirizzo locale      Indirizzo esterno      Stato      PID
TCP    0.0.0.0:135            0.0.0.0:0              LISTENING  1280
RpcSs
[svchost.exe]
TCP    0.0.0.0:445            0.0.0.0:0              LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING  7368
CDPSvc
[svchost.exe]
TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING  16668
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:27036          0.0.0.0:0              LISTENING  12312
[steam.exe]
TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING  812
[lsass.exe]
TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING  972
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING  848
Schedule
[svchost.exe]
TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING  2552
EventLog
[svchost.exe]
TCP    0.0.0.0:49672          0.0.0.0:0              LISTENING  3936
[spoolsv.exe]
TCP    0.0.0.0:49678          0.0.0.0:0              LISTENING  796
Impossibile ottenere informazioni sulla proprietà
TCP    127.0.0.1:1001         0.0.0.0:0              LISTENING  4256
[EWCSservice.exe]
TCP    127.0.0.1:6463         0.0.0.0:0              LISTENING  8428
[Discord.exe]
TCP    127.0.0.1:6463         127.0.0.1:60509        ESTABLISHED 8428
[Discord.exe]
TCP    127.0.0.1:9010         0.0.0.0:0              LISTENING  10048
[lghub_agent.exe]
TCP    127.0.0.1:9010         127.0.0.1:60477        ESTABLISHED 10048
[lghub_agent.exe]
TCP    127.0.0.1:9080         0.0.0.0:0              LISTENING  10048
[lghub_agent.exe]
TCP    127.0.0.1:9100         0.0.0.0:0              LISTENING  4320
[lghub_updater.exe]
TCP    127.0.0.1:9100         127.0.0.1:60505        ESTABLISHED 4320
[lghub_updater.exe]
TCP    127.0.0.1:9180         0.0.0.0:0              LISTENING  4320
[lghub_updater.exe]
TCP    127.0.0.1:27060        0.0.0.0:0              LISTENING  12312
[steam.exe]
TCP    127.0.0.1:45654        0.0.0.0:0              LISTENING  10048
[lghub_agent.exe]
TCP    127.0.0.1:60317        0.0.0.0:0              LISTENING  13156
[RiotClientServices.exe]
TCP    127.0.0.1:60477        127.0.0.1:9010        ESTABLISHED 15796
[lghub_system_tray.exe]
TCP    127.0.0.1:60505        127.0.0.1:9100        ESTABLISHED 10048

```

Successivamente apriamo il task manager andiamo nella sezione dettagli e inseriamo un PID dall'elenco in base alle nostre preferenze in questo caso io ho scelto il primo 1280.

Il **PID** (Process IDentifier) è un identificatore univoco assegnato dal sistema operativo a ogni processo in esecuzione. Ogni programma o processo che viene avviato su un sistema (che sia un'applicazione, un servizio di sistema o una parte di un'applicazione più grande) riceve un numero PID, che serve a distinguere quel processo da altri.

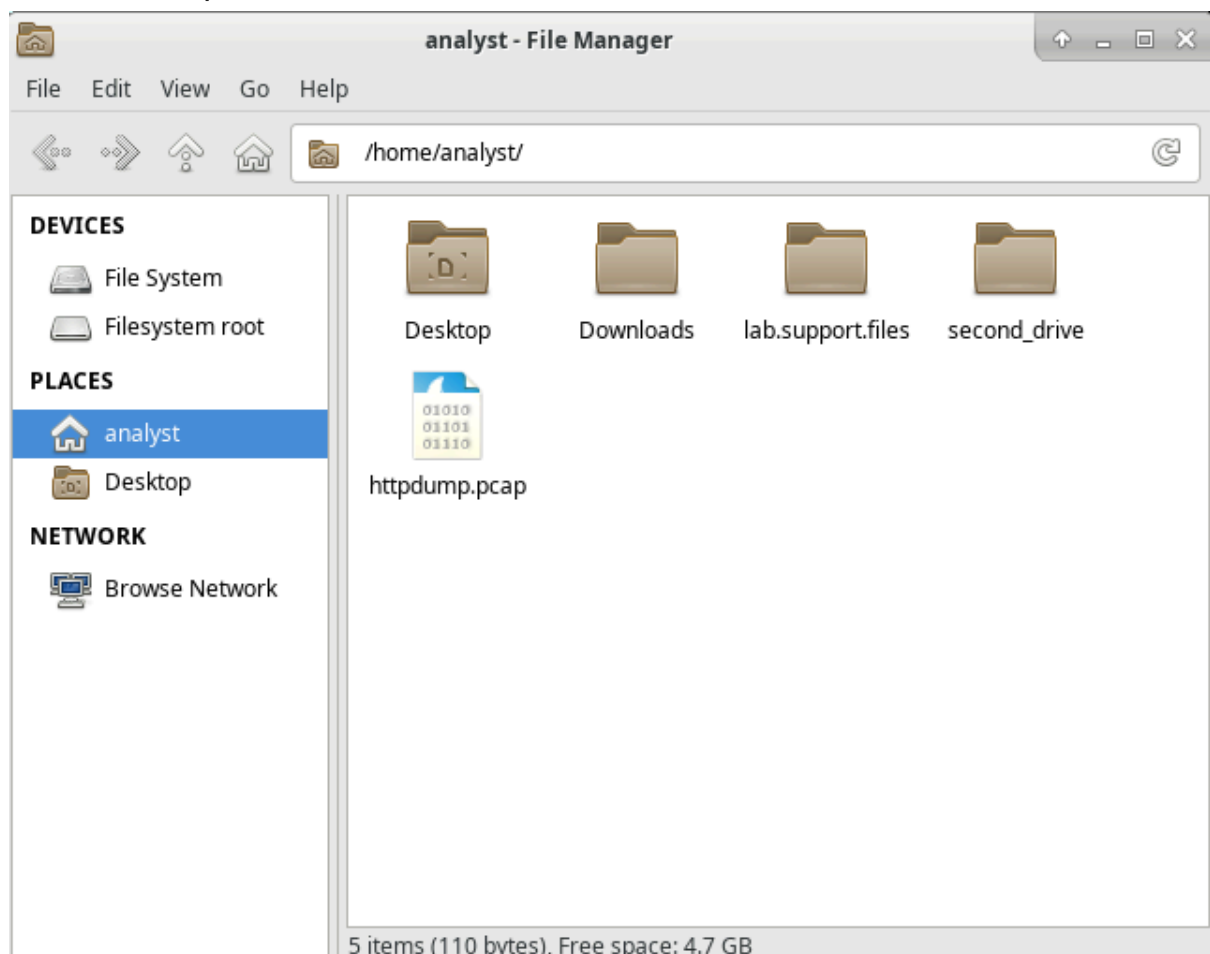
Il PID permette al sistema operativo e agli strumenti di monitoraggio di:

1. **Identificare** in modo univoco un processo.
2. **Monitorare** lo stato e le risorse consumate dal processo (CPU, memoria, ecc.).
3. **Gestire** i processi (terminare, sospendere, inviare segnali, ecc.).



Il TCP dump precedentemente eseguito ci ha dato in output un file denominato **httdump.pcap**.

Clicchiamo apri con e selezioniamo wireshark.



The screenshot shows the Wireshark interface with the 'httpdump.pcap' file loaded. The packet list pane displays a table of captured packets. The selected packet is number 150, which is an HTTP POST request to '/doLogin'.

No.	Time	Source	Destination	Protocol	Length	Info
44	7.806931	10.0.2.15	65.61.137.117	HTTP	399	GET /bank/login.jsp HTTP/1.1
46	7.879473	65.61.137.117	10.0.2.15	HTTP	256	HTTP/1.1 302 Found
48	7.987694	10.0.2.15	65.61.137.117	HTTP	447	GET /login.jsp HTTP/1.1
54	8.062632	65.61.137.117	10.0.2.15	HTTP	3228	HTTP/1.1 200 OK (text/html)
81	8.276625	10.0.2.15	65.61.137.117	HTTP	409	GET /style.css HTTP/1.1
89	8.349119	65.61.137.117	10.0.2.15	HTTP	1532	HTTP/1.1 200 OK (text/css)
150	20.856396	10.0.2.15	65.61.137.117	HTTP	637	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
154	20.936367	65.61.137.117	10.0.2.15	HTTP	303	HTTP/1.1 302 Found
156	20.942993	10.0.2.15	65.61.137.117	HTTP	594	GET /bank/main.jsp HTTP/1.1
162	21.027105	65.61.137.117	10.0.2.15	HTTP	2326	HTTP/1.1 200 OK (text/html)

## CATTURA TRAFFICO HTTPS

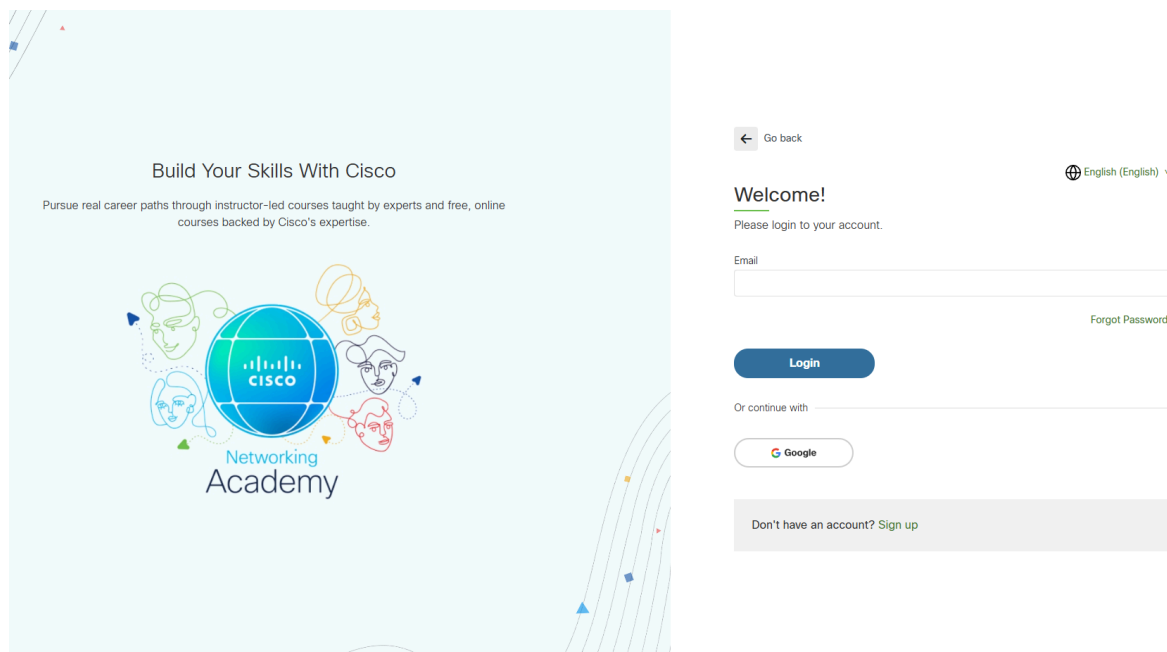
Fondamentalmente i passaggi sono gli stessi con solo qualche variazione nei comandi. Inseriamo il comando `sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap`



```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

    valid_lft 86296sec preferred_lft 86296sec
    inet6 fe80::a00:27ff:fe3c:a2d9/64 scope link
    valid_lft forever preferred_lft forever
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 b
ytes
^C1 packet captured
1 packet received by filter
0 packets dropped by kernel
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 b
ytes
^C975 packets captured
975 packets received by filter
0 packets dropped by kernel
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 b
ytes
^C1260 packets captured
1260 packets received by filter
0 packets dropped by kernel
[analyst@secOps ~]$
```

andiamo sul sito [www.netcad.com](http://www.netcad.com)



Come nella fase precedente troveremo un file chiamato httpsdump.pcap  
Apriamo con wireshark e troviamo come nel caso precedente questa  
schermata.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.15	104.16.248.249	TLSv1.2	110	Application Data
2	0.000044	10.0.2.15	104.16.248.249	TLSv1.2	133	Application Data
3	0.000383	104.16.248.249	10.0.2.15	TCP	60	443 → 52556 [ACK] Seq=1 Ack=57 Win=65535 Len=0
4	0.000383	104.16.248.249	10.0.2.15	TCP	60	443 → 52556 [ACK] Seq=1 Ack=136 Win=65535 Len=0
7	0.031225	104.16.248.249	10.0.2.15	TLSv1.2	286	Application Data, Application Data
8	0.031256	10.0.2.15	104.16.248.249	TCP	54	52556 → 443 [ACK] Seq=136 Ack=233 Win=63900 Len=0
15	0.169127	10.0.2.15	104.16.248.249	TLSv1.2	114	Application Data
16	0.169169	10.0.2.15	104.16.248.249	TLSv1.2	136	Application Data

## BONUS 1

### ESPLORAZIONE NMAP

-

apriamo il guida con il comando `man nmap`

**Nmap** (Network Mapper) è uno strumento open-source ampiamente utilizzato per l'analisi della rete e la sicurezza. È principalmente usato per **scansionare** le reti, identificare dispositivi connessi e raccogliere informazioni su di essi, come porte aperte, servizi in esecuzione, versioni di software e potenziali vulnerabilità. Nmap è uno degli strumenti di base per i professionisti della sicurezza informatica, amministratori di sistema e analisti di rete.

```
analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 04:41 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000027s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ -rw-r--r--  1 0      0          0 Mar 26  2018 ftp_test
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 127.0.0.1
|   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
|   At session startup, client count was 4
|   vsFTPD 3.0.3 - secure, fast, stable
|_ End of status
22/tcp    open  ssh      OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 b4:91:f9:f9:d6:79:25:86:44:c7:9e:f8:e0:e7:5b:bb (RSA)
|   256 06:12:75:fe:b3:89:29:4f:8d:f3:9e:9a:d7:c6:03:52 (ECDSA)
|_  256 34:5d:f2:d3:5b:9f:b4:b6:08:96:a7:30:52:8c:96:06 (ED25519)
Service Info: Host: Welcome

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.50 seconds
```

Come mostrato nell'immagine con il comando `nmap -A -T4 localhost`

**Scansiona il computer locale (localhost)** per raccogliere informazioni dettagliate.

**Rileva il sistema operativo e la versione dei servizi** in esecuzione sul dispositivo.

Esegue una **scansione completa delle porte aperte**, determinando se ci sono vulnerabilità note utilizzando gli **script di Nmap**.

**Traceroute:** Mostra il percorso che i pacchetti di rete percorrono per arrivare al tuo computer.

Utilizza un **template di scansione rapida (T4)** per eseguire il tutto in modo relativamente veloce.

```
[analyst@secOps ~]$ nmap -A -iL scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 04:42 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.22s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|_ 2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|_ 256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_ 256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Go ahead and ScanMe!
135/tcp    filtered mspc
139/tcp    filtered netbios-ssn
445/tcp    filtered microsoft-ds
9929/tcp   open  nping-echo   Nping echo
31337/tcp  open  tcpwrapped
32781/tcp  filtered unknown
Service Info: OS: 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 34.62 seconds
```

successivamente scannerizziamo la nostra network con il comando `nmap -A T4` seguito dal nostro indirizzo ip per ottenere tutte le informazioni

Quando esegui questo comando, Nmap fornisce le seguenti informazioni dettagliate:

### 1. Porte aperte:

- Verranno scansionate tutte le porte comuni e verrà visualizzato un elenco delle porte aperte sul dispositivo target (ad esempio, HTTP sulla porta 80, HTTPS sulla porta 443, FTP sulla porta 21, ecc.).

### 2. Servizi e versioni:

- Nmap cercherà di determinare **quali servizi** sono in esecuzione su ciascuna porta aperta e **le versioni specifiche** di quei servizi. Ad esempio, se sulla porta 80 è in esecuzione un server web, Nmap cercherà di identificare la versione esatta (ad esempio Apache 2.4.29).



### 3. Sistema operativo:

- **Rilevazione del sistema operativo:** Nmap cercherà di determinare quale sistema operativo è in uso sul dispositivo target (Windows, Linux, macOS, ecc.) e la versione di tale sistema operativo.

### 4. Traceroute:

- Verrà eseguito un **traceroute** per determinare il percorso che i pacchetti di rete percorrono per arrivare al dispositivo target, inclusi i router intermedi. Questo può aiutare a comprendere come i pacchetti viaggiano nella rete.

### 5. Vulnerabilità e configurazioni di sicurezza:

- Se sono attivi, gli script di **Nmap Scripting Engine (NSE)** possono cercare vulnerabilità specifiche o errori di configurazione sui dispositivi target. Questi script possono rivelare informazioni come:
  - Vulnerabilità conosciute (ad esempio, una versione di un software con una vulnerabilità critica).
  - Configurazioni errate (come la presenza di porte aperte inutili o servizi non sicuri).

```
[analyst@secOps ~]$ nmap -A -iL scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 04:42 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.22s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256  96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256  33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Go ahead and ScanMe!
135/tcp    filtered mspc
139/tcp    filtered netbios-ssn
445/tcp    filtered microsoft-ds
9929/tcp   open  nping-echo   Nping echo
31337/tcp  open  tcpwrapped
32781/tcp  filtered unknown
Service Info: OS: 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 34.62 seconds
```

L'ultimo step è quello di eseguire la scansione del sito scanme-nmap.org e otteniamo le medesime informazioni riguardo le porte aperte, l'OS del web server e le informazioni precedentemente citate.