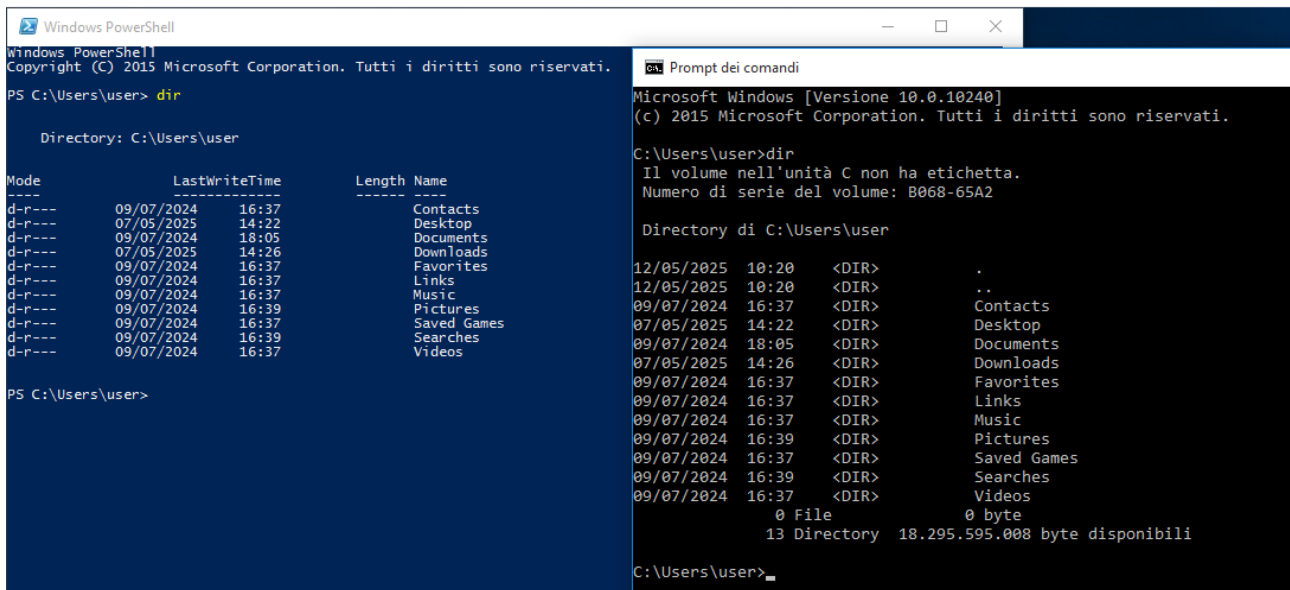


# Esercizio 1: Usare Windows PowerShell

## Domanda 1: Quali sono gli output del comando dir?



```
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

PS C:\Users\user> dir

Directory: C:\Users\user

Mode                LastWriteTime         Length Name
----                -
d-r-----       09/07/2024      16:37             Contacts
d-r-----       07/05/2025      14:22             Desktop
d-r-----       09/07/2024      18:05             Documents
d-r-----       07/05/2025      14:26             Downloads
d-r-----       09/07/2024      16:37             Favorites
d-r-----       09/07/2024      16:37             Links
d-r-----       09/07/2024      16:37             Music
d-r-----       09/07/2024      16:39             Pictures
d-r-----       09/07/2024      16:37             Saved Games
d-r-----       09/07/2024      16:39             Searches
d-r-----       09/07/2024      16:37             Videos

PS C:\Users\user>
```

```
Prompt dei comandi
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\user>dir
Il volume nell'unità C non ha etichetta.
Numero di serie del volume: B068-65A2

Directory di C:\Users\user

12/05/2025  10:20  <DIR>      .
12/05/2025  10:20  <DIR>      ..
09/07/2024  16:37  <DIR>      Contacts
07/05/2025  14:22  <DIR>      Desktop
09/07/2024  18:05  <DIR>      Documents
07/05/2025  14:26  <DIR>      Downloads
09/07/2024  16:37  <DIR>      Favorites
09/07/2024  16:37  <DIR>      Links
09/07/2024  16:37  <DIR>      Music
09/07/2024  16:39  <DIR>      Pictures
09/07/2024  16:37  <DIR>      Saved Games
09/07/2024  16:39  <DIR>      Searches
09/07/2024  16:37  <DIR>      Videos
               0 File               0 byte
               13 Directory  18.295.595.008 byte disponibili

C:\Users\user>
```

Il comando **dir** è un comando usato **elenare il contenuto di una directory** Entrambi mostrano le stesse cartelle nella directory **C:\Users\user**. Tuttavia **CMD** mostra informazioni sul volume e spazio disponibile

## Domanda 2: Prova un altro comando che hai usato nel prompt dei comandi, come ping, cd e ipconfig. Quali sono i risultati?

Il risultato del comando **cd (change directory)** ci mostra la directory dentro quale siamo



```
C:\Users\user>cd
C:\Users\user
C:\Users\user>
```

```
PS C:\Users\user> cd
PS C:\Users\user>
```

Il comando **ipconfig** mostra la **configurazione di rete** del computer (gli indirizzi IP, subnet mask e gateway)

```

PS C:\Users\user> ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione: station
    Indirizzo IPv4. . . . . : 192.168.1.15
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1

Scheda Tunnel isatap.station:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione: station

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 . . . . . : 2001:0:2851:782c:1cb0:15a:928a:9987
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::1cb0:15a:928a:9987%5
    Gateway predefinito . . . . . : ::

PS C:\Users\user>

```

```

C:\Users\user>ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione: station
    Indirizzo IPv4. . . . . : 192.168.1.15
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1

Scheda Tunnel isatap.station:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione: station

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 . . . . . : 2001:0:2851:782c:1cb0:15a:928a:9987
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::1cb0:15a:928a:9987%5
    Gateway predefinito . . . . . : ::

```

Il comando **ping**, invece, mostra la sua pagina **help**, questo perchè per funzionare a dovere, occorre un indirizzo **ip** con la quale comunicare.

```

PS C:\Users\user> ping

Sintassi: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment]
            [-4] [-6] target_name

Opzioni:
    -t             Esegue il ping dell'host specificato finché non viene
                   interrotto. Per visualizzare le statistiche e continuare -
                   digitare Control-Break; Per interrompere - digitare
                   Control-C.
    -a             Risolve gli indirizzi in nomi host.
    -n count       Numero di richieste echo da inviare.
    -l size        Dimensioni del buffer di invio.
    -f             Imposta il contrassegno per la disattivazione della
                   frammentazione nel pacchetto (solo IPv4).
    -i TTL         Durata (TTL, Time To Live).
    -v TOS         Tipo di servizio (TOS, Type Of Service) (solo IPv4).
                   Questa impostazione è deprecata e non ha alcun effetto sul
                   campo del tipo di servizio nell'intestazione IP.
    -r count       Registra la route per il conteggio degli hop (solo IPv4).
    -s count       Timestamp per il conteggio degli hop (solo IPv4).
    -j host-list   Route di origine libera lungo l'elenco host (solo IPv4).
    -k host-list   Route di origine vincolata lungo l'elenco host (solo IPv4).
    -w timeout     Timeout in millisecondi per l'attesa di ogni risposta.
    -R             Usa l'intestazione di routing anche per il test del routing
                   inverso (solo IPv6). In base a RFC 5095 l'utilizzo di questa
                   intestazione di routing è deprecato. Alcuni sistemi
                   potrebbero ignorare le richieste echo se viene utilizzata
                   questa intestazione.
    -S srcaddr     Indirizzo di origine da utilizzare.
    -c compartment Identificatore del raggruppamento di routing.
    -p             Esegue il ping dell'indirizzo di un provider
                   di virtualizzazione di rete di Hyper-V.
    -4             Impone l'utilizzo di IPv4.

```

```

C:\Users\user>ping

Sintassi: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment]
            [-4] [-6] target_name

Opzioni:
    -t             Esegue il ping dell'host specificato finché non viene
                   interrotto. Per visualizzare le statistiche e continuare -
                   digitare Control-Break; Per interrompere - digitare
                   Control-C.
    -a             Risolve gli indirizzi in nomi host.
    -n count       Numero di richieste echo da inviare.
    -l size        Dimensioni del buffer di invio.
    -f             Imposta il contrassegno per la disattivazione della
                   frammentazione nel pacchetto (solo IPv4).
    -i TTL         Durata (TTL, Time To Live).
    -v TOS         Tipo di servizio (TOS, Type Of Service) (solo IPv4).
                   Questa impostazione è deprecata e non ha alcun effetto sul
                   campo del tipo di servizio nell'intestazione IP.
    -r count       Registra la route per il conteggio degli hop (solo IPv4).
    -s count       Timestamp per il conteggio degli hop (solo IPv4).
    -j host-list   Route di origine libera lungo l'elenco host (solo IPv4).
    -k host-list   Route di origine vincolata lungo l'elenco host (solo IPv4).

```

Domanda 3: Qual è il comando PowerShell per dir?

```
PS C:\Users\user> Get-Alias dir
```

CommandType	Name	Version	Source
Alias	dir -> Get-ChildItem		

Il comando powershell per dir è **Get-ChildItem**

Domanda 4: Per visualizzare la tabella di routing con le rotte attive, inserisci netstat -r al prompt. Qual è il gateway IPv4?

```
PS C:\Users\user> netstat -r
```

=====

Elenco interfacce

```
4...08 00 27 86 8e d3 .....Intel(R) PRO/1000 MT Desktop Adapter
1.....Software Loopback Interface 1
6...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
5...00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
```

=====

IPv4 Tabella route

=====

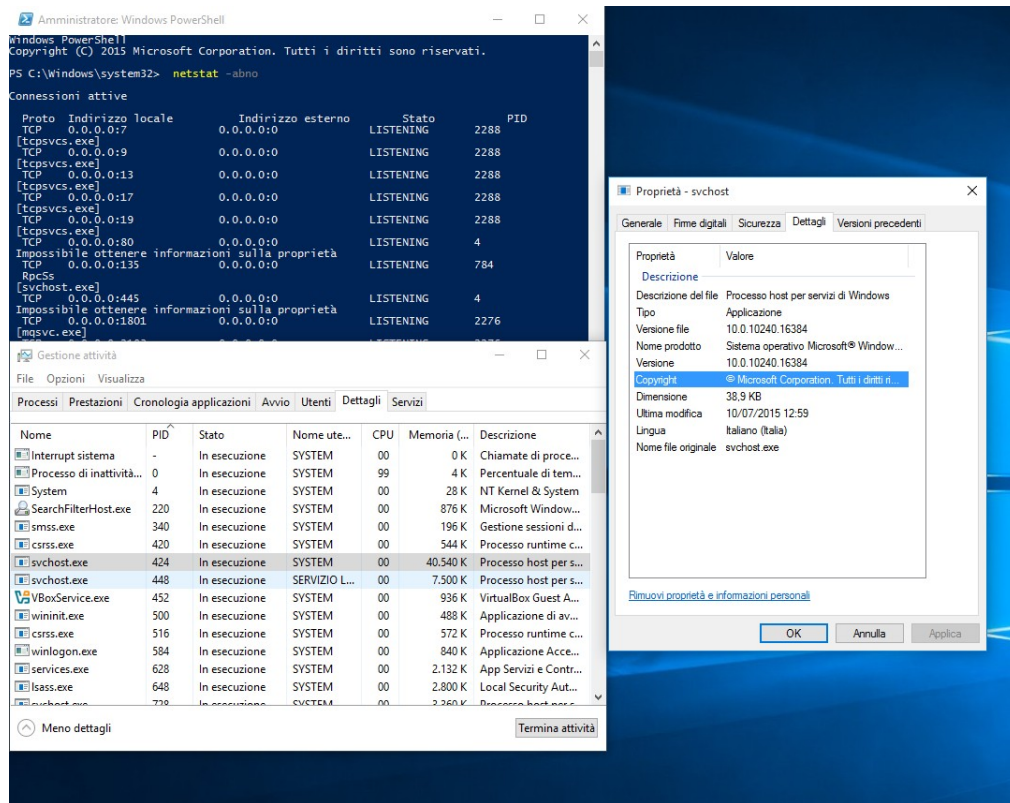
Route attive:

Indirizzo rete	Mask	Gateway	Interfaccia	Metrica
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.15	10
127.0.0.0	255.0.0.0	On-link	127.0.0.1	306
127.0.0.1	255.255.255.255	On-link	127.0.0.1	306
127.255.255.255	255.255.255.255	On-link	127.0.0.1	306
192.168.1.0	255.255.255.0	On-link	192.168.1.15	266
192.168.1.15	255.255.255.255	On-link	192.168.1.15	266
192.168.1.255	255.255.255.255	On-link	192.168.1.15	266
224.0.0.0	240.0.0.0	On-link	127.0.0.1	306
224.0.0.0	240.0.0.0	On-link	192.168.1.15	266
255.255.255.255	255.255.255.255	On-link	127.0.0.1	306
255.255.255.255	255.255.255.255	On-link	192.168.1.15	266

=====

Il gateway ipv4 è **192.168.1.1**

## Domanda 5: Quali informazioni puoi ottenere dalla scheda Dettagli e dalla finestra di dialogo Proprietà per il PID selezionato?



Nella scheda dettagli possiamo ottenere queste informazioni.

- Nome del prodotto
- Versione del file
- Descrizione
- Azienda
- Copyright

**Domanda 6: In una console PowerShell, inserisci clear-recyclebin al prompt. Cosa è successo ai file nel Cestino?**

```
PS C:\Users\user> clear-recyclebin
PS C:\Users\user>
Conferma
Eseguire l'operazione?
Esecuzione dell'operazione "Clear-RecycleBin" sulla destinazione "Tutto il contenuto
del Cestino".
[S] Sì [T] Sì a tutti [N] No [U] No a tutti [O] Sospendi [?] Guida
(il valore predefinito è "S"):_
```

Il contenuto del cestino è stato **eliminato**

**Domanda di Riflessione: PowerShell è stato sviluppato per l'automazione delle attività e la gestione della configurazione. Usando internet, ricerca comandi che potresti usare per semplificare i tuoi compiti come analista di sicurezza. Registra le tue scoperte.**

## **Raccolta Informazioni di Sistema**

**Get-Process:** Visualizza tutti i processi in esecuzione (come Task Manager):

**Get-Service:** Elenca tutti i servizi attivi e disattivi:

**Get-NetTCPConnection:** Mostra le connessioni di rete attive (simile a netstat):

## **Analisi dei Log di Sicurezza**

**Get-WinEvent:** Estrai eventi dai log di sicurezza

## **Network e Recon**

**Resolve-DnsName:** Per risolvere nomi DNS (simile a nslookup)

**Test-Connection:** Ping verso un host

## Difesa e Risposta a Incidenti

**Get-MpThreat:** Mostra minacce rilevate da Windows Defender

**Start-MpScan:** Avvia una scansione con Windows Defender

## Bonus 1: Esplorazione di Nmap

### Domanda 1: Cos'è Nmap? Per cosa viene usato nmap?

```
NMAP(1)                                Nmap Reference Guide                                NMAP(1)

NAME
    nmap - Network exploration tool and security / port scanner

SYNOPSIS
    nmap [Scan Type...] [Options] {target specification}

DESCRIPTION
    Nmap ("Network Mapper") is an open source tool for network exploration
    and security auditing. It was designed to rapidly scan large networks,
    although it works fine against single hosts. Nmap uses raw IP packets
    in novel ways to determine what hosts are available on the network,
    what services (application name and version) those hosts are offering,
    what operating systems (and OS versions) they are running, what type of
    packet filters/firewalls are in use, and dozens of other
```

**Nmap** è un potente strumento l'esplorazione e la mappatura delle reti.

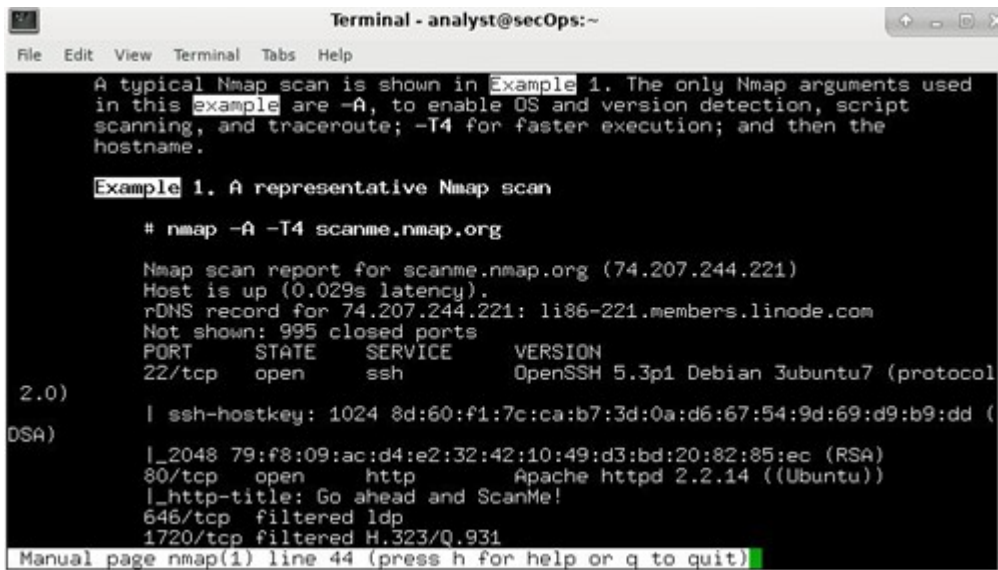
1 Permette di identificare quali dispositivi sono accesi e raggiungibili su una **determinata rete**.

2 Nmap può rilevare le **porte aperte** su un sistema remoto

3 Nmap è in grado di determinare **quale software** è in esecuzione su una determinata porta e **quale versione** specifica del servizio è attiva

4 Nmap può stimare il tipo di **sistema operativo**

## Domanda 2: Qual è il comando nmap usato?



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

A typical Nmap scan is shown in Example 1. The only Nmap arguments used
in this example are -A, to enable OS and version detection, script
scanning, and traceroute; -T4 for faster execution; and then the
hostname.

Example 1. A representative Nmap scan

# nmap -A -T4 scanme.nmap.org

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT      STATE      SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 5.3p1 Debian 3ubuntu7 (protocol
2.0)
| ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (
DSA)
|_ 2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp    open      http         Apache httpd 2.2.14 ((Ubuntu))
|_ http-title: Go ahead and ScanMe!
646/tcp   filtered  ldap
1720/tcp  filtered  H.323/Q.931

Manual page nmap(1) line 44 (press h for help or q to quit)
```

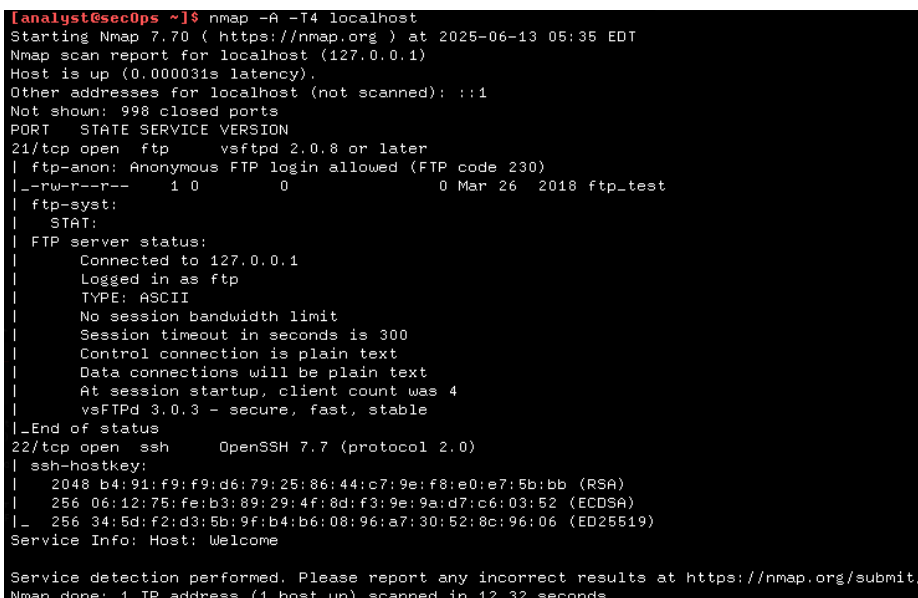
Il comando utilizzato è `nmap -n -T4 scanme.nmap.org`

## Domanda 3: Cosa fa l'opzione -A? Cosa fa l'opzione -T4?

L'opzione `-A` abilita la "scansione aggressiva".

Mentre l'opzione `-T4 (Timing template)` imposta il template di timing accelerando significativamente la scansione, ma la rende anche più "rumorosa".

## Domanda 4: Quali porte e servizi sono aperti?



```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-06-13 05:35 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000031s 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 12.32 seconds
```

Le porte aperte sono la **21(TCP)** e la **22(SSH)**



## Domanda 5: A quale rete appartiene la tua VM?

```
[analyst@secOps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:be:60:c7 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 85077sec preferred_lft 85077sec
    inet6 fd00::a00:27ff:febe:60c7/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86220sec preferred_lft 14220sec
    inet6 fe80::a00:27ff:febe:60c7/64 scope link
        valid_lft forever preferred_lft forever
```

La VM appartiene alla rete: **10.0.2.0/24**

## Domanda 6: Quanti host sono attivi?

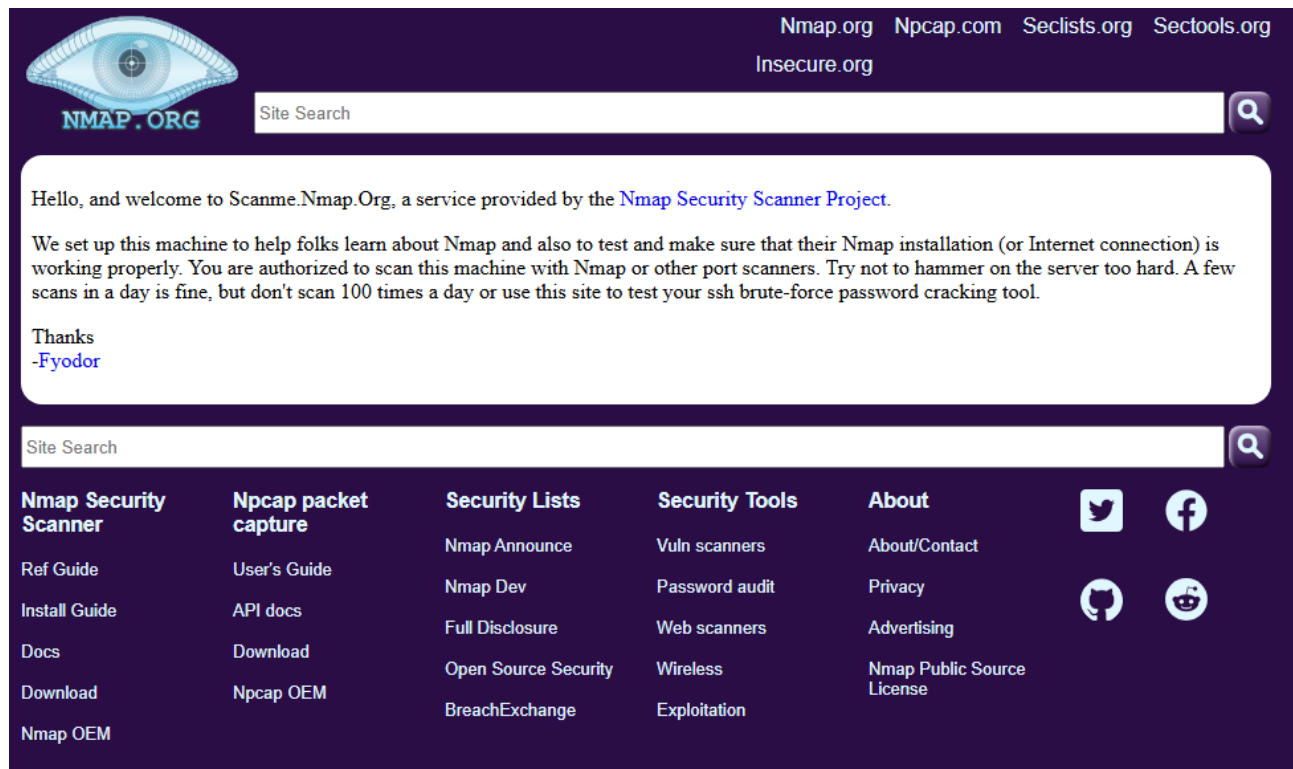
```
[analyst@secOps ~]$ nmap -A -iL 10.0.2.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2025-06-13 05:46 EDT
Nmap scan report for 10.0.2.15
Host is up (0.000043s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
| ftp-anon: Anonymous 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 10.0.2.15
|   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 3
|   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: 256 IP addresses (1 host up) scanned in 27.40 seconds
```

E attivo **1** solo host (ultima riga)



Domanda 7: Apri un browser web e naviga su [scanme.nmap.org](https://scanme.nmap.org). Leggi il messaggio pubblicato. Qual è lo scopo di questo sito?



E un server pubblico gestito dagli sviluppatori di Nmap, creato appositamente per consentire agli utenti di provare **scansioni di rete reali** usando Nmap senza rischiare di violare regole o leggi.

Domanda 8: Quali porte e servizi sono aperti? Quali porte e servizi sono filtrati? Qual è l'indirizzo IP del server? Qual è il sistema operativo?

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2025-06-13 06:03 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.18s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 filtered 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!
9929/tcp  open  nping-echo   Nping echo
31337/tcp open  tcpwrapped
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 29.95 seconds
```

### Porte e servizi aperti:

- Porta 22/tcp - SSH
- Porta 80/tcp - HTTP
- Porta 9929/tcp - nping-echo
- Porta 31337/tcp - tcpwrapped

### Porte e servizi filtrati:

- 996 porte filtrate ("996 filtered ports")

### Indirizzo IP del server:

45.33.32.156

### Sistema operativo:

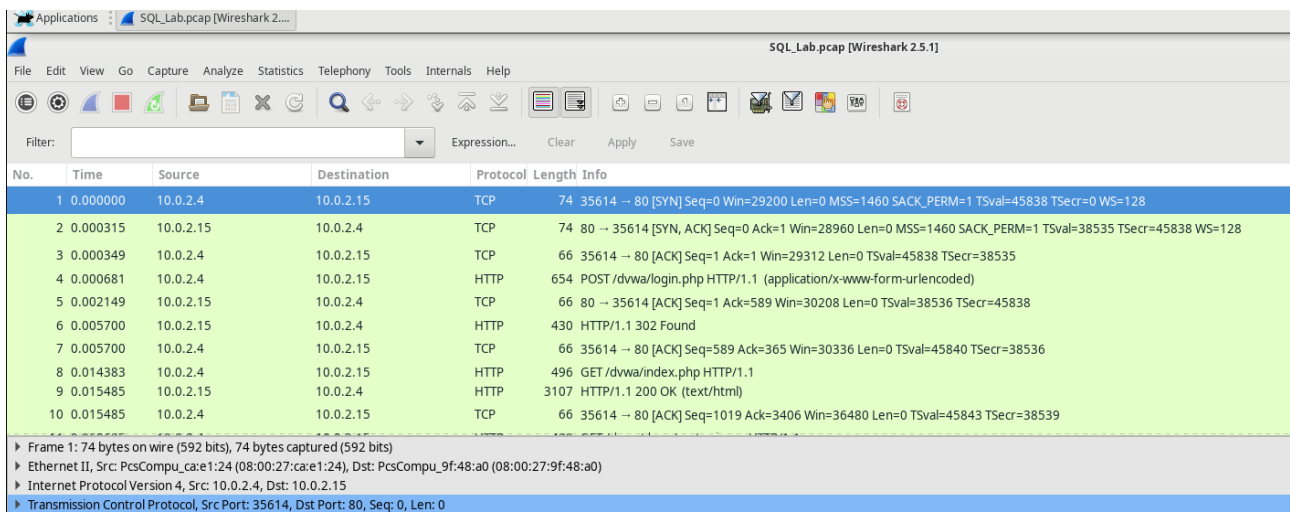
Ubuntu Linux

**Domanda Riflessione: Nmap è uno strumento potente per l'esplorazione e la gestione della rete. Come può Nmap aiutare con la sicurezza della rete? Come può Nmap essere usato da un attore malevolo come strumento nefasto?**

**Nmap può essere usato legittimamente** dagli amministratori per **identificare vulnerabilità, verificare configurazioni di sicurezza** e condurre una **verifica approfondita di rete autorizzati**. Invece può essere usato dagli attaccanti per mappare **reti target**, scoprire **servizi vulnerabili** e **raccogliere informazioni** per preparare attacchi. La differenza cruciale è **l'autorizzazione**: l'uso legittimo richiede permessi espliciti, mentre l'uso malevolo viola le policy di sicurezza e può essere illegale.

# Bonus 2: Attacco a un database MySQL

**Domanda 1: Quali sono i due indirizzi IP coinvolti in questo attacco di SQL injection in base alle informazioni visualizzate?**



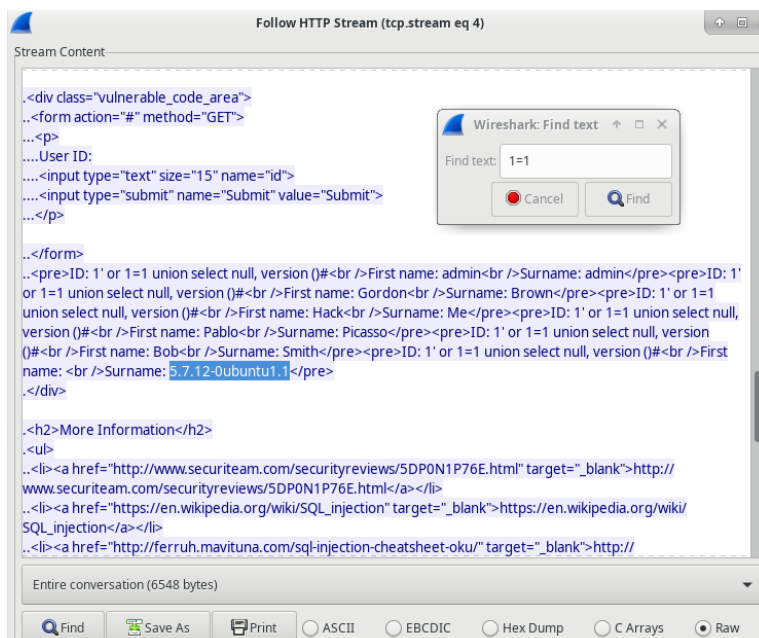
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.4	10.0.2.15	TCP	74	35614 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=45838 TSecr=0 WS=128
2	0.000315	10.0.2.15	10.0.2.4	TCP	74	80 → 35614 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=38535 TSecr=45838 WS=128
3	0.000349	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=45838 TSecr=38535
4	0.000681	10.0.2.4	10.0.2.15	HTTP	654	POST /dvwa/login.php HTTP/1.1 (application/x-www-form-urlencoded)
5	0.002149	10.0.2.15	10.0.2.4	TCP	66	80 → 35614 [ACK] Seq=1 Ack=589 Win=30208 Len=0 TSval=38536 TSecr=45838
6	0.005700	10.0.2.15	10.0.2.4	HTTP	430	HTTP/1.1 302 Found
7	0.005700	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=589 Ack=365 Win=30336 Len=0 TSval=45840 TSecr=38536
8	0.014383	10.0.2.4	10.0.2.15	HTTP	496	GET /dvwa/index.php HTTP/1.1
9	0.015485	10.0.2.15	10.0.2.4	HTTP	3107	HTTP/1.1 200 OK (text/html)
10	0.015485	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=1019 Ack=3406 Win=36480 Len=0 TSval=45843 TSecr=38539

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)  
Ethernet II, Src: PcsCompu\_ca:e1:24 (08:00:27:ca:e1:24), Dst: PcsCompu\_9f:48:a0 (08:00:27:9f:48:a0)  
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15  
Transmission Control Protocol, Src Port: 35614, Dst Port: 80, Seq: 0, Len: 0

I due indirizzi IP coinvolti nell'attacco di **SQL injection** sono:

1. 10.0.2.4 (Attaccante)
2. 10.0.2.15 (Target)

**Domanda 2: Qual è la versione?**



La versione del database  
risulta essere: **5.7.12-  
0ubuntu1.1**

## Domanda 3: Quale utente ha l'hash della password di 8d3533d75ae2c3966d7e0d4fcc69216b?



L'Hash appartiene all'utente "1337"

## Domanda 4: Qual è la password in chiaro?

### Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

I'm not a robot

reCAPTCHA

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

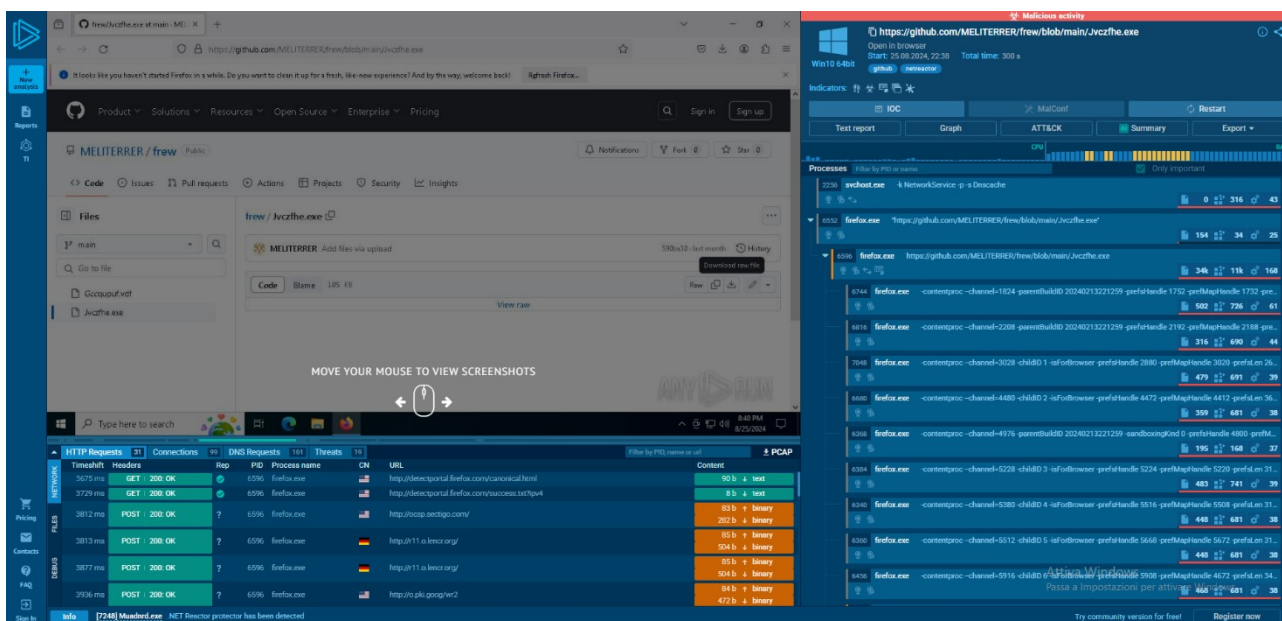
Hash	Type	Result
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley

Color Codes: **Green** Exact match, **Yellow** Partial match, **Red** Not found.

La password in chiaro è "charley"

# Esercizio 2: Studio Ioc

Studiare questo link di **anyrun** e spiegare queste minacce in un piccolo report: <https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281/>



## Analisi del Malware Muadnrd.exe

L'analisi dinamica del file Muadnrd.exe in ambiente sandbox Windows 10 ha identificato un Trojan Dropper ad alta pericolosità. Durante l'esecuzione, il malware ha stabilito connessioni verso domini sospetti come detectportal.firefox.com e ncap.sectigo.com, indicando la presenza di un'infrastruttura di comando e controllo attiva.

Il campione dimostra sofisticate capacità evasive attraverso process injection nel processo legittimo firefox.exe per mascherare le attività malevole, e utilizza timeout.exe per implementare ritardi strategici nelle operazioni. Particolarmente preoccupanti sono le multiple richieste POST verso IP esteri, suggerendo attività di esfiltrazione dati verso server controllati dagli attaccanti.

La minaccia è classificata ad alto rischio per la capacità di mantenere persistenza nel sistema e scaricare payload aggiuntivi. Si raccomanda l'isolamento immediato dei sistemi compromessi, il blocco dei domini C2 identificati, l'aggiornamento delle signature antivirus e l'avvio di un'indagine forense per valutare l'estensione completa della compromissione.