

# CyberOps Project

**Amin El Kassimi**

CyberSecurity EN  
Paolo Rampino  
Feb 20-21, 2026

## Executive Summary

Mission.....	1
Esercizio 1: Usare Windows PowerShell.....	2
Esercizio 2: Studio loc.....	11
Bonus 1: Esplorazione e Utilizzo Pratico di Nmap per la Ricognizione di Rete .....	26
Bonus 2 : Analisi Forense di un Attacco di SQL Injection su Database MySQL.....	34

## Mission

L'obiettivo principale di questo laboratorio è quello di applicare in modo concreto le conoscenze teoriche acquisite durante il corso, sperimentando direttamente strumenti e tecniche professionali utilizzati dagli analisti di sicurezza e dagli ethical hacker.

Nello specifico, il progetto si è articolato nelle seguenti esercitazioni:

- **Esercizio 1:** Esplorazione delle funzionalità di **Windows PowerShell** per l'esecuzione di comandi, cmdlet e automazione di operazioni di sistema (svuotamento cestino, analisi connessioni di rete, ecc.).
- **Esercizio 2:** Analisi dinamica di un campione di malware attraverso la piattaforma di sandbox online **ANY.RUN** (link fornito), con lo scopo di identificare e descrivere le minacce presenti nel report.
- **Bonus 1:** Approfondimento e utilizzo pratico di **Nmap** per la discovery di rete, lo scanning delle porte e l'identificazione di servizi attivi su localhost, rete locale e server remoto.
- **Bonus 2:** Analisi forense di un attacco di **SQL Injection** contro un database MySQL, effettuata esaminando un file PCAP con **Wireshark**.

## 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

## 1. QUALI SONO GLI OUTPUT DEL COMANDO DIR?

Eseguendo dir nella PowerShell, l'output mostra l'**elenco dettagliato dei file e delle cartelle** contenuti nella directory corrente (C:\Users\amine). Nello specifico, i dati visualizzati includono:

- **Mode**: Indica gli attributi del file o della cartella (ad esempio, d per directory e a per archivio/file).
- **LastWriteTime**: Mostra la data e l'ora dell'ultima modifica effettuata su ogni elemento.
- **Length**: Indica la dimensione dei file in byte (questo campo è vuoto per le directory).
- **Name**: Il nome del file o della cartella (come .ssh, Desktop, o .gitconfig).

PS C:\Users\amine> dir			
Directory: C:\Users\amine			
Mode	LastWriteTime	Length	Name
d----	12-Nov-25 22:54		.android
d----	12-Dec-24 19:14		.cache
d----	12-Dec-24 23:56		.codex
d----	05-Feb-26 10:31		.config
d----	23-Jul-24 12:59		.cursor
d----	22-Aug-25 20:58		.eclipse
d----	05-Aug-24 11:49		.gk
d----	19-Feb-26 12:08		.insomniac
d----	08-Oct-23 21:08		.m2
d----	24-Jul-24 12:24		.ms-ad
d----	06-Mar-25 17:29		.p2
d----	06-Feb-25 10:33		.redhat
d----	24-Jun-24 16:22		.ssh
d----	26-Jul-24 11:54		.VirtualBox
d----	20-Feb-26 14:19		.vscode
d----	13-Jul-23 08:07		ansel
d----	03-Feb-25 15:22		Apple
d----	26-Dec-24 21:05		Cisco Packet Tracer 9.0.0
d----	24-Dec-25 20:52		Contacts
d-r---	16-Apr-25 23:27		Desktop
d-r---	20-Feb-26 10:49		Documents
d-r---	06-Mar-25 17:27		Downloads
d-r---	20-Feb-26 10:59		Favorites
d-r---	16-Apr-25 23:27		Immagini
d-r---	16-Feb-26 09:50		Links
d-r---	19-Apr-25 16:29		Music
d-r---	02-Aug-25 19:06		npm-cache
d----	09-May-24 15:47		OneDrive
d----	03-Feb-26 14:17		Postman
d----	29-Apr-24 18:34		Searches
d-r---	16-Apr-25 23:27		Videos
d-r---	14-Feb-26 14:51		VirtualBox VMs
d----	17-Feb-26 16:23		
-a---	29-Apr-24 18:58	142	.angular-config.json
-a---	26-Jul-24 14:30	393	.gitconfig
-a---	12-Feb-25 10:51	20	.lessht
-a---	30-May-24 17:55	33	.node_repl_history
-a---	24-Dec-25 20:47	176	.packettracer

## 2. QUALI SONO I RISULTATI?

I risultati sono **identici in termini di funzionalità** in entrambe le console:

- **ipconfig**: Il comando visualizza correttamente la configurazione IP di Windows. Nel tuo caso specifico, mostra i dettagli della scheda Ethernet 2 (IP 192.168.50.1) e della scheda Wi-Fi (IP 192.168.1.14).
- **ping**: Poiché è stato digitato senza argomenti, il comando restituisce la guida all'uso ("Usage") con l'elenco di tutte le opzioni disponibili (come -t, -a, -n count, ecc.).
- **cd**: Il comando è stato accettato senza restituire errori, confermando la sua funzione di navigazione tra le directory, anche se in questo caso non sono stati specificati percorsi di spostamento.

```
PS C:\Users\amine> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::fd18:3f42:4f05:7cd3%11
  IPv4 Address. . . . . : 192.168.50.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Unknown adapter OpenVPN Data Channel Offload for Surfshark:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 1:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 2:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Wireless LAN adapter Wi-Fi:

  Connection-specific DNS Suffix . : station
  IPv4 Address. . . . . : 192.168.1.14
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.1.1
PS C:\Users\amine> ping

Usage: 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] [-p]
           [-4] [-6] target_name

Options:
  -t            Ping the specified host until stopped.
                 To see statistics and continue - type Control-Break;
                 To stop - type Control-C.
  -a            Resolve addresses to hostnames.
  -n count      Number of echo requests to send.
  -l size       Send buffer size.
  -f            Set Don't Fragment flag in packet (IPv4-only).
  -i TTL        Time To Live.
```

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

---

### 3. QUAL È IL COMANDO POWERSHELL PER DIR?

Come mostrato nello screenshot del laboratorio tramite il comando Get-Alias dir, il vero comando nativo di PowerShell (cmdlet) è:

**Get-ChildItem**

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

### 4. QUAL È IL GATEWAY IPV4?

Il **Gateway IPv4** predefinito (Default Gateway) è **192.168.1.1**.

```
PS C:\Users\amine> netstat -r
=====
Interface List
11...0a 00 27 00 00 0b .....VirtualBox Host-Only Ethernet Adapter
9.....OpenVPN Data Channel Offload
4...c4 03 a8 d1 4b a2 .....Microsoft Wi-Fi Direct Virtual Adapter
13...c6 03 a8 d1 4b a1 .....Microsoft Wi-Fi Direct Virtual Adapter #2
18...c4 03 a8 d1 4b a1 .....Killer(R) Wi-Fi 6E AX1675i 160MHz Wireless Network Adapter (211NGW)
8...c4 03 a8 d1 4b a5 .....Bluetooth Device (Personal Area Network)
1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination      Netmask        Gateway       Interface Metric
          0.0.0.0          0.0.0.0   192.168.1.1  192.168.1.14    35
         127.0.0.0        255.0.0.0     On-link      127.0.0.1    331
         127.0.0.1        255.255.255     On-link      127.0.0.1    331
127.255.255.255  255.255.255.255     On-link      127.0.0.1    331
         192.168.1.0        255.255.255.0     On-link    192.168.1.14    291
         192.168.1.14        255.255.255.255     On-link    192.168.1.14    291
         192.168.1.255        255.255.255.255     On-link    192.168.1.14    291
         192.168.50.0        255.255.255.0     On-link    192.168.50.1    281
         192.168.50.1        255.255.255.255     On-link    192.168.50.1    281
192.168.50.255  255.255.255.255     On-link    192.168.50.1    281
         224.0.0.0          240.0.0.0     On-link      127.0.0.1    331
         224.0.0.0          240.0.0.0     On-link    192.168.50.1    281
         224.0.0.0          240.0.0.0     On-link    192.168.1.14    291
         255.255.255.255        255.255.255.255     On-link      127.0.0.1    331
         255.255.255.255        255.255.255.255     On-link    192.168.50.1    281
         255.255.255.255        255.255.255.255     On-link    192.168.1.14    291
=====
Persistent Routes:
None

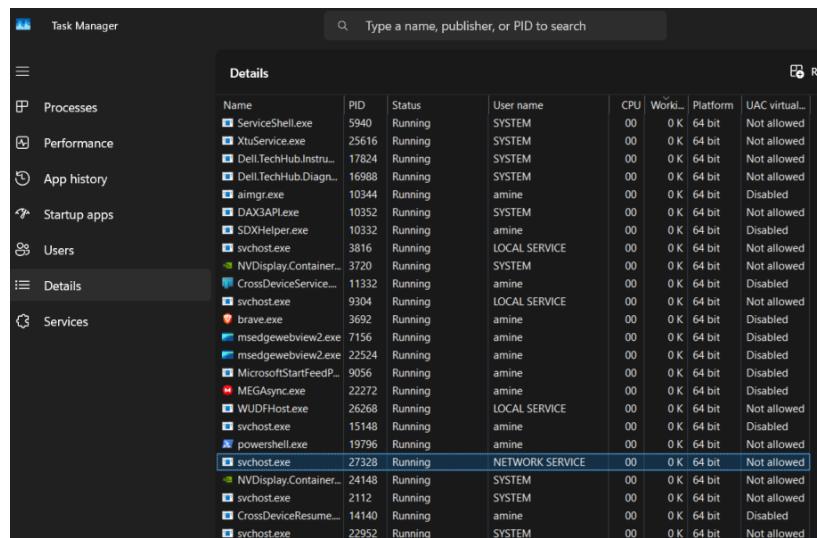
IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
  1    331 ::1/128          On-link
11    281 fe80::/64          On-link
11    281 fe80::fd18:3f42:4f05:7cd3/128
                           On-link
  1    331 ff00::/8          On-link
11    281 ff00::/8          On-link
=====
Persistent Routes:
None
```

## 5. QUALI INFORMAZIONI PUOI OTTENERE DALLA SCHEDA DETTAGLI E DALLA FINESTRA DI DIALOGO PROPRIETÀ PER IL PID SELEZIONATO?

Dalla colonna dei dettagli nel Task Manager, puoi visualizzare immediatamente:

- Nome dell'eseguibile:** Il nome del file che ha generato il processo (es. svchost.exe).
- PID (Process ID):** Il numero identificativo univoco assegnato dal sistema operativo (es. 27328).
- Stato:** Se il processo è attualmente in esecuzione (Running) o sospeso.
- Nome utente:** L'account sotto il quale il processo è in esecuzione (es. NETWORK SERVICE o amine).

- Utilizzo risorse:** Il consumo di **CPU** e **Memoria** (Working set) in tempo reale.
- Architettura e Sicurezza:** La piattaforma (es. 64 bit) e lo stato della virtualizzazione UAC.



Name	PID	Status	User name	CPU	Work...	Platform	UAC virtual...
ServiceShell.exe	5940	Running	SYSTEM	00	0 K	64 bit	Not allowed
Xt!Service.exe	25616	Running	SYSTEM	00	0 K	64 bit	Not allowed
Dell.TechHub.Instru...	17824	Running	SYSTEM	00	0 K	64 bit	Not allowed
Dell.TechHub.Diagn...	16988	Running	SYSTEM	00	0 K	64 bit	Not allowed
aimgr.exe	10344	Running	amine	00	0 K	64 bit	Disabled
DAX3APIL.exe	10352	Running	SYSTEM	00	0 K	64 bit	Not allowed
SDXHelper.exe	10332	Running	amine	00	0 K	64 bit	Disabled
svchost.exe	3816	Running	LOCAL SERVICE	00	0 K	64 bit	Not allowed
NVDisplay.Container...	3720	Running	SYSTEM	00	0 K	64 bit	Not allowed
CrossDeviceService...	11332	Running	amine	00	0 K	64 bit	Disabled
svchost.exe	9304	Running	LOCAL SERVICE	00	0 K	64 bit	Not allowed
brave.exe	3692	Running	amine	00	0 K	64 bit	Disabled
msedgewebview2.exe	7156	Running	amine	00	0 K	64 bit	Disabled
msedgewebview2.exe	22524	Running	amine	00	0 K	64 bit	Disabled
MicrosoftStartFeedP...	9056	Running	amine	00	0 K	64 bit	Disabled
MEGAsync.exe	22272	Running	amine	00	0 K	64 bit	Disabled
WUDFHost.exe	26268	Running	LOCAL SERVICE	00	0 K	64 bit	Not allowed
svchost.exe	15148	Running	amine	00	0 K	64 bit	Disabled
powershell.exe	19796	Running	amine	00	0 K	64 bit	Not allowed
svchost.exe	27328	Running	NETWORK SERVICE	00	0 K	64 bit	Not allowed
NVDisplay.Container...	24148	Running	SYSTEM	00	0 K	64 bit	Not allowed
svchost.exe	2112	Running	SYSTEM	00	0 K	64 bit	Not allowed
CrossDeviceResume...	14140	Running	amine	00	0 K	64 bit	Disabled
svchost.exe	22952	Running	SYSTEM	00	0 K	64 bit	Not allowed

## Informazioni dalla finestra di dialogo Proprietà

### Dalla scheda "Generale" (General)

Questa scheda fornisce i dati fondamentali del file eseguibile:

- Nome e Descrizione:** Il file si chiama svchost.exe ed è descritto come "Host Process for Windows Services".
- Percorso (Location):** Si trova in C:\Windows\System32, confermando che si tratta di un processo di sistema legittimo.
- Dimensioni:** Il file occupa **86.1 KB** (88.232 byte) su disco.
- Date Temporali:** Puoi vedere esattamente quando il file è stato creato, modificato e l'ultima volta che è stato eseguito (nel tuo caso, tutte le date riportano il **30 gennaio 2026**).

### Dalla scheda "Firme digitali" (Digital Signatures)

Questa è fondamentale per la cybersecurity per verificare l'integrità del processo:

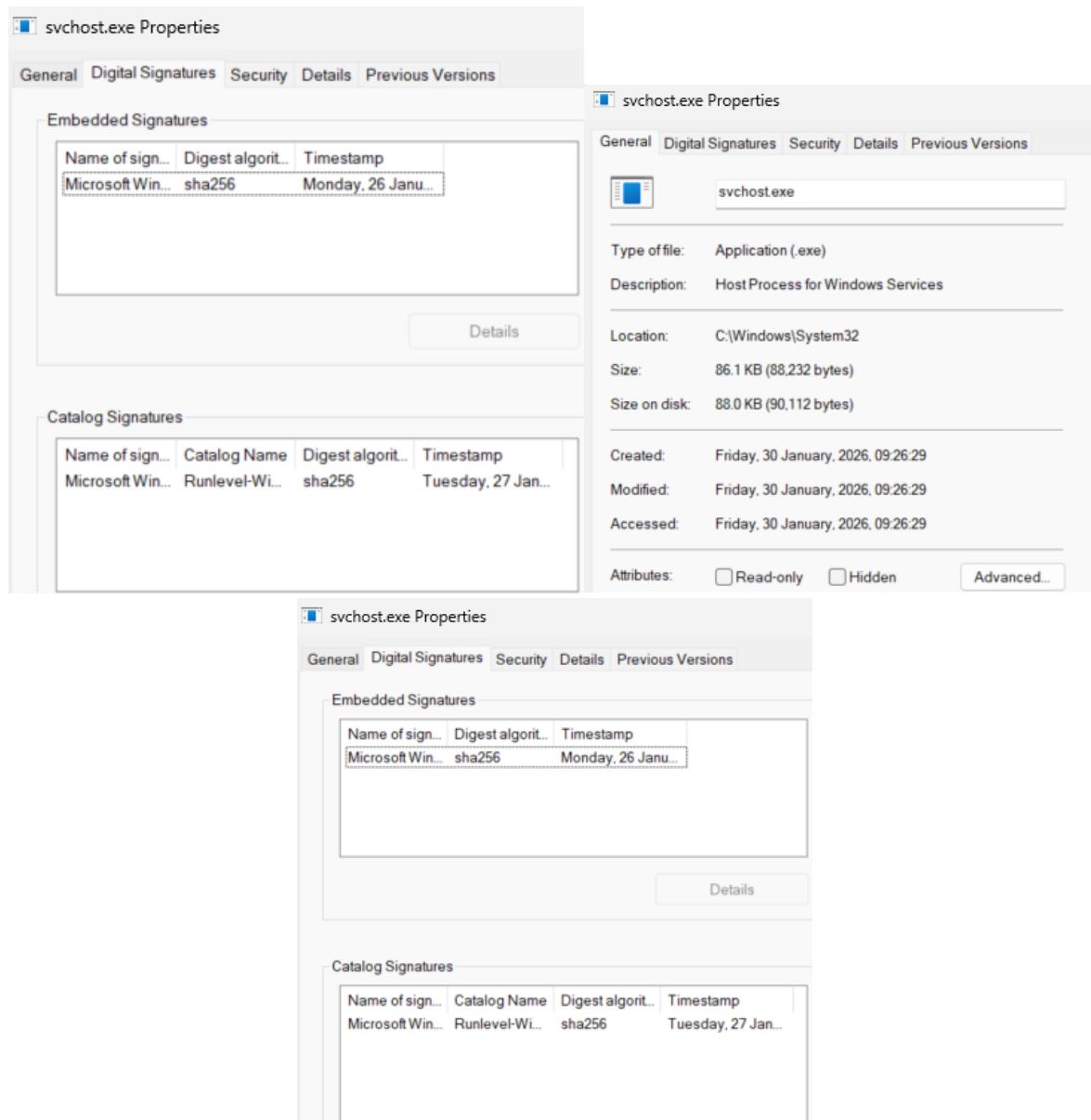
- Nome del firmatario:** Indica che il file è firmato ufficialmente da **Microsoft Windows**.

- **Algoritmo di hash:** Utilizza l'algoritmo **sha256** per garantire che il file non sia stato alterato da malware.
- **Timestamp:** Mostra la data e l'ora esatta in cui è stata apposta la firma.

### Dalla scheda "Sicurezza" (Security)

Qui puoi analizzare i permessi di accesso al file:

- **Nomi di gruppi o utenti:** Elenca chi ha diritti sul file, come SYSTEM, Administrators, e TrustedInstaller.
- **Autorizzazioni:** Specifica i permessi dettagliati (es. "Lettura ed esecuzione", "Lettura") per ogni gruppo selezionato. Ad esempio, per "ALL APPLICATION PACKAGES", i permessi sono limitati a lettura ed esecuzione.



Queste informazioni sono vitali per un analista SOC (CyberOps) per distinguere un vero processo di sistema da un **malware** che tenta di camuffarsi usando lo stesso nome.

---

## 6. COSA È SUCCESSO AI FILE NEL CESTINO?

I file che erano presenti nel Cestino sono stati **eliminati permanentemente** dal computer.

Dall'analisi del risultato si nota che:

- Inserito il comando clear-recyclebin nel prompt di PowerShell.
- Il sistema ha richiesto una conferma tramite il messaggio "Are you sure you want to perform this action?".
- Avendo risposto **y** (Yes), PowerShell ha eseguito l'operazione "Clear-RecycleBin" su tutto il contenuto del Cestino.

```
PS C:\Users\amine> clear-recyclebin

Confirm
Are you sure you want to perform this action?
Performing the operation "Clear-RecycleBin" on target "All of the contents of the Recycle Bin".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y
PS C:\Users\amine> |
```

Una volta controllato il cestino i file non erano più presenti.

## Esercizio 2: Studio loc

### Obiettivi dello Studio

L'obiettivo di questa attività di analisi è identificare e catalogare gli **Indicatori di Compromissione (IoC)** necessari per proteggere l'infrastruttura aziendale. Nello specifico, lo studio mira a:

- Estrarre le "impronte digitali" univoche del malware (Hashes MD5/SHA) per facilitarne il rilevamento.
- Mappare il comportamento del codice malevolo secondo le tattiche della matrice **MITRE ATT&CK**, identificando le fasi di Execution, Defense Evasion e Discovery.
- Monitorare l'attività di rete per individuare gli indirizzi IP e i domini di **Command & Control (C2)** utilizzati per l'esfiltrazione dei dati.

## ANYRUN

Any.Run è uno strumento fantastico studiando Cybersecurity ed Ethical Hacking perché permette di vedere il malware "in azione" senza rischiare la propria macchina.

The screenshot displays the ANY.RUN platform interface. On the left, a Windows desktop environment is shown with various icons like Recycle Bin, Microsoft Edge, and File Explorer. A message at the bottom says "MOVE YOUR MOUSE TO VIEW SCREENSHOTS". On the right, there's a detailed analysis window for a malicious activity. The analysis window includes tabs for "IOC", "ATT&CK", and "Tools". It shows a timeline of processes, network traffic, and DNS requests. A specific process named "svchost.exe" is highlighted, showing its activity over time. Below the main analysis window, there's a table of "Network Threats" with columns for "TimeShift", "Class", "PID", "Process name", and "Message". The threats listed include various types of traffic, mostly from "svchost.exe", such as attempting to access user content on GitHub and dynamic DNS queries to "duckdns.org".

## il Cuore dell'Analisi: La VM (Centro)

Al centro vedi il desktop della macchina virtuale (Windows 10).

- **Interattività:** si Puo cliccare e interagire con il sistema operativo come se fosse il proprio.
- **Timeline:** In alto a destra vediamo il tempo di esecuzione (300 secondi in questo caso)

## La "Process Tree" (Destra)

Questa è la sezione più importante per un analista. Mostra la gerarchia dei processi:

- **Gerarchia:** Vedere come firefox.exe (il browser) ha scaricato ed eseguito il file sospetto Jvczfhe.exe.
- **Colori:** I processi in **rosso** o **arancione** indicano attività sospette o malevole già identificate dalla sandbox.
- **Dettagli:** Cliccando su un singolo processo (es. Jvczfhe.exe), la parte inferiore della schermata si aggiornerà mostrando esattamente cosa ha fatto quel processo (file modificati, chiavi di registro, connessioni).

## Network & Activity (Sotto)

Qui monitoriamo come il malware comunica con l'esterno:

- **HTTP/DNS Requests:** Vedremo i domini contattati. Notare che log i riferimenti a duckdns.org, un servizio di DNS dinamico spessissimo usato dai malware (come RedLine) per nascondere l'IP del server di comando (C2).
- **Network Threats:** Segnala se il traffico corrisponde a "firme" note di minacce (IDS Rules).
- **Cifratura:** In basso a sinistra una nota interessante: .NET Reactor protector has been detected. Questo dice che il malware è "offuscato" per rendere difficile il lavoro di reverse engineering.

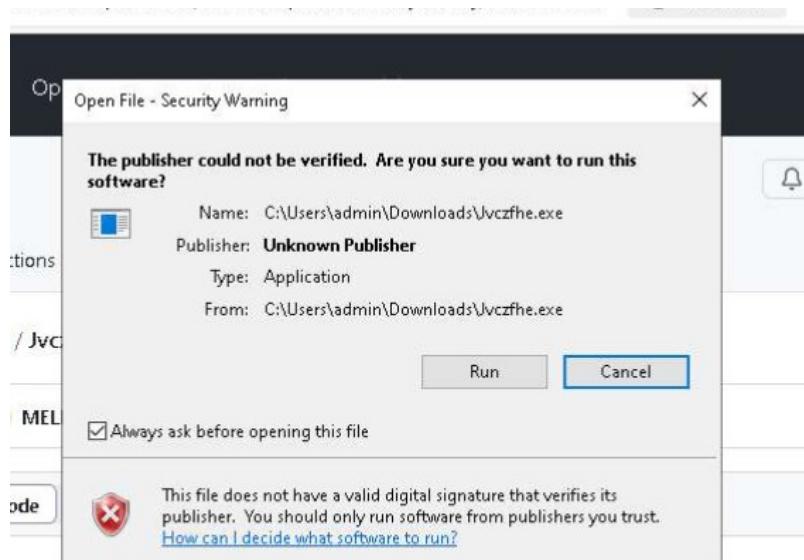
## Strumenti di Reportistica (In alto a destra)

- **IOC (Indicators of Compromise):** Cliccalo per avere subito la lista di IP, domini e hash (MD5/SHA256) da usare nel tuo studio o per bloccare la minaccia su altri sistemi.
- **ATT&CK:** Mappa il comportamento del malware sulle tattiche della matrice **MITRE ATT&CK** (fondamentale per il tuo percorso CyberOps).

## ANALISI

L'utente (o l'automazione della sandbox) ha visitato un repository GitHub (MELITERRER/frew).

- **Perché GitHub?** Gli attaccanti usano spesso GitHub perché è un dominio affidabile (whitelistato da molti firewall) per ospitare payload malevoli.
- **Il file:** Jvczfhe.exe viene scaricato direttamente dal browser.
- **Il file:** Muadrand.exe viene scaricato direttamente dal browser.



## Esecuzione e Social Engineering

L'immagine image\_e1f522.png mostra l'avviso di sicurezza di Windows: "The publisher could not be verified".

- **Analisi:** Questo conferma che il malware non ha una firma digitale valida (Unknown Publisher). In un contesto reale di **Social Engineering**, l'utente ignora l'avviso e clicca su "Run".



### La Tecnica della "Falsa Escursione" (image\_e1f544.png)

Vedi quel messaggio di errore: "*There was an error opening this document. The file is damaged...*"?

- **Questa è una trappola:** Molti malware (specialmente infostealer come RedLine) mostrano un **finto messaggio di errore** appena vengono eseguiti.
- **Lo scopo:** Far credere all'utente che il programma non abbia funzionato e che "sia finita lì". In realtà, mentre l'utente clicca su "OK", il malware è già partito in background e sta iniettando codice in processi come InstallUtil.exe.

Questa situazione si verifica ad entrambi i download ed esecuzione dei codici.

## Sunto dalla sezione Graph di Anyrun



In base alla **Process Tree** (l'albero dei processi), la diramazione dell'attacco si sviluppa in tre "ondate" principali che partono dal download iniziale.

### Prima Ondata: L'Innesco (Loader)

- **Processo Sorgente:** firefox.exe scarica ed esegue il file malevolo iniziale.
- **Primo File:** jvczfhe.exe viene avviato direttamente dal browser.
- **Obiettivo:** Creare l'ambiente per il resto dell'attacco e mostrare il finto messaggio di errore all'utente.

### Seconda Ondata: Esecuzione e Mascheramento

Il file iniziale jvczfhe.exe non compie l'azione finale, ma si dirama in più rami paralleli:

- **Ramo CMD:** Avvia cmd.exe, che a sua volta lancia timeout.exe. Questo serve a ritardare l'attacco (Anti-Sandbox) per non farsi scoprire subito.
- **Ramo Privilege/Injection:** Viene avviato installutil.exe, marcato esplicitamente come **THREAT**. Questo è un tool legittimo di Windows (LOLBIN) usato dal malware per "nascondere" il codice malevolo dentro un processo fidato.
- **Evoluzione:** Appare un secondo processo malevolo "gemello", muadnrd.exe (anch'esso marcato **THREAT**), che replica la stessa struttura di comandi.

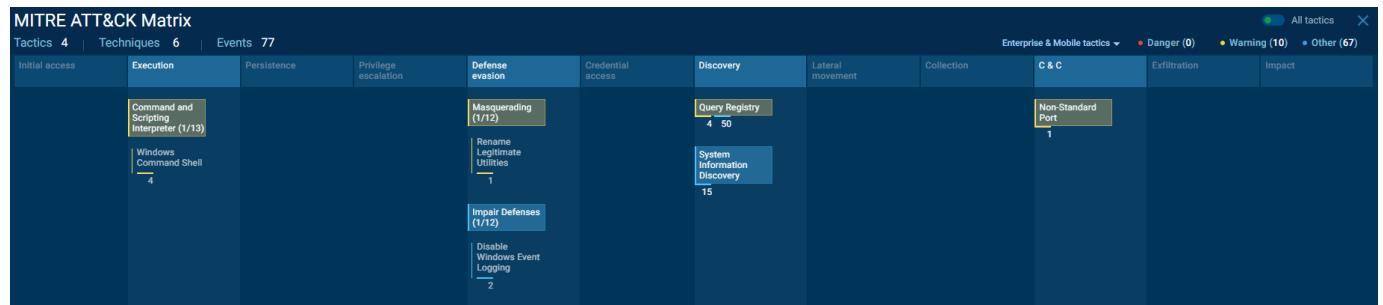
### Terza Ondata: Persistenza e Fallimento

- **WerFault.exe:** Sotto entrambi i rami principali (jvczfhe.exe e muadnrd.exe) compare il processo werfault.exe.
- **Significato:** Questo è il sistema di segnalazione errori di Windows. Indica che il malware, dopo aver tentato di esfiltrare i dati o iniettare codice, potrebbe aver forzato la chiusura o essere crashato, lasciando però l'infezione attiva nei processi iniettati come installutil.exe.

## MATRICE MITRE ATT&CK (IN ALTO/SCHERMATA DEDICATA)

Questa tabella è come un "identikit" del comportamento del criminale.

- Invece di dire solo "è un virus", spiega **come** si sta comportando: ad esempio se sta cercando di nascondersi (**Defense Evasion**) o se sta curiosando tra le informazioni del tuo sistema (**Discovery**).



### Execution:

#### 1. Command and Scripting Interpreter (T1059)

È la fase in cui il malware impedisce ordini al sistema operativo.

- Azione:** Abusa di strumenti già presenti nel PC (come terminali o linguaggi di scripting) per eseguire codice malevolo.
- Nel tuo caso:** Il malware utilizza la **Windows Command Shell** (cmd.exe) per agire. È stata rilevata l'esecuzione di comandi da parte dei processi Jvczfhe.exe e Muadnrd.exe.
- Trucco rilevato:** Utilizza TIMEOUT.EXE per ritardare l'esecuzione, una tecnica comune per evitare che l'utente o i sistemi di analisi si accorgano subito dell'attività sospetta.

#### 2. Windows Command Shell (T1059.003)

Questa è la specifica "lingua" usata per l'esecuzione su questo sistema.

- Dettaglio:** La shell di comando (cmd) è il prompt principale di Windows e può controllare quasi ogni aspetto del sistema.
- Utilizzo:** Gli attaccanti la usano per lanciare singoli comandi o file batch (.bat/.cmd) che eseguono lunghe sequenze di operazioni dannose in automatico.

- **Requisiti:** In questa analisi, l'attaccante opera con **permessi User** (utente standard), sufficienti per eseguire le operazioni di furto dati tipiche di un infostealer.

**Techniques details**

Get to know what this threat is about

Subtechniques ▾ T1059 Windows Command Shell ▾

● Warning (4)

**"Command and Scripting Interpreter"**

Permissions required:

Data sources:

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](#) while Windows installations include the Windows

**Techniques details**

Get to know what this threat is about

Subtechniques ▾ T1059.003 Windows Command Shell ▾

● Warning (4)

**"Windows Command Shell"**

Permissions required: User

Data sources:

Adversaries may abuse the Windows command shell for execution. The Windows command shell ([cmd](#)) is the primary command prompt on Windows systems. The Windows command prompt can be used to control almost any aspect of a system, with various permission levels required for different subsets of commands. The command prompt can be invoked remotely via [Remote Services](#) such as [SSH](#). (Citation: SSH in Windows) Batch files (ex: .bat or .cmd) also

- Uses [TIMEOUT.EXE](#) to delay execution (2)
  - 7520 cmd.exe (1)
  - 7876 cmd.exe (1)
- Starts [CMD.EXE](#) for commands execution (2)
  - 7492 Jvczfhe.exe (1)
  - 7824 Muadnrd.exe (1)

## Defense Evasion:

**Defense Evasion** (Evasione delle difese), ovvero il modo in cui il malware cerca di nascondersi dai sistemi di sicurezza e dall'utente. Nell'analisi di Any.Run, questa tattica è composta da due tecniche principali.

### 1. Masquerading (Mascheramento)

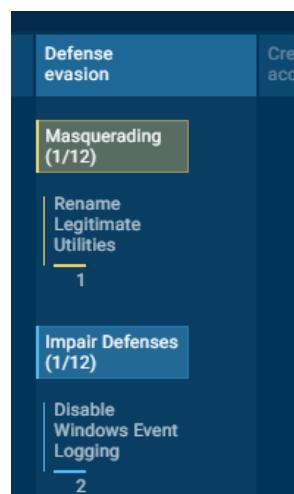
Questa tecnica (T1036) consiste nel manipolare gli artefatti del malware per farli apparire legittimi o innocui agli occhi dell'utente e degli strumenti di sicurezza.

- **Rename Legitimate Utilities (T1036.003):** Gli avversari rinominano utility di sistema legittime per tentare di evadere i meccanismi di sicurezza che monitorano l'uso di tali strumenti.
- **Azione rilevata:** Il processo firefox.exe (PID 6596) ha "droppato" (rilasciato nel sistema) un eseguibile Windows legittimo. Questo serve a confondere le acque: se un analista vede un file con un nome familiare, potrebbe non sospettare che sia parte di una catena di attacco.

### 2. Impair Defenses (Compromissione delle difese)

Oltre a nascondersi, il malware cerca attivamente di "azzoppare" le capacità di monitoraggio del computer.

- **Disable Windows Event Logging:** In questa specifica esecuzione, è stata rilevata la sottomossa per disabilitare i log degli eventi di Windows.
- **Perché lo fa:** Senza i log di sistema, non rimane traccia delle azioni compiute dal malware (come l'avvio di nuovi processi o modifiche al registro). Questo rende l'analisi forense post-incidente estremamente difficile per un team di Blue Teaming.



## Discovery: Query Registry ()

La tattica di **Discovery** (T1082 e T1012) rappresenta la fase in cui il malware "studia" l'ambiente in cui si trova per capire se è una vittima di valore o se è in una sandbox di analisi.

### 1. Query Registry (T1012)

Il malware interroga attivamente il Registro di Windows per raccogliere dati sul sistema. In questa analisi, i processi malevoli hanno eseguito queste operazioni:

- **Lettura del GUID della macchina:** Un identificativo unico per tracciare la vittima nei database degli attaccanti.
- **Lettura del nome del computer:** Utilizzato per profilare l'utente e il sistema.
- **Controllo delle lingue supportate:** Spesso gli infostealer controllano la lingua (es. russo, ucraino) per interrompere l'infezione se rilevano paesi che non intendono colpire.
- **Processi coinvolti:** Questa attività è stata compiuta da Jvczfhe.exe, InstallUtil.exe e Muadnrd.exe.

## System Information Discovery (T1082)

Questa tecnica serve per ottenere dettagli tecnici sull'hardware e sul software del PC vittima.

- **Dati raccolti:** Include versioni del sistema operativo, architettura della CPU (32 o 64 bit), quantità di RAM e patch di sicurezza installate.
- **Obiettivo:** Queste informazioni aiutano l'attaccante a personalizzare le fasi successive dell'attacco (es. decidere quale tipo di malware per il furto di password inviare successivamente).
- **Evidenze:** Sono stati registrati **15 eventi** legati alla scoperta di informazioni di sistema.

**Techniques details**  
Get to know what this threat is about

**T1012**  
**"Query Registry"**

**Permissions required:** User, Administrator, SYSTEM

**Data sources:**

Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software.

The Registry contains a significant amount of information about the operating system, configuration, software, and security. (Citation: Wikipedia Windows Registry)

Information can easily be queried using the [Reg](#) utility, though other means to access the Registry exist. Some of the information may help

- Reads the machine GUID from the registry (4)
  - 7492 Jvczfhe.exe (1)
  - 5152 InstallUtil.exe (1)
  - 7824 Muadnrd.exe (1)
  - 7248 Muadnrd.exe (1)
- Reads the computer name (4)
  - 7492 Jvczfhe.exe (1)
  - 5152 InstallUtil.exe (1)
  - 7824 Muadnrd.exe (1)
  - 7248 Muadnrd.exe (1)
- Checks supported languages (4)
  - 7492 Jvczfhe.exe (1)
  - 5152 InstallUtil.exe (1)
  - 7824 Muadnrd.exe (1)
  - 7248 Muadnrd.exe (1)

• Warning (4) • Other (50)

## Command & Control: Non-Standard Port ()

La fase di **C&C (Command and Control)** è il momento in cui il malware stabilisce un canale di comunicazione con l'attaccante per ricevere istruzioni o esfiltrare i dati rubati dal tuo sistema.

### 1. Non-Standard Port (T1571)

Questa tecnica consiste nell'utilizzare porte di comunicazione diverse da quelle canoniche (come la 80 per HTTP o la 443 per HTTPS) per passare inosservato ai firewall meno avanzati.

- **Azione Rilevata:** Il processo **InstallUtil.exe (PID 5152)** ha effettuato una connessione verso l'esterno utilizzando una porta non standard.
- **Scopo:** Gli attaccanti modificano le porte standard utilizzate dai protocolli per bypassare i filtri di rete o confondere l'analisi del traffico. Ad esempio, potrebbero far transitare traffico malevolo su porte normalmente ignorate dai controlli di sicurezza.

## 2. Indicatori di Rete (Network Threats)

Dalla schermata principale della sandbox, possiamo vedere l'attività di rete sospetta collegata a questa tattica:

- **DNS sospetti:** Sono state rilevate query DNS verso domini \*.duckdns.org.
- **Alert IDS:** Il sistema ha generato avvisi per "Potentially Bad Traffic" relativi a questi domini di Dynamic DNS, spesso usati come infrastruttura C&C temporanea dai criminali.

**Techniques details**

Get to know what this threat is about

● Warning

<p><a href="#">T1571</a></p> <p><b>"Non-Standard Port"</b></p> <p>Permissions required:</p> <p>Data sources:</p> <p>Adversaries may communicate using a protocol and port pairing that are typically not associated. For example, HTTPS over port 8088(Citation: Symantec Elfin Mar 2019) or port 587(Citation: Fortinet Agent Tesla April 2018) as opposed to the traditional port 443. Adversaries may make changes to the standard port used by a protocol to bypass filtering or muddle analysis/parsing of network data. Adversaries may also make changes to victim systems to abuse non-standard ports. For example,</p>	<ul style="list-style-type: none"> <li>● Connects to unusual port (1)</li> </ul> <p>5152 InstallUtil.exe (1)</p>
---	--

## CONCLUSIONE

### La Prima Ondata

The screenshot displays the analysis of the process [7492] Jvczfhe.exe. Key findings include:

- Main Information:** Code signing is Untrusted, and there are 0 process dumps.
- Threat Verdict:** Suspicious (51 OUT OF 100).
- Timeline of the process:** Shows events at 0 s, 22.10 s, and 62.16 s, with a note that the application crashes at 22.10 s.
- Process information:** Username: admin, SID: S-1-5-21-1693682860-607145093-2874071422-1001, IL: Microsoft Edge, Start: 22.10 s.
- File information:** Company: Microsoft Corporation, Description: Microsoft Edge, Version: 126.0.2592.113.
- Command line:** C:\Users\admin\Downloads\Jvczfhe.exe
- Other Threats:**
  - T1031 Query Registry (2): Reads security settings of Internet Explorer, Checks Windows Trust Settings.
  - T1059.005 Windows Command Shell (1): Starts CMD.EXE for commands execution.
  - T1011 Query Registry (6): Reads the software policy settings, Checks proxy server information, Reads Environment values, Reads the machine GUID from the registry, Reads the computer name, Checks supported languages.
  - T1561.002 Disable Windows Event Logging (1): Disables trace logs.
  - T1082 System Information Discovery (4): Reads Environment values, Reads the machine GUID from the registry, Reads the computer name, Checks supported languages.
- Running Processes:** A list on the left shows several processes, with [7492] Jvczfhe.exe and [7520] Cmd.exe being the most prominent.

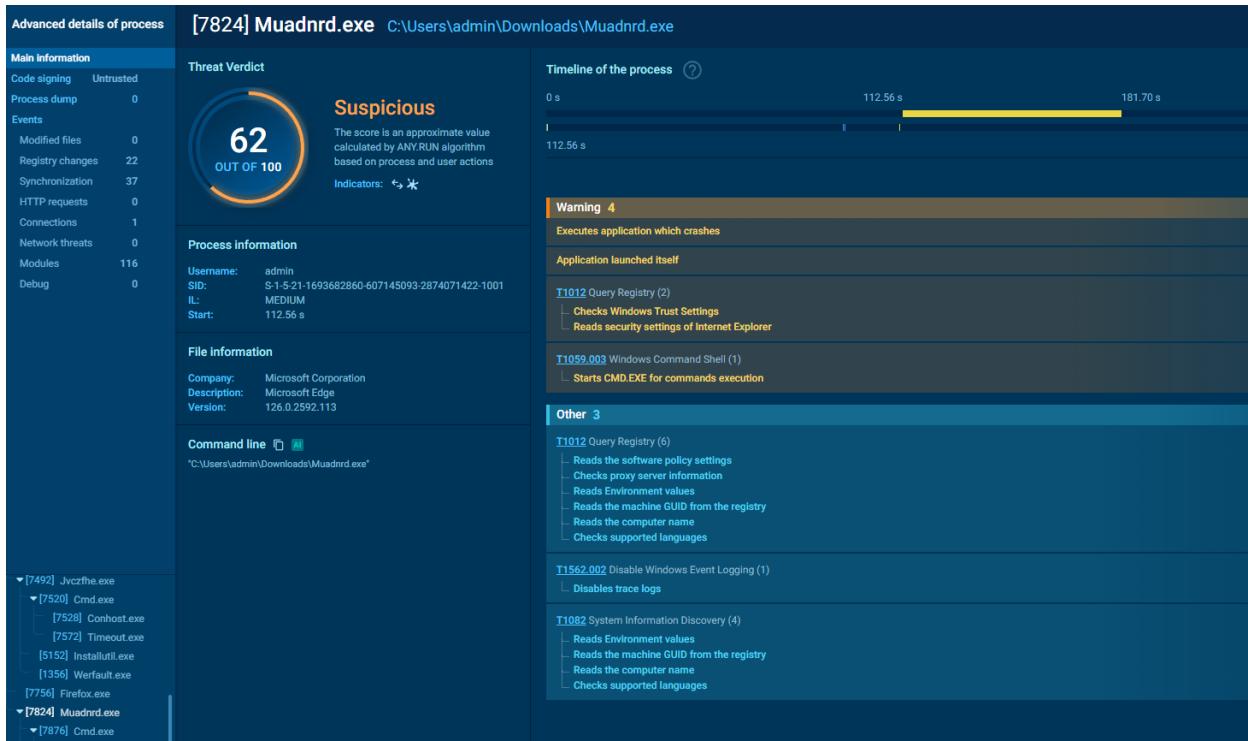
**Jvczfhe.exe:** È il primo file eseguito dopo il download. Come abbiamo visto negli screenshot , è questo processo a generare il finto messaggio di errore per ingannare l'utente.

### Esecuzione e Mascheramento (Execution & Evasion)

Il malware non agisce da solo, ma crea dei "figli" per compiere il lavoro sporco:

- **cmd.exe:** Viene avviato da jvczfhe.exe per eseguire comandi di sistema. Da qui vedi nascere timeout.exe, usato per ritardare l'attacco e confondere l'analisi.
- **installutil.exe (THREAT):** Questo è un punto critico. Il malware abusa di un'utilità legittima di Windows per caricare il codice malevolo. Essendo un processo "fidato" di Microsoft, serve a bypassare i controlli dell'antivirus (**Masquerading**).

## La Seconda Ondata



- Muadnrd.exe (THREAT):** Un altro processo malevolo che si attiva in parallelo.
- Anche questo avvia la sua istanza di cmd.exe e timeout.exe per gestire la propria esecuzione in modo furtivo.

## Attività Post-Infezione (Discovery)

Mentre questi processi sono attivi, l'albero mostra che stanno effettuando operazioni di **Discovery**:

- Leggono il **GUID della macchina** e il **nome del computer** dal registro.
- Controllano le **lingue supportate** dal sistema.
- Tentano di disabilitare i log (Disable Windows Event Logging) per non lasciare tracce del loro passaggio.

**Identificazione Univoca (Hashes):** Questi codici rappresentano l'impronta digitale del malware. In un contesto aziendale, verrebbero utilizzati per scansionare l'intera rete alla ricerca di file identici.

- **MD5:** 00B5E91B42712471CDFBDB37B715670C
- **SHA1:** D9550361E5205DB1D2DF9D02CC7E30503B8EC3A2
- **SHA256:**  
0307EE805DF8B94733598D5C3D62B28678EAEBF1CA3689FA678A3780DD3DF0  
D3DF0

## General Info

---

URL:	<a href="https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe">https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe</a>
Full analysis:	<a href="https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281">https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281</a>
Verdict:	Malicious activity
Analysis date:	August 25, 2024 at 22:38:59
OS:	Windows 10 Professional (build: 19045, 64 bit)
Tags:	<a href="#">github</a> <a href="#">netreactor</a>
Indicators:	
MD5:	00B5E91B42712471CDFBDB37B715670C
SHA1:	D9550361E5205DB1D2DF9D02CC7E30503B8EC3A2
SHA256:	0307EE805DF8B94733598D5C3D62B28678EAEBF1CA3689FA678A3780DD3DF0
SSDeep:	3:N8tEd7QyQ3FJMERCNuN:2uRQyQ3zMsCNa

## Indicatori di Rete (C&C)

Durante l'esecuzione, entrambi i processi principali hanno stabilito connessioni verso l'esterno per comunicare con l'infrastruttura dell'attaccante:

- **IP di Destinazione:** 185.199.110.133
- **Porta:** 443 (HTTPS)
- **ASN:** FASTLY
- **Dettaglio:** La connessione avviene verso domini GitHub (usati come repository per il payload o per l'esfiltrazione).

Advanced details of process		[7492] Jvczfhe.exe C:\Users\admin\Downloads\Jvczfhe.exe								
		Put the slider in the desired position or select the desired segment by yourself <a href="#">?</a>								
		22.105 s								
		Time	Type	Rep	CN	Src IP	Port	Dst IP	Port	ASN
Main information		+21956 ms	TCP	?		185.199.110.133	443	VM	49790	FASTLY
Events										
Modified files		0								
Registry changes		23								
Synchronization		37								
HTTP requests		0								
Connections		1								

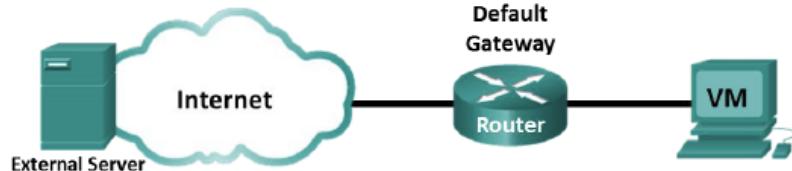
Advanced details of process		[7824] Muadnrd.exe C:\Users\admin\Downloads\Muadnrd.exe								
		Put the slider in the desired position or select the desired segment by yourself <a href="#">?</a>								
		112.567 s								
		Time	Type	Rep	CN	Src IP	Port	Dst IP	Port	ASN
Main information		+20754 ms	TCP	?		185.199.110.133	443	VM	59019	FASTLY
Events										
Modified files		0								
Registry changes		22								
Synchronization		37								
HTTP requests		0								
Connections		1								

## Firma Digitale Falsa

Il malware tenta di apparire legittimo dichiarando di appartenere a **Microsoft Corporation**. Tuttavia, l'analisi del certificato mostra un verdetto di **Untrusted** poiché la catena di certificati è stata revocata.

# Bonus 1: Esplorazione e Utilizzo Pratico di Nmap per la Ricognizione di Rete

## 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

```

File Edit View Terminal Tabs Help
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
    characteristics. While Nmap is commonly used for security audits, many
    systems and network administrators find it useful for routine tasks such
    as network inventory, managing service upgrade schedules, and monitoring
    host or service uptime.

    The output from Nmap is a list of scanned targets, with supplemental
    information on each depending on the options used. Key among that
    information is the "interesting ports table". That table lists the port
    number and protocol, service name, and state. The state is either open,
    filtered, closed, or unfiltered. Open means that an application on the
    target machine is listening for connections/packets on that port.
    Filtered means that a firewall, filter, or other network obstacle is
    blocking the port so that Nmap cannot tell whether it is open or closed.
    Closed ports have no application listening on them, though they could
    open up at any time. Ports are classified as unfiltered when they are
    responsive to Nmap's probes, but Nmap cannot determine whether they are
    open or closed. Nmap reports the state combinations open|filtered and
    closed|filtered when it cannot determine which of the two states
    describe a port. The port table may also include software version
    details when version detection has been requested. When an IP protocol
    scan is requested (-S0), Nmap provides information on supported IP
    protocols rather than listening ports.

    In addition to the interesting ports table, Nmap can provide further
    information on targets, including reverse DNS names, operating system
    guesses, device types, and MAC addresses.

  
```

## 1. COS'È NMAP?

Nmap (abbreviazione di Network Mapper) è un **tool open source** fondamentale per chiunque operi nel networking o nella sicurezza informatica. È essenzialmente uno scanner di rete che "interroga" i dispositivi inviando pacchetti IP per ottenere informazioni sulla loro configurazione e sul loro stato.

## 2. PER COSA VIENE USATO NMAP?

Basandosi sulla descrizione, Nmap viene utilizzato principalmente per due scopi:

1. **Security Auditing & Pentesting:** Per identificare vulnerabilità, rilevare host attivi, mappare i servizi esposti e identificare versioni software vulnerabili o firewall presenti.
2. **Amministrazione di Rete:**
  - o Effettuare l'inventario dei dispositivi connessi.
  - o Monitorare se un server o un servizio è "up" (attivo) o "down".
  - o Gestire i cicli di aggiornamento (verificando quali macchine eseguono ancora vecchie versioni di un servizio).

```

File Edit View Terminal Tabs Help
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 ldp
1720/tcp  filtered H.323/Q.931
9929/tcp  open     nping-echo  Nping echo
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.39
OS details: Linux 2.6.39
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
[Cut first 10 hops for brevity]
11 17.65 ms li86-221.members.linode.com (74.207.244.221)

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds

The newest version of Nmap can be obtained from https://nmap.org. The newest version of this man page is available at
https://nmap.org/book/man.html. It is also included as a chapter of Nmap Network Scanning: The Official Nmap Project Guide to Network
Discovery and Security Scanning (see https://nmap.org/book/).
```

**OPTIONS SUMMARY**

### 3. QUAL È IL COMANDO NMAP USATO?

il comando Nmap utilizzato è il seguente:

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

### 4. COSA FA L'OPZIONE -A?

```
-A: Enable OS detection, version detection, script scanning, and traceroute
```

- **-A**: Abilita diverse funzioni avanzate contemporaneamente, tra cui il rilevamento del sistema operativo (OS detection), la rilevazione della versione dei servizi, la scansione tramite script (NSE) e il traceroute.

### 5. COSA FA L'OPZIONE -T4?

l'opzione **-T4** serve a impostare un modello di tempistica (**timing template**) per rendere la scansione più rapida.

```
-T paranoid|sneaky|polite|normal|aggressive|insane (Set a timing template)
While the fine-grained timing controls discussed in the previous section are powerful and effective, some people find them confusing. Moreover, choosing the appropriate values can sometimes take more time than the scan you are trying to optimize. Fortunately, Nmap offers a simpler approach, with six timing templates. You can specify them with the -T option and their number (0-5) or their name. The template names are paranoid (0), sneaky (1), polite (2), normal (3), aggressive (4), and insane (5). The first two are for IDS evasion. Polite mode slows down the scan to use less bandwidth and target machine resources. Normal mode is the default and so -T3 does nothing. Aggressive mode speeds scans up by making the assumption that you are on a reasonably fast and reliable network. Finally insane mode assumes that you are on an extraordinarily fast network or are willing to sacrifice some accuracy for speed.

These templates allow the user to specify how aggressive they wish to be, while leaving Nmap to pick the exact timing values. The templates also make some minor speed adjustments for which fine-grained control options do not currently exist. For example, -T4 prohibits the dynamic scan delay from exceeding 10 ms for TCP ports and -T5 caps that value at 5 ms. Templates can be used in combination with fine-grained controls, and the fine-grained controls that you specify will take precedence over the timing template default for that parameter. I recommend using -T4 when scanning reasonably modern and reliable networks. Keep that option even when you add fine-grained controls so that you benefit from those extra minor optimizations that it enables.

If you are on a decent broadband or ethernet connection, I would recommend always using -T4. Some people love -T5 though it is too aggressive for my taste. People sometimes specify -T2 because they think it is less likely to crash hosts or because they consider themselves to be polite in general. They often don't realize just how slow -T1 polite really is. Their scan may take ten times longer than a default scan. Machine crashes and bandwidth problems are rare with the default timing options (-T3) and so I normally recommend that for cautious scanners. Omitting version detection is far more effective than playing with timing values at reducing these problems.

While -T0 and -T1 may be useful for avoiding IDS alerts, they will take an extraordinarily long time to scan thousands of machines or ports. For such a long scan, you may prefer to set the exact timing values you need rather than rely on the canned -T0 and -T1 values.

The main effects of T0 are serializing the scan so only one port is scanned at a time, and waiting five minutes between sending each probe. T1 and T2 are similar but they only wait 15 seconds and 0.4 seconds, respectively, between probes. T3 is Nmap's default behavior, which includes parallelization. T4 does the equivalent of
--max-rtt-timeout 1250ms --min-rtt-timeout 100ms --initial-rtt-timeout 500ms --max-retries 6 and sets the maximum TCP and SCTP scan delay to 10ms. T5 does the equivalent of
--max-rtt-timeout 300ms --min-rtt-timeout 50ms --initial-rtt-timeout 250ms --max-retries 2 --host-timeout 15m --script-timeout 10m as well as setting the maximum TCP and SCTP scan delay to 5ms. Maximum UDP scan delay is not set by T4 or T5, but it can be set with the --max-scan-delay option.
```

In base alla documentazione fornita nell'immagine, ecco cosa dice specificamente la descrizione riguardo all'opzione **-T4**:

- **Definizione:** L'opzione -T4 corrisponde al modello di tempistica denominato "aggressive".
- **Velocità e Affidabilità:** Questa impostazione accelera le scansioni partendo dal presupposto che l'utente stia operando su una rete ragionevolmente moderna, veloce e affidabile.
- **Ottimizzazioni Tecniche:** L'uso di -T4 impedisce al ritardo dinamico della scansione (*dynamic scan delay*) di superare i **10 ms** per le porte TCP.
- **Raccomandazioni d'uso:** Viene consigliato l'uso di -T4 se si dispone di una connessione a banda larga o ethernet decente, poiché è meno probabile che causi il crash degli host o problemi di larghezza di banda rispetto alla modalità -T5 ("insane").

l'opzione **-T4** serve a impostare un modello di tempistica (**timing template**) per rendere la scansione più rapida.

---

## 6. QUALI PORTE E SERVIZI SONO APERTI?

### Porte e Servizi Aperti

Dalla tabella dei risultati si vedono chiaramente due porte nello stato **open**:

- **Porta 21/tcp:** Il servizio associato è **ftp**.
- **Porta 22/tcp:** Il servizio associato è **ssh**.

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-19 12:02 -0500
Failed to resolve "-A".
Failed to resolve "-T4".
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000023s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
```

---

## 7. A QUALE RETE APPARTIENE LA TUA VM?

In base all'output del comando ip address che ho appena lanciato sul mio terminale, ecco i dettagli della rete a cui appartiene la mia VM:

La mia VM appartiene alla rete **10.0.2.0/24**.

Ecco come ho ricavato i dati dall'interfaccia enp0s3:

- **Indirizzo IPv4:** Il mio indirizzo IP specifico è 10.0.2.15.
- **Subnet Mask:** La notazione /24 indica una maschera di sottorete 255.255.255.0.
- **Indirizzo di Broadcast:** Il broadcast per questa rete è 10.0.2.255.

Inoltre, vedo l'interfaccia di loopback (lo) con il classico indirizzo 127.0.0.1/8, che sto usando per i test locali su Nmap.

```
[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 85028sec preferred_lft 85028sec
    inet6 fd17:625c:f037:2:a00:27ff:fe2f:87a7/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86236sec preferred_lft 14236sec
    inet6 fe80::a00:27ff:fe2f:87a7/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
```

---

## 8. QUANTI HOST SONO ATTIVI?

Non ci sono host Attivi

---

## 9. QUAL È LO SCOPO DI QUESTO SITO?

Lo scopo di **scanme.nmap.org** è fornire un bersaglio autorizzato per testare e imparare a usare lo scanner Nmap. Il sito serve per aiutare gli utenti a verificare che la propria installazione di Nmap funzioni correttamente e per fare pratica con le varie opzioni di scansione senza rischiare di violare sistemi privati o non autorizzati.

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-20 10:53 -0500
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.17s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 997 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-favicon: Nmap Project
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
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 29.54 seconds
```

## 10. QUALI PORTE E SERVIZI SONO APERTI?

### Porte e servizi aperti

Le porte nello stato **open** e i relativi servizi/software sono:

- **22/tcp**: Servizio **ssh** (Software: OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13).
- **53/tcp**: Servizio **domain** (Software: dnsmasq 2.84).
- **80/tcp**: Servizio **http** (Software: Apache httpd 2.4.7).

## 11. QUALI PORTE E SERVIZI SONO FILTRATI?

### Porte e servizi filtrati

- Nmap segnala che ci sono **997 porte filtrate** (stato filtered) che non hanno fornito risposta (*no-response*). I servizi specifici per queste porte non vengono elencati individualmente nell'output sintetico.
- 

## 12. QUAL È L'INDIRIZZO IP DEL SERVER?

### Indirizzo IP del server

- L'indirizzo IP rilevato per scanme.nmap.org è **45.33.32.156**
- 

## 13. QUAL È IL SISTEMA OPERATIVO?

### Sistema Operativo

- Il sistema operativo rilevato è **Linux**.
  - Nmap specifica inoltre che si tratta di una distribuzione basata su kernel Linux (CPE: cpe:/o:linux:linux\_kernel).
- 

## 13. DOMANDE DI 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?**

### Il lato "buono": La difesa e la gestione

Per noi che lavoriamo sulla protezione dei sistemi, Nmap è un alleato incredibile. Ci permette di:

- **Capire cosa abbiamo "in casa"**: Spesso in reti grandi non si sa nemmeno quanti dispositivi siano collegati; Nmap ci aiuta a fare un inventario preciso.
- **Vedere cosa vede un hacker**: Facendo una scansione, scopriamo quali porte sono aperte (come la 21 per l'FTP o la 22 per l'SSH che abbiamo visto prima) e se stiamo usando versioni software vecchie e vulnerabili.
- **Controllare i firewall**: Ci dice se una porta è "filtered", confermandoci che i nostri filtri di rete stanno effettivamente bloccando il traffico indesiderato.

- **Manutenzione:** È utilissimo per monitorare l'uptime dei server o capire quando è il momento di aggiornare un servizio che è rimasto indietro.

### Il lato "oscuro": L'uso malevolo

Purtroppo, le stesse funzioni che usiamo per difenderci possono essere usate da un malintenzionato per farci del male:

- **Ricognizione (Footprinting):** Un attaccante usa Nmap come prima mossa per mappare la rete vittima, capire che sistemi operativi usiamo e trovare la "porta lasciata aperta".
  - **Precisione chirurgica:** Sapere che versione esatta di Apache o OpenSSH stai usando (come abbiamo visto nell'output di scanme.nmap.org) permette a un hacker di cercare l'exploit perfetto su database come Exploit-DB.
  - **Furtività:** Un attore malevolo esperto non userebbe mai -T4 (che è troppo rumoroso e facile da beccare dai sistemi IDS), ma sceglierrebbe modalità molto lente come -To o -T1 per muoversi nell'ombra, scansionando una porta ogni tanto per non far scattare gli allarmi.
-

## Bonus 2 : Analisi Forense di un Attacco di SQL Injection su Database MySQL

### Obiettivi

In questo laboratorio, visualizzare un file PCAP di un attacco precedente contro un database MySQL.

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

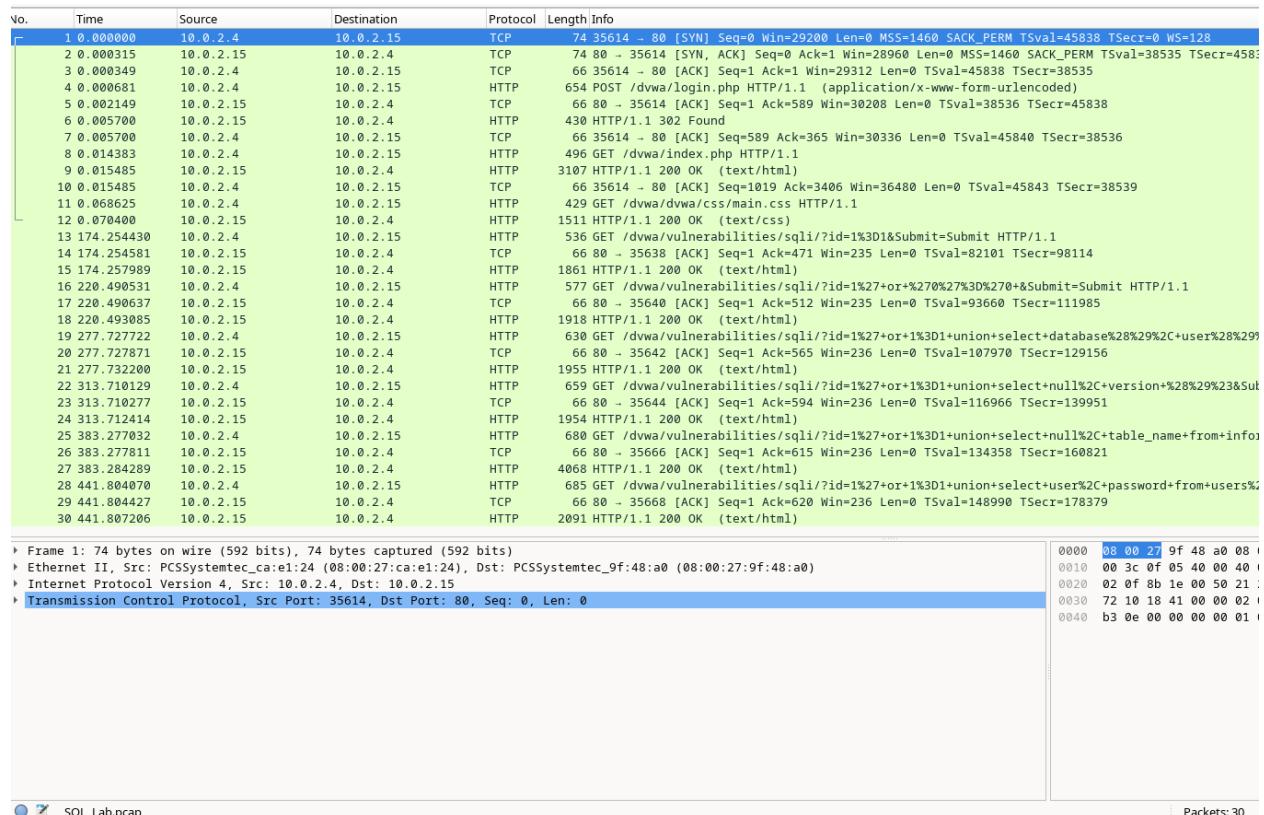
Parte 6: L'attacco di SQL Injection si conclude.

### 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 MySQL. In questo laboratorio, visualizzerai gli attacchi al database MySQL e risponderai alle domande.

**Risorse Richieste** -> Macchina virtuale CyberOps Workstation

Il file PCAP si apre in Wireshark e visualizza il traffico di rete catturato. Questo file di cattura si estende per un periodo di 8minuti ✓ 441 secondi), la durata di questo attacco di SQL injection.



## 1. QUALI SONO I DUE INDIRIZZI IP COINVOLTI IN QUESTO ATTACCO DI SQL INJECTION IN BASE ALLE INFORMAZIONI VISUALIZZATE?

indirizzi IP coinvolti nell'attacco sono i seguenti:

- **10.0.2.4**: Questo è l'indirizzo IP della **sorgente** (l'aggressore) che invia le richieste GET contenenti le istruzioni SQL malevole.
- **10.0.2.15**: Questo è l'indirizzo IP della **destinazione** (la vittima), ovvero il server che ospita l'applicazione vulnerabile e il database SQL.

## 2.QUAL È LA VERSIONE?

**Risultato ottenuto:** Il database ha risposto con la stringa **5.7.12-0ubuntu1.1**.

**Significato:** Si tratta di una **versione di MySQL** (o un fork compatibile) in esecuzione su un sistema operativo Ubuntu.

Sebbene il nome del sistema operativo appaia nella stringa restituita, l'obiettivo primario dell'attaccante in questa fase dell'esercizio è identificare esattamente quale versione del database stia girando per poter cercare exploit specifici per quel servizio

## 3.COSA FAREBBE PER L'AGGRESSORE IL COMANDO MODIFICATO DI (1' OR 1=1 UNION SELECT NULL, COLUMN\_NAME FROM INFORMATION\_SCHEMA.COLUMNS WHERE TABLE\_NAME='USERS')?

Il comando estraе i **nomi delle colonne** (la struttura) della tabella **users**. Questo è un passaggio fondamentale per l'attaccante: prima di rubare i dati, deve conoscere come si chiamano i campi (es. user, password, email) per poter poi formulare la query finale di esfiltrazione.

## 4.QUALE UTENTE HA L'HASH DELLA PASSWORD DI 8D3533D75AE2C3966D7E0D4FCC69216B?

```
<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: 0d107d09f5bbe40cade3de5c71e9e9b7</pre>
<pre>ID: 1' or 1=1 union select user, password from users<br />First name: smithy<br />Surname: 5f4dcc3b5aa765d61d8327deb882cf99</pre>
```

Riordinando il codice html si e' scoperto che nella corrispondenza dell'hash il nome utente e' **1337**

## 5.QUAL È LA PASSWORD IN CHIARO?

Usando un sito web come <https://crackstation.net/>, viene decifrato l'hash della password con il cracker di hash :

Hash	Type	Result
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley

## DOMANDE DI RIFLESSIONE:

### 6. QUAL È IL RISCHIO CHE LE PIATTAFORME UTILIZZINO IL LINGUAGGIO SQL?

il rischio principale per le piattaforme che utilizzano il linguaggio SQL (poiché i siti web sono comunemente basati su database) è la vulnerabilità agli attacchi di **SQL injection**. I rischi specifici che ne derivano includono:

- La falsificazione delle identità e il furto di credenziali.
- Il compimento di varie altre azioni dannose sul sistema
- La manomissione e l'alterazione dei dati correnti presenti nel database.

### 7. 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?

The **OWASP Cheat Sheet Series** was created to provide a concise collection of high value information on specific application security topics. These cheat sheets were created by various application security professionals who have expertise in specific topics.

The screenshot shows a dark-themed web interface for the OWASP Cheat Sheet Series. At the top, there are navigation links for 'File', 'Container', 'Trainee', and 'To Do | Board'. The main title 'OWASP Cheat Sheet Series' is displayed next to a logo. On the right side, there is a search bar with a magnifying glass icon. The main content area features a sidebar with a tree-like navigation menu. Under the 'OWASP Cheat Sheet Series' heading, the 'SQL Injection Prevention Cheat Sheet' is selected. The main content area contains an 'Introduction' section with text explaining the purpose of the sheet and listing two methods for prevention:

This cheat sheet will help you prevent SQL injection flaws in your applications. It will define what SQL injection is, explain where those flaws occur, and provide four options for defending against SQL injection attacks. **SQL Injection attacks are common because:**

1. SQL Injection vulnerabilities are very common, and
2. The application's database is a frequent target for attackers because it typically contains interesting/critical data.

To avoid SQL injection flaws, developers need to:

1. Stop writing dynamic queries with string concatenation or
2. Prevent malicious SQL input from being included in executed queries.