



EPICODE

Laboratorio day 5 -Cisco CyberOps e any.run

By Xian Long Qiu

Panoramica

Scopo

Questa esercitazione ha lo scopo di esplorare funzioni **PowerShell** utili in contesto forense e di analizzare comportamenti malevoli di un file caricato sulla piattaforma **Any.run**, allo scopo di identificare **indicatori di compromissione (IoC)**, **tecniche di evasione**, e **comandi sospetti**.

Bonus

Durante l'esercitazione sono state svolte attività integrative per approfondire la sicurezza delle reti e delle applicazioni:

- Scansione con **Nmap** sulla macchina CyberOps Workstation per rilevare servizi attivi, porte aperte e informazioni di sistema.
- Simulazione di **attacchi SQL Injection** per analizzare vulnerabilità nei form di input e comprendere come gli attaccanti possano estrarre dati sensibili.



Strumenti



-[PowerShell](#) è una shell a riga di comando avanzata e un linguaggio di scripting sviluppato da Microsoft, progettato per l'automazione delle attività di amministrazione e la gestione dei sistemi Windows.



-[Any.run](#) è una sandbox interattiva online che consente di analizzare il comportamento di file sospetti o URL in tempo reale all'interno di un sistema Windows simulato.



-[Nmap](#) è uno strumento di scansione rete che rileva host attivi, porte aperte e servizi in esecuzione. Viene usato per analizzare la sicurezza dei sistemi e identificare potenziali vulnerabilità.



-[Wireshark](#) è uno strumento per l'analisi del traffico di rete. Permette di catturare e ispezionare pacchetti in tempo reale per identificare problemi, anomalie o attività sospette sulla rete. È usato in ambito forense, sicurezza e troubleshooting.

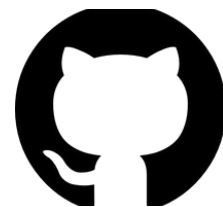


Origine traccia

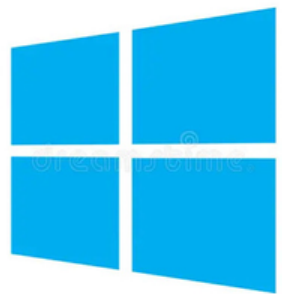
Il presente report è relativo al Modulo 3 - Settimana 3 lezione 5 del corso sulla piattaforma Epicode

Fonte

Repository <https://github.com/XLQcyber/CS0225>



Ambiente di lavoro



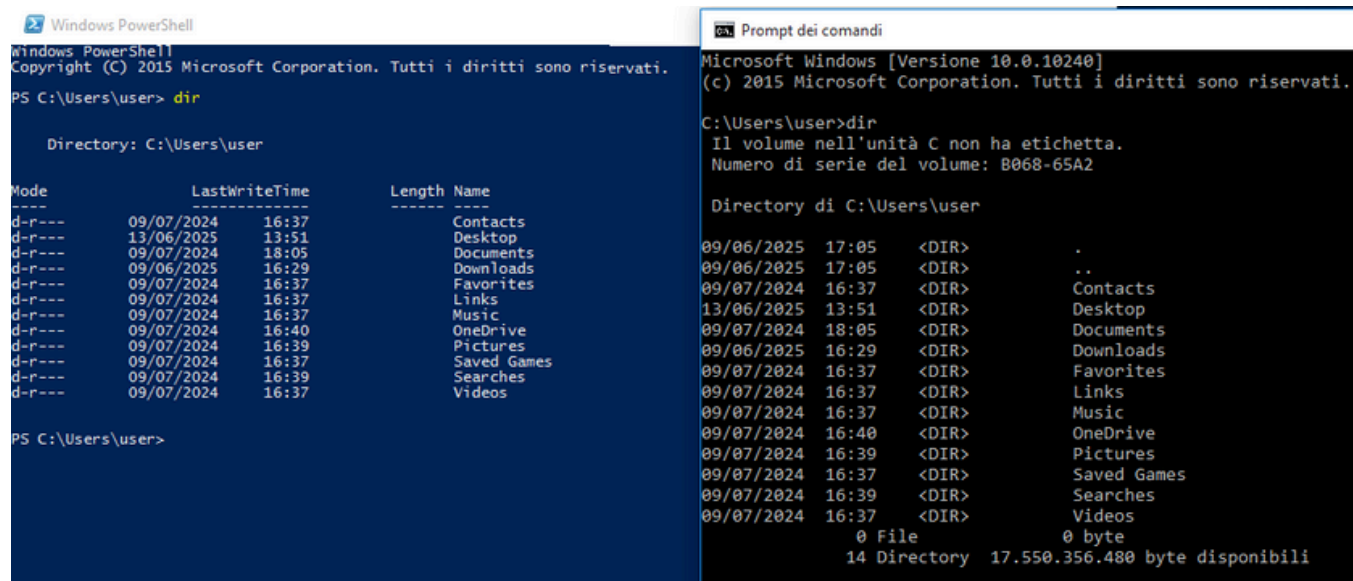
Windows 10 Pro è una versione del sistema operativo Microsoft pensata per ambienti professionali. Rispetto alla versione Home, include funzionalità avanzate per la sicurezza, la gestione dei dispositivi e l'amministrazione di rete. Tra le caratteristiche principali ci sono BitLocker per la crittografia, il supporto al dominio Active Directory, la virtualizzazione con Hyper-V e la gestione tramite criteri di gruppo (Group Policy). È particolarmente adatto per tecnici, amministratori di sistema e ambienti aziendali.



La Cisco CyberOps Workstation è una macchina virtuale progettata per la formazione e la simulazione in ambito cybersecurity operativa. Include strumenti e ambienti utili per esercitazioni di monitoraggio, analisi forense, gestione di incidenti e difesa delle reti.

Utilizzata in contesti didattici e professionali, permette di fare pratica su casi reali, sfruttando software come Wireshark, Nmap, PowerShell e piattaforme di analisi malware come Any.run.

PowerShell



The image shows two side-by-side terminal windows. The left window is Windows PowerShell, and the right is the Command Prompt. Both show the output of the 'dir' command in the C:\Users\user directory. PowerShell's output is a formatted table with columns for Mode, LastWriteTime, Length, and Name. The Command Prompt's output is a plain text list of files and directories with their dates, times, and names.

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

PS C:\Users\user> dir

Directory: C:\Users\user

Mode                LastWriteTime         Length Name
----                -
d-r--          09/07/2024   16:37             Contacts
d-r--          13/06/2025   13:51             Desktop
d-r--          09/07/2024   18:05             Documents
d-r--          09/06/2025   16:29             Downloads
d-r--          09/07/2024   16:37             Favorites
d-r--          09/07/2024   16:37             Links
d-r--          09/07/2024   16:37             Music
d-r--          09/07/2024   16:40             OneDrive
d-r--          09/07/2024   16:39             Pictures
d-r--          09/07/2024   16:37             Saved Games
d-r--          09/07/2024   16:39             Searches
d-r--          09/07/2024   16:37             Videos

PS C:\Users\user>
```

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

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

Directory di C:\Users\user

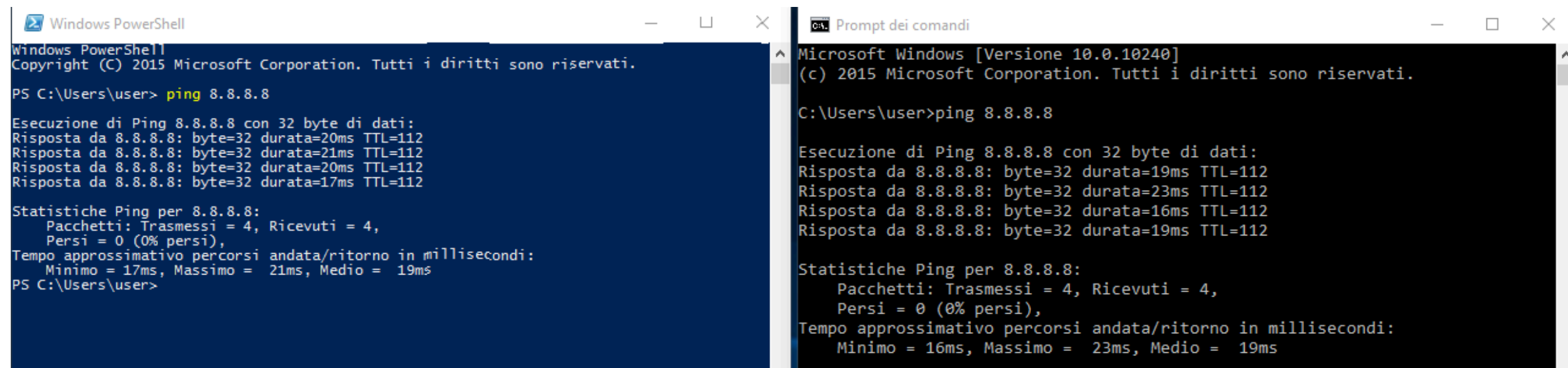
09/06/2025  17:05  <DIR>          .
09/06/2025  17:05  <DIR>          ..
09/07/2024  16:37  <DIR>          Contacts
13/06/2025  13:51  <DIR>          Desktop
09/07/2024  18:05  <DIR>          Documents
09/06/2025  16:29  <DIR>          Downloads
09/07/2024  16:37  <DIR>          Favorites
09/07/2024  16:37  <DIR>          Links
09/07/2024  16:40  <DIR>          Music
09/07/2024  16:39  <DIR>          OneDrive
09/07/2024  16:37  <DIR>          Pictures
09/07/2024  16:39  <DIR>          Saved Games
09/07/2024  16:39  <DIR>          Searches
09/07/2024  16:37  <DIR>          Videos
0 File              0 byte
14 Directory        17.550.356.480 byte disponibili
```

1. Output di dir:

- cmd dir: produce un output testuale semplice con data, ora, dimensione e nome dei file.
- PowerShell dir: restituisce un output in formato tabellare, con informazioni più dettagliate come permessi, data dell'ultima modifica, dimensione e nome.

In pratica, PowerShell restituisce un elenco più strutturato e ricco di informazioni rispetto al classico dir di cmd ed e' alias di dir.

2. L'output è uguale, ma in PowerShell il comando ping è un alias.



The image shows two side-by-side terminal windows. The left window is Windows PowerShell, and the right is the Command Prompt. Both show the output of the 'ping' command to 8.8.8.8. PowerShell's output is more detailed, showing individual response times and statistics. The Command Prompt's output is simpler, showing only the response times and statistics.

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

PS C:\Users\user> ping 8.8.8.8

Esecuzione di Ping 8.8.8.8 con 32 byte di dati:
Risposta da 8.8.8.8: byte=32 durata=20ms TTL=112
Risposta da 8.8.8.8: byte=32 durata=21ms TTL=112
Risposta da 8.8.8.8: byte=32 durata=20ms TTL=112
Risposta da 8.8.8.8: byte=32 durata=17ms TTL=112

Statistiche Ping per 8.8.8.8:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 17ms, Massimo = 21ms, Medio = 19ms
PS C:\Users\user>
```

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

C:\Users\user>ping 8.8.8.8

Esecuzione di Ping 8.8.8.8 con 32 byte di dati:
Risposta da 8.8.8.8: byte=32 durata=19ms TTL=112
Risposta da 8.8.8.8: byte=32 durata=23ms TTL=112
Risposta da 8.8.8.8: byte=32 durata=16ms TTL=112
Risposta da 8.8.8.8: byte=32 durata=19ms TTL=112

Statistiche Ping per 8.8.8.8:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 16ms, Massimo = 23ms, Medio = 19ms
```



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

3. Il comando del alias dir e' Get-ChildItem, è il cmdlet che elenca i file e le cartelle in una directory.

4. L'indirizzo IP del gateway predefinito è 192.168.208.147.

```
-r Visualizza la tabella di routing.
```

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

Elenco interfacce

3...08 00 27 84 66 35Intel(R) PRO/1000 MT Desktop Adapter
1.....Software Loopback Interface 1
5...00 00 00 00 00 00 00 e0	Microsoft ISATAP Adapter
4...00 00 00 00 00 00 00 e0	Microsoft Teredo Tunneling Adapter

```
=====
```

IPv4 Tabella route

```
=====
```

Route attive:

Indirizzo rete	Mask	Gateway	Interfaccia	Metrica
0.0.0.0	0.0.0.0	192.168.208.147	192.168.208.78	10



5. Ho selezionato il processo con PID 2188.

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

Connessioni attive

Proto	Indirizzo locale	Indirizzo esterno	Stato	PID
TCP	0.0.0.0:7	0.0.0.0:0	LISTENING	2188
[tcpsvcs.exe]				
TCP	0.0.0.0:9	0.0.0.0:0	LISTENING	2188

TCPSVCS.EXE	2188	In esecuzione	SERVIZIO L...	00	224 K	TCP/IP Services Application
-------------	------	---------------	---------------	----	-------	-----------------------------

Nella scheda Dettagli è possibile visualizzare informazioni quali stato, nome utente, utilizzo CPU, memoria fisica (RAM) e descrizione del processo.

Nella scheda Proprietà del processo si possono ottenere dettagli sul tipo di file, percorso, dimensioni, data di creazione, data di modifica, data di ultimo accesso, attributi, proprietario, versione e lingua.



6. Al file nel cestino vengono fornite opzioni per rimuovere o sospendere l'elemento, con una guida esplicativa. Ho scelto l'opzione "S" (sì) e il cestino è stato svuotato.

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





Riflessione Comandi per analista di sicurezza

1. 🎯 Ispezione dei processi e rilevamento malware

- Get-Process – Elenca i processi attivi, utile per individuare eseguibili sospetti.
- Get-CimInstance -Class Win32_Process | Select ProcessId,ProcessName,CommandLine – Mostra dettagli sul comando di avvio di ciascun processo.
- Stop-Process -Id <PID> – Termina processi malevoli .

2. 🌐 Reti e connessioni

- Get-NetTCPConnection – Visualizza connessioni TCP attive, equivalente moderno di netstat
- Get-NetUDPEndpoint – Elenca porte UDP in ascolto.

3. 📁 File e analisi cartelle

- Get-ChildItem -Recurse -Force – Scansiona ricorsivamente file e cartelle, anche nascosti

4. 📄 Eventi di sistema e auditing

- Get-WinEvent -LogName Security – Estrae i log di sicurezza, fondamentali per analisi.

5. 🛡️ Servizi, startup e persistenza

- Get-ItemProperty 'HKCU:\...\Run' e Get-ChildItem HKLM:\...\Run* – Controllo voci di autorun su registro
- Remove-ItemProperty – Elimina voci di persistenza (es. malware)



6. Controllo utenti, gruppi e condivisioni

- Get-LocalUser e Get-LocalGroupMember Administrators – Verifica account e autorizzazioni locali .
- Get-SmbShare – Elenco delle condivisioni SMB attive

7. Hash e integrità file

- Get-FileHash -Algorithm SHA256 – Calcola hash per verifica integrità dei file

8. Moduli e automazione

- Install-Module -Name PSSecurity, Invoke-SecurityScan – Estensioni per security assessment
- Invoke-Command, Enable-PSRemoting – Gestione remota su host multipli
- New-ScheduledTask – Per attivare i task automatizzati di sicurezza

Esercizio 2 any.run

Durante l'analisi del malware `jvczfhe.exe` su Any.run, è stato osservato che questo processo avvia un secondo eseguibile chiamato `muadnrd.exe`, il quale a sua volta attiva un **trojan horse** mascherato da processo legittimo di **Microsoft Edge**.

Il malware `jvczfhe.exe` ha tentato di stabilire una **connessione in uscita** verso l'indirizzo IP **91.92.253.47** sulla porta 5152 (porta non standard), ma il tentativo è **fallito**. Di conseguenza, ha eseguito il secondo file eseguibile, `muadnrd.exe`, che ha ripreso l'attacco usando tecniche di **DNS spoofing**. Nelle richieste DNS è stata identificata una richiesta sospetta verso il **dominio** `egehgdhjbhjtire.duckdns.org`, che risolve allo stesso IP **91.92.253.47**.

Nel contesto di `jvczfhe.exe` è stata rilevata anche l'esecuzione di `installutil.exe`, usato per interrogare il **registro di sistema** e recuperare informazioni come GUID e nome del computer (tecnica riconducibile alla matrice MITRE ATT&CK).

Un **processo figlio di** `muadnrd.exe` esegue la stessa interrogazione al registro di sistema vista in precedenza.

Tutti questi processi sono rimasti **inosservati** da antivirus e firewall grazie alla tecnica di **masquerading**, mascherando il proprio comportamento tramite l'esecuzione ritardata di `timeout.exe`, richiamato da `cmd.exe`.

Inoltre, i due eseguibili principali mostrano caratteristiche di **polimorfismo**, poiché il file scaricato non genera allarmi di pericolosità durante il download.

Bonus nmap

1. Nmap (Network Mapper) è uno strumento open source utilizzato per la scansione e l'analisi delle reti.
2. Nmap viene utilizzato principalmente per:
 - Scansione delle reti – per identificare host attivi e dispositivi collegati
 - Scansione delle porte – per rilevare quali porte TCP/UDP sono aperte su un sistema
 - Rilevamento dei servizi – per scoprire quali servizi (es. HTTP, SSH, FTP) sono in esecuzione e con quale versione
 - Identificazione del sistema operativo – per stimare quale OS è installato su un host remoto
 - Riconoscimento nella cybersecurity – per raccogliere informazioni preliminari durante attività di pentesting o analisi forense
 - Valutazione delle vulnerabilità – tramite script automatizzati del Nmap Scripting Engine (NSE)
3. Il comando nmap usato è `nmap -A -T4 scanme.nmap.org`



4. L'opzione -A abilita:

- Rilevamento del sistema operativo (OS fingerprinting)
- Rilevamento versione dei servizi in esecuzione sulle porte aperte
- Script scanning (usa Nmap Scripting Engine, NSE, per eseguire script di analisi)
- Traceroute per identificare il percorso di rete verso l'host

L'opzione -T4 di Nmap serve a impostare la velocità/aggressività della scansione su un livello "aggressive", cioè abbastanza veloce ma ancora affidabile.

5. Le porte aperte sono:

-21 ftp

-22 ssh

6. Indirizzo IP host: 192.168.208.16/24

Subnet mask: 255.255.255.0

7. Gli host attivi sono:

- 192.168.208.16 (la mia macchina)
- 192.168.208.147 con la porta 53 aperta (servizio DNS, hotspot telefonico)



8. Lo scopo principale è educativo: imparare a usare Nmap in modo legale e sicuro, verificare il funzionamento della propria installazione di Nmap e avere un esempio reale di host con porte aperte.

9.1 Le porte aperte sono 22 ssh, 80 http, 9929 nping-echo e 31337 tcpwrapped.

9.2 Non ci sono le porte filtrate.

9.3 L'indirizzo del server è 45.33.32.156.

9.4 Il sistema operativo è linux.



Riflessione nmap

🛡 Come può Nmap aiutare con la **sicurezza della rete**?

Nmap è uno strumento fondamentale per gli amministratori di sistema e i professionisti della cybersecurity perché consente di:

1. **Identificare dispositivi e servizi attivi nella rete**

→ Utile per mantenere un inventario aggiornato e rilevare dispositivi non autorizzati.

2. **Verificare le porte aperte e i servizi esposti**

→ Aiuta a rilevare configurazioni errate o servizi inutili che andrebbero disattivati.

3. **Analizzare vulnerabilità note**

→ Grazie all'Nmap Scripting Engine (NSE), è possibile eseguire script di analisi specifici per cercare versioni vulnerabili di software o configurazioni deboli.

4. **Effettuare controlli periodici**

→ Le scansioni regolari permettono di rilevare cambiamenti sospetti o non autorizzati nella rete



💀 Come può Nmap essere usato da un **attore malevolo**?

Dall'altro lato, Nmap è anche uno degli strumenti più usati dagli attaccanti nella fase di ricognizione (**recon**), ovvero:

1. Mappare la rete target

→ Un attore malevolo può identificare l'architettura della rete, gli host attivi e i servizi disponibili.

2. Rilevare porte e versioni dei software

→ Informazioni utili per pianificare attacchi mirati, come exploit su versioni vulnerabili di software.

3. Individuare punti deboli

→ Come servizi non protetti, sistemi mal configurati o dispositivi dimenticati (es. stampanti, NAS).

4. Eseguire scansioni stealth

→ Con opzioni come -sS, -T0, --spoof-mac, un attaccante può cercare di passare inosservato.



Bonus attacco a un database MySQL

1. I due indirizzi IP coinvolti nell'attacco di SQL injection sono 10.0.2.4 e 10.0.2.15.
2. La versione del database è 5.7.12-0ubuntu1.1.
3. L'utente che ha l'hash della password 8d3533d75ae2c3966d7e0d4fcc69216b è 1337.
4. La password in chiaro corrispondente all'hash è charley.



Riflessione rischio e prevenzione attachi sql

I **rischi** che le piattaforme utilizzino il linguaggio SQL sono:

- **Accesso non autorizzato ai dati** (es. rubare utenti e password)
- **Modifica o cancellazione di dati**
- **Esecuzione di comandi amministrativi**
- **Controllo completo del database o del sistema host**

I 2 metodi per **prevenire** attacchi sql injection son:

-☒ 1. **Utilizzare query parametrizzate** (Prepared Statements)

Le query parametrizzate separano i comandi SQL dai dati forniti dall'utente, impedendo che input malevoli vengano interpretati come parte della query.

☒ 2. **Validazione e sanificazione dell'input utente**

Assicurarsi che tutti i dati inseriti dall'utente siano:

- verificati (validazione) → Es. solo numeri per un ID utente.
- ripuliti (sanificazione) → Rimozione o codifica di caratteri pericolosi (' , -- , ; , ecc.).