

# Usare Windows PowerShell

- **Parte 2 Esplorare i comandi del Prompt dei Comandi e di PowerShell.**

1. Quali sono gli output del comando dir?

Gli output su powershell e su cmd sono simili, in pratica ci viene mostrato il contenuto della directory in cui ci troviamo.

Le uniche differenze sono:

- In Powershell vediamo gli attributi del file, come per esempio d (directory), a (archivio) e i vari permessi come r (sola lettura)
- In CMD vediamo solo se si tratta di una directory o meno, vediamo però i byte disponibili

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

Installa la versione più recente di PowerShell per nuove funzionalità
e miglioramenti. https://aka.ms/PSWindows

PS C:\Users\paolo> dir

Directory: C:\Users\paolo

Mode                LastWriteTime         Length Name
----                -
d-----          04/06/2025   23:26           .prefs
d-----          25/09/2025   16:10       .VirtualBo
x
d-----          30/06/2025   14:11       .vscode
d-----          18/06/2024   12:32       ansel
d-----          18/01/2025   17:39       Apple
d-----          22/07/2025   11:44       Cisco
d-----          29/01/2025   21:24       8.2.2
d-----          21/09/2025   16:02       Contacts
d-----          20/09/2025   23:22       Desktop
d-----          20/09/2025   23:22       Documents

16/09/2025  23:38 <DIR>      .
15/03/2025  22:32 <DIR>      ..
22/11/2024  23:25      6.579 -1.14-windows.xml
30/06/2025  15:30          7 .bash_history
30/06/2025  15:17      183 .gitconfig
22/07/2025  09:30      176 .packettracer
30/06/2025  14:22      164 .php_history
04/06/2025  23:26 <DIR>      .prefs
25/09/2025  16:10 <DIR>      .VirtualBox
30/06/2025  14:11 <DIR>      .vscode
18/06/2024  12:32 <DIR>      ansel
10/01/2025  18:39 <DIR>      Apple
22/07/2025  11:44 <DIR>      Cisco Packet Tracer 8.2.2
29/01/2025  22:24 <DIR>      Contacts
21/09/2025  16:02 <DIR>      Desktop
20/09/2025  23:22 <DIR>      Documents
```

2. Prova un altro comando che hai usato nel prompt dei comandi, come ping, cd e ipconfig. Quali sono i risultati?

Utilizzando ipconfig su entrambi i terminali i risultati sono gli stessi

- **Parte 3 Esplorare i cmdlet.**

a. I comandi PowerShell, chiamati cmdlet, sono costruiti nella forma di una stringa verbo-nome. Per identificare il comando PowerShell per elencare le sottodirectory e i file in una directory, inserisci Get-Alias dir al prompt di PowerShell.

**Qual è il comando PowerShell per dir?**

Il comando powershell per dir è Get-ChildItem

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

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

- **Parte 4 Esplorare il comando netstat usando PowerShell.**

1. **Qual è il gateway IPv4?**

Utilizzando netstat -r vediamo le tabelle di routing con le rotte attive. In questo caso il gateway ipv4 è 192.168.1.1

```
Route attive:
```

Indirizzo rete	Mask	Gateway	Interfaccia	Metrica
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.100	35
127.0.0.0	255.0.0.0	On-link	127.0.0.1	331

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

Dalla scheda dettagli possiamo vedere il PID, lo stato se in esecuzione o sospeso, il nome utente che si riferisce all'account specifico con cui viene eseguito sul sistema operativo, l'utilizzo della CPU, Il Delta working set (memoria) indica la variazione della quantità di memoria RAM che un processo sta utilizzando attivamente, vediamo anche la piattaforma e la visualizzazione controllo dell'utente account.


Dalla finestra di proprietà vediamo invece le dimensioni, la data di creazione, ultimo accesso, nella scheda firme digitali vediamo la provenienza del file.

Mentre nella scheda di sicurezza vediamo chi può fare cosa con questo elemento, vediamo infatti i gruppi degli utenti e i relativi permessi.

svchost.exe	1412	In esecuzione	SERVIZIO LOCALE	00	0 K	64 bit	Non consentito
-------------	------	---------------	-----------------	----	-----	--------	----------------

Proprietà - svchost

Generale Fime digitali Sicurezza Dettagli Versioni precedenti

 svchost

Tipo di file: Applicazione (.exe)

Descrizione: Processo host per servizi di Windows

Percorso: C:\Windows\System32

Dimensioni: 86,1 KB (88.232 byte)

Dimensioni su disco: 88,0 KB (90.112 byte)

Data creazione: mercoledì 10 settembre 2025, 09:25:10

Ultima modifica: mercoledì 10 settembre 2025, 09:25:10

Ultimo accesso: Oggi 26 settembre 2025, 33 minuti fa

Attributi: ☐ Sola lettura ☐ Nascosto

Proprietà - svchost

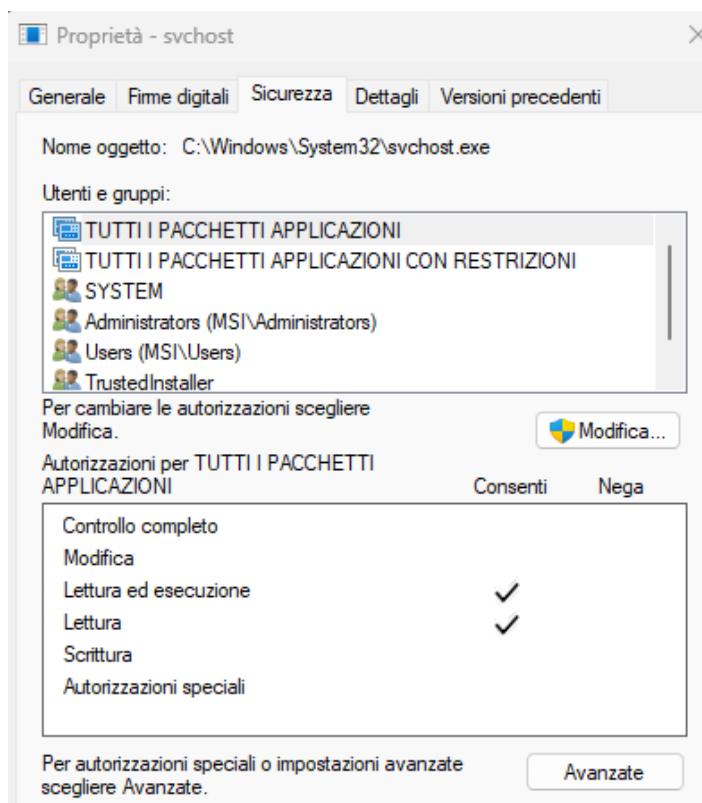
Generale Fime digitali Sicurezza Dettagli Versioni precedenti

Fime incorporate

Nome firmatario:	Algoritmo con cl...	Timestamp
Microsoft Windo...	sha256	mercoledì 27 agosto 2...

Fime del catalogo

Nome firmatario:	Nome catalogo	Algoritmo con cl...	Time
Microsoft Windows	Runlevel-Win2...	sha256	merc



- **Parte 5 Svuotare il cestino usando PowerShell.**

In una console PowerShell, inserisci `clear-recyclebin` al prompt. **Cosa è successo ai file nel Cestino?**

Eseguendo il comando nella console PowerShell, mi viene chiesta la conferma, e una volta che confermo la scelta, i file presenti nel cestino vengono eliminati.

```
PS C:\Users\paolo> 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
```

**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.**

Dei comandi che possono essere utili per i compiti da analista di sicurezza ho trovato:

**Processi** → `Get-Process` Elenca tutti i processi in esecuzione. Può essere filtrato per cercare processi con un percorso nullo (`$_ .Path -eq $null`) o con nomi sospetti (malware).

**Network** → `Get-NetTCPConnection` Mostra le connessioni di rete attive (equivalente più potente di `netstat`). Utile per rilevare comunicazioni C2 (Command and Control) o esfiltrazione di dati.

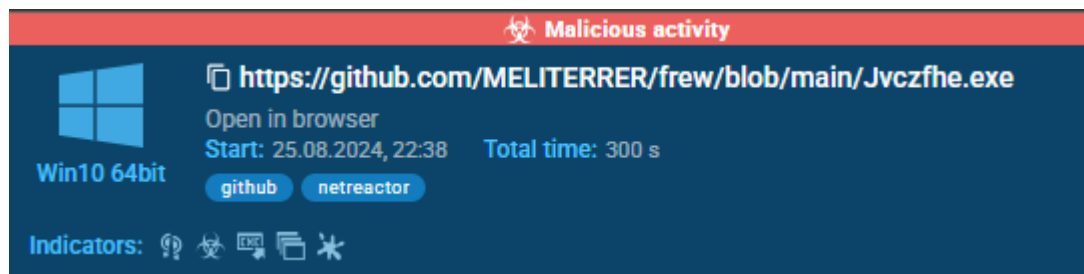
**File Hashing** → `Get-FileHash -Path <Percorso>` Calcola l'hash crittografico (es. SHA256) di un file. Fondamentale per confrontare i file con i database di IoC noti (es. VirusTotal).

**Servizi** → `Get-Service` Elenca tutti i servizi in esecuzione. Usato per identificare servizi anomali o non necessari che potrebbero essere usati come persistenza.

**Event Log** → `Get-WinEvent` Interroga i registri eventi di Windows. Essenziale per il "log analysis", in particolare per cercare:

## Riepilogo Dettagliato dell'Analisi di Minaccia: Jvczfhe.exe

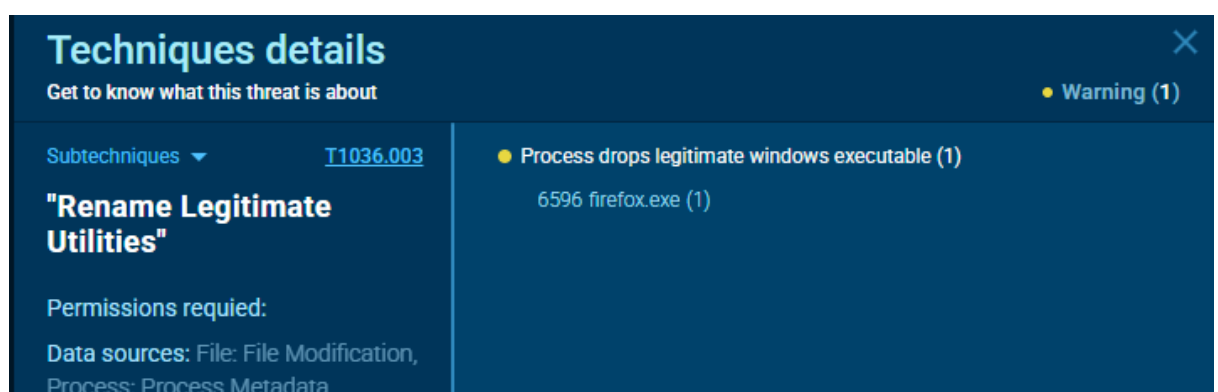
L'analisi sandbox di **ANY.RUN** per il file collegato ha identificato l'attività come **maliziosa**. I dati disponibili indicano chiaramente che il file analizzato è un programma dannoso. Possiamo notare ciò subito, appena apriamo il link.



Possiamo già notare negli indicatori, alcune informazioni che ci aiutano a far capire che il programma trattato è malevolo, come ad esempio la presenza di un cattivo certificato.

Successivamente, spostandosi nel pannello ATT&CK si notano degli avvisi:

- Un avviso è relativo al processo di firefox, che contiene in maniera deliberata un eseguibile, più precisamente un repository Github, segnale da non sottovalutare.



- Più pertinenti al programma eseguibile vediamo due avvisi. Il primo è relativo al fatto che questo eseguibile lancia un cmd eseguendo del codice malevolo. Lo troviamo infatti nella colonna Execution di anyrun.

## Techniques details

Get to know what this threat is about

Warning (4)

Subtechniques [T1059.003](#)

### "Windows Command Shell"

Permissions required: User

Data sources: Command: Command Execution, Process: Process Creation

Adversaries may abuse the Windows command shell for execution. The Windows command

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

Image: C:\Windows\SysWOW64\cmd.exe

Cmdline: "cmd" /c timeout 21 & exit

Questo comando eseguito da cmd può sembrare innocuo ma è un meccanismo di difesa, viene infatti sfruttato per evadere la rilevazione. Successivamente troviamo altri avvisi riguardanti sempre lo stesso file i quali ci avvisano che il file ha la possibilità di leggere le impostazioni di sicurezza di internet explorer e visualizzare le impostazioni di Windows Trust. Troviamo questo avviso nella colonna Discovery. Viene fatto ciò da una persona malintenzionata per reperire informazioni circa il sistema e la sua configurazione.

## Techniques details

Get to know what this threat is about

Warning (4) Other (50)

[T1012](#)

### "Query Registry"

Permissions required: User, Administrator, SYSTEM

Data sources: Process: OS API Execution, Windows Registry: Windows Registry Key Access, Command: Command Execution, Process: Process Creation

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

- Reads security settings of Internet Explorer (2)
  - 7492 Jvczfhe.exe (1)
  - 7824 Muadnrd.exe (1)
- Checks Windows Trust Settings (2)
  - 7492 Jvczfhe.exe (1)
  - 7824 Muadnrd.exe (1)
- Reads the software policy settings (26)

Operation: read

Name: CrossCertDownloadIntervalHours

Value: 168

Key: HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates\ChainEngine\Config

TypeValue: REG\_DWORD

Sempre nella colonna Discovery abbiamo altri avvisi che mostrano che il malware legge i valori del sistema, il nome del computer e altro.

- Appartenente alla colonna Defense evasion troviamo un avviso che ci dice che il malware disabilita le tracce nei log, rendendo molto difficile da intercettare.

Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery
Command and Scripting Interpreter (1/12) Windows Command Shell 4			Masquerading (1/11) Rename Legitimate Utilities 1  Impair Defenses (1/11) Disable Windows Event Logging 2		Query Registry 4 50  System Information Discovery 15

Analizzando tutto ciò possiamo constatare che si può trattare di un Trojan, anche se non prova per niente a nascondersi, avendo un nome che solamente leggendolo ci fa pensare a un malware.

## • Bonus 1

### 1. Cos'è Nmap? Per cosa viene usato nmap?

Nmap è un tool open source utilizzato per network exploration security auditing, è stato progettato per scansionare rapidamente grandi reti, sebbene funzioni bene contro singoli host..

### 2. Qual è il comando nmap usato?

Il comando nmap usato è `nmap -A -T4 scanme.nmap.org`

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  ldap
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
```

### 3. Cosa fa l'opzione A? Cosa fa l'opzione T4?

L'opzione A abilita la ricerca del sistema operativo, la versione, lo script scanning e traceroute mentre T4 abilita l'esecuzione più veloce.

## ● Parte 2 Scansione delle Porte Aperte

### 1. Scansiona il tuo localhost.

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.97 ( https://nmap.org ) at 2025-09-26 06:33 -0400
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000068s 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 4
|     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 11.55 seconds
```

Le porte aperte sono la 21 FTP e la 22 SSH

## 2. Scansione la tua rete

```
[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 85241sec preferred_lft 85241sec
    inet6 fd17:625c:f037:2:a00:27ff:fe2f:87a7/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86249sec preferred_lft 14249sec
    inet6 fe80::a00:27ff:fe2f:87a7/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
```

La mia VM appartiene alla rete **10.0.2.15/24**

**Quanti host sono attivi?**

C'è un solo host attivo.

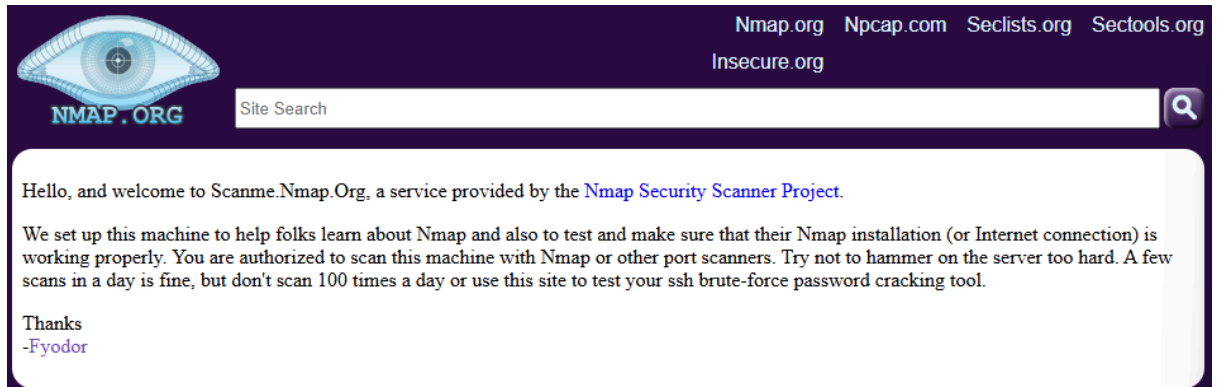
```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.97 ( https://nmap.org ) at 2025-09-26 06:40 -0400
Nmap scan report for 10.0.2.15
Host is up (0.000054s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-lrw-r--r--  1 0      0          0 Mar 26  2018 ftp_test
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 10.0.2.15
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     At session startup, client count was 3
|     vsFTPD 3.0.5 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 10.0 (protocol 2.0)
Service Info: Host: Welcome

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (1 host up) scanned in 65.08 seconds
```



- **Scansiona un server remoto**

Andando sul sito troviamo un messaggio che ci dice che questo server è stato creato per permettere agli utenti di imparare Nmap.



Una volta eseguita la scansione troviamo:

- Porta 22 SSH, porta 80 HTTP, porta 9929 nping-echo, porta 31337 tcpwrapped. Queste sono le porte aperte
- 996 porte tcp filtrate
- L'indirizzo IP è 45.33.32.156
- Sistema operativo Linux

### **Come può nmap aiutare con la sicurezza della rete?**

Nmap può aiutare con la sicurezza delle rete grazie ai suoi molteplici usi. Per esempio grazie alla scansione delle porte si può verificare se ci sono porte aperte per sbaglio o se qualche porta ha una versione ormai obsoleta. Può anche verificare che un firewall funzioni, mostrando le porte filtrate.

### **Come può Nmap essere usato da un attore malevolo come strumento nefasto?**

Nmap può essere usato in modo malevolo da un attaccante appunto per verificare la presenza di porte obsolete aperte o porte erroneamente lasciate aperte. Nmap dispone anche di script che possono testare attivamente le debolezze, come può essere ad esempio una vulnerabilità nota su un servizio o credenziali banali su qualche servizio aperto.

- **Bonus 2: Attacco a un database MySQL**

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

I due indirizzi IP coinvolti nell'attacco sono **10.0.2.4** e **10.0.2.15**

Source	Destination
10.0.2.4	10.0.2.15
10.0.2.15	10.0.2.4

**Qual è la versione?**

La versione è 5.7.12-0ubuntu1.1

```
r 1=1 union select null, version ()#<br />Fir  
</pre><pre>ID: 1' or 1=1 union select null, v  
>Surname: Smith</pre><pre>ID: 1' or 1=1 union  
name: <br />Surname: 5.7.12-0ubuntu1.1</pre>
```

**Cosa farebbe per l'aggressore il comando modificato di 1' OR 11 UNION SELECT null, column\_name FROM INFORMATION\_SCHEMA.columns WHERE table\_name='users'?**

Questo comando mira a recuperare i nomi di tutte le colonne nella tabella users del database

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

L'utente 1337

```
ord from users#<br />First name: 1337<br />Surname: 8d3533d75ae2c3966d7e  
0d4fcc69216b</pre><pre>ID: 1' or 1=1 union select user, password from us
```

Una volta decifrata con crackstation otteniamo come risultato **charley**.

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

Il rischio è appunto determinato dalla vulnerabilità alle iniezioni di codice sql, se infatti non viene sanificato l'input con dei filtri che bloccano certi tipi di caratteri, un attaccante potrebbe approfittarne.

**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?**

Un primo metodo potrebbe essere l'utilizzo delle stored procedure. Le stored procedure (procedure memorizzate) predefinite possono agire come un livello di separazione tra l'applicazione e l'esecuzione di SQL dinamico.

Una stored procedure è un insieme di istruzioni SQL precompilate e memorizzate nel database. Quando l'applicazione necessita di accedere ai dati, invece di costruire una nuova query SQL, si limita a **chiamare la stored procedure** e a passarle gli input come parametri.

Quando le stored procedure sono scritte correttamente, il motore del database tratta l'input fornito come dati impedendo che qualsiasi sintassi SQL iniettata possa essere eseguita come comando.

Un secondo metodo consiste nell'utilizzo di query parametrizzate (prepared statements). Questo approccio separa il codice SQL dai dati inseriti dall'utente, garantendo che l'input venga trattato solo come valore e non come parte eseguibile della query, prevenendo così l'iniezione di codice maligno.