Report 20/02/2026 Cristiano Samuel Vanvitelli

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 Ioc, esplorare funzionalità di Nmap e analizzare un file .pcap di un attacco precedente contro un database SQL.

Strumenti

Windows 10: Esecuzione Poweshell, studio Ioc

CyberOps Workstation: Esecuzione nmap,MySQL

Fase1 – PowerShell

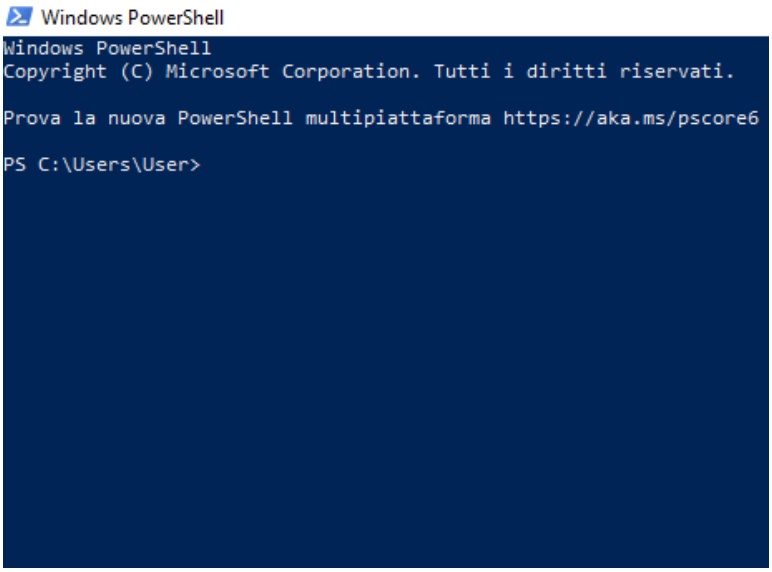

*Fig.1 PowerShell

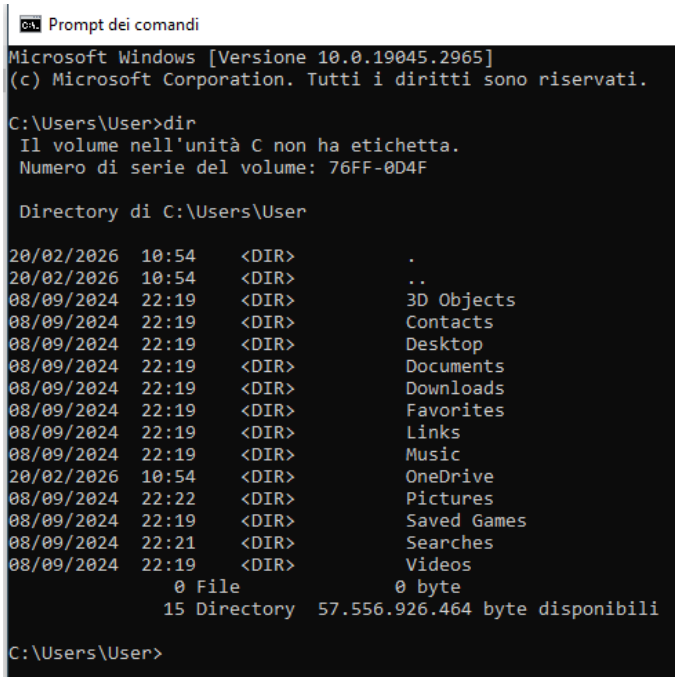

*Fig.2 Comando dir cmd

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

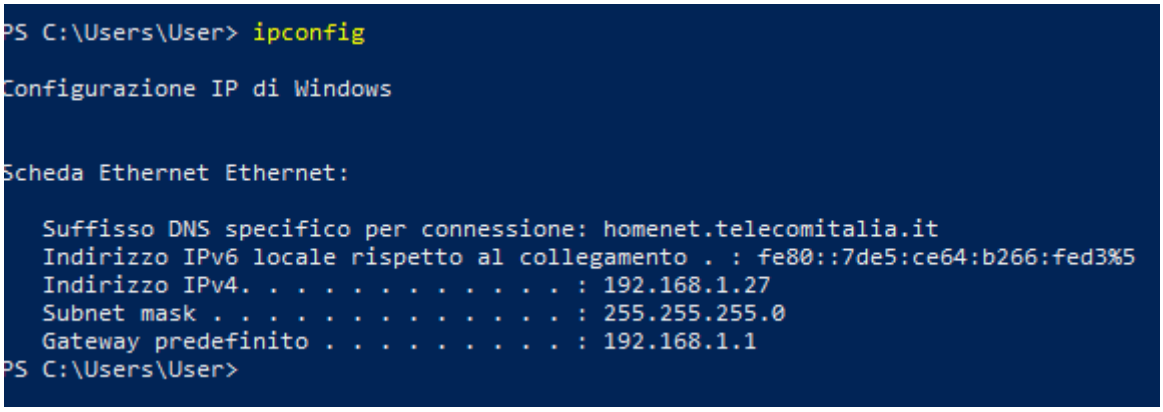

*Fig.3 Comando ipconfig

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.

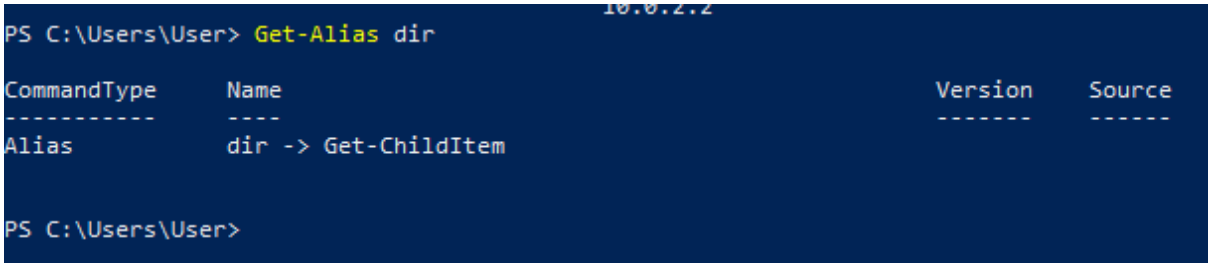

*Fig.4 Comando Alias dir

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

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

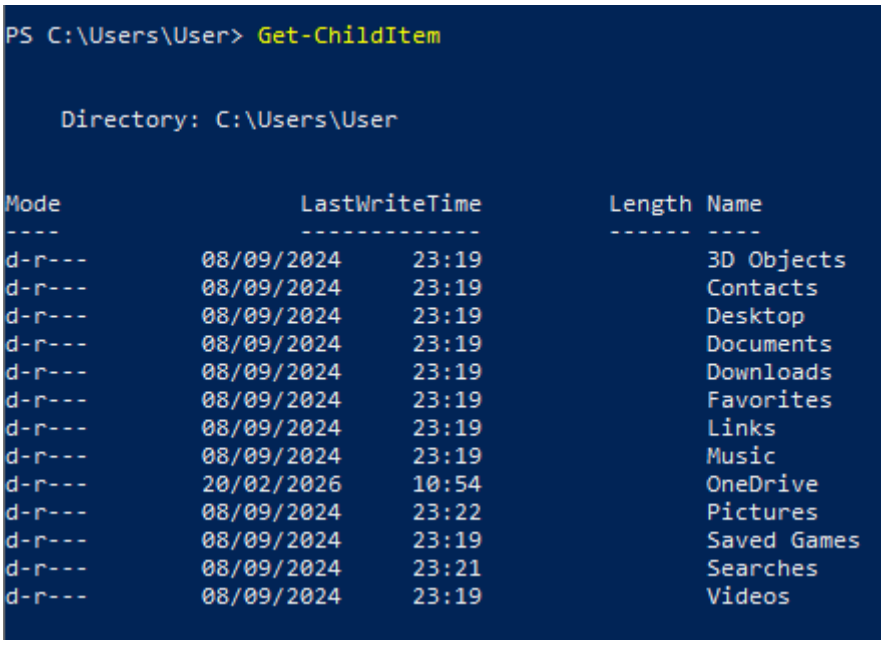

*Fig.5 Comando in esecuzione

```
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 Metrica 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.

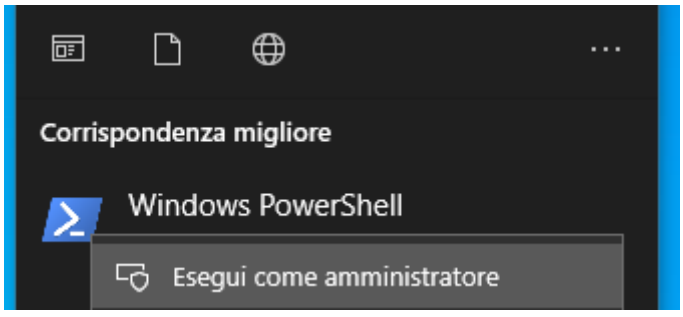

*Fig.7 Esecuzione powershell come amministratore

```
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

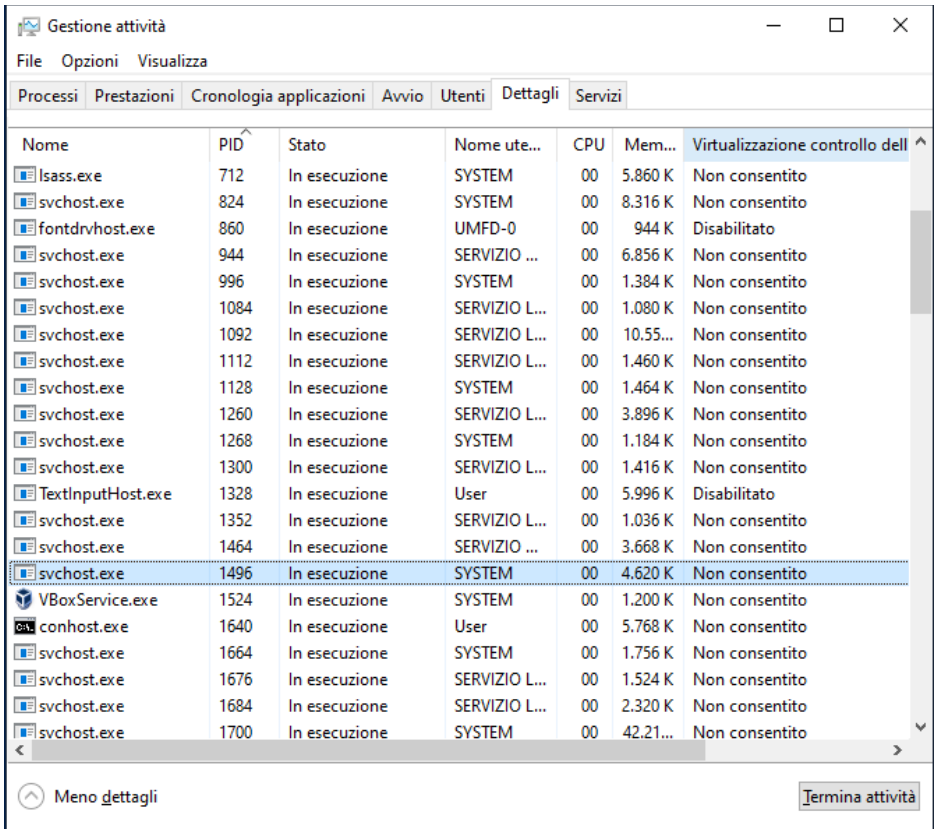

*Fig.9 Dettagli processo svchost.exe

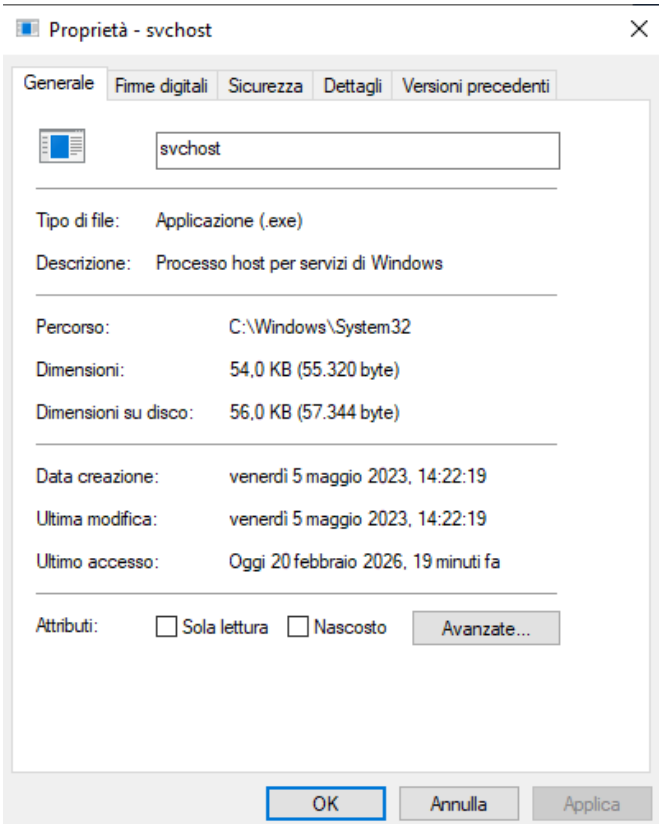

Fig.10 Verifica proprietà processo

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**

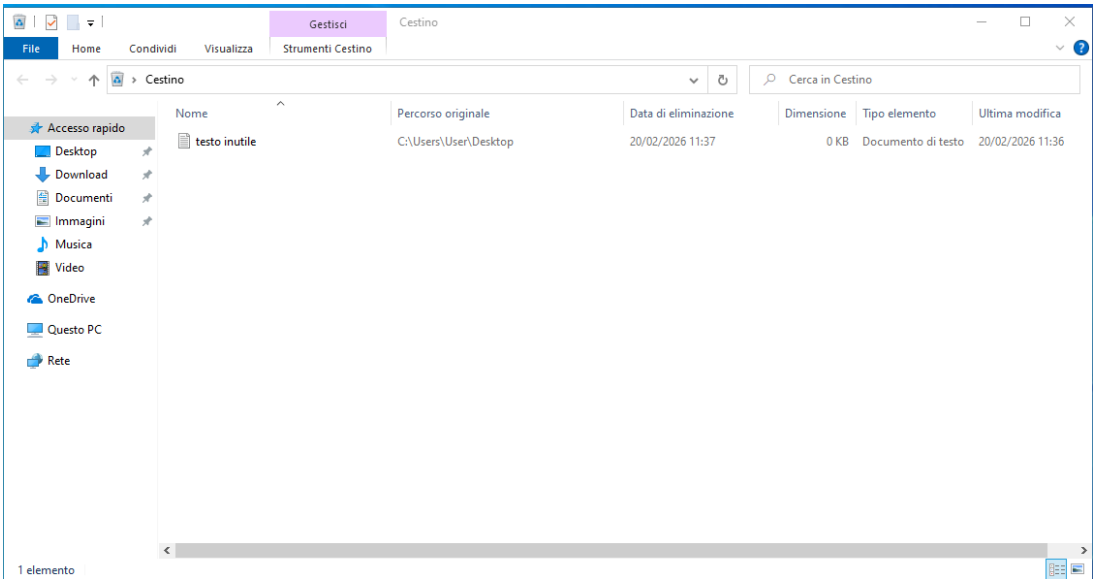

*Fig.11 Controllo cestino pre-clear

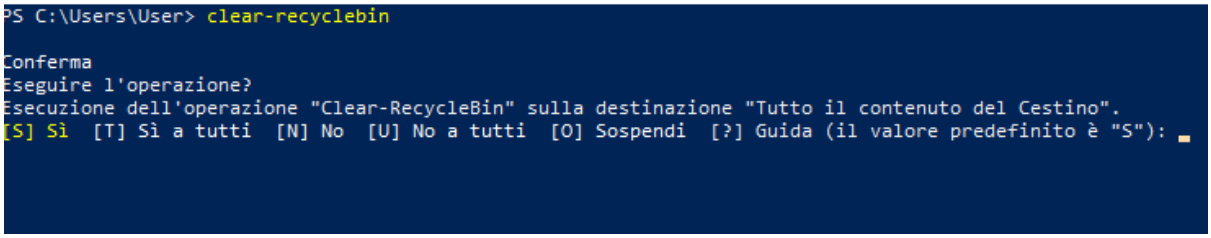

*Fig.12 Comando clear-recyclebin

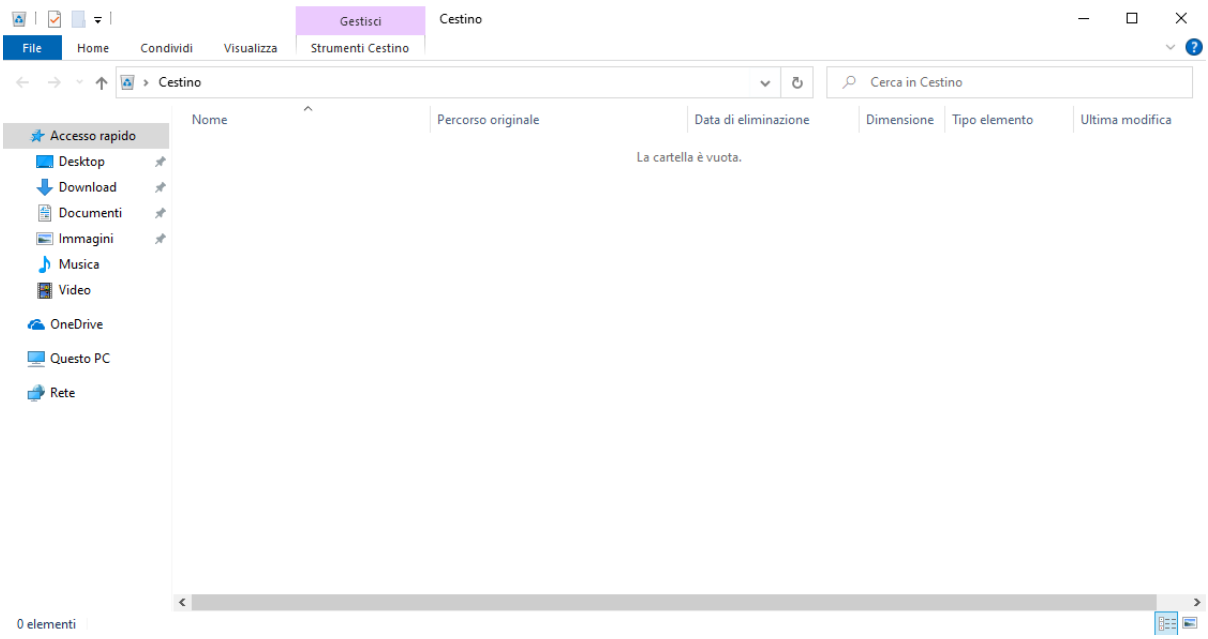

Fig.13 Controllo cestino post-clear

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 statio 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 – Ioc

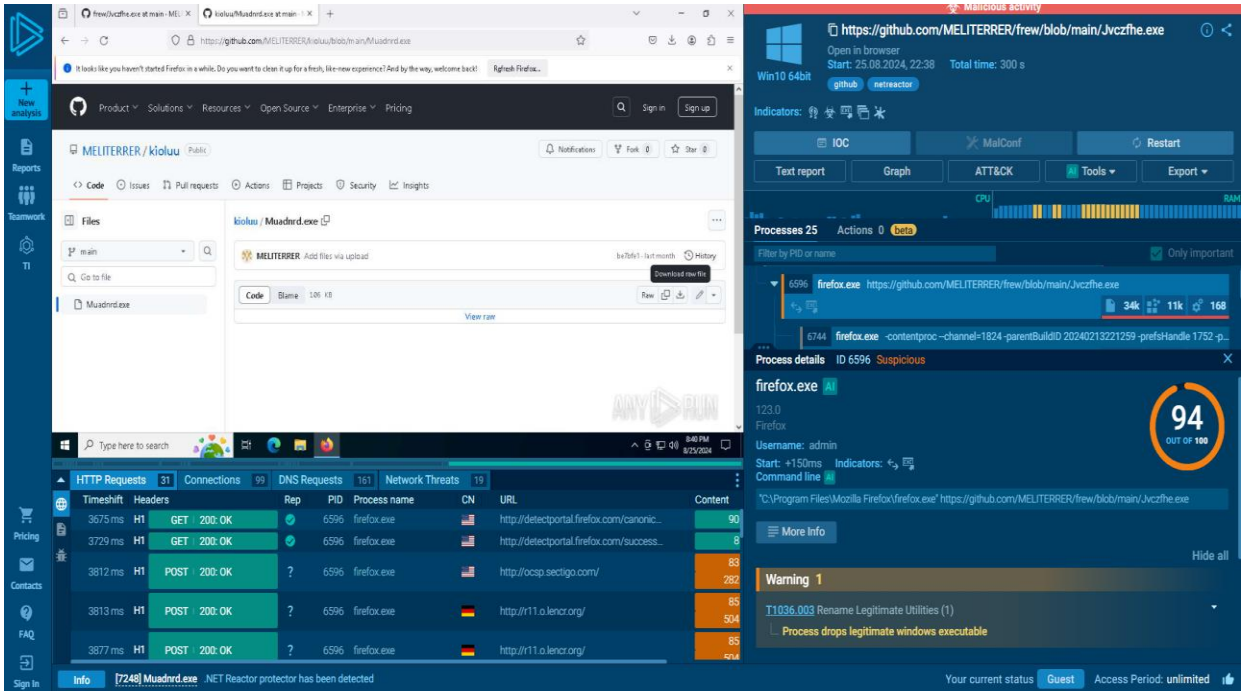

Fig.14 Schermata principale Any.run

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.

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.

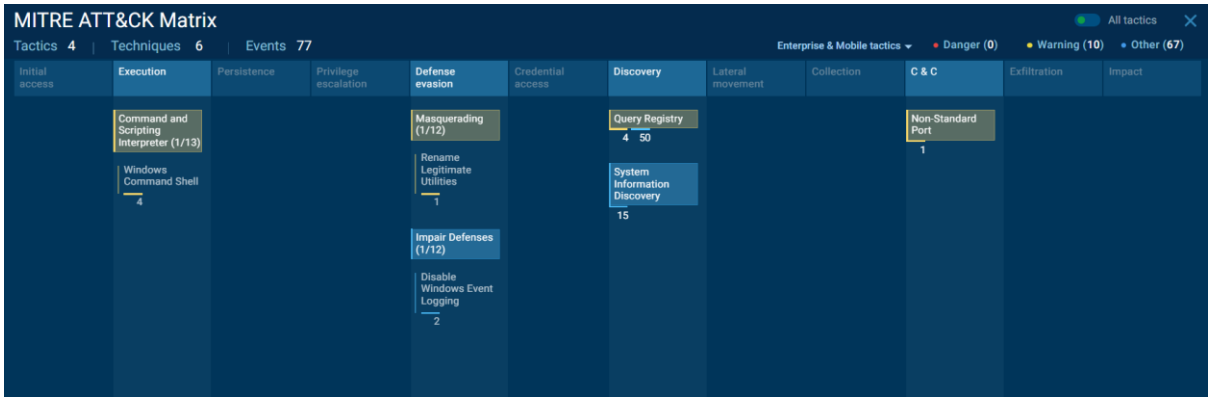

Fig.17 Tipi di attacco utilizzati dagli eseguibili

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 J**vczfhe.exe** ha rinominato il proprio malware con un nome di un processo di Windows legittimo per il download di risorse **(installutil.exe)** apparendo 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

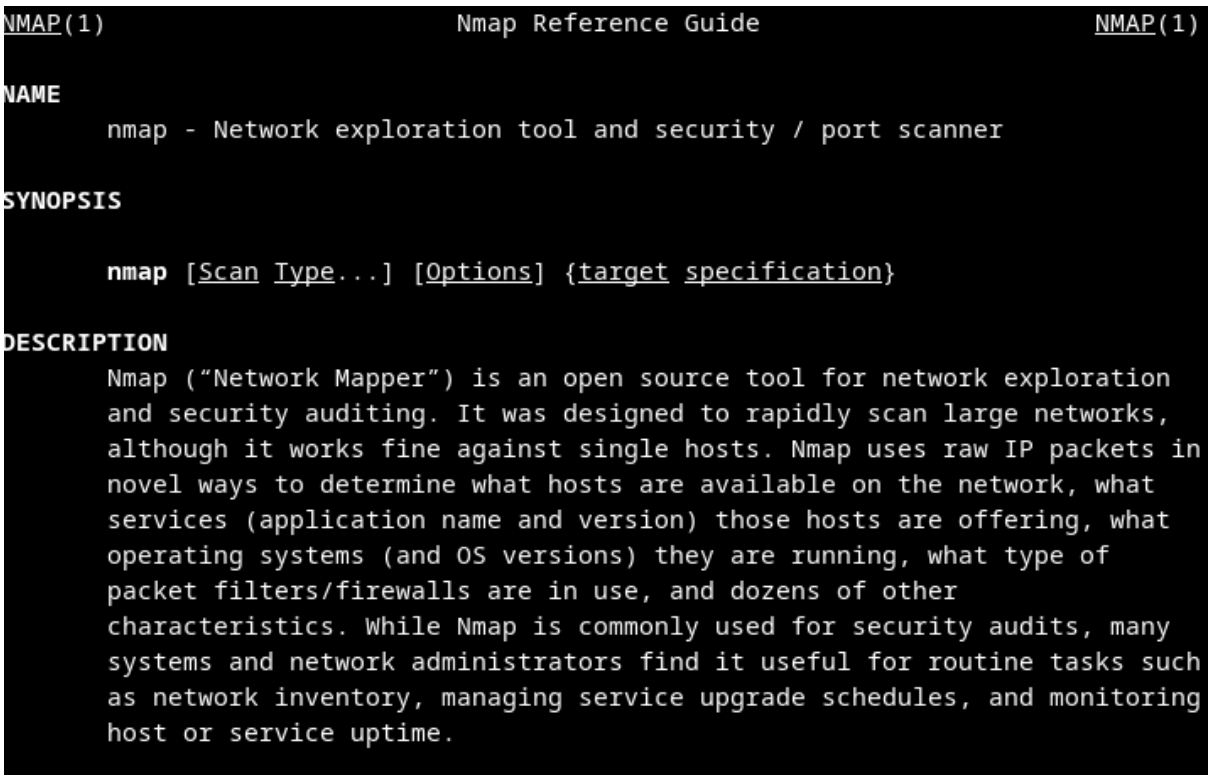

**Fig.18 Manuale nmap*

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.

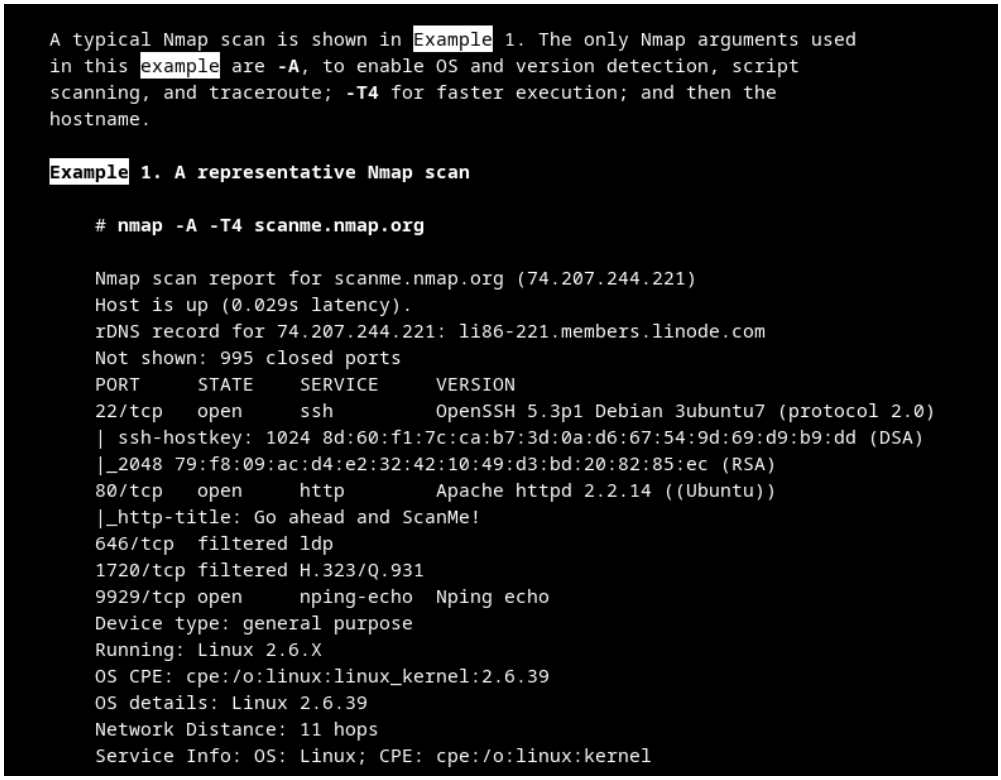

**Fig. 19 Filtro /example*

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

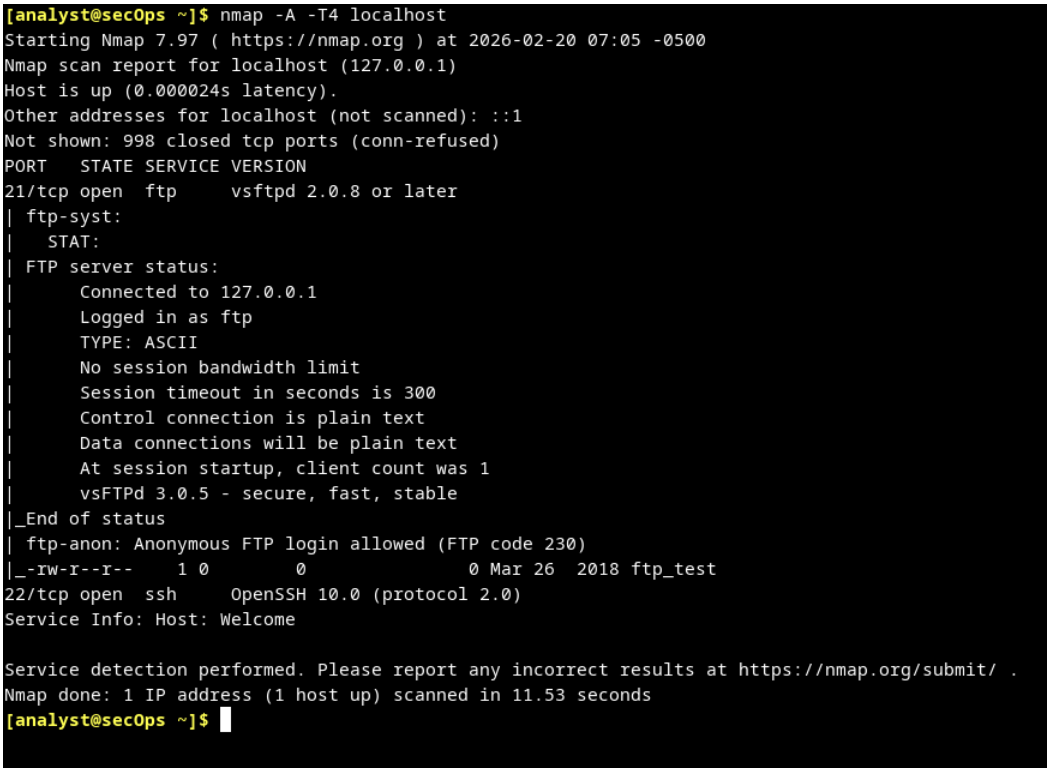

**Fig.20 Scansione nmap localhost*

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)

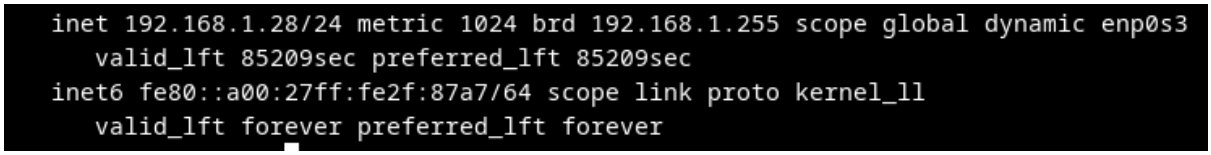

**Fig.21 Comando ip address*

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);

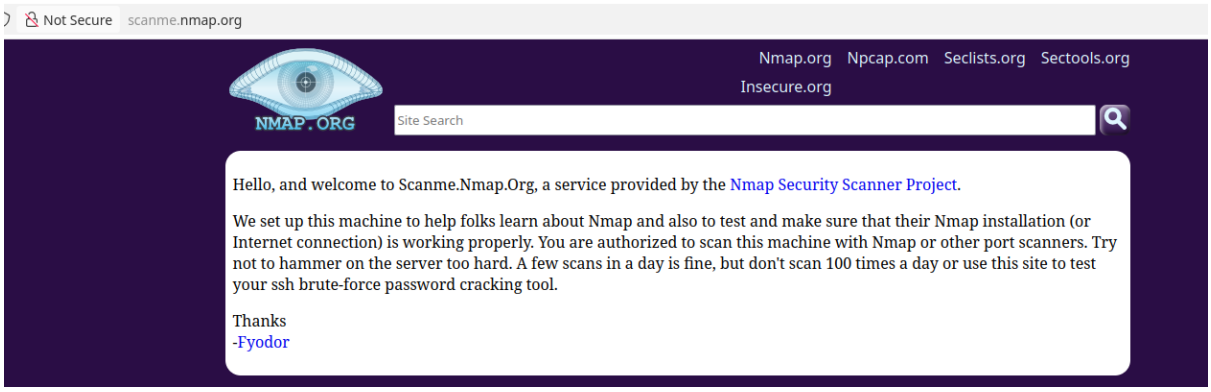

Fig.22 Pagina nmap

Qual è lo scopo di questo sito? Per testare se l'installazione di nmap o la connessione internet funzioni 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

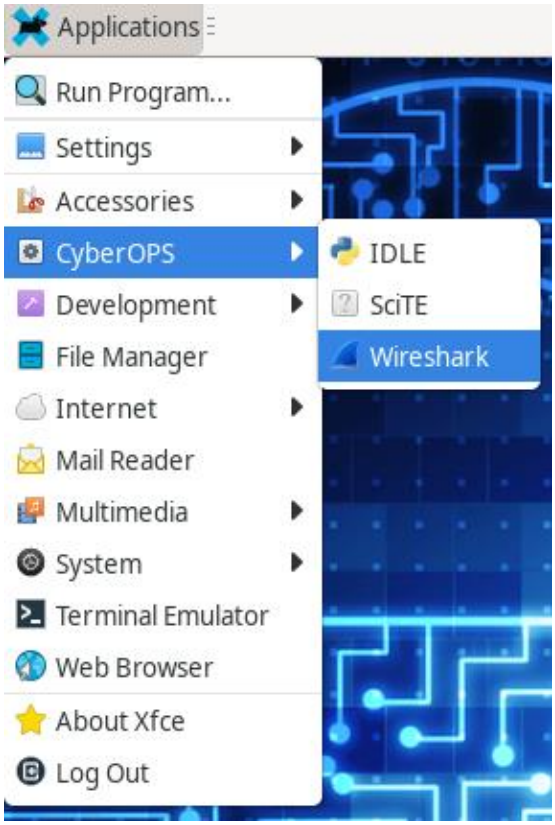

**Fig.24 Apertura Wireshark*

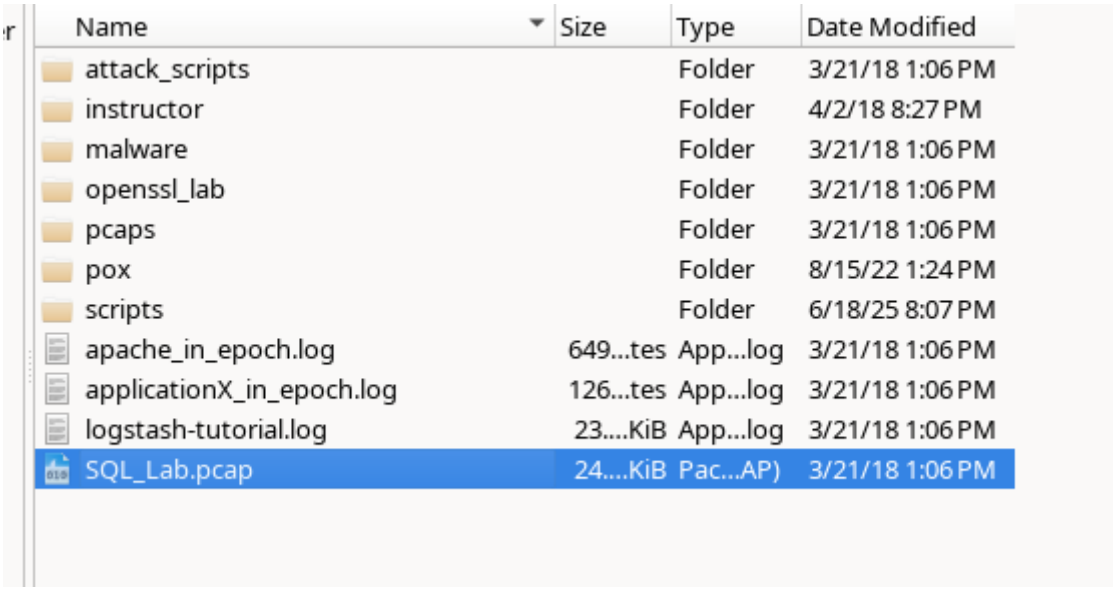

*Fig.25 Apertura file .pcap

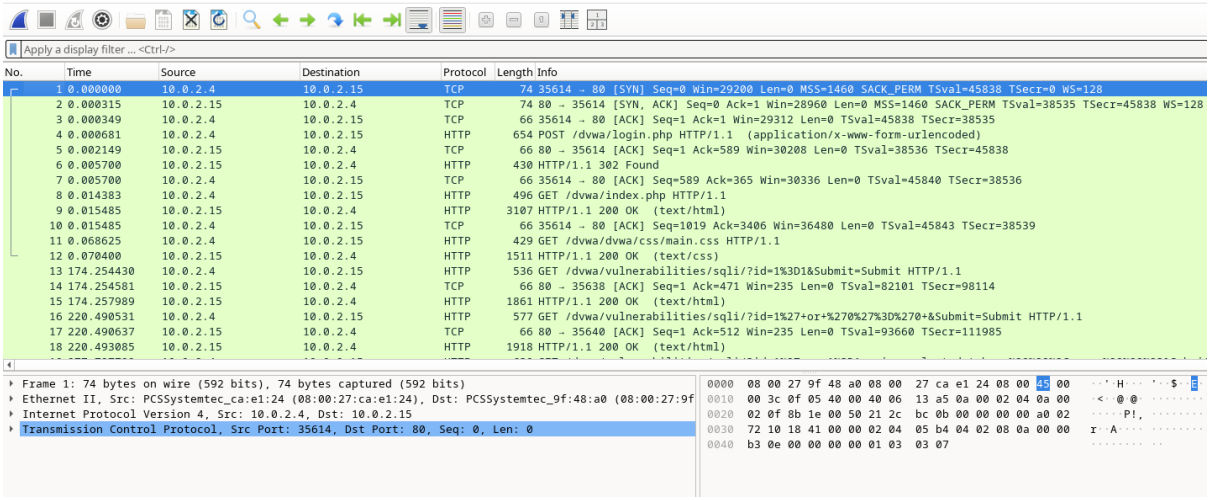

*Fig.26 File .pcap SQL

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)

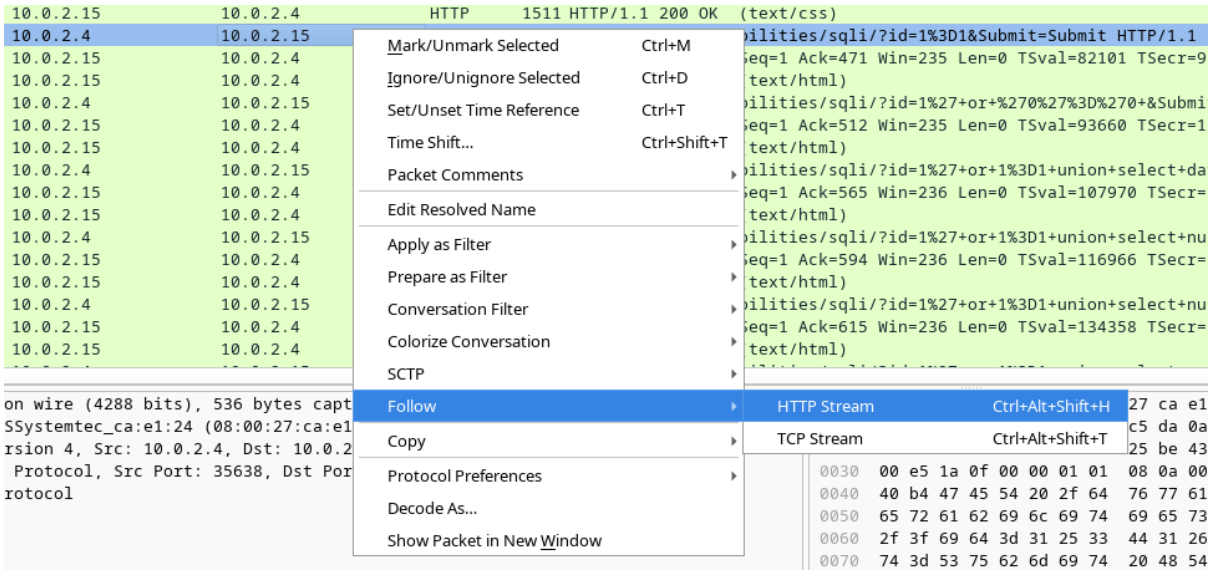

*Fig.27 Flusso http

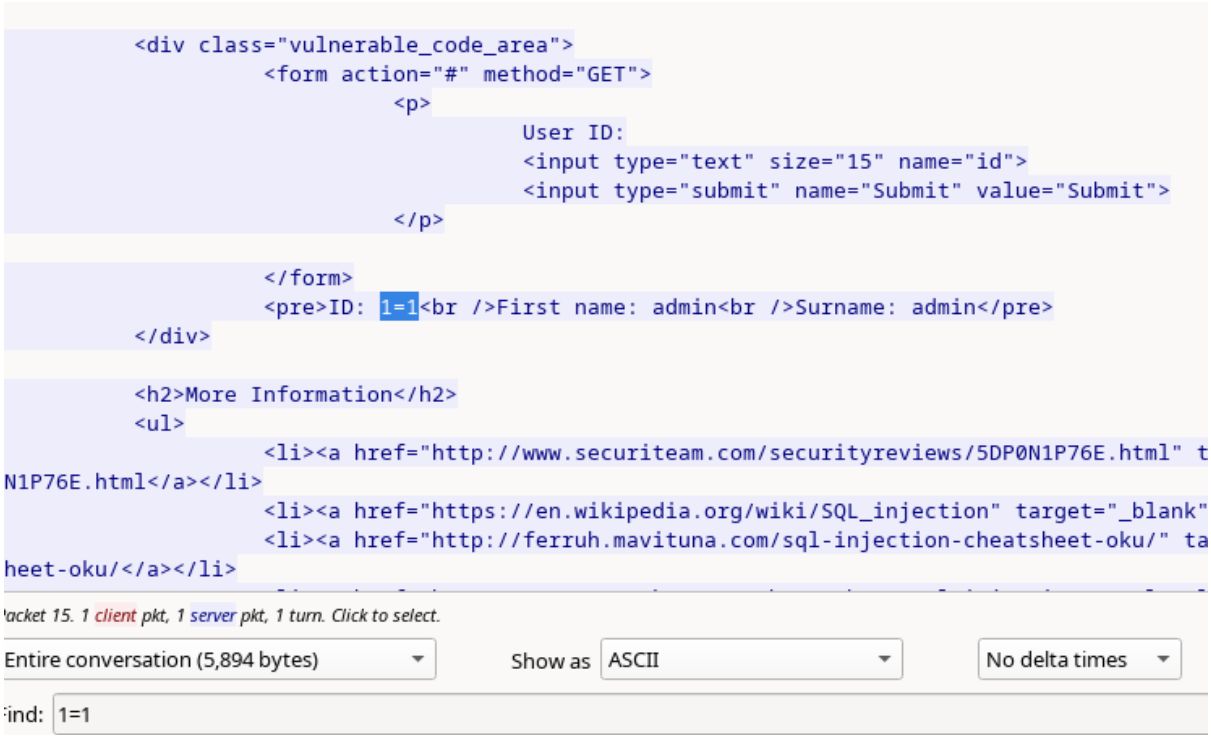

*Fig.28 Tentativo vulnerabilità SQL

*Fig.29 Risposta DVWA

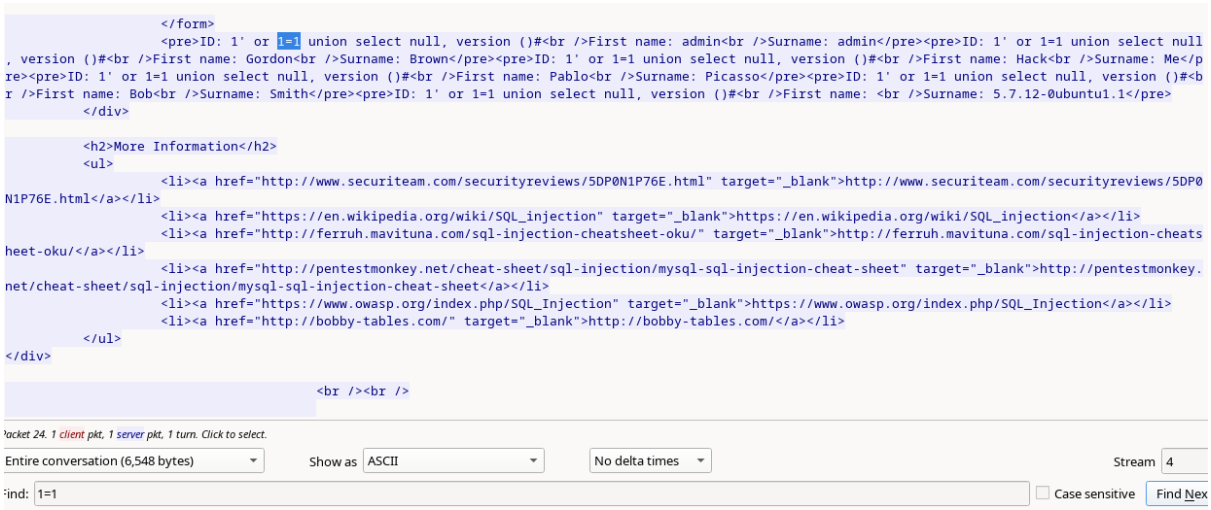

*Fig.30 Identificazione versione DVWA

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

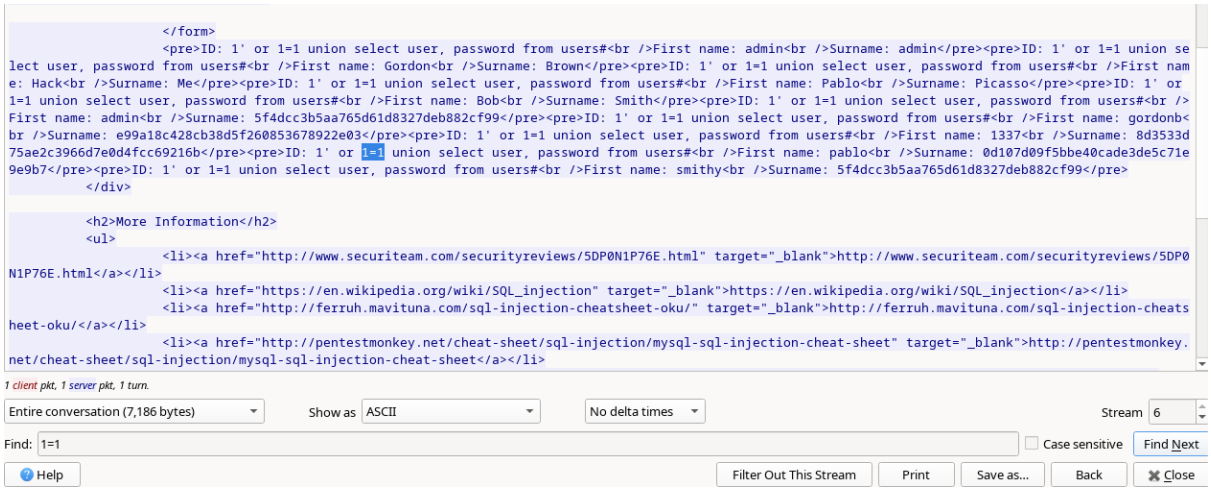

Fig.31 Identificazione passwords

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.