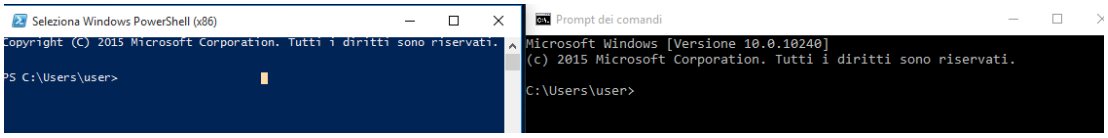
# Progetto settimanale.

## Esercizio 1: Usare Windows PowerShell.

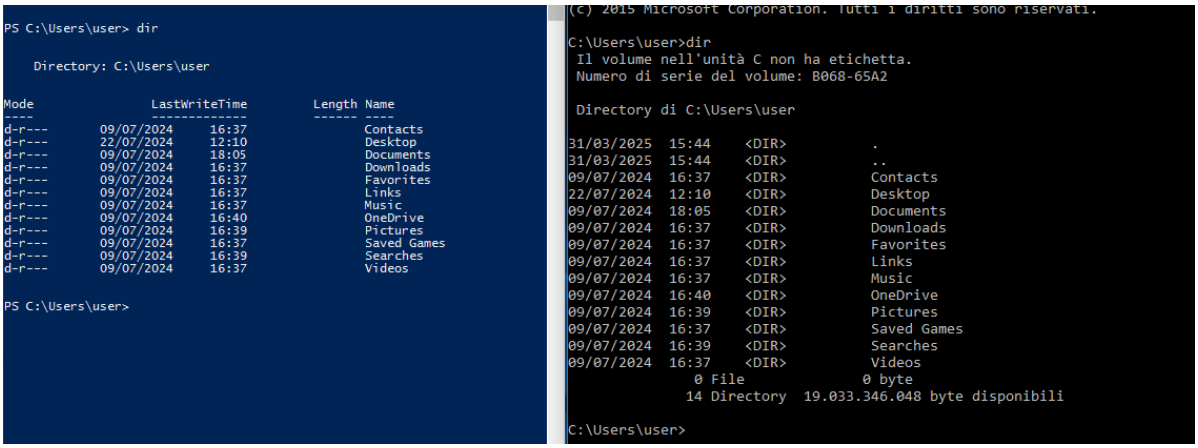
**L'obiettivo del laboratorio è esplorare alcune delle funzioni di PowerShell:**

**Istruzioni Parte 1: Accedere alla console PowerShell.**



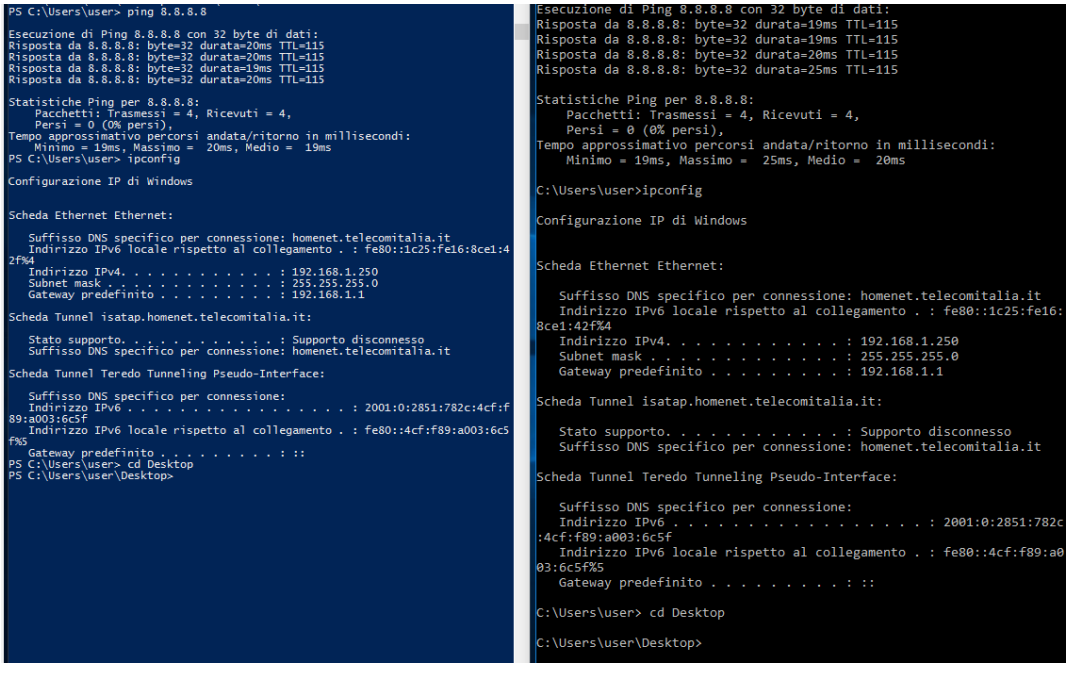

**Parte 2: Esplorare i comandi del Prompt dei Comandi e di PowerShell.**

1) **Quali sono gli output del comando dir?**




2) **Quali sono i risultati? Dopo aver dato i comandi ping, cd e ipconfig.**

I risultati sono gli stessi sia in powershell che nel prompt dei comandi.



**Parte 3: Esplorare i cmdlet.**

3) **Qual è il comando PowerShell per dir? Il comando è Get-childitem**

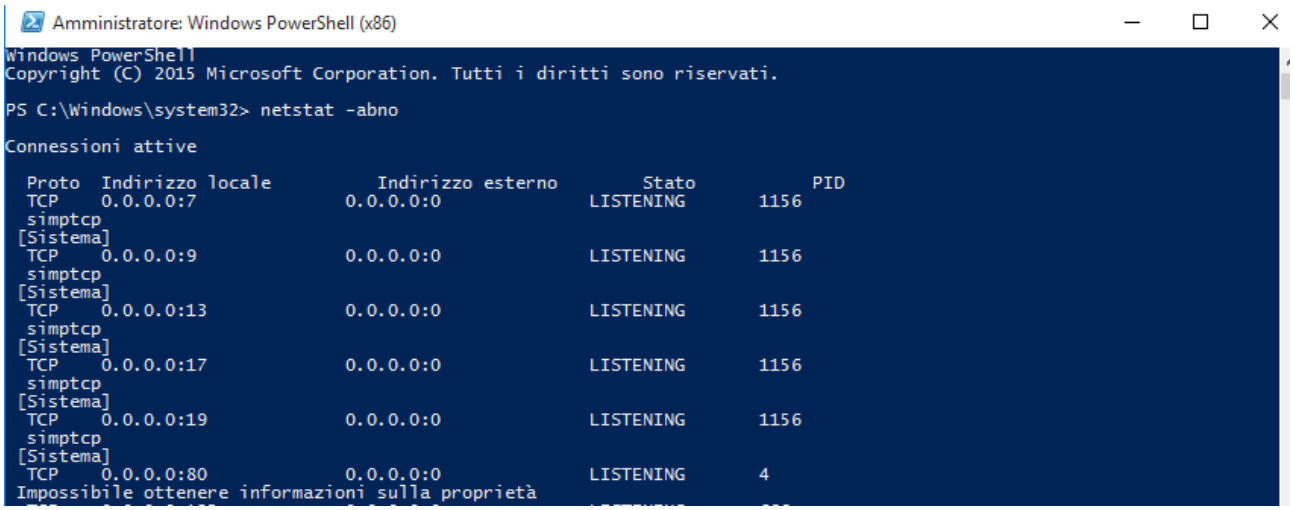
```
PS C:\Users\user\Desktop> Get-Alias dir

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

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

4) **Qual è il gateway IPv4? Il gateway è 192.168.1.1**

**Seguo le istruzioni.**

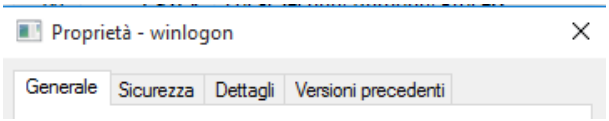



5) **Quali informazioni puoi ottenere dalla scheda Dettagli e dalla finestra di dialogo Proprietà per il PID selezionato?**

   Posso ottenere informazioni generali sul processo: il tipo di file, la descrizione, il percorso, le dimensioni, la data di creazione e l'ultima modifica

   Posso ottenere informazioni sulla sicurezza: utenti e gruppi e permessi sul processo.

   Posso ottenere informazioni dettagliate per esempio sul copyright.




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

6) **Cosa è successo ai file nel Cestino dopo aver digitato clear-recyclebin?**

   I file sono stati eliminati dal cestino.

**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.**

Su internet ho trovato vari comandi per semplificare il compito di un analista di sicurezza

- Comandi per la gestione della sicurezza:
  **Get-ExecutionPolicy**: Per visualizzare la policy di esecuzione corrente
  **Set-ExecutionPolicy**: Per impostare la policy di esecuzione (Restricted, Unrestricted, AllSigned, etc.).
  **Get-ExecutionPolicy -List**: Per visualizzare la policy di esecuzione per l'ambito corrente e per tutti gli ambiti (utente, macchina).

- Gestione dei Processi:
  **Get-Process**: Per visualizzare tutti i processi in esecuzione.
  **Get-Process -Id <ID_processo>**: Per visualizzare informazioni su un processo specifico tramite ID.
  **Get-Process | Sort-Object CPUUsageOnProcessor**: Per ordinare i processi in base all'utilizzo della CPU.
  Stop-Process: Per terminare un processo.

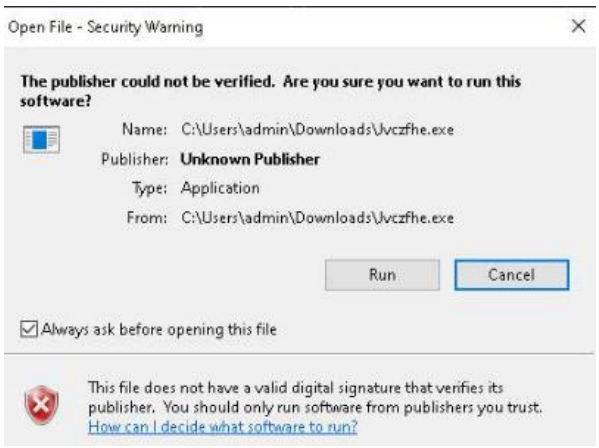
- Gestione del Firewall:
  **Get-NetFirewallRule**: Per visualizzare le regole del firewall.
  **Get-NetFirewallProfile**: Per visualizzare il profilo del firewall.
  **New-NetFirewallRule**: Per creare una nuova regola del firewall.
  **Set-NetFirewallRule**: Per modificare una regola del firewall.
  **Remove-NetFirewallRule**: Per eliminare una regola del firewall.

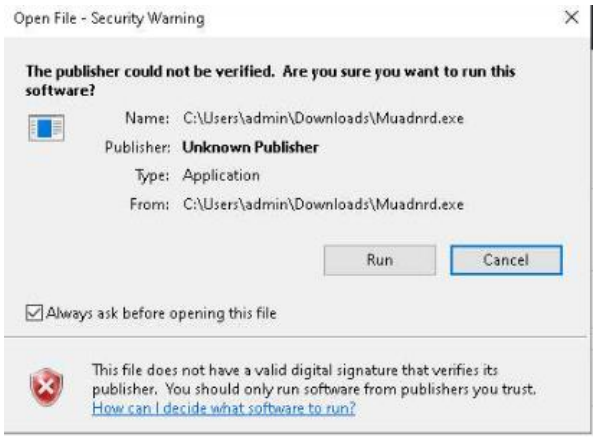
## Esercizio 2: Studio IoC.

**Studiare questo link di anyrun e spiegare queste minacce in un piccolo report.** https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281/

### Parte 1: Descrizione.

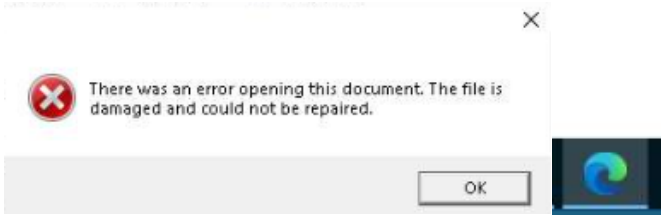
Aperto il link appare subito l'azione intrapresa dall'utente della sandbox anyrun. L'azione messa in atto prevedere il download e l'esecuzione di due file eseguibili: **Jvczfhe.exe** e **Muadnrd.exe**




### Parte 2: Esecuzione Jvczfhe.exe

Una volta cliccato su run, appare sia l'icona di MicrosoftEdge sia un pop up di errore come a far intendere all'utente che il file è danneggiato e non è stato possibile eseguirlo. Ma sarà veramente così?




Nel mentre però il file eseguibile **Jvczfhe.exe** ha già fatto diverse azioni e alcune abbastanza sospette:

- **Esegue un processo che si blocca** → Attività non usuale:
  Image: C:\Windows\SysWOW64\WerFault.exe
  Cmdline: C:\WINDOWS\SysWOW64\WerFault.exe -u -p 7492 -s 2676
- **Legge le impostazioni di sicurezza** → Warning System Security:
  Key:HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Security
  Typevalue: REG_SZ
- **Controlla le impostazioni di Sicurezza di Windows** → Warning general:

Value 146432

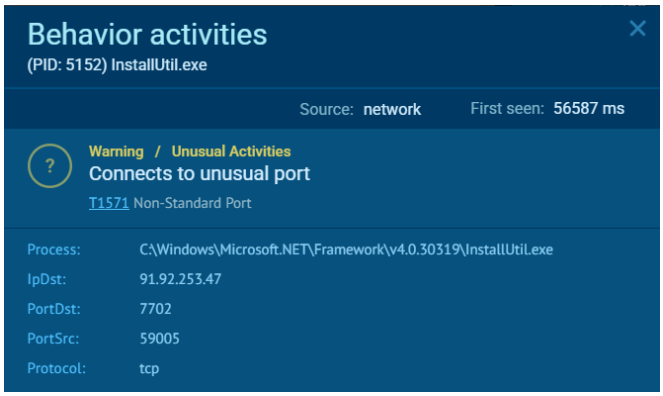
key:HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing

Typevalue: REG_DWORD

- **Attiva CMD.exe per l'esecuzione dei comandi (Command Execution)** → Warning general.

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

  Cmdline: "cmd" /c timeout 21 & exit
- **Crea un processo figlio conhost.exe**
- **Esegue un timeout 21.**
- **Il processo (PID: 5152) InstallUtil.exe si connette ad una porta non usuale** → Unusual Activity.



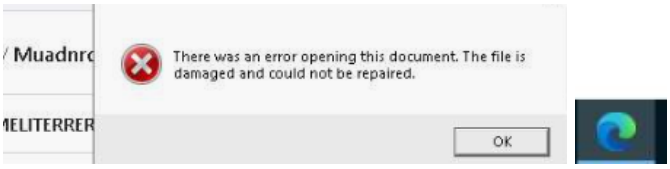

- Si rintraccia l'azione di .Net Reactor usato per prevenire la reverse engeneering.
- Infine, viene avviato il processo **WerFault.exe** un modulo di report errori di Windows.

Gli Indicatori di compromissione sono:

- La connessione alla rete avviata.
- Processo si è bloccato.
- Il certificato non è valido.
- Lettura delle chiavi di registro di windows.
- Attivazione CMD.exe per l'esecuzione dei comandi.
- Connessione del processo a porta non standard.
- Il punteggio assegnato da VirusTotal dopo l'analisi. 

**Parte 3: Esecuzione Muadnrd.exe**

Anche il file eseguibile **Muadnrd.exe** pone in atto visivamente un comportamento simile facendo apparire un pop up di errore e una connessione a MicrosoftEdge.



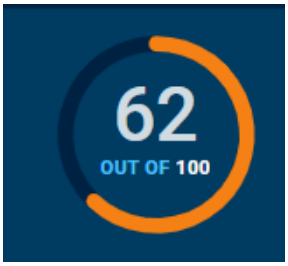

Ma quali azione avrà compiuto nel mentre? Saranno uguali o diverse rispetto all'altro file?

- **Esegue un processo che si blocca → Attività non usuale**:
  Image: C:\Windows\SysWOW64\WerFault.exe
  cmdline: C:\WINDOWS\SysWOW64\WerFault.exe -u -p 7824 -s 2888
- **Il programma si lancia da solo → Azione sospetta:**
  image: C:\Users\admin\Downloads\Muadnrd.exe
  cmdChild: "C:\Users\admin\Downloads\Muadnrd.exe"
  cmdParent: "C:\Users\admin\Downloads\Muadnrd.exe"
- **Controlla le impostazioni di Sicurezza di Windows → Warning General:**
  value: 146432
  key:HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing
  typeValue: REG_DWORD
- **Legge le impostazioni di sicurezza → Warning System Security**:
  HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Security
  Typevalue: REG_SZ
- **Attiva CMD.exe per l'esecuzione dei comandi (Command Execution)** → Warning general.
  Image: C:\Windows\SysWOW64\cmd.exe
  Cmdline: "cmd" /c timeout 21 & exit
- Anche in questo caso si rintraccia anche l'azione di .**Net Reactor** usato per prevenire la reverse engeneering.


- Infine, viene avviato il processo **WerFault.exe** un modulo di report degli errori di Windows.

Gli Indicatori di compromissione sono:

- Connessione alla rete avviata.
- Processo si è bloccato.
- Il programma si lancia da solo.
- Il certificato non è valido.
- Lettura delle chiavi di registro di windows.
- Attivazione CMD.exe per l'esecuzione dei comandi.
- Il punteggio assegnato da VirusTotal dopo l'analisi.




**Best practise.**

L'esercizio ha dimostrato quanto sia importante seguire le seguenti best practise:

- Non scaricare ed eseguire programmi e applicazioni che hanno una provenienza dubbia e autore sconosciuto e il certificato digitale scaduto o non valido.
- Prima di scaricare un file è sempre bene farlo esaminare da scanner di virus (come VirusTotal) per rilevare la presenza di malware e altri tipi di minacce.
- Se possibile eseguire, aprire e scaricare file di dubbia provenienza in un ambiente controllato come una sandbox come Cuckoo o VMFlare per evitare di compromettere il sistema.
- Aggiornare il SO con le ultime patch di sicurezza e mantenere il SO aggiornato.

**N.B: noto anche delle incongruenze nella sezione DNS Request ma non so interpretarle del tutto.**

## Bonus 1: Esplorazione di Nmap.

**Obiettivi**

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

**Seguo i passaggi e rispondo alle domande.**

1) **Cos'è Nmap?** Nmap è un tool per scannerizzare la rete e fare audit di sicurezza.

```
NAME
       nmap - Network exploration tool and security / port scanner
```

2) **Per cosa viene usato nmap?** È utilizzato per scannerizzare rapidamente una rete estesa e per singoli host e determinare quali servizi sono attivi, quali porte sono aperte e qual è il sistema operativo degli host

```
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.
```

3) **Qual è il comando nmap usato nell'esempio 1?** Il comando usato è **nmap -A -t4 scanme.nmap.org.**
4) **Cosa fa l'opzione -A?** Rende possibile identificare il SO e la versione, il rilevamento delle versioni dei servizi, utilizza script Nmap per raccogliere ulteriori dettagli e vulnerabilità potenziali e può anche mostrare il percorso di rete verso l'host
5) **Cosa fa l'opzione -T4?** Rende l'esecuzione più veloce ottimizzando le tempistiche tra le richieste.

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

6) **Quali porte e servizi sono aperti? Registra il software che fornisce i servizi.**

   Porta 21 – ftp – vsftpd 2.0.8

   Porta 22 – ssh – Open SSH 7.7 (protocol 2.0)

```
Not shown: 998 closed ports
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 5
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 b4:91:f9:f9:d6:79:25:86:44:c7:9e:f8:e0:e7:5b:bb (RSA)
|   256 06:12:75:fe:b3:89:29:4f:8d:f3:9e:9a:d7:c6:03:52 (ECDSA)
|_  256 34:5d:f2:d3:5b:9f:b4:b6:08:96:a7:30:52:8c:96:06 (ED25519)
Service Info: Host: Welcome
```

**Passo 2: Scansiona la tua rete.**

7) **A quale rete appartiene la tua VM?** Inet 192.168.1.0/24
8) **Quanti host sono attivi?** 46 host.

**Passo 3: Scansiona un server remoto.**

9) **Qual è lo scopo del sito scanme.nmap.org?** Aiutare le persone a capire il funzionamento di nmap e per testare il funzionamento delle scansioni.
10) **Quali porte e servizi sono aperti?**

    22/tcp - ssh

    80/tcp – http

    9929/tcp nping-echo Nping echo

    31337/tcp - tcpwrapped

11) **Quali porte e servizi sono filtrati?** Nel mio caso nessuna porta e nessun servizio.

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2025-06-13 07:52 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.19s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed ports
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)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open  http       Apache httpd 2.4.7 ((Ubuntu))
|_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 29.99 seconds
```

12) **Qual è l'indirizzo IP del server?** 45.33.32.156
13) **Qual è il 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 è uno strumento prezioso in quanto permette di:

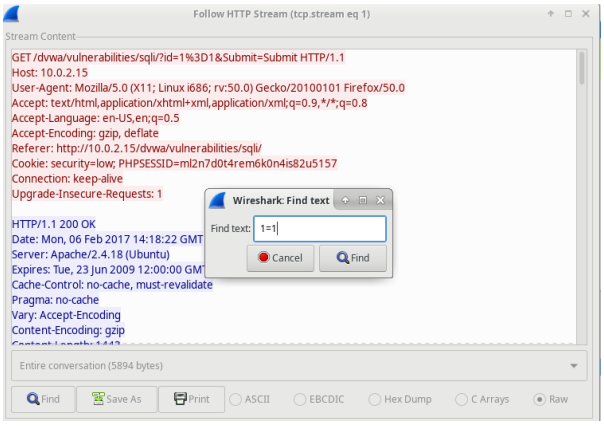
- identificare quali dispositivi sono connessi alla rete e quali servizi (come server web, database, ecc.) sono attivi.
- di individuare attraverso scansioni più approfondite porte aperte non autorizzate o servizi vulnerabili che potrebbero essere sfruttati da attaccanti.
- capire la topologia della rete, i dispositivi e le configurazioni, per migliorare la gestione e la sicurezza.
- Testare le difese attraverso la simulazione diretta di attacchi per verificare la robustezza delle misure di sicurezza implementate.

Nmap può anche essere uno strumento pericoloso in quanto permette ad un eventuale attaccante di effettuare tutte le operazioni sopra descritte con l'intenzione di nuocere ad un sistema o organizzazione.

## Bonus 2: Attacco a un database MySQL

14) **Quali sono i due indirizzi IP coinvolti in questo attacco di SQL injection in base alle informazioni visualizzate?**
IP sorgente 10.0.2.4
IP destinazione 10.0.2.15

**Seguo le istruzioni.**




1=1 → La stringa di ricerca crea un'istruzione SQL che sarà sempre vera.

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

**Seguo le istruzioni.**

```
..</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</
pre><pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Hack<br />Surname: Me</pre><pre>ID:
1' or 1=1 union select database(), user()#<br />First name: Pablo<br />Surname: Picasso</pre><pre>ID: 1' or 1=1
union select database(), user()#<br />First name: Bob<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union select
database(), user()#<br />First name: dvwa<br />Surname: root@localhost</pre>
.</div>
```

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

15) **Qual è la versione?** 5.7.12-0ubuntu1.1

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

16) **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’)?**
Il comando permetterebbe all’aggressore di ottenere una lista di tutte le colonne della tabella users, che potrebbe contenere dati sensibili come username, password, e-mail, ecc e potrebbe usare queste informazioni per ulteriori attacchi, come estrarre dati specifici o compromettere l'intero sistema.

**Parte 6: L'attacco di SQL Injection si conclude.**

17) **Quale utente ha l'hash della password di 8d3533d75ae2c3966d7e0d4fcc69216b?** L'utente 1337.
18) **Qual è la password in chiaro?** La password in chiaro è **'charley'**

| Hash | Type | Result |
|---|---|---|
| 8d3533d75ae2c3966d7e0d4fcc69216b | md5 | charley |

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

**Domande di riflessione.**

**Qual è il rischio che le piattaforme utilizzino il linguaggio SQL?** Per le piattaforme che non sono adeguatamente protette, l'uso del linguaggio SQL può esporre i dati sensibili a potenziali attacchi, come le SQL injection di cui abbiamo avuto un esempio nel file di cattura.

**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?**

- Il primo metodo è la **sanitizzazione dell'input dell'utente** assicurandosi che siano nel formato atteso e privi di caratteri o sequenze sospette.
- Utilizzare **query parametrizzate** in modo che l'input dell'utente venga trattato come semplice dato e non come parte del comando SQL.
- Implementare un firewall per applicazioni web (WAF)

Giulia Campagna

13/06/2025

Giulia Campagna