Relazione Tecnica Finale: Progetto Cyber Security & Ethical Hacking

Studente: Rocco Paolo Caccamo

Modulo: Cybersecurity & Ethical Hacking (Epicode)

Data: 20 Febbraio 2026

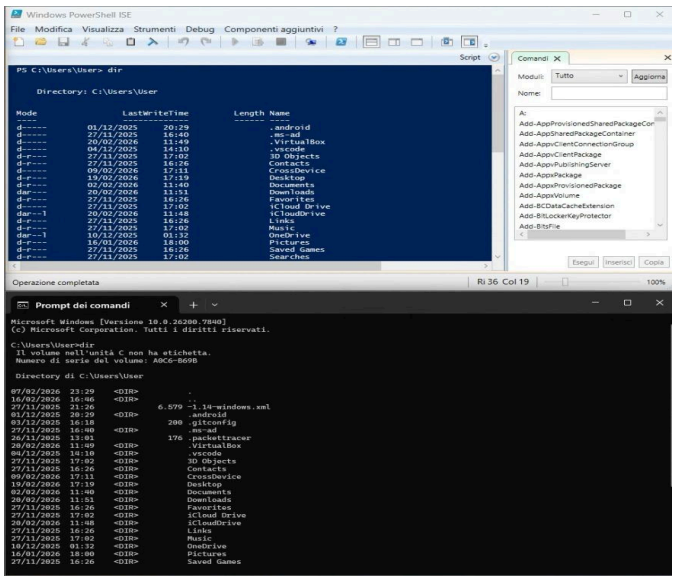
1. Gestione del Sistema tramite Windows PowerShell

Il primo laboratorio ha analizzato l'efficacia di **PowerShell** come motore di automazione. PowerShell si distingue dal prompt classico per la sua natura orientata agli oggetti e per l'integrazione profonda con il framework .NET.

Analisi Comparativa e Cmdlet

Durante i test, abbiamo risposto ai quesiti fondamentali sulle differenze operative tra le shell:

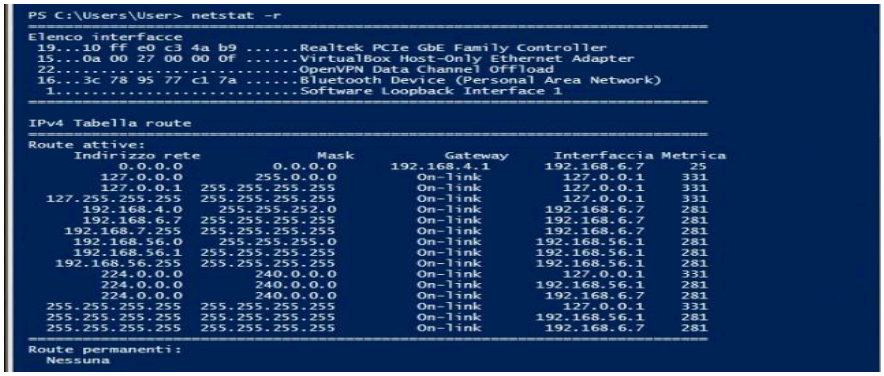
Output di `dir` e interoperabilità: Il test ha confermato che il comando `dir` elenca file e directory con attributi dettagliati. In PowerShell, questo è possibile perché `dir` è un **alias** del cmdlet nativo `Get-ChildItem`, come verificato tramite il comando `Get-Alias dir`.



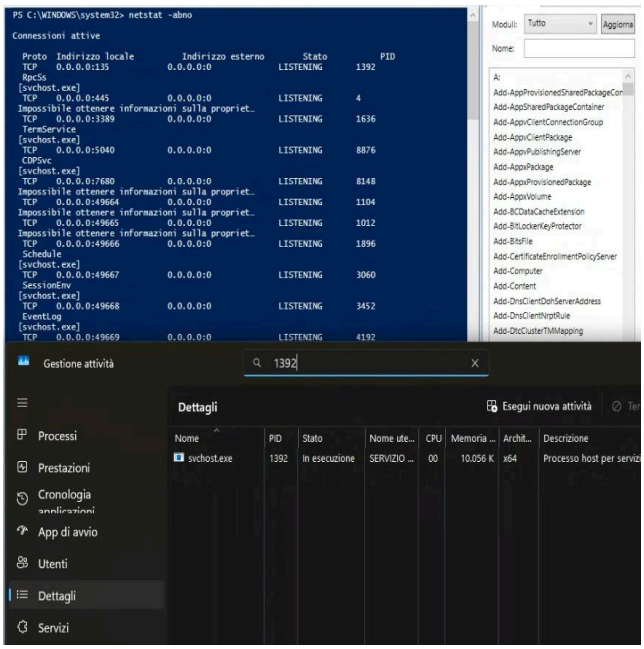
- **Strumenti di Diagnostica**: Comandi come `ping` e `ipconfig` mantengono la loro efficacia. La sessione di test ha mostrato una connessione stabile verso Google con una latenza di **21ms**.

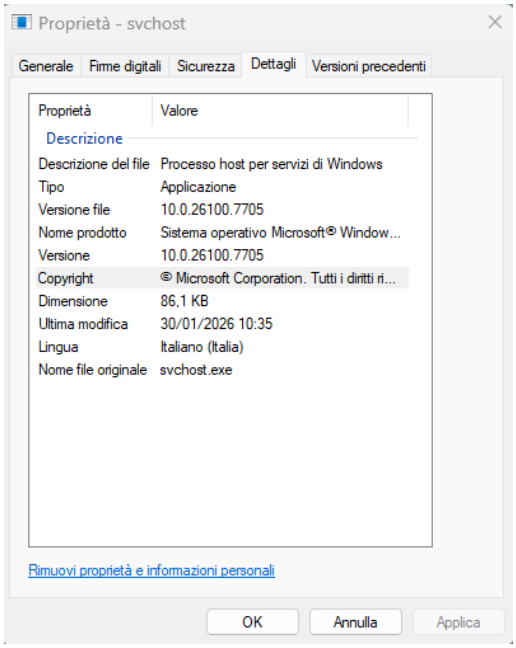
Monitoraggio di Rete e Sicurezza dei Processi

- **Identificazione del Gateway**: Attraverso l'analisi della tabella di routing con `netstat -r`, è stato isolato il Gateway IPv4 all'indirizzo **192.168.4.1**.



- **Analisi Forense dei Processi**: Per rispondere al quesito sulle informazioni ottenibili dal PID, è stato analizzato il processo **1392**. È stato identificato come `svchost.exe`, un processo host critico eseguito dall'utente `SERVIZIO DI RETE`. Le proprietà avanzate mostrano la collocazione in `System32` e la firma digitale





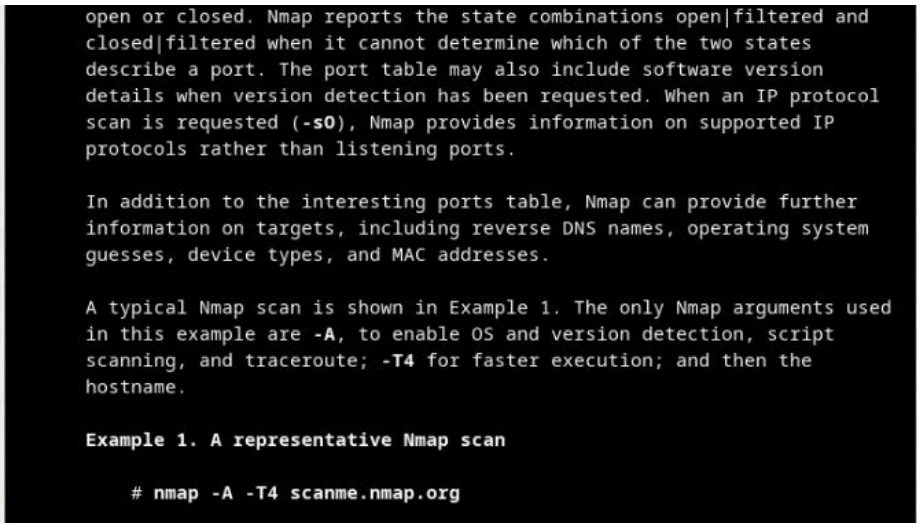
---

2. Network Scanning con Nmap

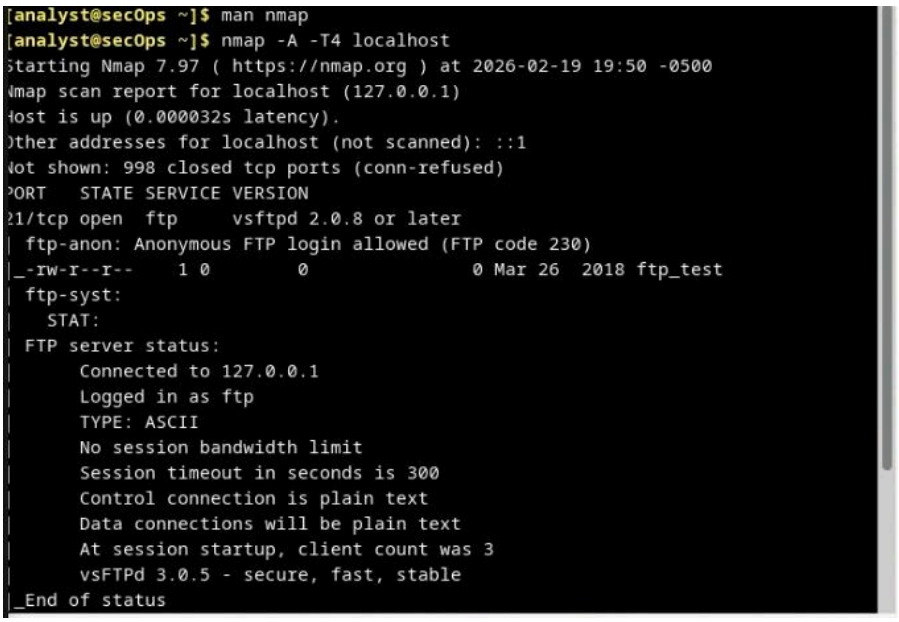
L'attività è proseguita con la fase di ricognizione tramite **Nmap**, lo standard industriale per la scoperta della rete e l'audit di sicurezza.

Riscontri Tecnici e Risposte al Manuale

- **Funzionalità di Nmap**: Consultando le pagine `man nmap`, abbiamo stabilito che l'opzione `-A` abilita il rilevamento completo (OS, versioni e script), mentre `-T4` ottimizza i tempi di scansione.



- **Scansione Localhost e LAN**: Il test sul localhost ha rivelato un servizio **FTP (porta 21)** gestito dal software **vsftpd 2.0.8**. La scansione della subnet `10.0.2.0/24` ha confermato la presenza di **1 host attivo** con servizi SSH e FTP configurati.



```
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-19 19:55 -0500
Nmap scan report for 10.0.2.15
Host is up (0.000032s latency).
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 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
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        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://nm
ap.org/submit/ .
Nmap done: 256 IP addresses (1 host up) scanned in 56.11 seconds
[analyst@secOps ~]$
```

- **Target Remoto (`scanme.nmap.org`)**: Il server risiede all'IP **45.33.32.156**. Oltre alle porte SSH (22) e HTTP (80), sono state identificate numerose porte in stato **filtered**, segno della presenza di un firewall o di filtri di pacchetto.

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-19 20:06 -0500
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:bb2
f
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; pro
tocol 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-title: Go ahead and ScanMe!
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-favicon: Nmap Project
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 28.96 seconds
[analyst@secOps ~]$
```

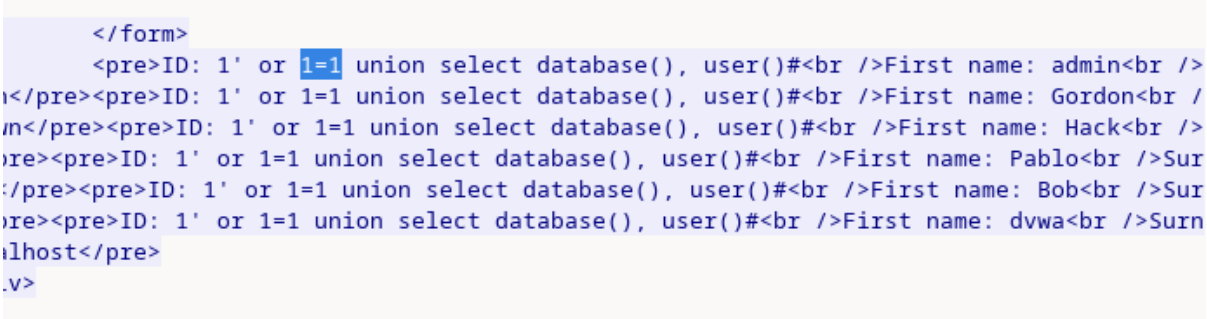
---

3. Analisi di un Attacco SQL Injection

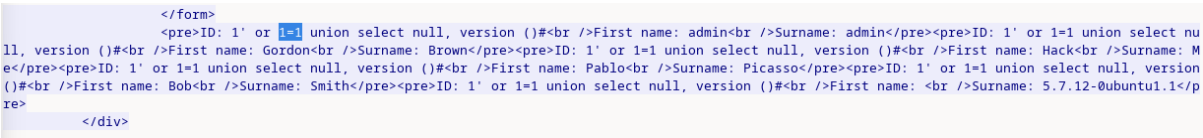
L'esame forense di un file PCAP in Wireshark ha permesso di decostruire un attacco di SQL Injection passo dopo passo.

Analisi del Flusso Dati

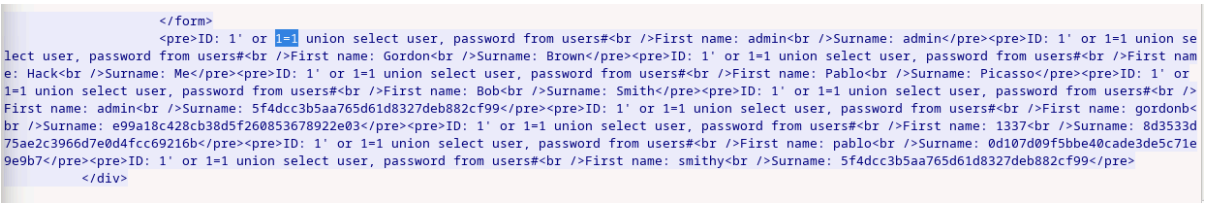
- **Vettori di Attacco**: L'attaccante (**10.0.2.4**) ha utilizzato stringhe come `1' or 1=1` per forzare il database a rispondere con dati non autorizzati.



- **Esfiltrazione**: Tramite iniezioni mirate, sono stati estratti il nome del database (**dvwa**), l'utente (**root@localhost**) e la versione del database (**5.7.12-0ubuntu1.1**).



- **Compromissione delle Credenziali**: L'attacco ha permesso il recupero degli hash delle password. L'utente `1337` è associato all'hash `8d3533d75ae2c3966d7e0d4fcc69216b`, che corrisponde alla password in chiaro `charley`.



---

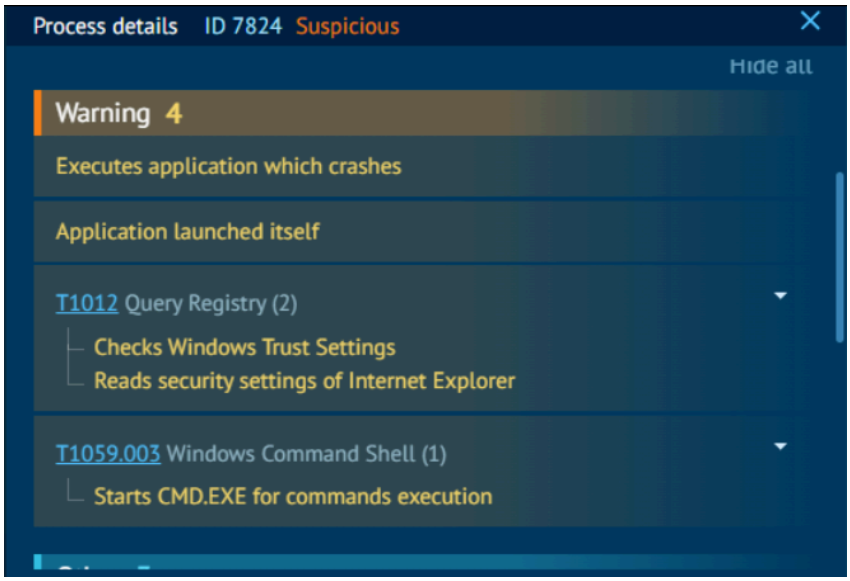
4. Analisi Malware con ANY.RUN

Infine, è stata condotta un'analisi dinamica sul malware `Muadnrd.exe` utilizzando la sandbox interattiva **ANY.RUN**.

Indicatori di Compromissione (IOC)

Il verdetto è di **"Malicious Activity"**. Il malware ha evidenziato comportamenti furtivi:

- **Evasione**: Query al registro di sistema (**T1012**) per analizzare le impostazioni di sicurezza.



- **Mascheramento**: Utilizzo di processi di sistema come `WerFault.exe` e `firefox.exe` per nascondere l'attività malevola.

- **Minacce di Rete**: Sono state rilevate **19 minacce di rete** durante l'analisi, indicando tentativi di comunicazione con server esterni C2.

---

5. Osservazioni Finali e Analisi Critica

A conclusione delle attività di laboratorio, è possibile trarre considerazioni di alto livello che integrano le nozioni teoriche con le evidenze pratiche riscontrate:

5.1 Il Ruolo dell'Automazione nella Difesa

L'utilizzo di **PowerShell** non è stato solo un esercizio di sintassi. La capacità di correlare PID (come il 1392) a servizi specifici (`svchost.exe`) e di analizzare tabelle di routing in tempo reale è la base della *Incident Response*. Un analista moderno deve saper automatizzare queste verifiche: un sistema compromesso può essere identificato più velocemente tramite script PowerShell che analizzano anomalie nei processi rispetto a un controllo manuale.

5.2 Nmap: La Doppia Faccia della Network Exploration

I test eseguiti su `scanme.nmap.org` e sulla rete LAN dimostrano che la visibilità è il primo passo sia per l'attacco che per la difesa.

- **Osservazione:** Il rilevamento di porte "filtered" indica la presenza di contromisure attive (Firewall/IDS).
- **Riflessione:** Per un Ethical Hacker, Nmap serve a mappare il perimetro; per un amministratore di sistema, serve a verificare che la superficie di attacco sia ridotta al minimo indispensabile (es. chiudere la porta 21 FTP se non necessaria, dato che vsftpd è un target comune).

5.3 La Fragilità del Perimetro Web (SQL Injection)

L'analisi forense dell'attacco SQLi ha evidenziato come un singolo punto di ingresso non sanitizzato (campo di input) possa portare alla compromissione totale della base dati.

- **Punto Critico:** L'esfiltrazione dell'hash MD5 (`8d3533d7...`) dimostra che anche se le password non sono in chiaro, l'uso di algoritmi obsoleti e la mancanza di "salt" rendono la protezione inefficace contro attacchi di dizionario (come dimostrato con CrackStation).
- **Soluzione Strategica:** Non basta filtrare i dati; è necessario adottare una difesa in profondità che includa **Prepared Statements**, hashing moderno (come Argon2 o bcrypt) e il principio del "minimo privilegio" per l'utente del database.

5.4 L'Evoluzione delle Minacce (Malware Analysis)

L'esperienza con **ANY.RUN** sul malware `Muadnrd.exe` sottolinea che il malware moderno non è più un semplice script, ma un software sofisticato capace di *evasione*. L'uso di processi legittimi (`WerFault.exe`) per scopi malevoli rende la rilevazione basata solo sulle firme (antivirus tradizionali) insufficiente, rendendo indispensabile l'analisi comportamentale (EDR/Sandboxing).

Conclusioni

Il progetto ha dimostrato che la sicurezza informatica non è un prodotto, ma un processo continuo. Dalla gestione dei privilegi locali in PowerShell alla messa in sicurezza delle query SQL, ogni passaggio è un anello di una catena. La vera sfida dell'hacking etico non è solo trovare la vulnerabilità, ma comprendere la logica che l'ha permessa per implementare soluzioni di mitigazione che siano strutturali e non solo temporanee.