

## **Relazione sullo Svolgimento del Laboratorio: 3.3.11 Lab – Using Windows PowerShell**

### **Introduzione**

Il laboratorio "Using Windows PowerShell" ha lo scopo di esplorare alcune delle funzionalità di PowerShell, uno strumento avanzato per l'automazione e la gestione dei sistemi operativi Windows. PowerShell è una combinazione tra un prompt dei comandi e un linguaggio di scripting, che permette agli utenti di eseguire comandi, automatizzare attività e interagire con il sistema operativo in modo efficiente. Attraverso questo laboratorio, sono state esaminate le differenze tra il tradizionale Command Prompt e PowerShell, nonché alcune funzionalità specifiche di quest'ultimo.

### **Parte 1: Accesso alla Console di PowerShell**

1. Accesso a PowerShell :
  - Ho aperto PowerShell cercandolo tramite il menu Start.
  - Successivamente, ho aperto anche il Command Prompt (Prompt dei Comandi) per confrontare i due ambienti.
2. Confronto tra PowerShell e Command Prompt :
  - Entrambi gli ambienti consentono di eseguire comandi, ma PowerShell offre funzionalità più avanzate grazie alla sua natura di linguaggio di scripting.
  - Ho notato che PowerShell utilizza un formato più strutturato e dettagliato per visualizzare i risultati dei comandi.

### **Parte 2: Esplorazione dei Comandi**

1. Comando `dir` :
  - Ho eseguito il comando `dir` sia in PowerShell che nel Command Prompt.
  - L'output di entrambi i comandi mostra una lista di file e cartelle, ma PowerShell include informazioni aggiuntive come attributi/mode, rendendo l'output più completo.

```
Windows PowerShell
PS C:\Users\Flavi> dir

Directory: C:\Users\Flavi

Mode                LastWriteTime         Length Name
----                -
d-----         10/04/2025         18:03         .VirtualBox
d-----         05/02/2025         10:52         .vscode
d-----         21/02/2025         09:45         Cisco Packet Tracer 8.2.2
d-r-----        15/02/2025         18:28         Contacts
d-----        12/03/2024         23:37         Documents
d-r-----        11/04/2025         00:07         Downloads
d-r-----        15/02/2025         18:28         Favorites
d-r-----        15/02/2025         18:28         Links
d-r-----        15/02/2025         18:28         Music
dar--l         11/04/2025         09:02         OneDrive
d-r-----        15/02/2025         18:28         Saved Games
d-r-----        15/02/2025         18:28         Searches
d-r-----        15/02/2025         18:28         Videos
-a-----        21/02/2025         09:43         176 .packettracer

PS C:\Users\Flavi>
```

```
Prompt dei comandi
Il volume nell'unità C è Windows
Numero di serie del volume: 1A4A-6320

Directory di C:\Users\Flavi

11/04/2025  09:01  <DIR>         .
15/02/2025  02:45  <DIR>         ..
21/02/2025  10:43                176 .packettracer
10/04/2025  18:03  <DIR>         .VirtualBox
05/02/2025  11:52  <DIR>         .vscode
21/02/2025  10:45  <DIR>         Cisco Packet Tracer 8.2.2
15/02/2025  19:28  <DIR>         Contacts
13/03/2024  00:37  <DIR>         Documents
11/04/2025  00:07  <DIR>         Downloads
15/02/2025  19:28  <DIR>         Favorites
15/02/2025  19:28  <DIR>         Links
15/02/2025  19:28  <DIR>         Music
11/04/2025  09:02  <DIR>         OneDrive
15/02/2025  19:28  <DIR>         Saved Games
15/02/2025  19:28  <DIR>         Searches
15/02/2025  19:28  <DIR>         Videos
          1 File          176 byte
        15 Directory 183.541.231.616 byte disponibili

C:\Users\Flavi>
```

## 2. Altri Comandi :

- Ho testato altri comandi comuni, come ping, cd e ipconfig, in entrambi gli ambienti.
- I risultati sono simili, ma PowerShell offre una maggiore flessibilità e possibilità di elaborazione avanzata dei dati.

```
Windows PowerShell
d-r--- 11/04/2025 00:07 Downloads
d-r--- 15/02/2025 18:28 Favorites
d-r--- 15/02/2025 18:28 Links
d-r--- 15/02/2025 18:28 Music
dar--l 11/04/2025 09:02 OneDrive
d-r--- 15/02/2025 18:28 Saved Games
d-r--- 15/02/2025 18:28 Searches
d-r--- 15/02/2025 18:28 Videos
-a--- 21/02/2025 09:43 176 .packettracer

PS C:\Users\Flavi> ping www.google.com

Esecuzione di Ping www.google.com [142.251.209.36] con 32 byte di dati:
Risposta da 142.251.209.36: byte=32 durata=14ms TTL=115
Risposta da 142.251.209.36: byte=32 durata=14ms TTL=115
Risposta da 142.251.209.36: byte=32 durata=14ms TTL=115
Risposta da 142.251.209.36: byte=32 durata=14ms TTL=115

Statistiche Ping per 142.251.209.36:
  Pacchetti: Trasmessi = 4, Ricevuti = 4,
  Persi = 0 (0% persi),
  Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 14ms, Massimo = 14ms, Medio = 14ms
PS C:\Users\Flavi>
```

```
Prompt dei comandi
15/02/2025 19:28 <DIR> Favorites
15/02/2025 19:28 <DIR> Links
15/02/2025 19:28 <DIR> Music
11/04/2025 09:02 <DIR> OneDrive
15/02/2025 19:28 <DIR> Saved Games
15/02/2025 19:28 <DIR> Searches
15/02/2025 19:28 <DIR> Videos
          1 File          176 byte
          15 Directory 183.541.231.616 byte disponibili

C:\Users\Flavi>ping www.google.com

Esecuzione di Ping www.google.com [142.251.209.36] con 32 byte di dati:
Risposta da 142.251.209.36: byte=32 durata=14ms TTL=115
Risposta da 142.251.209.36: byte=32 durata=13ms TTL=115
Risposta da 142.251.209.36: byte=32 durata=14ms TTL=115
Risposta da 142.251.209.36: byte=32 durata=14ms TTL=115

Statistiche Ping per 142.251.209.36:
  Pacchetti: Trasmessi = 4, Ricevuti = 4,
  Persi = 0 (0% persi),
  Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 13ms, Massimo = 14ms, Medio = 13ms
C:\Users\Flavi>
```

### Parte 3: Esplorazione dei Cmdlets

#### 1. Cmdlets in PowerShell :

- Ho scoperto che i comandi in PowerShell, chiamati cmdlets , seguono una struttura standard del tipo "verbo-nome". Ad esempio, il comando dir è in realtà un alias per il cmdlet Get-ChildItem.
- Utilizzando il comando Get-Alias dir, ho verificato che dir corrisponde effettivamente a Get-ChildItem.

```
Amministratore: Windows PowerShell

PS C:\WINDOWS\system32> Get-Alias dir

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

PS C:\WINDOWS\system32>
```

## 2. Ricerca Online :

- Ho effettuato una ricerca su Internet per approfondire i cmdlets disponibili in PowerShell, scoprendo che esistono migliaia di cmdlets per automatizzare compiti complessi.

## Parte 4: Esplorazione del Comando netstat

### 1. Opzioni di netstat :

- Ho eseguito il comando netstat -help per visualizzare le opzioni disponibili per il comando netstat. Questo comando fornisce informazioni sulle connessioni di rete attive, le porte in ascolto e altre statistiche di rete.

```
PS C:\Users\Flavi> netstat --help

Mostra le statistiche del protocollo e le connessioni di rete TCP/IP correnti.

NETSTAT [-a] [-b] [-e] [-f] [-i] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

-a          Mostra tutte le connessioni e le porte di ascolto.
-b          Mostra l'eseguibile coinvolto nella creazione di ogni connessione o
           porta di ascolto. In alcuni casi, eseguibili noti ospitano
           più componenti indipendenti e in questi casi la
           sequenza dei componenti coinvolti nella creazione della connessione
           o della porta di ascolto viene visualizzata. In questo caso, il nome dell'eseguibile
           è in [] in basso, in alto si trova il componente chiamato,
           e così via fino al raggiungimento di TCP/IP. Tenere presente che questa opzione
           può essere dispendiosa in termini di tempo e non andrà a buon fine a meno che non si disponga delle
           autorizzazioni sufficienti.
-c          Visualizza un elenco di processi ordinati in base al numero di
TCP o UDP   porte attualmente utilizzate.
-d          Mostra il valore DSCP associato a ogni connessione.
-e          Mostra le statistiche Ethernet. Potrebbe essere in combinazione con l'opzione
           -s.
-f          Mostra Fully Qualified Domain Names (FQDN) per gli indirizzi
           stranieri.
-i          Mostra il tempo in cui una connessione TCP si trova nel suo stato corrente.
-n          Mostra i numeri di indirizzi e porte in formato numerico.
-o          Mostra l'ID processo di proprietà associato a ogni connessione.
-p proto    Mostra le connessioni per il protocollo specificato dal protocollo; il protocollo
           può essere: TCP, UDP, ICMPv6 o UDPv6. Se usato con l'opzione -s
           per mostrare le statistiche per protocollo, il protocollo potrebbe essere:
           IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
-q          Mostra tutte le connessioni, le porte di ascolto e le porte
           TCP non di ascolto associate. Le porte non di ascolto associate potrebbero essere associate o meno
           a una connessione attiva.
-r          Mostra la tabella di routing.
-s          Mostra le statistiche per protocollo. Per impostazione predefinita, le statistiche vengono
           mostrate per IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP e UDPv6;
           l'opzione -p potrebbe essere usata per specificare un sottoinsieme dell'opzione predefinita.
-t          Mostra lo stato di offload della connessione corrente.
-x          Mostra connessioni NetworkDirect, listener ed endpoint
           condivisi.
-y          Mostra il modello di connessione TCP per tutte le connessioni.
           Non può essere in combinazione con altre opzioni.
interval    Mostra di nuovo le statistiche selezionate, inserendo intervalli di secondi
           tra ogni visualizzazione. Premi CTRL+C per interrompere la nuova visualizzazione delle
           statistiche. Se omissa, netstat stamperà le
           informazioni sulla configurazione corrente una volta.

PS C:\Users\Flavi>
```

## 2. Visualizzazione della Tabella di Routing :

- Con il comando `netstat -r`, ho visualizzato la tabella di routing IPv4 e IPv6. Nell'esempio fornito, il gateway predefinito era 192.168.1.1.

```
PS C:\Users\Flavi> netstat -r

=====
Elenco interfacce
23.....NordLynx Tunnel
16...00 d8 61 e5 68 c9 .....Realtek PCIe GbE Family Controller
4...0a 00 27 00 00 04 .....VirtualBox Host-Only Ethernet Adapter
3.....OpenVPN Data Channel Offload
10...00 ff 3f e0 4c be .....TAP-NordVPN Windows Adapter V9
5...4c 1d 96 6c a7 60 .....Microsoft Wi-Fi Direct Virtual Adapter
6...4e 1d 96 6c a7 5f .....Microsoft Wi-Fi Direct Virtual Adapter #2
20...4c 1d 96 6c a7 5f .....Intel(R) Wi-Fi 6 AX200 160MHz
19...4c 1d 96 6c a7 63 .....Bluetooth Device (Personal Area Network)
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      192.168.1.2      25
      10.5.0.0      255.255.0.0      On-link      10.5.0.2      261
      10.5.0.2      255.255.255.255      On-link      10.5.0.2      261
      10.5.255.255      255.255.255.255      On-link      10.5.0.2      261
      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      192.168.1.2      281
      192.168.1.2      255.255.255.255      On-link      192.168.1.2      281
      192.168.1.255      255.255.255.255      On-link      192.168.1.2      281
      192.168.56.0      255.255.255.0      On-link      192.168.56.1      281
      192.168.56.1      255.255.255.255      On-link      192.168.56.1      281
      192.168.56.255      255.255.255.255      On-link      192.168.56.1      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      192.168.56.1      281
      224.0.0.0      240.0.0.0      On-link      192.168.1.2      281
      224.0.0.0      240.0.0.0      On-link      10.5.0.2      261
      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      192.168.56.1      281
      255.255.255.255      255.255.255.255      On-link      192.168.1.2      281
      255.255.255.255      255.255.255.255      On-link      10.5.0.2      261
=====
Route permanenti:
Nessuna
```

```
IPv6 Tabella route
=====
Route attive:
Interf Metrica Rete Destinazione      Gateway
-----
1      331 ::1/128      On-link
4      281 fe80::/64      On-link
16     281 fe80::/64      On-link
23     261 fe80::/64      On-link
16     281 fe80::581d:e30d:935e:77db/128      On-link
4      281 fe80::6420:aa16:99e2:8bd7/128      On-link
23     261 fe80::b919:4b0e:da8d:471f/128      On-link
1      331 ff00::/8      On-link
4      281 ff00::/8      On-link
16     281 ff00::/8      On-link
23     261 ff00::/8      On-link
=====
Route permanenti:
Nessuna
```

### 3. Processi Associati alle Connessioni TCP :

- Ho eseguito il comando `netstat -abno` per visualizzare i processi associati alle connessioni TCP attive. Questo comando include anche l'ID del processo (PID).

```
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  1892
RpcEptMapper
[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  5160
CDPSvc
[svchost.exe]
TCP    0.0.0.0:5426             0.0.0.0:0            LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:7680             0.0.0.0:0            LISTENING  13568
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49664            0.0.0.0:0            LISTENING  1616
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49665            0.0.0.0:0            LISTENING  1440
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49666            0.0.0.0:0            LISTENING  2336
Schedule
[svchost.exe]
TCP    0.0.0.0:49667            0.0.0.0:0            LISTENING  3256
```

- Utilizzando Task Manager, ho individuato il processo associato al PID 8256, scoprendo che si trattava di `AggregatorHost.exe`, un servizio di sistema in esecuzione con privilegi di rete.

Dettagli							
Nome	PID	Stato	Nome ute...	CPU	Memoria (...)	Archite...	Descrizione
AggregatorHost.exe	8256	In esecuzione	SYSTEM	00	4.956 K	x64	Microsoft (R) Aggregator Host
amdfendrsr.exe	3244	In esecuzione	SYSTEM	00	1.536 K	x64	AMD Crash Defender Service
amdow.exe	18500	In esecuzione	Flavi	00	868 K	x64	Radeon Settings: Desktop Overlay
AMDRSServ.exe	3252	In esecuzione	Flavi	00	3.044 K	x64	Radeon Settings: Host Service
AMDRSSrcExt.exe	5364	In esecuzione	Flavi	00	13.492 K	x64	Radeon Settings: Source Extension
ApplicationFrameHo...	3772	In esecuzione	Flavi	00	21.020 K	x64	Application Frame Host

## Parte 5: Svuotamento del Cestino con PowerShell

### 1. Preparazione :

- Ho riempito il Cestino con alcuni file di prova, come documenti di testo creati con Notepad.

### 2. Svuotamento del Cestino :

- Ho eseguito il comando `clear-recyclebin` in PowerShell per svuotare il Cestino. Il sistema ha richiesto una conferma prima di procedere.
- Dopo aver confermato l'operazione, tutti i file nel Cestino sono stati eliminati definitivamente.

```
PS C:\Users\Flavi> 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"):
```

## Riflessioni Finali

PowerShell è uno strumento estremamente potente per la gestione e l'automazione di sistemi Windows. Durante il laboratorio, ho apprezzato la versatilità e la precisione dei cmdlets rispetto ai comandi tradizionali del Command Prompt. In particolare, ho trovato interessante la possibilità di combinare comandi per ottenere risultati complessi, come l'identificazione dei processi associati alle connessioni di rete.

Durante la ricerca online, ho scoperto ulteriori comandi utili per un analista della sicurezza, come:

- `Get-Process`: Visualizza i processi in esecuzione.
- `Stop-Process`: Termina un processo specifico.
- `Get-EventLog`: Recupera i log di sistema per l'analisi delle minacce.
- `Invoke-WebRequest`: Esegue richieste HTTP/HTTPS per testare API o siti web.

Questi comandi possono essere utilizzati per automatizzare attività ripetitive, monitorare la sicurezza della rete e rispondere rapidamente a incidenti.

## Conclusioni

Il laboratorio mi ha permesso di acquisire una comprensione pratica delle funzionalità di base di PowerShell e di apprezzarne il potenziale per l'automazione e

la gestione dei sistemi. PowerShell è uno strumento indispensabile per chi lavora nel campo della sicurezza informatica, poiché consente di eseguire operazioni complesse in modo rapido ed efficiente. Continuerò a esplorare ulteriormente le sue funzionalità per migliorare le mie competenze in ambito di sicurezza e automazione.



## Relazione sullo Svolgimento del Laboratorio: 10.6.7 Lab – Using Wireshark to Examine HTTP and HTTPS Traffic

### Introduzione

Il laboratorio "Using Wireshark to Examine HTTP and HTTPS Traffic" si propone di esplorare le differenze tra il traffico di rete generato da protocolli HTTP e HTTPS utilizzando strumenti di cattura e analisi del traffico come tcpdump e Wireshark. Il protocollo HTTP (HyperText Transfer Protocol) è un protocollo di livello applicazione che trasmette dati in chiaro, mentre HTTPS (HTTP Secure) aggiunge uno strato di sicurezza crittografica per proteggere i dati scambiati tra client e server. Durante il laboratorio, ho utilizzato la macchina virtuale CyberOps Workstation per acquisire e analizzare pacchetti di rete relativi a sessioni HTTP e HTTPS.

### Parte 1: Cattura e Visualizzazione del Traffico HTTP

1. Avvio della Macchina Virtuale e Apertura del Terminale :
  - Ho avviato la macchina virtuale CyberOps Workstation e mi sono autenticato con le credenziali fornite:
    - Username: analyst
    - Password: cyberops.
2. Identificazione dell'Interfaccia di Rete :
  - Utilizzando il comando ip address, ho identificato l'interfaccia di rete principale (enp0s3) e il suo indirizzo IP (10.0.2.15).

```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
[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
       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:ad:8d:f0 brd ff:ff:ff:ff:ff:ff
   inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 86357sec preferred_lft 86357sec
   inet6 fd00::a00:27ff:fead:8df0/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 86358sec preferred_lft 14358sec
   inet6 fe80::a00:27ff:fead:8df0/64 scope link
       valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```

3. Cattura del Traffico HTTP con tcpdump :
  - Ho avviato tcpdump con il seguente comando:

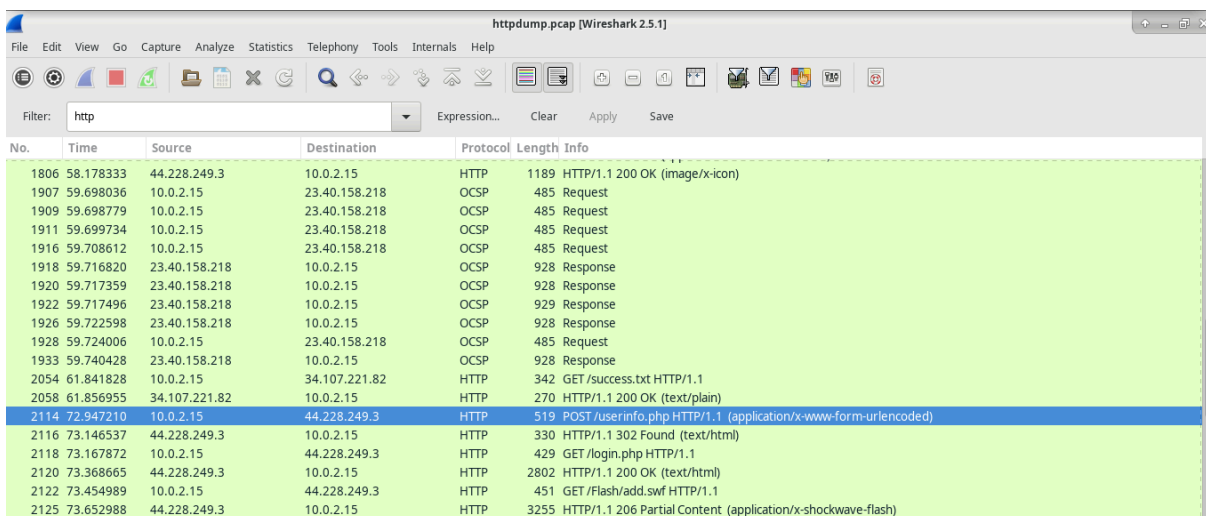
- `sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap`

```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

- `-i enp0s3`: Specifica l'interfaccia di rete da monitorare.
- `-s 0`: Imposta la lunghezza dello snapshot a 0, catturando l'intero pacchetto.
- `-w httpdump.pcap`: Salva i pacchetti catturati in un file .pcap per l'analisi successiva.
- Ho quindi visitato il sito web <http://testphp.vulnweb.com/login.php> utilizzando un browser all'interno della VM. Dopo aver inserito le credenziali (test come nome utente e password), ho chiuso il browser e interrotto la cattura premendo CTRL+C.

#### 4. Analisi del Traffico HTTP con Wireshark :

- Ho aperto il file `httpdump.pcap` in Wireshark e applicato un filtro per visualizzare solo il traffico HTTP (`http`).
- Ho selezionato un messaggio HTTP POST contenente le credenziali inviate al server. Espandendo la sezione HTML Form URL Encoded, ho osservato che le informazioni relative al nome utente (`uid=test`) e alla password (`passw=test`) erano visibili in chiaro.



No.	Time	Source	Destination	Protocol	Length	Info
1806	58.178333	44.228.249.3	10.0.2.15	HTTP	1189	HTTP/1.1 200 OK (image/x-icon)
1907	59.698036	10.0.2.15	23.40.158.218	OCSP	485	Request
1909	59.698779	10.0.2.15	23.40.158.218	OCSP	485	Request
1911	59.699734	10.0.2.15	23.40.158.218	OCSP	485	Request
1916	59.708612	10.0.2.15	23.40.158.218	OCSP	485	Request
1918	59.716820	23.40.158.218	10.0.2.15	OCSP	928	Response
1920	59.717359	23.40.158.218	10.0.2.15	OCSP	928	Response
1922	59.717496	23.40.158.218	10.0.2.15	OCSP	929	Response
1926	59.722598	23.40.158.218	10.0.2.15	OCSP	928	Response
1928	59.724006	10.0.2.15	23.40.158.218	OCSP	485	Request
1933	59.740428	23.40.158.218	10.0.2.15	OCSP	928	Response
2054	61.841828	10.0.2.15	34.107.221.82	HTTP	342	GET /success.txt HTTP/1.1
2058	61.856955	34.107.221.82	10.0.2.15	HTTP	270	HTTP/1.1 200 OK (text/plain)
2114	72.947210	10.0.2.15	44.228.249.3	HTTP	519	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
2116	73.146537	44.228.249.3	10.0.2.15	HTTP	330	HTTP/1.1 302 Found (text/html)
2118	73.167872	10.0.2.15	44.228.249.3	HTTP	429	GET /login.php HTTP/1.1
2120	73.368665	44.228.249.3	10.0.2.15	HTTP	2802	HTTP/1.1 200 OK (text/html)
2122	73.454989	10.0.2.15	44.228.249.3	HTTP	451	GET /Flash/add.swf HTTP/1.1
2125	73.652988	44.228.249.3	10.0.2.15	HTTP	3255	HTTP/1.1 206 Partial Content (application/x-shockwave-flash)

No.	Time	Source	Destination	Protocol	Length	Info
2114	72.947210	10.0.2.15	44.228.249.3	HTTP	519	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
2116	73.146537	44.228.249.3	10.0.2.15	HTTP	330	HTTP/1.1 302 Found (text/html)

▶ Frame 2114: 519 bytes on wire (4152 bits), 519 bytes captured (4152 bits)  
 ▶ Ethernet II, Src: PcsCompu\_ad:8d:f0 (08:00:27:ad:8d:f0), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)  
 ▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 44.228.249.3  
 ▶ Transmission Control Protocol, Src Port: 58076, Dst Port: 80, Seq: 920, Ack: 10784, Len: 465  
 ▶ Hypertext Transfer Protocol  
 ▼ HTML Form URL Encoded: application/x-www-form-urlencoded

▼ Form item: "uname" = "Admin"  
 Key: uname  
 Value: Admin  
 ▼ Form item: "pass" = ""  
 Key: pass  
 Value:

```

0100 2a 3b 71 3d 30 2e 38 0d 0a 41 63 63 65 70 74 2d *;q=0.8..Accept-
0110 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55 53 2c Language : en-US,
0120 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74 en;q=0.5..Accept
0130 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c -Encodin g: gzip,
0140 20 64 65 6e 66 61 74 65 0d 0a 52 65 66 65 72 65 -Eflate ..Refere
0150 72 3a 20 68 74 74 70 3a 2f 2f 74 65 73 74 70 68 r: http://testph
0160 70 2e 76 75 6c 6e 77 65 62 2e 63 6f 6d 2f 6c 6f p.vulnwe b.com/lo
0170 67 69 6e 2e 70 68 70 0d 0a 43 6f 6e 74 65 6e 74 gin.php. Content
0180 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69 -Type: a pplicati
0190 6f 6e 2f 78 2d 77 77 77 2d 66 6f 72 6d 2d 75 72 on/x-www-form-ur
01a0 6c 65 6e 63 6f 64 65 64 0d 0a 43 6f 6e 74 65 6e lencoded ..Conten
01b0 74 2d 4c 65 6e 67 74 68 3a 20 31 37 0d 0a 43 6f t-Length : 17..Co
01c0 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection : keep-a
01d0 6c 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e live..Up grade-In
01e0 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a secure-R equests:
01f0 20 31 0d 0a 0d 0a 75 6e 61 6d 65 3d 41 64 6d 69 1....un ame=Admi
0200 6e 26 70 61 73 73 3d n&pass=
  
```

## Parte 2: Cattura e Visualizzazione del Traffico HTTPS

### 1. Cattura del Traffico HTTPS con tcpdump :

- Ho avviato nuovamente tcpdump con un comando simile, ma questa volta ho salvato il traffico in un file chiamato httpsdump.pcap:
- `sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap`

```

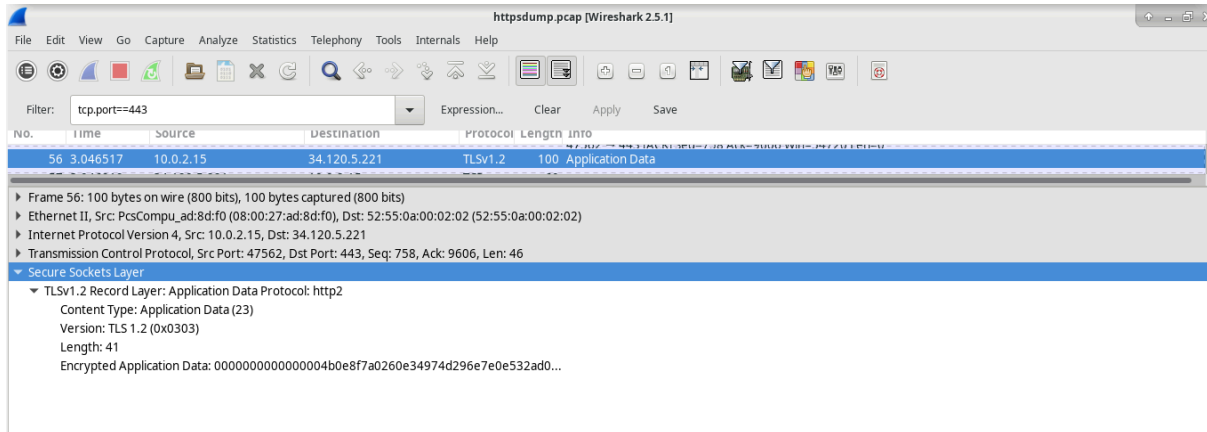
[analyst@sec0ps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
  
```

- Ho visitato il sito web <https://www.netacad.com> e ho effettuato il login utilizzando le mie credenziali NetAcad. Dopo aver completato l'operazione, ho chiuso il browser e interrotto la cattura premendo CTRL+C.

### 2. Analisi del Traffico HTTPS con Wireshark :

- Ho aperto il file httpsdump.pcap in Wireshark e applicato un filtro per visualizzare solo il traffico HTTPS (`tcp.port==443`).
- Ho selezionato un messaggio Application Data relativo alla sessione HTTPS. A differenza del traffico HTTP, il contenuto del messaggio era crittografato e non leggibile.

- Espandendo la sezione Secure Sockets Layer (SSL/TLS 1.2), ho notato che i dati erano protetti da TLSv1.2, rendendo impossibile la visualizzazione delle informazioni sensibili.



## Riflessioni Finali

Durante il laboratorio, ho compreso chiaramente le differenze fondamentali tra HTTP e HTTPS:

- HTTP : Il traffico è in chiaro, il che lo rende vulnerabile a intercettazioni e attacchi come il packet sniffing. Le informazioni sensibili, come credenziali e dati personali, possono essere facilmente lette da un attaccante.
- HTTPS : Il traffico è crittografato utilizzando protocolli come TLS, garantendo la confidenzialità e l'integrità dei dati. Anche se un attaccante intercetta il traffico, non può decifrare i dati senza la chiave crittografica.

L'utilizzo di strumenti come tcpdump e Wireshark è stato fondamentale per comprendere il funzionamento di questi protocolli. La capacità di analizzare il traffico di rete è una competenza essenziale per un analista della sicurezza informatica, poiché permette di identificare comportamenti anomali o sospetti.

## Conclusioni

Questo laboratorio ha fornito una panoramica pratica sulle differenze tra HTTP e HTTPS e sull'importanza della crittografia nel traffico di rete. Ho appreso come utilizzare strumenti come tcpdump per catturare il traffico e Wireshark per analizzarlo.

Queste competenze sono cruciali per monitorare e proteggere le reti da potenziali minacce.

In futuro, continuerò ad approfondire l'uso di questi strumenti per migliorare le mie capacità di analisi del traffico di rete e per riconoscere attività sospette o malevole.

## **Relazione sullo Svolgimento del Laboratorio: 9.3.8 Lab – Exploring Nmap**

### **Introduzione**

Il laboratorio "Exploring Nmap" si propone di esplorare l'utilizzo di Nmap , uno strumento potente per la scansione della rete e l'analisi della sicurezza. Nmap è ampiamente utilizzato per scoprire host, servizi e vulnerabilità all'interno di una rete. Durante il laboratorio, ho imparato a utilizzare le funzionalità di base di Nmap per identificare porte aperte, servizi attivi e informazioni sul sistema operativo sia su dispositivi locali che remoti.

### **Parte 1: Esplorazione di Nmap**

1. Avvio della Macchina Virtuale e Accesso al Terminale :
  - Ho avviato la macchina virtuale CyberOps Workstation e mi sono autenticato con le credenziali fornite:
    - Username: analyst
    - Password: cyberops.
2. Consultazione delle Pagine del Manuale (man pages) :
  - Ho utilizzato il comando `man nmap` per consultare le pagine del manuale di Nmap.

**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.

The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key among that information is the "interesting ports table". That table lists the port number and protocol, service name, and state. The state is either open, filtered, closed, or unfiltered. Open means that an application on the target machine is listening for connections/packets on that port. Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed. Closed ports have no application listening on them, though they could open up at any time. Ports are classified as unfiltered when they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or closed. Nmap reports the state combinations open|filtered and closed|filtered when it cannot determine which of the two states describe a port. The port table may also include software version details when version detection has been requested. When an IP protocol scan is requested (**-s0**), Nmap provides information on supported IP protocols rather than listening ports.

In addition to the interesting ports table, Nmap can provide further information on targets, including reverse DNS names, operating system guesses, device types, and MAC addresses.

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.

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

TRACEROUTE (using port 53/tcp)
HOP RTT ADDRESS
[Cut first 10 hops for brevity]
11 17.65 ms li86-221.members.linode.com (74.207.244.221)

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
```

The newest version of Nmap can be obtained from <https://nmap.org>. The newest version of this man page is available at <https://nmap.org/book/nan.html>. It is also included as a chapter of Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning (see <https://nmap.org/book/>).

- Attraverso le man pages, ho scoperto che Nmap è un tool di esplorazione della rete e di scansione della sicurezza. È utilizzato per identificare host attivi, porte aperte, servizi in esecuzione e sistemi operativi.
3. Funzionalità Principali di Nmap :
    - Ho appreso che Nmap può essere utilizzato per:
      - Scoprire host attivi nella rete.
      - Identificare porte aperte e servizi associati.
      - Rilevare il sistema operativo e altre informazioni critiche.
      - Eseguire test di sicurezza per individuare vulnerabilità.
  4. Switch Analizzati :
    - -A: Abilita la rilevazione del sistema operativo, la versione dei servizi, lo script scanning e il traceroute.
    - -T4: Aumenta la velocità di esecuzione limitando il ritardo dinamico delle scansioni TCP a 10 ms.
  5. Esplorazione delle Opzioni :
    - Utilizzando i comandi di ricerca (/example), ho esaminato esempi pratici di utilizzo di Nmap. Ad esempio, il comando `nmap -A -T4 scanme.nmap.org` è stato analizzato per comprendere come eseguire una scansione avanzata su un server remoto.

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

1. Scansione del localhost :
  - Ho eseguito il comando `nmap -A -T4 localhost` per analizzare il mio dispositivo locale.



```

[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-04-11 07:56 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000038s latency).
Other addresses for localhost (not scanned): ::1
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 3
|   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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.75 seconds

```

- Risultati:
  - Porte aperte :
    - 21/tcp: Servizio FTP (vsftpd).
    - 22/tcp: Servizio SSH (OpenSSH).
  - Software associato :
    - FTP: vsftpd.
    - SSH: OpenSSH.

## 2. Scansione della Rete Locale :

- Ho determinato l'indirizzo IP e la subnet mask della mia VM utilizzando il comando ip address.

```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
[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
        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:ad:8d:f0 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 86357sec preferred_lft 86357sec
    inet6 fd00::a00:27ff:fead:8df0/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86358sec preferred_lft 14358sec
    inet6 fe80::a00:27ff:fead:8df0/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```

- Ho eseguito il comando `nmap -A -T4 <network_address>/<prefix>` per scansionare la rete locale. Ad esempio:
- `nmap -A -T4 10.0.2.0/24`

```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2025-04-11 08:23 EDT
Nmap scan report for 10.0.2.15
Host is up (0.000044s latency).
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 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 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (1 host up) scanned in 26.53 seconds
```

- Risultati:
  - Ho identificato gli host attivi nella rete locale.
  - Per ogni host, ho elencato le porte aperte e i servizi disponibili. Ad esempio:
    - 21/tcp: FTP.
    - 22/tcp: SSH.

### 3. Scansione di un Server Remoto :

- Ho visitato il sito [scanme.nmap.org](https://scanme.nmap.org) per ottenere informazioni sul suo scopo. Il sito consente agli utenti di testare Nmap in modo sicuro.
- Ho eseguito il comando:
- `nmap -A -T4 scanme.nmap.org`

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2025-04-11 08:35 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 filtered 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 30.37 seconds
```

- Risultati:
  - Porte aperte :
    - 22/tcp: SSH.
    - 80/tcp: HTTP.
    - 9929/tcp: Nping-echo.
    - 31337/tcp: tcpwrapped.
  - Porte filtrate :
    - 25/tcp: SMTP.
    - 135/tcp: MSRPC.
    - 139/tcp: NetBIOS.
    - 445/tcp: Microsoft-DS.
  - Indirizzo IP :
    - IPv4: 45.33.32.156.
    - IPv6: 2600:3c01::f03c:91ff:fe18:bb2f.
  - Sistema operativo : Ubuntu Linux.

## **Riflessioni Finali**

Durante il laboratorio, ho compreso quanto Nmap sia uno strumento versatile e potente per la gestione e la sicurezza delle reti. Le sue funzionalità includono:

- Identificazione di host e servizi : Utile per creare un inventario della rete e assicurarsi che tutti i dispositivi siano correttamente configurati.
- Rilevamento di vulnerabilità : Consente di individuare porte aperte o servizi non autorizzati che potrebbero rappresentare un rischio per la sicurezza.
- Analisi del sistema operativo : Aiuta a identificare dispositivi con sistemi operativi obsoleti o non patchati.

Tuttavia, Nmap può anche essere utilizzato da attori malevoli per condurre attività di ricognizione. Un attaccante potrebbe utilizzare Nmap per mappare una rete, identificare porte aperte e pianificare attacchi mirati.

## **Conclusioni**

Questo laboratorio mi ha permesso di acquisire familiarità con Nmap e di comprendere le sue applicazioni pratiche. Ho imparato a utilizzare switch specifici per eseguire scansioni avanzate e a interpretare i risultati per valutare la sicurezza di una rete. Queste competenze sono fondamentali per un analista della sicurezza informatica, poiché consentono di identificare e mitigare potenziali minacce.

In futuro, continuerò a esplorare le funzionalità avanzate di Nmap e ad applicarle in scenari reali per migliorare la sicurezza delle reti.

# **Relazione sullo Svolgimento del Laboratorio: 17.2.6 Lab – Attacking a MySQL Database**

## **Introduzione**

Il laboratorio "Attacking a MySQL Database" si propone di analizzare un attacco di tipo SQL Injection utilizzando un file di cattura di rete (PCAP) precedentemente registrato. L'obiettivo è comprendere come un attaccante può sfruttare vulnerabilità in applicazioni web per interagire direttamente con un database SQL. Durante il laboratorio, ho utilizzato Wireshark , uno strumento di analisi del traffico di rete, per esaminare passo-passo le fasi di un attacco SQL Injection e rispondere a domande specifiche relative ai dati estratti.

## **Parte 1: Apertura di Wireshark e Caricamento del File PCAP**

1. Avvio della Macchina Virtuale :
  - Ho avviato la macchina virtuale CyberOps Workstation e mi sono autenticato con le credenziali fornite:
    - Username: analyst
    - Password: cyberops.
2. Apertura di Wireshark :
  - Ho aperto Wireshark seguendo il percorso: Applications > CyberOPS > Wireshark .
  - Successivamente, ho caricato il file PCAP fornito (SQL\_Lab.pcap) navigando nella directory /home/analyst/lab.support.files.
3. Analisi Iniziale :
  - Il file PCAP conteneva il traffico di rete relativo a un attacco SQL Injection durato circa 8 minuti (441 secondi).
  - Ho identificato i due indirizzi IP coinvolti nell'attacco:
    - Attaccante : 10.0.2.4
    - Vittima (server) : 10.0.2.15

No.	Time	Source	Destination	Protocol	Length	Info
11	0.068625	10.0.2.4	10.0.2.15	HTTP	429	GET /dwa/dwa/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 /dwa/vulnerabilities/sql/?id=1%3D1&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 TSval=82101 TSecr=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 /dwa/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 TSval=93660 TSecr=111985
18	220.493085	10.0.2.15	10.0.2.4	HTTP	1918	HTTP/1.1 200 OK (text/html)
19	277.727722	10.0.2.4	10.0.2.15	HTTP	630	GET /dwa/vulnerabilities/sql/?id=1%27+or+1%3D1+union+select+database%28%29%2C+user%28%29%23&Submit=Submit HTTP/1.1
20	277.727871	10.0.2.15	10.0.2.4	TCP	66	80 → 35642 [ACK] Seq=1 Ack=565 Win=236 Len=0 TSval=107970 TSecr=129156
21	277.732200	10.0.2.15	10.0.2.4	HTTP	1955	HTTP/1.1 200 OK (text/html)
22	313.710129	10.0.2.4	10.0.2.15	HTTP	659	GET /dwa/vulnerabilities/sql/?id=1%27+or+1%3D1+union+select+null%2C+version+%28%29%23&Submit=Submit HTTP/1.1
23	313.710277	10.0.2.15	10.0.2.4	TCP	66	80 → 35644 [ACK] Seq=1 Ack=594 Win=236 Len=0 TSval=116966 TSecr=139951
24	313.712414	10.0.2.15	10.0.2.4	HTTP	1954	HTTP/1.1 200 OK (text/html)
25	383.277032	10.0.2.4	10.0.2.15	HTTP	680	GET /dwa/vulnerabilities/sql/?id=1%27+or+1%3D1+union+select+null%2C+table_name+from+information_schema HTTP/1.1
26	383.277811	10.0.2.15	10.0.2.4	TCP	66	80 → 35666 [ACK] Seq=1 Ack=615 Win=236 Len=0 TSval=134358 TSecr=160821
27	383.284289	10.0.2.15	10.0.2.4	HTTP	4068	HTTP/1.1 200 OK (text/html)
28	441.804070	10.0.2.4	10.0.2.15	HTTP	685	GET /dwa/vulnerabilities/sql/?id=1%27+or+1%3D1+union+select+user%2C+password+from+users%23&Submit=Submit HTTP/1.1
29	441.804427	10.0.2.15	10.0.2.4	TCP	66	80 → 35668 [ACK] Seq=1 Ack=620 Win=236 Len=0 TSval=148990 TSecr=178379
30	441.807206	10.0.2.15	10.0.2.4	HTTP	2091	HTTP/1.1 200 OK (text/html)

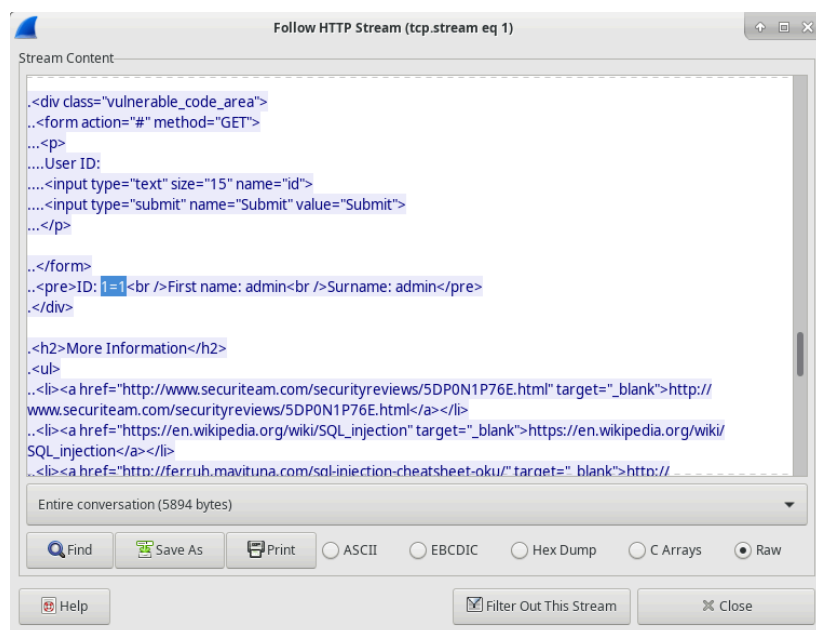
## Parte 2: Visualizzazione dell'Attacco SQL Injection

### 1. Seguendo il Flusso HTTP :

- Ho selezionato la riga 13 del file PCAP, che rappresentava una richiesta HTTP GET, e ho seguito il flusso HTTP (Follow > HTTP Stream).
- Nella finestra visualizzata, ho osservato il traffico tra l'attaccante (in rosso) e il server (in blu).

### 2. Ricerca della Query 1=1 :

- Utilizzando la funzione di ricerca (Find), ho individuato la query 1=1, che è una tecnica comune per testare la vulnerabilità di un'applicazione a SQL Injection.
- L'attaccante aveva inserito questa query in un campo di ricerca (es. UserID) per verificare se il database rispondeva in modo anomalo. La risposta positiva ha confermato la vulnerabilità.



### 3. Conclusione :

- La query `1=1` crea una condizione sempre vera, permettendo all'attaccante di manipolare il comportamento del database e ottenere informazioni sensibili.

## Parte 3: Continuazione dell'Attacco SQL Injection

### 1. Nuova Query :

- Ho selezionato la riga 19 e seguito nuovamente il flusso HTTP.
- L'attaccante aveva inserito una query più complessa:
- `1' or 1=1 union select database(), user()#`
- Questa query ha restituito il nome del database (`dvwa`) e l'utente del database (`root@localhost`), oltre a visualizzare account utente.

### 2. Significato della Query :

- La clausola `union select` combina i risultati di due query, mentre `#` commenta il resto della query originale, impedendo errori.



## Parte 4: Estrazione delle Informazioni di Sistema

### 1. Query per il Versioning :

- Ho selezionato la riga 22 e seguito il flusso HTTP.
- L'attaccante aveva inserito la query:
- sql
- 1' or 1=1 union select null, version()#
- Questa query ha restituito la versione del database MySQL: MySQL 5.7.12-0 .

### 2. Importanza delle Informazioni :

- Conoscere la versione del database permette all'attaccante di pianificare ulteriori exploit specifici.

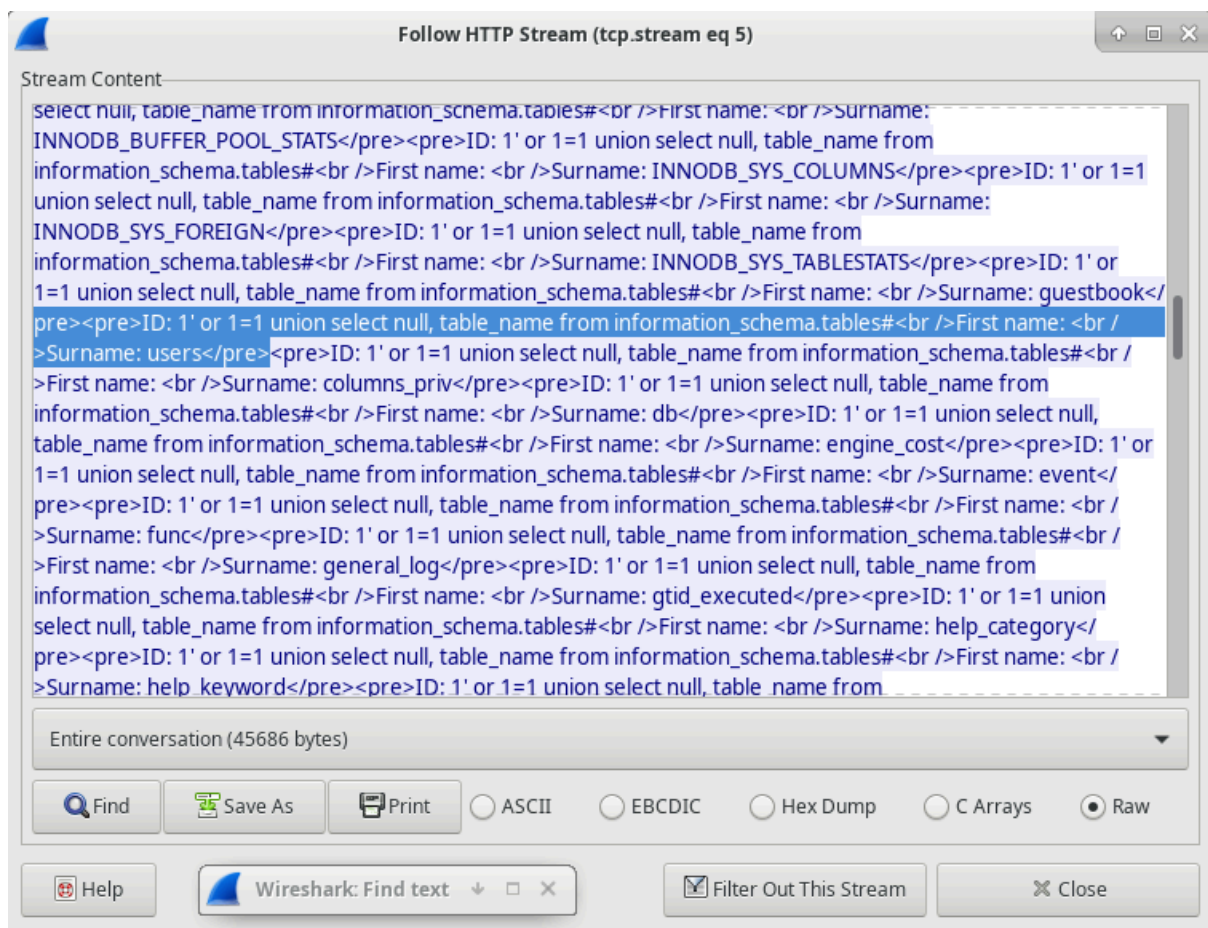




## Parte 5: Estrazione delle Tabelle del Database

### 1. Query per le Tabelle :

- Ho selezionato la riga 25 e seguito il flusso HTTP.
- L'attaccante aveva inserito la query:
- sql
- 1' or 1=1 union select null, table\_name from information\_schema.tables#
- Questa query ha restituito un elenco di tutte le tabelle presenti nel database.



### 2. Modifica della Query :

- Una query modificata come:
- 1' OR 1=1 UNION SELECT null, column\_name FROM INFORMATION\_SCHEMA.columns WHERE table\_name='users'

- avrebbe restituito solo le colonne della tabella users, riducendo l'output e rendendolo più mirato.

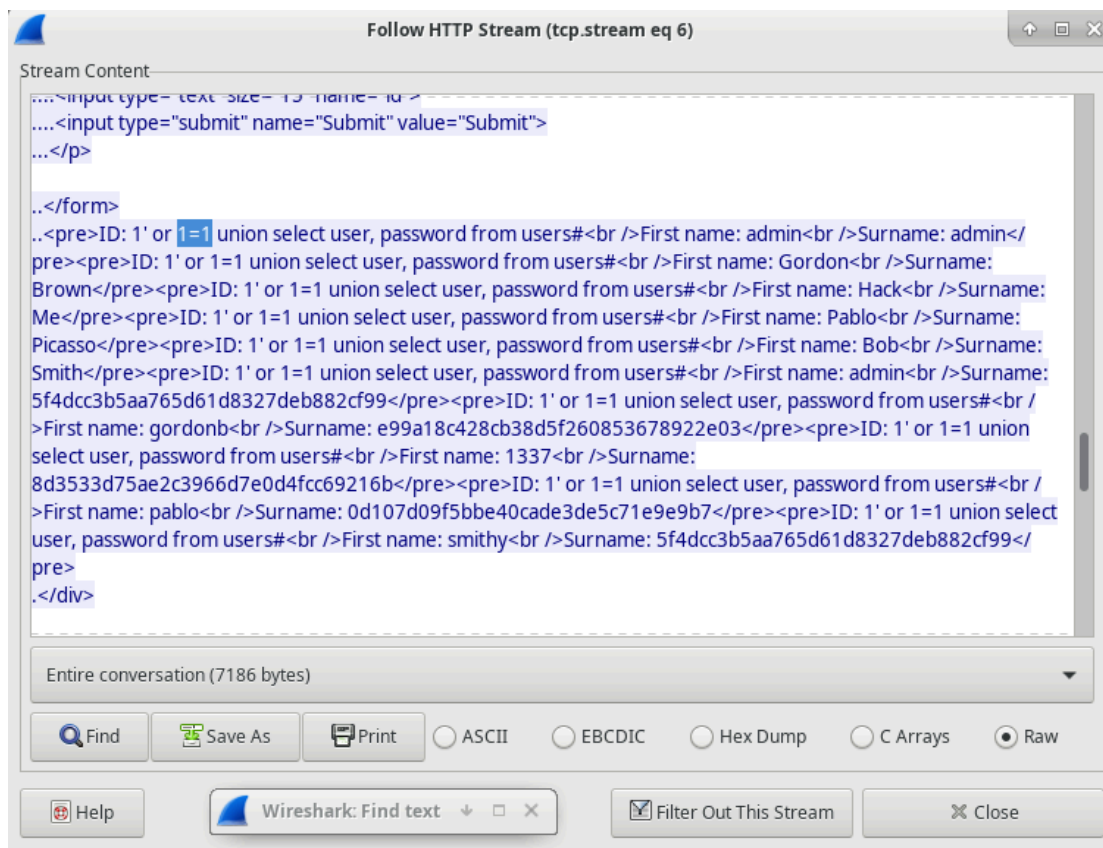
## Parte 6: Estrazione delle Credenziali Utente

### 1. Query per le Password :

- Ho selezionato la riga 28 e seguito il flusso HTTP.
- L'attaccante aveva inserito la query:
- sql
- 1' or 1=1 union select user, password from users#
- Questa query ha restituito gli username e gli hash delle password degli utenti.

### 2. Decodifica dell'Hash :

- Uno degli hash restituiti era 8d3533d75ae2c3966d7e0d4fcc69216b, associato all'utente 1337.
- Utilizzando un servizio online come [CrackStation](#), ho decodificato l'hash, scoprendo che la password in chiaro era: charley .



## Riflessioni Finali

Durante il laboratorio, ho compreso quanto gli attacchi SQL Injection possano essere devastanti per la sicurezza di un sistema. Attraverso semplici query malevole, un attaccante può:

- Identificare vulnerabilità nel database.
- Estrarre informazioni sensibili, come nomi di tabelle, utenti e password.
- Compromettere l'integrità e la riservatezza dei dati.

Ho anche appreso che la prevenzione di tali attacchi richiede misure proattive, come:

- Filtraggio degli input utente : Validare e sanificare tutti gli input prima di elaborarli.
- Uso di parametri nelle query : Evitare di concatenare direttamente gli input nelle query SQL.
- Monitoraggio delle query : Analizzare regolarmente le query eseguite sul database per rilevare comportamenti anomali.
- Disabilitazione di funzionalità non necessarie : Ridurre la superficie di attacco disabilitando funzionalità superflue.

## Conclusioni

Questo laboratorio mi ha permesso di acquisire una comprensione pratica degli attacchi SQL Injection e delle loro implicazioni sulla sicurezza. Utilizzando Wireshark, ho imparato a interpretare il traffico di rete e a identificare le tecniche utilizzate dagli attaccanti per compromettere un database. Queste competenze sono fondamentali per un analista della sicurezza informatica, poiché consentono di rilevare e mitigare potenziali minacce.

In futuro, continuerò a esplorare altre tecniche di attacco e difesa per migliorare la mia capacità di proteggere le reti e i sistemi da minacce esterne.