

# Cyber Security & Ethical Hacking

Cisco CyberOps

**Sara Maimone**

**S11.L5**

13/12/2024



## Indice

1. <b>Relazione dettagliata sull'utilizzo di Windows PowerShell</b> .....	Pagina 3
a. Introduzione .....	Pagina 3
b. Parte 1: Accesso alla console PowerShell .....	Pagina 3
c. Parte 2: Esplorazione dei comandi .....	Pagina 4
d. Parte 3: Comandi avanzati di rete .....	Pagina 6
e. Parte 4: Automazione e gestione file .....	Pagina 8
f. Conclusioni .....	Pagina 9
2. <b>Relazione: Cattura e Analisi del Traffico HTTP e HTTPS</b> .....	Pagina 10
a. Introduzione .....	Pagina 10
b. Parte 1: Cattura del traffico HTTP .....	Pagina 10
c. Parte 2: Cattura del traffico HTTPS .....	Pagina 12
d. Conclusioni .....	Pagina 13
3. <b>Relazione: Analisi di un Attacco di SQL Injection</b> .....	Pagina 14
a. Introduzione .....	Pagina 14
b. Passaggi e Osservazioni .....	Pagina 14
i. Identificazione degli IP .....	Pagina 14
ii. Verifica della vulnerabilità .....	Pagina 14
iii. Recupero di informazioni sensibili .....	Pagina 15
c. Rischi e Conseguenze degli Attacchi SQL Injection .....	Pagina 17
d. Prevenzione degli Attacchi SQL Injection .....	Pagina 17
e. Conclusioni .....	Pagina 17
4. <b>Relazione sull'Uso di Nmap per il Port Scanning</b> .....	Pagina 18
a. Introduzione .....	Pagina 18
b. Analisi del Traffico di Rete con Nmap .....	Pagina 18
i. Scan del Localhost .....	Pagina 18
ii. Scan della Rete Locale .....	Pagina 18
iii. Sistemi Operativi e Versioni .....	Pagina 19
c. Utilizzo di Nmap nella Sicurezza della Rete .....	Pagina 19

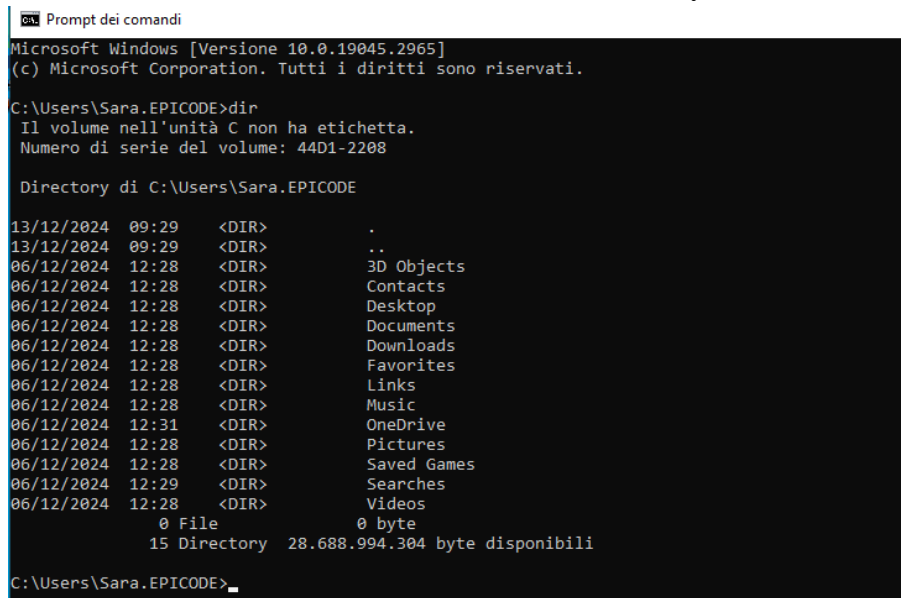
# Relazione dettagliata sull'utilizzo di Windows PowerShell

## Introduzione

PowerShell è un potente strumento per l'automazione di attività amministrative e la gestione di sistemi Windows. Questo laboratorio guida attraverso l'esplorazione di comandi base e avanzati per comprenderne le funzionalità, confrontandole con quelle del Prompt dei comandi.

## Parte 1: Accesso alla console PowerShell

1. Avvio di PowerShell e Prompt dei comandi
  - a. PowerShell è stato aperto cercandolo dal menu Start.
  - b. Parallelamente, è stato avviato il Prompt dei comandi per confrontare i due ambienti.
2. Primi comandi
  - a. Esecuzione del comando `dir` in entrambi gli strumenti per visualizzare i contenuti della directory corrente.



```

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

C:\Users\Sara.EPICODE>dir
Il volume nell'unità C non ha etichetta.
Numero di serie del volume: 44D1-2208

Directory di C:\Users\Sara.EPICODE

13/12/2024 09:29 <DIR>      .
13/12/2024 09:29 <DIR>      ..
06/12/2024 12:28 <DIR>      3D Objects
06/12/2024 12:28 <DIR>      Contacts
06/12/2024 12:28 <DIR>      Desktop
06/12/2024 12:28 <DIR>      Documents
06/12/2024 12:28 <DIR>      Downloads
06/12/2024 12:28 <DIR>      Favorites
06/12/2024 12:28 <DIR>      Links
06/12/2024 12:28 <DIR>      Music
06/12/2024 12:31 <DIR>      OneDrive
06/12/2024 12:28 <DIR>      Pictures
06/12/2024 12:28 <DIR>      Saved Games
06/12/2024 12:29 <DIR>      Searches
06/12/2024 12:28 <DIR>      Videos
               0 File             0 byte
               15 Directory 28.688.994.304 byte disponibili

C:\Users\Sara.EPICODE>
```

Risultato: Il comando dir produce un output simile, ma PowerShell lo restituisce in un formato più dettagliato e strutturato.

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

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

PS C:\Users\Sara.EPICODE> dir

    Directory: C:\Users\Sara.EPICODE

Mode                LastWriteTime         Length Name
----                -
d-r---            06/12/2024      12:28           3D Objects
d-r---            06/12/2024      12:28           Contacts
d-r---            06/12/2024      12:28           Desktop
d-r---            06/12/2024      12:28           Documents
d-r---            06/12/2024      12:28           Downloads
d-r---            06/12/2024      12:28           Favorites
d-r---            06/12/2024      12:28           Links
d-r---            06/12/2024      12:28           Music
d-r---            06/12/2024      12:31           OneDrive
d-r---            06/12/2024      12:28           Pictures
d-r---            06/12/2024      12:28           Saved Games
d-r---            06/12/2024      12:29           Searches
d-r---            06/12/2024      12:28           Videos

PS C:\Users\Sara.EPICODE> 
```

## Parte 2: Esplorazione dei comandi

### 1. Comandi tradizionali

- a. Nel Prompt dei comandi e in PowerShell sono stati testati comandi standard:
  - i. ping: Per verificare la connessione a un host remoto.
  - ii. cd: Per cambiare directory.
  - iii. ipconfig: Per visualizzare la configurazione di rete.
- b. Osservazioni: Entrambi supportano questi comandi, ma PowerShell consente l'uso di cmdlet nativi più specifici.

## 1. Uso dei cmdlet di PowerShell

- c. Comando `Get-Alias` dir: Identifica il cmdlet equivalente a `dir`, ovvero `Get-ChildItem`, che fornisce ulteriori funzionalità.

```
PS C:\Users\Sara.EPICODE> Get-Alias dir

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

PS C:\Users\Sara.EPICODE> Get-ChildItem

Directory: C:\Users\Sara.EPICODE

Mode                LastWriteTime         Length Name
----                -
d-r--              06/12/2024   12:28             3D Objects
d-r--              06/12/2024   12:28             Contacts
d-r--              06/12/2024   12:28             Desktop
d-r--              06/12/2024   12:28             Documents
d-r--              06/12/2024   12:28             Downloads
d-r--              06/12/2024   12:28             Favorites
d-r--              06/12/2024   12:28             Links
d-r--              06/12/2024   12:28             Music
d-r--              06/12/2024   12:31             OneDrive
d-r--              06/12/2024   12:28             Pictures
d-r--              06/12/2024   12:28             Saved Games
d-r--              06/12/2024   12:29             Searches
d-r--              06/12/2024   12:28             Videos
```

- d. Ricerca online: Scoperti cmdlet come `Get-Help` e `Get-Command` per esplorare funzionalità avanzate.

## Parte 3: Comandi avanzati di rete

### 1. Esecuzione di `netstat`

- a. Comando `netstat -h`: Mostra opzioni disponibili.

```
Windows PowerShell
PS C:\Users\Sara.EPICODE> netstat -h

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

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

-a Visualizza tutte le connessioni e le porte di ascolto.
-b Visualizza l'eseguibile coinvolto nella creazione di ogni connessione o porta di ascolto. In alcuni casi, host di eseguibili noti più componenti indipendenti e in questi casi il sequenza di componenti coinvolti nella creazione della connessione o la porta in ascolto. In questo caso, l'eseguibile il nome è in [] nella parte inferiore, in alto è il componente che ha chiamato, e così via fino al raggiungimento di TCP/IP. Si noti che questa opzione può richiedere molto tempo e avrà esito negativo, a meno che non siano sufficienti autorizzazioni.
-e visualizza le statistiche Ethernet. È possibile combinare opzione.
-f Visualizza nomi di dominio completi (FQDN) per stranieri indirizzi.
-n Visualizza indirizzi e numeri di porta in formato numerico.
-o Visualizza l'ID del processo proprietario associato a ogni connessione.
-p proto Mostra le connessioni per il protocollo specificato da proto; proto può essere qualsiasi: TCP, UDP, TCPv6 o UDPv6. Se usato con -s opzione per la visualizzazione delle statistiche per protocollo, Proto può essere qualsiasi: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
-q Visualizza tutte le connessioni, le porte di ascolto e i binding non in ascolto di porte TCP. Le porte di nonlistening associate possono o meno essere essere associate a una connessione attiva.
-r Visualizza la tabella di routing.
-s Visualizza le statistiche per protocollo. Per impostazione predefinita, le statistiche vengono visualizzate per IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP e UDPv6; l'opzione -p può essere utilizzata per specificare un sottoinsieme del valore predefinito.
-t Visualizza lo stato corrente di offload della connessione.
-x Visualizza connessioni NetworkDirect, listener e condivisi endpoint.
-y Visualizza il modello di connessione TCP per tutte le connessioni. Non può essere combinato con le altre opzioni.
intervallo Rivalutazione le statistiche selezionate, la sospensione dell'intervallo di secondi tra ogni schermo. Premere CTRL+C per interrompere la rivalutazione Statistiche. Se viene omissa, netstat stamperà il informazioni di configurazione una volta.

PS C:\Users\Sara.EPICODE>
```

- b. Comando `netstat -r`: Visualizza la tabella di routing attiva.

```
PS C:\Users\Sara.EPICODE> netstat -r
=====
Elenco interfacce
 5...08 00 27 f0 cf bd .....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   192.168.1.161  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       192.168.1.161  281
  192.168.1.161       255.255.255.255 On-link       192.168.1.161  281
  192.168.1.255       255.255.255.255 On-link       192.168.1.161  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       192.168.1.161  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       192.168.1.161  281
=====
Route permanenti:
 Nessuna

IPv6 Tabella route
=====
Route attive:
  Interf Metrica Rete Destinazione      Gateway
  1      331  ::1/128             On-link
  1      331  ff00::/8             On-link
=====
Route permanenti:
 Nessuna
PS C:\Users\Sara.EPICODE>
```

Comando `netstat -abno`: Mostra connessioni attive con i rispettivi PID.

```

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

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

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  872
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  6068
CDPSvc
[svchost.exe]
TCP    0.0.0.0:5357             0.0.0.0:0         LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:7680             0.0.0.0:0         LISTENING  5144
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49664            0.0.0.0:0         LISTENING  652
[lsass.exe]
TCP    0.0.0.0:49665            0.0.0.0:0         LISTENING  500
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49666            0.0.0.0:0         LISTENING  1256
Eventlog
[svchost.exe]
TCP    0.0.0.0:49667            0.0.0.0:0         LISTENING  816
Schedule
[svchost.exe]
TCP    0.0.0.0:49668            0.0.0.0:0         LISTENING  2524
[spoolsv.exe]
TCP    0.0.0.0:49669            0.0.0.0:0         LISTENING  652
[lsass.exe]
TCP    0.0.0.0:49670            0.0.0.0:0         LISTENING  636
Impossibile ottenere informazioni sulla proprietà
TCP    192.168.1.161:1139       0.0.0.0:0         LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP    192.168.1.161:50298      20.54.37.64:443   ESTABLISHED  2924
WpnService
[svchost.exe]
TCP    192.168.1.161:50704      20.190.147.9:443  TIME_WAIT    0
TCP    192.168.1.161:50705      20.190.147.9:443  TIME_WAIT    0
TCP    192.168.1.161:50725      192.229.221.95:80 TIME_WAIT    0
TCP    192.168.1.161:50726      95.101.114.18:443 ESTABLISHED  5620

```

## 2. Analisi dei processi

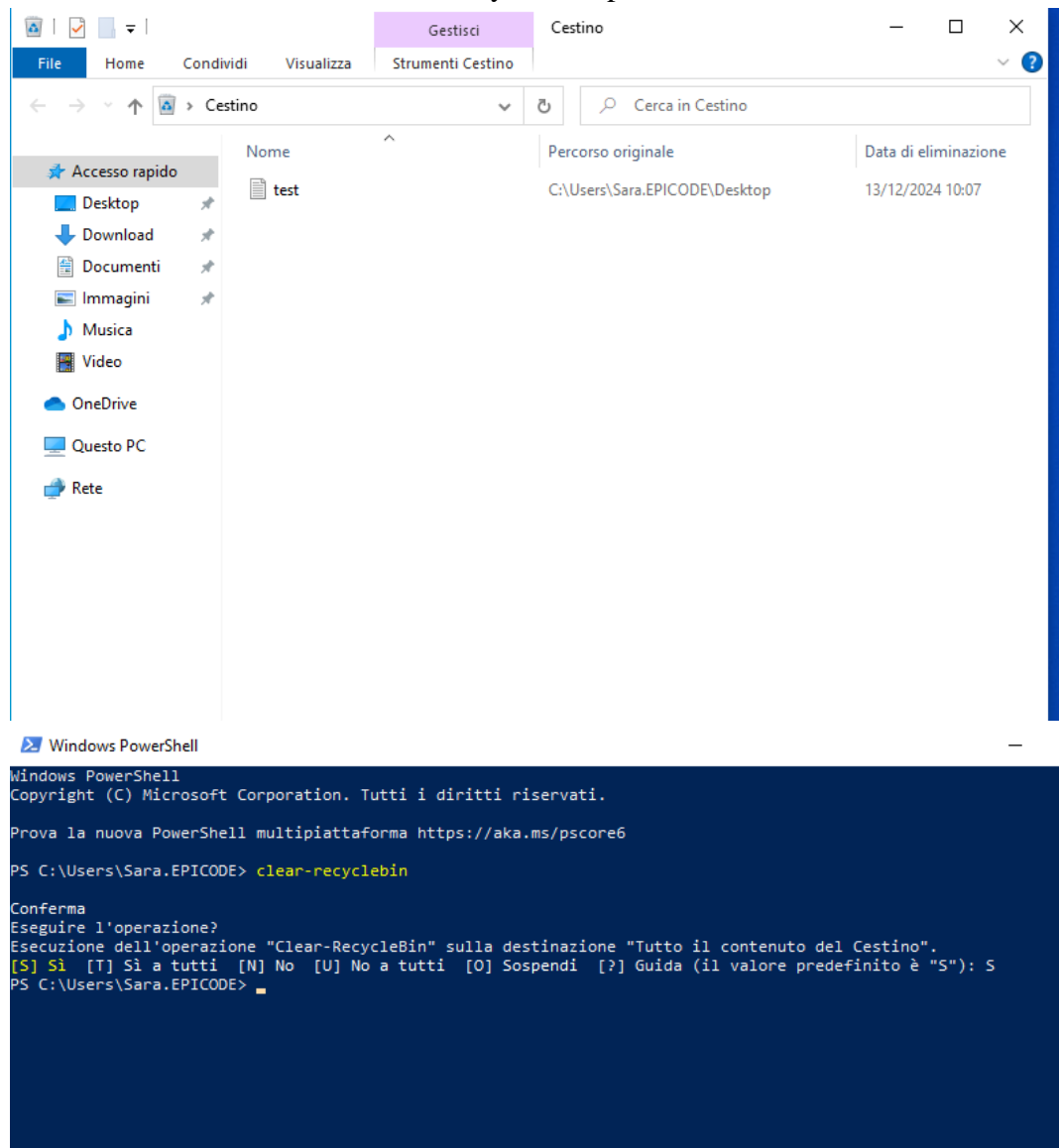
- Apertura del Task Manager: Utilizzato per ordinare i processi per PID e analizzare il processo associato a un PID identificato tramite netstat.
- Informazioni disponibili: Nome del processo, percorso eseguibile, utilizzo risorse.

svchost.exe	904	In esecuzione	SYSTEM	00	8.808 K	Non consentito
svchost.exe	964	In esecuzione	SERVIZIO DI RETE	00	6.988 K	Non consentito

## Parte 4: Automazione e gestione file

### 1. Gestione del Cestino

- a. Creazione di file di test e loro spostamento nel Cestino.
- b. Esecuzione del comando `Clear-RecycleBin` per eliminarli definitivamente.



### 2. Ricerca di comandi utili

- a. Individuati cmdlet per la sicurezza informatica, come:
  - i. `Get-EventLog`: Per analizzare i log degli eventi.
  - ii. `Test-Connection`: Per verificare la latenza di rete.
  - iii. `Set-Service`: Per gestire servizi in rete.



## Conclusioni

Questo laboratorio ha mostrato l'efficacia di PowerShell come strumento per:

- Automatizzare attività complesse.
- Migliorare l'analisi di rete e sicurezza.
- Ridurre il tempo richiesto per la gestione dei sistemi rispetto a strumenti grafici.

PowerShell si rivela essenziale per amministratori di sistema e analisti di sicurezza, grazie alla sua flessibilità e potenza.

# Relazione: Cattura e Analisi del Traffico HTTP e HTTPS con tcpdump e Wireshark

## Introduzione

Il presente laboratorio si è concentrato sull'esplorazione del traffico HTTP e HTTPS utilizzando tcpdump e Wireshark. Si è trattato di catturare pacchetti di rete per osservare le differenze tra il traffico non criptato (HTTP) e quello criptato (HTTPS). L'obiettivo è comprendere la natura della trasmissione dei dati e i benefici di HTTPS rispetto a HTTP.

## Parte 1: Cattura del traffico HTTP

### 1. Avvio di tcpdump e cattura del traffico HTTP

- a. È stato avviato il terminale e utilizzato il comando:

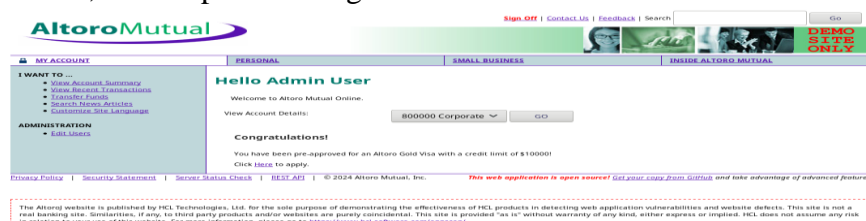
```
sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
```

Questo comando ha catturato il traffico sulla rete, scrivendo i pacchetti in un file httpdump.pcap.

```
[analyst@secOps Desktop]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C3466 packets captured
3466 packets received by filter
0 packets dropped by kernel
[analyst@secOps Desktop]$
```

### 2. Navigazione su un sito HTTP

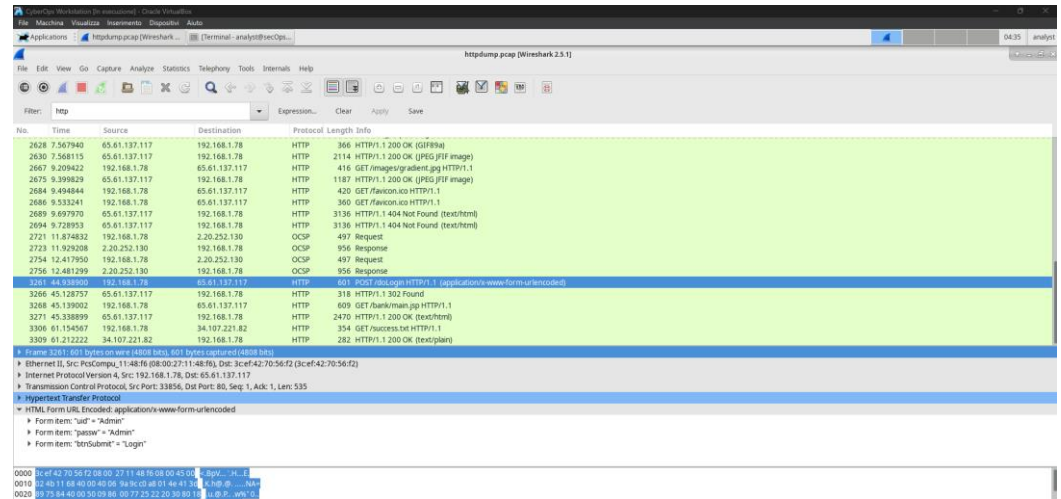
- a. Abbiamo visitato il sito <http://www.altoromutual.com/login.jsp>, che utilizza HTTP, per generare traffico non criptato.



- b. Durante l'inserimento delle credenziali, i dati sono stati trasmessi in chiaro, il che ha permesso di catturare informazioni sensibili come il nome utente e la password.

### 3. Visualizzazione del traffico HTTP in Wireshark

- a. Il file httpdump.pcap è stato aperto con Wireshark, utilizzando il filtro http.
- b. Abbiamo selezionato un messaggio POST e espanso la sezione HTML Form URL Encoded, ottenendo informazioni come:
  - i. Il nome utente inviato (Admin).
  - ii. La password (Admin).



## Parte 2: Cattura del traffico HTTPS

### 1. Avvio di tcpdump e cattura del traffico HTTPS

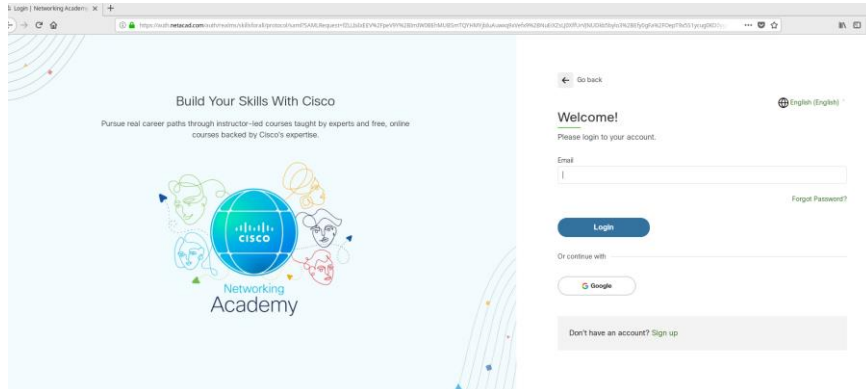
- a. È stato utilizzato il comando:

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

per registrare il traffico HTTPS. Il file risultante è stato denominato httpsdump.pcap.

### 2. Navigazione su un sito HTTPS

- a. È stato visitato il sito [www.netacad.com](https://www.netacad.com), che utilizza HTTPS.

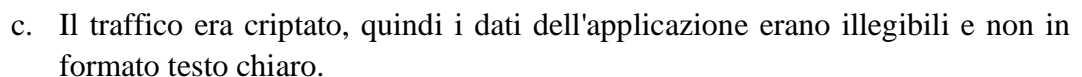


- b. Dopo aver effettuato l'accesso con le credenziali, il traffico HTTPS è stato registrato.

```
[analyst@sec0ps Desktop]$ 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
^C2143 packets captured
2143 packets received by filter
0 packets dropped by kernel
[analyst@sec0ps Desktop]$
```

- c. Durante la cattura, è stato osservato che l'URL del sito era <https://>, indicando una connessione sicura.

- Il file `httpsdump.pcap` è stato aperto in Wireshark con il filtro `tcp.port==443`.
- Abbiamo selezionato un messaggio Application Data, espandendo la sezione  
Secure                      Sockets                      Layer                      (SSL).



- Vantaggi di HTTPS rispetto a HTTP:
  - HTTPS offre crittografia, garantendo che i dati trasmessi tra il client e il server siano protetti da intercettazioni. Ciò è particolarmente importante per la protezione delle credenziali e di altre informazioni sensibili.
  - HTTP, al contrario, trasmette i dati in chiaro, rendendo facile per un attaccante intercettare e visualizzare i contenuti.
- Tutti i siti HTTPS sono sicuri?
  - No, non tutti i siti che utilizzano HTTPS sono sicuri. Mentre HTTPS garantisce la crittografia, non protegge contro attacchi come il phishing o altre minacce legate alla fiducia nel sito. È fondamentale fare attenzione a dove si naviga, anche se il sito utilizza HTTPS.

13

## Relazione: Analisi di un Attacco di SQL Injection

# Introduzione

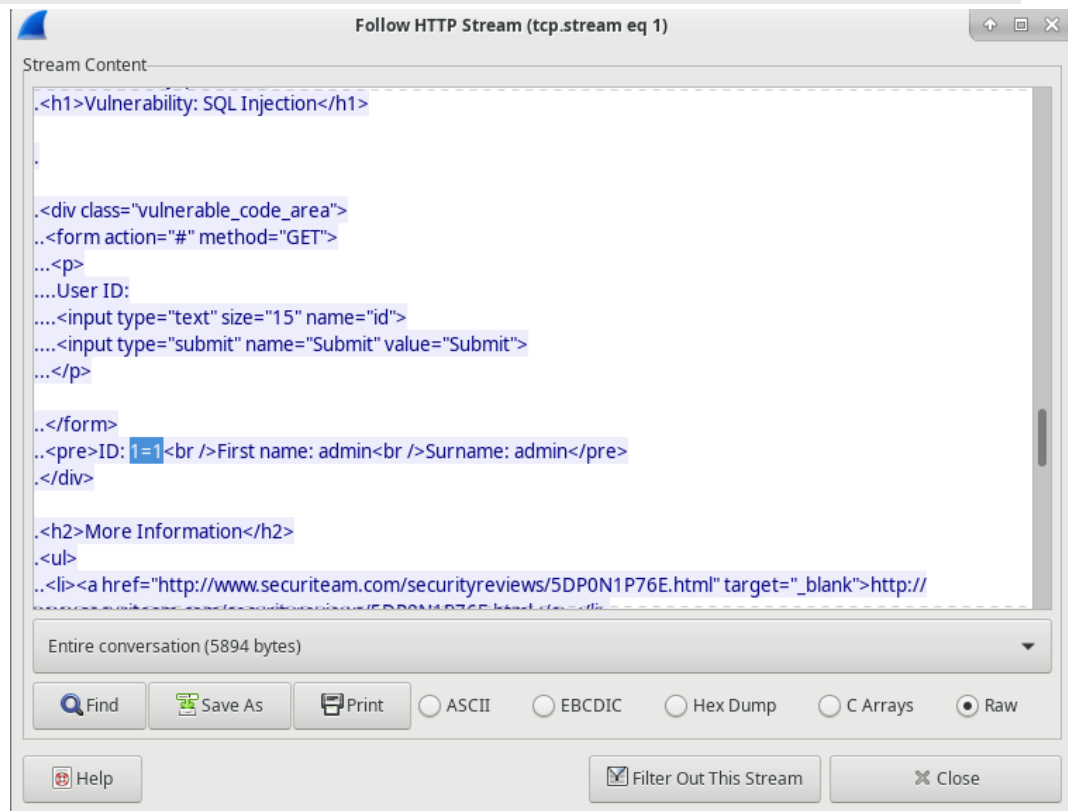
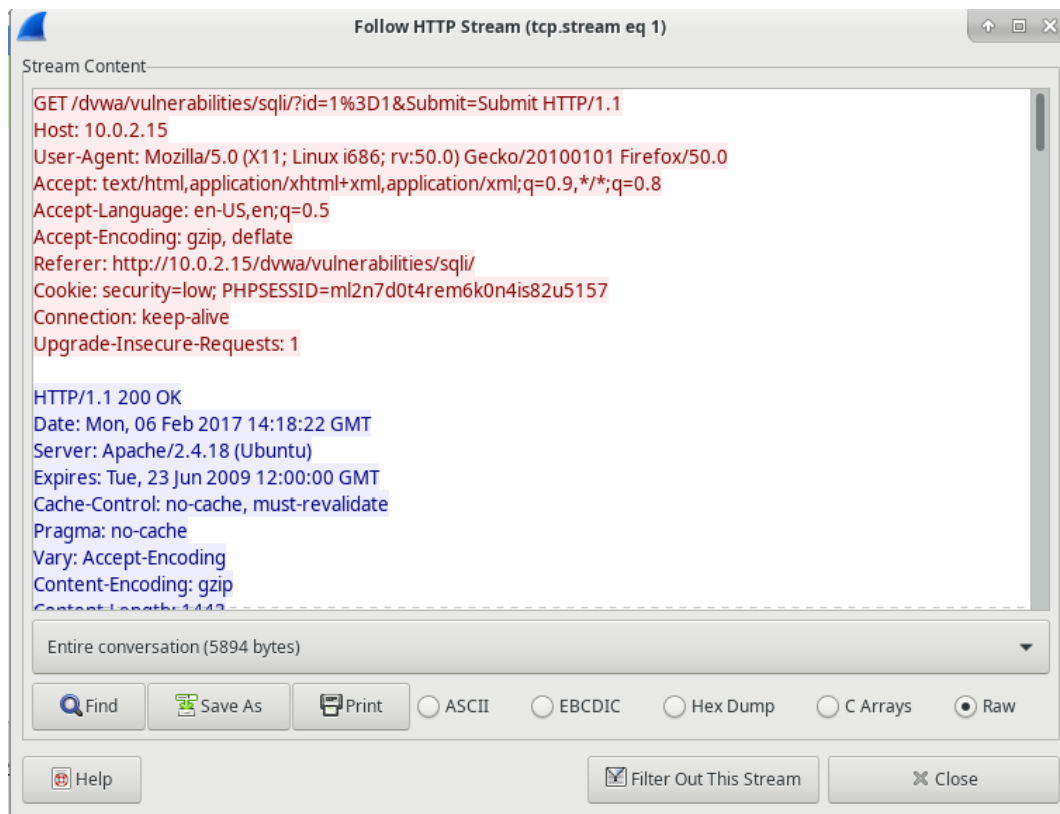
Nel presente laboratorio, è stato analizzato un attacco di SQL Injection tramite Wireshark, utilizzando un file di cattura PCAP (SQL\_Lab.pcap). L'obiettivo era esaminare il traffico di rete durante l'attacco, osservando come un attaccante sfrutti le vulnerabilità di un'applicazione web per ottenere informazioni dal database tramite query SQL malformate.

## Passaggi e Osservazioni

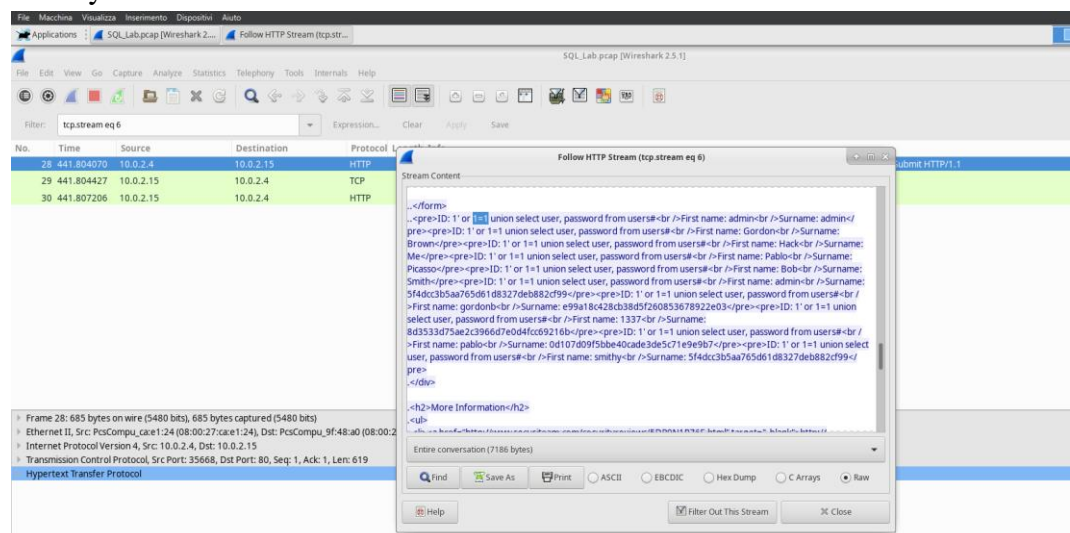
- ## 1. Cattura del Traffico e Identificazione degli IP

[illegible]

- a. Durante l'attacco, i due indirizzi IP coinvolti sono stati identificati tramite Wireshark. L'indirizzo sorgente è stato il client dell'attaccante, mentre il destinatario era il server di destinazione.
2. Inizio dell'Attacco e Verifica della Vulnerabilità
  - a. L'attaccante ha inviato la query 1=1 nel campo di ricerca UserID, causando una risposta positiva dalla base di dati (invece di un errore di login), confermando la vulnerabilità alla SQL injection



1. Proseguimento dell'Attacco e Recupero di Informazioni Sensibili
  - b. La query successiva, 1' OR 1=1 UNION SELECT database(), user()#, ha rivelato il nome del database (dvwa) e l'utente del database (root@localhost), confermando che l'attaccante aveva ottenuto informazioni sensibili.
3. Recupero della Versione di MySQL
  - a. Utilizzando la query 1' OR 1=1 UNION SELECT NULL, version()#, l'attaccante ha ottenuto la versione di MySQL (5.7.12-0).
4. Elenco delle Tabelle del Database
  - a. Con la query 1' OR 1=1 UNION SELECT NULL, table\_name FROM information\_schema.tables#, sono state recuperate tutte le tabelle del database. Successivamente, la query è stata modificata per filtrare solo le tabelle contenenti il termine users.
5. Recupero di Password Hash
  - a. Infine, l'attaccante ha utilizzato la query 1' OR 1=1 UNION SELECT user, password FROM users#, ottenendo una lista di utenti e le relative password hash. È stato trovato l'utente 1337 con l'hash 8d3533d75ae2c3966d7e0d4fcc69216b, che è stato decrittato come la password charley.





## Rischi e Conseguenze degli Attacchi SQL Injection

Un attacco di SQL injection può compromettere gravemente la sicurezza di un'applicazione web, poiché consente all'attaccante di:

- Accedere e manipolare i dati sensibili nel database.
- Ottenere informazioni sugli utenti, comprese le credenziali di accesso.
- Potenzialmente eseguire comandi arbitrari, compromettere il sistema e causare danni significativi.

L'uso improprio di SQL senza le necessarie precauzioni può portare a vulnerabilità enormi in applicazioni web che gestiscono dati sensibili.

## Prevenzione degli Attacchi SQL Injection

Dopo aver esaminato il laboratorio, sono state identificate due misure di protezione contro gli attacchi di SQL injection:

1. Filtraggio e Validazione dell'Input dell'Utente: È fondamentale controllare e validare correttamente i dati immessi dagli utenti prima di inserirli nelle query SQL, per evitare l'inserimento di comandi malevoli.
2. Utilizzo di Stored Procedures e Parametri: L'impiego di stored procedures e l'uso di query parametrizzate riducono significativamente il rischio di iniezioni SQL, poiché i parametri non vengono trattati come parte del comando SQL eseguibile.

## Conclusioni

Il laboratorio ha dimostrato come un attacco di SQL injection possa essere utilizzato per ottenere informazioni riservate da un database vulnerabile. È fondamentale adottare misure preventive, come la validazione dell'input e l'uso di tecniche di query sicure, per proteggere le applicazioni web da questi attacchi.

## Relazione sull'Uso di Nmap per il Port Scanning

### Introduzione

Nmap è un potente strumento di esplorazione di rete utilizzato per scoprire host attivi, determinare le porte aperte e identificare i servizi offerti. Viene comunemente utilizzato sia per scopi di auditing di sicurezza che per scoprire vulnerabilità all'interno di una rete. Nel laboratorio, sono stati esplorati vari comandi di Nmap per eseguire scansioni di porte sulla rete locale, sul proprio host e su un server remoto.

### Analisi del Traffico di Rete con Nmap

#### 1. Scan del Localhost

- a. Utilizzando il comando `nmap -A -T4 localhost`, sono stati rilevati i seguenti servizi:

- i. Porta 21/tcp: FTP (vsftpd)
- ii. Porta 22/tcp: SSH (OpenSSH)

```
[analyst@sec0ps Desktop]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 04:45 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000028s 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 4
|     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: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
```

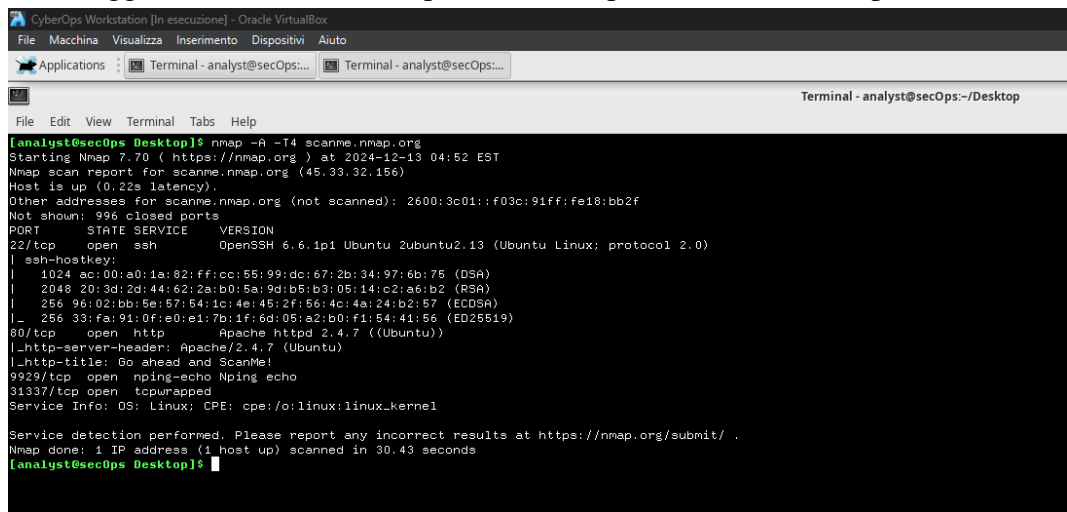
#### 2. Scan della Rete Locale

3. L'indirizzo IP della VM era 192.168.1.78 con una subnet mask 255.255.255.0.

Utilizzando Nmap, sono stati identificati altri host nella rete 192.169.1.0/24 (i risultati variano in base alla configurazione della rete).

- a. Eseguendo una scansione di Nmap su [scanme.nmap.org](https://scanme.nmap.org), i servizi aperti includevano:
  - i. Porta 22/tcp: SSH
  - ii. Porta 80/tcp: HTTP
  - iii. Porta 9929/tcp: Nping Echo

- b. I servizi filtrati includevano porte come 135/tcp (msrpc) e 445/tcp (microsoft-ds), suggerendo che alcune porte erano protette o non rispondevano.



```
[analyst@secOps Desktop]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 04:52 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.22s 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 30.43 seconds
[analyst@secOps Desktop]$
```

#### 4. Sistemi Operativi e Versioni

- a. Nmap ha identificato il sistema operativo del server remoto come Ubuntu Linux.

### Utilizzo di Nmap nella Sicurezza della Rete

Nmap è utile per la gestione e la sicurezza di rete, permettendo di:

- Identificare porte aperte e vulnerabilità.
- Effettuare scansioni per scoprire servizi non sicuri.
- Fornire un inventario completo della rete per garantire che tutti i sistemi siano adeguatamente protetti.

Tuttavia, può anche essere usato da attaccanti per mappare la rete e identificare potenziali vettori di attacco.