

PROGETTO S11/L5

Analisi avanzate: Un approccio pratico



1. UTILIZZO WINDOWS POWERSHELL

PoweShell è un'interfaccia a riga di comando creato da Microsoft per automatizzare e gestire i sistemi. A differenza del vecchio Prompt dei comandi (CMD) permette di eseguire script per automatizzare le attività, utilizza oggetti e metodi, facilitando la gestione dei dati e delle configurazioni.

1.1 DIFFERENZE TRA CMD E POWERSHELL

Digitando il comando **dir** notiamo la prima differenza. Su PoweShell, oltre alle informazioni presenti su CMD, ci vengono mostrati anche i permessi che sono stati assegnati ai file ed alle cartelle.

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

Installa la versione più recente di PowerShell per nuove funzionalità e miglioramenti. https://aka.ms/PSWindows

PS C:\Users\andre> dir

Directory: C:\Users\andre

Mode                LastWriteTime         Length Name
----                -
d-----          05/02/2025   17:02             .idlerc
d-----          21/03/2025   09:10             .ms-ad
d-----          11/04/2025   08:35             .VirtualBox
d-----          05/02/2025   14:58             .vscode
d-----          24/02/2025   22:20             Cisco Packet Tracer 8.2.2
d-r-----         04/02/2025   21:18             Contacts
d-r-----         11/04/2025   08:58             Desktop
d-r-----         10/04/2025   15:38             Documents
d-r-----         10/04/2025   18:02             Downloads
d-r-----         04/02/2025   21:18             Favorites
d-r-----         04/02/2025   21:18             Links
d-r-----         04/02/2025   21:18             Music
dar-----         29/01/2025   19:20             OneDrive
d-r-----         11/04/2025   08:43             Pictures
d-r-----         04/02/2025   21:18             Saved Games
d-r-----         04/02/2025   21:18             Searches
d-r-----         04/02/2025   21:18             Videos
d-----          08/04/2025   13:59             VirtualBox VMs
-a-----          24/02/2025   21:49             176 .packettracer
-a-----          06/02/2025   15:32             26 .python_history
-a-----          05/02/2025   22:14             516 Untitled-1.py
-a-----          05/02/2025   16:07             355 Untitled-2.py

PS C:\Users\andre>
```

```
Prompt dei comandi
Microsoft Windows [Versione 10.0.26100.3775]
(c) Microsoft Corporation. Tutti i diritti riservati.

C:\Users\andre>dir
Il volume nell'unità C è Acer
Numero di serie del volume: 3A57-209E

Directory di C:\Users\andre

21/03/2025  10:10    <DIR>      .
04/02/2025  20:08    <DIR>      ..
05/02/2025  18:02    <DIR>      .idlerc
21/03/2025  10:10    <DIR>      .ms-ad
24/02/2025  22:49    <DIR>      .packettracer
06/02/2025  16:32    <DIR>      .python_history
11/04/2025  08:35    <DIR>      .VirtualBox
05/02/2025  15:58    <DIR>      .vscode
24/02/2025  23:20    <DIR>      Cisco Packet Tracer 8.2.2
04/02/2025  22:18    <DIR>      Contacts
11/04/2025  08:58    <DIR>      Desktop
10/04/2025  15:38    <DIR>      Documents
10/04/2025  18:02    <DIR>      Downloads
04/02/2025  22:18    <DIR>      Favorites
04/02/2025  22:18    <DIR>      Links
04/02/2025  22:18    <DIR>      Music
29/01/2025  20:20    <DIR>      OneDrive
11/04/2025  08:43    <DIR>      Pictures
04/02/2025  22:18    <DIR>      Saved Games
04/02/2025  22:18    <DIR>      Searches
05/02/2025  23:14    <DIR>      516 Untitled-1.py
05/02/2025  17:07    <DIR>      355 Untitled-2.py
04/02/2025  22:18    <DIR>      Videos
08/04/2025  13:59    <DIR>      VirtualBox VMs
                                4 File             1.073 byte
                                20 Directory      164.965.990.400 byte disponibili

C:\Users\andre>
```

Tuttavia in CMD ci viene mostrato spazio ancora disponibile sul disco espresso in byte. Provando invece ad inserire altri comandi, come **ping**, **ipconfig** e **cd** ci restituiscono lo stesso output a livello di informazioni. Nell'esempio abbiamo utilizzato il comando **ping**

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

Installa la versione più recente di PowerShell per nuove funzionalità e miglioramenti. https://aka.ms/PSWindows

PS C:\Users\andre> ping 192.168.1.1

Esecuzione di Ping 192.168.1.1 con 32 byte di dati:
Risposta da 192.168.1.1: byte=32 durata=1ms TTL=64
Risposta da 192.168.1.1: byte=32 durata=1ms TTL=64
Risposta da 192.168.1.1: byte=32 durata=1ms TTL=64
Risposta da 192.168.1.1: byte=32 durata=1ms TTL=64
Risposta da 192.168.1.1: byte=32 durata=7ms TTL=64

Statistiche Ping per 192.168.1.1:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 1ms, Massimo = 7ms, Medio = 2ms

PS C:\Users\andre>
```

```
Prompt dei comandi
Microsoft Windows [Versione 10.0.26100.3775]
(c) Microsoft Corporation. Tutti i diritti riservati.

C:\Users\andre>ping 192.168.1.1

Esecuzione di Ping 192.168.1.1 con 32 byte di dati:
Risposta da 192.168.1.1: byte=32 durata=1ms TTL=64
Risposta da 192.168.1.1: byte=32 durata=1ms TTL=64
Risposta da 192.168.1.1: byte=32 durata=1ms TTL=64
Risposta da 192.168.1.1: byte=32 durata=2ms TTL=64

Statistiche Ping per 192.168.1.1:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 1ms, Massimo = 2ms, Medio = 1ms

C:\Users\andre>
```

1.2 ESPLORAZIONE DEI CMDLETS

I comandi di PowerShell sono comandi speciali identificati da una stringa verbo-nome. progettati per eseguire azioni specifiche.

Per esempio il cmdlet **Get-Alias** ci permette di capire quale cmdlet viene eseguito in una determinata circostanza. Andando a digitare **Get-Alias dir** ci dice che viene eseguito il cmdlet **Get-ChildItem**

```
Windows PowerShell
PS C:\Users\andre> Get-Alias dir

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

1.3 IL COMANDO NETSTAT

Il comando **netstat** è utilizzato per monitorare le connessioni di rete attive.

Con il comando **netstat -r** otteniamo l'elenco delle interfacce di rete

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

=====
Elenco interfacce
25.....WireGuard Tunnel
 8...40 c2 ba fd be bd .....Realtek PCIe GbE Family Controller
20...0a 00 27 00 00 14 .....VirtualBox Host-Only Ethernet Adapter
11...4c 49 6c 5c 70 0c .....Microsoft Wi-Fi Direct Virtual Adapter
 9...4e 49 6c 5c 70 0b .....Microsoft Wi-Fi Direct Virtual Adapter #2
13...4c 49 6c 5c 70 0b .....Intel(R) Wi-Fi 6 AX101
 6...4c 49 6c 5c 70 0f .....Bluetooth Device (Personal Area Network)
 1.....Software Loopback Interface 1
=====
```

e la tabella delle route attive. Notiamo che l'indirizzo IPv4 del gateway è 192.168.1.1.

Eseguendo come Amministratore una seconda sessione di PowerShell, utilizzeremo il comando **netstat -abno**, che ci permette di visualizzare le connessioni attive

```
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  1452
RpcSs
[svchost.exe]
TCP    0.0.0.0:445             0.0.0.0:0              LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:4343            0.0.0.0:0              LISTENING  4624
[AcerCCAgent.exe]
TCP    0.0.0.0:4449            0.0.0.0:0              LISTENING  4632
[AcerDIAgent.exe]
TCP    0.0.0.0:5040            0.0.0.0:0              LISTENING  8700
CDPSvc
[svchost.exe]
TCP    0.0.0.0:5141            0.0.0.0:0              LISTENING  4656
[AcerQAAgent.exe]
TCP    0.0.0.0:7680            0.0.0.0:0              LISTENING  11216
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:46760           0.0.0.0:0              LISTENING  5188
[AcerSysMonitorService.exe]
TCP    0.0.0.0:49664           0.0.0.0:0              LISTENING  1136
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49665           0.0.0.0:0              LISTENING  708
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49666           0.0.0.0:0              LISTENING  2024
Schedule
[svchost.exe]
TCP    0.0.0.0:49667           0.0.0.0:0              LISTENING  2772
EventLog
[svchost.exe]
TCP    0.0.0.0:49668           0.0.0.0:0              LISTENING  4072
[spoolsv.exe]
TCP    0.0.0.0:49692           0.0.0.0:0              LISTENING  1108
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:58995           0.0.0.0:0              LISTENING  4780
[AcerPixyService.exe]
TCP    10.2.0.2:139            0.0.0.0:0              LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP    10.2.0.2:49905           10.2.0.1:65432         ESTABLISHED 12568
[ProtonVPNService.exe]
TCP    10.2.0.2:49925           170.72.238.205:443     ESTABLISHED 23272
[CiscoCollabHost.exe]
```

Il comando può identificare eventuali processi sospetti che utilizzano la nostra connessione, indicando per ciascun processo il **PID (Process Identifier)**

Proviamo a controllare il PID **1136**

TCP	[::]:5141	[::]:0	LISTENING	4656
[AcerQAAgent.exe]				
TCP	[::]:7680	[::]:0	LISTENING	11216
Impossibile ottenere informazioni sulla proprietà				
TCP	[::]:46760	[::]:0	LISTENING	5188
[AcerSysMonitorService.exe]				
TCP	[::]:49664	[::]:0	LISTENING	1136
Impossibile ottenere informazioni sulla proprietà				
TCP	[::]:49665	[::]:0	LISTENING	708
Impossibile ottenere informazioni sulla proprietà				
TCP	[::]:49666	[::]:0	LISTENING	2024
Schedule				
[svchost.exe]				
TCP	[::]:49667	[::]:0	LISTENING	2772
EventLog				

Apriamo il Task Manager e andiamo sulla pagina **Dettagli**.

Gestione attività		Dettagli							Esegui nuova attività		Termina attività	...
		Nome	PID	Stato	Nome utente	CPU	Memoria (...)	Architet...	Descrizione			
Processi		ApplicationFrameHo...	972	In esecuzione	andre	00	1.208 K	x64	Application Frame Host			
Prestazioni		msedgewebview2.exe	1056	In esecuzione	andre	00	1.368 K	x64	WebView2 Utilità: Audio Service			
Cronologia applicazioni		services.exe	1108	In esecuzione	SYSTEM	00	3.232 K		App Servizi e Controller			
App di avvio		lsalss.exe	1128	In esecuzione	SYSTEM	00	460 K	x64	Credential Guard & VBS Key Isolation			
Utenti		lsass.exe	1136	In esecuzione	SYSTEM	00	5.444 K		Local Security Authority Process			
Dettagli		svchost.exe	1284	In esecuzione	SYSTEM	00	10.648 K	x64	Processo host per servizi di Windows			
		WUDFHost.exe	1316	In esecuzione	SERVIZIO L...	00	172 K	x64	Windows Driver Foundation - Processo host Framework driver modalità utente			
		fontdrvhost.exe	1336	In esecuzione	UMFD-0	00	104 K	x64	Usermode Font Driver Host			
		svchost.exe	1452	In esecuzione	SERVIZIO D...	00	8.596 K	x64	Processo host per servizi di Windows			
		svchost.exe	1500	In esecuzione	SYSTEM	00	1.404 K	x64	Processo host per servizi di Windows			
		svchost.exe	1664	In esecuzione	SYSTEM	00	360 K	x64	Processo host per servizi di Windows			
		svchost.exe	1688	In esecuzione	SERVIZIO L...	00	3.644 K	x64	Processo host per servizi di Windows			
		svchost.exe	1712	In esecuzione	SERVIZIO L...	00	592 K	x64	Processo host per servizi di Windows			
		svchost.exe	1728	In esecuzione	SERVIZIO L...	00	792 K	x64	Processo host per servizi di Windows			

Possiamo vedere che il PID 1136 è associato al processo **lsass.exe**. L'utente è **SYSTEM** e sta utilizzando **5.444 k** di memoria.

1.4 SVUOTARE IL CESTINO DA POWERSHELL

I comandi di PowerShell possono semplificare la gestione di una rete di computer di grandi dimensioni. Ad esempio, se si desidera implementare una nuova soluzione di sicurezza su tutti i server della rete, è possibile utilizzare un comando o uno script di PowerShell per implementare e verificare che i servizi siano in esecuzione.

Proviamo a svuotare il cestino da PowerShell utilizzando **clear-recyclebin**

```
Windows PowerShell
PS C:\Users\andre> 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"): t
PS C:\Users\andre>
```

Con questo comando riusciamo a cancellare permanentemente il contenuto del cestino.

2. ESAMINARE TRAFFICO HTTP E HTTPS CON WIRESHARK

2.1 TRAFFICO HTTP

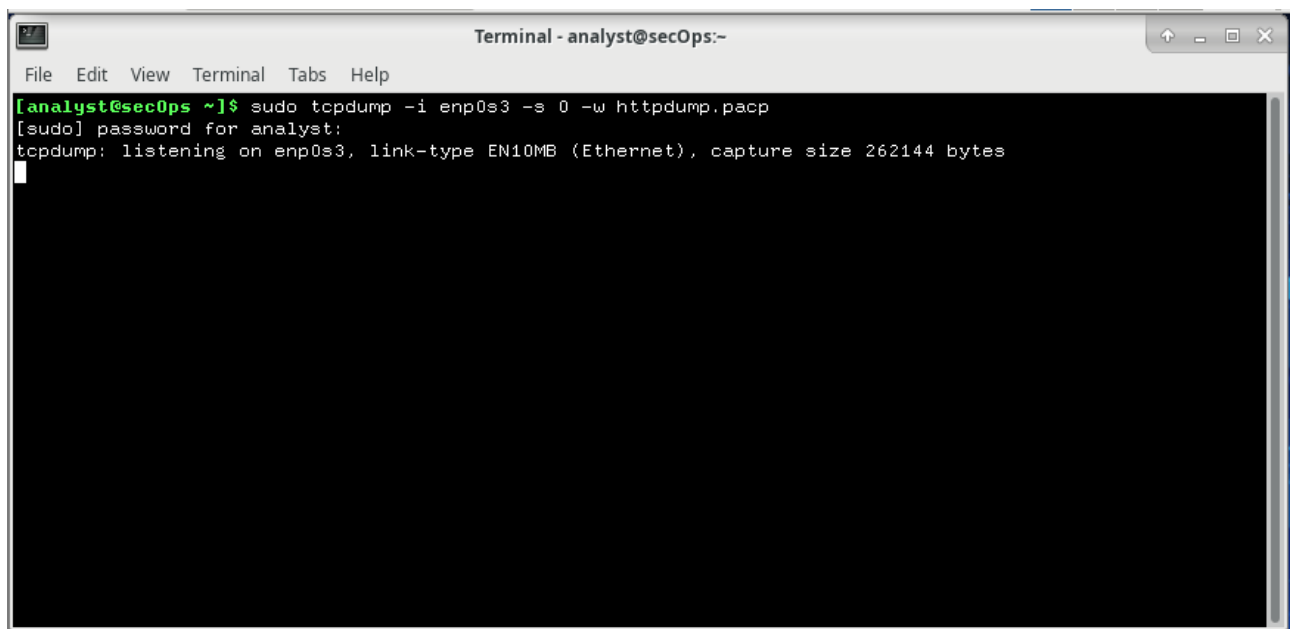
In questa parte utilizzeremo il comando **tcpdump** per catturare il contenuto nel traffico HTTP; con il comando salveremo il traffico catturato in un file **.pcap** per la successiva analisi con Wireshark sulla macchina virtuale CyberOps Workstation.

Per prima cosa apriamo il terminale e digitiamo il comando **ip address**

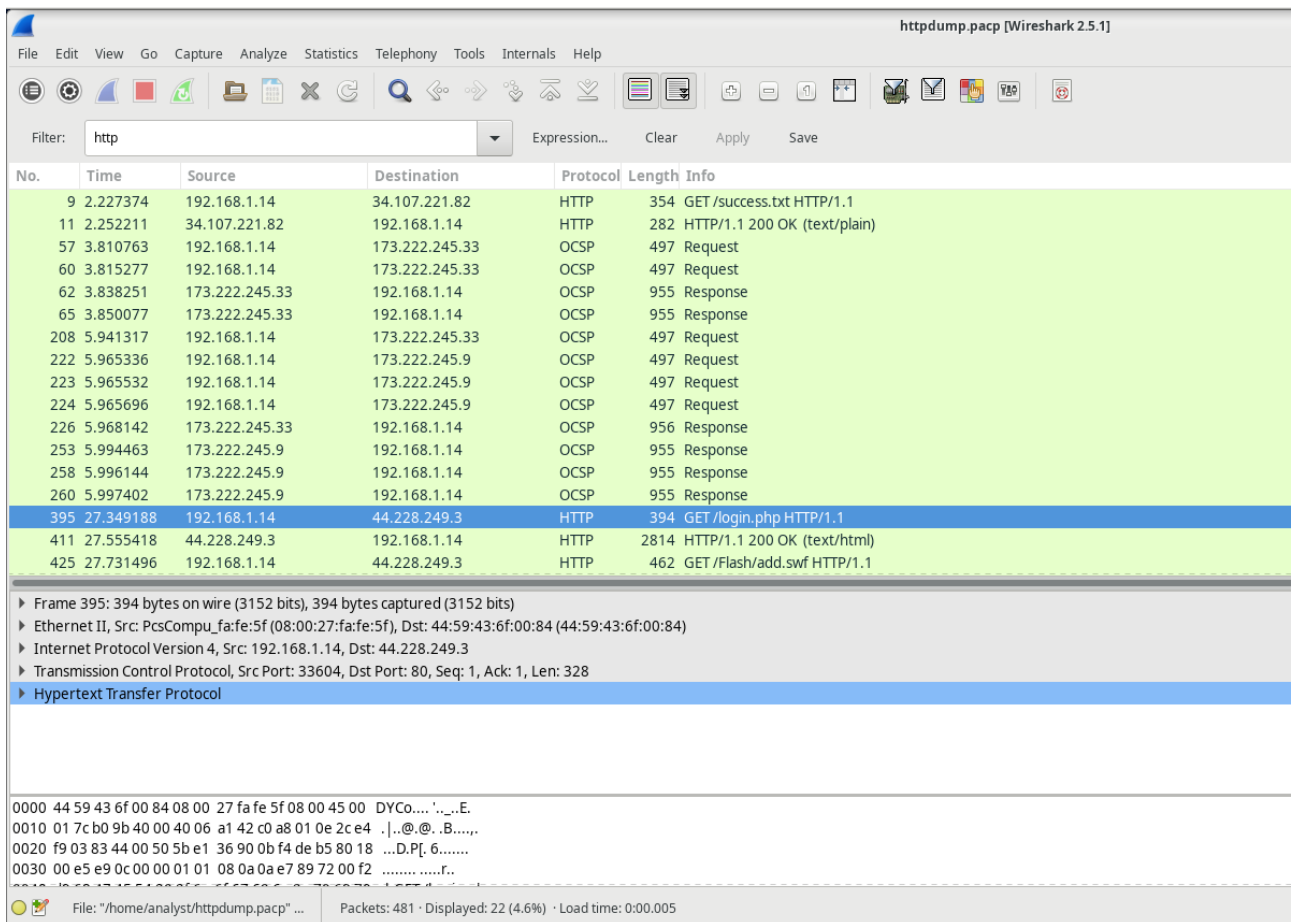
```
[analyst@secOps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ovs-system: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 96:66:1d:a1:bc:e8 brd ff:ff:ff:ff:ff:ff
3: s1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 9e:e6:57:6f:c0:45 brd ff:ff:ff:ff:ff:ff
4: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:fa:fe:5f brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.14/24 brd 192.168.1.255 scope global dynamic enp0s3
        valid_lft 85959sec preferred_lft 85959sec
    inet6 fe80::a00:27ff:fefa:fe5f/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```

Qui notiamo che l'interfaccia di rete interessata è **enp0s3** con indirizzo IP **192.168.1.14/24**.

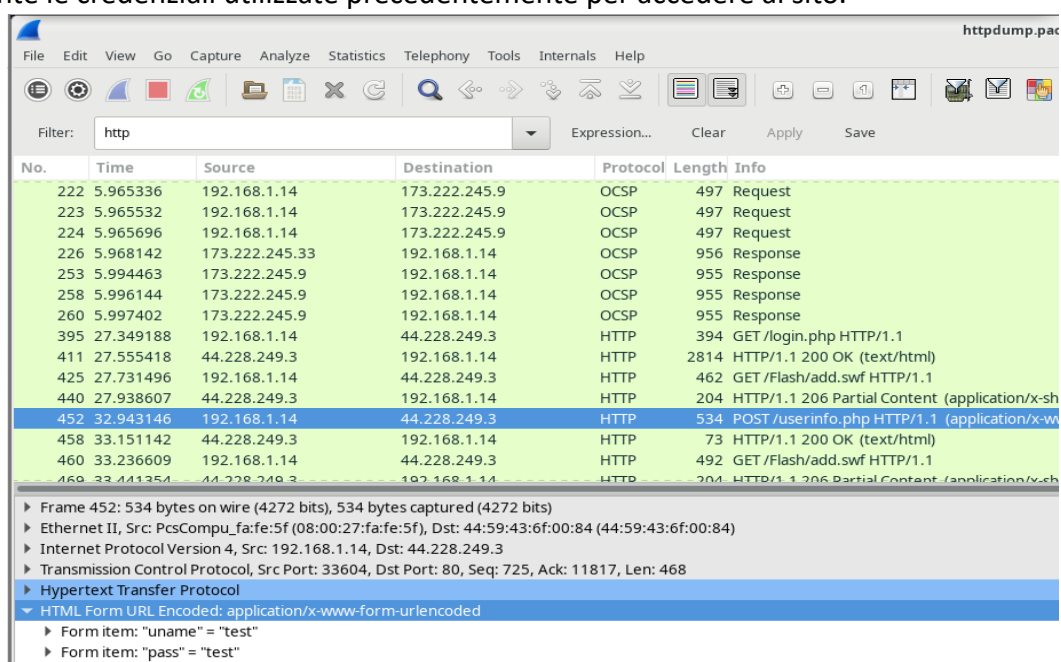
Catturiamo il traffico TCP con il comando **sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap**



Apriamo una pagina Firefox e ci colleghiamo alla pagina <http://testphp.vulnweb.com/login.php>.
Accediamo al portale e subito dopo terminiamo la cattura sul terminale con CTRL+C
Avviamo Wireshark e apriamo il file .pcap salvato.



Sul filtro inseriamo http per visualizzare i pacchetti che hanno utilizzato questo protocollo..
Troveremo la richiesta **POST** e in **HTML Form URL Encoded: application/x-www-form-urlencoded** contenente le credenziali utilizzate precedentemente per accedere al sito.



2.2 CATTURA TRAFFICO HTTPS

Per la cattura del traffico HTTPS la procedura di preparazione è la medesima, solo che in questo caso proveremo a visitare il sito **netacad.com** ed il comando sul terminale sarà **sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap**

[← Go back](#)

[English \(English\) ^](#)

Welcome!

Please login to your account.


Email

Password

[Forgot Password?](#)

Login

Or continue with

 Google

Don't have an account? [Sign up](#)

Stavolta troveremo dei pacchetti Application Data e il relativo payload risulterà illeggibile poiché crittografato tramite TLS.

150.13823844.212.234.95192.168.1.14TLSv1.23546Application Data, Application Data, Application Data

160.138252192.168.1.1444.212.234.95TCP6652406 → 443 [ACK] Seq=547 Ack=35161 Win=3076 Len=0

▶ Frame 15: 3546 bytes on wire (28368 bits), 3546 bytes captured (28368 bits)

▶ Ethernet II, Src: 44:59:43:6f:00:84 (44:59:43:6f:00:84), Dst: PcsCompu_fa:fe:5f (08:00:27:fa:fe:5f)

▶ Internet Protocol Version 4, Src: 44.212.234.95, Dst: 192.168.1.14

▶ Transmission Control Protocol, Src Port: 443, Dst Port: 52406, Seq: 31681, Ack: 547, Len: 3480

▶ [3 Reassembled TCP Segments (16263 bytes): #11(5187), #13(10080), #15(996)]

Secure Sockets Layer

▼ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls

Content Type: Application Data (23)

Version: TLS 1.2 (0x0303)

Length: 16258

Encrypted Application Data: 000000000000000034baf4f8901f19ed8ef7d006492652a32d...

Secure Sockets Layer

000017 03 03 3f 82 00 00 00 00 00 00 00 34 ba f4 f8 ...2... ..4...

001090 1f 19 ed 8e f7 d0 06 49 26 52 a3 2d e5 7e be I&R.~.

002068 e9 10 11 65 23 67 52 33 32 55 eb 03 c7 13 84 ...h...e#gR 32U.....

003004 18 61 28 61 25 ad 87 94 f2 fb 40 85 da 72 c4 ...a(a%.. ...@..r.

00409f 4e 81 6e bb 25 06 8c 2f 3a 1d 10 c1 3f a9 42 ...N.n.%.. /:....?..B

00508e 3d f5 b2 03 5f 7e 34 40 c4 f0 1a af 5d 17 f1 ...~4 @...1

Frame (3546 bytes)

Reassembled TCP (16263 bytes)

3. ESPLORAZIONE NMAP

Nmap è uno strumento di ricognizione di rete. Viene utilizzato per scansionare la rete e determinare quali host sono attivi (indirizzi IP e sistema operativo) e i servizi in esecuzione. Per poter conoscere le funzionalità del tool possiamo digitare sul terminale il comando **man nmap**, che ci darà la guida di utilizzo del tool.

```
NMAP(1)                                Nmap Reference Guide                                NMAP(1)

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.

    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: 1186-221.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/2.2.14 ((Ubuntu))
```

Proviamo ad effettuare una scansione del localhost con **nmap -A -T4 localhost**

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-04-11 07:54 EDT
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 6
|     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 11.49 seconds
[analyst@secOps ~]$
```

Possiamo notare:

- 21/tcp: servizio ftp che esegue vsftpd 2.0.8
- 22/tcp: servizio ssh che esegue OpenSSH 7.7

Proviamo ora ad effettuare una scansione della rete col comando **nmap -A -T4 192.168.1.0/24**

Poichè all'interno di questa rete sono connessi diversi dispositivi, risulta difficile elencarli tutti.

Alcuni di questi hanno tutte le porte chiuse.

Prendiamo in analisi l'host con ip **192.168.1.7**. Notiamo le porte:

- 1080/tcp: servizio socks5
- 8009/tcp: servizio http
- 8888/tcp: tcpwrapped
- 9080/tcp: glrpc?

```
Nmap scan report for 192.168.1.7
Host is up (0.0077s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE VERSION
1080/tcp   open  socks5   (No authentication; connection failed)
|_ socks-auth-info:
|_  No authentication
8009/tcp   open  http      Amazon Whisperplay DIAL REST service
|_ _ajp-methods: Failed to get a valid response for the OPTION request
|_ _http-title: Site doesn't have a title (text/plain).
8888/tcp   open  tcpwrapped
9080/tcp   open  glrpc?
|_ fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 200 OK
|     Date: Fri, 11 Apr 2025 14:03:51 CEST
|     Server: NRDP/2020.1.3.1
|     Connection: close
|     Cache-Control: no-cache
|     Content-Length: 0
|     status:ok
|   GetRequest:
|     HTTP/1.0 200 OK
|     Date: Fri, 11 Apr 2025 14:03:10 CEST
|     Server: NRDP/2020.1.3.1
|     Connection: close
|     Cache-Control: no-cache
|     Content-Length: 0
|     status:ok
|_ service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port:8009-TCP,Vz7,7051:720=4/1111Time=87F80808P-x86_64-unknown-linux-gnu
SF-Tr(GetRequest,99,"HTTP/1.0:x202000lx200K\r\nDate:\r\nx20Fri:\r\nx2011:\r\nx20\r\n
SF:x202025\r\nx2014:03:10\r\nx20CEST\r\n\r\nServer:\r\nx20NRDP/2020.1.3.1\r\n\r\nConnect
SF:ion:\r\nx20close\r\n\r\nCache-Control:\r\nx20no-cache\r\n\r\nContent-Length:\r\nx209\r\n\r\n
SF:\r\n\r\nstatus=ok")X(FourOhFourRequest,99,"HTTP/1.0:x202000lx200K\r\nDate:
SF:\r\nx20Fri:\r\nx2011:\r\nx20\r\nx202025\r\nx2014:03:51\r\nx20CEST\r\n\r\nServer:\r\nx20NRDP/20
SF:20\r\nx201.3.1\r\n\r\nConnection:\r\nx20close\r\n\r\nCache-Control:\r\nx20no-cache\r\n\r\nCo
SF:ntent-Length:\r\nx209\r\n\r\nstatus=ok");
Service Info: Device: media device
```

Proviamo ad effettuare una scansione completa del sito scanme.nmap.org con il comando **nmap -A -T4 scanme.nmap.org**, -A serve per effettuare la scansione completa, -T4 indica il numero di thread che vengono eseguiti in parallelo

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2025-04-11 07:42 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.18s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|_ 2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|_ 256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_ 256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Go ahead and ScanMe!
9929/tcp  open  nping-echo   Nping echo
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.42 seconds
```

Da qui possiamo notare che le porte aperte rilevate sono:

- Indirizzo IPv4 45.33.32.156 e Ipv6 2600:3c01::f03c:91ff:fe18:bb2f
- 22/tcp: servizio ssh che esegue OpenSSH 6.6.1p1 Ubuntu, sono inoltre mostrate le chiavi host per DSA, RSA, ECDSA, ED25519
- 80/tcp: servizio http che esegue Apache httpd 2.4.7
- 9929/tcp: servizio nping-echo
- 31337/tcp: servizio tcpwrapped
- Sistema Operativo: Linux

4. ATTACCO A UN DATABASE MySQL

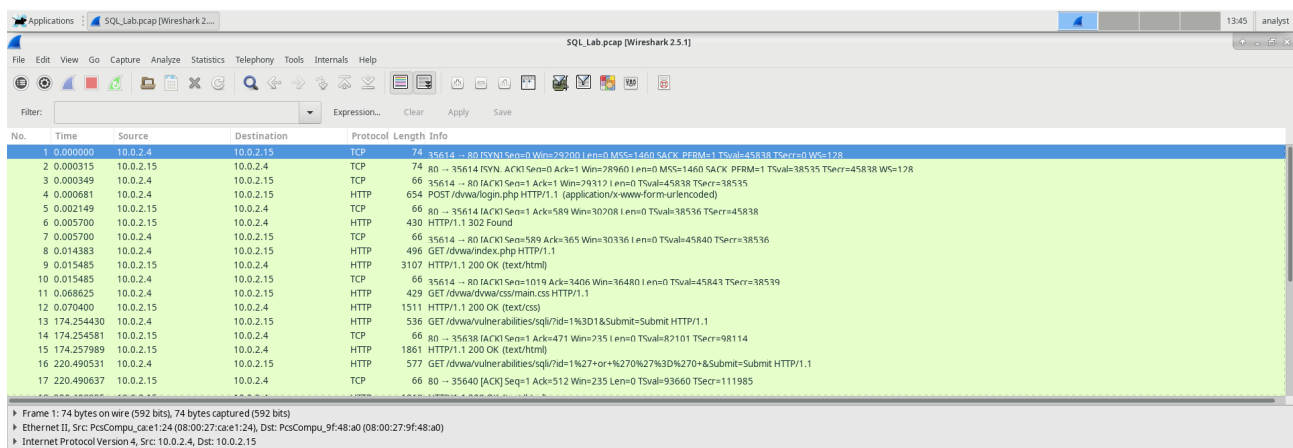
Gli attacchi SQL Injection consentono agli hacker malintenzionati di digitare istruzioni SQL in un sito web e ricevere una risposta dal database. Ciò consente agli aggressori di manomettere i dati correnti nel database, falsificare le identità e compiere altri illeciti.

Apertura di Wireshark e Caricamento del File PCAP

Sono stati seguiti i seguenti passaggi per aprire Wireshark e caricare il file PCAP fornito:

Avvio della macchina virtuale CyberOps Workstation. Clic su **Applications > CyberOPS > Wireshark** sul desktop per avviare l'applicazione Wireshark. Nell'applicazione Wireshark, è stato cliccato su **Open** situato al centro della finestra sotto la sezione Files. Navigazione attraverso la directory **/home/analyst/** e ricerca della cartella **lab.support.files**. All'interno di questa directory, è stato aperto il file **SQL_Lab.pcap**. e. Il file PCAP si è aperto in Wireshark, visualizzando il traffico di rete catturato durante un periodo di 441 secondi (circa 8 minuti), la durata dell'attacco di SQL injection.

In base alle informazioni visualizzate nel file PCAP, i due indirizzi IP coinvolti nell'attacco di SQL injection sono **10.0.2.4** e **10.0.2.15**.

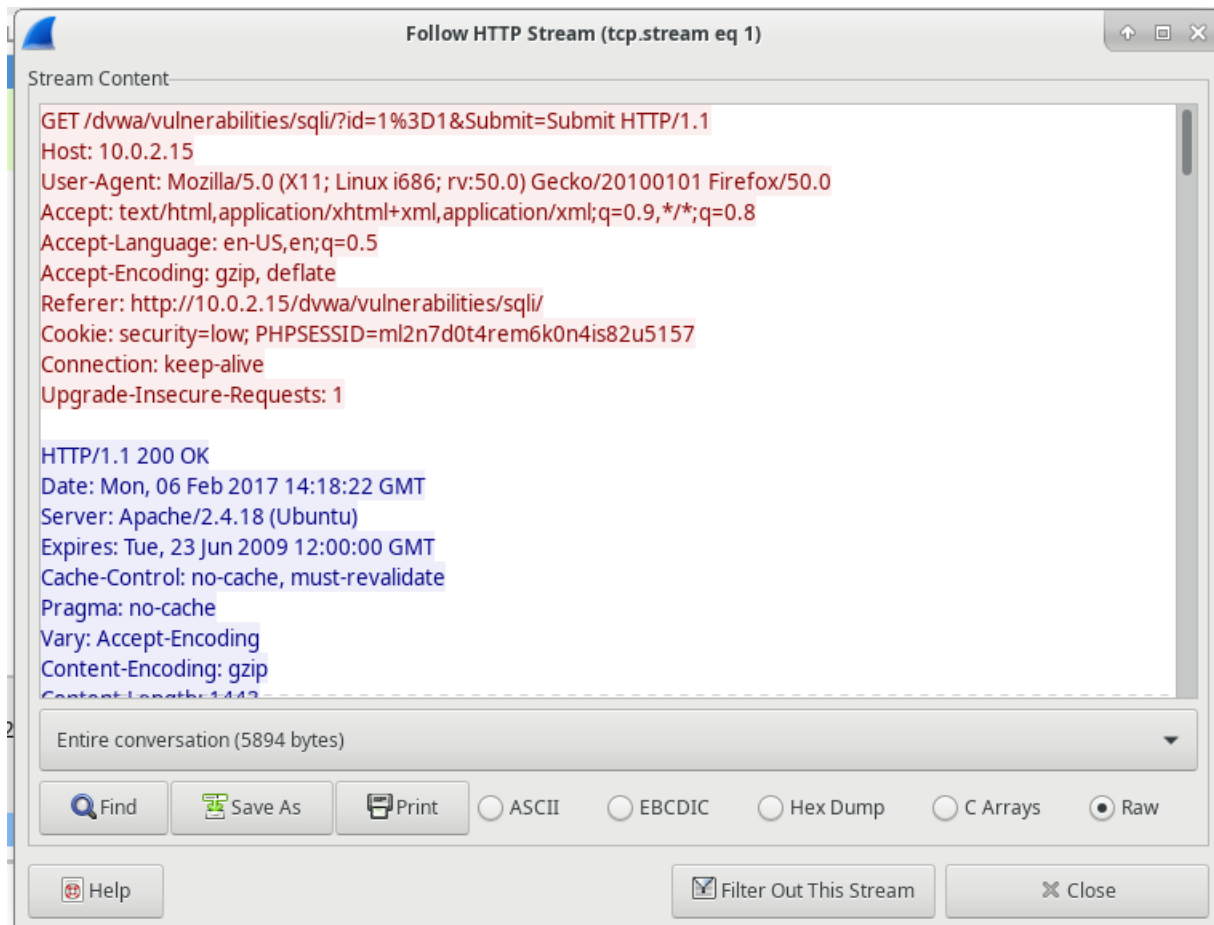


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.4	10.0.2.15	TCP	74	35614 → 80 [ACK] Seq=1190292001 Len=0 MSS=1460 SACK_PERM=1 TSval=38535 TSecr=45838 Win=178
2	0.000315	10.0.2.15	10.0.2.4	TCP	74	80 → 35614 [RST] Seq=0 Ack=1 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=38535 TSecr=45838 Win=178
3	0.000349	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=45838 TSecr=38535
4	0.000681	10.0.2.4	10.0.2.15	HTTP	654	POST /dwa/login.php HTTP/1.1 (application/x-www-form-urlencoded)
5	0.002149	10.0.2.15	10.0.2.4	TCP	66	80 → 35614 [ACK] Seq=1 Ack=589 Win=30208 Len=0 TSval=38536 TSecr=45838
6	0.005700	10.0.2.15	10.0.2.4	HTTP	430	HTTP/1.1 302 Found
7	0.005700	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=589 Ack=365 Win=30336 Len=0 TSval=45840 TSecr=38536
8	0.014383	10.0.2.4	10.0.2.15	HTTP	496	GET /dwa/index.php HTTP/1.1
9	0.015485	10.0.2.15	10.0.2.4	HTTP	3107	HTTP/1.1 200 OK (text/html)
10	0.015485	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=1019 Ack=3406 Win=36480 Len=0 TSval=45843 TSecr=38539
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

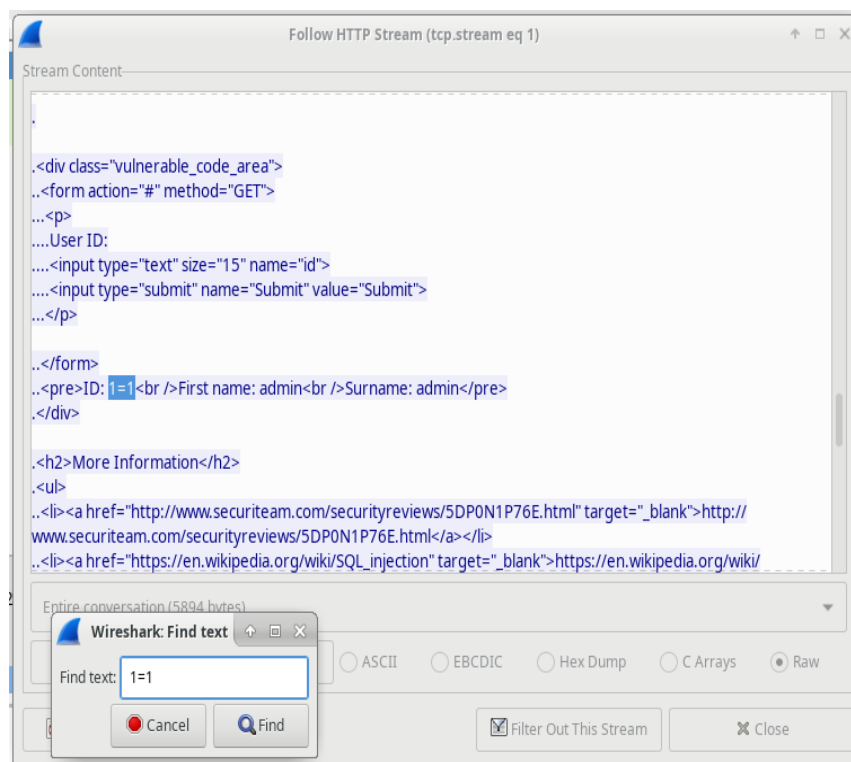
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: PcsCompu_care1:24 (08:00:27:ca:e1:24), Dst: PcsCompu_9f:48:a0 (08:00:27:9f:48:a0)
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15

Visualizzazione dell'Inizio dell'Attacco SQL Injection

All'interno della cattura Wireshark, è stata effettuata una clic con il tasto destro sulla linea 13 e selezionata l'opzione **Follow HTTP Stream**. La linea 13 è stata scelta in quanto rappresenta una richiesta HTTP GET, utile per seguire il flusso di dati a livello applicativo che precede il test della query per l'SQL injection.



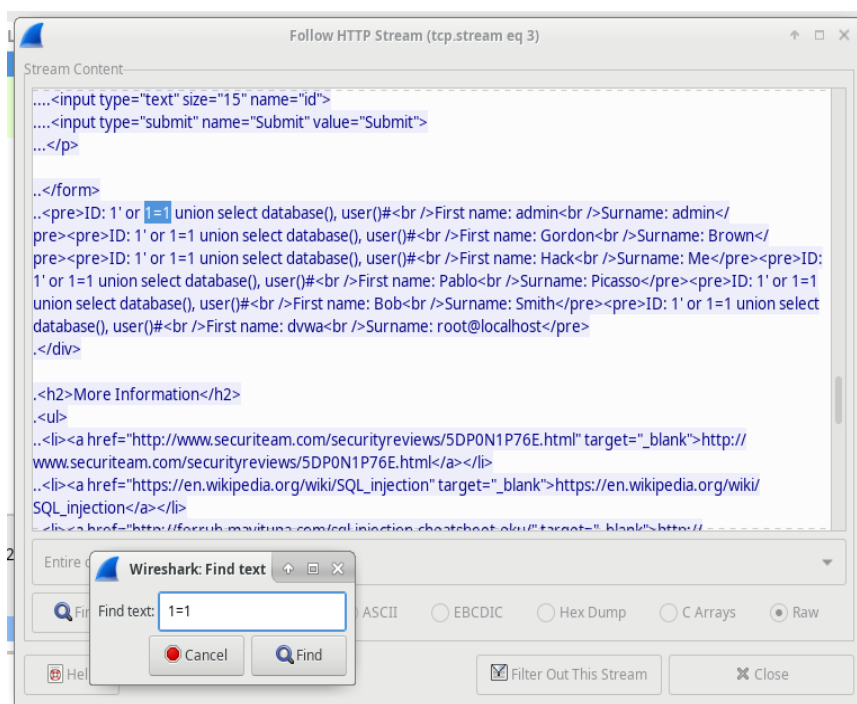
Il traffico sorgente è visualizzato in rosso, indicando che l'host 10.0.2.4 ha inviato una richiesta GET all'host 10.0.2.15. In blu, il dispositivo di destinazione (10.0.2.15) risponde alla sorgente. b. Nel campo **Find**, è stato inserito il testo **1=1** e cliccato su **Find Next**. L'attaccante ha inserito una query (**1=1**) in un campo di ricerca UserID sul target 10.0.2.15 per verificare se l'applicazione fosse vulnerabile a SQL injection. Invece di ricevere un messaggio di fallimento del login, l'applicazione ha risposto con un record dal database. Questo ha confermato all'attaccante la possibilità di inserire comandi SQL e ricevere risposte dal database. La stringa di ricerca **1=1** crea un'istruzione SQL che sarà sempre vera, rendendo irrilevante l'input effettivo nel campo.



La Continuazione dell'Attacco SQL Injection

In questa fase, è stata analizzata la prosecuzione dell'attacco:

All'interno della cattura Wireshark, è stata effettuata una clic con il tasto destro sulla linea 19 e selezionata l'opzione **Follow HTTP Stream**. Nel campo **Find**, è stato inserito il testo **1=1** e cliccato su **Find Next**. L'attaccante ha inserito una query (**1' or 1=1 union select database(), user()#**) in un campo di ricerca UserID sul target 10.0.2.15. Invece di un messaggio di fallimento del login, l'applicazione ha risposto con le seguenti informazioni:

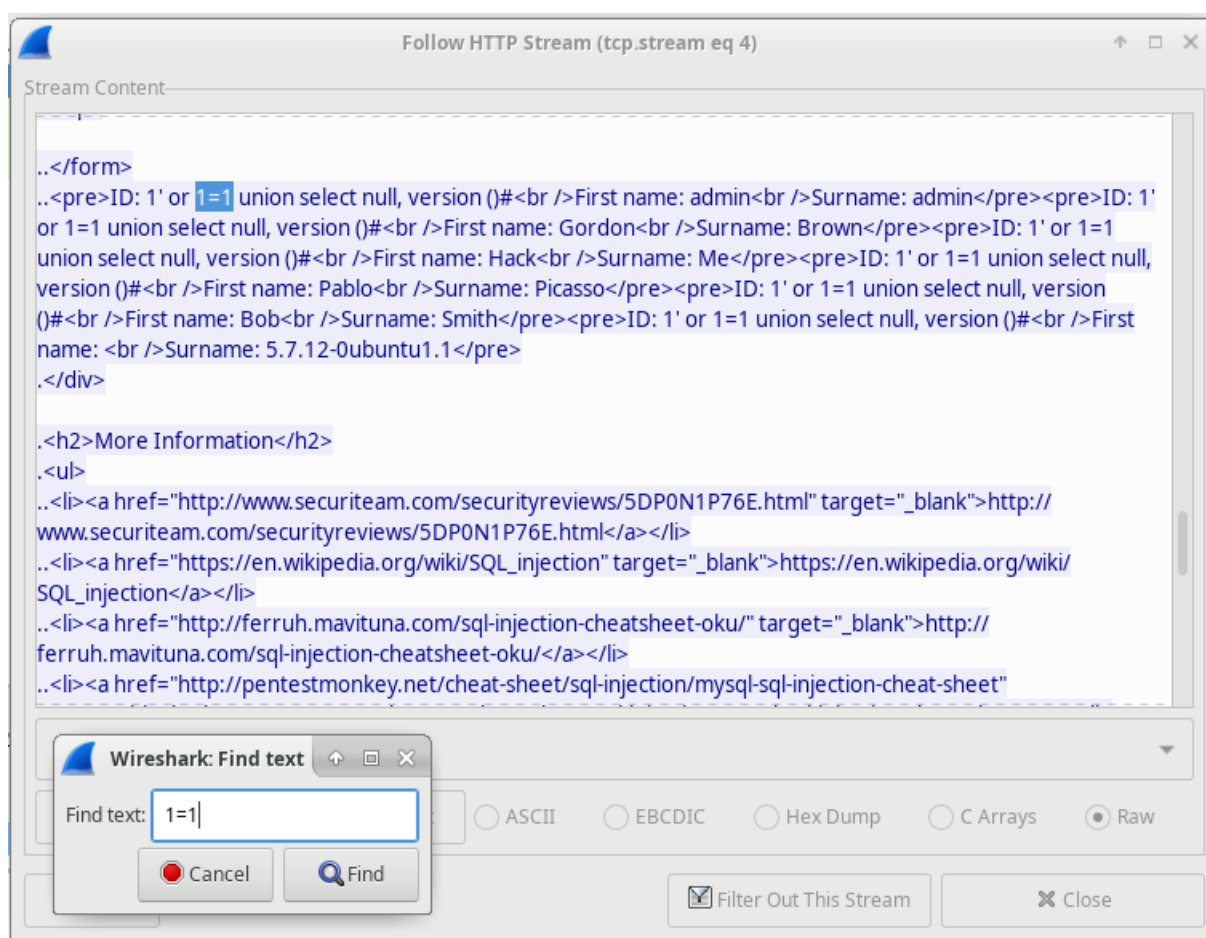


Il nome del database è **dvwa** e l'utente del database è **root@localhost**. Sono stati visualizzati anche diversi account utente. d. La finestra **Follow HTTP Stream** è stata chiusa. e. È stato cliccato su **Clear display filter** per visualizzare l'intera conversazione Wireshark.

L'Attacco SQL Injection Fornisce Informazioni di Sistema

L'attaccante ha continuato l'attacco, mirando a informazioni più specifiche:

All'interno della cattura Wireshark, è stata effettuata una clic con il tasto destro sulla linea 22 e selezionata l'opzione **Follow HTTP Stream**. Il traffico sorgente (in rosso) mostra l'invio di una richiesta GET all'host 10.0.2.15. Il dispositivo di destinazione (in blu) risponde alla sorgente. Nel campo **Find**, è stato inserito il testo **1=1** e cliccato su **Find Next**. L'attaccante ha inserito una query (**1' or 1=1 union select null, version ()#**) in un campo di ricerca UserID sul target 10.0.2.15 per ottenere l'identificatore della versione del database. La versione è visibile alla fine dell'output, immediatamente prima del tag di chiusura HTML `</pre></div>`.



La versione del database è **MySQL 5.7.12-0**.

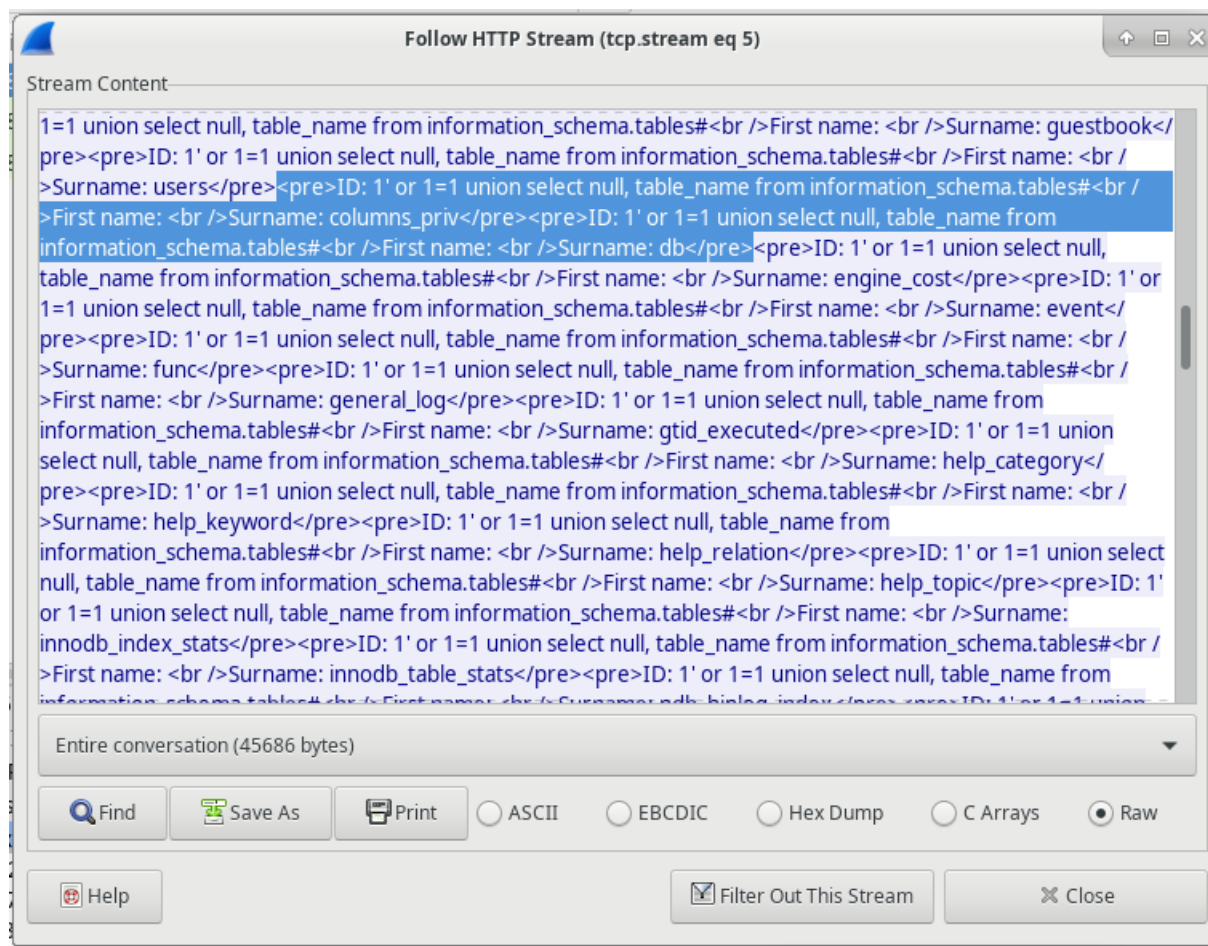
La finestra **Follow HTTP Stream** è stata chiusa. e. È stato cliccato su **Clear display filter** per visualizzare l'intera conversazione Wireshark.

L'Attacco SQL Injection e le Informazioni sulle Tabelle

L'attaccante, consapevole della presenza di numerose tabelle SQL contenenti informazioni, ha tentato di individuarle:

All'interno della cattura Wireshark, è stata effettuata una clic con il tasto destro sulla linea 25 e

selezionata l'opzione **Follow HTTP Stream**. La sorgente (in rosso) ha inviato una richiesta GET all'host 10.0.2.15. Il dispositivo di destinazione (in blu) risponde alla sorgente. Nel campo **Find**, è stato inserito il testo **users** e cliccato su **Find Next**. c. L'attaccante ha inserito una query (**1'or 1=1 union select null, table_name from information_schema.tables#**) in un campo di ricerca UserID sul target 10.0.2.15 per visualizzare tutte le tabelle presenti nel database. Questa query ha prodotto un output molto ampio di numerose tabelle, poiché l'attaccante ha specificato "null" senza ulteriori filtri.



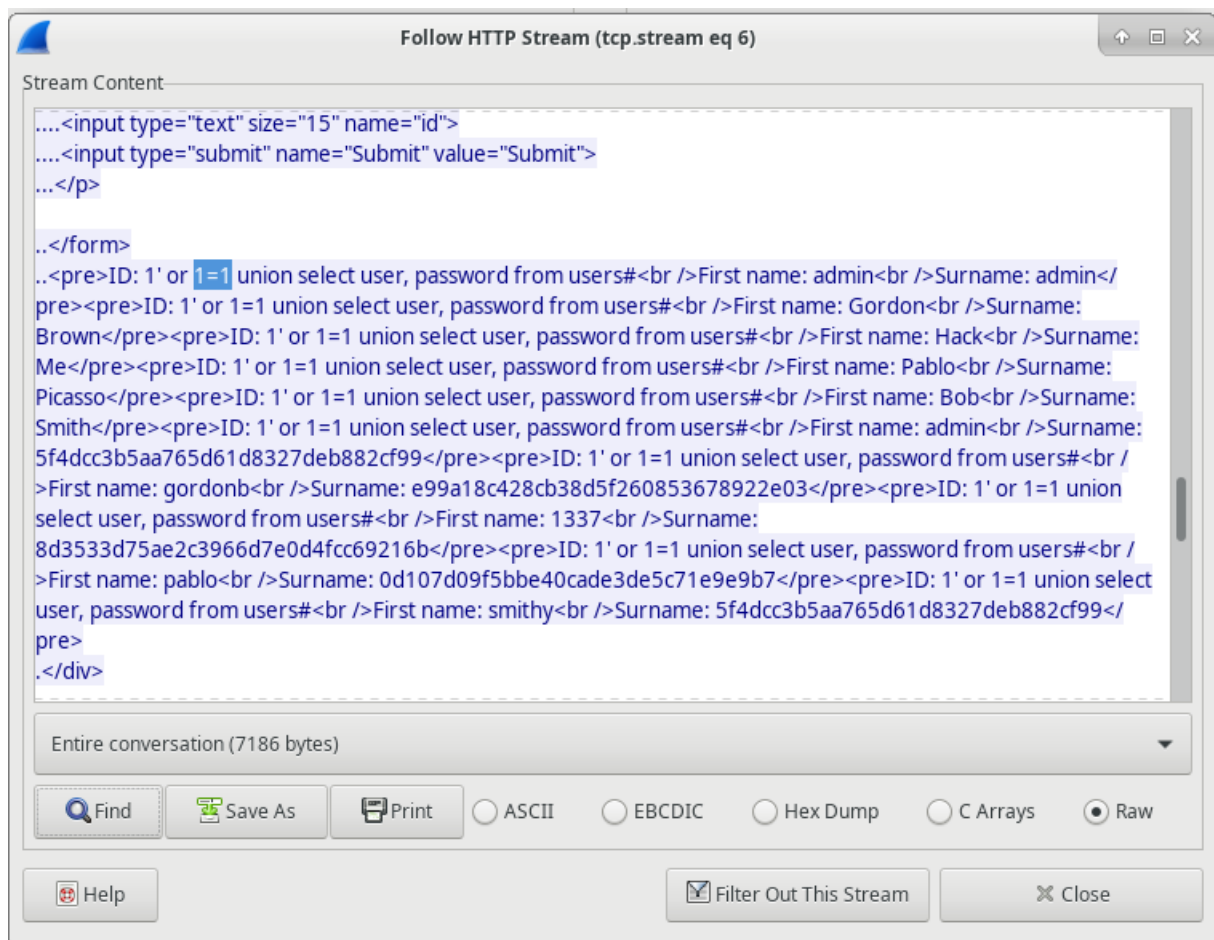
Cosa farebbe per l'attaccante il comando modificato (1' OR 1=1 UNION SELECT null, column_name FROM INFORMATION_SCHEMA.columns WHERE table_name='users')?

Il comando modificato (**1' OR 1=1 UNION SELECT null, column_name FROM INFORMATION_SCHEMA.columns WHERE table_name='users'**) farebbe sì che il database risponda con un output molto più breve, filtrato per la presenza della parola "users" nel nome della tabella. Invece di elencare tutte le tabelle, mostrerebbe solo i nomi delle colonne appartenenti alla tabella denominata "users". La finestra **Follow HTTP Stream** è stata chiusa. e. È stato cliccato su **Clear display filter** per visualizzare l'intera conversazione Wireshark.

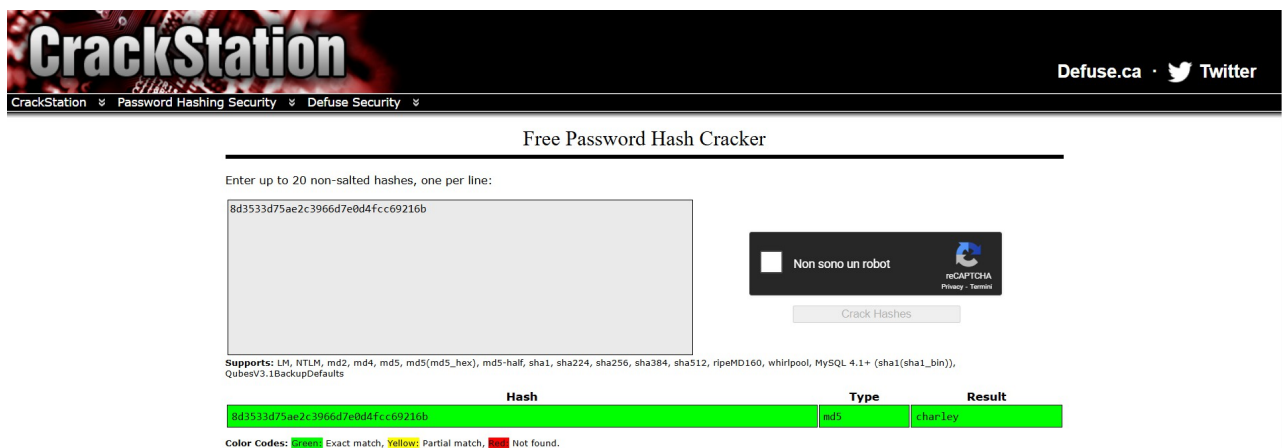
La Conclusione dell'Attacco SQL Injection

L'attacco si è concluso con l'ottenimento delle password hash: all'interno della cattura Wireshark, è stata effettuata una clic con il tasto destro sulla linea 28 e selezionata l'opzione **Follow HTTP Stream**. La sorgente (in rosso) ha inviato una richiesta GET all'host 10.0.2.15. Il dispositivo di destinazione (in blu) risponde alla sorgente. b. È stato cliccato su **Find** e digitato **1=1**. Dopo aver localizzato l'entry, è stato cliccato su **Cancel** nella finestra di ricerca. L'attaccante ha inserito una query (**1'or 1=1 union select user, password from users#**) in un campo di ricerca UserID sul target

10.0.2.15 per estrarre nomi utente e password hash



L'utente con la password hash **8d3533d75ae2c3966d7e0d4fcc69216b** è **1337**. Utilizzando un sito web come <https://crackstation.net/>, la password hash è stata copiata nel tool di cracking.



La password in chiaro è **charley**.