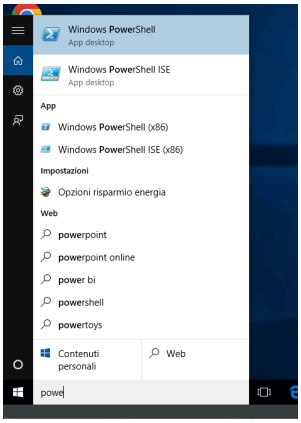
Utilizzo di Windows PowerShell

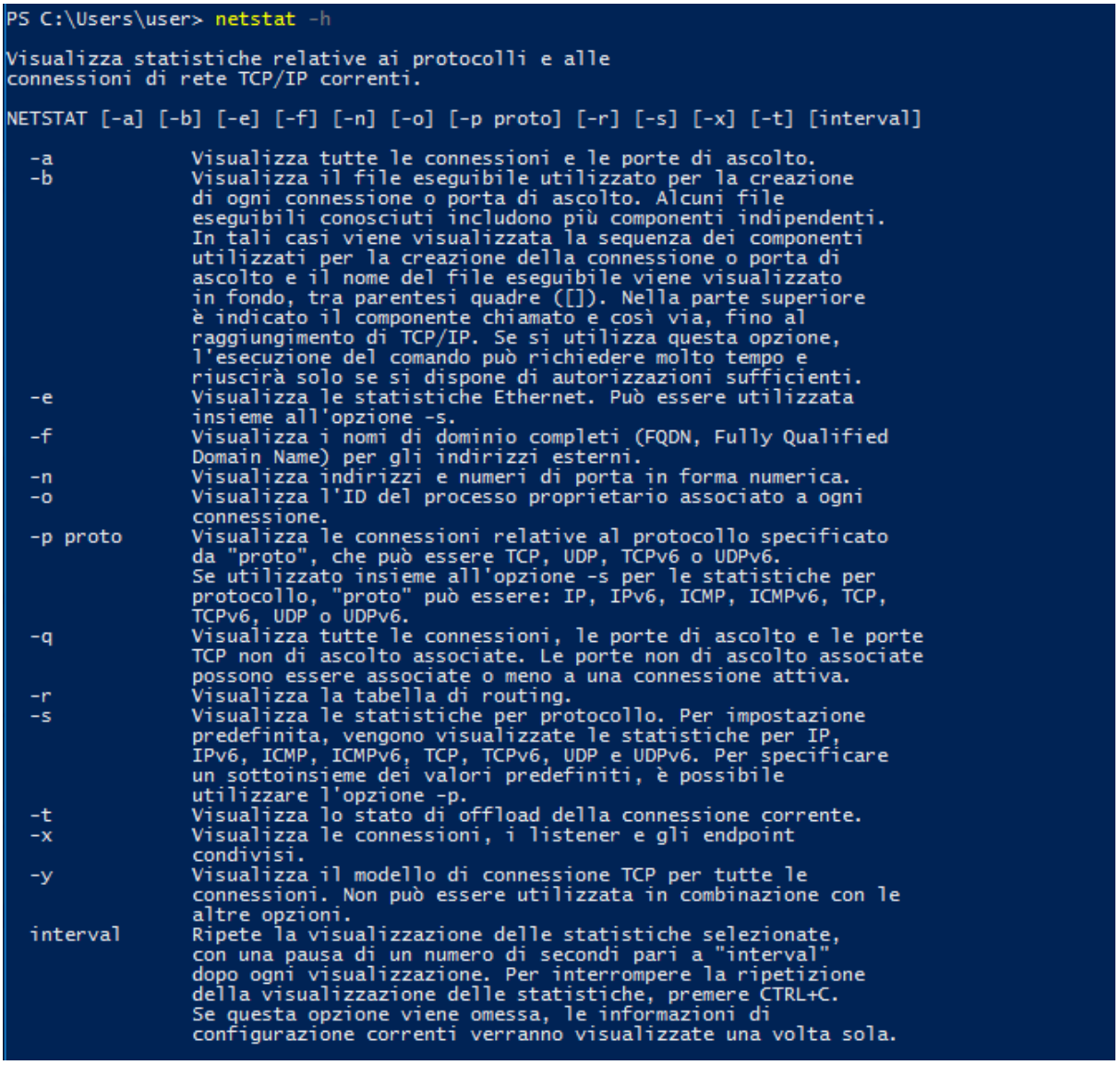
Per prima cosa ho cercato PowerShell e l'ho avviato



Successivamente ho dato i programmi che suggeriva la guida:
dir che mi elenca tutte le directory, ipconfig mi fa vedere tutte le schede di rete ed infine Get-Alias dir serve per verificare a quale comando è associato l'alias **`dir`**

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


    Directory: C:\Users\user


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        09/07/2024     16:37                Contacts
d-r---        28/01/2025     14:22                Desktop
d-r---        09/07/2024     18:05                Documents
d-r---        28/01/2025     14:22                Downloads
d-r---        09/07/2024     16:37                Favorites
d-r---        09/07/2024     16:37                Links
d-r---        09/07/2024     16:37                Music
d-r---        09/07/2024     16:40                OneDrive
d-r---        09/07/2024     16:39                Pictures
d-r---        09/07/2024     16:37                Saved Games
d-r---        09/07/2024     16:39                Searches
d-r---        09/07/2024     16:37                Videos


PS C:\Users\user> ipconfig

Configurazione IP di Windows


Scheda Ethernet Ethernet:

   Suffisso DNS specifico per connessione: station
   Indirizzo IPv6 . . . . . . . . . . . . . . . . : fd00::6c5f:d73c:7359:3182
   Indirizzo IPv6 temporaneo. . . . . . . . . . . : fd00::98c4:259:6b63:fd0
   Indirizzo IPv6 locale rispetto al collegamento . : fe80::6c5f:d73c:7359:3182%4
   Indirizzo IPv4. . . . . . . . . . . . . . . . : 10.0.2.15
   Subnet mask . . . . . . . . . . . . . . . . . : 255.255.255.0
   Gateway predefinito . . . . . . . . . . . . . : fe80::2%4
                                                   10.0.2.2

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

   Suffisso DNS specifico per connessione:
   Indirizzo IPv6 . . . . . . . . . . . . . . . . : 2001:0:2851:782c:481:d2c2:a2be:cce
   Indirizzo IPv6 locale rispetto al collegamento . : fe80::481:d2c2:a2be:cce%5
   Gateway predefinito . . . . . . . . . . . . . :

Scheda Tunnel isatap.station:

   Stato supporto. . . . . . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione: station
PS C:\Users\user> Get-Alias dir

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

Seguendo sempre la guida ho digitato il comando netstat -h che mi fa vedere tutti i possibili comandi che posso utilizzare e a cosa servono



```
PS C:\Users\user> netstat -h

Visualizza statistiche relative ai protocolli e alle
connessioni di rete TCP/IP correnti.

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

  -a            Visualizza tutte le connessioni e le porte di ascolto.
  -b            Visualizza il file eseguibile utilizzato per la creazione
                di ogni connessione o porta di ascolto. Alcuni file
                eseguibili conosciuti includono più componenti indipendenti.
                In tali casi viene visualizzata la sequenza dei componenti
                utilizzati per la creazione della connessione o porta di
                ascolto e il nome del file eseguibile viene visualizzato
                in fondo, tra parentesi quadre ([]). Nella parte superiore
                è indicato il componente chiamato e così via, fino al
                raggiungimento di TCP/IP. Se si utilizza questa opzione,
                l'esecuzione del comando può richiedere molto tempo e
                riuscirà solo se si dispone di autorizzazioni sufficienti.
  -e            Visualizza le statistiche Ethernet. Può essere utilizzata
                insieme all'opzione -s.
  -f            Visualizza i nomi di dominio completi (FQDN, Fully Qualified
                Domain Name) per gli indirizzi esterni.
  -n            Visualizza indirizzi e numeri di porta in forma numerica.
  -o            Visualizza l'ID del processo proprietario associato a ogni
                connessione.
  -p proto      Visualizza le connessioni relative al protocollo specificato
                da "proto", che può essere TCP, UDP, TCPv6 o UDPv6.
                Se utilizzato insieme all'opzione -s per le statistiche per
                protocollo, "proto" può essere: IP, IPv6, ICMP, ICMPv6, TCP,
                TCPv6, UDP o UDPv6.
  -q            Visualizza tutte le connessioni, le porte di ascolto e le porte
                TCP non di ascolto associate. Le porte non di ascolto associate
                possono essere associate o meno a una connessione attiva.
  -r            Visualizza la tabella di routing.
  -s            Visualizza le statistiche per protocollo. Per impostazione
                predefinita, vengono visualizzate le statistiche per IP,
                IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP e UDPv6. Per specificare
                un sottoinsieme dei valori predefiniti, è possibile
                utilizzare l'opzione -p.
  -t            Visualizza lo stato di offload della connessione corrente.
  -x            Visualizza le connessioni, i listener e gli endpoint
                condivisi.
  -y            Visualizza il modello di connessione TCP per tutte le
                connessioni. Non può essere utilizzata in combinazione con le
                altre opzioni.
  interval      Ripete la visualizzazione delle statistiche selezionate,
                con una pausa di un numero di secondi pari a "interval"
                dopo ogni visualizzazione. Per interrompere la ripetizione
                della visualizzazione delle statistiche, premere CTRL+C.
                Se questa opzione viene omessa, le informazioni di
                configurazione correnti verranno visualizzate una volta sola.
```

Ho usato -r che serve a farmi visualizzare le tabelle di routing

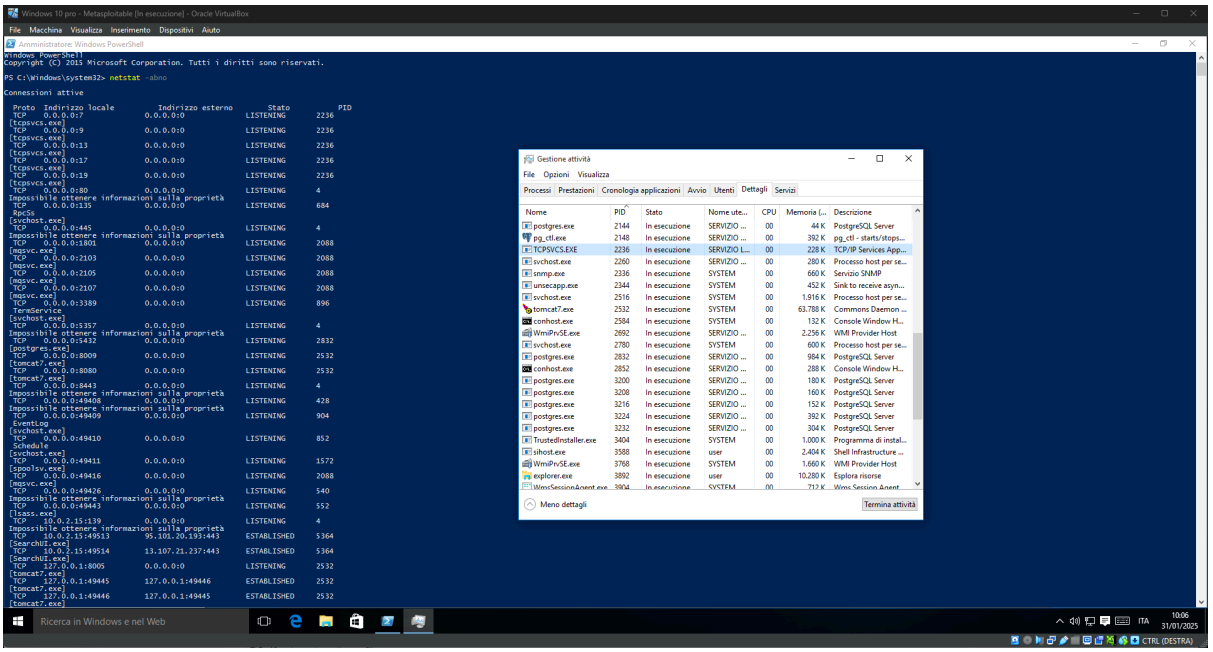
```
PS C:\Users\user> netstat -r
===========================================================================
Elenco interfacce
  4...08 00 27 44 aa 62 ......Intel(R) PRO/1000 MT Desktop Adapter
  1...........................Software Loopback Interface 1
  5...00 00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
  3...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
===========================================================================

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     10
         10.0.2.0    255.255.255.0         On-link         10.0.2.15    266
        10.0.2.15  255.255.255.255         On-link         10.0.2.15    266
       10.0.2.255  255.255.255.255         On-link         10.0.2.15    266
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link         10.0.2.15    266
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link         10.0.2.15    266
===========================================================================
Route permanenti:
  Nessuna

IPv6 Tabella route
===========================================================================
Route attive:
 Interf Metrica Rete Destinazione      Gateway
  4    266 ::/0                     fe80::2
  1    306 ::1/128                  On-link
  5    306 2001::/32                On-link
  5    306 2001:0:2851:782c:481:d2c2:a2be:cce/128
                                    On-link
  4    266 fd00::/64                On-link
  4    266 fd00::6c5f:d73c:7359:3182/128
                                    On-link
  4    266 fd00::98c4:259:6b63:fd0/128
                                    On-link
  4    266 fe80::/64                On-link
  5    306 fe80::/64                On-link
  5    306 fe80::481:d2c2:a2be:cce/128
                                    On-link
  4    266 fe80::6c5f:d73c:7359:3182/128
                                    On-link
  1    306 ff00::/8                 On-link
  4    266 ff00::/8                 On-link
  5    306 ff00::/8                 On-link
===========================================================================
Route permanenti:
  Nessuna
PS C:\Users\user>
```

Successivamente ho avviato PowerShell come amministratore (per poter utilizzare più comandi) facendo tasto destro esegui come amministratore

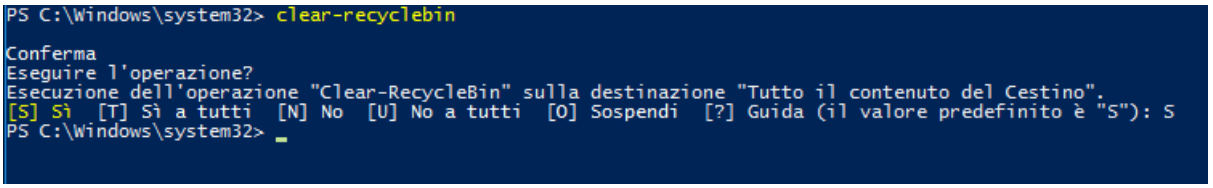
Ho usato netstat -abno che mi fa vedere tutte le connessioni attive con i programmi

```
PS C:\Windows\system32> netstat -abno

Connessioni attive

  Proto  Indirizzo locale          Indirizzo esterno        Stato           PID
  TCP    0.0.0.0:7              0.0.0.0:0              LISTENING       2236
 [tcpsvcs.exe]
  TCP    0.0.0.0:9              0.0.0.0:0              LISTENING       2236
 [tcpsvcs.exe]
  TCP    0.0.0.0:13             0.0.0.0:0              LISTENING       2236
 [tcpsvcs.exe]
  TCP    0.0.0.0:17             0.0.0.0:0              LISTENING       2236
 [tcpsvcs.exe]
  TCP    0.0.0.0:19             0.0.0.0:0              LISTENING       2236
 [tcpsvcs.exe]
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
 Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       684
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
 Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:1801           0.0.0.0:0              LISTENING       2088
 [mqsvc.exe]
  TCP    0.0.0.0:2103           0.0.0.0:0              LISTENING       2088
 [mqsvc.exe]
  TCP    0.0.0.0:2105           0.0.0.0:0              LISTENING       2088
 [mqsvc.exe]
  TCP    0.0.0.0:2107           0.0.0.0:0              LISTENING       2088
 [mqsvc.exe]
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       896
  TermService
 [svchost.exe]
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
 Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:5432           0.0.0.0:0              LISTENING       2832
 [postgres.exe]
  TCP    0.0.0.0:8009           0.0.0.0:0              LISTENING       2532
 [tomcat7.exe]
  TCP    0.0.0.0:8080           0.0.0.0:0              LISTENING       2532
 [tomcat7.exe]
  TCP    0.0.0.0:8443           0.0.0.0:0              LISTENING       4
 Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:49408          0.0.0.0:0              LISTENING       428
 Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:49409          0.0.0.0:0              LISTENING       904
  EventLog
 [svchost.exe]
  TCP    0.0.0.0:49410          0.0.0.0:0              LISTENING       852
  Schedule
 [svchost.exe]
  TCP    0.0.0.0:49411          0.0.0.0:0              LISTENING       1572
 [spoolsv.exe]
  TCP    0.0.0.0:49416          0.0.0.0:0              LISTENING       2088
 [mqsvc.exe]
  TCP    0.0.0.0:49426          0.0.0.0:0              LISTENING       540
 Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:49443          0.0.0.0:0              LISTENING       552
 [lsass.exe]
  TCP    10.0.2.15:139          0.0.0.0:0              LISTENING       4
 Impossibile ottenere informazioni sulla proprietà
  TCP    10.0.2.15:49513        95.101.20.193:443      ESTABLISHED     5364
 [SearchUI.exe]
  TCP    10.0.2.15:49514        13.107.21.237:443      ESTABLISHED     5364
 [SearchUI.exe]
  TCP    127.0.0.1:8005         0.0.0.0:0              LISTENING       2532
 [tomcat7.exe]
  TCP    127.0.0.1:49445        127.0.0.1:49446        ESTABLISHED     2532
 [tomcat7.exe]
  TCP    127.0.0.1:49446        127.0.0.1:49445        ESTABLISHED     2532
 [tomcat7.exe]
```

Successivamente ho aperto il task manager sono andato su dettagli e ho confrontato il primo pid della foto precedente per visualizzare la dimensione e se fosse realmente in esecuzione del programma in questo caso tcpsvcs.exe

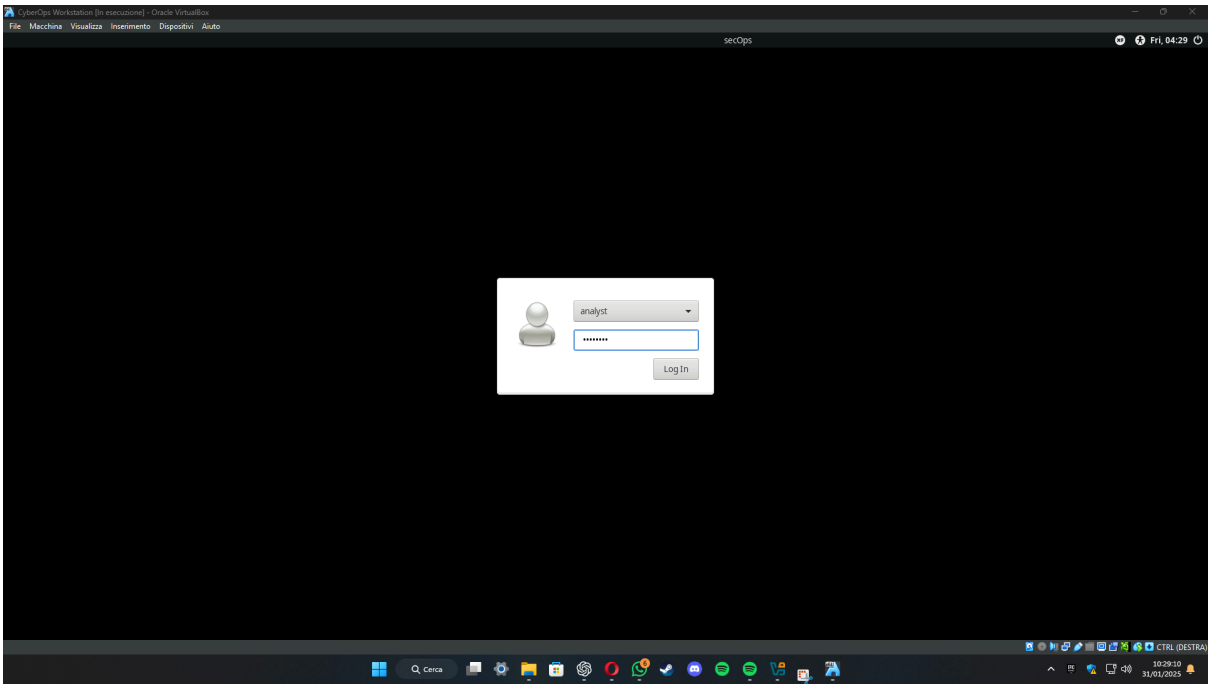


Infine ho utilizzato clear-recyclebin per la pulizia del cestino presente nel desktop



Utilizzo di Wireshark per Esaminare il Traffico HTTP e HTTPS

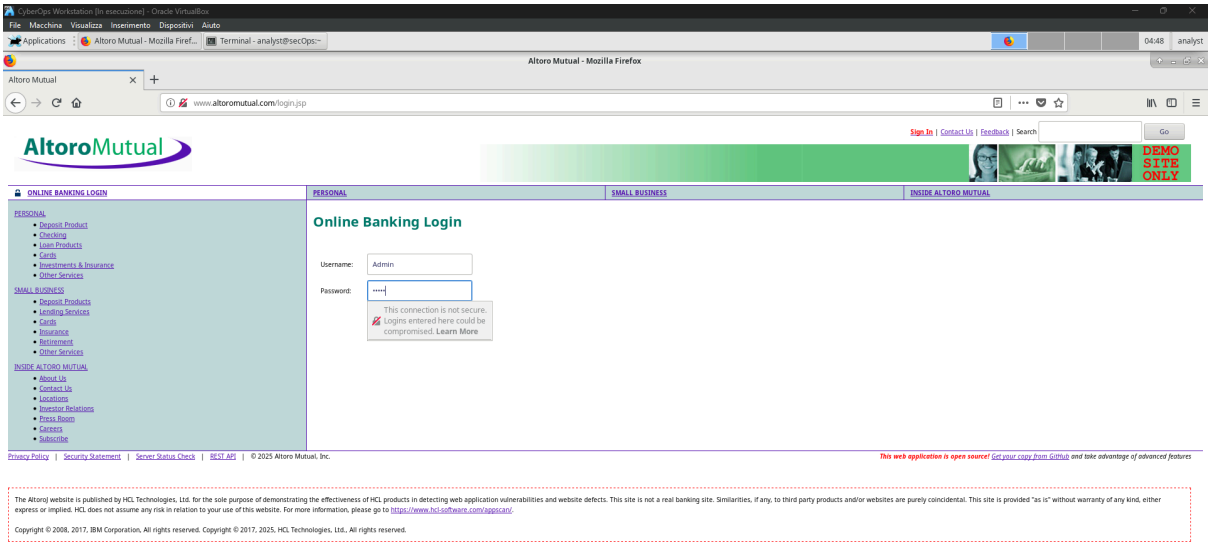
Sono entrato nella VM con la password:cyberops

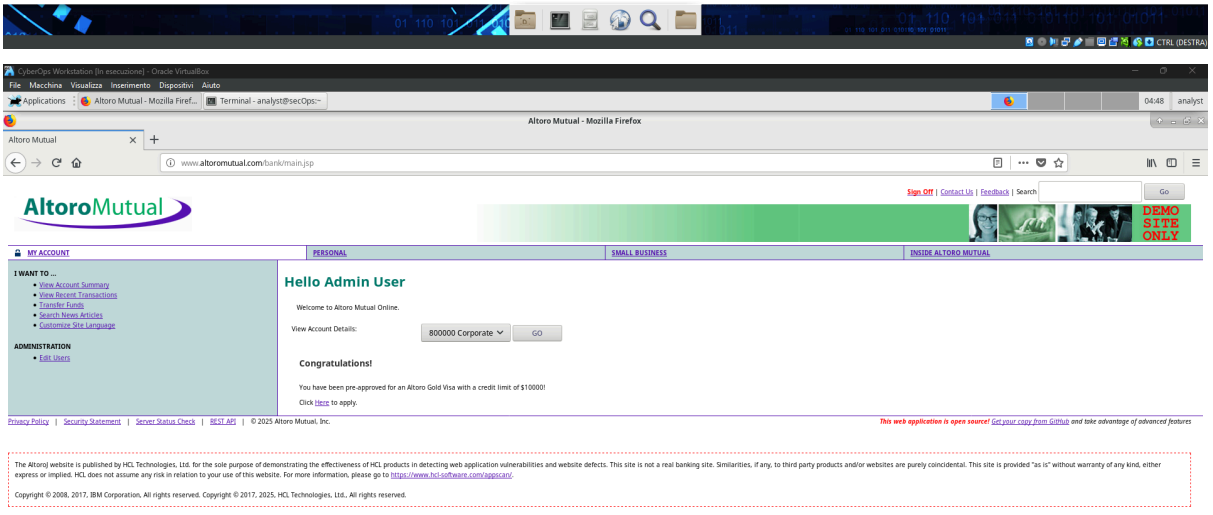


Successivamente ho aperto il terminale e ho prima visto le schede di rete attive e poi ho avviato tcpdump per analizzare il traffico HTTP con -i per specificare l'interfaccia di rete -s specifica la lunghezza dell'istantanea per ogni pacchetto 0= 262144 ed infine -w per scrivere il risultato in un file

```
[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 08:00:27:19:12:44 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 86055sec preferred_lft 86055sec
    inet6 fd00::a00:27ff:fe19:1244/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 86055sec preferred_lft 14055sec
    inet6 fe80::a00:27ff:fe19:1244/64 scope link
       valid_lft forever preferred_lft forever
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Sono andato sul sito indicato nella guida inserendo come username Admin e password Admin

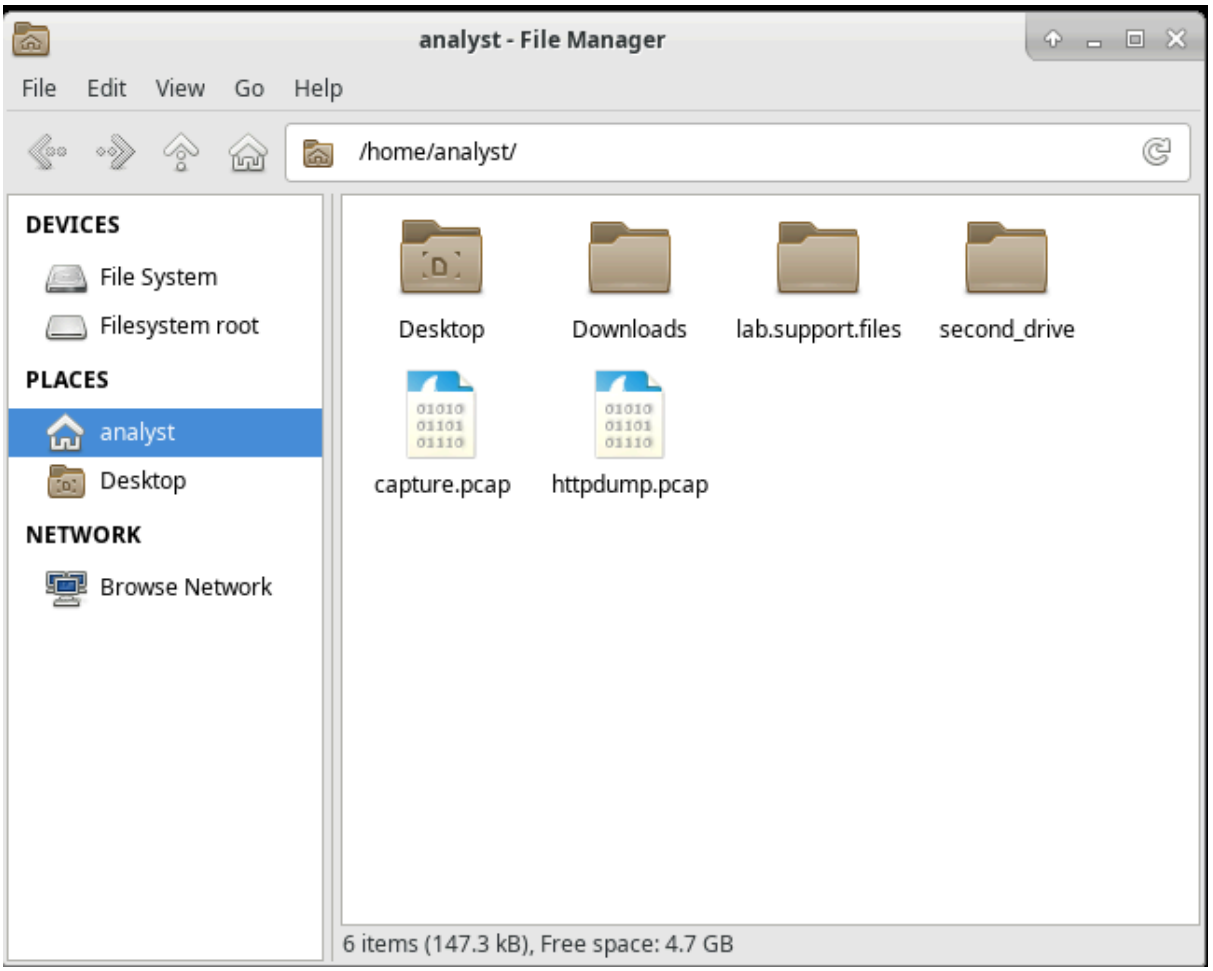




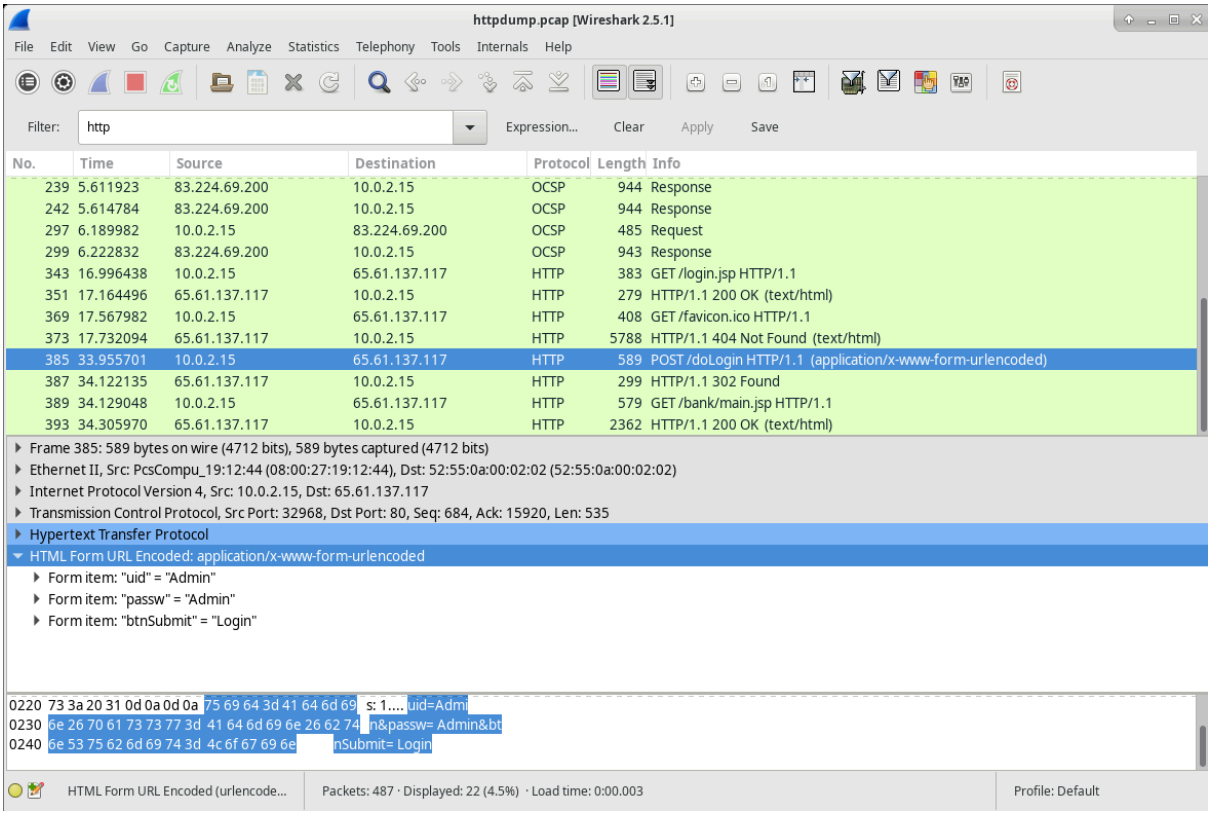
Successivamente ho chiuso la pagina web e con control+C ho fermato il listening del tcpdump

```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C487 packets captured
487 packets received by filter
0 packets dropped by kernel
[analyst@secOps ~]$
```

Mi ha salvato il file httpdump.pcap



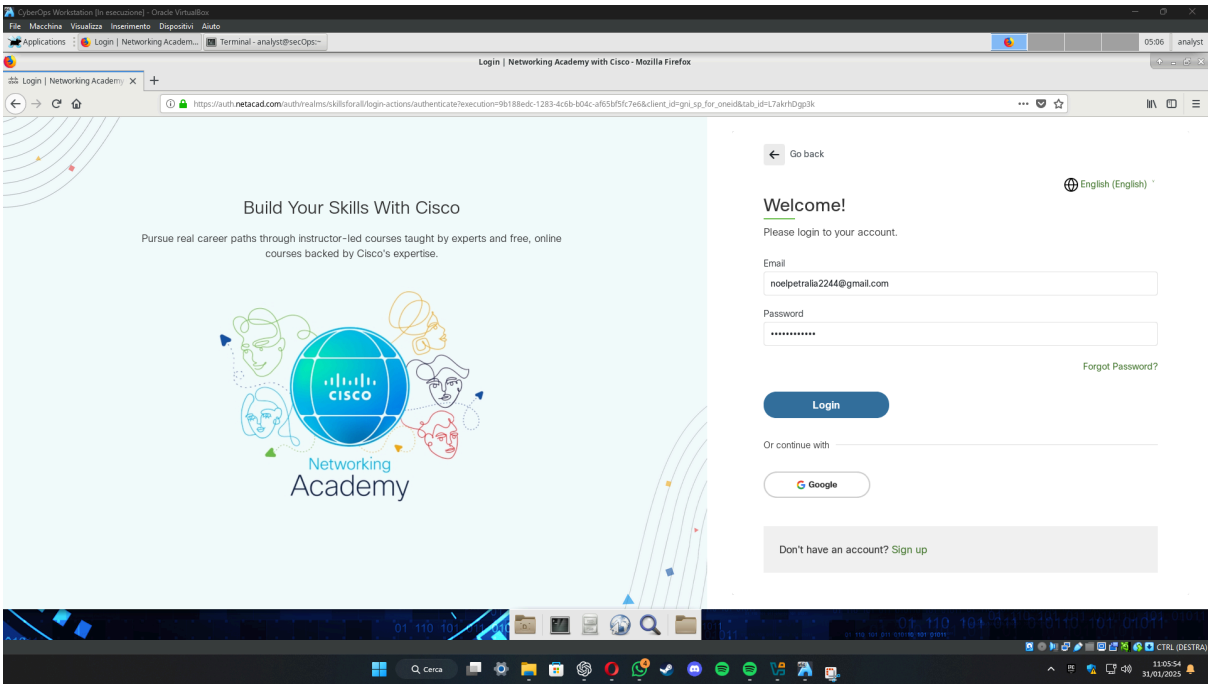
Ho Inserito come filtro http in modo che mi facesse vedere solo i protocolli http successivamente ho cercato il Post e da come si vede dall'immagine si vedono le credenziali inserite questo ci indica quanto è facile vedere le credenziali inserite per un attaccante per quanto riguarda il protocollo HTTP



Ho utilizzato lo stesso comando di prima ma cambiando nome del file perche questa volta dobbiamo analizzare il protocollo HTTPS

```
[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
```

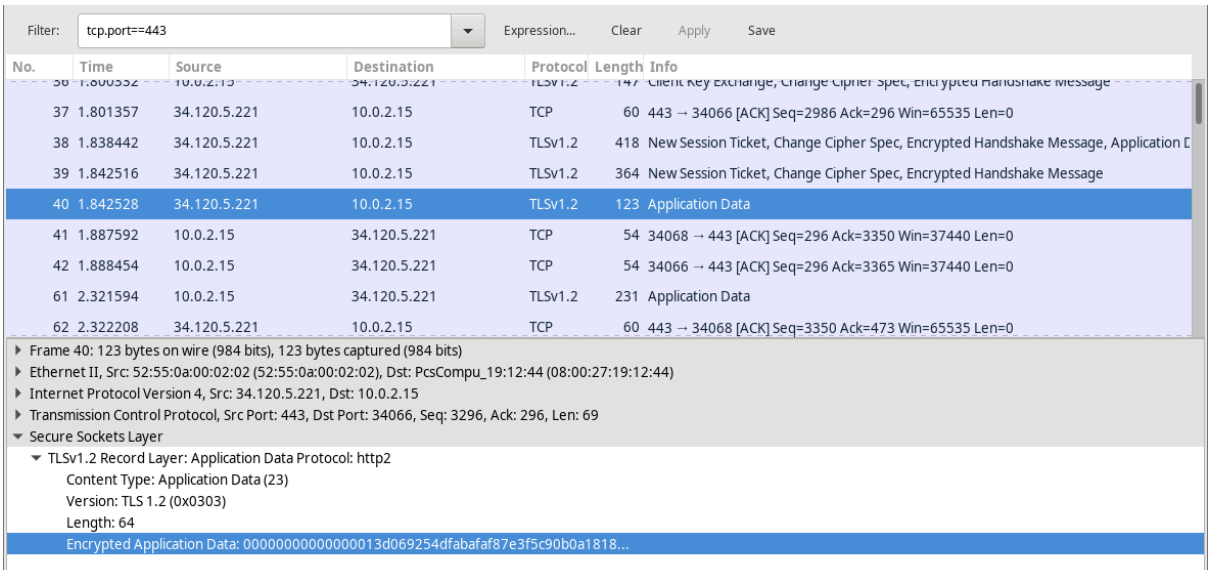
Sono andato sul sito suggerito dalla guida, poi su log in, collegandomi con le mie credenziali



Ho fatto lo stesso procedimento di prima ovvero chiudere la pagina web e stoppare il listening con control+c

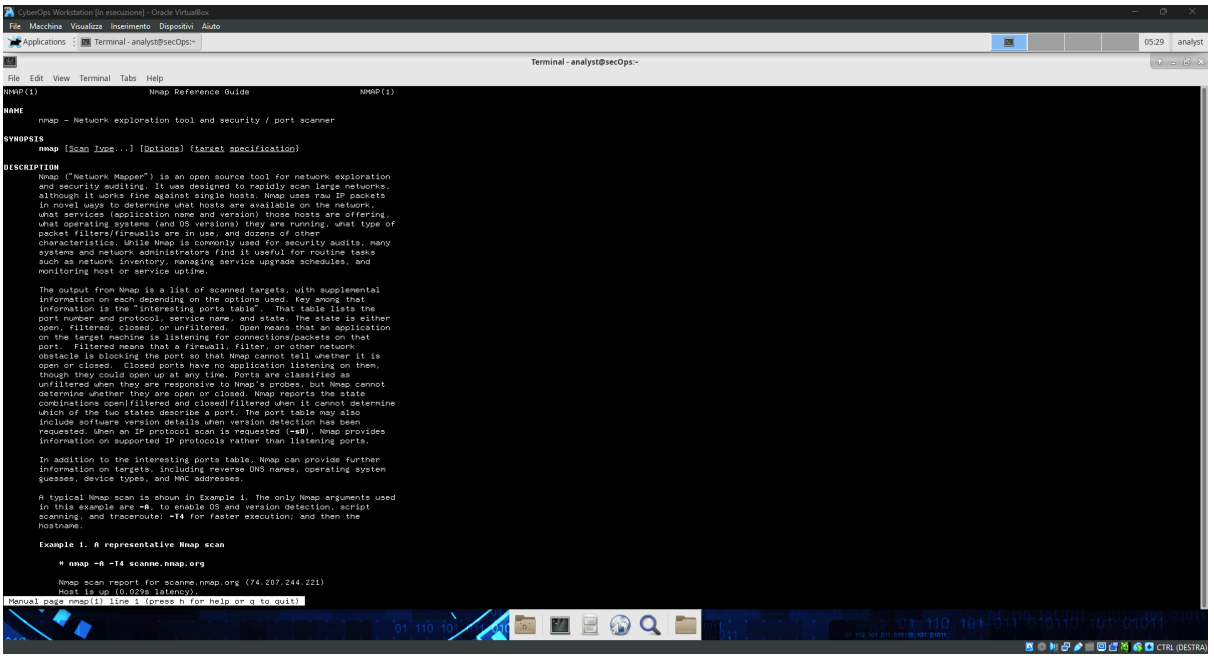
```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C5882 packets captured
5882 packets received by filter
0 packets dropped by kernel
```

Ho filtrato la porta 443 ovvero HTTPS analizzando Application Data analizzando che utilizza un protocollo di sicurezza TLSv1.2 che non permette di visualizzare le credenziali come si vede da foto il messaggio è criptato



Bonus 1 Esplorazione di Nmap

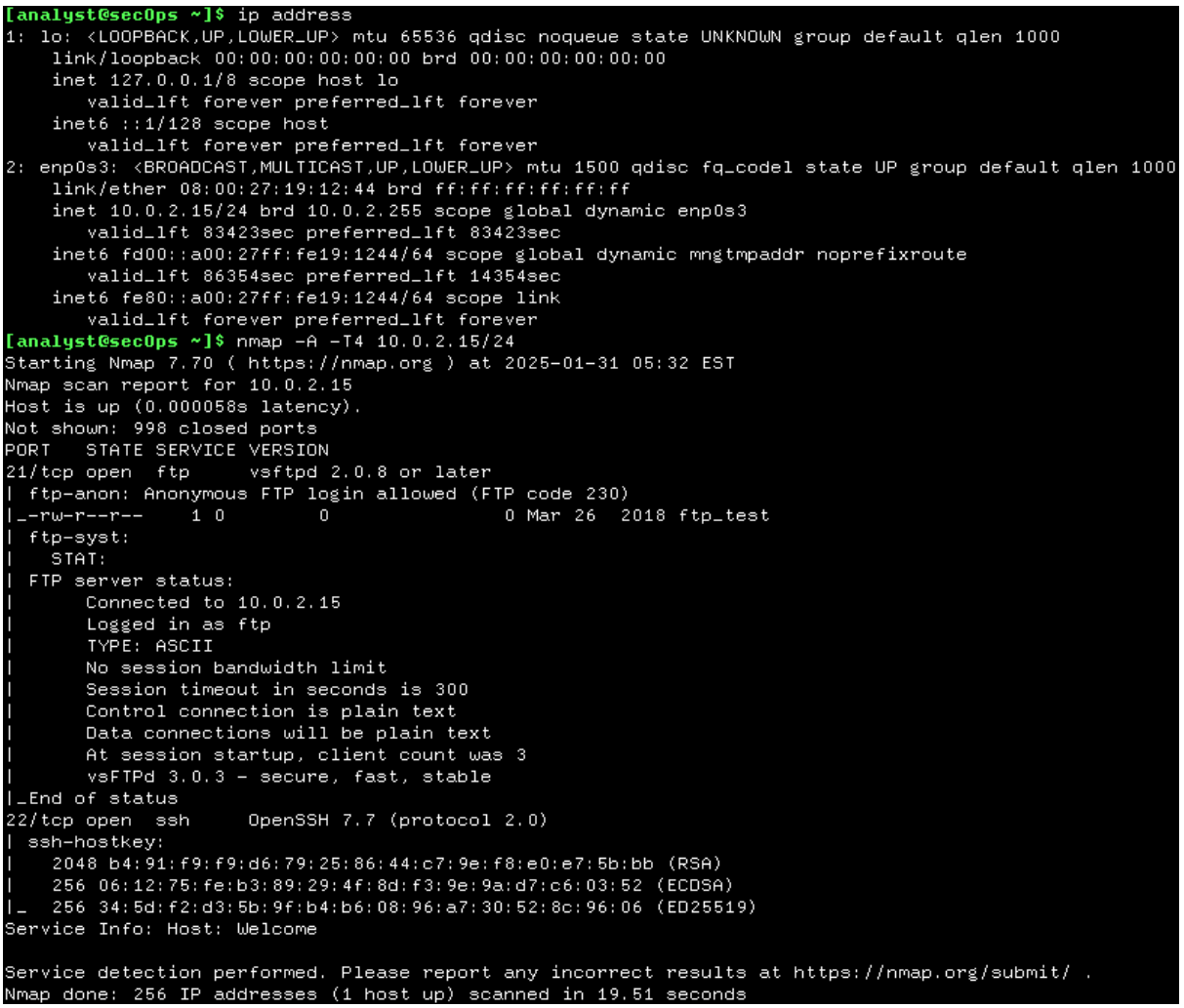
Sono entrato nel terminale e ho digitato man nmap che mi forniva una guida e mi indicava cosa facesse il comando nmap



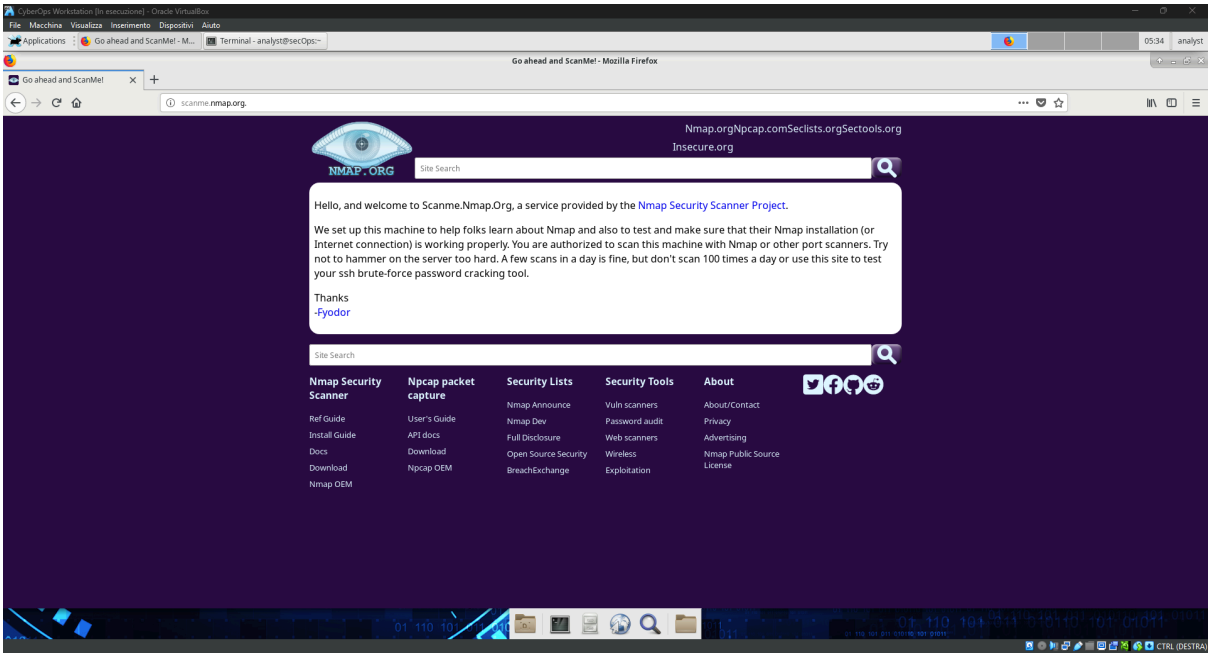
Ho avviato una scansione localhost analizzando le due porte aperte ovvero 21 ftp con la sua versione e 22 ssh con la relativa versione

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-01-31 05:30 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000062s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0               0 Mar 26  2018 ftp_test
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 127.0.0.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 b4:91:f9: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 12.03 seconds
```

Per prima cosa ho visualizzato l'indirizzo ip della mia scheda di rete con il prefisso ovvero 10.0.2.15/24; successivamente ho avviato una scansione della mia scheda di rete utilizzando l'indirizzo ip menzionato precedentemente e ho osservato che mi dava le stesse impostazioni di porta aperte uguali a quelli della prima scansione effettuata



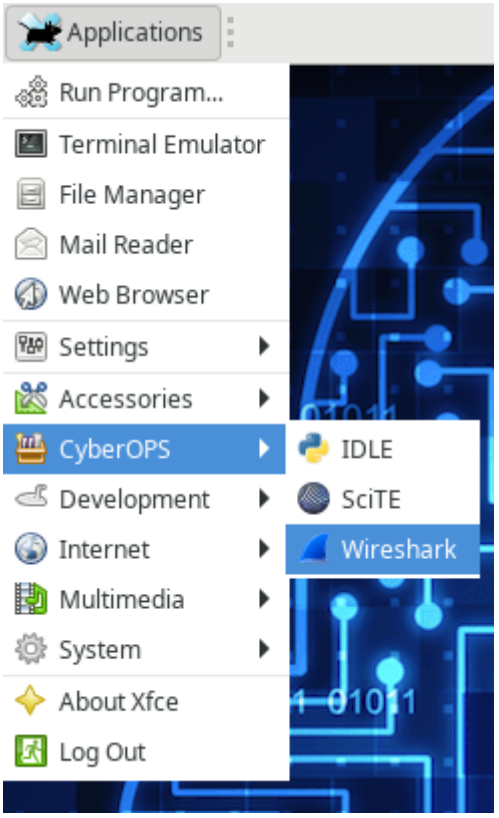
Successivamente seguendo la guida sono andato nel sito **scanme.nmap.org** che permette agli utenti di conoscere Nmap e testare la loro installazione di Nmap



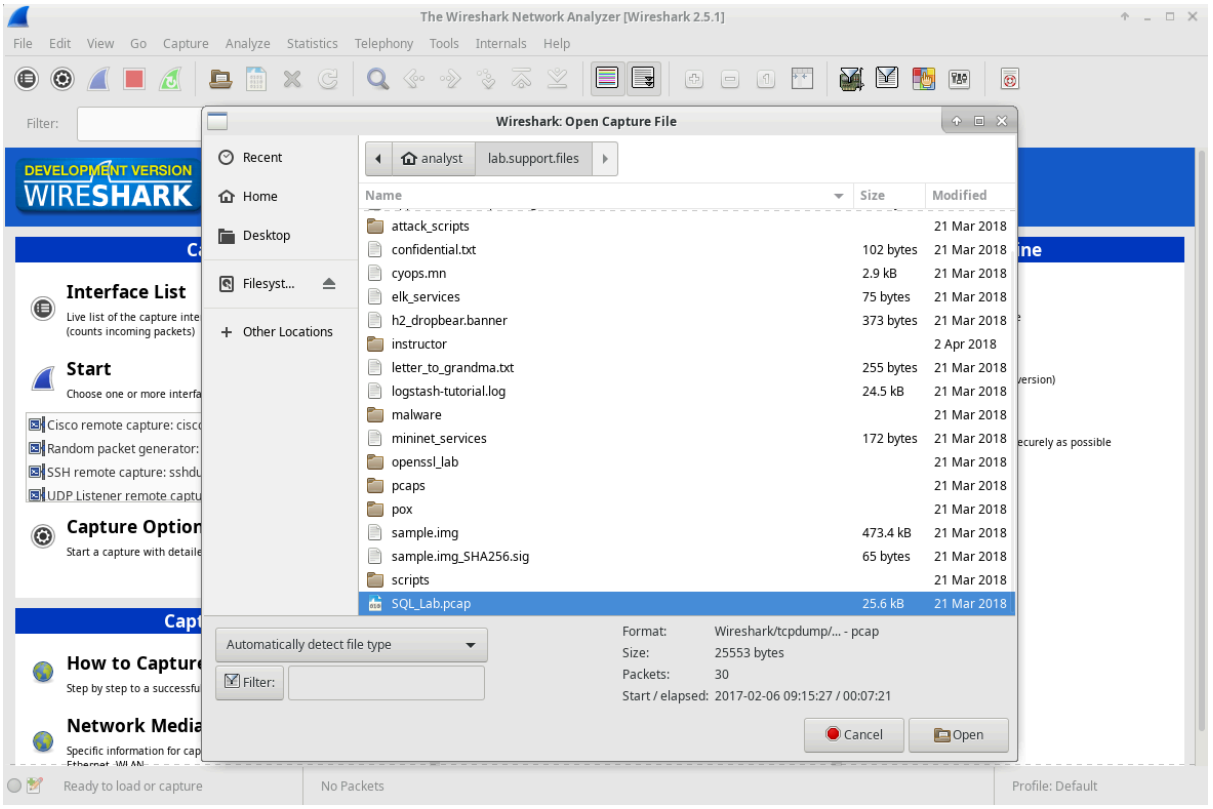
In fine ho avviato una scansione del sito web menzionato prima e dalla scansione ho analizzato le seguenti porte aperte: 22 ssh con la relativa versione, 53 domain con la relativa versione ed in fine 80 http con la relativa versione.

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2025-01-31 05:34 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.19s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 filtered ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
53/tcp   open  domain     dnsmasq 2.84
| dns-nsid:
|_  bind.version: dnsmasq-2.84
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
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 29.98 seconds
```

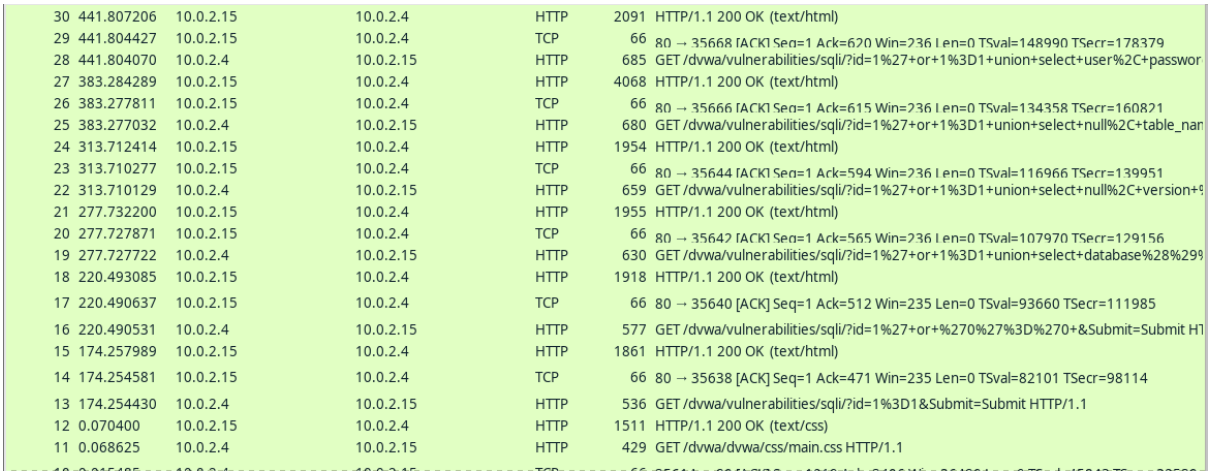
Bonus 2 Attacco a un Database MySQL



Ho cercato il file in questione che diceva la guida

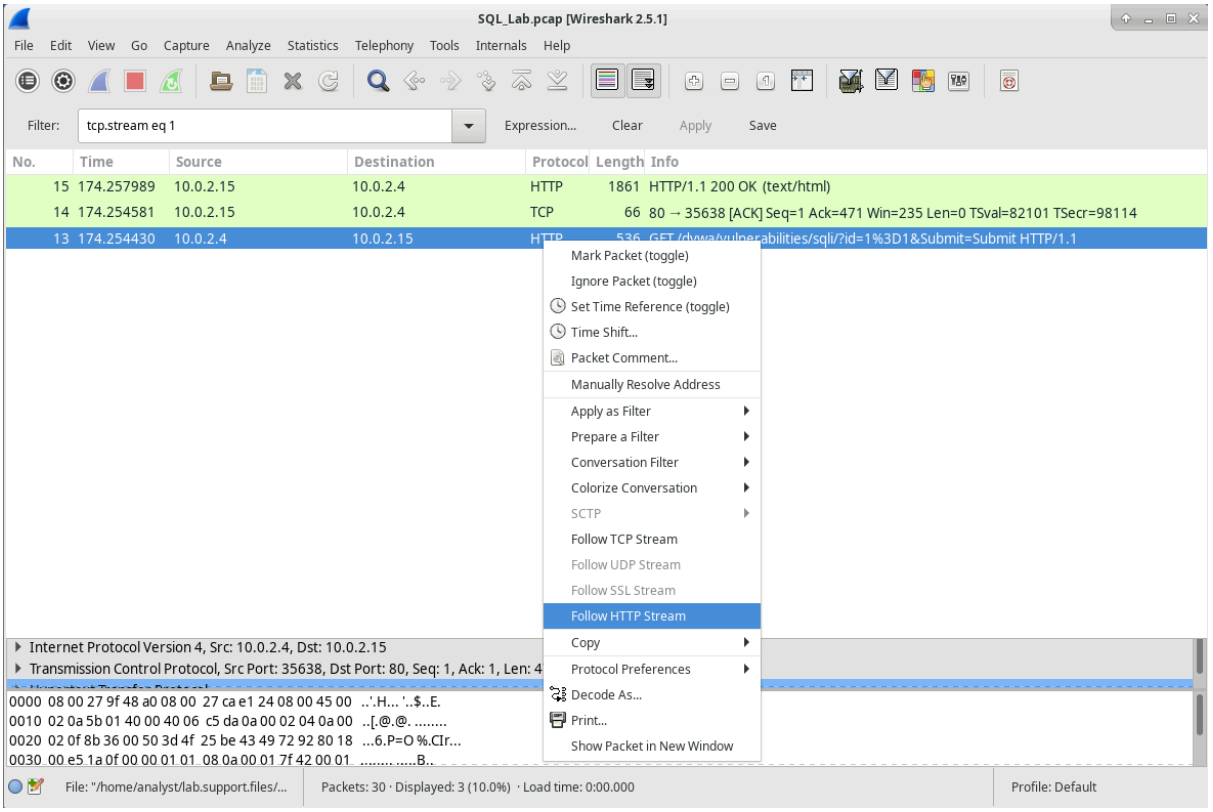


Dalla chiamata 30 ovvero l'ultima si può analizzare che la scansione è durata 441 secondi all'incirca 8 minuti e oltre il tempo si possono vedere i due indirizzi ip coinvolti

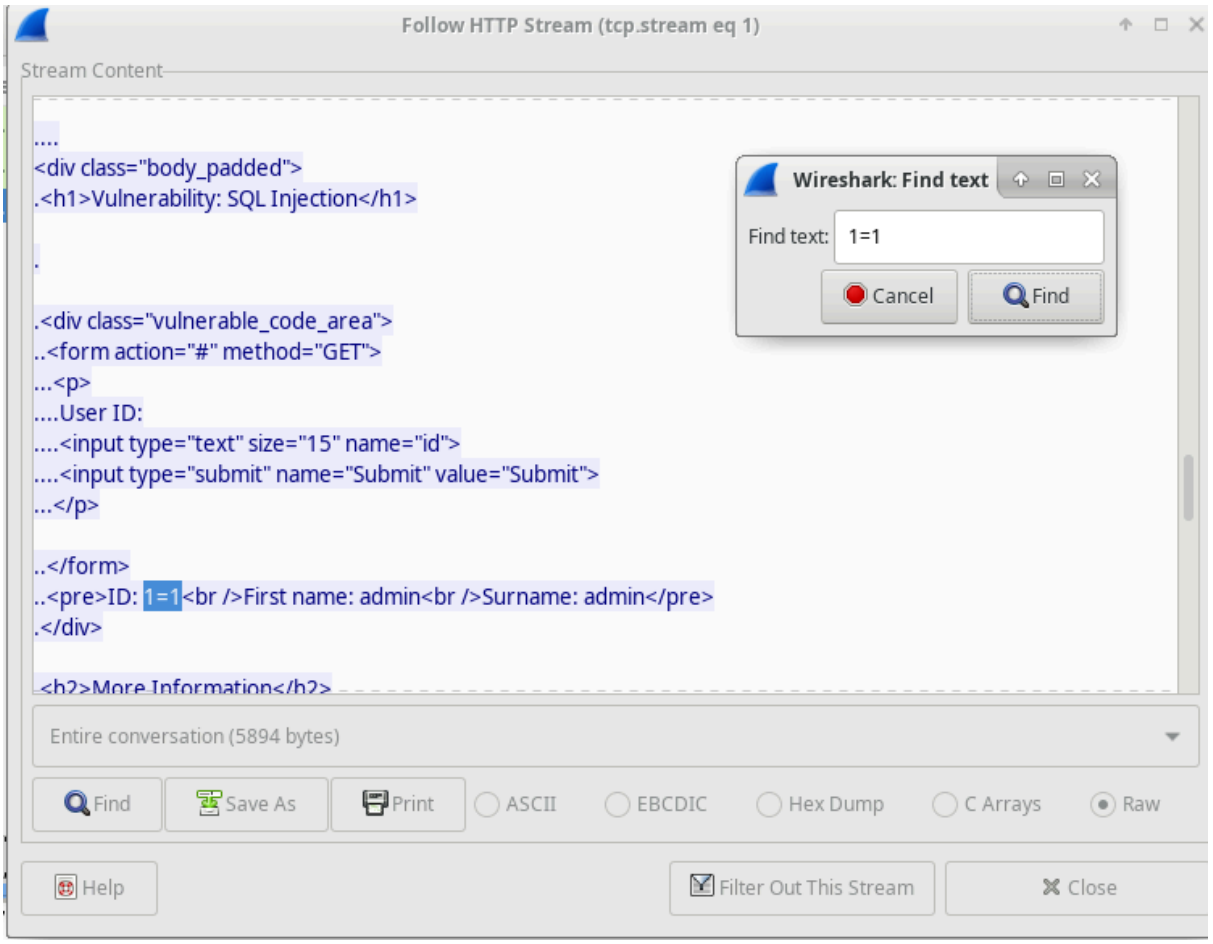


30	441.807206	10.0.2.15	10.0.2.4	HTTP	2091	HTTP/1.1 200 OK (text/html)
29	441.804427	10.0.2.15	10.0.2.4	TCP	66	80 → 35668 [ACK] Seq=1 Ack=620 Win=236 Len=0 TSval=148990 TSecr=178379
28	441.804070	10.0.2.4	10.0.2.15	HTTP	685	GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+user%2C+passwor
27	383.284289	10.0.2.15	10.0.2.4	HTTP	4068	HTTP/1.1 200 OK (text/html)
26	383.277811	10.0.2.15	10.0.2.4	TCP	66	80 → 35666 [ACK] Seq=1 Ack=615 Win=236 Len=0 TSval=134358 TSecr=160821
25	383.277032	10.0.2.4	10.0.2.15	HTTP	680	GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+null%2C+table_nar
24	313.712414	10.0.2.15	10.0.2.4	HTTP	1954	HTTP/1.1 200 OK (text/html)
23	313.710277	10.0.2.15	10.0.2.4	TCP	66	80 → 35644 [ACK] Seq=1 Ack=594 Win=236 Len=0 TSval=116966 TSecr=139951
22	313.710129	10.0.2.4	10.0.2.15	HTTP	659	GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+null%2C+version+%
21	277.732200	10.0.2.15	10.0.2.4	HTTP	1955	HTTP/1.1 200 OK (text/html)
20	277.727871	10.0.2.15	10.0.2.4	TCP	66	80 → 35642 [ACK] Seq=1 Ack=565 Win=236 Len=0 TSval=107970 TSecr=129156
19	277.727722	10.0.2.4	10.0.2.15	HTTP	630	GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+database%28%29%
18	220.493085	10.0.2.15	10.0.2.4	HTTP	1918	HTTP/1.1 200 OK (text/html)
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
16	220.490531	10.0.2.4	10.0.2.15	HTTP	577	GET /dvwa/vulnerabilities/sqli/?id=1%27+or+%270%27%3D%270+&Submit=Submit HT
15	174.257989	10.0.2.15	10.0.2.4	HTTP	1861	HTTP/1.1 200 OK (text/html)
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
13	174.254430	10.0.2.4	10.0.2.15	HTTP	536	GET /dvwa/vulnerabilities/sqli/?id=1%3D1&Submit=Submit HTTP/1.1
12	0.070400	10.0.2.15	10.0.2.4	HTTP	1511	HTTP/1.1 200 OK (text/css)
11	0.068625	10.0.2.4	10.0.2.15	HTTP	429	GET /dvwa/dvwa/css/main.css HTTP/1.1

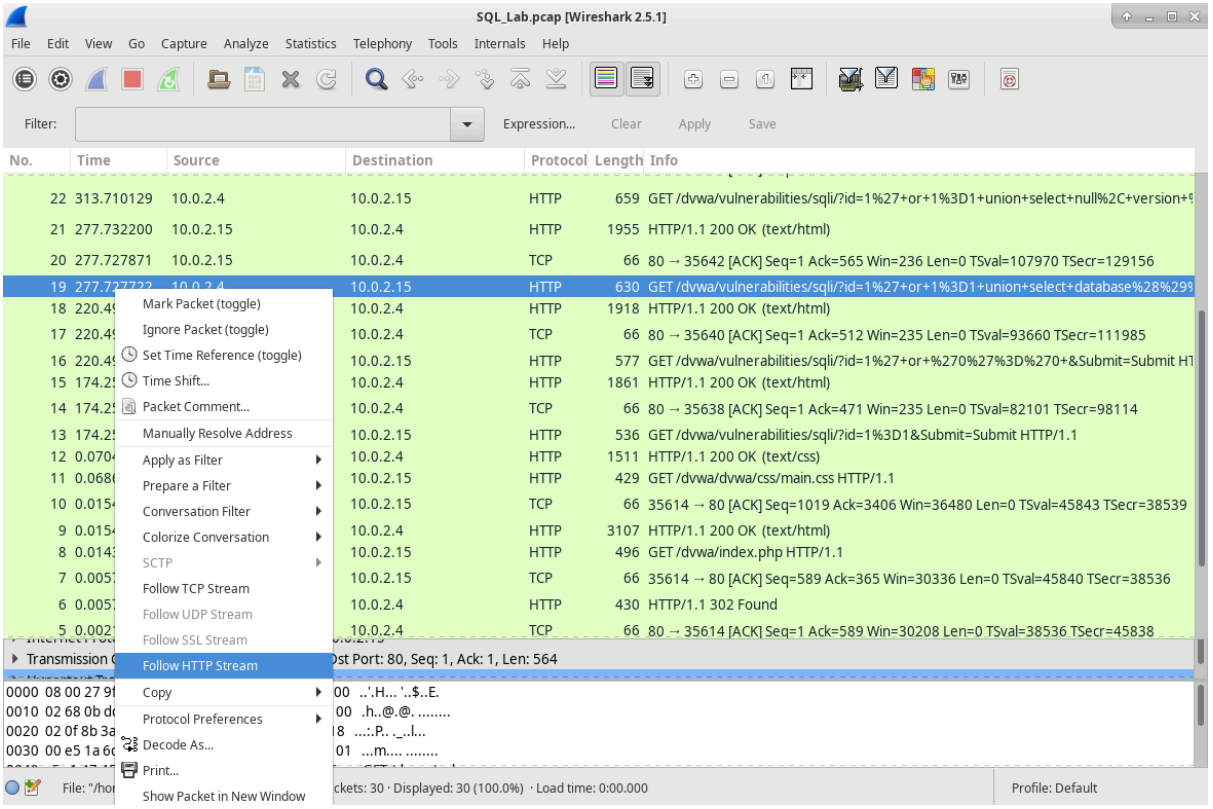
Ho analizzato per prima cosa la chiamata 13 andando su Follow HTTP Stream



premendo su find ho inserito il comando 1=1; L'attaccante ha inserito la query **(1=1)** in un campo di ricerca UserID sul target **10.0.2.15** per verificare se l'applicazione è vulnerabile a **SQL Injection** e lo è

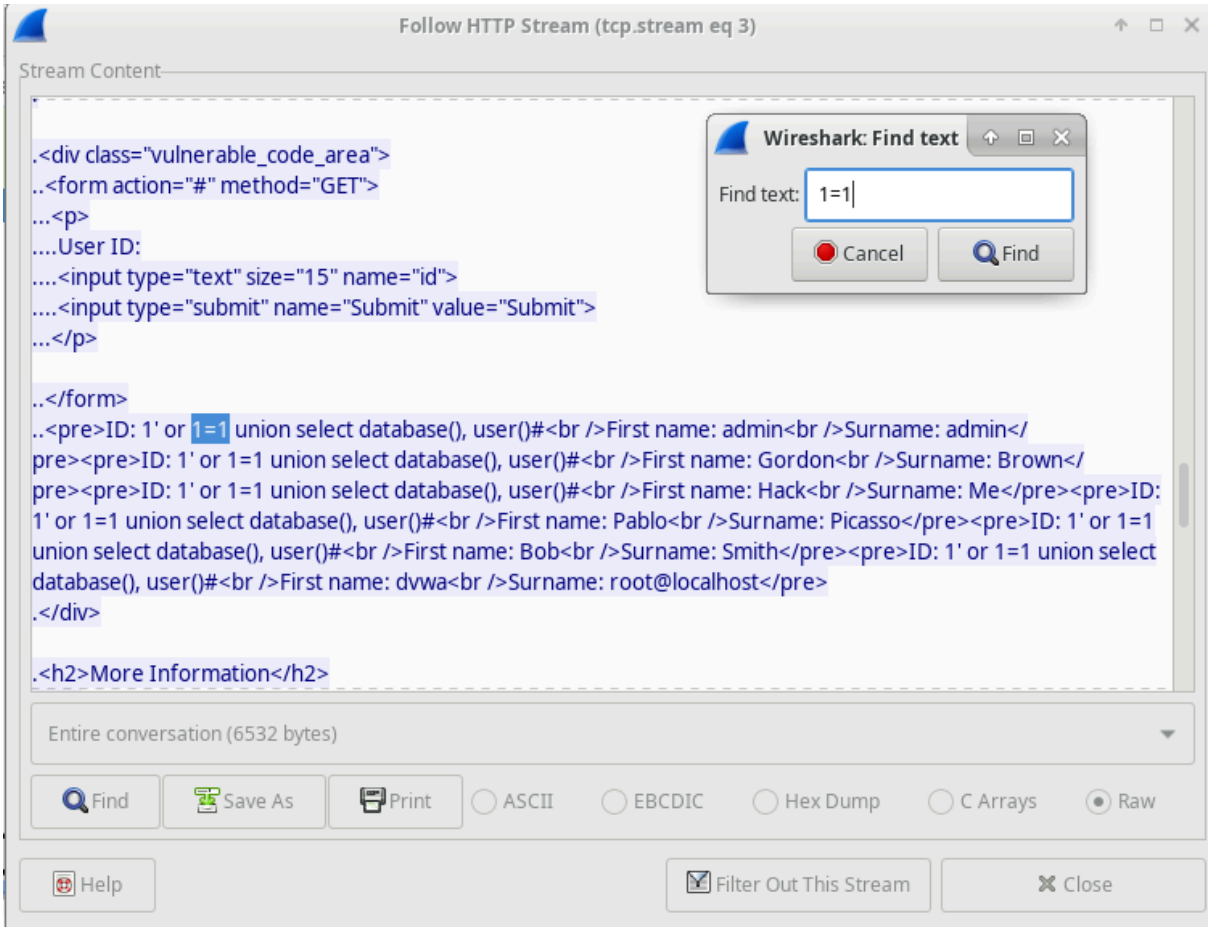


Ho utilizzato lo stesso procedimento di prima per il canale 19

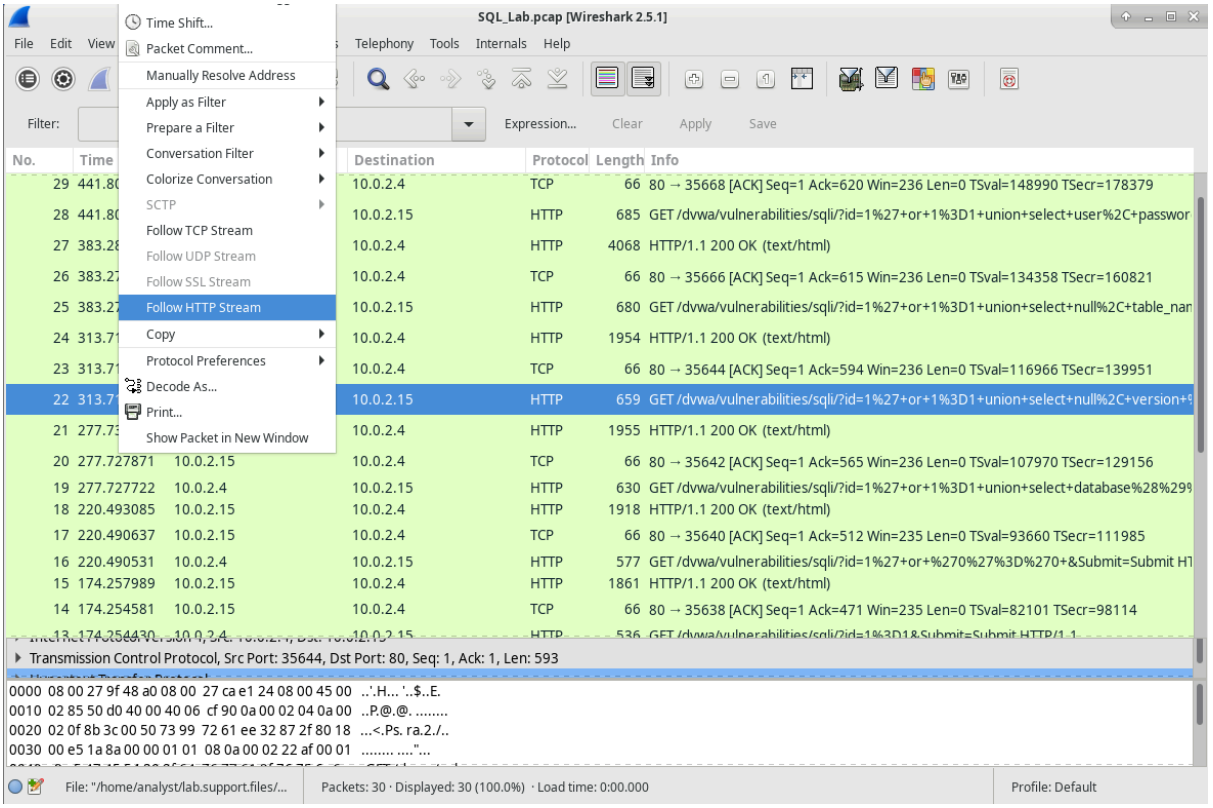


Utilizzando sempre lo stesso comando questa volta nel canale 19 osservando che Il nome del database è **dvwa** e l'utente del database è **root@localhost**. Inoltre, vengono visualizzati più account utente.

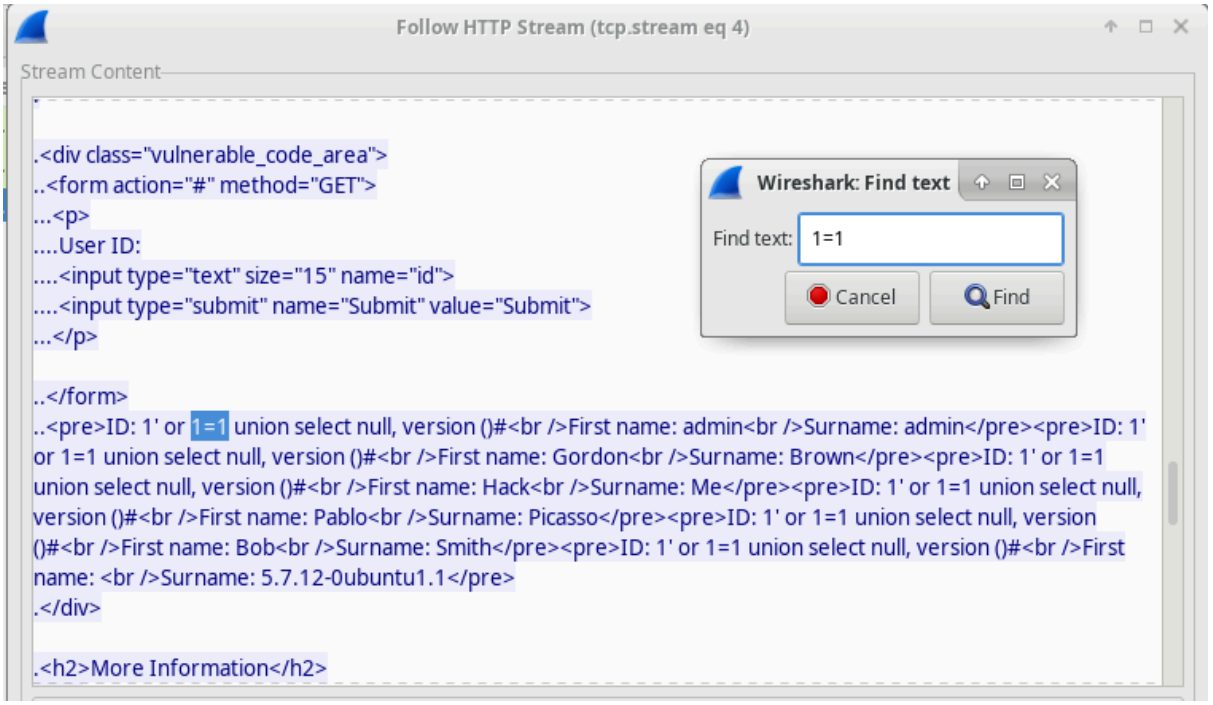
- **Questo indica che l'attacco SQL Injection ha avuto successo**, consentendo all'attaccante di ottenere informazioni sensibili dal database.



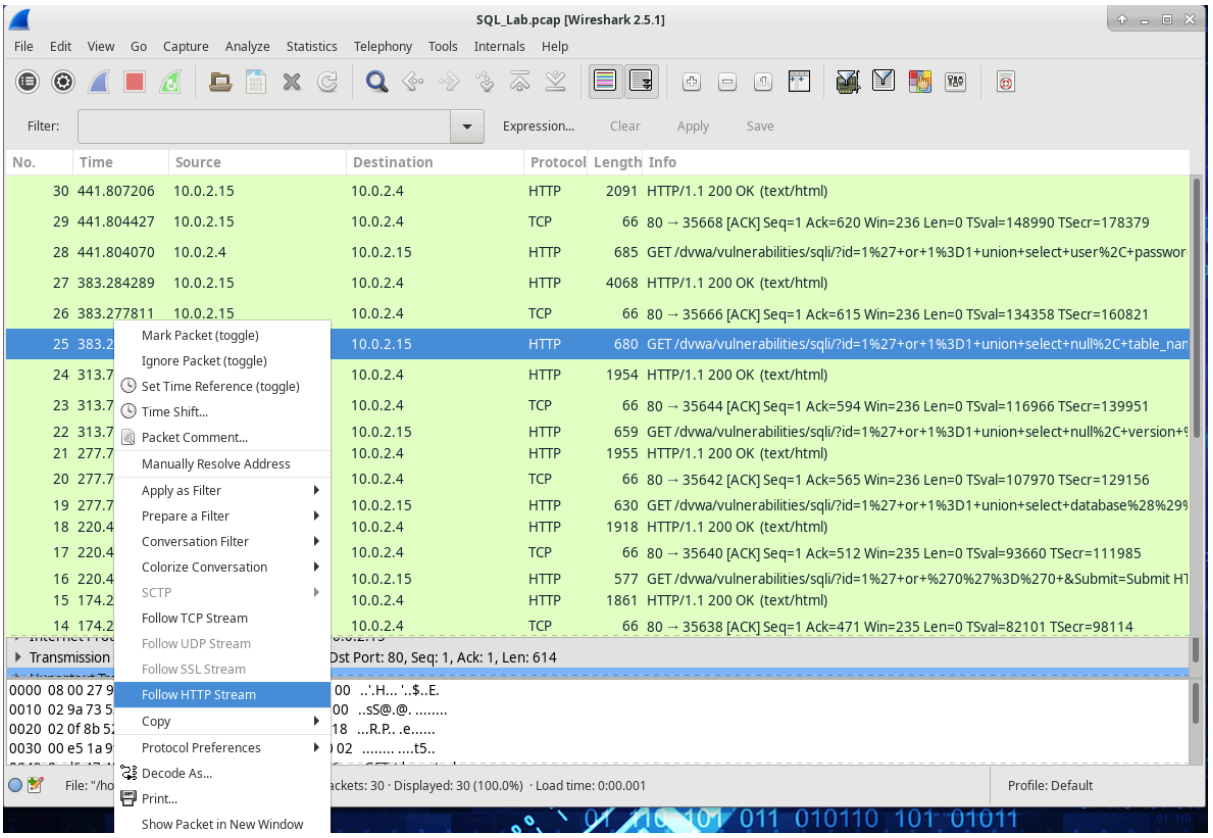
Stesso procedimento per il canale 22



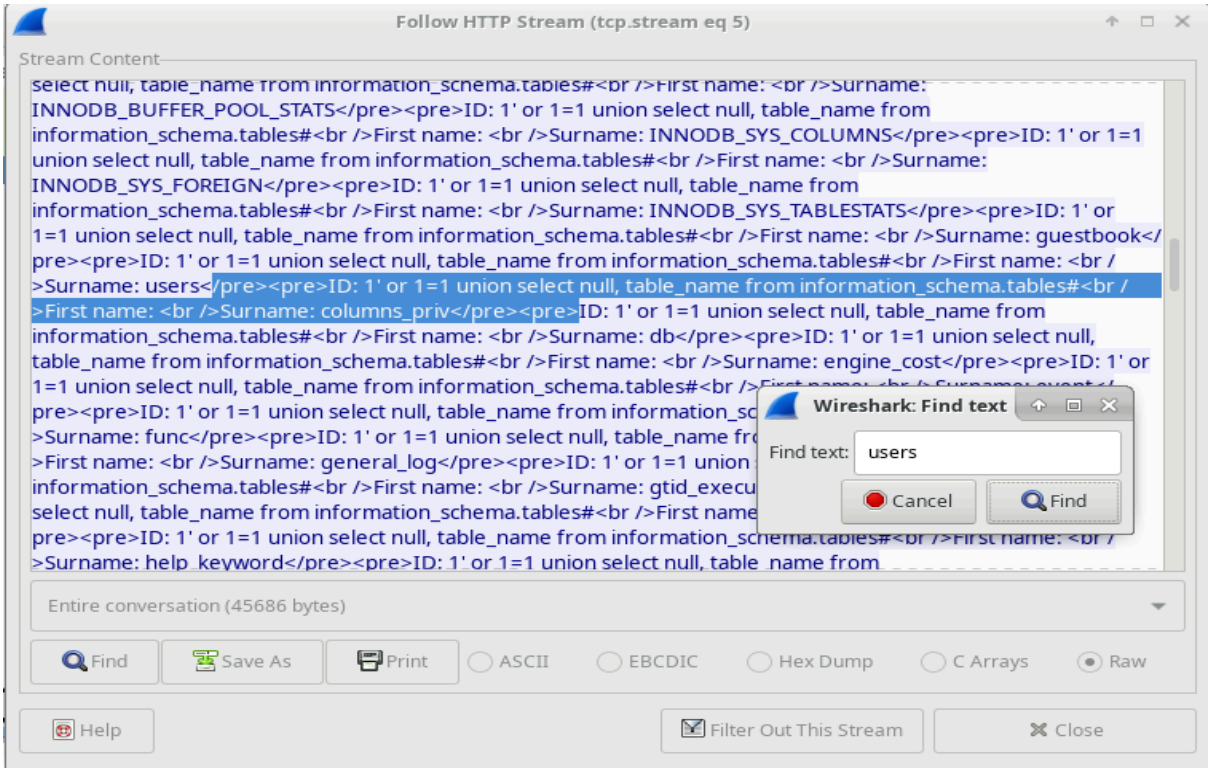
Utilizzando sempre lo stesso comando sono riuscito a trovare la versione del database ovvero **MySQL 5.7.12-0**



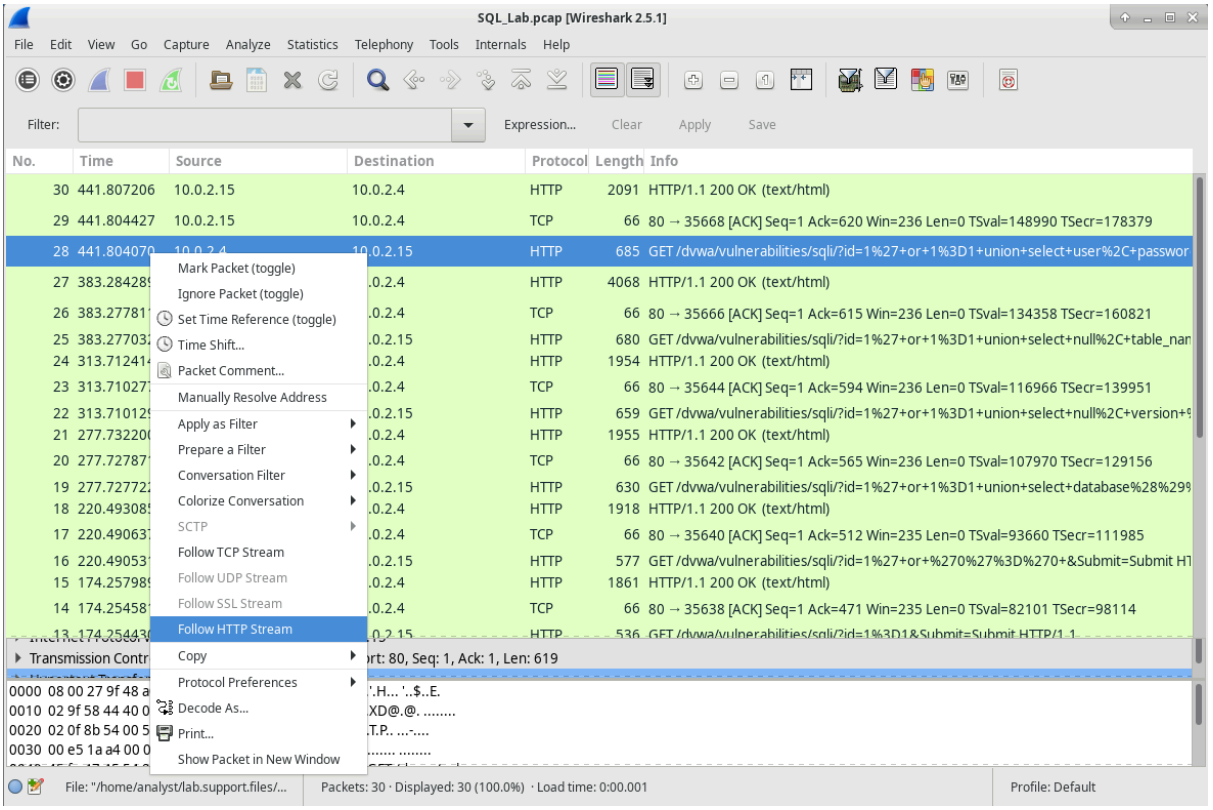
Stesso procedimento per il canale 25



Questa volta ho dato il comando users la quale mi ha indicato in quale posizione troviamo users



Stesso procedimento canale 28



Questa volta ritorno al comando 1=1 che mi ha permesso di visualizzare gli utenti e le password in formato hash, ma utilizzando https://crackstation.net/ che ci permette di visualizzare le password da un formato hash ad un formato leggibile.