

**RELAZIONE**  
**RITISH BHANTOOA**

## **INDICE:**

- 1. INTRODUZIONE AGLI ESERCIZI**
- 2. WINDOWS POWERSHELL**
- 3. WIRESHARK**
- 4. NMAP**
- 5. MYSQL**
- 6. CONCLUSIONI**

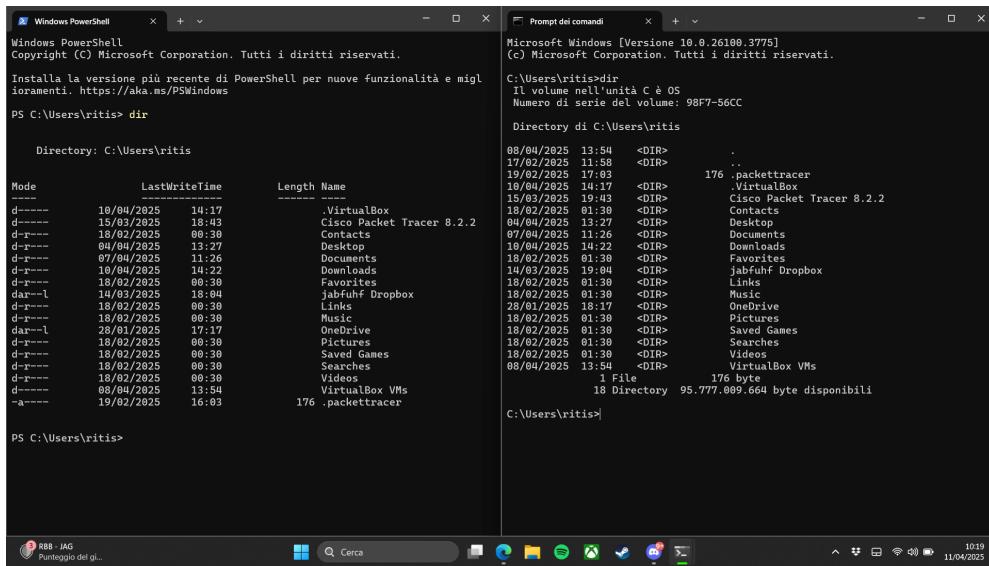
### **1. INTRODUZIONE AGLI ESERCIZI**

L'esercizio di oggi richiedeva i seguenti punti

- L'utilizzo di **Windows Powershell**
- L'analisi di pacchetti HTTP e HTTPS tramite **Wireshark**
- Scansione delle porte tramite **NMAP**
- Attacco a un database **MySQL** e analisi dei pacchetti **PCAP**

## 2. WINDOWS POWERSHELL

- Prima di tutto accediamo alla **Powershell** e al **Prompt dei comandi** di Windows, cercandoli una volta cliccato il pulsante **Start**, successivamente inseriamo il comando **dir** in entrambe le finestre, ci verrà visualizzato un elenco di sottodirectory, file e informazioni.



The screenshot shows two side-by-side command-line windows on a Windows desktop. The left window is titled 'Windows PowerShell' and the right is titled 'Prompt dei comandi'. Both show the output of the 'dir' command in the C:\Users\ritis\ directory. The output lists various files and folders with their names, last write times, and sizes. The 'Prompt dei comandi' window also displays system information like the volume name (C) and serial number.

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

Install la versione più recente di PowerShell per nuove funzionalità e miglioramenti. https://aka.ms/PSWindows
PS C:\Users\ritis> dir

Directory: C:\Users\ritis

Mode LastWriteTime      Length Name
---- -            -           -
d----- 18/04/2025 14:17          .VirtualBox
d----- 15/03/2025 18:43          Cisco Packet Tracer 8.2.2
d----- 18/02/2025 00:30          Contacts
d----- 04/04/2025 13:27          Desktop
d----- 07/04/2025 11:26          Documents
d----- 10/04/2025 15:22          Downloads
d----- 18/02/2025 00:30          Favorites
dar---l 14/03/2025 18:04          jabfuH Dropbox
d----- 18/02/2025 00:30          Links
d----- 18/02/2025 00:30          Music
d----- 18/02/2025 00:30          Pictures
d----- 18/02/2025 00:30          Saved Games
d----- 18/02/2025 00:30          Saved Videos
d----- 18/02/2025 00:30          Videos
d----- 08/04/2025 13:54          VirtualBox VMs
-a----  19/02/2025 16:03          176 .packettracer

C:\Users\ritis>

Microsoft Windows [Versione 10.0.26100.3775]
(c) Microsoft Corporation. Tutti i diritti riservati.

C:\Users\ritis>dir
Il volume nell'unità C è OS
Numero di serie del volume: 98F7-56CC

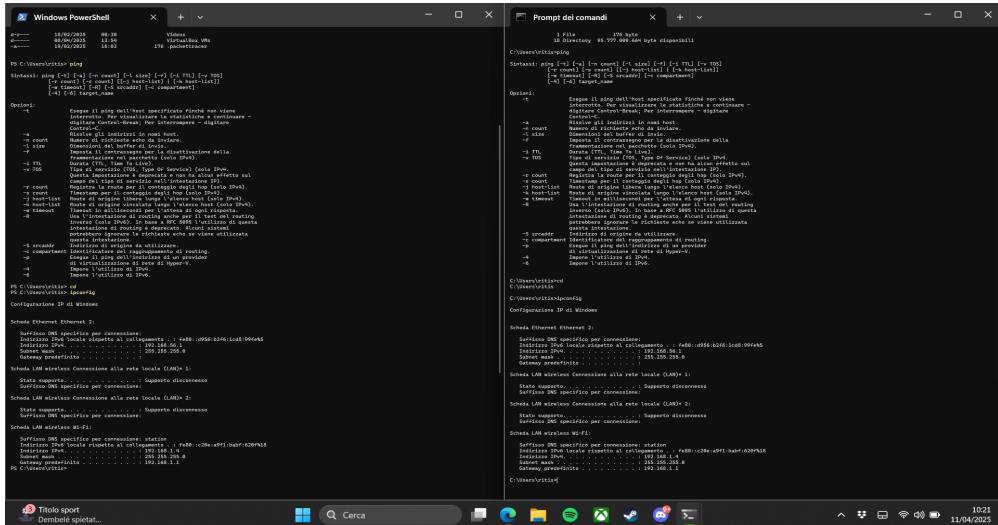
Directory di C:\Users\ritis

08/04/2025 13:54 <DIR> .
17/02/2025 11:58 <DIR> ..
18/02/2025 10:17 <DIR> .VirtualBox
15/03/2025 19:43 <DIR> Cisco Packet Tracer 8.2.2
18/02/2025 01:39 <DIR> Contacts
04/04/2025 13:27 <DIR> Desktop
07/04/2025 11:26 <DIR> Documents
10/04/2025 14:22 <DIR> Downloads
18/02/2025 01:30 <DIR> Favorites
14/03/2025 15:00 <DIR> JabfuH Dropbox
18/02/2025 01:30 <DIR> Links
18/02/2025 01:39 <DIR> Music
28/01/2025 18:17 <DIR> OneDrive
18/02/2025 01:30 <DIR> Pictures
18/02/2025 01:30 <DIR> Saved Games
18/02/2025 01:30 <DIR> Saved Videos
08/04/2025 13:54 <DIR> VirtualBox VMs
          1 File          176 byte
          18 Directory 95.777.009.664 byte disponibili

C:\Users\ritis>
```

- In seguito ci viene chiesto di inserire in entrambe le finestre i

comandi **ping**, **cd**, **ipconfig**, entrambe le finestre ci daranno le stesse informazioni



- Adesso inseriamo il comando **Get-Alias dir** nel prompt di PowerShell

```
PS C:\Users\ritis> get-alias dir
CommandType      Name
-----          -----
Alias           dir -> Get-ChildItem
```

Un cmdlet è un comando in Microsoft PowerShell progettato per eseguire un compito specifico. I cmdlet sono generalmente parte di moduli PowerShell e sono scritti in .NET. Ogni cmdlet segue uno schema di denominazione "verbo-sostantivo", il che rende facile capirne la funzione. Ecco alcuni esempi:

- **Get-Process**: Ottiene informazioni sui processi attualmente in esecuzione.
- **Set-Item**: Modifica il valore di un elemento nel file system o nel registro.
- **Get-Service**: Ottiene lo stato dei servizi registrati nel sistema.

I cmdlet possono essere richiamati dalla console PowerShell o utilizzati all'interno di script per automatizzare compiti amministrativi. Ci sono migliaia di cmdlet disponibili in PowerShell, il che consente agli utenti di eseguire una vasta gamma di operazioni di amministrazione e gestione di sistema.

- Inseriamo il comando **netstat -h** netstat per visualizzare le opzioni

## disponibili per questo comando sulla PowerShell

```
PS C:\Users\ritis> netstat -h netstat
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 TCP o UDP porte attualmente utilizzate.
-d Mostra il valore DSCP associato a ogni connessione.
-e Mostra le statistiche Ethernet. Potrebbe essere in combinazione con l'opzione -s.
-f Mostra Fully Qualified Domain Names (FQDN) per gli indirizzi stranieri.
-i Mostra il tempo in cui una connessione TCP si trova nel suo stato corrente.
-n Mostra i numeri di indirizzi e porte in formato numerico.
-o Mostra l'ID processo di proprietà associato a ogni connessione.
-p proto Mostra le connessioni per il protocollo specificato dal protocollo; il protocollo può essere: TCP, UDP, TCPv6 o UDPv6. Se usato con l'opzione -s per mostrare le statistiche per protocollo, il protocollo potrebbe essere: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
-q Mostra tutte le connessioni, le porte di ascolto e le porte TCP non di ascolto associate. Le porte non di ascolto associate potrebbero essere associate a meno di una connessione attiva.
-r Mostra la tabella di routing.
-s Mostra le statistiche per protocollo. Per impostazione predefinita, le statistiche vengono mostrate per IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP e UDPv6; l'opzione -p potrebbe essere usata per specificare un sottoinsieme dell'opzione predefinita.
-t Mostra lo stato di offload della connessione corrente.
-x Mostra connessioni NetworkDirect, listener ed endpoint condivisi.
-y Mostra il modello di connessione TCP per tutte le connessioni.
Non può essere in combinazione con altre opzioni.
interval Mostra di nuovo le statistiche selezionate, inserendo intervalli di secondi tra ogni visualizzazione. Premi CTRL+C per interrompere la nuova visualizzazione delle statistiche. Se omesso, netstat stamperà le informazioni sulla configurazione corrente una volta.
```

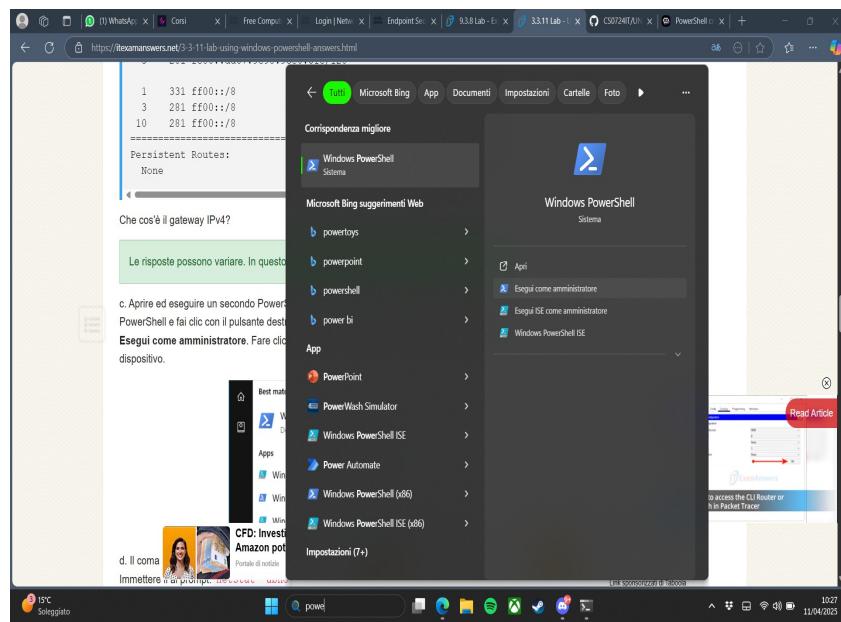
- Inseriamo, quindi, **netstat -r** per farci visualizzare la tabella di routing

```
PS C:\Users\ritis> netstat -r
=====
ELENCO INTERFAZI
5...0a 00 27 00 00 05 .....VirtualBox Host-Only Ethernet Adapter
17...96 bb 43 eb ed 33 .....Microsoft Wi-Fi Direct Virtual Adapter
3...d6 bb 43 eb ed 33 .....Microsoft Wi-Fi Direct Virtual Adapter #2
18...94 bb 43 eb ed 33 .....Realtek 8821CE Wireless LAN 802.11ac PCI-E NIC
1..... ....Software Loopback Interface 1
=====

IPV4 TABELLA ROUTE
=====
Route attive:
Indirizzo rete          Mask      Gateway    Interfaccia Metrica
          0.0.0.0        0.0.0.0   192.168.1.1  192.168.1.4    55
          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
          192.168.1.0     255.255.255.0  On-link     192.168.1.4    311
          192.168.1.4     255.255.255.255  On-link     192.168.1.4    311
          192.168.1.255   255.255.255.255  On-link     192.168.1.4    311
          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     192.168.1.4    311
          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     192.168.1.4    311
=====
Route permanenti:
Nessuna

IPV6 TABELLA ROUTE
=====
Route attive:
Interf. Metrica Rete Destinazione      Gateway
      1      331 ::1/128                On-link
      5      281 fe80::/64              On-link
     18      311 fe80::/64              On-link
     18      311 fe80::c20e:a9f1:babf:620f/128
                                         On-link
      5      281 fe80::d956:b2f6:1cd8:99fe/128
                                         On-link
      1      331 ff00::/8               On-link
      5      281 ff00::/8               On-link
     18      311 ff00::/8               On-link
=====
Route permanenti:
Nessuna
PS C:\Users\ritis>
```

- Adesso avviamo una Windows Powershell come amministratore



E inseriamo il comando **netstat -abno**, dopo poi aprireremo il **Task Manager**, dovremo passare sulla scheda **Dettagli**, fare clic su **PID**, così che ci vengano messi in ordine, e ricerca il PID che dice **servizio di rete**, che nel nostro caso è il **1764**.

Nome	PID	Stato	Nome utente	CPU	Memoria (x)	Architet.	Descr...
Interrupt sistema	-	In esec.	SYSTEM	00	0 K		Chia...
Processo di inattività	0	In esec.	SYSTEM	92	8 K		Perce...
System	4	In esec.	SYSTEM	01	12 K		NT K...
Secure System	236	In esec.	SYSTEM	00	64.372 K		NT K...
Registry	280	In esec.	SYSTEM	00	12.712 K		NT K...
smss.exe	844	In esec.	SYSTEM	00	180 K		Gest...
cssrs.exe	1184	In esec.	SYSTEM	00	972 K		Proce...
wmminit.exe	1316	In esec.	SYSTEM	00	340 K		App...
services.exe	1400	In esec.	SYSTEM	00	3.924 K		App ...
EpicGameLauncher...	1416	In esec.	nitis	00	136.392 K	x64	EpicG...
mssed.exe	1476	In esec.	nitis	00	13.908 K	x64	Micro...
lsalso.exe	1476	In esec.	SYSTEM	00	556 K	x64	Crede...
lsass.exe	1492	In esec.	SYSTEM	00	6.032 K		Local ...
svchost.exe	1624	In esec.	SYSTEM	00	10.436 K	x64	Proce...
fondtvrhost.exe	1652	In esec.	UMDF-D	00	152 K	x64	User...
mssed.exe	1700	In esec.	nitis	00	26.520 K	x64	Micro...
Dropbox.exe	1720	In esec.	nitis	00	648 K	x64	Drop...
svchost.exe	1760	In esec.	SERVIZIO...	00	1.320 K	x64	Proce...
svchost.exe	1764	In esec.	SERVIZIO...	00	9.140 K	x64	Proce...
svchost.exe	1816	In esec.	SYSTEM	00	688 K	x64	Proce...
svchost.exe	1820	In esec.	SYSTEM	00	1.788 K	x64	Proce...
mssedgewebview2.exe	1840	In esec.	nitis	00	2.960 K	x64	WebV...
svchost.exe	1884	In esec.	SERVIZIO...	00	1.084 K	x64	Proce...
svchost.exe	1984	In esec.	SYSTEM	00	392 K	x64	Proce...
svchost.exe	1992	In esec.	SYSTEM	00	892 K	x64	Proce...
SnippingTool.exe	2028	In esec.	nitis	00	23.756 K	x64	Snipp...
svchost.exe	2044	In esec.	SERVIZIO...	00	2.892 K	x64	Proce...
svchost.exe	2144	In esec.	SERVIZIO...	00	2.012 K	x64	Proce...
mssedgewebview2.exe	2160	In esec.	nitis	00	25.140 K	x64	Utilità
svchost.exe	2188	In esec.	SYSTEM	00	476 K	x64	Proce...
svchost.exe	2212	In esec.	SYSTEM	00	460 K	x64	Proce...
conhost.exe	2228	In esec.	nitis	00	2.676 K	x64	Host ...
svchost.exe	2284	In esec.	SERVIZIO...	00	4.008 K	x64	Proce...
mssedgewebview2.exe	2372	In esec.	nitis	00	13.580 K	x64	WebV...
svchost.exe	2376	In esec.	SERVIZIO...	00	1.064 K	x64	Proce...
svchost.exe	2388	In esec.	SERVIZIO...	00	1.280 K	x64	Proce...

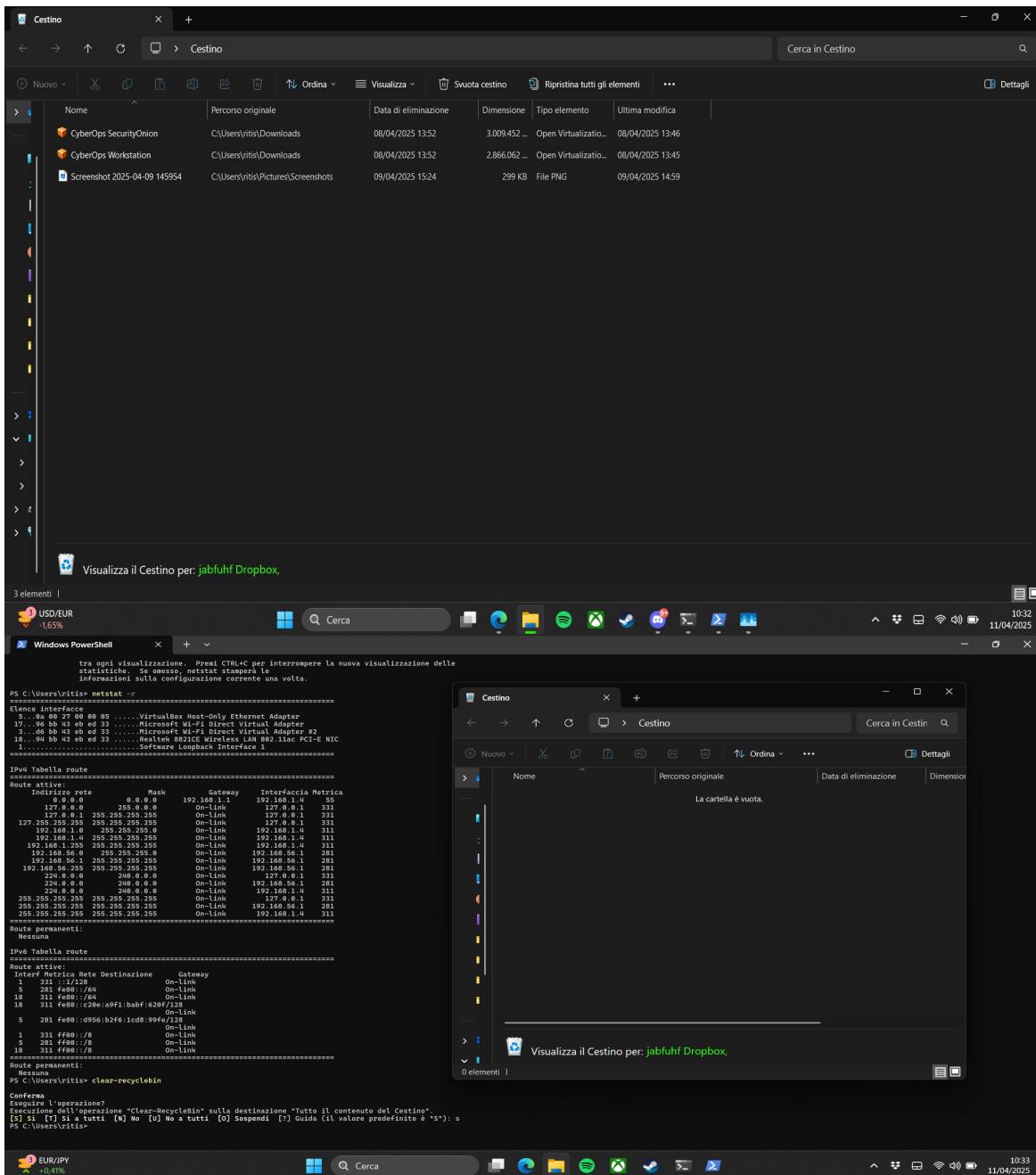
- Una volta qui andiamo a controllare le **proprietà** di questo PID

Dettagli							
	Nome	PID	Stato	Nome utente	CPU	Memoria (...	Architet...
[+]	Interrupt sistema	-	In esec...	SYSTEM	01	0 K	Chia...
[+]	Processo di inattività ...	0	In esec...	SYSTEM	77	8 K	Perce...
[+]	System	4	In esec...	SYSTEM	01	12 K	NT K...
[+]	Secure System	236	In esec...	SYSTEM	00	64.372 K	NT K...
[+]	Registry	280	In esec...	SYSTEM	00	12.736 K	NT K...
[+]	smss.exe	844	In esec...	SYSTEM	00	180 K	Gesti...
[+]	csrss.exe	1184	In esec...				
[+]	winit.exe	1316	In esec...				
[+]	services.exe	1400	In esec...				
[+]	EpicGamesLauncher...	1416	In esec...				
[+]	msedge.exe	1464	In esec...	svchost			
[+]	Lsalso.exe	1476	In esec...				
[+]	lsass.exe	1492	In esec...				
[+]	svchost.exe	1624	In esec...				
[+]	fontdrvhost.exe	1652	In esec...				
[+]	msedge.exe	1700	In esec...				
[+]	Dropbox.exe	1720	In esec...				
[+]	svchost.exe	1760	In esec...				
[+]	svchost.exe	1764	In esec...				
[+]	svchost.exe	1816	In esec...				
[+]	svchost.exe	1820	In esec...				
[+]	msedgewebview2.exe	1840	In esec...				
[+]	svchost.exe	1884	In esec...				
[+]	svchost.exe	1984	In esec...				
[+]	svchost.exe	1992	In esec...				
[+]	svchost.exe	2044	In esec...				
[+]	svchost.exe	2144	In esec...				
[+]	msedgewebview2.exe	2160	In esec...				
[+]	svchost.exe	2188	In esec...				
[+]	svchost.exe	2212	In esec...				
[+]	conhost.exe	2228	In esec...				
[+]	svchost.exe	2284	In esec...				
[+]	msedgewebview2.exe	2372	In esec...	ritis	00	13.580 K	x64
[+]	svchost.exe	2376	In esec...	SERVIZIO L...	00	1.040 K	x64
[+]	svchost.exe	2388	In esec...	SERVIZIO L...	00	1.284 K	x64
[+]	steamwebhelper.exe	2484	In esec...	ritis	00	56.524 K	x64

Queste ci dicono che il PID 1764 è associato a **svhost.exe**, ci dice che è un servizio di rete e che utilizza **9140K** di memoria.

Come ultimo passaggio ci viene detto di svuotare il cestino dalla

## PowerShell attraverso il comando **clear-recyclebin**



## 3. WIRESHARK

- Aprire il terminale e inserire i comandi **ip address** e **sudo tcpdump -i eth0 -s 0 -w httpdump.pcap**

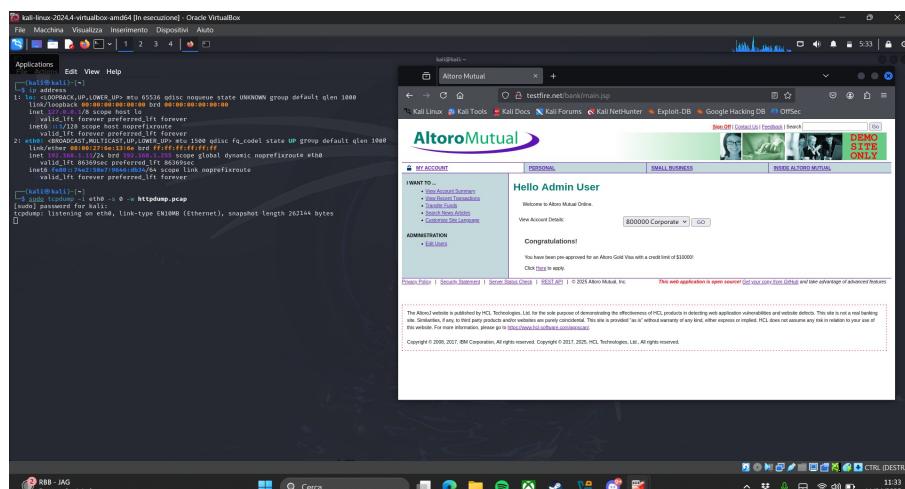
```
kali@kali: ~
File Actions Edit View Help
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:6e:13:6e brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.11/24 brd 192.168.1.255 scope global dynamic noprefixroute
        valid_lft 86196sec preferred_lft 86196sec
    inet6 fe80::74e2:50e7:9646:db34/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
(kali㉿kali)-[~]
$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for kali:
tcpdump: enp0s3: No such device exists
(No such device exists)

(kali㉿kali)-[~]
$ sudo tcpdump -i eth0 -s 0 -w httpdump.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
44 bytes
```

Il comando **ip address** ci visualizzerà le informazioni di rete, mentre il comando **tcpdump**, si avvia e registra il traffico di rete sull'interfaccia eth0.

Successivamente andiamo su sito di **altomutual** ed eseguiamo l'accesso con:

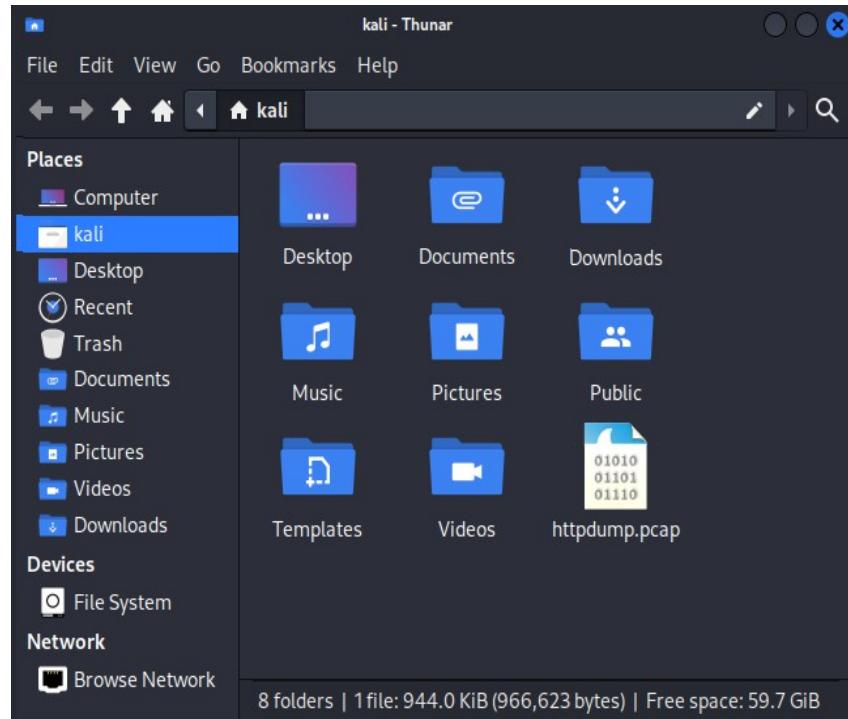
- Nome utente: **Admin**
- Password: **Admin**



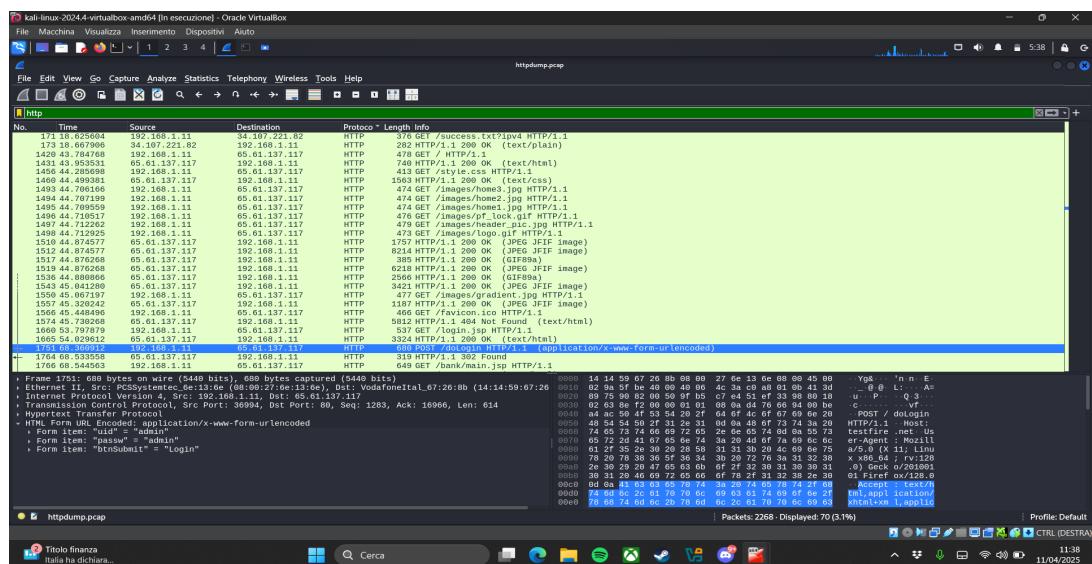
Ritorniamo sul prompt dei comandi e con **CNTRL+C** interrompiamo

l'acquisizione del pacchetto.

Andiamo a cercare sul **File Manager** e sulla cartella **Kali** cerchiamo il file **httpdump.pcap** e apriamolo con **Wireshark**



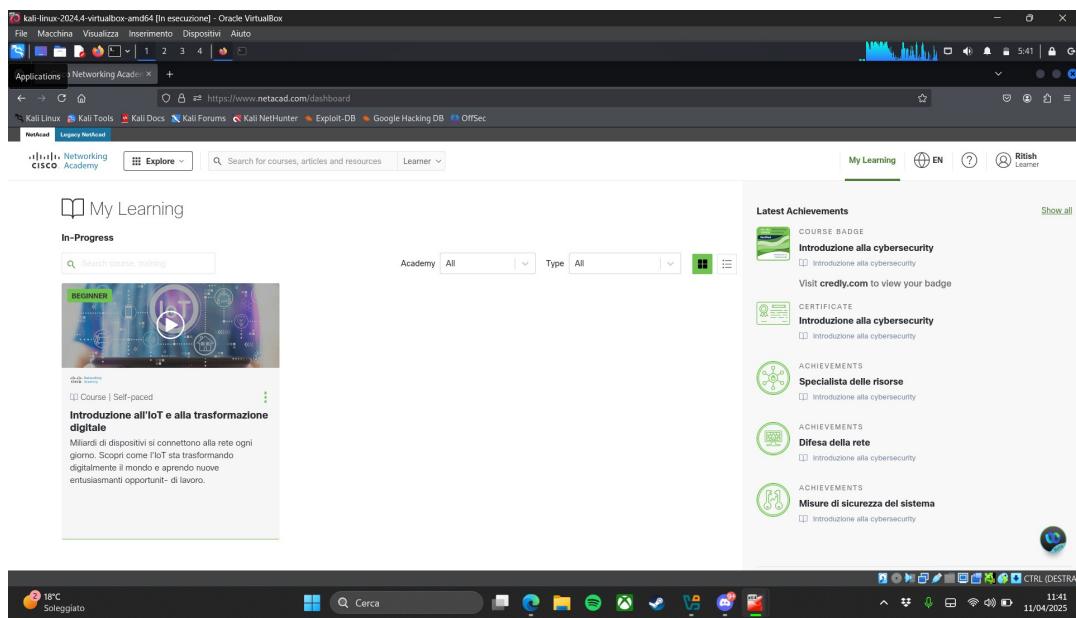
Una volta aperto su Wireshark, nella barra di filtro cerchiamo **http** e clicchiamo su applica e sfogliamo fino al messaggio **POST**. Nella finestra inferiore ci verrà visualizzata la sezione **URL del modulo HTML codificato application/x-www-form-urlencoded**, e vedremo che verranno visualizzate l'username e la password del sito che abbiamo usato in precedenza.



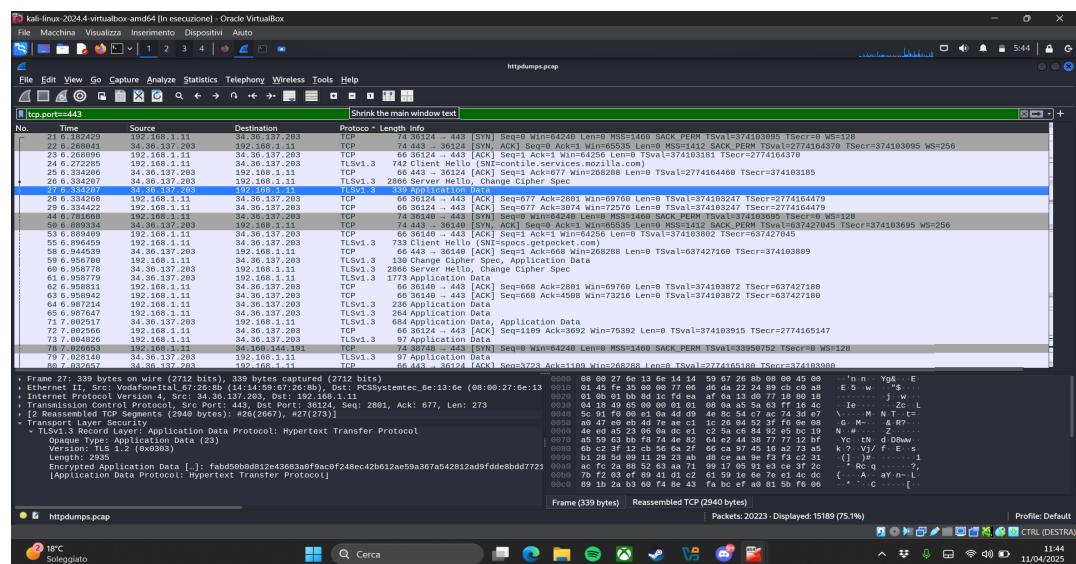
Adesso utilizziamo di nuovo il comando **tcpdump** mettendo però

come file **httpsdump.pcap**.

Accediamo su Netacad, cerchiamo il file su File Manager e lo apriamo di nuovo su Wireshark.

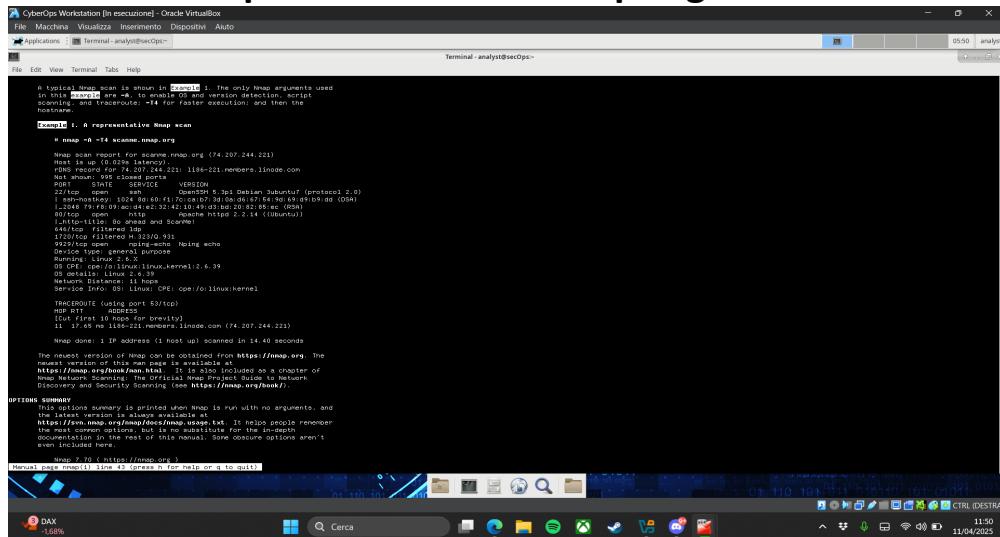


Una volta su Wireshark nella barra dei filtri ricerchiamo **tcp.port==443** e selezioniamo il messaggio di **Application Data**, nella finestra inferiore espandiamo la sezione **Secure Sockets Layer**, successivamente espandere l'**application data protocol**, noteremo che il payload dei dati non può essere visualizzato a casa della crittografia **TLSv1.2**.

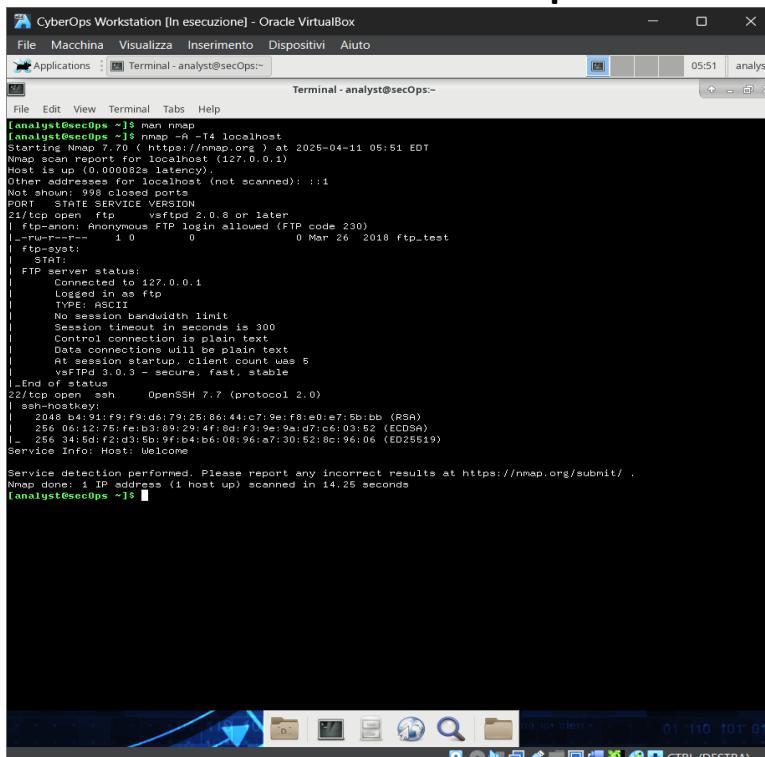


## 4. NMAP

Dal prompt del terminale scriviamo **man nmap** che, ci farà visualizzare il manuale su comando nmap, comando che serve a scansionare host e porte di un dispositivo per trovare possibili porte aperte. Da questo manuale vediamo come il comando nmap utilizzato sia **nmap -A -T4 scanme.nmap.org**.



Dal terminale inseriamo il comando **nmap -A -T4 localhost**



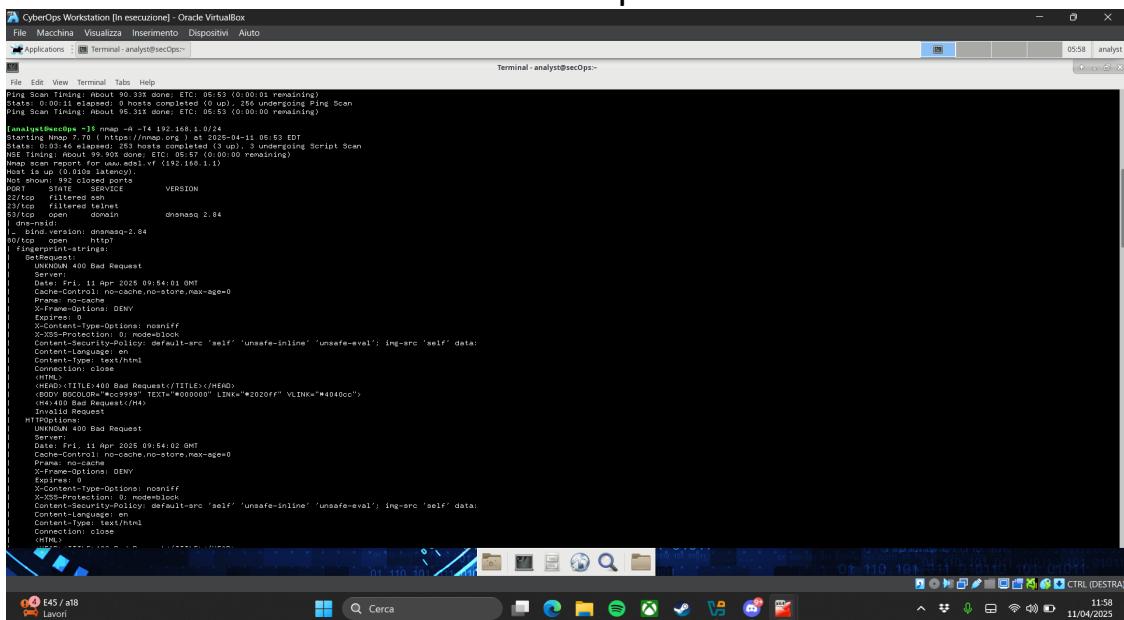
Come vedremo le porte aperte saranno la **21/TCP:FTP** e la **22/TCP:SSH**, rispettivamente con i servizi di **ftp:vsftpd**, e di **OpenSSH**.

Successivamente andremo a scansionare la nostra rete, prima però

dobbiamo sapere il nostro indirizzo IP e la nostra subnet mask,  
quindi utilizzeremo il comando **ip address**

```
[analyst@secOps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:29:3d:42 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.10/24 brd 192.168.1.255 scope global dynamic enp0s3
        valid_lft 86153sec preferred_lft 86153sec
    inet6 fe80::a00:27ff:fe29:3d42/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```

Il nostro indirizzo ip è **192.168.1.10**, a questo punto allora possiamo scansionare la nostra rete tramite il comando **nmap -A -T4 192.168.1.0/24**, questo comando ci scansionerà tutti i dispositivi che sono connessioni alla rete e fanno parte della rete **1.0**.



Adesso eseguiamo la scansione di un server remoto tramite il

comando che abbiamo trovato nel manuale **nmap -A -T4**  
[scanme.nmap.org](http://scanme.nmap.org)

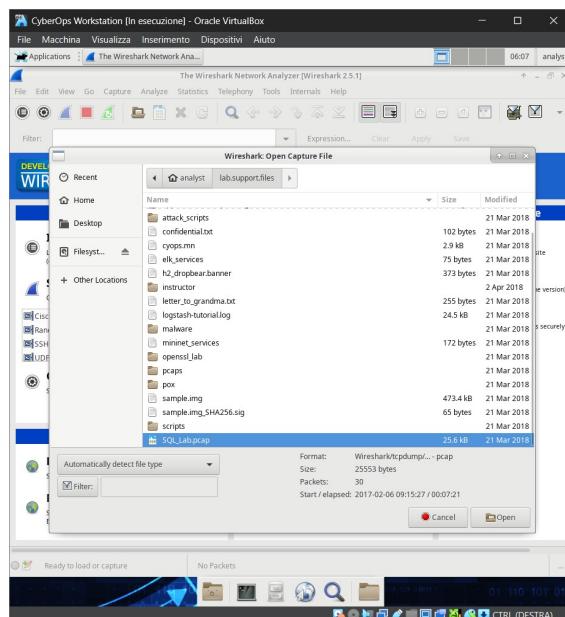
```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.00 ( https://nmap.org ) at 2025-04-11 06:00 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.20s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 994 closed ports
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:f2:56:4c: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      dnsmaq 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!
2601/tcp  filtered zebra
9929/tcp  open     nping-echo Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 29.26 seconds
[analyst@secOps ~]$
```

Questo comando ci visualizzerà i servizi e le porte aperte, quei porte e servizi sono filtrati, l'indirizzo IP del server e infine il sistema operativo.

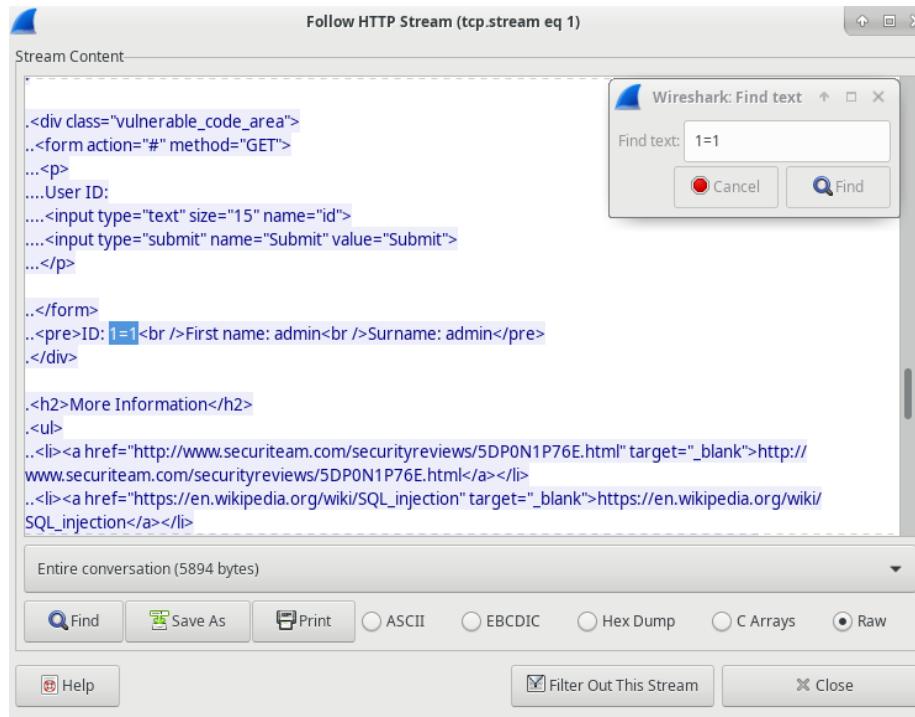
## 5. MySQL

Apriamo **WireShark**, clicchiamo su **Open** al centro dell'applicazione, dalla cartella che ci verrà aperta spostiamoci sulla directory **lab.support.files** e apriamo il file **SQL\_Lab.pcap**, una volta aperto il file vedremo l'acquisizione del traffico con durata 8 minuti, tramite SQL injection, con due indirizzo **10.0.2.4** e **10.0.2.15**.

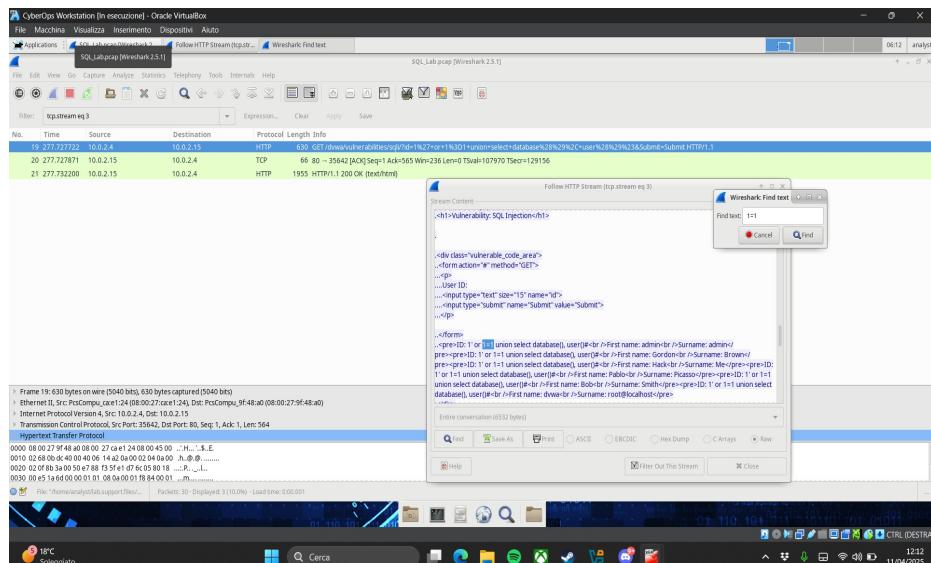


Clicchiamo con il tasto destro sulla riga 13 e scegliamo l'opzione

**follow HTTP Stream**, qui avremo una finestra che mostrerà in rosso il traffico di origine e in blu il dispositivo di destinazione, qui andiamo su **Find** e inseriamo **1=1** e clicchiamo invio  
Da questa riga capiamo che l'attaccante ha voluto verificare se il target 10.0.2.15 fosse vulnerabile all'SQL injection, invece di rispondere con un messaggio di errore l'applicazione ha risposto con un record da un database, così facendo capire all'attaccante di poter inserire un comando SQL.



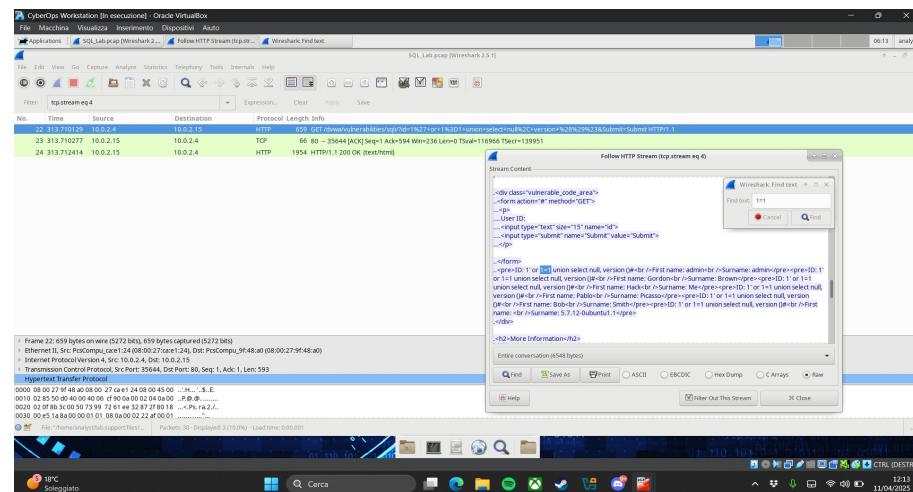
Adesso spostiamoci sulla riga 19 con lo stesso procedimento del precedente



Anche in questo caso, dopo l'inserimento della stringa (**1'** o **1=1**

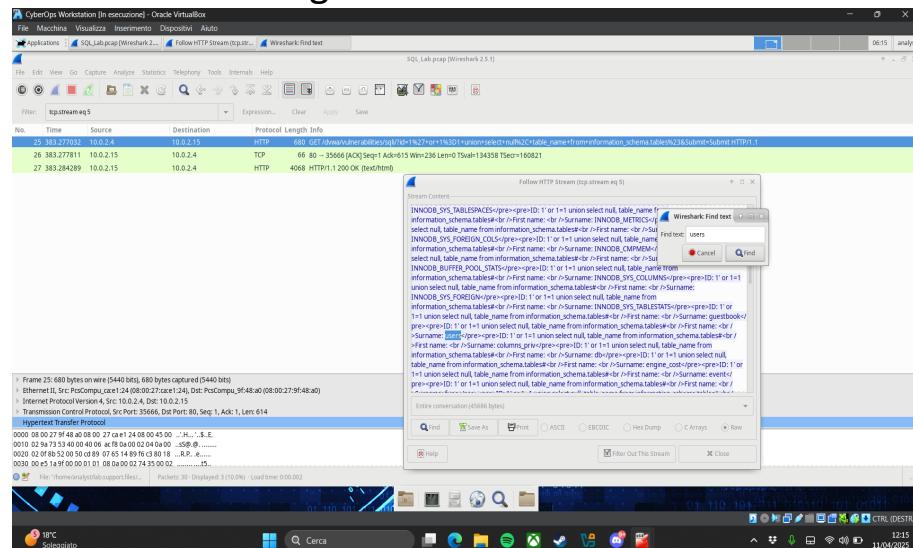
**union select database(), user()#** non viene mandato un messaggio di errore bensì, viene visualizzato il nome del database **DVWA** e l'utente **root@localhost**.

Spostiamoci sulla riga 22



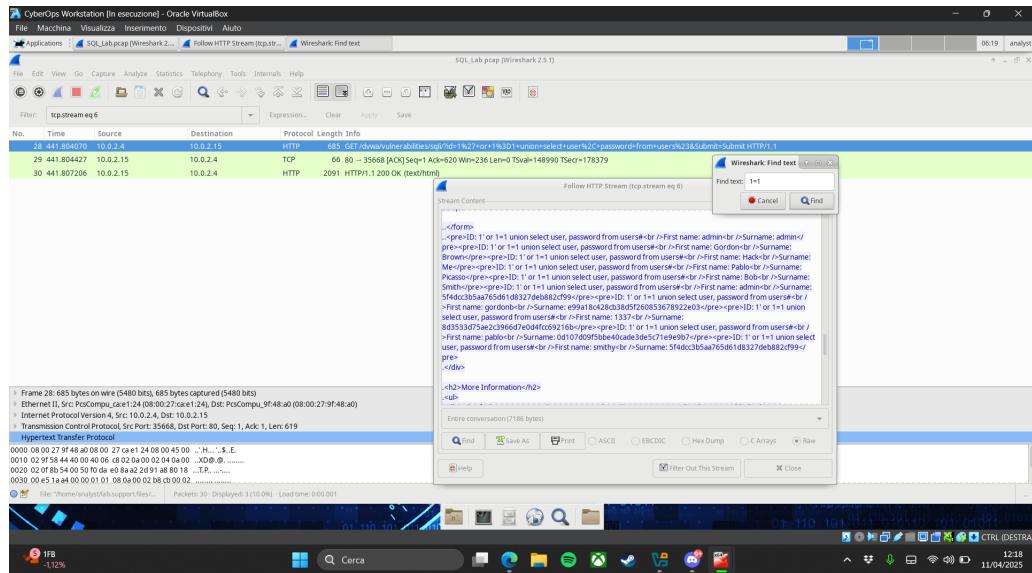
Inserendo la stringa **(1' o 1=1 union select null, version ()#)**  
l'attaccante è risalito alla versione **MySQL 5.7.12-0**.

Adesso andiamo alla riga 25



In questo caso nel campo di ricerca inseriamo **users**, trovando così, attraverso la stessa stringa **(1' o 1=1 union select null, table\_name da information\_schema.tables#)**, tutte le tabelle nel database

Infine andiamo alla riga 28



inserendo nel campo di ricerca **1=1** e la stringa (**1' o 1=1 unione seleziona utente, password da users#**), all'attaccante verrano visualizzati tutti i nomi utenti e le password in formato hash

## 6. CONCLUSIONI

Nel presente rapporto sono stati esplorati vari strumenti e tecniche di sicurezza informatica tramite esercizi pratici, fornendo una comprensione approfondita delle operazioni fondamentali per l'analisi e la gestione della rete.

- **Windows PowerShell:** L'utilizzo di PowerShell ha permesso di acquisire familiarità con comandi efficaci per l'amministrazione del sistema, come la visualizzazione di processi attivi e l'analisi della rete. La conoscenza dei cmdlet e la loro applicazione sono essenziali per automatizzare compiti e migliorare l'efficienza operativa.
- **Wireshark:** L'analisi del traffico di rete tramite Wireshark ha rivelato l'importanza della cattura e dell'analisi dei pacchetti. L'esercizio ha dimostrato come le informazioni sensibili, come le credenziali di accesso, possano essere facilmente estratte da pacchetti non protetti e ha evidenziato l'impatto della crittografia sulle comunicazioni sicure.
- **Nmap:** L'uso di Nmap ha mostrato come sia possibile rilevare porte aperte e servizi su un dispositivo e una rete, facilitando

l'identificazione di potenziali vulnerabilità. La scansione della rete ha rivelato la necessità di monitorare attivamente i dispositivi connessi per garantire la sicurezza.

- **MySQL e SQL Injection:** L'esercizio di SQL injection ha illuminato le vulnerabilità che possono esistere nei database e ha evidenziato la necessità di implementare misure di sicurezza robuste per proteggere i dati sensibili. La comprensione delle tecniche di attacco consente agli amministratori di database di difendersi meglio da potenziali minacce.

In sintesi, il rapporto sottolinea l'importanza di una formazione pratica nella sicurezza informatica, fornendo le basi per l'identificazione e la mitigazione delle vulnerabilità. La combinazione di strumenti come PowerShell, Wireshark, Nmap e pratiche di SQL injection costituisce un approccio integrato per migliorare la sicurezza della rete e dei sistemi.