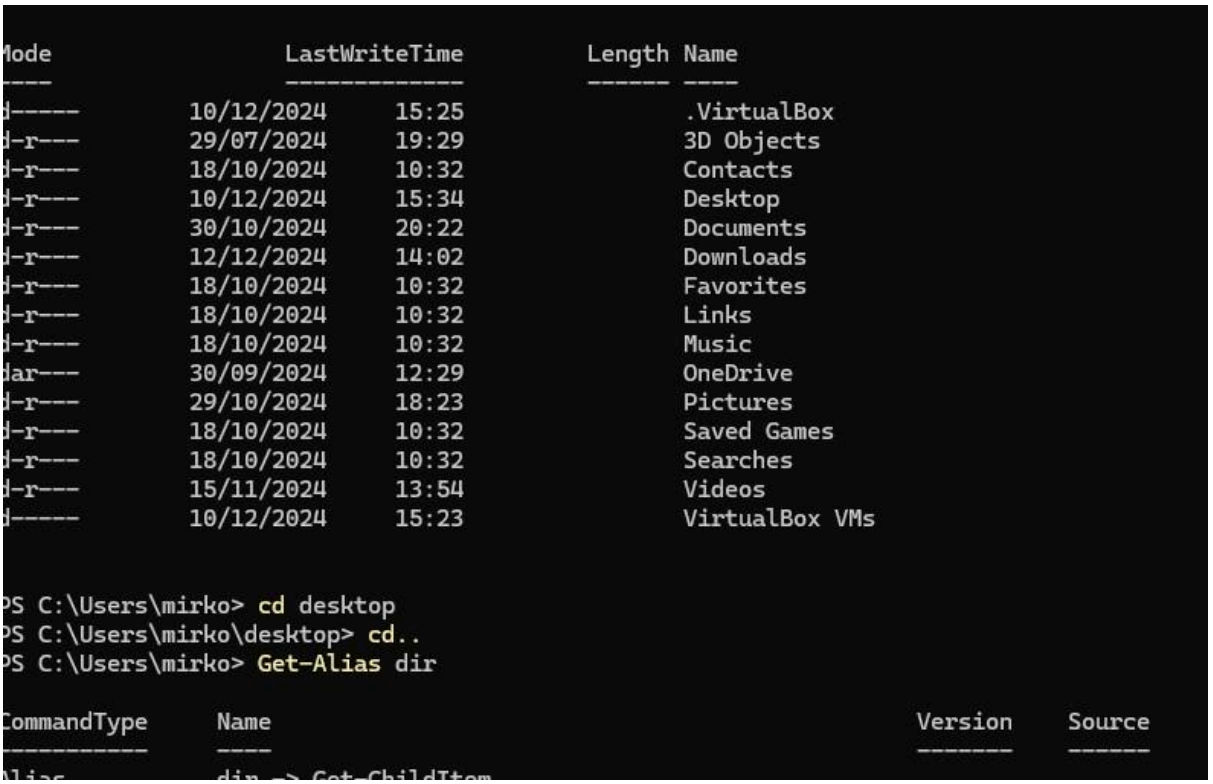
S11L5
INDICE
-esplorazione comandi powershell (1,2,3,4)
–utilizzo wireshark per esaminare traffico http e https (4,5,6,7)
-bonus 1 (7,8,9)

ESPLORAZIONE COMANDI POWERSHELL

Apriamo il menu start e apriamo il windows powershell
Come primo comando vediamo dir
Il comando dir visualizza l'elenco dei file e delle cartelle all'interno di una directory specificata (o della directory corrente se non viene indicata alcuna directory). Può essere usato con varie opzioni per personalizzare la visualizzazione.



In questo screen vediamo altri comandi ad esempio cd che ci permette di cambiare directory oppure get alias dir, getchilditem
In PowerShell, `dir` è effettivamente un alias per il comando `Get-ChildItem`. Quindi, quando usi `dir` in PowerShell, sta eseguendo il comando `Get-ChildItem`, che elenca i file e le cartelle nella directory corrente o in quella specificata.

Il prossimo comando che andiamo a vedere e netstat -r

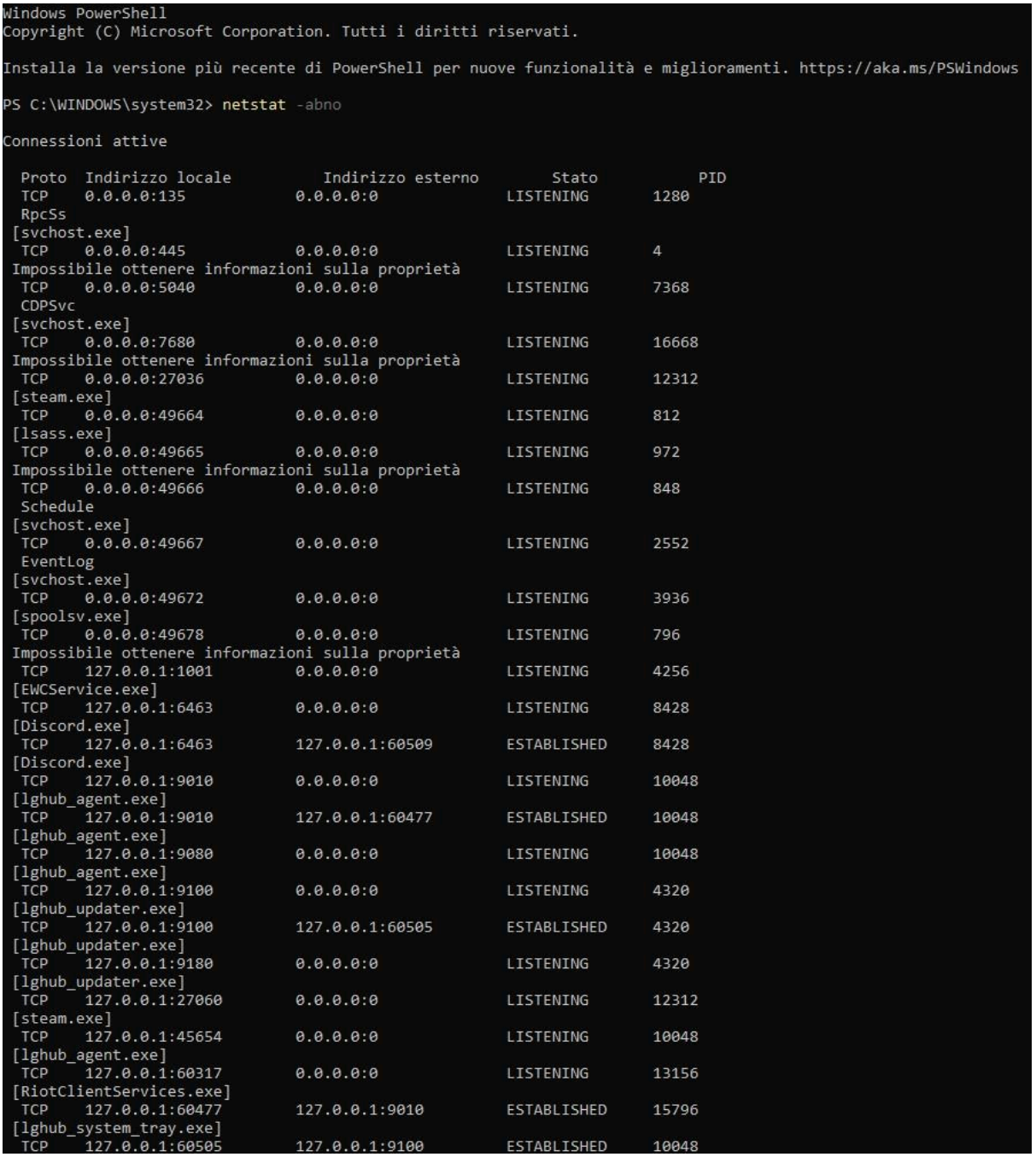
Il comando `netstat -r` serve per visualizzare la **tabella di routing** del sistema, che mostra come i pacchetti di rete vengono indirizzati tra le diverse reti e sottoreti a livello di sistema operativo.

La **tabella di routing** contiene informazioni cruciali per il funzionamento della rete, come la destinazione, la rete di gateway, l'interfaccia di rete utilizzata e altre informazioni relative al percorso seguito dai pacchetti.

```
PS C:\Users\mirko> netstat -r
===========================================================================
Elenco interfacce
 12...0a 00 27 00 00 0c ......VirtualBox Host-Only Ethernet Adapter
 15...74 56 3c d9 dc 73 ......Realtek Gaming 2.5GbE Family Controller
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Tabella route
===========================================================================
Route attive:
     Indirizzo rete            Mask          Gateway     Interfaccia Metrica
          0.0.0.0          0.0.0.0    192.168.178.1   192.168.178.43     35
        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
     192.168.56.0    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
    192.168.178.0    255.255.255.0         On-link    192.168.178.43    291
   192.168.178.43  255.255.255.255         On-link    192.168.178.43    291
  192.168.178.255  255.255.255.255         On-link    192.168.178.43    291
        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    192.168.178.43    291
  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    192.168.178.43    291
===========================================================================
Route permanenti:
```

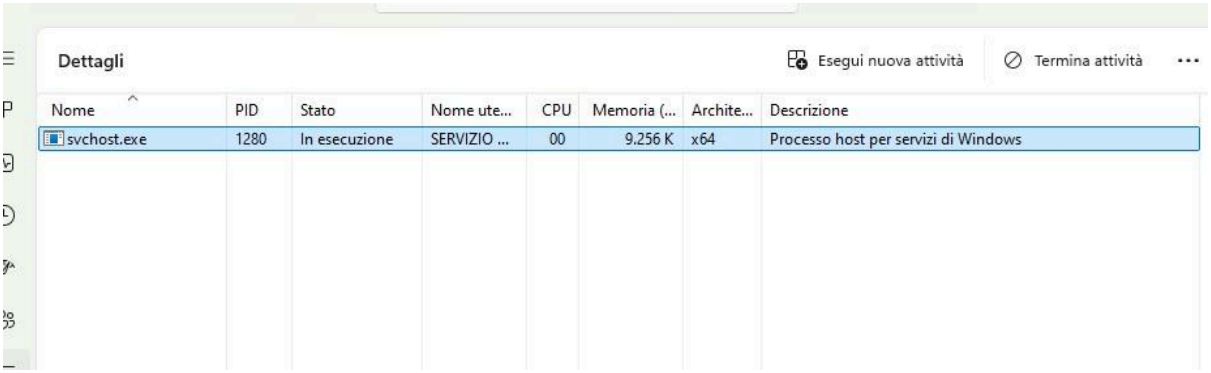
Per il prossimo comando netstat -abno dobbiamo aprire il powershell come amministratore.
Il comando `netstat -abno` è una variante avanzata di `netstat`, utilizzato per ottenere informazioni dettagliate sulle connessioni di rete attive e sui processi associati a quelle connessioni in un sistema Windows.
-a: Visualizza **tutte** le connessioni e le porte di ascolto (inclusi i collegamenti in entrata e in uscita). Mostra sia le connessioni TCP che UDP.
-b: Mostra il **nome del programma** (processo) associato a ciascuna connessione o porta di ascolto. Questo aiuta a identificare quale applicazione o servizio sta utilizzando una specifica connessione di rete.
-n: Visualizza gli **indirizzi IP e le porte** numerici anziché i nomi di dominio e i nomi di servizio. Questo è utile per ottenere una visualizzazione più rapida dei dettagli di rete, senza risolvere i nomi.
-o: Mostra l'**ID del processo (PID)** che ha aperto la connessione o la porta. Questo consente di associare la connessione di rete a un particolare processo in esecuzione nel sistema



Successivamente apriamo il task manager andiamo nella sezione dettagli e inseriamo un PID dall'elenco in base alle nostre preferenze in questo caso io ho scelto il primo 1280.
Il **PID** (Process IDentifier) è un identificatore univoco assegnato dal sistema operativo a ogni processo in esecuzione. Ogni programma o processo che viene avviato su un sistema (che sia un'applicazione, un servizio di sistema o una parte di un'applicazione più grande) riceve un numero PID, che serve a distinguere quel processo da altri.

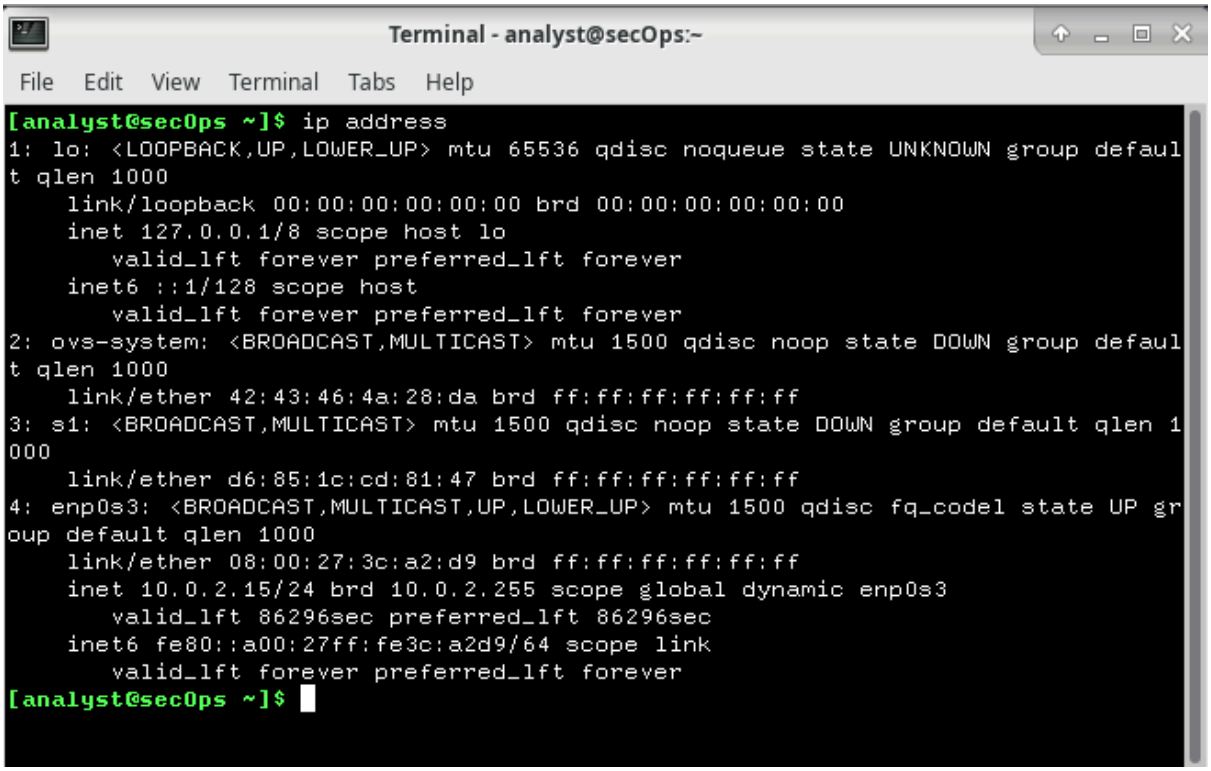
Il PID permette al sistema operativo e agli strumenti di monitoraggio di:

1. **Identificare** in modo univoco un processo.
2. **Monitorare** lo stato e le risorse consumate dal processo (CPU, memoria, ecc.).
3. **Gestire** i processi (terminare, sospendere, inviare segnali, ecc.).

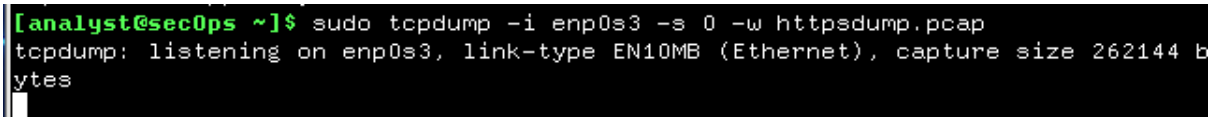


Il PID è una chiave per raccogliere informazioni dettagliate su un processo in esecuzione. Con il PID, puoi identificare il programma, monitorare l'utilizzo delle risorse, ottenere informazioni sulle connessioni di rete e risolvere eventuali problemi legati ai processi, come il consumo eccessivo di risorse o processi sospetti.

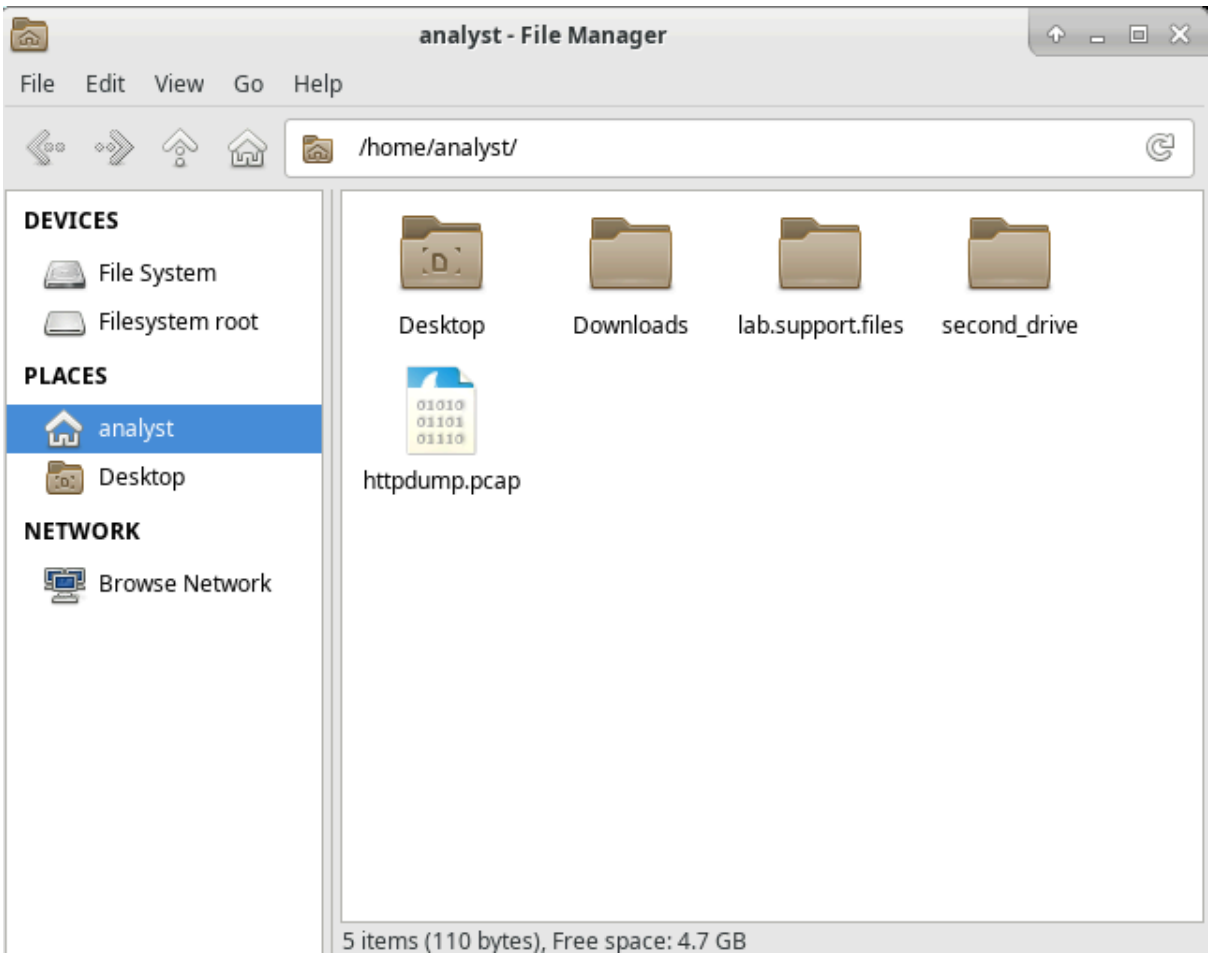
ANALISI TRAFFICO HTTP E HTTPS

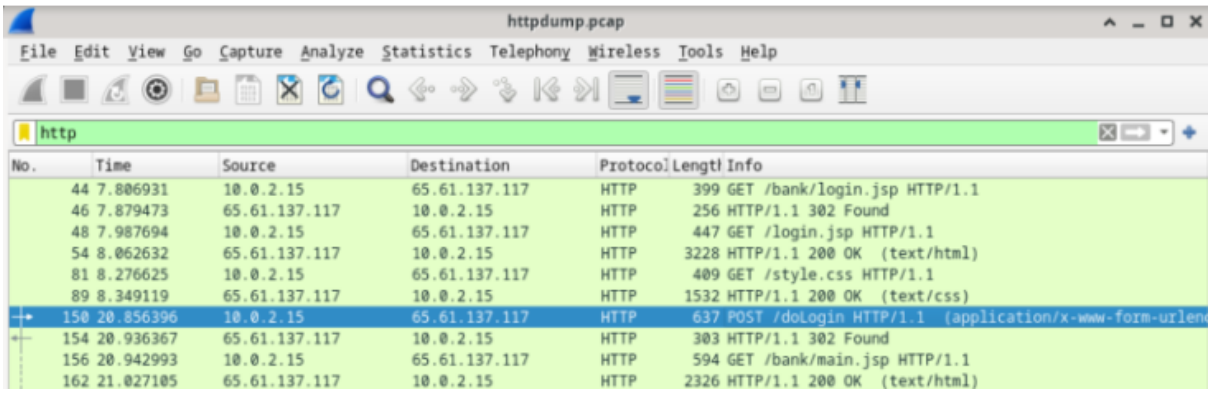


La prima cosa da fare è il comando ip address.
Successivamente usiamo il comando sudo tcpdump –i enp0s3 –s 0 –w httpdump.pcap
Serve per **catturare il traffico di rete** sulla tua interfaccia di rete specificata (in questo caso `enp0s3`) e salvarlo in un file in formato `.pcap` (Packet Capture), che può essere poi analizzato con strumenti come **Wireshark**.

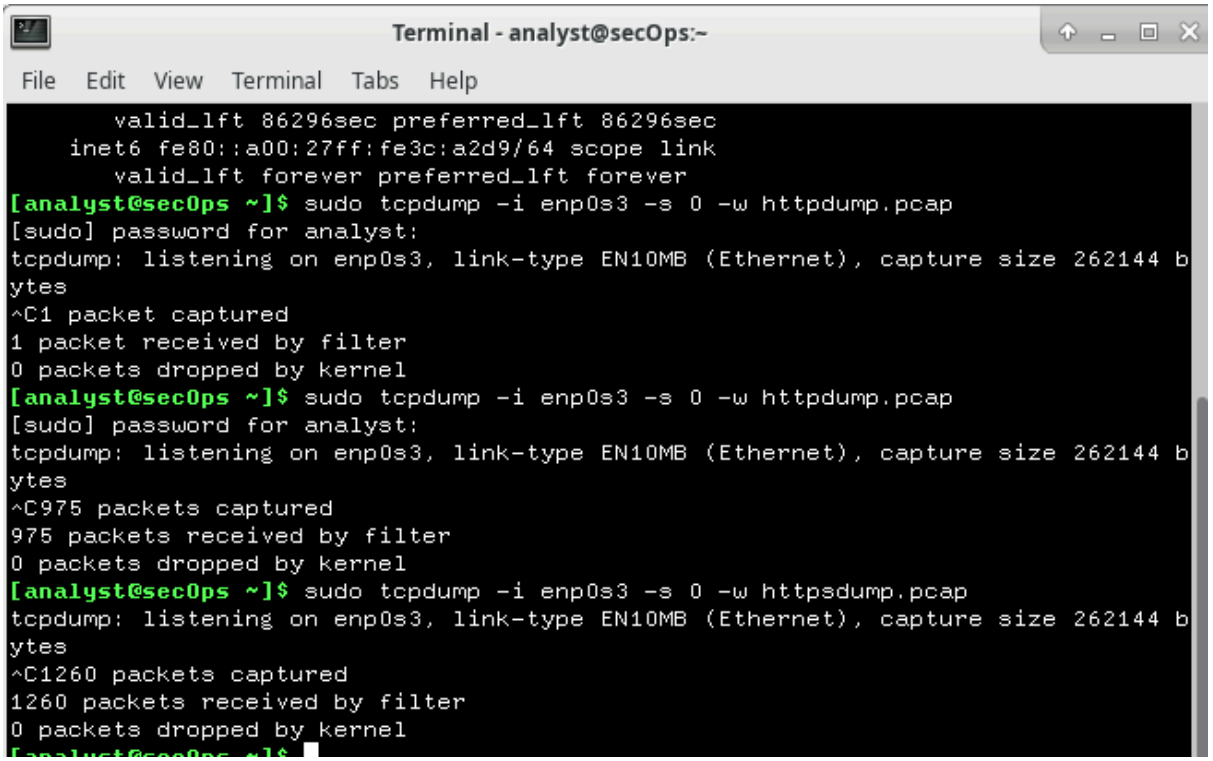


Il TCP dump precedentemente eseguito ci da in output un file denominato **httpdump.pcap.**
Clicchiamo apri con e selezioniamo wireshark.

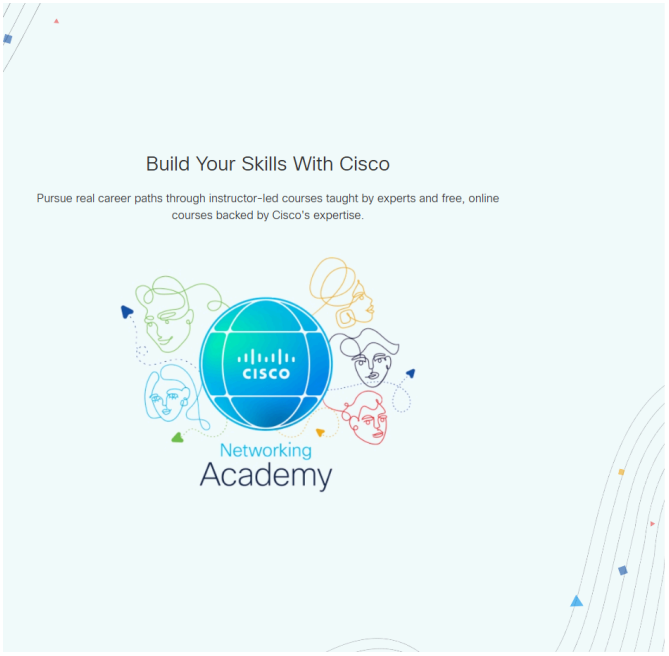


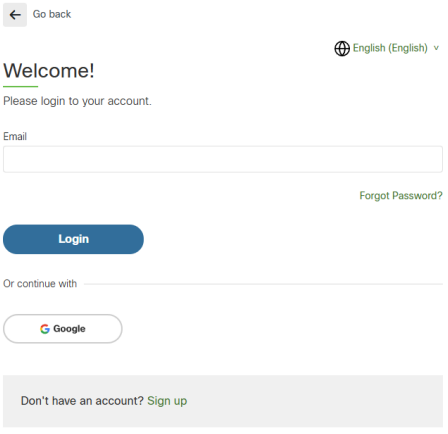


CATTURA TRAFFICO HTTPS
Fondamentalmente i passaggi sono gli stessi con solo qualche variazione nei comandi. Inseriamo il comando `sudo tcpdump –i enp0s3 –s 0 –w httpsdump.pcap`

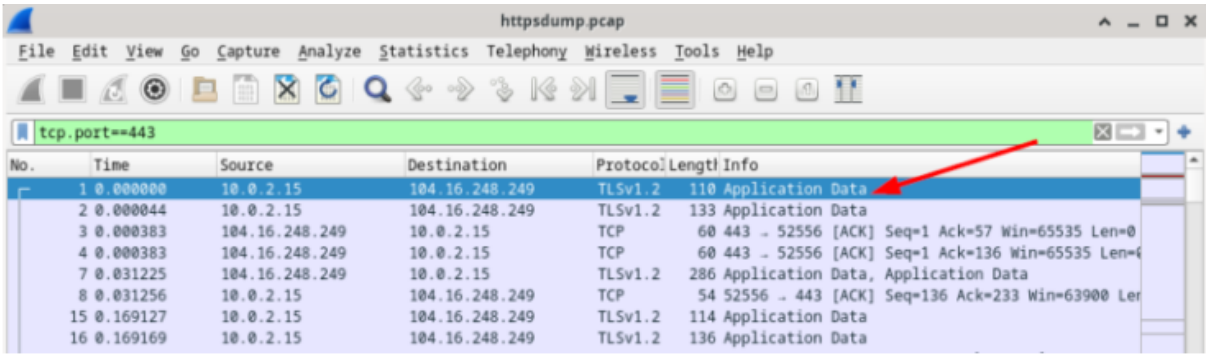


andiamo sul sito www.netcad.com





Come nella fase precedente troveremo un file chiamato httpsdump.pcap
Apriamo con wireshark e troviamo come nel caso precedente questa schermata.



BONUS 1

ESPLORAZIONE NMAP

-

apriamo il guida con il comando man nmap

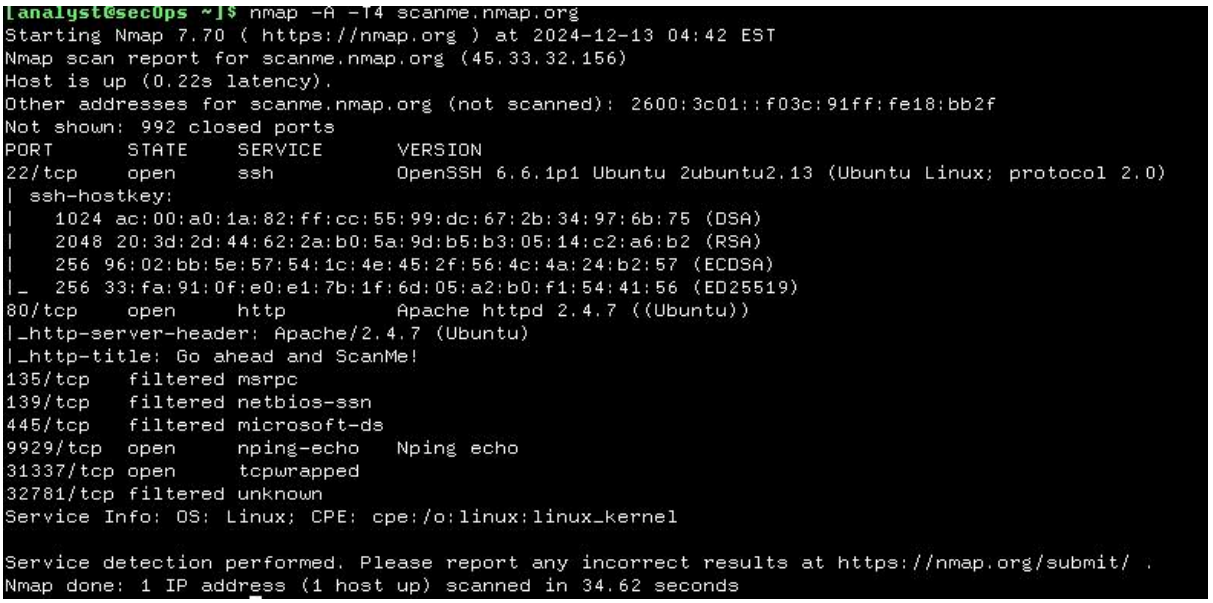
Nmap (Network Mapper) è uno strumento open-source ampiamente utilizzato per l'analisi della rete e la sicurezza. È principalmente usato per **scansionare** le reti, identificare dispositivi connessi e raccogliere informazioni su di essi, come porte aperte, servizi in esecuzione, versioni di software e potenziali vulnerabilità. Nmap è uno degli strumenti di base per i professionisti della sicurezza informatica, amministratori di sistema e analisti di rete.

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 04:41 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000027s 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 11.50 seconds
```

Come mostrato nell’immagine con il comando nmap -A -T4 localhost

Scansiona il computer locale (`localhost`) per raccogliere informazioni dettagliate.
Rileva il sistema operativo e la **versione dei servizi** in esecuzione sul dispositivo.
Esegue una **scansione completa delle porte aperte**, determinando se ci sono vulnerabilità note utilizzando gli **script di Nmap**.
Traceroute: Mostra il percorso che i pacchetti di rete percorrono per arrivare al tuo computer.
Utilizza un **template di scansione rapida (T4)** per eseguire il tutto in modo relativamente veloce.

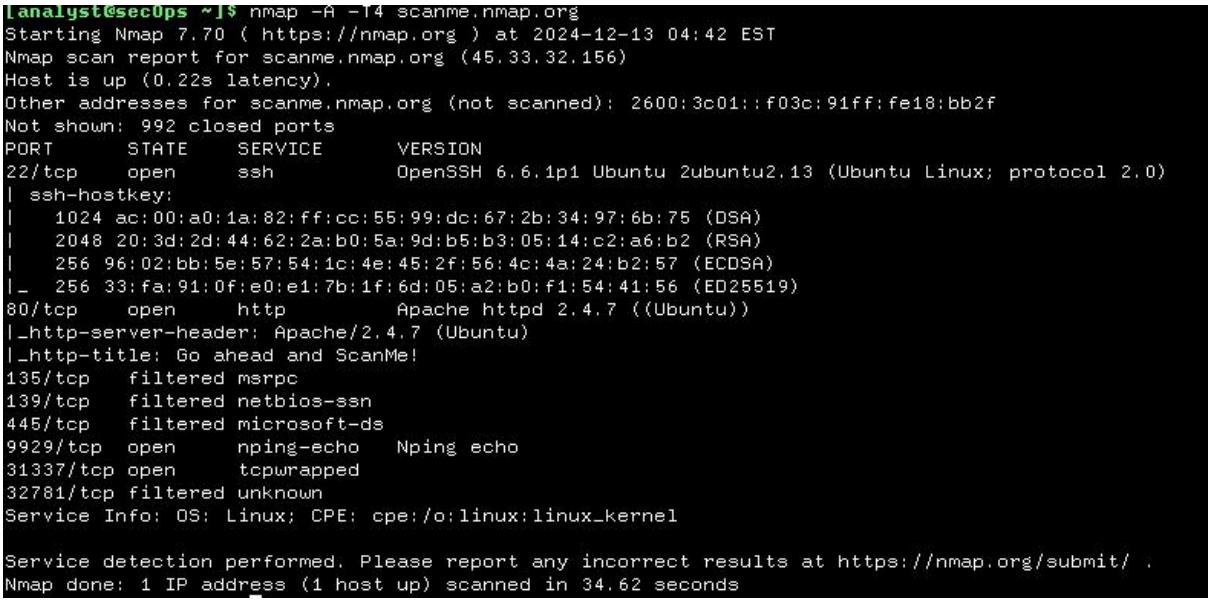


successivamente scannerizziamo la nostra network con il comando nmap -A T4 seguito dal nostro indirizzo ip per ottenere tutte le informazioni

Quando esegui questo comando, Nmap fornisce le seguenti informazioni dettagliate:

1. **Porte aperte**:
    - Verranno scansionate tutte le porte comuni e verrà visualizzato un elenco delle porte aperte sul dispositivo target (ad esempio, HTTP sulla porta 80, HTTPS sulla porta 443, FTP sulla porta 21, ecc.).
2. **Servizi e versioni**:
    - Nmap cercherà di determinare **quali servizi** sono in esecuzione su ciascuna porta aperta e **le versioni specifiche** di quei servizi. Ad esempio, se sulla porta 80 è in esecuzione un server web, Nmap cercherà di identificare la versione esatta (ad esempio Apache 2.4.29).

3. **Sistema operativo**:
    - **Rilevazione del sistema operativo**: Nmap cercherà di determinare quale sistema operativo è in uso sul dispositivo target (Windows, Linux, macOS, ecc.) e la versione di tale sistema operativo.
4. **Traceroute**:
    - Verrà eseguito un **traceroute** per determinare il percorso che i pacchetti di rete percorrono per arrivare al dispositivo target, inclusi i router intermedi. Questo può aiutare a comprendere come i pacchetti viaggiano nella rete.
5. **Vulnerabilità e configurazioni di sicurezza**:
    - Se sono attivi, gli script di **Nmap Scripting Engine (NSE)** possono cercare vulnerabilità specifiche o errori di configurazione sui dispositivi target. Questi script possono rivelare informazioni come:
        - Vulnerabilità conosciute (ad esempio, una versione di un software con una vulnerabilità critica).
        - Configurazioni errate (come la presenza di porte aperte inutili o servizi non sicuri).



L’ultimo step è quello di eseguire la scansione del dito scanme-nmap.org e otteniamo le medesime informazioni riguardo le porte aperte. l’OS del web server e le informazioni precedentemente citate.