

# Analisi avanzate: Un approccio pratico

---



# INDICE

---

01

PowerShell e  
Automazione

02

Cattura e Analisi  
del Traffico HTTP

03

Esplorare Nmap

04

Attacco a un  
Database MySQL

# INTRODUZIONE

NEL CONTESTO DELLA SICUREZZA INFORMATICA E DELL'ANALISI DI RETE, STRUMENTI E TECNICHE COME POWERSHELL, NMAP, WIRESHARK E L'ANALISI DEGLI ATTACCHI SQL RAPPRESENTANO RISORSE ESSENZIALI PER COMPRENDERE E MITIGARE LE MINACCIE CHE LE INFRASTRUTTURE IT AFFRONTANO QUOTIDIANAMENTE. LE QUATTRO ATTIVITÀ ESPLORATE IN QUESTO PERCORSO OFFRONO UN PANORAMA COMPLETO, PASSANDO DALL'AUTOMAZIONE DEI PROCESSI CON POWERSHELL, ALL'ESPLORAZIONE E SCANSIONE DELLE RETI CON NMAP, FINO ALLA CATTURA E ANALISI DEL TRAFFICO HTTP E ALLA VALUTAZIONE DI UN ATTACCO SQL A UN DATABASE MYSQL.

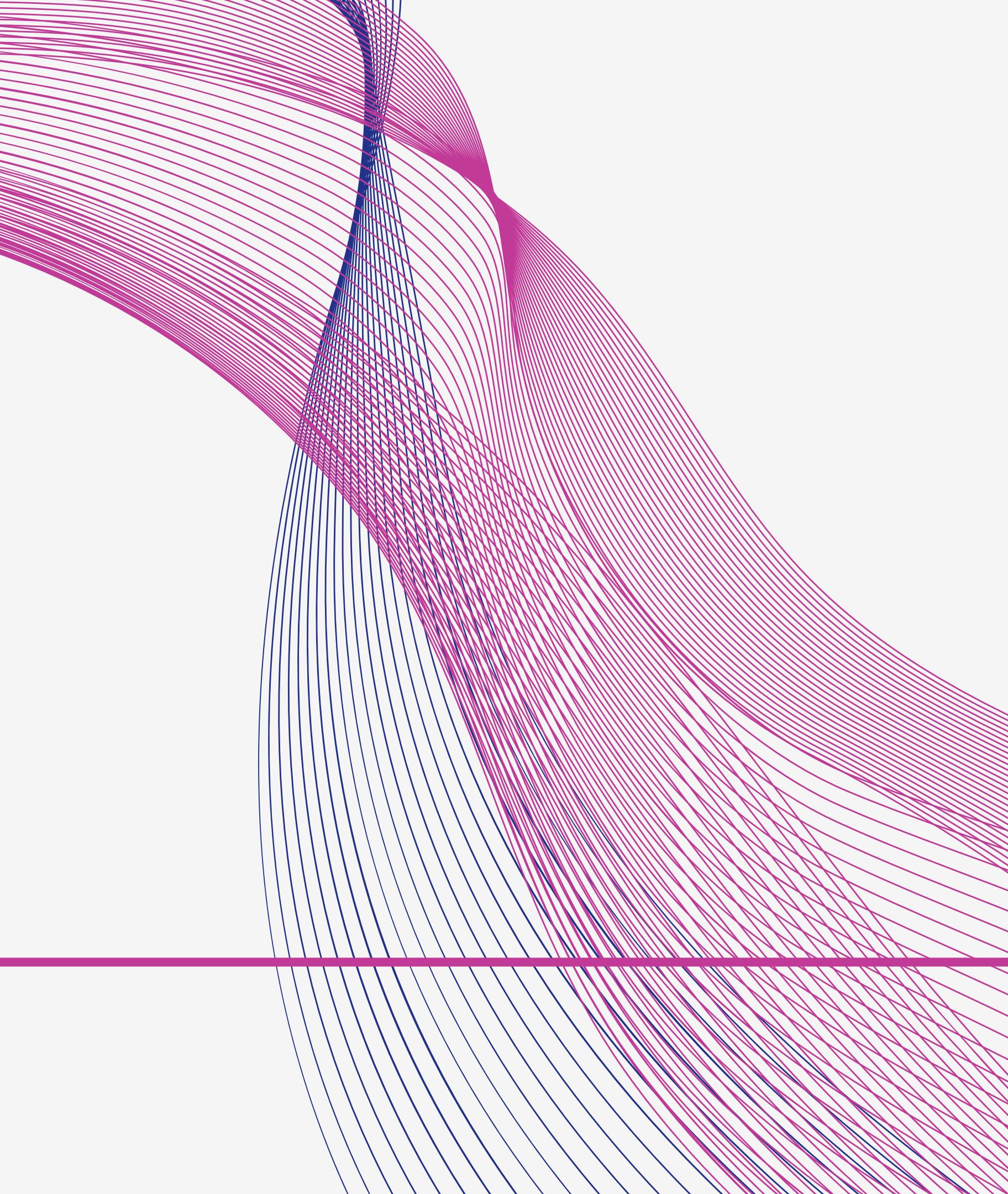
L'USO DI POWERSHELL MOSTRA COME L'AUTOMAZIONE DEI TASK POSSA RIDURRE GLI ERRORI UMANI, MIGLIORARE L'EFFICIENZA E CONTRIBUIRE ALLA SICUREZZA TRAMITE SCRIPT PERSONALIZZATI PER L'ESECUZIONE DI ATTIVITÀ COMPLESSE O RIPETITIVE.

CON NMAP, SI EVIDENZIA L'IMPORTANZA DELLA SCOPERTA DELLE RISORSE DI RETE E DELLA SCANSIONE DELLE PORTE PER IDENTIFICARE VULNERABILITÀ POTENZIALI, RENDENDOLO UNO STRUMENTO INDISPENSABILE PER L'AUDITING DELLA SICUREZZA.

L'ANALISI DEL TRAFFICO HTTP CON WIRESHARK RIVELA COME UN ATTENTO STUDIO DEL FLUSSO DI DATI POSSA ESSERE UTILE NON SOLO PER IDENTIFICARE POTENZIALI ATTACCHI, MA ANCHE PER COMPRENDERNE IL MODUS OPERANDI.

INFINE, L'ANALISI DELL'ATTACCO A UN DATABASE MYSQL TRAMITE UN FILE PCAP DI SQL INJECTION OFFRE UN'OPPORTUNITÀ PRATICA PER COMPRENDERE LE IMPLICAZIONI DI UN ATTACCO MIRATO, LE VULNERABILITÀ CHE LO CONSENTONO E LE CONTROMISURE PREVENTIVE CHE POSSONO ESSERE ADOTTATE.

QUESTE ATTIVITÀ COMBINANO ASPETTI TEORICI E PRATICI, FORNENDO UNA PANORAMICA SULLE TECNICHE ESSENZIALI PER ANALIZZARE, RILEVARE E RISPONDERE ALLE MINACCIE INFORMATICHE IN UN AMBIENTE REALE.



# POWERSHELL E AUTOMAZIONE

- Introduzione
- Parte 1: Accedere alla console di PowerShell
- Parte 2: Esplorare i comandi del Prompt dei comandi e di PowerShell
- Parte 3: Esplorare i cmdlet di PowerShell
- Parte 4: Usare il comando netstat con PowerShell
- Parte 5: Svuotare il Cestino con PowerShell
- Domanda di riflessione
- Conclusioni

# PowerShell e Automazione

PowerShell è uno strumento potente di automazione e gestione delle configurazioni sviluppato da Microsoft per il sistema operativo Windows. È utilizzato principalmente per amministrare e automatizzare attività di sistema, grazie alla sua sintassi basata su comandi (cmdlet) e script. PowerShell offre funzionalità avanzate rispetto al tradizionale Prompt dei comandi, rendendolo un alleato fondamentale per gli amministratori di sistema e i professionisti IT.

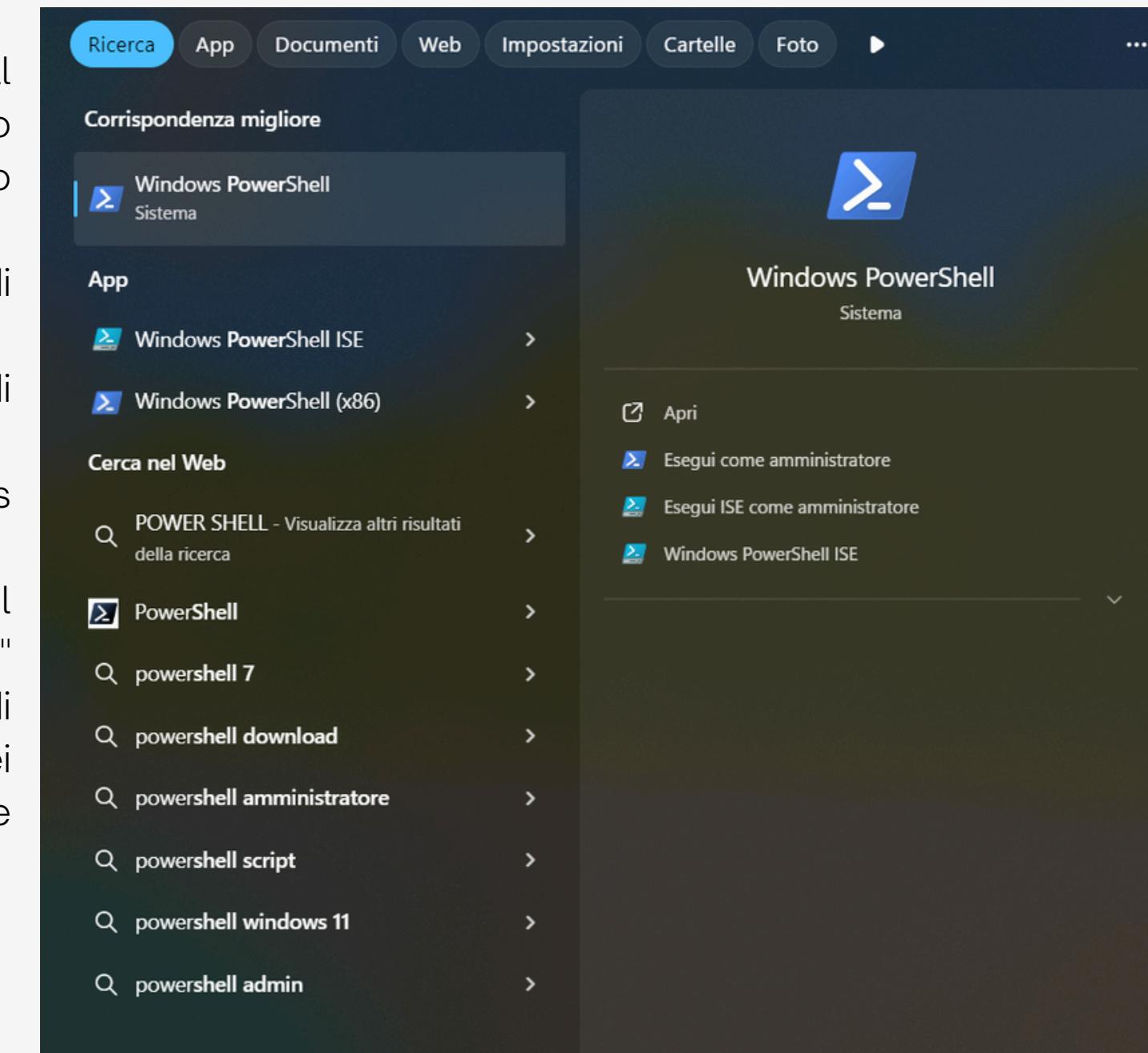
Questo laboratorio esplorerà vari aspetti di PowerShell, tra cui i comandi di base, la gestione dei processi, e l'esecuzione di operazioni avanzate come il monitoraggio delle connessioni di rete e la gestione dei file di sistema. Inoltre, faremo un confronto tra PowerShell e il Prompt dei comandi, mostrando come PowerShell offra funzionalità più robuste e flessibili.

# ACCEDERE ALLA CONSOLE DI POWERSHELL

Il primo passo per esplorare PowerShell è avviare la sua console. Questo processo può essere eseguito facilmente seguendo questi passaggi:

- Fare clic sul pulsante Start di Windows.
- Digitare "PowerShell" nella barra di ricerca.
- Selezionare l'applicazione Windows PowerShell dai risultati.

In modo simile, è possibile accedere al Prompt dei comandi digitando "cmd" nella barra di ricerca. La console di PowerShell è più potente del Prompt dei comandi e consente di eseguire comandi più complessi.

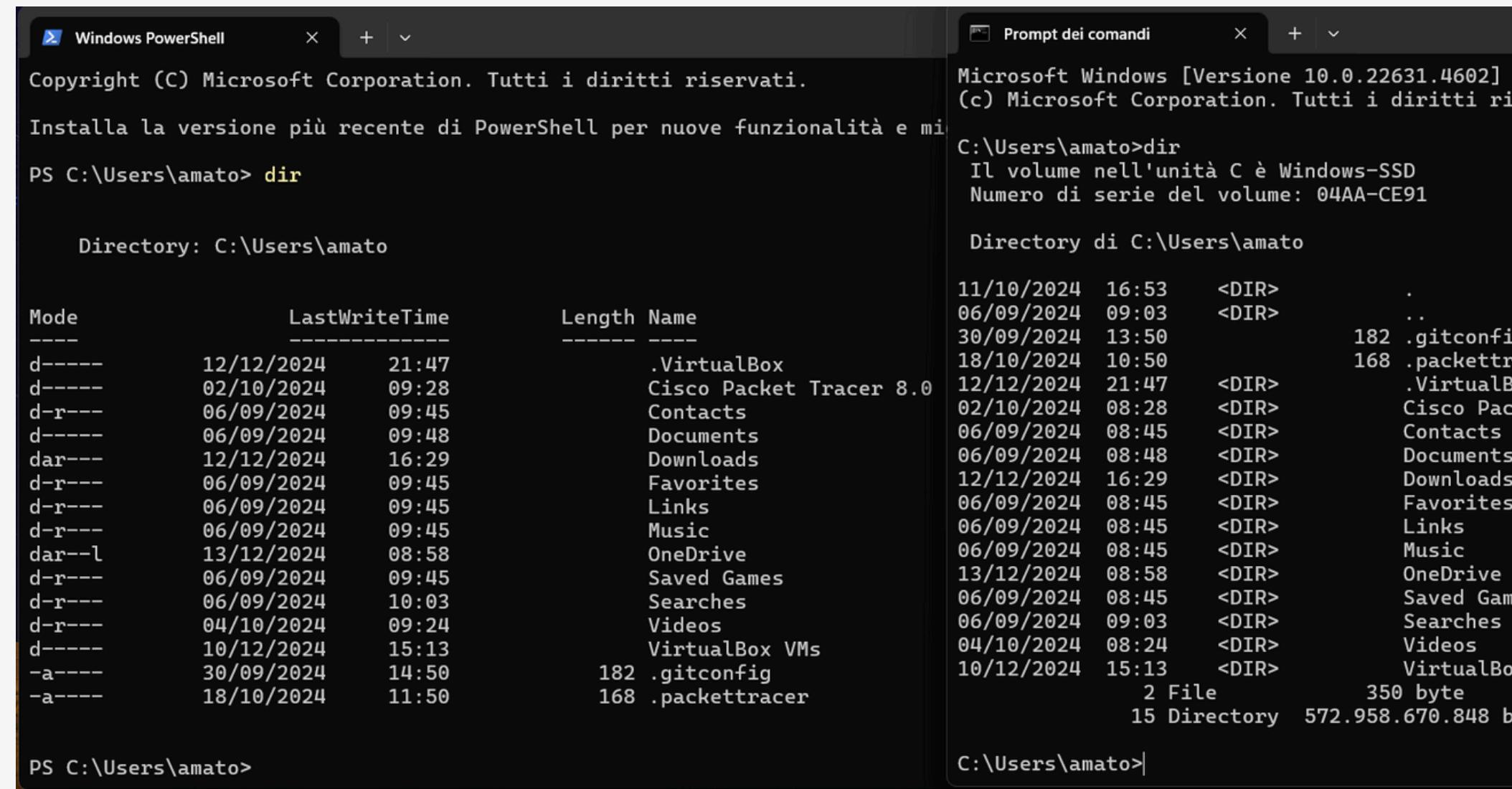


# ESPLORARE I COMANDI DEL PROMPT DEI COMANDI E DI POWERSHELL

Una volta aperte entrambe le console, possiamo eseguire comandi di base come dir (per visualizzare i file e le cartelle) in entrambi gli ambienti.

- Prompt dei comandi: digitare dir per ottenere l'elenco delle cartelle e dei file.
- PowerShell: digitare dir mostra anche un elenco simile, ma con informazioni aggiuntive come attributi dei file, permessi e modalità.

Prova anche altri comandi, come ping, cd, o ipconfig, che producono risultati simili in entrambe le console. Tuttavia, PowerShell offre una maggiore flessibilità e opzioni per i comandi.



The screenshot shows two side-by-side command-line windows. The left window is titled "Windows PowerShell" and the right is titled "Prompt dei comandi". Both are running on Windows 10. In both windows, the command "dir" is run from the directory "C:\Users\amato". The output lists various files and folders in the directory, including ".VirtualBox", "Cisco Packet Tracer 8.0", "Contacts", "Documents", "Downloads", "Favorites", "Links", "Music", "OneDrive", "Saved Games", "Searches", "Videos", ".gitconfig", and ".packettracer". The PowerShell window provides more detailed information for each item, such as mode (d----, d---r, etc.), last write time, length, and name. The PowerShell window also shows the total number of files (2) and bytes (350), and the total number of directories (15) and bytes (572.958.670.848).

Mode	LastWriteTime	Length	Name
d----	12/12/2024 21:47		.VirtualBox
d----	02/10/2024 09:28		Cisco Packet Tracer 8.0
d-r--	06/09/2024 09:45		Contacts
d----	06/09/2024 09:48		Documents
dar---	12/12/2024 16:29		Downloads
d-r--	06/09/2024 09:45		Favorites
d-r--	06/09/2024 09:45		Links
d-r--	06/09/2024 09:45		Music
dar--l	13/12/2024 08:58		OneDrive
d-r--	06/09/2024 09:45		Saved Games
d-r--	06/09/2024 10:03		Searches
d-r--	04/10/2024 09:24		Videos
d----	10/12/2024 15:13		VirtualBox VMs
-a----	30/09/2024 14:50	182	.gitconfig
-a----	18/10/2024 11:50	168	.packettracer

## ESPLORARE I CMDLET DI POWERSHELL

PowerShell utilizza i cmdlet, comandi che sono scritti in modo verbale (verboso-sostantivo, come Get-ChildItem) per eseguire operazioni specifiche. Un esempio è il comando Get-Alias, che mostra gli alias di comandi. Ad esempio, eseguendo il comando:

`Get-Alias dir`

scopriremo che dir è un alias per il cmdlet Get-ChildItem. Questa è una caratteristica importante di PowerShell, poiché consente agli utenti di usare comandi familiari del Prompt dei comandi pur beneficiando delle potenzialità di PowerShell.

```
PS C:\Users\amato> Get-Alias dir
```

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

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

## USARE IL COMANDO NETSTAT CON POWERSHELL

Uno dei comandi avanzati in PowerShell è netstat, che mostra le connessioni di rete attive e altre informazioni utili. Per utilizzare netstat, possiamo eseguire diversi comandi:

- netstat -h: visualizza l'help di netstat.
- netstat -r: visualizza la tabella di routing IPv4.
- netstat -abn: mostra i dettagli delle connessioni TCP attive, inclusi protocollo, indirizzo locale/remoto, stato e PID (identificativo del processo).

Per eseguire questi comandi con privilegi di amministratore, è necessario avviare PowerShell come amministratore (cliccando con il tasto destro e selezionando "Esegui come amministratore").

```
PS C:\Users\amato> netstat -r
=====
Elenco interfacce
 5...0a 00 27 00 00 05 ....VirtualBox Host-Only Ethernet Adapter
17...d2 39 57 e7 56 0f ....Microsoft Wi-Fi Direct Virtual Adapter
10...f2 39 57 e7 56 0f ....Microsoft Wi-Fi Direct Virtual Adapter #2
14...d0 39 57 e7 56 0f ....Realtek RTL8852BE WiFi 6 802.11ax PCIe Adapter
15...d0 39 57 e7 56 10 ....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    192.168.1.1  192.168.1.9    50
    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     192.168.1.9    306
    192.168.1.9    255.255.255.255  On-link     192.168.1.9    306
  192.168.1.255  255.255.255.255  On-link     192.168.1.9    306
    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     192.168.1.9    306
  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     192.168.1.9    306
=====

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
```

# USARE IL COMANDO NETSTAT CON POWERSHELL

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

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

NETSTAT[-a] [-b] [-e] [-f] [-i] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [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.
-i      Visualizza il tempo trascorso da una connessione TCP nel suo stato corrente.
-n      Visualizza indirizzi e numeri di porta in forma numerica.
-o      Visualizza l'ID del processo proprietario associato a ogni connessione.
-p proto Visualizza le connessioni relative al protocollo specificato da "proto",
       che può essere TCP, UDP, TCPv6 o UDPv6. Se utilizzato insieme all'opzione -s
       per le statistiche per protocollo, "proto" può essere:
       IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
-q      Visualizza tutte le connessioni, le porte di ascolto
       e le porte TCP non di ascolto associate. Le porte non di ascolto associate possono essere associate o meno
       a una connessione attiva.
-r      Visualizza la tabella di routing.
-s      Visualizza le statistiche per protocollo. Per impostazione predefinita, vengono
       visualizzate le statistiche per IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP e UDPv6.
       Per specificare un sottoinsieme dei valori predefiniti, è possibile utilizzare l'opzione -p.
-t      Visualizza lo stato di offload della connessione corrente.
-x      Visualizza le connessioni, i listener e gli endpoint
       condivisi.
-y      Visualizza il modello di connessione TCP per tutte le connessioni.
Non può essere utilizzata in combinazione con le altre opzioni.
interval Ripete la visualizzazione delle statistiche selezionate, con una pausa di un numero di secondi
```

# USARE IL COMANDO NETSTAT CON POWERSHELL

The screenshot shows a Windows desktop environment. On the left, a dark-themed PowerShell window displays the output of the command `netstat -abno`. The output lists various network connections, mostly listening on port 0.0.0.0:0, with some entries indicating they are unable to retrieve ownership information. On the right, a light-themed Task Manager window titled "Gestione attività" is open, showing a list of processes. The "Dettagli" tab is selected, displaying columns for Nome (Name), PID (Process ID), Stato (Status), Nome utente (User Name), CPU (CPU usage), Memoria (Memory), and Architet... (Architecture). The list includes system processes like Interrupt sistema, Processo di inattività, System, Secure System, and numerous svchost.exe instances, along with other services and system components.

```
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   1624
  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   10992
  CDPSvc
  [svchost.exe]
  TCP    0.0.0.0:7680          0.0.0.0:0          LISTENING   1468
  Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:49664         0.0.0.0:0          LISTENING   1288
  [lsass.exe]
  TCP    0.0.0.0:49665         0.0.0.0:0          LISTENING   1180
  Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:49666         0.0.0.0:0          LISTENING   2268
  EventLog
  [svchost.exe]
  TCP    0.0.0.0:49667         0.0.0.0:0          LISTENING   3408
  Schedule
  [svchost.exe]
  TCP    0.0.0.0:49670         0.0.0.0:0          LISTENING   4148
  [spoolsv.exe]
  TCP    0.0.0.0:49672         0.0.0.0:0          LISTENING   1252
```

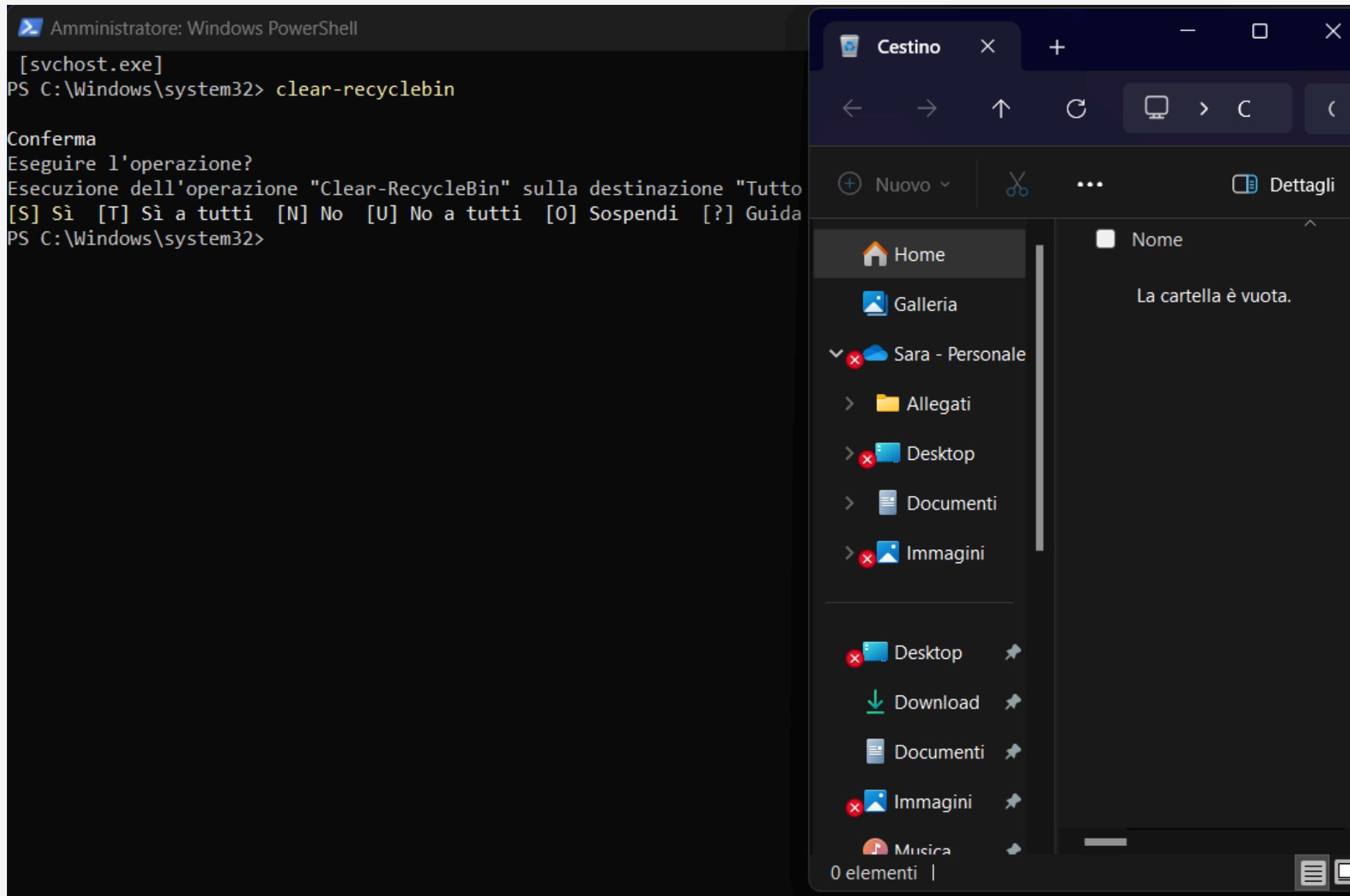
Nome	PID	Stato	Nome utente	CPU	Memoria (...)	Architet...
Interrupt sistema	-	In esec...	SYSTEM	00	0 K	
Processo di inattività	0	In esec...	SYSTEM	95	8 K	
System	4	In esec...	SYSTEM	00	12 K	
Secure System	140	In esec...	SYSTEM	00	47.976 K	
conhost.exe	148	In esec...	amato	00	472 K	x64
Registry	204	In esec...	SYSTEM	00	6.232 K	
FnHotkeyCapsLKNum...	364	In esec...	amato	00	700 K	x64
smss.exe	732	In esec...	SYSTEM	00	168 K	
RuntimeBroker.exe	872	In esec...	amato	00	1.564 K	x64
csrss.exe	1088	In esec...	SYSTEM	00	864 K	
wininit.exe	1180	In esec...	SYSTEM	00	324 K	
services.exe	1252	In esec...	SYSTEM	00	4.028 K	
Lsalso.exe	1272	In esec...	SYSTEM	00	496 K	x64
lsass.exe	1288	In esec...	SYSTEM	00	6.476 K	x64
svchost.exe	1300	In esec...	SYSTEM	00	21.116 K	x64
CiscoCollabHost.exe	1376	In esec...	amato	00	1.880 K	x64
svchost.exe	1468	In esec...	SERVIZIO D...	00	3.212 K	
svchost.exe	1492	In esec...	SYSTEM	00	10.040 K	x64
fontdrvhost.exe	1520	In esec...	UMFD-0	00	284 K	x64
explorer.exe	1612	In esec...	amato	00	161.592 K	x64
svchost.exe	1624	In esec...	SERVIZIO D...	00	9.336 K	x64
IntelCpHDCPSvc.exe	1640	In esec...	SYSTEM	00	400 K	x64
svchost.exe	1672	In esec...	SYSTEM	00	1.684 K	x64

# SVUOTARE IL CESTINO CON POWERSHELL

Un'altra funzionalità avanzata di PowerShell è la gestione dei file, come ad esempio svuotare il Cestino. Per farlo, possiamo eseguire il comando:

`clear-recyclebin`

Questo comando elimina definitivamente i file nel Cestino, una funzionalità utile per la gestione dello spazio di archiviazione. Dopo aver eseguito il comando, è possibile verificare che il Cestino sia effettivamente vuoto.



# Domanda di riflessione

Ricercando online, possiamo scoprire che PowerShell è utile anche per attività di analisi della sicurezza, come il monitoraggio delle connessioni di rete, la gestione dei log di sistema e l'automazione di task di sicurezza. Esempi di comandi utili includono:

- Get-EventLog: per raccogliere informazioni sui log di sistema.
- Get-NetTCPConnection: per monitorare le connessioni TCP attive.
- Get-WinEvent: per raccogliere eventi di sicurezza e sistema da Event Viewer.

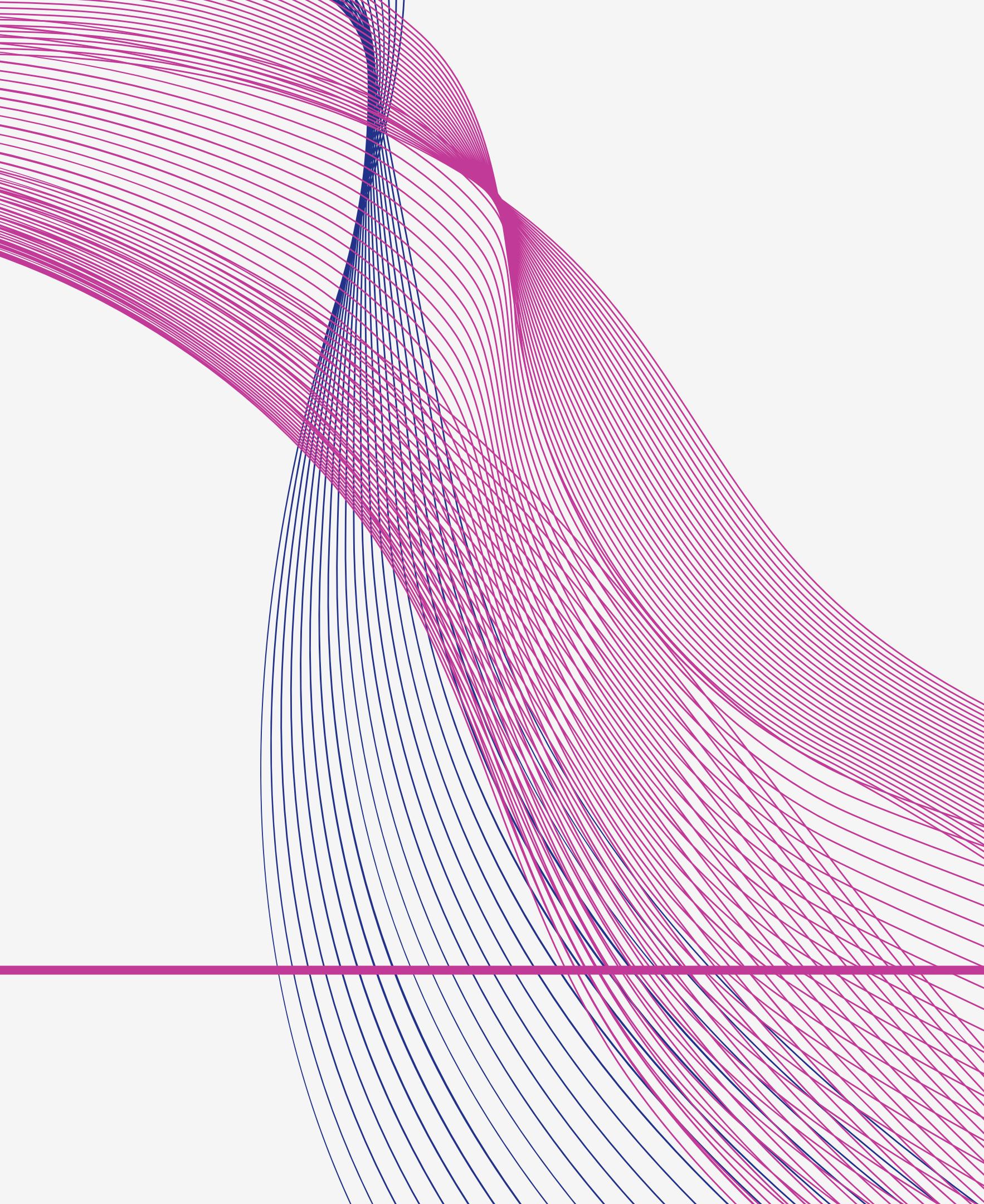
Questi comandi sono fondamentali per gli amministratori di sistema nella gestione della sicurezza e nella risposta agli incidenti.

# Conclusione

PowerShell è uno strumento molto potente e versatile per l'automazione e la gestione delle configurazioni in ambiente Windows. Ha una sintassi chiara e fornisce numerosi comandi e funzionalità avanzate che superano le capacità del Prompt dei comandi. Dall'esplorazione dei comandi di base all'automazione delle operazioni quotidiane, PowerShell offre agli amministratori di sistema un potente strumento per migliorare l'efficienza e la sicurezza operativa.

In conclusione, imparare ad utilizzare PowerShell in modo efficiente è essenziale per gestire ambienti Windows avanzati, automatizzare attività ripetitive e monitorare la sicurezza del sistema.

A large, abstract graphic element consisting of numerous thin, wavy lines in a muted purple color. These lines are densely packed in the lower half of the slide, creating a sense of depth and motion. They curve and overlap, forming a dynamic pattern that suggests data flow or complex system architecture. The lines transition into a more solid, darker purple shape towards the top right corner of the slide.



# CATTURA E ANALISI DEL TRAFFICO HTTP

- Introduzione
- Parte 1: Cattura e Analisi del Traffico HTTP
  - 1.1 Preparazione della cattura
  - 1.2 Generazione del traffico HTTP
  - 1.3 Analisi del traffico HTTP con Wireshark
- Parte 2: Cattura e Analisi del Traffico HTTPS
  - 2.1 Preparazione della cattura
  - 2.2 Generazione del traffico HTTPS
  - 2.3 Analisi del traffico HTTPS con Wireshark
- Riflessioni
- 4.1 Vantaggi di HTTPS rispetto a HTTP
- 4.2 I limiti della sicurezza HTTPS
- Conclusione

# Cattura e Analisi del Traffico HTTP

In questo laboratorio, esploreremo il traffico di rete generato tramite i protocolli HTTP e HTTPS. Utilizzeremo Wireshark per analizzare i pacchetti di rete e osservare le differenze tra il traffico criptato e quello non criptato. Comprendere queste differenze è essenziale per la sicurezza informatica, poiché i dati sensibili trasmessi su HTTP possono essere facilmente intercettati, mentre HTTPS fornisce una protezione criptata.

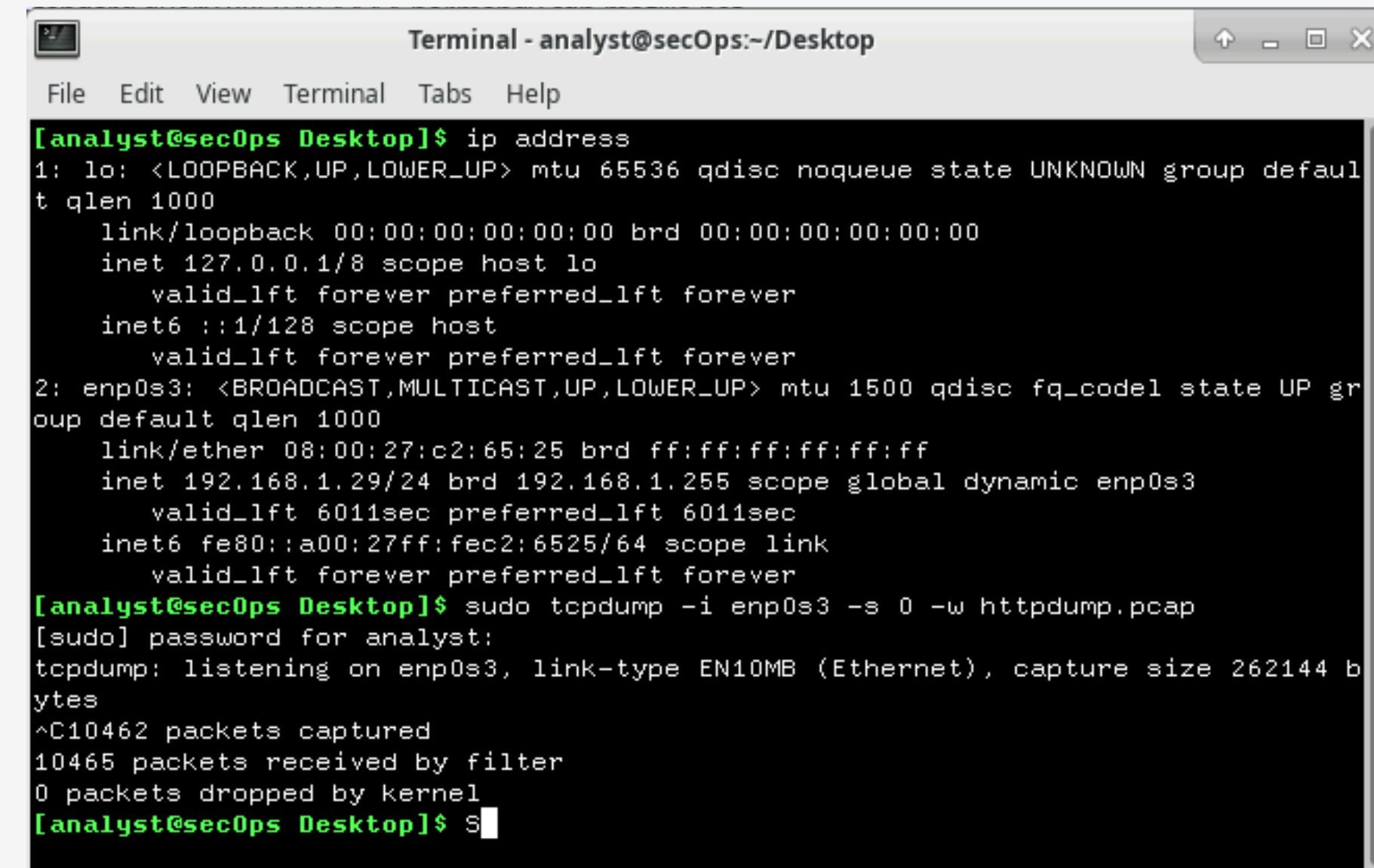
# CATTURA E ANALISI DEL TRAFFICO HTTP

## Preparazione della cattura

Per iniziare, avvia la cattura del traffico HTTP utilizzando tcpdump. Apri il terminale della macchina virtuale e usa il seguente comando:

```
sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
```

- -i enp0s3 indica l'interfaccia di rete da cui catturare il traffico (modifica questo parametro in base alla tua configurazione di rete).
- -s 0 cattura la dimensione completa del pacchetto.
- -w httpdump.pcap salva il traffico in un file .pcap.

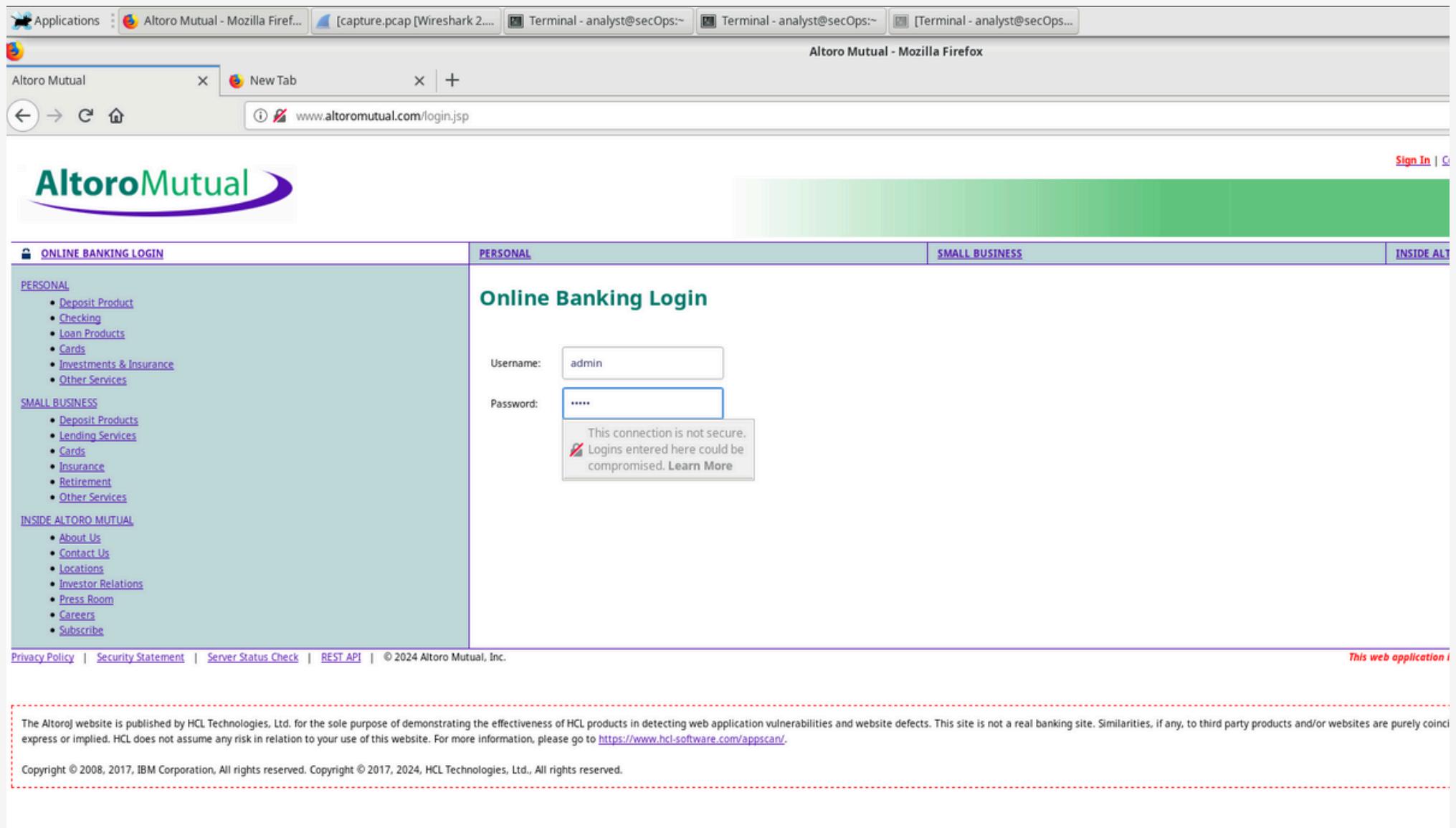


```
Terminal - analyst@secOps:~/Desktop
File Edit View Terminal Tabs Help
[analyst@secOps Desktop]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        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:c2:65:25 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.29/24 brd 192.168.1.255 scope global dynamic enp0s3
        valid_lft 6011sec preferred_lft 6011sec
    inet6 fe80::a00:27ff:fec2:6525/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps Desktop]$ 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
^C10462 packets captured
10465 packets received by filter
0 packets dropped by kernel
[analyst@secOps Desktop]$
```

# CATTURA E ANALISI DEL TRAFFICO HTTP

## Generazione del traffico HTTP

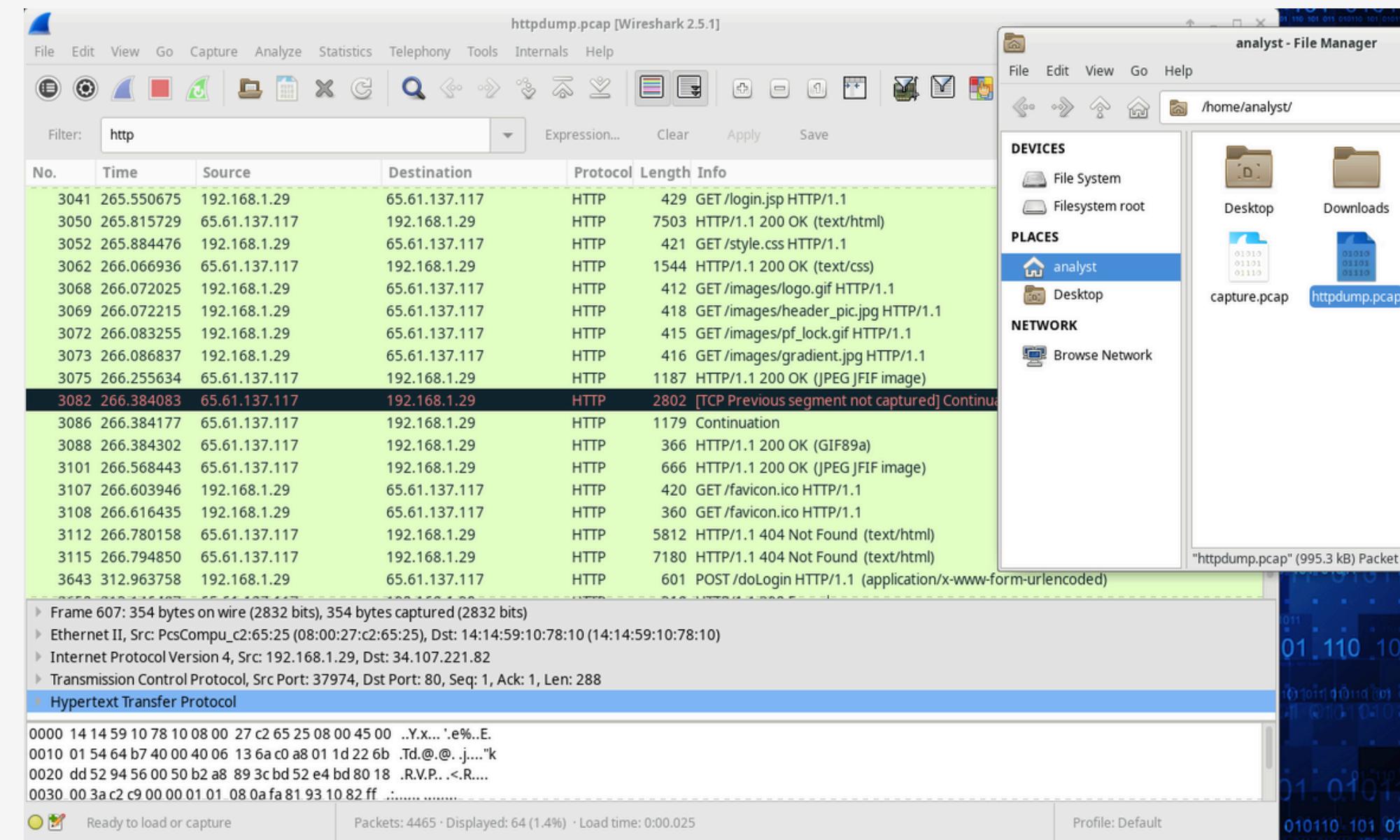
Apri il browser della VM e visita il sito <http://www.altoromutual.com/login.jsp>. Inserisci il nome utente e la password (Admin/Admin) per generare traffico HTTP non sicuro. Questo traffico sarà visibile nella cattura.



# CATTURA E ANALISI DEL TRAFFICO HTTP

## Analisi del traffico HTTP con Wireshark

Apri il file httpdump.pcap con Wireshark e filtra i pacchetti utilizzando il filtro http. Cerca i messaggi di tipo POST, che contengono i dati inviati dal browser. In Wireshark, osserva come le credenziali (username e password) sono visibili in chiaro, poiché il traffico non è criptato.



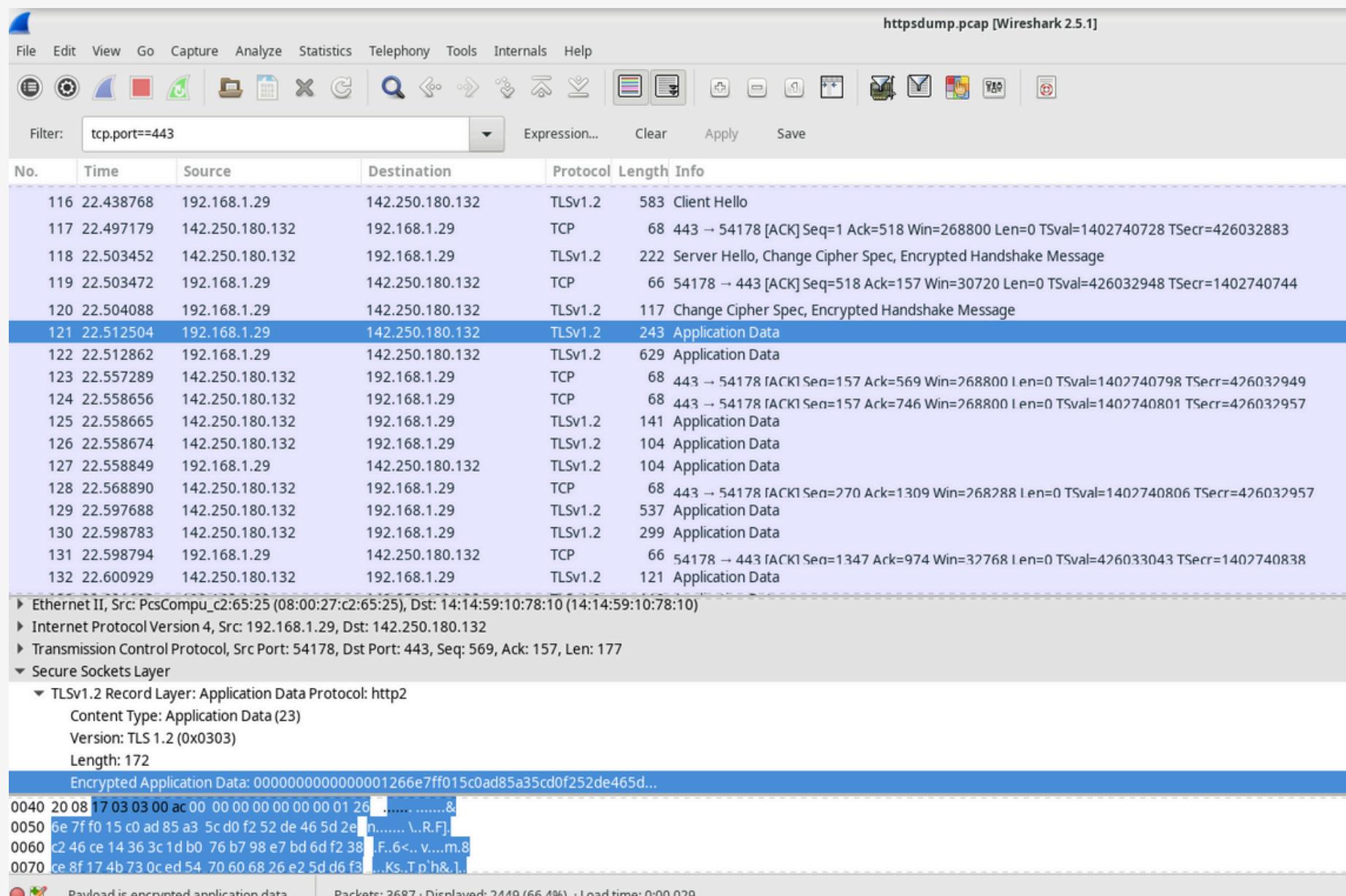
# CATTURA E ANALISI DEL TRAFFICO HTTPS

## Generazione del traffico HTTPS

Visita il sito <https://www.netacad.com> e accedi con le tue credenziali NetAcad. Questo traffico sarà sicuro grazie al protocollo HTTPS.

## Analisi del traffico HTTPS con Wireshark

Apri il file httpsdump.pcap con Wireshark e applica il filtro `tcp.port==443`, che è la porta standard per il traffico HTTPS. Nella sezione TLS/SSL, i dati saranno criptati e non leggibili, il che dimostra che il traffico è protetto da intercettazioni.



# Riflessioni

Vantaggi di HTTPS rispetto a HTTP

- Protezione da intercettazioni: HTTPS cifra i dati, rendendo difficile per un attaccante intercettare le informazioni trasmesse.
- Integrità dei dati: Previene modifiche ai dati durante la trasmissione, assicurando che ciò che viene inviato non venga alterato.

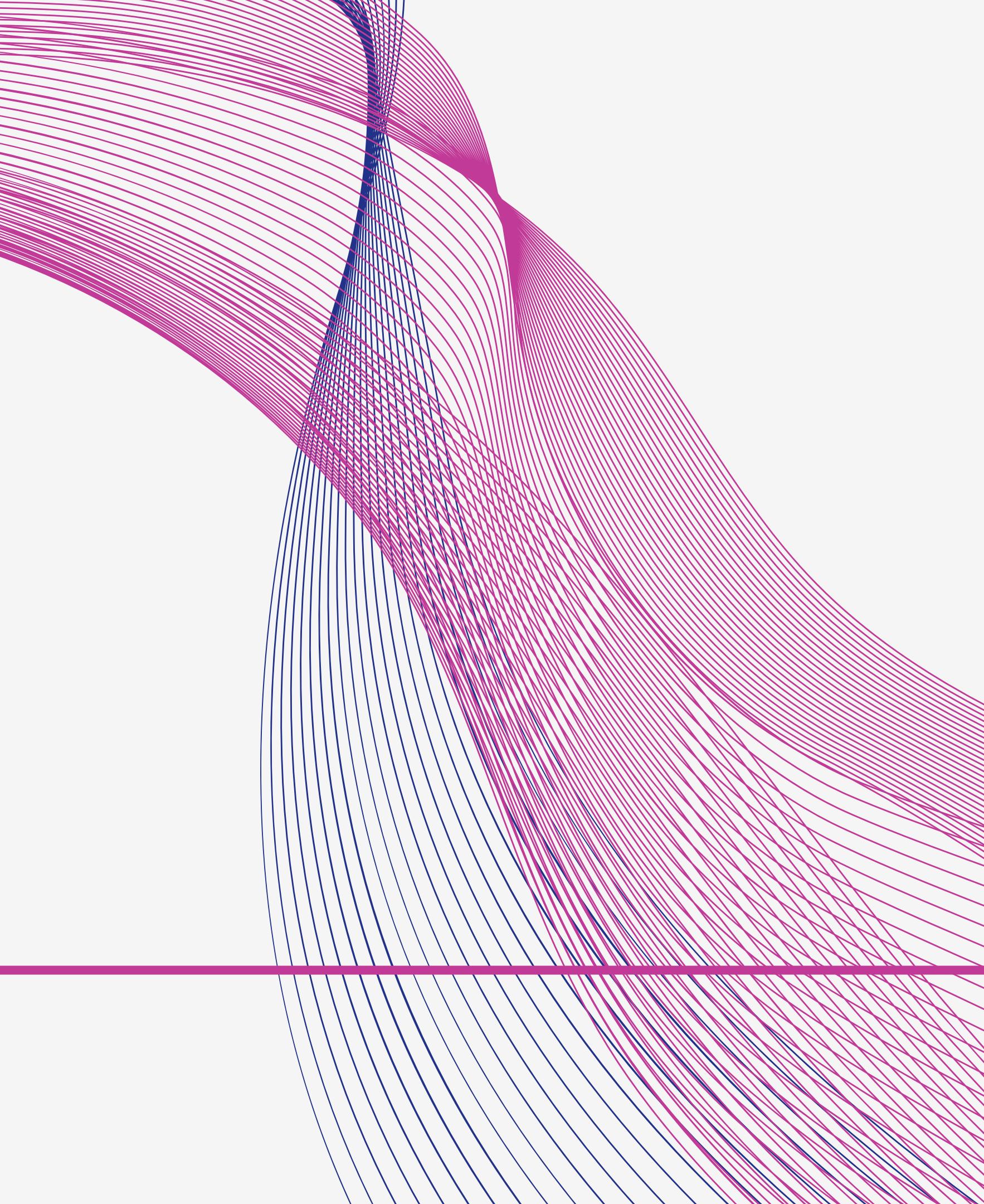
I limiti della sicurezza HTTPS

Nonostante HTTPS offre una protezione significativa, non è immune da attacchi. I criminali informatici possono configurare siti web con HTTPS fasulli, usando certificati SSL non validi per rubare dati sensibili degli utenti. Pertanto, HTTPS non garantisce una sicurezza assoluta.

# Conclusione

In questo laboratorio, abbiamo osservato come i dati trasmessi tramite HTTP sono vulnerabili a intercettazioni, mentre HTTPS fornisce una protezione criptata che assicura la riservatezza e l'integrità dei dati. Tuttavia, è importante ricordare che HTTPS da solo non è sufficiente a garantire la sicurezza, e l'adozione di misure aggiuntive come il controllo dei certificati SSL è fondamentale per prevenire attacchi.





# ESPLORAZIONE DI NMAP

---

- Introduzione
  - Parte 1: Esplorare Nmap
  - 1.1 Panoramica di Nmap
  - 1.2 Esplorazione della pagina man di Nmap
  - 1.3 Comando esempio: nmap -A -T4 scanme.nmap.org
  - Parte 2: Scansione di Porte Aperte
  - 2.1 Scansione del localhost
  - 2.2 Scansione della rete locale
  - 2.3 Scansione di un server remoto
  - Domande di Riflessione
  - Conclusione
-

# Esplorazione di Nmap

---

La scansione delle porte è una tecnica fondamentale utilizzata in fase di ricognizione per identificare le porte aperte e i servizi attivi su un host. In questo laboratorio, esploreremo l'uso di Nmap, uno degli strumenti più potenti e conosciuti per l'auditing della sicurezza e l'esplorazione delle reti.

# ESPLORARE NMAP

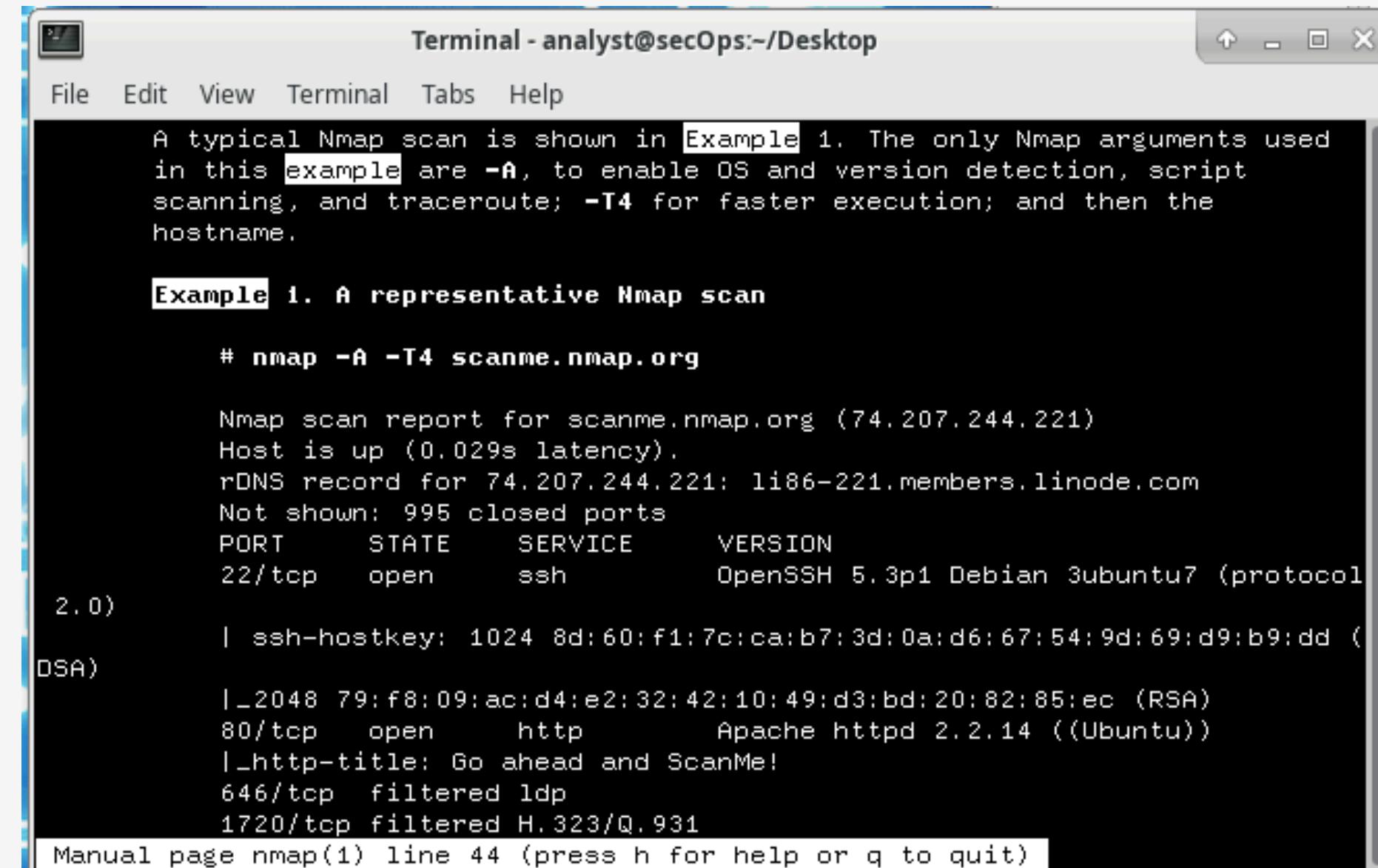
## Panoramica di Nmap

Nmap (Network Mapper) è uno strumento utilizzato per esplorare reti e scannerizzare porte, rilevando gli host attivi, i servizi disponibili e il sistema operativo in uso. È molto utilizzato in ambito di sicurezza per l'auditing delle reti.

[Esplorazione della pagina man di Nmap](#)  
Apri un terminale nella VM CyberOps Workstation e digita il comando:

**man nmap**

Questo comando mostra la documentazione di Nmap. Puoi navigare tra le pagine usando i tasti freccia e cercare termini specifici con /termine o ?termine.



The screenshot shows a terminal window titled "Terminal - analyst@secOps:~/Desktop". The window contains a command-line interface for the Nmap tool. At the top, there is a menu bar with options: File, Edit, View, Terminal, Tabs, Help. Below the menu, a message reads: "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." This is followed by a section titled "Example 1. A representative Nmap scan". The command entered is "# nmap -A -T4 scanme.nmap.org". The output of the scan is displayed, showing the host is up with 0.029s latency, an rDNS record for 74.207.244.221, and various open ports including 22/tcp (ssh), 80/tcp (http), and 646/tcp (filtered). The output concludes with "Manual page nmap(1) line 44 (press h for help or q to quit)".

# ESPLORARE NMAP

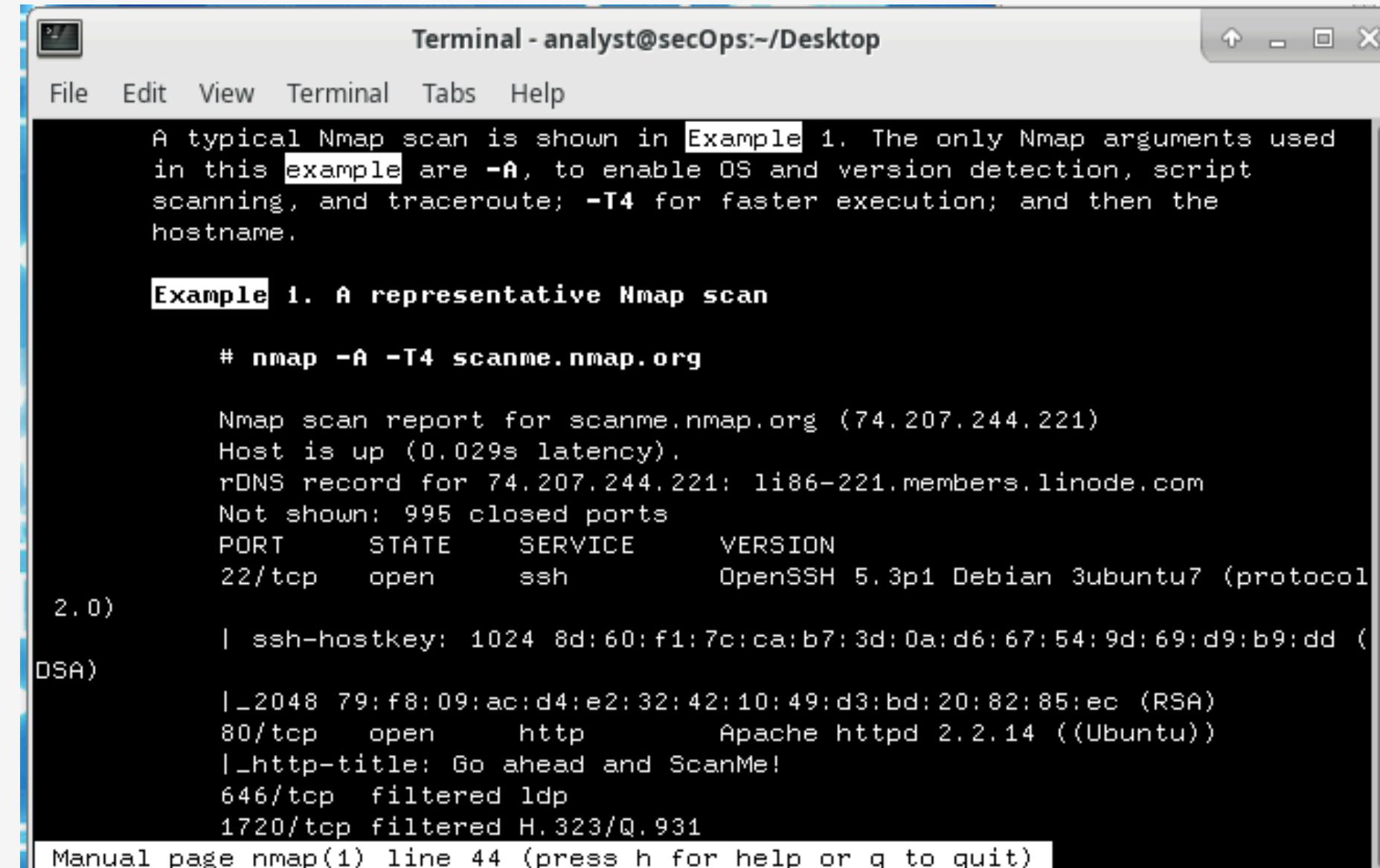
Comando esempio:

`nmap -A -T4 scanme.nmap.org`

Il comando nmap -A -T4 scanme.nmap.org esegue una scansione completa, rilevando il sistema operativo, la versione dei servizi e utilizzando i traceroute. La flag -T4 velocizza la scansione.

- -A: Rilevamento sistema operativo, versioni, script e traceroute.
- -T4: Velocizzazione della scansione, limitando i ritardi di scansione.

Esplora la pagina man per ulteriori dettagli e digita q per uscire.



The terminal window title is "Terminal - analyst@secOps:~/Desktop". The menu bar includes File, Edit, View, Terminal, Tabs, and Help. The main text area displays the following Nmap scan output:

```
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).
rDNS record for 74.207.244.221: 1186-221.members.linode.com
Not shown: 995 closed ports
PORT      STATE     SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 5.3p1 Debian 3ubuntu7 (protocol
                               2.0)
          | ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
          |_2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp    open      http         Apache httpd 2.2.14 ((Ubuntu))
          |_http-title: Go ahead and ScanMe!
646/tcp   filtered  ldp
1720/tcp  filtered H.323/Q.931

Manual page nmap(1) line 44 (press h for help or q to quit)
```

# SCANSIONE DI PORTE APERTE

## Scansione del localhost

Apri un terminale e digita:

nmap -A -T4 localhost

Esempio di output:

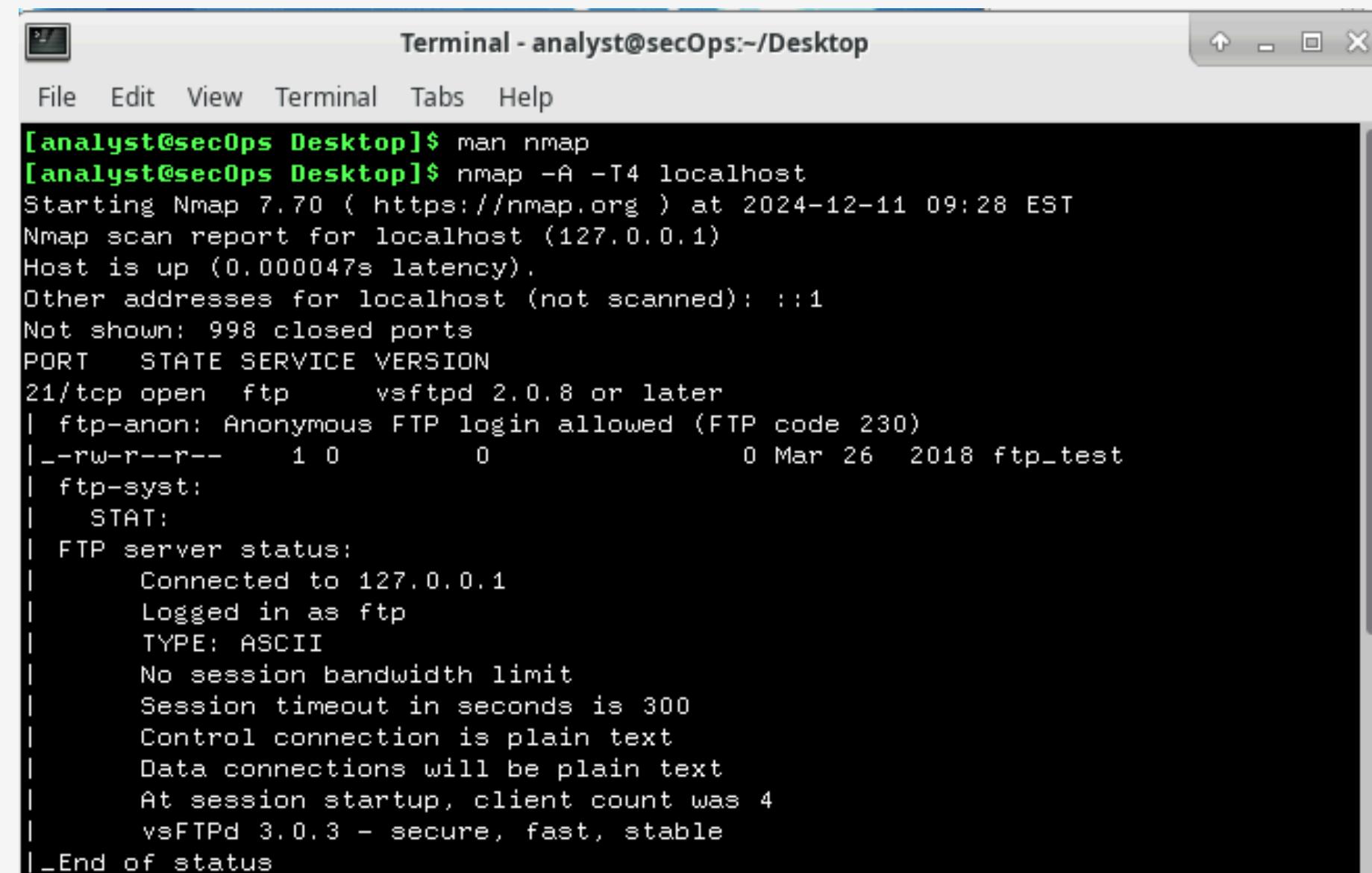
PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.0.8 or later

22/tcp open ssh OpenSSH

Domande:

- Quali porte e servizi sono aperti?
- Risposta: Porte 21/tcp (ftp) e 22/tcp (ssh).
- Quale software fornisce i servizi?
- Risposta: vsftpd per ftp e OpenSSH per ssh.



The screenshot shows a terminal window titled "Terminal - analyst@secOps:~/Desktop". The window contains the following text:

```
[analyst@secOps Desktop]$ man nmap
[analyst@secOps Desktop]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-11 09:28 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000047s 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
```

# SCANSIONE DI PORTE APERTE

## Scansione della rete locale

Determinare l'indirizzo IP della macchina con:

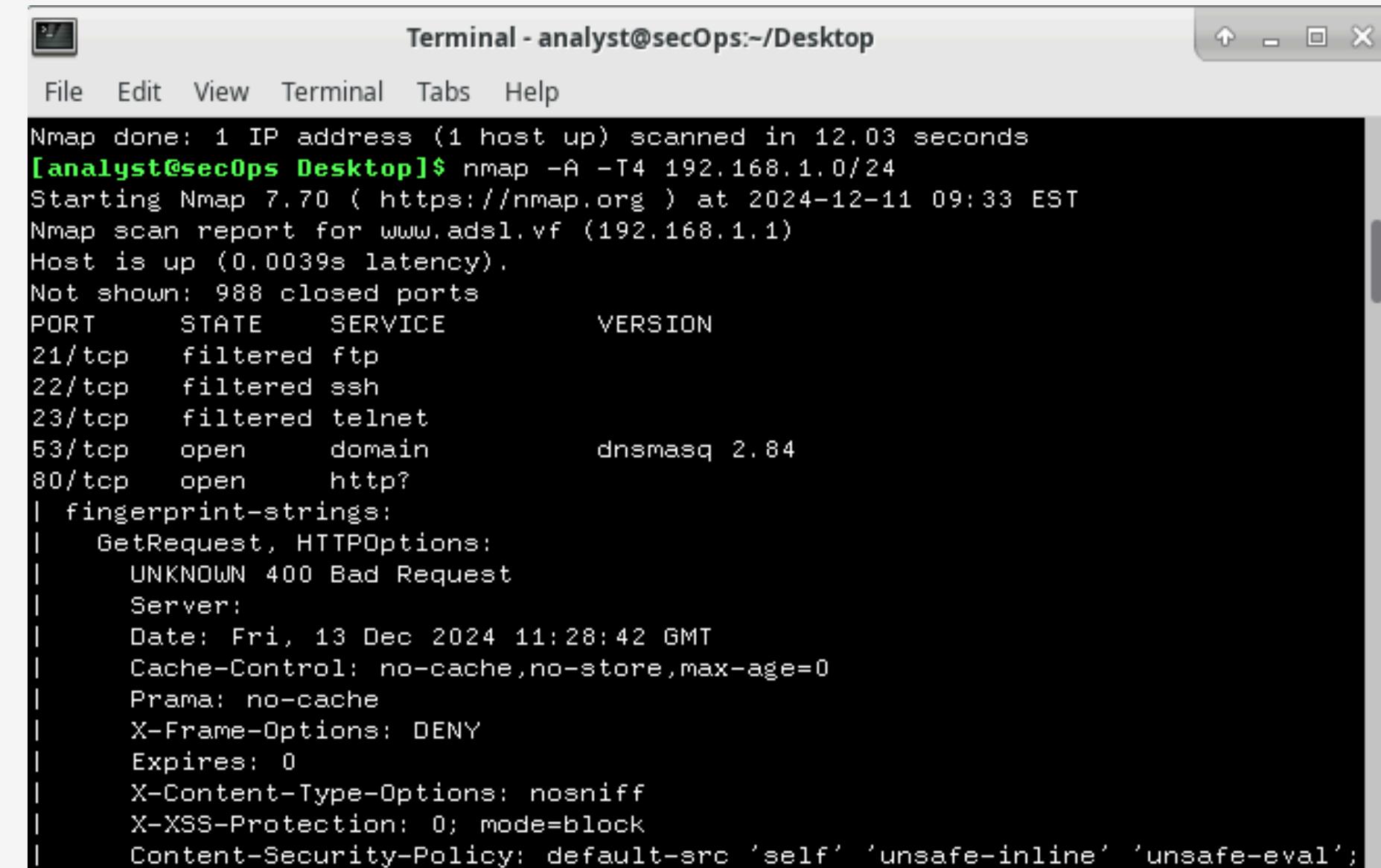
ip address

Esegui una scansione della rete locale con:

**nmap -A -T4 192.168.1.0/24**

Domande:

- Quanti host sono attivi?
- Risposta: Varie risposte, dipende dalla rete.
- Quali indirizzi IP e servizi sono stati rilevati?
- Risposta: Dipende dagli host attivi sulla LAN.



The screenshot shows a terminal window titled "Terminal - analyst@secOps:~/Desktop". The window contains the output of an Nmap scan. The output includes the following information:

```
Nmap done: 1 IP address (1 host up) scanned in 12.03 seconds
[analyst@secOps Desktop]$ nmap -A -T4 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-11 09:33 EST
Nmap scan report for www.adsl.vf (192.168.1.1)
Host is up (0.0039s latency).
Not shown: 988 closed ports
PORT      STATE     SERVICE          VERSION
21/tcp    filtered  ftp
22/tcp    filtered  ssh
23/tcp    filtered  telnet
53/tcp    open      domain          dnsmasq 2.84
80/tcp    open      http?
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     UNKNOWN 400 Bad Request
|   Server:
|     Date: Fri, 13 Dec 2024 11:28:42 GMT
|     Cache-Control: no-cache,no-store,max-age=0
|     Pragma: no-cache
|     X-Frame-Options: DENY
|     Expires: 0
|     X-Content-Type-Options: nosniff
|     X-XSS-Protection: 0; mode=block
|     Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval';
```

# SCANSIONE DI PORTE APERTE

## Scansione della rete locale

Determinare l'indirizzo IP della macchina con:

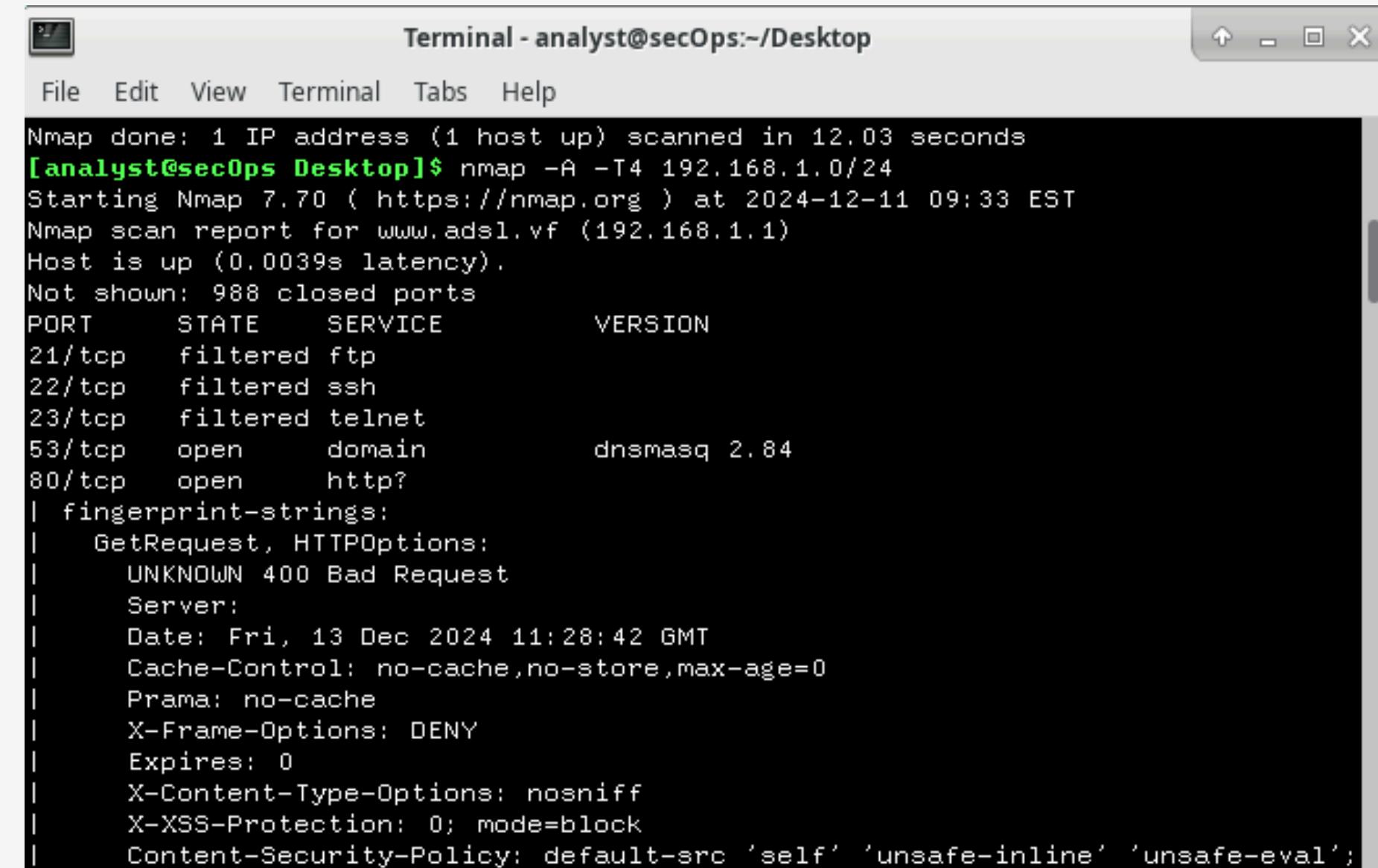
ip address

Esegui una scansione della rete locale con:

**nmap -A -T4 192.168.1.0/24**

Domande:

- Quanti host sono attivi?
- Risposta: Varie risposte, dipende dalla rete.
- Quali indirizzi IP e servizi sono stati rilevati?
- Risposta: Dipende dagli host attivi sulla LAN.



The screenshot shows a terminal window titled "Terminal - analyst@secOps:~/Desktop". The window contains the output of an Nmap scan. The output includes the following information:

```
Nmap done: 1 IP address (1 host up) scanned in 12.03 seconds
[analyst@secOps Desktop]$ nmap -A -T4 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-11 09:33 EST
Nmap scan report for www.adsl.vf (192.168.1.1)
Host is up (0.0039s latency).
Not shown: 988 closed ports
PORT      STATE     SERVICE          VERSION
21/tcp    filtered  ftp
22/tcp    filtered  ssh
23/tcp    filtered  telnet
53/tcp    open      domain          dnsmasq 2.84
80/tcp    open      http?
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     UNKNOWN 400 Bad Request
|   Server:
|     Date: Fri, 13 Dec 2024 11:28:42 GMT
|     Cache-Control: no-cache,no-store,max-age=0
|     Pragma: no-cache
|     X-Frame-Options: DENY
|     Expires: 0
|     X-Content-Type-Options: nosniff
|     X-XSS-Protection: 0; mode=block
|     Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval';
```

# SCANSIONE DI PORTE APERTE

## Scansione di un server remoto

Visita il sito [scanme.nmap.org](http://scanme.nmap.org) e scansiona con:

**nmap -A -T4 scanme.nmap.org**

Esempio di output:

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 6.6.180
6.6.180/tcp	open	http	Apache httpd 2.4.7

Domande:

- Quali porte e servizi sono aperti?
- Risposta: 22/tcp (ssh), 80/tcp (http).
- Quali porte e servizi sono filtrati?
- Risposta: 135/tcp (msrpc), 139/tcp (netbios-ssn).
- Qual è l'indirizzo IP del server?
- Risposta: 45.33.32.156.
- Qual è il sistema operativo?
- Risposta: Ubuntu Linux.

The screenshot shows a terminal window titled "Terminal - analyst@secOps:~/Desktop". The window contains the output of an Nmap scan. The output includes the following information:

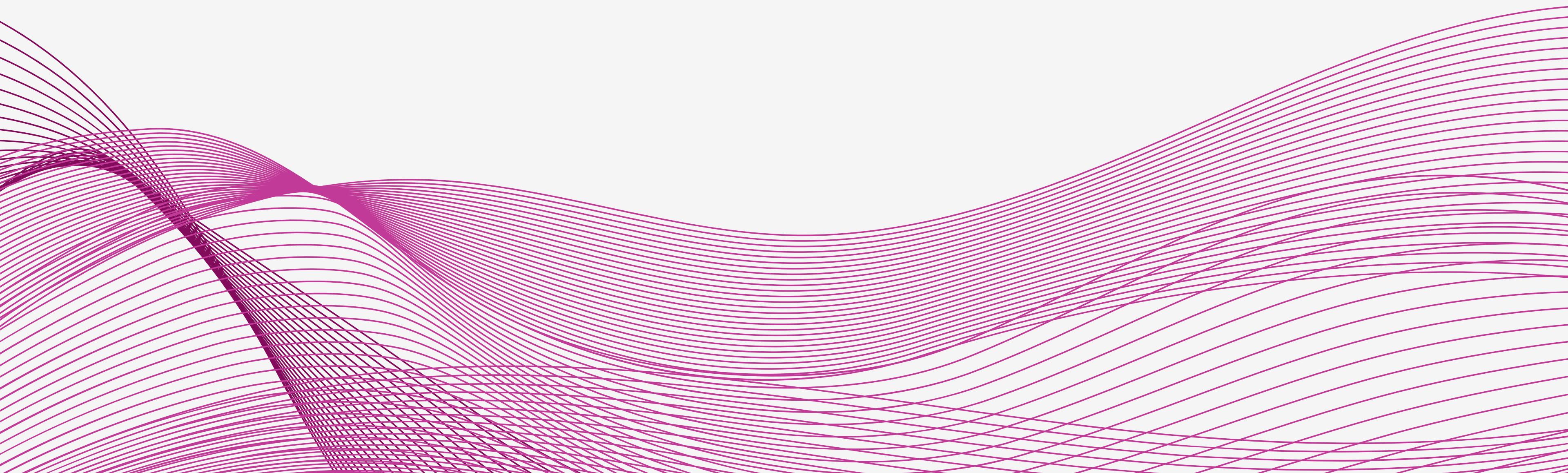
```
Nmap done: 1 IP address (1 host up) scanned in 12.03 seconds
[analyst@secOps Desktop]$ nmap -A -T4 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-11 09:33 EST
Nmap scan report for www.adsl.vf (192.168.1.1)
Host is up (0.0039s latency).
Not shown: 988 closed ports
PORT      STATE      SERVICE          VERSION
21/tcp    filtered  ftp
22/tcp    filtered  ssh
23/tcp    filtered  telnet
53/tcp    open       domain          dnsmasq 2.84
80/tcp    open       http?
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     UNKNOWN 400 Bad Request
|   Server:
|     Date: Fri, 13 Dec 2024 11:28:42 GMT
|     Cache-Control: no-cache,no-store,max-age=0
|     Prama: no-cache
|     X-Frame-Options: DENY
|     Expires: 0
|     X-Content-Type-Options: nosniff
|     X-XSS-Protection: 0; mode=block
|     Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval';
```

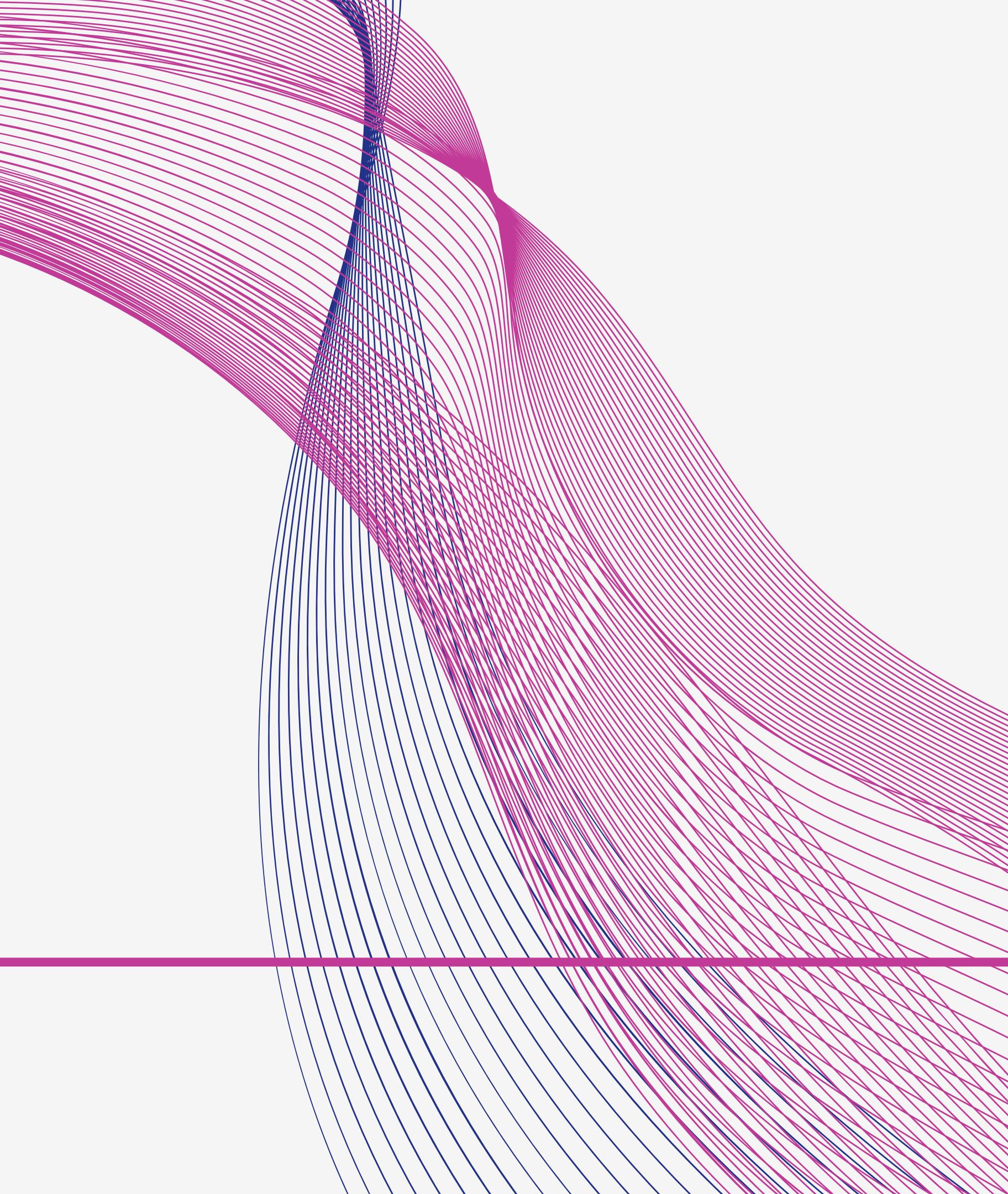
# Riflessioni

- Come può Nmap aiutare nella sicurezza delle reti? Risposta: Nmap è utile per identificare vulnerabilità, porte aperte e servizi non autorizzati, contribuendo a migliorare la sicurezza della rete.
- Come può essere usato da un attore malevolo? Risposta: Un attaccante potrebbe usare Nmap per raccogliere informazioni sulla rete, identificando porte aperte e vulnerabilità per pianificare futuri attacchi.

# Conclusione

Nmap è uno strumento fondamentale per la sicurezza delle reti. Consente di identificare host attivi, porte aperte e vulnerabilità, essendo utile sia per l'amministrazione della rete che per i test di penetrazione. Tuttavia, come tutti gli strumenti potenti, può essere usato anche in modo malevolo, quindi è essenziale monitorare e proteggere la rete da scansioni non autorizzate.





# ANALISI DI UN ATTACCO SQL INJECTION

- Introduzione
- Parte 1: Aprire Wireshark e Caricare il File PCAP
- Parte 2: Analizzare l'Inizio dell'Attacco SQL Injection
- Parte 3: Continuazione dell'Attacco SQL Injection
- Parte 4: L'Attacco SQL Injection Fornisce Informazioni di Sistema
- Parte 5: Informazioni sulle Tabelle Tramite SQL Injection
- Parte 6: Conclusione dell'Attacco SQL Injection
- Domande di Riflessione
- Conclusione

# **Analisi di un attacco SQL Injection**

Gli attacchi SQL Injection rappresentano una delle minacce più comuni per la sicurezza delle applicazioni web. Essi sfruttano vulnerabilità nei sistemi che non filtrano correttamente i dati immessi dall'utente, permettendo a un attaccante di manipolare le query SQL per accedere e alterare i dati nel database.

In questo laboratorio, esplorerai un attacco SQL Injection analizzando il traffico di rete catturato in un file PCAP. Esaminerai come l'attacco si sviluppa e come raccogliere informazioni sensibili dai sistemi vulnerabili.

# APRIRE WIRESHARK E CARICARE IL FILE PCAP

Wireshark è uno strumento di analisi del traffico di rete che ti permette di osservare il traffico in tempo reale o analizzare file PCAP.

1. Avvia la VM CyberOps Workstation.
2. Apri Wireshark dal menu Applicazioni > CyberOPS > Wireshark.
3. Clicca su Open e naviga nella directory /home/analyst/.
4. Seleziona il file SQL\_Lab.pcap per caricare il traffico relativo all'attacco SQL Injection.

Domanda:

Quali sono i due indirizzi IP coinvolti in questo attacco SQL Injection?

Risposta: Gli indirizzi IP coinvolti sono 10.0.2.15 (attaccante) e 10.0.2.20 (target).

The screenshot shows the Wireshark interface with the title bar "SQL\_Lab.pcap [Wireshark 2.5.1]". The main window displays a list of network frames. The first frame (Frame 1) is highlighted in blue and expanded in the bottom pane, showing details about the Ethernet II frame, Internet Protocol Version 4, and Transmission Control Protocol.

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
2	0.000315	10.0.2.15	10.0.2.4	TCP	74	80 → 35614 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=38535
3	0.000349	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=45838 TSecr=38535
4	0.000681	10.0.2.4	10.0.2.15	HTTP	654	POST /dvwa/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=30208 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	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=589 Ack=365 Win=30336 Len=0 TSval=45840 TSecr=38536
8	0.014383	10.0.2.4	10.0.2.15	HTTP	496	GET /dvwa/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 /dvwa/dvwa/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 /dvwa/vulnerabilities/sqlinjection/?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 TSval=82101 TSecr=98114
15	174.257989	10.0.2.15	10.0.2.4	HTTP	1861	HTTP/1.1 200 OK (text/html)

# APRIRE WIRESHARK E CARICARE IL FILE PCAP

## Analizzare l'Inizio dell'Attacco SQL Injection

- 1.In Wireshark, fai clic destro sulla linea 13 e seleziona Follow > HTTP Stream.
- 2.Inserisci 1=1 nel campo di ricerca e clicca su Find Next.
- 3.L'aggressore inserisce una query 1=1 nella casella di ricerca "UserID" del target 10.0.2.15. La query 1=1 è sempre vera, il che consente all'attaccante di manipolare i dati.

Domanda:

Qual è l'indirizzo IP del target e cosa indica la risposta del database?

Risposta: L'indirizzo IP del target è 10.0.2.15. La risposta del database indica che l'attacco ha avuto successo, mostrando un record invece di un messaggio di errore.

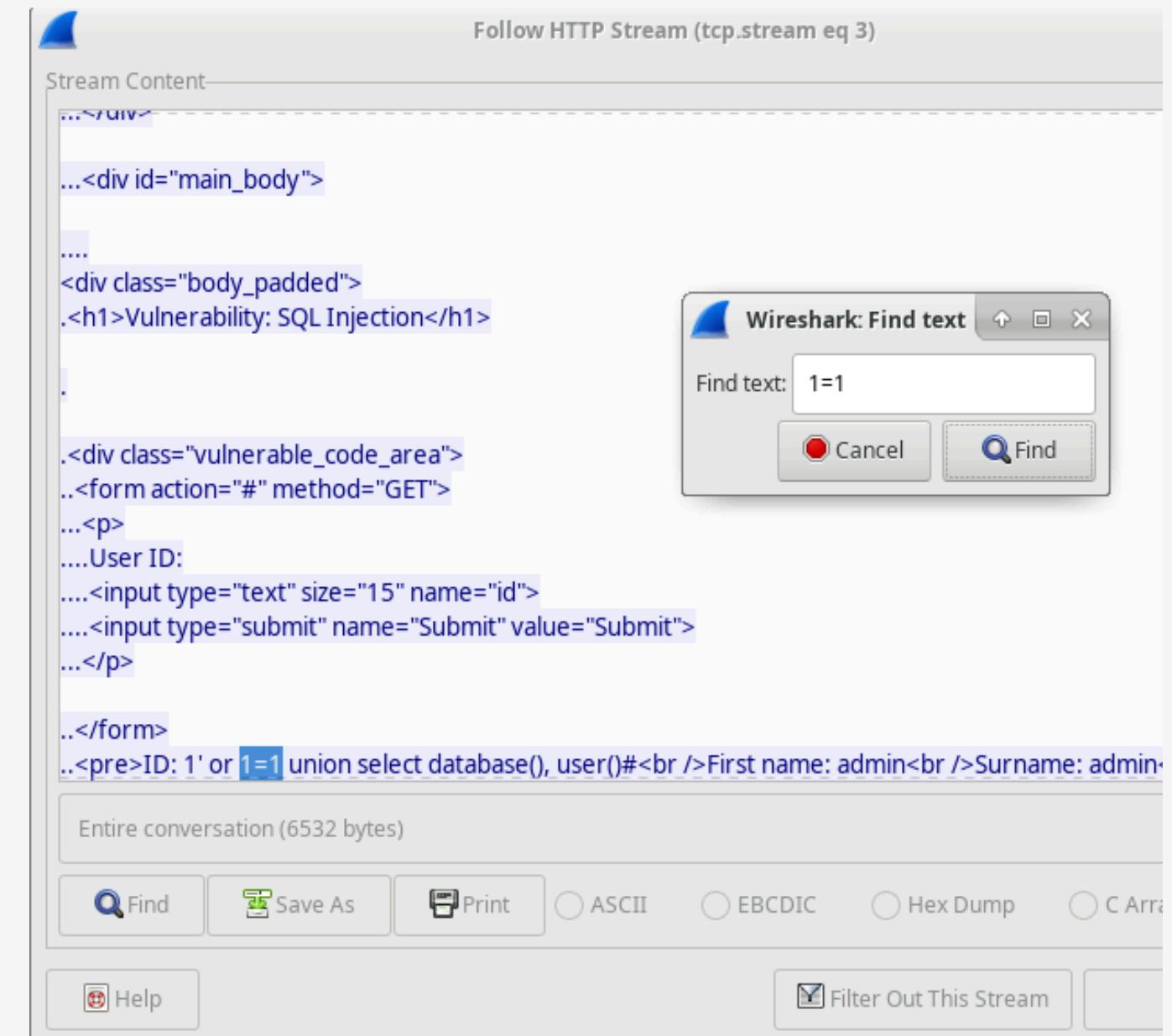
## Continuazione dell'Attacco SQL Injection

- 1.Fai clic destro sulla linea 19 e seleziona Follow > HTTP Stream.
- 2.Inserisci la query 1' or 1=1 union select database(), user()# nel campo di ricerca.
- 3.La risposta include:
  - Nome del database: dvwa
  - Utente del database: root@localhost

Domanda:

Quali informazioni sono state ottenute durante questa parte dell'attacco?

Risposta: Il nome del database è dvwa e l'utente del database è root@localhost.



# APRIRE WIRESHARK E CARICARE IL FILE PCAP

## L'Attacco SQL Injection Fornisce Informazioni di Sistema

- 1.Fai clic destro sulla linea 22 e seleziona Follow > HTTP Stream.
- 2.Inserisci la query 1' or 1=1 union select null, version()# nel campo di ricerca.
- 3.La risposta mostra la versione di MySQL:
  - Versione MySQL: 5.7.12-0

Domanda:

Cosa farebbe la query 1' OR 1=1 UNION SELECT null, column\_name FROM INFORMATION\_SCHEMA.columns WHERE table\_name='users'?

Risposta: Il database risponderebbe con i nomi delle colonne della tabella users.

## Informazioni sulle Tabelle Tramite SQL Injection

- 1.Fai clic destro sulla linea 25 e seleziona Follow > HTTP Stream.
- 2.Inserisci users nel campo di ricerca.
- 3.L'aggressore inserisce la query 1' or 1=1 union select null, table\_name from information\_schema.tables# per visualizzare tutte le tabelle del database.

Domanda:

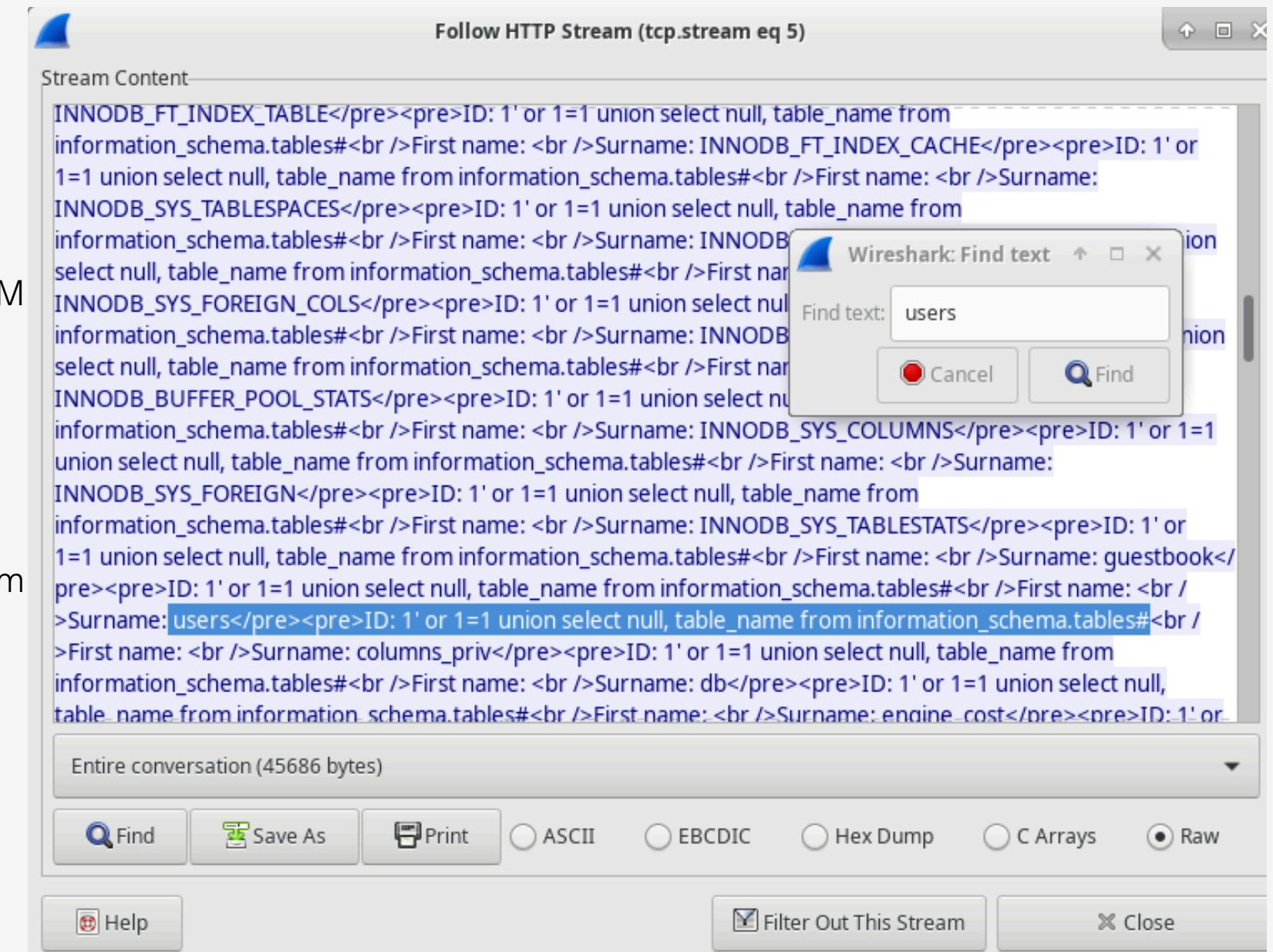
Quale utente ha l'hash della password 8d3533d75ae2c3966d7e0d4fcc69216b?

Risposta: L'utente con l'hash della password è 1337.

Domanda:

Qual è la password in chiaro per l'hash 8d3533d75ae2c3966d7e0d4fcc69216b?

Risposta: La password in chiaro è charley.



# APRIRE WIRESHARK E CARICARE IL FILE PCAP

## Conclusione dell'Attacco SQL Injection

- 1.Fai clic destro sulla linea 28 e seleziona Follow > HTTP Stream.
- 2.L'aggressore inserisce la query 1'or 1=1 union select user, password from users# per ottenere i nomi utente e gli hash delle password.



# Riflessioni

Domanda:

Qual è il rischio dell'uso del linguaggio SQL sulle piattaforme web?

Risposta: L'uso non sicuro di SQL in applicazioni web espone i sistemi a vulnerabilità, come l'**SQL Injection**, che permette agli attaccanti di manipolare e accedere ai dati sensibili.

Domanda:

Quali sono due metodi per prevenire gli attacchi SQL Injection?

Risposta:

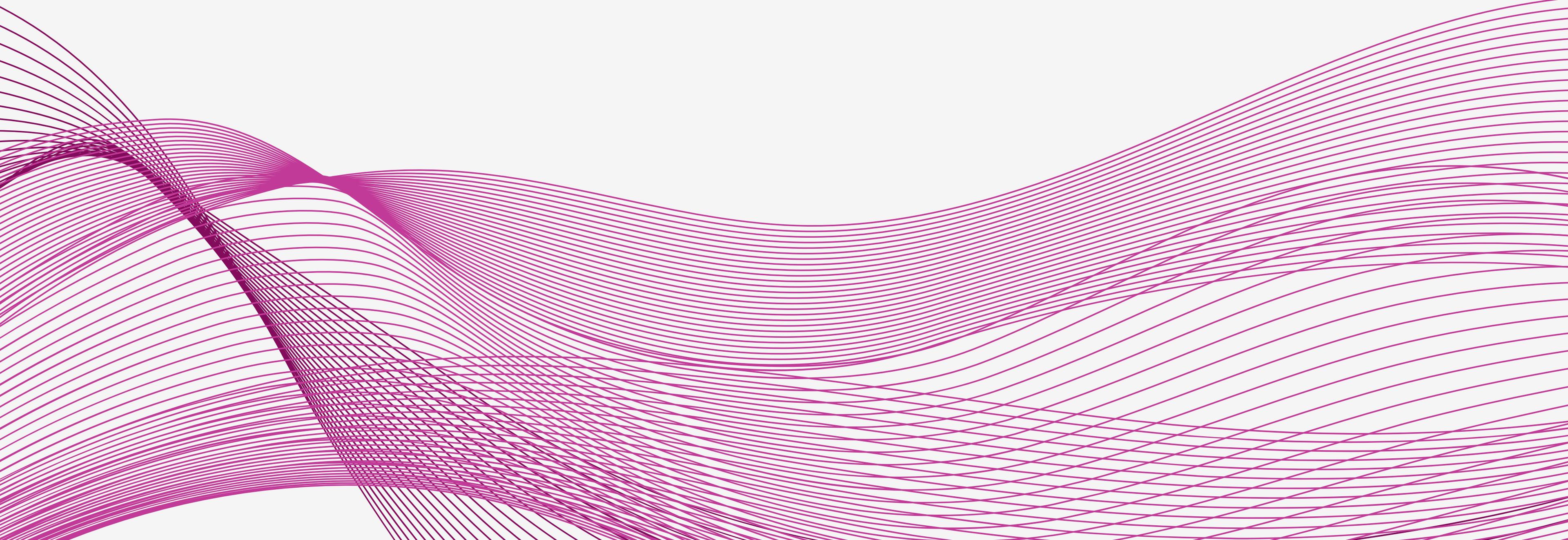
Filtrare l'input dell'utente.

Utilizzare parametri con procedure memorizzate.

Altri metodi includono implementare un firewall per applicazioni web, monitorare le istruzioni SQL e disabilitare funzionalità non necessarie nei database.

# Conclusione

Questo laboratorio ha illustrato come un attacco SQL Injection può essere analizzato tramite l'analisi di un file PCAP in Wireshark. Abbiamo visto come raccogliere informazioni critiche da un database vulnerabile e come prevenire questi attacchi mediante buone pratiche di sicurezza.



# CONCLUSIONI

---

L'integrazione di strumenti e tecniche avanzate come PowerShell, Nmap, Wireshark e l'analisi di SQL Injection dimostra quanto sia cruciale un approccio olistico alla sicurezza informatica e all'analisi delle reti. Queste quattro attività hanno evidenziato la sinergia tra automazione, analisi del traffico e rilevamento delle vulnerabilità per garantire la protezione e la resilienza delle infrastrutture IT.

L'uso di PowerShell ha mostrato come l'automazione possa non solo semplificare operazioni complesse, ma anche offrire un controllo preciso sulle risorse, aumentando l'efficienza operativa e riducendo i rischi legati all'errore umano.

L'esplorazione di reti con Nmap ha sottolineato l'importanza di una consapevolezza situazionale. Identificare host attivi, porte aperte e servizi in esecuzione è essenziale per prevenire attacchi mirati e rinforzare la sicurezza.

L'analisi del traffico HTTP con Wireshark ha dimostrato come il monitoraggio dei dati in transito possa fornire una visione dettagliata delle comunicazioni tra dispositivi, evidenziando attività sospette e rilevando vulnerabilità che potrebbero essere sfruttate dagli aggressori.

Infine, lo studio dell'attacco SQL Injection su un database MySQL ha evidenziato i rischi derivanti da una mancata validazione degli input utente. Comprendere le tecniche di attacco e la loro analisi tramite Wireshark permette non solo di rilevare incidenti di sicurezza, ma anche di definire strategie preventive come l'uso di query parametrizzate e la segmentazione dei privilegi.

Questi strumenti e approcci, se utilizzati con competenza e consapevolezza, offrono un potente arsenale per affrontare le sfide moderne della sicurezza informatica, proteggendo le reti da minacce esterne e prevenendo compromissioni di dati critici. L'applicazione combinata di queste conoscenze è la chiave per un ambiente IT sicuro e resiliente.

 Amato Sara

**GRAZIE**