

## Indice:

### Introduzione;

### Svolgimento PowerShell/Prompt;

Che cos'è PowerShell;

Che cos'è il prompt di Windows;

Pratica;

Conclusione;

### Svolgimento WireShark;

Che cosa sono i protocolli HTTP e HTTPS;

Pratica;

Conclusione;

## Introduzione:

Nel laboratorio di questa fine settimana, ci è stato dato come compito, quello di utilizzare **powershell** ed il **prompt** di windows e scoprire le funzioni di quest'ultimi;

E come secondo compito, quello di utilizzare **Wireshark** per esaminare il traffico **HTTP** e **HTTPS**;

## Svolgimento compito 1:

### Che cos'è PowerShell:

**PowerShell** è sia una console di comando che un linguaggio di scripting. PowerShell include inoltre funzionalità che permettono di creare script per automatizzare compiti e interagire con il sistema operativo Windows.

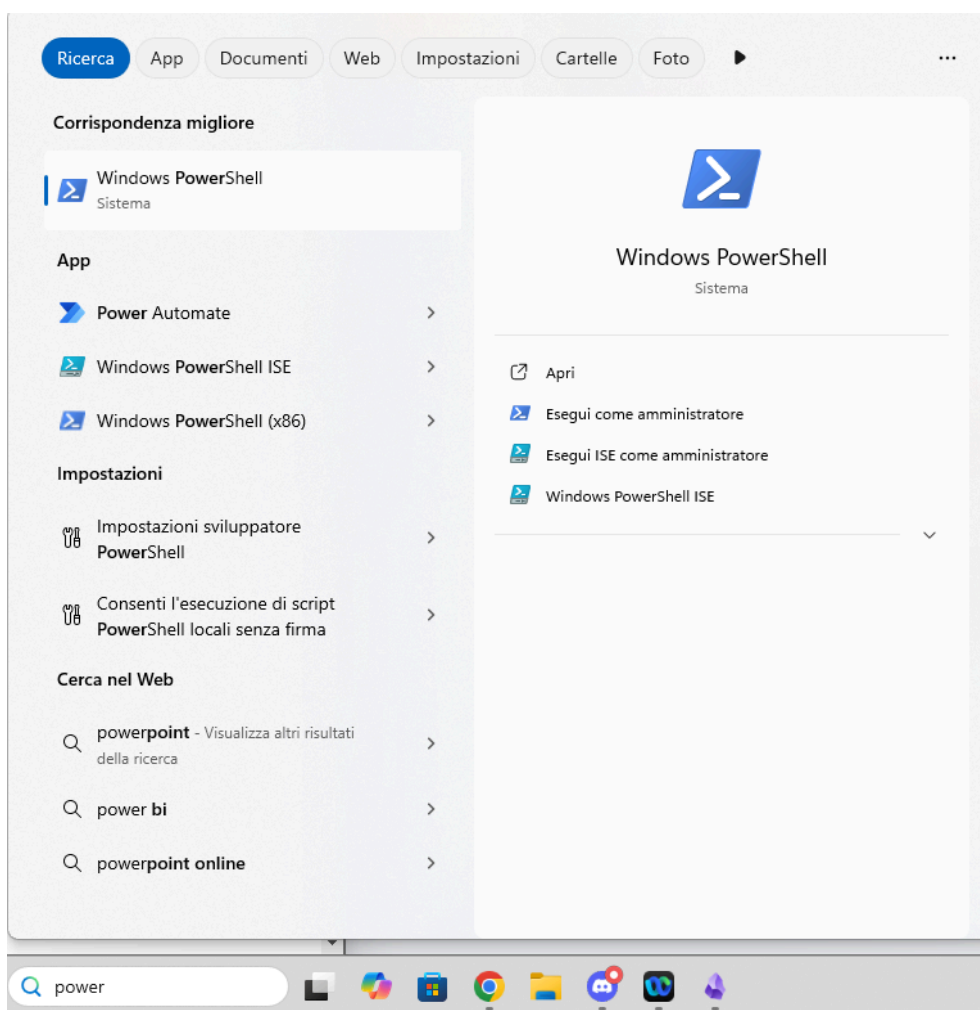
### Che cos'è il prompt di Windows:

Il **CMD** (prompt) di Windows è un'interfaccia a **riga di comando** che permette di interagire con il sistema operativo eseguendo comandi manualmente. Si usa per gestire operazioni di base, come file e configurazioni, ed è utile per risolvere problemi o automatizzare semplici attività.

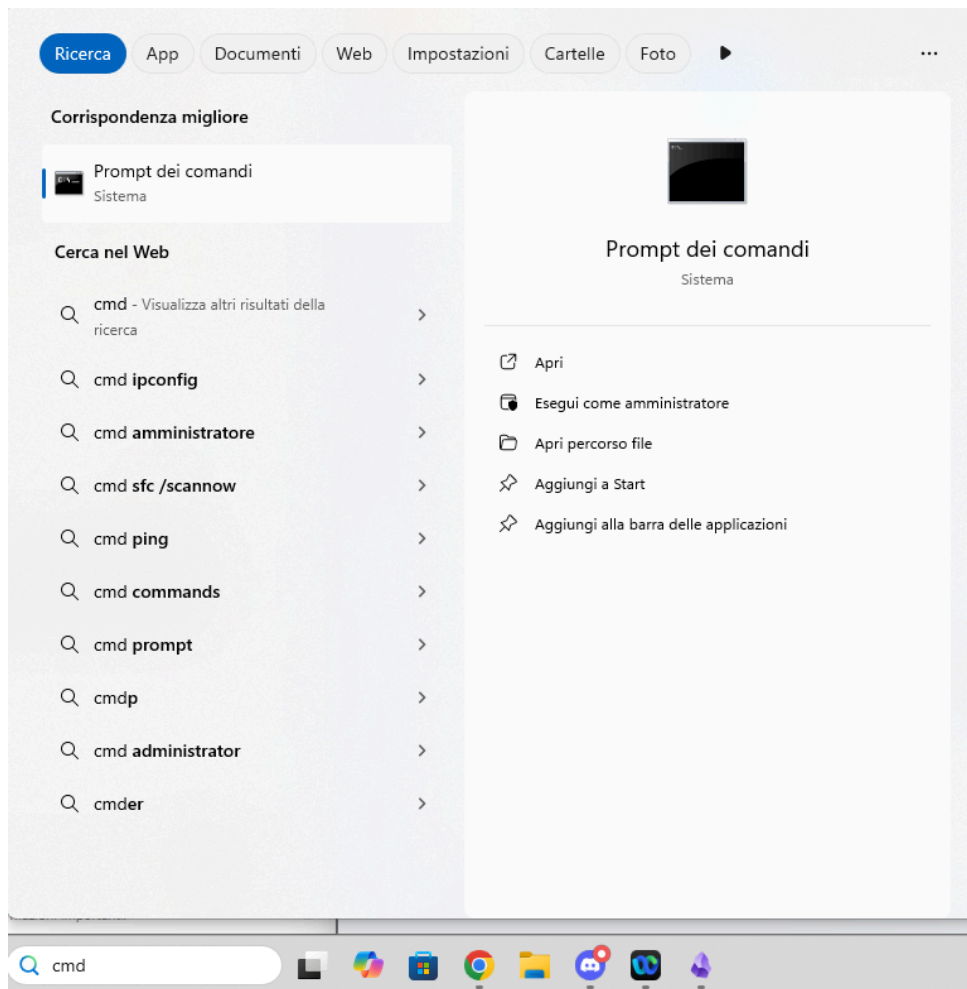
## Pratica:

### Parte 1:

Per avviare PowerShell andiamo sulla barra rapida di windows e digitiamo **power**, successivamente clicchiamo per aprire **Windows PowerShell**;



Per avviare invece il prompt sempre sulla barra di ricerca digitiamo **cmd**;



## Parte 2:

Il primo compito è stato quello di comparare il comando **dir** e **ping**, e notiamo che sono simili;

## dir

Prompt dei comandi

C:\Users\loren>dir

Il volume nell'unità C è Windows

Numero di serie del volume: 6E5B-325C

Directory di C:\Users\loren

13/12/2024	10:59	<DIR>	.
29/10/2024	16:02	<DIR>	..
19/11/2024	16:10	<DIR>	.idlerc
12/12/2024	15:12	<DIR>	.VirtualBox
06/11/2024	14:45	<DIR>	.vscode
29/10/2024	16:53	<DIR>	ansel
29/10/2024	15:58	<DIR>	Contacts
11/12/2024	14:50	<DIR>	Desktop
18/11/2024	12:54	<DIR>	Documents
12/12/2024	22:39	<DIR>	Downloads
29/10/2024	15:58	<DIR>	Favorites
29/10/2024	15:58	<DIR>	Links
29/10/2024	15:58	<DIR>	Music
29/10/2024	15:59	<DIR>	OneDrive
29/11/2024	17:54	<DIR>	Pictures
29/10/2024	15:58	<DIR>	Saved Games
29/10/2024	16:02	<DIR>	Searches
29/10/2024	16:53	<DIR>	Videos
11/12/2024	14:57	<DIR>	VirtualBox VMs
			0 File 0 byte
			19 Directory 598.495.535.104 byte disponibili

C:\Users\loren>

Windows PowerShell

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

PS C:\Users\loren> dir

Directory: C:\Users\loren

Mode	LastWriteTime	Length	Name
d----	19/11/2024 16:10		.idlerc
d----	12/12/2024 15:12		.VirtualBox
d----	06/11/2024 14:45		.vscode
d----	29/10/2024 16:53		ansel
d-r--	29/10/2024 15:58		Contacts
dar--	11/12/2024 14:50		Desktop
d-r--	18/11/2024 12:54		Documents
d-r--	12/12/2024 22:39		Downloads
d-r--	29/10/2024 15:58		Favorites
d-r--	29/10/2024 15:58		Links
d-r--	29/10/2024 15:58		Music
d-r--	29/10/2024 15:59		OneDrive
d-r--	29/11/2024 17:54		Pictures
d-r--	29/10/2024 15:58		Saved Games
d-r--	29/10/2024 16:02		Searches
d-r--	29/10/2024 16:53		Videos
d-r--	29/10/2024 16:53		VirtualBox VMs
d----	11/12/2024 14:57		VirtualBox VMs

PS C:\Users\loren> |

## ping

```
Prompt dei comandi
Microsoft Windows [Versione 10.0.26100.2695]
(c) Microsoft Corporation. Tutti i diritti riservati.

C:\Users\loren>ping 8.8.8.8

Esecuzione di Ping 8.8.8.8 con 32 byte di dati:
Risposta da 8.8.8.8: byte=32 durata=20ms TTL=60
Risposta da 8.8.8.8: byte=32 durata=20ms TTL=60
Risposta da 8.8.8.8: byte=32 durata=19ms TTL=60
Risposta da 8.8.8.8: byte=32 durata=20ms TTL=60

Statistiche Ping per 8.8.8.8:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 19ms, Massimo = 20ms, Medio = 19ms

C:\Users\loren>

Windows PowerShell
PS C:\Users\loren> ping 8.8.8.8

Esecuzione di Ping 8.8.8.8 con 32 byte di dati:
Risposta da 8.8.8.8: byte=32 durata=20ms TTL=60
Risposta da 8.8.8.8: byte=32 durata=20ms TTL=60
Risposta da 8.8.8.8: byte=32 durata=20ms TTL=60
Risposta da 8.8.8.8: byte=32 durata=20ms TTL=60

Statistiche Ping per 8.8.8.8:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 20ms, Massimo = 20ms, Medio = 20ms
PS C:\Users\loren> |
```

### Parte 3:

Ci ha chiesto poi di trovare il comando **cmdlet** su powershell equivalente a **dir**, e grazie al comando **Get-Alias**, siamo riusciti a trovarlo:

```
Windows PowerShell
PS C:\Users\loren> Get-Alias dir

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

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

### Get-ChildItem

```
Windows PowerShell
PS C:\Users\loren> Get-ChildItem

Directory: C:\Users\loren

Mode                LastWriteTime         Length Name
----                -
d-----          19/11/2024      16:10             .idlerc
d-----          12/12/2024      15:12             .VirtualBox
d-----          06/11/2024      14:45             .vscode
d-----          29/10/2024      16:53             ansel
d-r-----          29/10/2024      15:58             Contacts
dar-----          11/12/2024      14:50             Desktop
d-r-----          18/11/2024      12:54             Documents
d-r-----          12/12/2024      22:39             Downloads
d-r-----          29/10/2024      15:58             Favorites
d-r-----          29/10/2024      15:58             Links
d-r-----          29/10/2024      15:58             Music
d-r-----          29/10/2024      15:59             OneDrive
d-r-----          29/11/2024      17:54             Pictures
d-r-----          29/10/2024      15:58             Saved Games
d-r-----          29/10/2024      16:02             Searches
d-r-----          29/10/2024      16:53             Videos
d-----          11/12/2024      14:57             VirtualBox VMs

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

Un **cmdlet** (**command-let**) in PowerShell è un comando progettato per eseguire una singola funzione specifica. I cmdlet sono l'elemento base del linguaggio

PowerShell e sono simili ai comandi in altri shell, come i comandi Bash in Linux o i comandi CMD in Windows. Tuttavia, i cmdlet sono molto più **potenti** e **strutturati**.

## Parte 4:

Esploriamo ed utilizziamo **netstat** in powershell, comando utilizzato per **visualizzare** informazioni sulle **connessioni di rete**, **porte aperte** etc...

Con il comando **netstat -r** vediamo tutte le **tabelle di routing**;

```
Windows PowerShell
PS C:\Users\loren> netstat -r

=====
Elenco interfacce
 3...60 cf 84 62 09 b7 .....Realtek Gaming 2.5GbE Family Controller
14...0a 00 27 00 00 0e .....VirtualBox Host-Only Ethernet Adapter
 6...0a 00 27 00 00 06 .....VirtualBox Host-Only Ethernet Adapter #2
 4...5a cd c9 a2 e2 ff .....Microsoft Wi-Fi Direct Virtual Adapter
 8...5a cd c9 a2 f2 ef .....Microsoft Wi-Fi Direct Virtual Adapter #2
 9...58 cd c9 a2 c2 df .....MediaTek Wi-Fi 6E MT7922 (RZ616) 160MHz Wireless LAN Card
15...58 cd c9 a2 c2 e0 .....Bluetooth Device (Personal Area Network)
 1.....Software Loopback Interface 1
=====
```

Una **tabella di routing** (routing table) è una struttura dati utilizzata dai router e dai dispositivi di rete, come i computer, per determinare la strada (o il percorso) migliore per inviare i pacchetti di dati attraverso una rete

Possiamo anche avviare powershell come **amministratore** per avere funzioni in più;

**non sono amministratore;**

```
Route permanenti:
Nessuna
PS C:\Users\loren> netstat -abno
Per eseguire l'operazione richiesta è necessaria l'esecuzione con privilegi elevati.
PS C:\Users\loren> |
```

**sono amministratore;**

```
Amministratore: Windows PowerShell
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:\windows\system32> netstat -abno

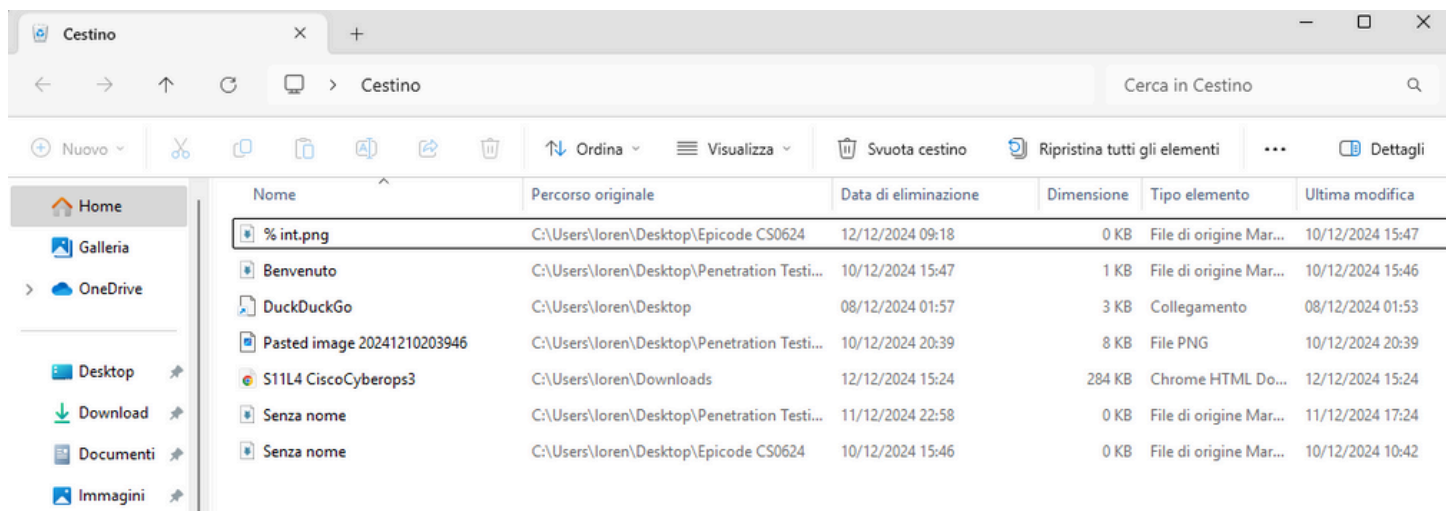
Connessioni attive

Proto  Indirizzo locale      Indirizzo esterno      Stato      PID
TCP    0.0.0.0:135             0.0.0.0:0              LISTENING  1520
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  7064
CDPSvc
[svchost.exe]
TCP    0.0.0.0:6850            0.0.0.0:0              LISTENING  18360
```

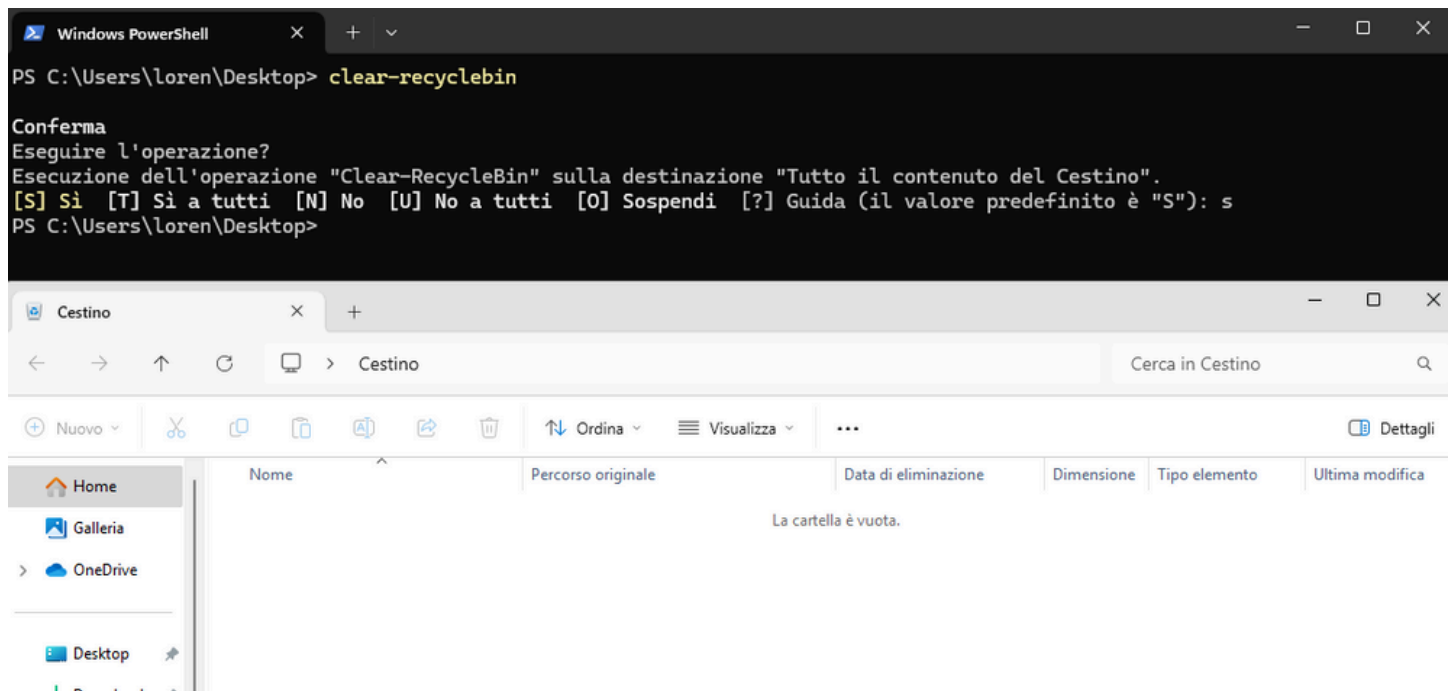
Il comando **netstat -abno** fornisce un'ampia panoramica sulle **connessioni di rete**, le **porte** in ascolto e i **processi associati** (PID). Ogni parametro ha una funzione specifica:

## Parte 5:

Infine il compito ci ha chiesto di svuotare il **cestino** utilizzando powershell;



Assodato che nel cestino ci sono dei file da eliminare, procediamo su powershell;



## Conclusioni:

Questo laboratorio ha fornito una panoramica delle potenzialità di PowerShell come strumento di automazione e gestione dei sistemi Windows. Abbiamo esplorato comandi base, come `dir` e `netstat`, evidenziando le differenze tra PowerShell e il Prompt dei Comandi, nonché l'utilizzo dei *cmdlet* per eseguire operazioni avanzate. In particolare, l'uso di comandi come `Get-ChildItem` e `clear-recyclebin` ha dimostrato come PowerShell possa semplificare attività quotidiane e amministrative. Inoltre, abbiamo visto come monitorare le connessioni di rete e i processi con dettagli precisi grazie a PowerShell, rendendolo uno strumento essenziale per professionisti IT e analisti della sicurezza.

## Svolgimento Compito 2:

### Che cosa sono i protocolli HTTP e HTTPS:

**HTTP:** È utilizzato per siti web che non richiedono una trasmissione sicura di dati, come informazioni pubbliche che non comportano rischi di violazioni della privacy.

**HTTPS:** È essenziale per siti web che richiedono una connessione sicura, o qualsiasi altro sito dove vengano trasmesse informazioni sensibili, come password, numeri di carte di credito, o dati personali.

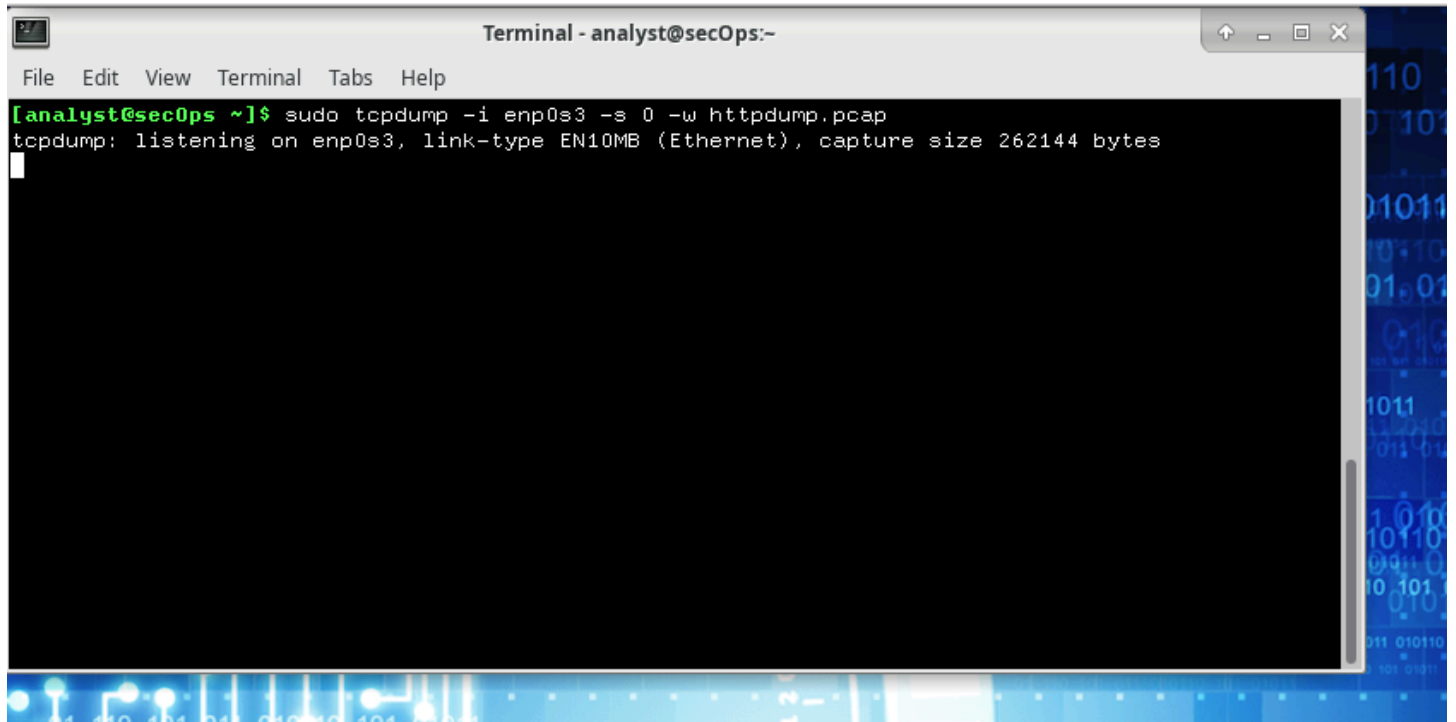
### Pratica:

#### Parte HTTP:

Per questo compito avremmo bisogno della macchina virtuale **CyberOps Workstation VM**, una volta avviata apriamo il prompt e digitiamo il seguente comando:

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

Il seguente comando avvia il **tcpdump**, lo **strumento di cattura dei pacchetti** di rete;

A screenshot of a terminal window titled "Terminal - analyst@secOps:~". The terminal shows the command `sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap` being executed. The output of the command is `tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes`. The terminal has a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help". The background of the terminal window is a dark blue color with a pattern of binary code (0s and 1s) and some glowing blue dots at the bottom.

Successivamente dal browser della VM andiamo sul sito:

<http://www.altoromutual.com/login.jsp>



Applications | Altoro Mutual - Mozilla Firef... | Terminal - analyst@secOps:~

Altoro Mutual - Mozilla Firefox

Altoro Mutual x +

www.althoromutual.com/login.jsp

[Sign In](#) | [Contact Us](#) | [Feedback](#) | Search

# AltoroMutual

<a href="#">ONLINE BANKING LOGIN</a>	<a href="#">PERSONAL</a>	<a href="#">SMALL BUSINESS</a>	<a href="#">INSIDE AL</a>
--------------------------------------	--------------------------	--------------------------------	---------------------------

[PERSONAL](#)

- [Deposit Product](#)
- [Checking](#)
- [Loan Products](#)
- [Cards](#)
- [Investments & Insurance](#)
- [Other Services](#)

[SMALL BUSINESS](#)

- [Deposit Products](#)
- [Lending Services](#)
- [Cards](#)
- [Insurance](#)
- [Retirement](#)
- [Other Services](#)

[INSIDE ALTORO MUTUAL](#)

- [About Us](#)

## Online Banking Login

Username:

Password:

Login

Essendo che questo sito utilizza il protocollo HTTP, non sicuro digitiamo le credenziali **Admin** ed **Admin**, e premiamo invio;

Altoro Mutual - Mozilla Firefox

Altoro Mutual x +

www.altoromutual.com/login.jsp

[Sign In](#) | [Contact Us](#) | [Feedback](#) | Search

# AltoroMutual

[ONLINE BANKING LOGIN](#)

[PERSONAL](#)

[SMALL BUSINESS](#)

[INSIDE ALTORO MUTUAL](#)

[PERSONAL](#)

- [Deposit Product](#)
- [Checking](#)
- [Loan Products](#)
- [Cards](#)
- [Investments & Insurance](#)
- [Other Services](#)

[SMALL BUSINESS](#)

- [Deposit Products](#)
- [Lending Services](#)
- [Cards](#)
- [Insurance](#)
- [Retirement](#)
- [Other Services](#)

## Online Banking Login

Username:

Password:

This connection is not secure.  
Logins entered here could be compromised. [Learn More](#)

Successivamente torniamo sul prompt e clicchiamo **control + C**, per bloccare la cattura dei pacchetti;

Altoro Mutual - Mozilla Firefox

Altoro Mutual

www.altoromutual.com/bank/main.jsp

Sign Off | Contact Us | Feedback | Search

Go

**AltoroMutual**

PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

**MY ACCOUNT**

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

**Hello Admin User**

Welcome to Altoro Mutual Online.

View Account Details:

800000 Corporate GO

**Congratulations!**

You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!

Click [Here](#) to apply.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2024 Altoro Mutual, Inc.

Terminal - analyst@secOps:~

```
File Edit View Terminal Tabs Help

[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C3789 packets captured
3798 packets received by filter
0 packets dropped by kernel
[analyst@secOps ~]$
```

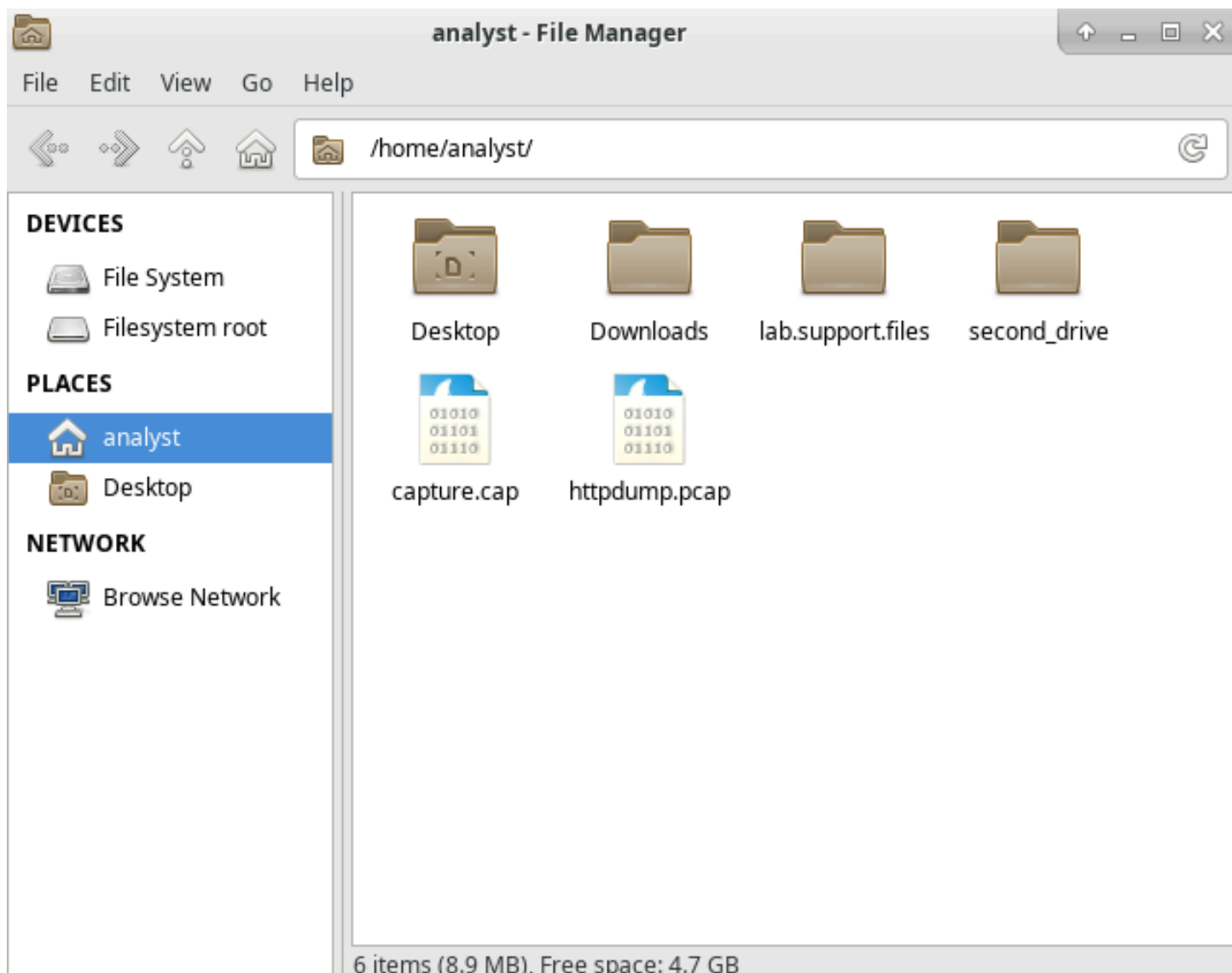
copy from GitHub and take advantage of advanced ;

detecting web application vulnerabilities and we

ite is provided "as is" without warranty of any kind

<https://www.hcl-software.com/appscan/>.

Andiamo poi ad aprire la cattura che abbiamo salvato come **httpdump.pcap** in **Wireshark**;



Applichiamo il filtro **http**, e cerchiamo una **richiesta POST**. Successivamente apriamo **HTML Form URL** ed essendo che è un protocollo HTTP, i dati non saranno criptati, infatti possiamo vedere (evidenziati in giallo), **username** e **password**;

Filter:

http

Expression...

Clear

Apply

Save

No.	Time	Source	Destination	Protocol	Length	Info
3622	177.384763	65.61.137.117	192.168.0.116	HTTP	187	HTTP/1.1 304 Not Modified
3624	177.384912	65.61.137.117	192.168.0.116	HTTP	189	HTTP/1.1 304 Not Modified
3626	177.390802	65.61.137.117	192.168.0.116	HTTP	188	HTTP/1.1 304 Not Modified
3644	182.683493	192.168.0.116	65.61.137.117	HTTP	601	POST /doLogin HTTP/1.1 (application/x-www-form
3645	182.835908	65.61.137.117	192.168.0.116	HTTP	339	HTTP/1.1 302 Found
3647	182.838233	192.168.0.116	65.61.137.117	HTTP	619	GET /bank/main.jsp HTTP/1.1
3651	182.988005	65.61.137.117	192.168.0.116	HTTP	2410	HTTP/1.1 200 OK (text/html)
3719	189.359623	192.168.0.116	104.18.38.233	OCSP	496	Request
3721	189.390684	104.18.38.233	192.168.0.116	OCSP	894	Response
3723	189.391073	192.168.0.116	104.18.38.233	OCSP	496	Request
3727	189.422931	104.18.38.233	192.168.0.116	OCSP	894	Response

[Full request URI: <http://www.altoromutual.com/doLogin>]

[HTTP request 4/5]

[Prev request in frame: 3592]

[Response in frame: 3645]

[Next request in frame: 3647]

File Data: 37 bytes

▼ HTML Form URL Encoded: application/x-www-form-urlencoded

▼ Form item: "uid" = "Admin"

Key: uid

Value: Admin

▼ Form item: "passw" = "Admin"

Key: passw

Value: Admin

▼ Form item: "btnSubmit" = "Login"

Key: btnSubmit

Value: Login

Questa cosa può essere una vulnerabilità molto **grave**, ad esempio per un attacco **MITM** (Man in The Middle);

## Parte HTTPS:

Per catturare il traffico HTTPS, facciamo lo stesso procedimento di prima nel cmd;

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

[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Successivamente andiamo su qualsiasi sito in HTTPS, ed effettuiamo un **login**;

Una volta effettuate il login chiudiamo la cattura del traffico, e apriamo il file in WireShark, filtrando con **tcp.port==443** per vedere solo il traffico HTTPS;

Filter: tcp.port==443

No.	Time	Source	Destination	Protocol	Length	Info
11676	294.540895	192.168.0.116	142.251.143.202	TCP	66	50306 → 443 [ACK] Seq=2594 Ack=21573 Win=114
11677	294.540934	142.251.143.202	192.168.0.116	TLSv1.2	104	Application Data
11678	294.546738	192.168.0.116	142.251.143.202	TLSv1.2	112	Application Data
11679	294.569617	142.251.143.202	192.168.0.116	TCP	66	443 → 50306 [ACK] Seq=21611 Ack=2640 Win=268
11680	294.574387	192.168.0.116	18.65.64.35	TLSv1.2	208	Application Data
11681	294.581754	18.65.64.35	192.168.0.116	TCP	66	443 → 50562 [ACK] Seq=17681 Ack=1314 Win=70
11682	294.581758	18.65.64.35	192.168.0.116	TLSv1.2	505	Application Data
11685	294.583121	192.168.0.116	18.65.64.35	TCP	66	50562 → 443 [ACK] Seq=1314 Ack=18120 Win=71
11688	294.648374	192.168.0.116	104.26.10.146	TLSv1.2	149	Application Data
11689	294.677415	104.26.10.146	192.168.0.116	TLSv1.2	727	Application Data

▶ Frame 11701: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits)

▶ Ethernet II, Src: 6c:a0:b4:28:82:99 (6c:a0:b4:28:82:99), Dst: PcsCompu\_62:44:9f (08:00:27:62:44:9f)

▶ Internet Protocol Version 4, Src: 34.120.129.162, Dst: 192.168.0.116

▶ Transmission Control Protocol, Src Port: 443, Dst Port: 37832, Seq: 5669, Ack: 1788, Len: 74

▼ Secure Sockets Layer

- ▼ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
  - Content Type: Application Data (23)
  - Version: TLS 1.2 (0x0303)
  - Length: 69
  - Encrypted Application Data: 00000000000000095b55cbca1a782927fdff6c60730a9410...

Vediamo che tutti il traffico in entrata dai protocolli **HTTPS** è criptato, e non possiamo leggere il contenuto;

## **Conclusione:**

In questo laboratorio, abbiamo esplorato l'utilizzo di Wireshark per catturare e analizzare il traffico di rete HTTP e HTTPS. La cattura del traffico HTTP ci ha permesso di osservare come i dati vengano trasmessi in chiaro sulla rete, evidenziando potenziali vulnerabilità legate alla sicurezza. In contrasto, l'analisi del traffico HTTPS ha dimostrato come la crittografia protegga la privacy delle comunicazioni, rendendo più difficile per un osservatore intercettare i dati. Tuttavia, è stato evidente che, sebbene HTTPS offra un livello di sicurezza superiore, la gestione delle chiavi e dei certificati è fondamentale per evitare vulnerabilità.