



CYBER SECURITY



CyberOps

- Analizzeremo, esploreremo alcune delle funzioni di PowerShell.
- Utilizzeremo Wireshark per Esaminare il Traffico HTTP e HTTPS

PowerShell

Per accedere alla console PowerShell dovremo cliccare il tasto start e cercarla nella barra di ricerca . Ciò che ci apparirà somiglierà molto alla schermata del prompt dei comandi , adesso andiamo ad esplorare alcuni comandi e accostarli al cmd.

```
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\elisa> dir  
  
Directory: C:\Users\elisa  
  
Mode LastWriteTime Length Name  
---- -- -  
d---- 07/12/2024 16:32 .VirtualBox  
d-r--- 03/10/2024 15:02 Contacts  
d-r--- 11/12/2024 09:10 Desktop  
d-r--- 03/10/2024 15:02 Documents  
dar--- 11/12/2024 09:10 Downloads  
d-r--- 03/10/2024 15:02 Favorites  
d-r--- 03/10/2024 15:02 Links  
d-r--- 03/10/2024 15:02 Music  
dar--l 03/11/2024 10:20 OneDrive  
d-r--- 21/10/2024 16:25 Pictures  
d-r--- 03/10/2024 15:02 Saved Games  
d-r--- 07/10/2024 08:18 Searches  
d-r--- 02/12/2024 18:14 Videos  
d----- 02/12/2024 12:19 VirtualBox VMs  
  
PS C:\Users\elisa>  
  
Microsoft Windows [Versione 10.0.22631.4460]  
(c) Microsoft Corporation. Tutti i diritti riservati.  
C:\Users\elisa>dir  
Il volume nell'unità C non ha etichetta.  
Numero di serie del volume: 0030-818E  
  
Directory di C:\Users\elisa  
  
17/10/2024 11:05 <DIR> .  
07/10/2024 07:18 <DIR> ..  
07/12/2024 16:32 <DIR> .VirtualBox  
03/10/2024 14:02 <DIR> Contacts  
11/12/2024 09:10 <DIR> Desktop  
03/10/2024 14:02 <DIR> Documents  
11/12/2024 09:10 <DIR> Downloads  
03/10/2024 14:02 <DIR> Favorites  
03/10/2024 14:02 <DIR> Links  
03/10/2024 14:02 <DIR> Music  
03/11/2024 10:20 <DIR> OneDrive  
21/10/2024 15:25 <DIR> Pictures  
03/10/2024 14:02 <DIR> Saved Games  
07/10/2024 07:18 <DIR> Searches  
02/12/2024 18:14 <DIR> Videos  
02/12/2024 12:19 <DIR> VirtualBox VMs  
0 File 0 byte  
16 Directory 27.325.894.656 byte disponibili  
  
C:\Users\elisa>
```

In questo caso abbiamo eseguito il comando "dir", in entrambe le finestre vediamo un elenco di sottodirectory e file, e informazioni associate come tipo, dimensione del file, data e ora dell'ultima scrittura.

```
PS C:\Users\elesa> ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet 3:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::3e92:8
6f8:31c:c1b4%13
    Indirizzo IPv4. . . . . : 192.168.56.1
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . :

Scheda LAN wireless Connessione alla rete locale (LAN)* 1:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

Scheda LAN wireless Connessione alla rete locale (LAN)* 10:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

Scheda LAN wireless Wi-Fi:

    Suffisso DNS specifico per connessione: station
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::6367:7
499:6ee4:7344%14
    Indirizzo IPv4. . . . . : 192.168.1.5
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1

Scheda Ethernet Connessione di rete Bluetooth:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

C:\Users\elesa>ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet 3:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::3e9
2:86f8:31c:c1b4%13
    Indirizzo IPv4. . . . . : 192.168.56.1
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . :

Scheda LAN wireless Connessione alla rete locale (LAN)* 1:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

Scheda LAN wireless Connessione alla rete locale (LAN)* 10:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

Scheda LAN wireless Wi-Fi:

    Suffisso DNS specifico per connessione: station
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::636
7:7499:6ee4:7344%14
    Indirizzo IPv4. . . . . : 192.168.1.5
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1

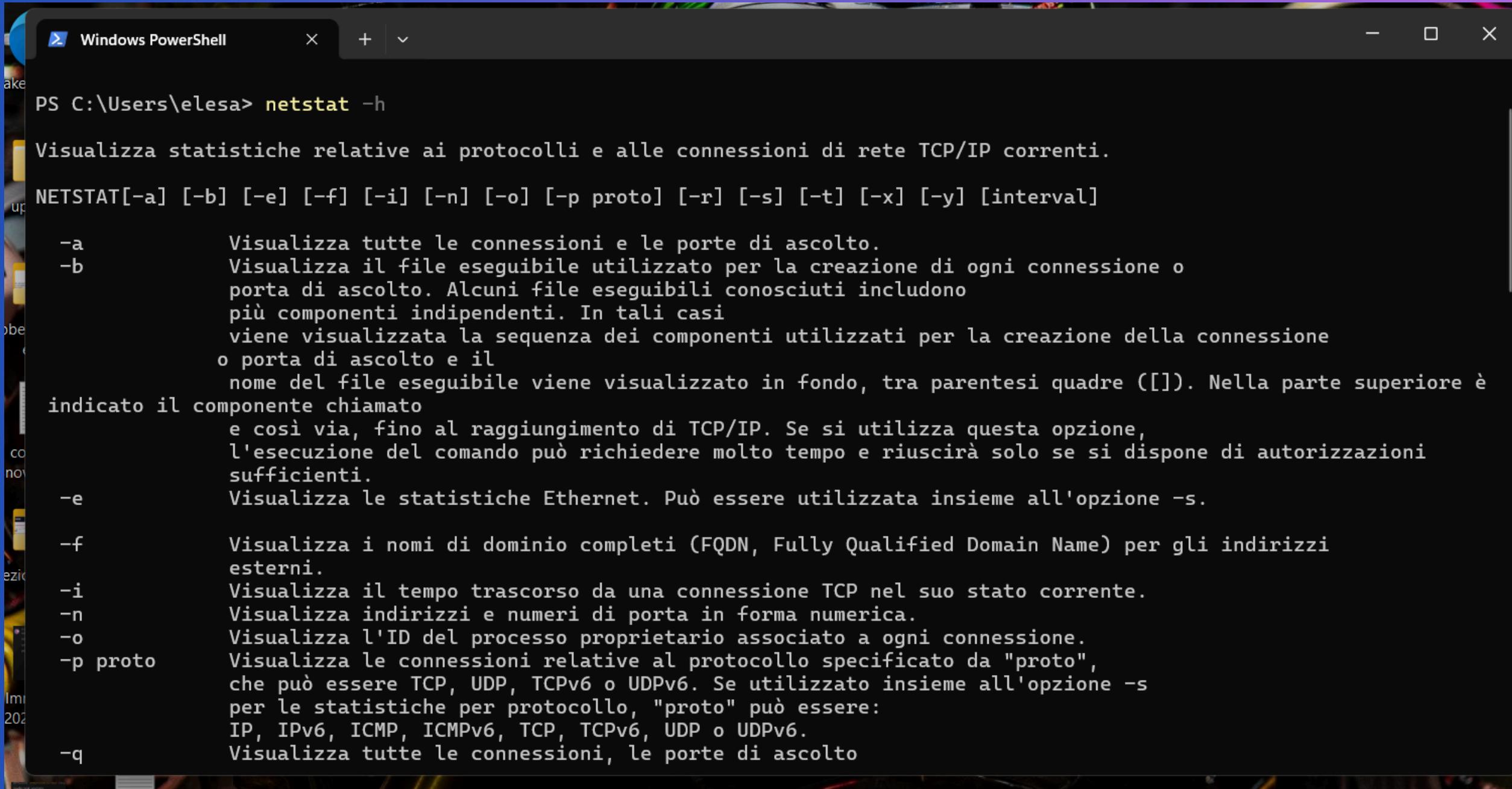
Scheda Ethernet Connessione di rete Bluetooth:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

Scheda Ethernet Ethernet:
```

In quest'altro caso abbiamo eseguito il comando "ipconfig" e possiamo vedere che le due finestre si somigliano molto nel riscontro che ci forniscono

Ora andremo ad inserire sul prompt di PowerShell il comando netstat -h.



```
PS C:\Users\elesta> 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
```

per visualizzare le opzioni disponibili per il netstat comando.

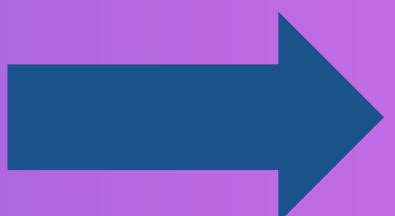
Per visualizzare la tabella di routing con i percorsi attivi, andremo a digitare sempre sullo stesso prompt il comando netstat -r



```
Windows PowerShell
PS C:\Users\elisa> netstat -r
=====
Elenco interfacce
13...0a 00 27 00 00 0d .....VirtualBox Host-Only Ethernet Adapter
16...28 a0 6b 62 43 f1 .....Microsoft Wi-Fi Direct Virtual Adapter
18...2a a0 6b 62 43 f0 .....Microsoft Wi-Fi Direct Virtual Adapter #2
14...28 a0 6b 62 43 f0 .....Intel(R) Wi-Fi 6 AX201 160MHz
15...28 a0 6b 62 43 f4 .....Bluetooth Device (Personal Area Network)
12...8c b0 e9 e3 79 ab .....Realtek PCIe GbE 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   192.168.1.1  192.168.1.5    30
        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      192.168.1.5    286
        192.168.1.5     255.255.255.255  On-link      192.168.1.5    286
        192.168.1.255    255.255.255.255  On-link      192.168.1.5    286
        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      192.168.1.5    286
255.255.255.255    255.255.255.255  On-link      127.0.0.1    331
```

Ora andremo ad eseguire un'altro PowerShell ma con privilegi elevati , la procedura per eseguirlo è: fare clic su Start , poi cerca PowerShell e fai clic con il pulsante destro del mouse su Windows PowerShell e seleziona Esegui come amministratore . Fai clic su Sì per consentire a questa app di apportare modifiche al dispositivo. Una volta aperto andremo a mettere il comando “netstat -abno” ,che può anche visualizzare i processi associati alle connessioni TCP attive.



```
Administrator: 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

Conessioni attive

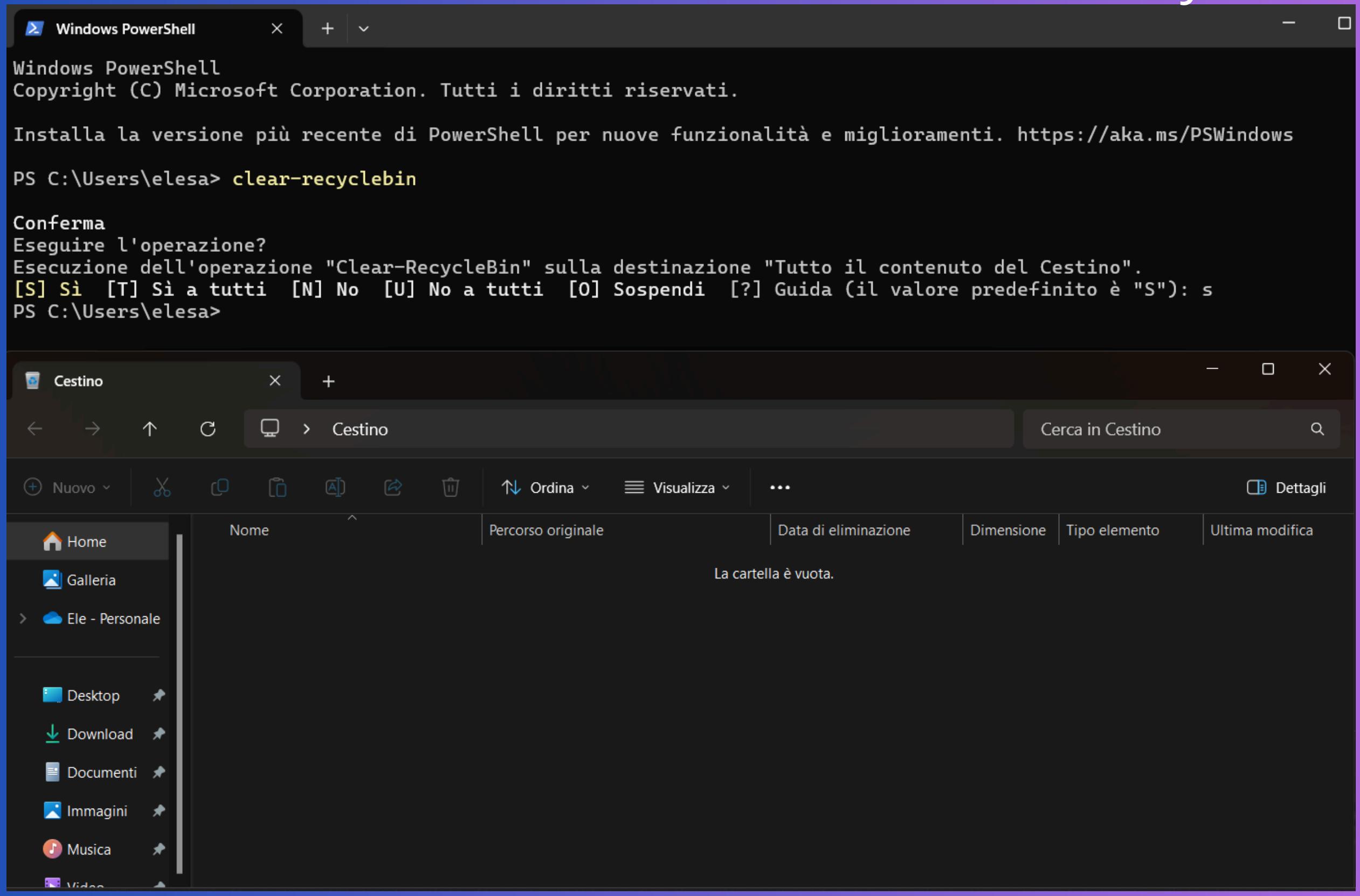
  Proto  Indirizzo locale        Indirizzo esterno      Stato      PID
  TCP    0.0.0.0:135           0.0.0.0:0            LISTENING   1352
  RpcSs
  [svchost.exe]
  TCP    0.0.0.0:445           0.0.0.0:0            LISTENING   4
  Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:5040          0.0.0.0:0            LISTENING   8772
  CDPSvc
  [svchost.exe]
  TCP    0.0.0.0:7260          0.0.0.0:0            LISTENING   19068
  [Sistema]
  TCP    0.0.0.0:45823          0.0.0.0:0            LISTENING   17660
  [WindowsMCFCore.exe]
  TCP    0.0.0.0:49664          0.0.0.0:0            LISTENING   1072
  [lsass.exe]
  TCP    0.0.0.0:49665          0.0.0.0:0            LISTENING   984
  Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:49668          0.0.0.0:0            LISTENING   2860
  EventLog
  [svchost.exe]
  TCP    0.0.0.0:49669          0.0.0.0:0            LISTENING   1856
```



Fatto ciò adesso apriamo Task Manager e andiamo alla scheda Dettagli . Fai clic sull'intestazione PID in modo che i PID siano in ordine poi seleziona uno dei PID dai risultati di netstat -abno, facciamo clic con il pulsante destro del mouse sul PID selezionato nel Task Manager per aprire la finestra di dialogo Proprietà per ulteriori informazioni. Da qui potremo vedere per ogni processo il suo utente e quanta memoria sta utilizzando

Dettagli									Esegui nuova attività		Termina attività	...
	Nome	PID	Stato	Nome utente	CPU	Memoria ...	Architet...	Descrizione				
	Interrupt sistema	-	In esecuzione	SYSTEM	00	0 K		Chiamate di procedura differite e ISR (Interrupt Service R...				
	Processo di inattività ...	0	In esecuzione	SYSTEM	86	8 K		Percentuale di tempo di inattività del processore				
	System	4	In esecuzione	SYSTEM	01	12 K		NT Kernel & System				
	Secure System	108	In esecuzione	SYSTEM	00	31.724 K		NT Kernel & System				
	msedgewebview2.exe	112	In esecuzione	elesa	00	1.048 K	x64	WebView2 Utilità: Audio Service				
	Registry	160	In esecuzione	SYSTEM	00	3.072 K		NT Kernel & System				
	SamsungAnalyticsSer...	324	In esecuzione	SYSTEM	00	1.284 K	x64	SamsungAnalyticsService				
	smss.exe	588	In esecuzione	SYSTEM	00	84 K		Gestione sessioni di Windows				
	services.exe	732	In esecuzione	SYSTEM	00	3.432 K		App Servizi e Controller				
	csrss.exe	892	In esecuzione	SYSTEM	00	776 K		Processo runtime client server				
	svchost.exe	972	In esecuzione	SYSTEM	00	320 K	x64	Processo host per servizi di Windows				
	wininit.exe	984	In esecuzione	SYSTEM	00	384 K		Applicazione di avvio di Windows				
	lalso.exe	1056	In esecuzione	SYSTEM	00	512 K	x64	Credential Guard & VBS Key Isolation				
	lsass.exe	1072	In esecuzione	SYSTEM	00	6.624 K	x64	Local Security Authority Process				
	svchost.exe	1164	In esecuzione	SERVIZIO L...	00	824 K	x64	Processo host per servizi di Windows				
	svchost.exe	1188	In esecuzione	SYSTEM	00	15.988 K	x64	Processo host per servizi di Windows				
	svchost.exe	1212	In esecuzione	SYSTEM	00	1.100 K	x64	Processo host per servizi di Windows				
	fontdrvhost.exe	1216	In esecuzione	UMFD-0	00	252 K	x64	Usermode Font Driver Host				
	WUDFHost.exe	1260	In esecuzione	SERVIZIO L...	00	3.284 K	x64	Windows Driver Foundation - Processo host Framework ...				
	SystemSettings.exe	1304	Sospeso	elesa	00	0 K	x64	Impostazioni				
	winlogon.exe	1336	In esecuzione	SYSTEM	00	652 K	x64	Applicazione Accesso a Windows				
	svchost.exe	1352	In esecuzione	SERVIZIO D...	00	11.876 K	x64	Processo host per servizi di Windows				
	svchost.exe	1404	In esecuzione	SYSTEM	00	1.428 K	x64	Processo host per servizi di Windows				
	svchost.exe	1484	In esecuzione	SYSTEM	00	324 K	x64	Processo host per servizi di Windows				

Ora andiamo a vedere un ultimo comando , come svuotare il nostro cestino sempre tramite PowerShell, tramite il comando “clear-recyclebin”.



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

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

PS C:\Users\elesta> clear-recyclebin

Conferma
Eseguire l'operazione?
Esecuzione dell'operazione "Clear-RecycleBin" sulla destinazione "Tutto il contenuto del Cestino".
[S] Sì [T] Si a tutti [N] No [U] No a tutti [O] Sospendi [?] Guida (il valore predefinito è "S"): s
PS C:\Users\elesta>

Cestino
Nome
Percorso originale
Data di eliminazione
Dimensione
Tipo elemento
Ultima modifica
```

The PowerShell window shows the command `clear-recyclebin` being run, followed by a confirmation dialog asking if the user wants to execute the operation. The user has selected 'Sì' (Yes). The Recycle Bin interface below shows that the trash is empty.

Traffico HTTP e HTTPS



Adesso andremo a catturare e visualizzare il traffico HTTP.

Primo passaggio accendere la nostra VM CyberOps Workstation e immettere le credenziali :Nome utente: analista ,Password: cyberops. Una volta aperta la VM andremo ad aprire un terminali ed eseguire il comando “ip address”.

Mentre siamo nel terminale, inserisci il comando “sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap”. Inserisci la password cyberops per l'analista utente appena richiesto. (tranquillo se non vedrai nessuna password che viene scritta).



CyberOps Workstation [In esecuzione] - Oracle VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

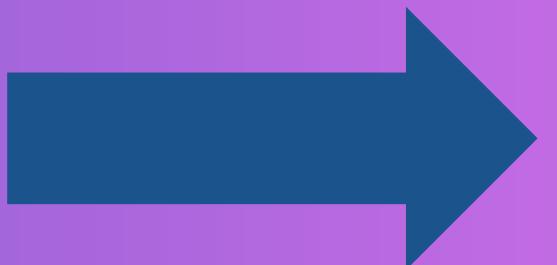
Applications Terminal - analyst@secOps:~/Desktop

Terminal - analyst@secOps:~/Desktop

```
: 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
: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
  link/ether 08:00:27:e8:2a:b5 brd ff:ff:ff:ff:ff:ff
  inet 192.168.1.7/24 brd 192.168.1.255 scope global dynamic enp0s3
    valid_lft 3385sec preferred_lft 3385sec
  inet6 fe80::a00:27ff:fee8:2ab5/64 scope link
    valid_lft forever preferred_lft forever
analyst@secOps Desktop]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
sudo] password for analyst:
cpdump: illegal token: -
analyst@secOps Desktop]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
cpdump: illegal token: -
analyst@secOps Desktop]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
sudo] password for analyst:
cpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```



una volta eseguito ciò apriamo il browser Web dalla barra di avvio all'interno della VM CyberOps Workstation e andiamo su <http://www.altoromutual.com/login.jsp> ,Poiché questo sito web utilizza HTTP, il traffico non è crittografato. Inserisci il nome utente Admin e la password Admin e fai clic su Accedi .Poi chiudiamo il browser web e ritorniamo alla finestra del terminale in cui è in esecuzione tcpdump. Digitare CTRL+C per interrompere la cattura del pacchetto.



Il tcpdump, eseguito nel passaggio precedente, ha stampato l'output in un file denominato httpdump.pcap. Questo file si trova nella directory home dell'analista utente .

Fare clic sull'icona File Manager sul desktop e andare alla cartella home dell'analista utente . Fare doppio clic sul file httpdump.pcap e si aprirà WhireShark.



Nell'applicazione Wireshark, filtra per http e fai clic su Applica.
Arriva e clicca sul messaggio POST ,Nella finestra inferiore viene visualizzato il messaggio. Espandi la sezione HTML Form URL Encoded: application/x-www-form-urlencoded .



CyberOps Workstation [In esecuzione] - Oracle VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

Applications : Desktop - File Manager httpdump.pcap [Wireshark ...] Terminal - analyst@secOps...

Desktop - File Manager

File Edit View Go Help

DEVICES

- File System
- Filesystem root

PLACES

- analyst
- Desktop

NETWORK

- Browse Network

httpdump.pcap [Wireshark 2.5.1]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1859	236.548302	65.61.137.117	192.168.1.7	HTTP	5283	HTTP/1.1 200 OK (GIF89a)
1861	236.572447	65.61.137.117	192.168.1.7	HTTP	1187	HTTP/1.1 200 OK (JPEG JFIF image)
1866	236.601023	65.61.137.117	192.168.1.7	HTTP	366	HTTP/1.1 200 OK (GIF89a)
1873	236.766729	65.61.137.117	192.168.1.7	HTTP	666	HTTP/1.1 200 OK (JPEG JFIF image)
1880	236.800208	192.168.1.7	65.61.137.117	HTTP	420	GET /favicon.ico HTTP/1.1
1884	236.967028	65.61.137.117	192.168.1.7	HTTP	7180	HTTP/1.1 404 Not Found (text/html)
1913	243.990700	192.168.1.7	34.107.221.82	HTTP	354	GET /success.txt HTTP/1.1
1919	244.008689	34.107.221.82	192.168.1.7	HTTP	282	HTTP/1.1 200 OK (text/plain)
2055	273.370887	192.168.1.7	65.61.137.117	HTTP	601	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)

► Frame 2055: 601 bytes on wire (4808 bits), 601 bytes captured (4808 bits)
► Ethernet II, Src: PcsCompu_e8:2a:b5 (08:00:27:e8:2a:b5), Dst: 80:16:05:ec:69:e0 (08:16:05:ec:69:e0)
► Internet Protocol Version 4, Src: 192.168.1.7, Dst: 65.61.137.117
► Transmission Control Protocol, Src Port: 50032, Dst Port: 80, Seq: 1, Ack: 1, Len: 535
▼ Hypertext Transfer Protocol
► POST /doLogin HTTP/1.1\r\nHost: www.altoromutual.com\r\nUser-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:59.0) Gecko/20100101 Firefox/59.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nReferer: http://www.altoromutual.com/login.jsp\r\nContent-Type: application/x-www-form-urlencoded\r\n► Content-Length: 37\r\n

0000 80 16 05 ec 69 e0 08 00 27 e8 2a b5 08 00 45 00i... !*...E.
0010 02 4b b0 84 40 00 40 06 fb c6 c0 a8 01 07 41 3d .K..@.A=
0020 89 75 c3 70 00 50 b9 14 40 b2 80 ce 72 d9 80 18 .u.p.P. @....r...
0030 00 e5 8e 9f 00 00 01 01 08 0a c6 13 f0 8c 01 a3

File: "/home/analyst/Desktop/httpdu... Packets: 2398 · Displayed: 50 (2.1%) · Load time: 0:00.014 Profile: Default

Ora utilizzerai tcpdump dalla riga di comando di una workstation Linux per catturare il traffico HTTPS. Dopo aver avviato tcpdump, genererai traffico HTTPS mentre tcpdump registra il contenuto del traffico di rete. Questi record saranno nuovamente analizzati utilizzando Wireshark. Mentre sei nel terminale, immetti il comando “sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap”. Immetti la password cyberops per l'analista utente quando richiesto. Apriamo un browser Web dalla barra di avvio all'interno della VM CyberOps Workstation. Andare su www.netacad.com e accediamo , una volta fatto chiudiamo il browser e ritorniamo alla finestra del terminale in cui è in esecuzione tcpdump. Digitare CTRL+C per interrompere la cattura del pacchetto.



Ora nuovamente sul desktop avremo un nuovo file ma stavolta “HTTPS” dove faremo doppio clic per aprirlo e si attiverà WhireShark , dove andremo subito immettere nella barra dei filtri questo “tcp.port==443” e fai clic su Applica . Sfoglia i diversi messaggi “HTTPS” e seleziona messaggio “Dati applicazione”. Espandiamo completamente la sezione Secure Sockets Layer e andremo a cliccare su “ dati applicazione crittografati” , li troveremo il payload anche se non si vedrà in chiaro poichè crittografato tramite TLSv1.2.



httpsdump.pcap [Wireshark 2.5.1]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.port==443 Go back in packet history Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
79	29.810129	192.168.1.7	34.120.5.221	TCP	74	32250 → 445 [RST] Seq=296 Win=0 Len=0
80	29.816434	34.120.5.221	192.168.1.7	TLSv1.2	141	Application Data

[TCP Segment Len: 75]
Sequence number: 3295 (relative sequence number)
[Next sequence number: 3370 (relative sequence number)]
Acknowledgment number: 296 (relative ack number)
1000 = Header Length: 32 bytes (8)
▶ Flags: 0x018 (PSH, ACK)
Window size value: 1050
[Calculated window size: 268800]
[Window size scaling factor: 256]
Checksum: 0x4221 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
▶ [SEQ/ACK analysis]
▶ [Timestamps]
TCP payload (75 bytes)

▼ Secure Sockets Layer
▼ TLSv1.2 Record Layer: Application Data Protocol: http2
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 70
Encrypted Application Data: 00000000000000014ca56bb487d4433914b74a4f713811f5...

0040 00 5a 17 03 03 00 46 00 00 00 00 00 00 01 4c .Z....F.....L
0050 a5 6b b4 87 d4 43 39 14 b7 4a 4f 71 38 11 f5 74 .k...C9. .JOq8..t
0060 d9 fb 9e 53 79 75 76 4a df ae 6e da 6e 80 19 84 ...Syuvj ..n.n...
0070 e0 3f 35 a3 a9 63 14 d2 7b f9 a8 bb 14 c2 6a 73 .?5..c..{....is

Secure Sockets Layer (ssl), 75 bytes Packets: 8303 · Displayed: 5839 (70.3%) · Load time: 0:00.059 Profile: Default

Matteo Piccinini