



Utilizzo di Windows PowerShel

Di Carmine Malangone



INDICE

- Introduzione
- Obiettivi
- Accedere a PowerShell
- Esplorazione dei comandi
- Comandi cmdlet
- Comandi Netstart
- Gestione del cestino
- Conclusioni



Introduzione

PowerShell rappresenta uno degli strumenti più potenti e versatili per l'amministrazione di sistemi Windows. Si distingue per essere sia una console di comando che un linguaggio di scripting, consentendo l'automazione e la gestione avanzata delle risorse. Questo laboratorio mira a esplorare alcune delle principali funzionalità di PowerShell, fornendo un'introduzione pratica ai suoi comandi, ai cmdlet e alle sue capacità di integrazione con altri strumenti di sistema. L'obiettivo è acquisire familiarità con PowerShell attraverso esercitazioni mirate, approfondendo l'uso del prompt dei comandi, l'esecuzione di cmdlet specifici e alcune funzionalità di gestione del sistema.



Obiettivi

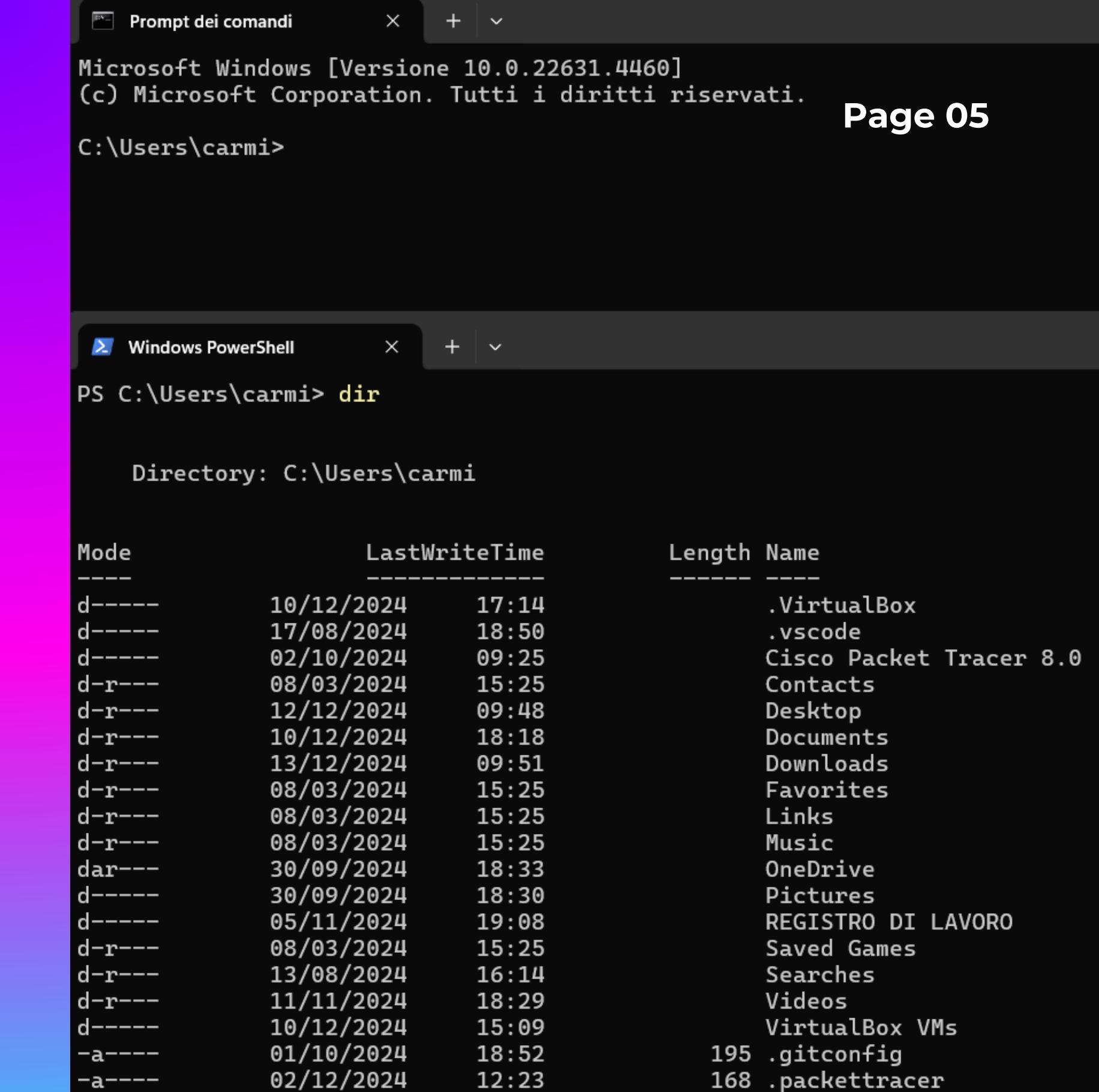
1. Accedere alla console di **PowerShell**.
2. Esplorare e confrontare i comandi del prompt dei comandi con quelli di **PowerShell**.
3. Approfondire l'uso dei cmdlet.
4. Analizzare l'uso del comando **netstat** tramite **PowerShell**.
5. Gestire il Cestino di Windows utilizzando comandi **PowerShell**.

Accedere alla console di PowerShell.

Accesso alla console di PowerShell L'accesso a PowerShell si effettua tramite il menu Start, cercando e selezionando “PowerShell”. Parallelamente, il prompt dei comandi è accessibile con lo stesso metodo. Questi due strumenti, pur avendo alcune somiglianze, differiscono profondamente in termini di funzionalità e flessibilità.

Cos’è PowerShell

PowerShell è una shell di scripting e un linguaggio di automazione sviluppato da Microsoft, progettato per la gestione e l'amministrazione dei sistemi. Ecco un elenco delle principali caratteristiche e utilizzi di PowerShell:



The image shows two separate windows of the Windows Command Prompt (cmd.exe) running on Windows 10. Both windows have the title 'Prompt dei comandi'.
The top window displays the system information:
Microsoft Windows [Versione 10.0.22631.4460]
(c) Microsoft Corporation. Tutti i diritti riservati.
C:\Users\carmi>
The bottom window has the title 'Windows PowerShell' and displays the command 'dir' (list directory). It shows the contents of the 'C:\Users\carmi' directory, listing various folders and files with their last write times and sizes:
PS C:\Users\carmi> dir

Directory: C:\Users\carmi

Mode LastWriteTime Length Name
---- <----- <-----
d---- 10/12/2024 17:14 .VirtualBox
d---- 17/08/2024 18:50 .vscode
d---- 02/10/2024 09:25 Cisco Packet Tracer 8.0
d-r-- 08/03/2024 15:25 Contacts
d-r-- 12/12/2024 09:48 Desktop
d-r-- 10/12/2024 18:18 Documents
d-r-- 13/12/2024 09:51 Downloads
d-r-- 08/03/2024 15:25 Favorites
d-r-- 08/03/2024 15:25 Links
d-r-- 08/03/2024 15:25 Music
dar-- 30/09/2024 18:33 OneDrive
d---- 30/09/2024 18:30 Pictures
d---- 05/11/2024 19:08 REGISTRO DI LAVORO
d-r-- 08/03/2024 15:25 Saved Games
d-r-- 13/08/2024 16:14 Searches
d-r-- 11/11/2024 18:29 Videos
d---- 10/12/2024 15:09 VirtualBox VMs
-a--- 01/10/2024 18:52 .gitconfig
-a--- 02/12/2024 12:23 .packettracer
195 .gitconfig
168 .packettracer

Prompt dei comandi

```
Il volume nell'unità C è OS
Numero di serie del volume: E428-DF0F

Directory di C:\Users\carmi

05/12/2024 22:44 <DIR> .
13/08/2024 15:14 <DIR> ..
01/10/2024 17:52 195 .gitconfig
02/12/2024 12:23 168 .packettracer
10/12/2024 17:14 <DIR> .VirtualBox
17/08/2024 17:50 <DIR> .vscode
02/10/2024 08:25 <DIR> Cisco Packet Tracer 8.0
08/03/2024 15:25 <DIR> Contacts
12/12/2024 09:48 <DIR> Desktop
10/12/2024 18:18 <DIR> Documents
13/12/2024 09:51 <DIR> Downloads
08/03/2024 15:25 <DIR> Favorites
08/03/2024 15:25 <DIR> Links
08/03/2024 15:25 <DIR> Music
30/09/2024 17:33 <DIR> OneDrive
30/09/2024 17:30 <DIR> Pictures
05/11/2024 19:08 <DIR> REGISTRO DI LAVORO
08/03/2024 15:25 <DIR> Saved Games
13/08/2024 15:14 <DIR> Searches
11/11/2024 18:29 <DIR> Videos
10/12/2024 15:09 <DIR> VirtualBox VMs
2 File 363 byte
19 Directory 28.638.994.432 byte disponibili
```

c:\Users\carmi>

Windows PowerShell

```
PS C:\Users\carmi> dir
```

Directory: C:\Users\carmi

Mode	LastWriteTime	Name
d----	10/12/2024 17:14	.VirtualBox
d----	17/08/2024 18:50	.vscode
d----	02/10/2024 09:25	Cisco Packet Tracer 8.0
d-r---	08/03/2024 15:25	Contacts
d-r---	12/12/2024 09:48	Desktop
d-r---	10/12/2024 18:18	Documents
d-r---	13/12/2024 09:51	Downloads
d-r---	08/03/2024 15:25	Favorites
d-r---	08/03/2024 15:25	Links
d-r---	08/03/2024 15:25	Music
dar---	30/09/2024 18:33	OneDrive
d----	30/09/2024 18:30	Pictures
d----	05/11/2024 19:08	REGISTRO DI LAVORO
d-r---	08/03/2024 15:25	Saved Games
d-r---	13/08/2024 16:14	Searches
d-r---	11/11/2024 18:29	Videos
d----	10/12/2024 15:09	VirtualBox VMs
-a----	01/10/2024 18:52	195 .gitconfig
-a----	02/12/2024 12:23	168 .packettracer

Esplorazione dei comandi

Page 06

Il comando **dir**, eseguito in entrambe le console, restituisce un elenco delle sottodirectory e dei file con informazioni come tipo, dimensione, data e ora dell'ultima modifica. In PowerShell, l'output è più dettagliato grazie agli attributi aggiuntivi visualizzati. Provando altri comandi come **ping**, **cd** e **ipconfig**, si nota che gli output sono simili, dimostrando una continuità di utilizzo per chi proviene dal prompt dei comandi.

```
Windows PowerShell      x + v
PS C:\Users\carmi> ipconfig
Configurazione IP di Windows

Scheda Ethernet Ethernet:
  Suffisso DNS specifico per connessione:
  Indirizzo IPv6 locale rispetto al collegamento . : fe80::12d8:b9ae:ada9:e2c1%28
  Indirizzo IPv4. . . . . : 192.168.56.1
  Subnet mask . . . . . : 255.255.255.0
  Gateway predefinito . . . . . :

Scheda LAN wireless Connessione alla rete locale (LAN)* 9:
  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:
  Indirizzo IPv6 locale rispetto al collegamento . : fe80::bbd4:f40b:ad46:a0a3%12
  Indirizzo IPv4. . . . . : 192.168.149.250
  Subnet mask . . . . . : 255.255.255.0
  Gateway predefinito . . . . . : 192.168.149.34

Scheda Ethernet Connessione di rete Bluetooth:
  Stato supporto. . . . . : Supporto disconnesso
  Suffisso DNS specifico per connessione:
PS C:\Users\carmi>
```

Ipconfig PowerShell

```
C:\Users\carmi>ipconfig
Configurazione IP di Windows

Scheda Ethernet Ethernet:
  Suffisso DNS specifico per connessione:
  Indirizzo IPv6 locale rispetto al collegamento . : fe80::12d8:b9ae:ada9:e2c1%28
  Indirizzo IPv4. . . . . : 192.168.56.1
  Subnet mask . . . . . : 255.255.255.0
  Gateway predefinito . . . . . :

Scheda LAN wireless Connessione alla rete locale (LAN)* 9:
  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:
  Indirizzo IPv6 locale rispetto al collegamento . : fe80::bbd4:f40b:ad46:a0a3%12
  Indirizzo IPv4. . . . . : 192.168.149.250
  Subnet mask . . . . . : 255.255.255.0
  Gateway predefinito . . . . . : 192.168.149.34

Scheda Ethernet Connessione di rete Bluetooth:
  Stato supporto. . . . . : Supporto disconnesso
  Suffisso DNS specifico per connessione:
```

Ipconfig Command Prompt

Comandi cmdlet

I cmdlet sono comandi nativi di PowerShell costruiti seguendo la sintassi verbo-nome. Ad esempio, per elencare file e directory, si utilizza **Get-ChildItem**. Questo è confermato eseguendo il comando **Get-Alias dir**, che mostra l'alias **dir** collegato al cmdlet **Get-ChildItem**. Ulteriori informazioni sui cmdlet sono accessibili tramite ricerche su Internet o comandi integrati di PowerShell come **Get-Help**.

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

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

PS C:\Users\carmi> Get-Alias dir

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

PS C:\Users\carmi>
```

Utilizzo del comando netstat

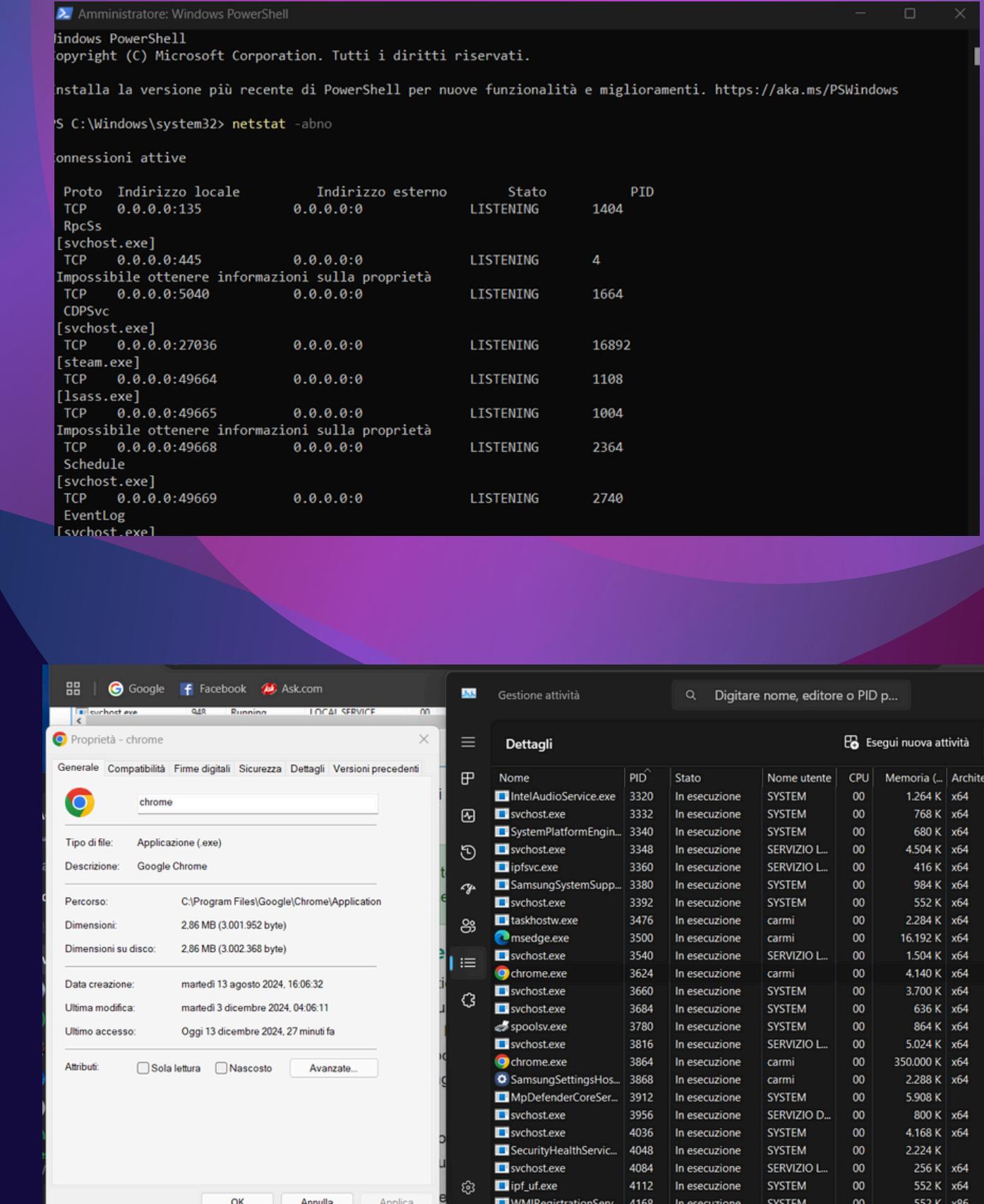
PowerShell consente di eseguire il comando **netstat** per monitorare le connessioni di rete e i processi correlati. Di seguito sono riportati alcuni degli usi principali di **netstat** in **PowerShell**:

- **Visualizzazione delle opzioni disponibili:** Il comando **netstat -h** elenca tutte le opzioni utilizzabili con **netstat**, fornendo una guida per personalizzare l'analisi delle connessioni di rete.
- **Tabella di routing:** Utilizzando **netstat -r**, è possibile visualizzare la tabella di routing che include i percorsi attivi e le informazioni sugli indirizzi di rete.
- **Connessioni TCP attive e processi associati:** Il comando **netstat -abno** elenca tutte le connessioni TCP attive, indicando anche il **PID** (Process Identifier) dei processi correlati. Questo è utile per identificare eventuali processi sospetti o indesiderati.

In particolare, è possibile:

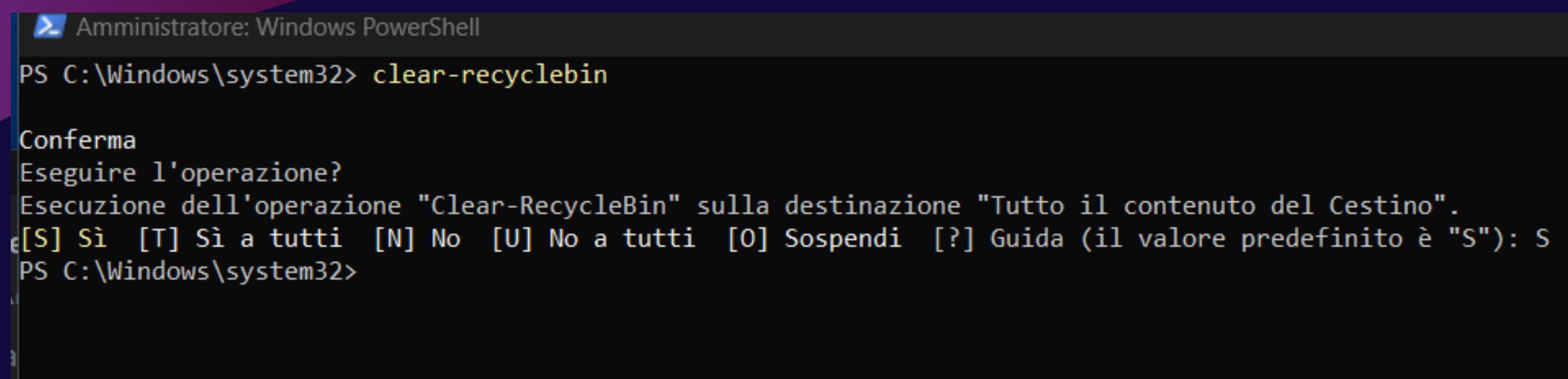
1. Eseguire **netstat -abno** per identificare i PID delle connessioni attive.
2. Aprire il Task Manager e ordinare i processi per PID tramite la scheda “**Dettagli**”.
3. Selezionare un PID specifico e accedere alle sue proprietà (clic destro sul processo) per ottenere informazioni aggiuntive.

Questa combinazione di strumenti consente di migliorare la gestione delle risorse di rete, identificare problemi di sicurezza e monitorare l'attività dei processi in tempo reale.



GESTIONE DEL CESTINO

PowerShell offre comandi per semplificare operazioni comuni. Ad esempio, il comando **Clear-RecycleBin** consente di svuotare il Cestino in modo rapido e automatizzato. Questo comando si rivela particolarmente utile in ambienti aziendali per gestire numerosi dispositivi in rete, riducendo il tempo necessario rispetto ai metodi tradizionali.



The screenshot shows a Windows PowerShell window titled "Amministratore: Windows PowerShell". The command "clear-recyclebin" is entered at the prompt. A confirmation dialog box appears, asking "Conferma Eseguire l'operazione?". The message below it states "Esecuzione dell'operazione \"Clear-RecycleBin\" sulla destinazione \"Tutto il contenuto del Cestino\"." and provides options "[S] Sì [T] Sì a tutti [N] No [U] No a tutti [O] Sospendi [?] Guida (il valore predefinito è \"S\")." The user has selected "[S] Sì". The command history at the bottom shows "PS C:\Windows\system32>".

```
PS C:\Windows\system32> clear-recyclebin

Conferma
Eseguire l'operazione?

Esecuzione dell'operazione "Clear-RecycleBin" sulla destinazione "Tutto il contenuto del Cestino".
[S] Sì [T] Sì a tutti [N] No [U] No a tutti [O] Sospendi [?] Guida (il valore predefinito è "S"): S
PS C:\Windows\system32>
```



Conclusioni

Il laboratorio ha permesso di esplorare le potenzialità di PowerShell, evidenziandone la flessibilità e l'efficienza rispetto al prompt dei comandi tradizionale. Dall'esecuzione di comandi comuni all'uso di cmdlet e alla gestione avanzata delle risorse di sistema, PowerShell si è dimostrato uno strumento indispensabile per amministratori di sistema e professionisti IT. La sua capacità di integrare funzionalità di scripting con comandi interattivi lo rende una piattaforma ideale per automatizzare attività complesse e migliorare la produttività.

Consigliamo di approfondire ulteriormente l'uso dei cmdlet e la creazione di script per sfruttare appieno le sue potenzialità.



Parte 2

Utilizzo di Wireshark per Esaminare il Traffico HTTP e HTTPS

Di Carmine Malangone



INDICE

Obiettivi del laboratorio

Contesto e risorse

Svolgimento del laboratorio

- Parte 1: Cattura e traffico visualizzazione HTTP
- Parte 2: Cattura e traffico visualizzazione HTTPS

Conclusioni



Introduzione

Il traffico web è uno degli elementi fondamentali delle comunicazioni digitali moderne, reso possibile da protocolli come HTTP e HTTPS. HTTP (HyperText Transfer Protocol) è il protocollo più comune per la trasmissione di dati sul web, ma manca di qualsiasi meccanismo di protezione per i dati scambiati. HTTPS, d'altra parte, utilizza la crittografia per proteggere la confidenzialità e l'integrità delle informazioni trasmesse.

Questa relazione analizza le caratteristiche del traffico HTTP e HTTPS, evidenziandone le differenze attraverso la cattura e l'analisi dei pacchetti di rete. L'obiettivo del laboratorio è acquisire competenze pratiche nell'uso di strumenti come tcpdump e Wireshark per esaminare le comunicazioni su questi protocolli, comprendendo i rischi associati e il ruolo della crittografia.

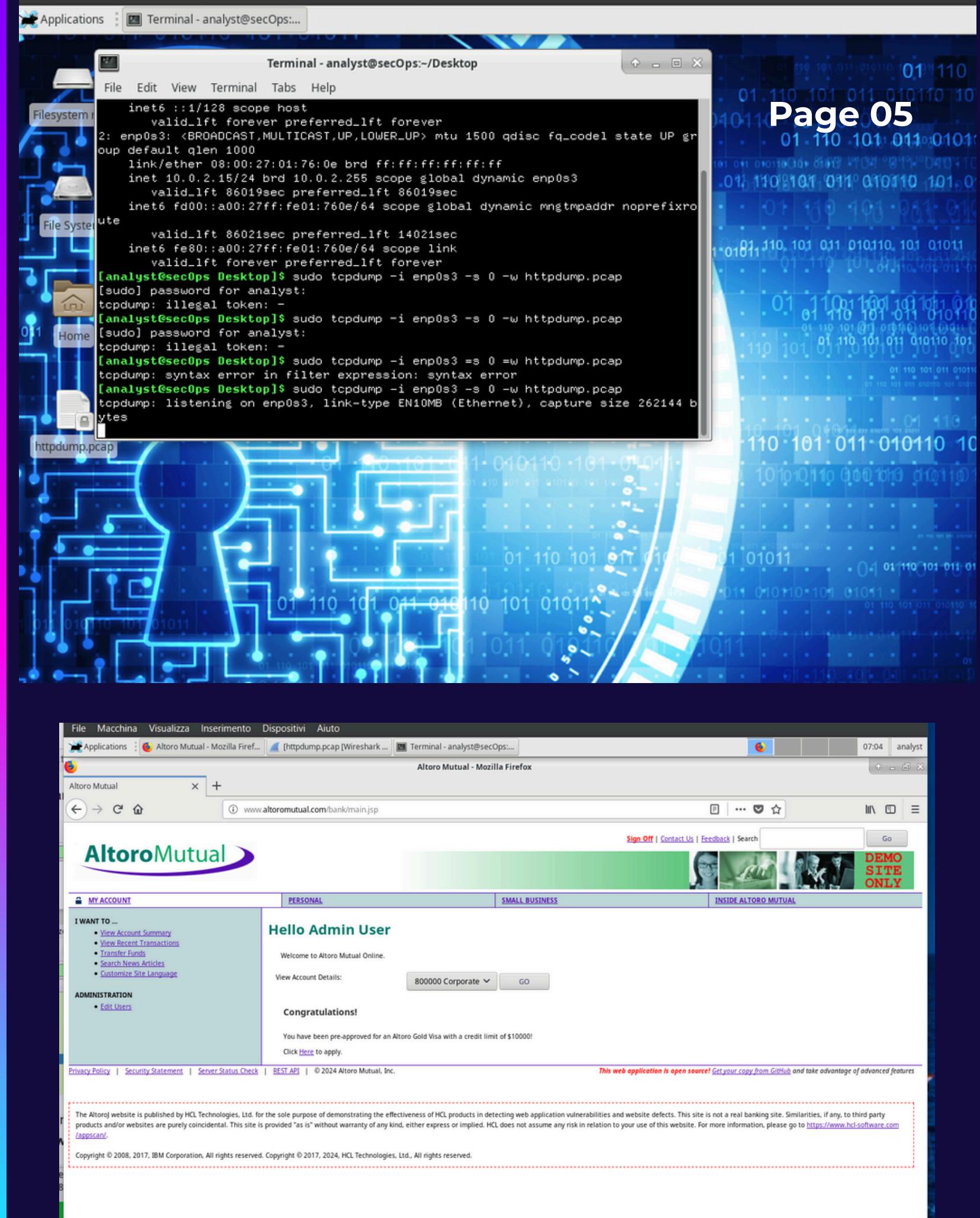


Obiettivi

1. **Catturare e visualizzare il traffico HTTP.**
2. **Catturare e visualizzare il traffico HTTPS.**

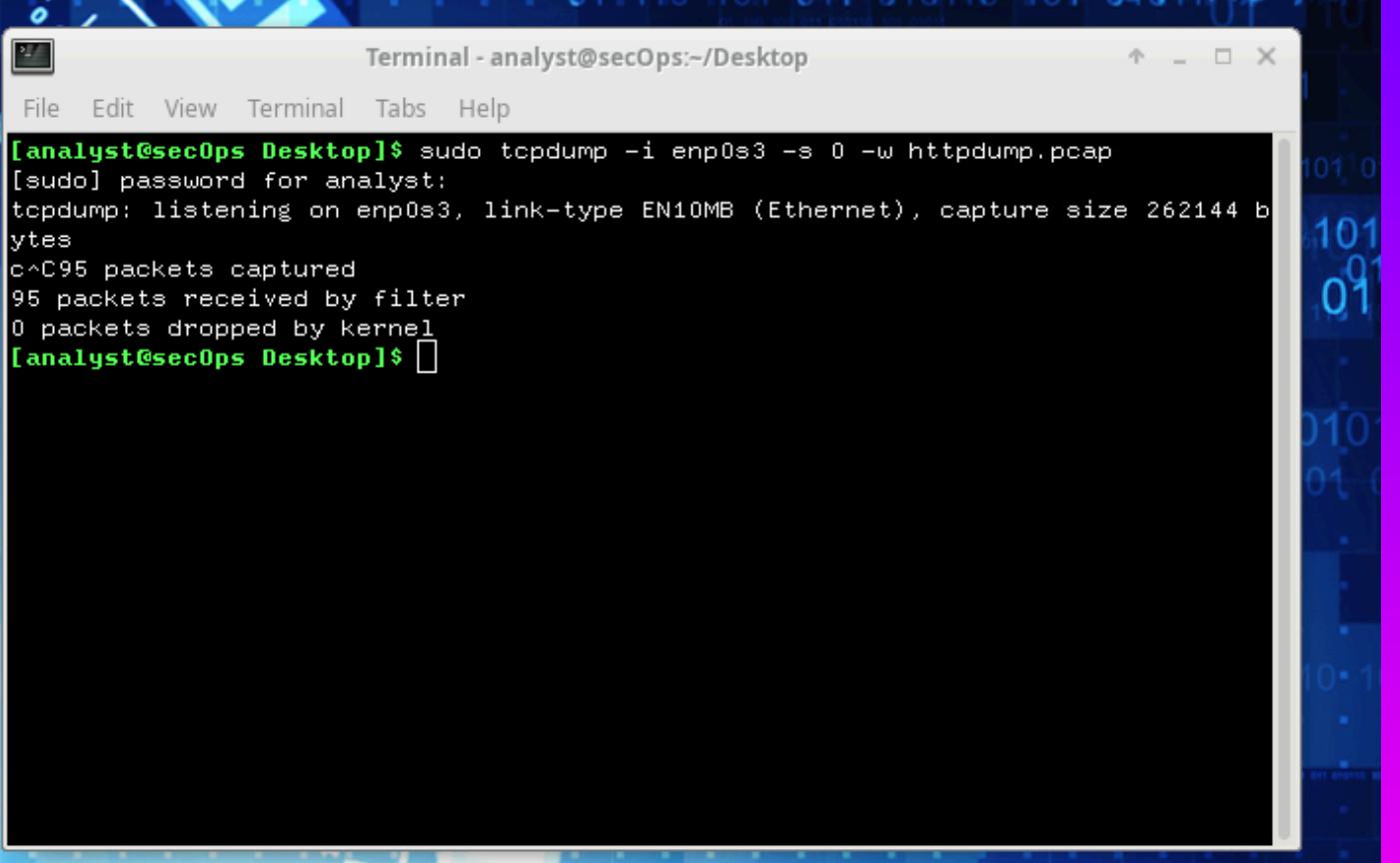
Avvio di tcpdump

- Lanciare il comando **`sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap`** per catturare il traffico HTTP sull'interfaccia specificata.
- Avviare un browser web e accedere al sito Accesso alla console di PowerShell. L'accesso a PowerShell si effettua tramite il menu Start, cercando e selezionando “PowerShell”. Parallelamente, il prompt dei comandi è accessibile con lo stesso metodo. Questi due strumenti, pur avendo alcune somiglianze, differiscono profondamente in termini di funzionalità e flessibilità.
- Poiché il sito utilizza HTTP, i dati trasmessi non sono crittografati.
- Inserire le credenziali di esempio (Admin/Admin) e accedere al sito.
- Arrestare la cattura premendo **`CTRL+C`** nel terminale.

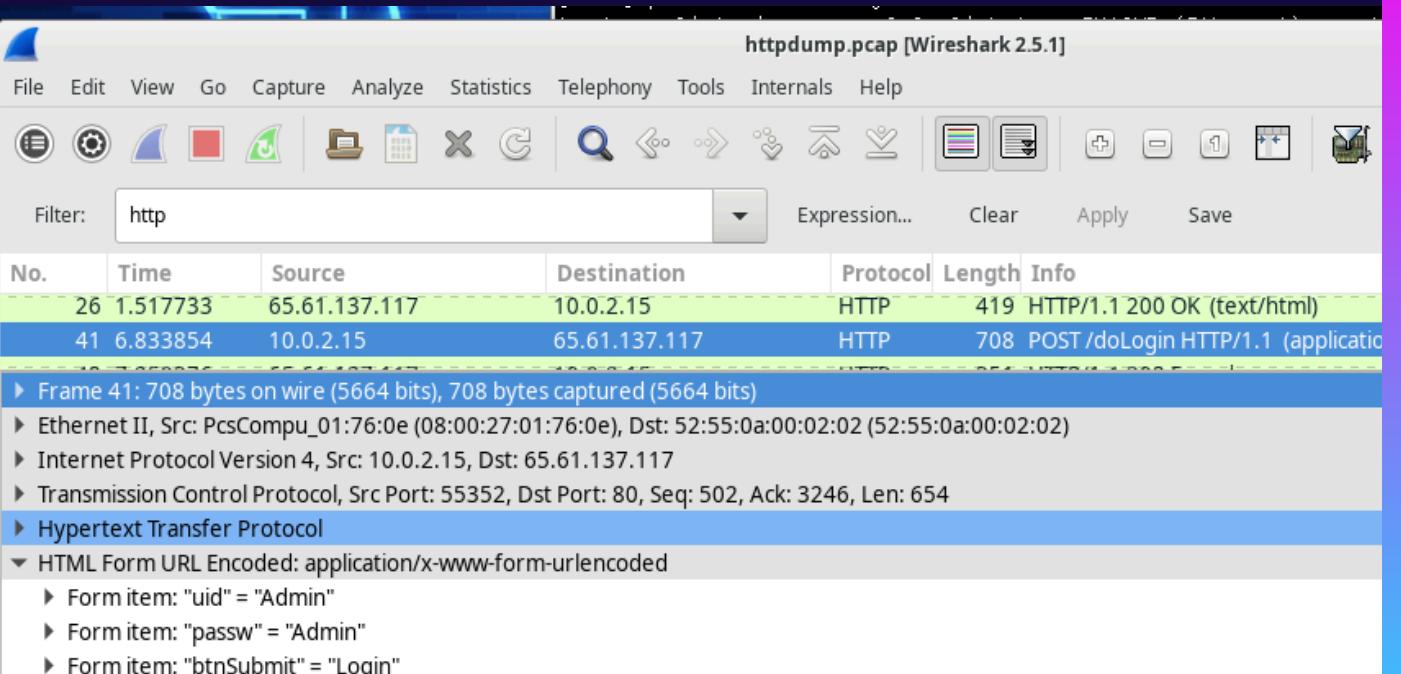


Analisi con Wireshark

- Aprire il file **httpdump.pcap** con Wireshark e filtrare il traffico utilizzando il filtro **http**.
- Esaminare il messaggio POST nella sezione inferiore, espandendo la sezione **HTML Form URL Encoded**. Questo permette di visualizzare in chiaro l'UID e la password utilizzati.



```
[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
c^C95 packets captured
95 packets received by filter
0 packets dropped by kernel
[analyst@secOps Desktop]$
```



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
26	1.517733	65.61.137.117	10.0.2.15	HTTP	419	HTTP/1.1 200 OK (text/html)
41	6.833854	10.0.2.15	65.61.137.117	HTTP	708	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)

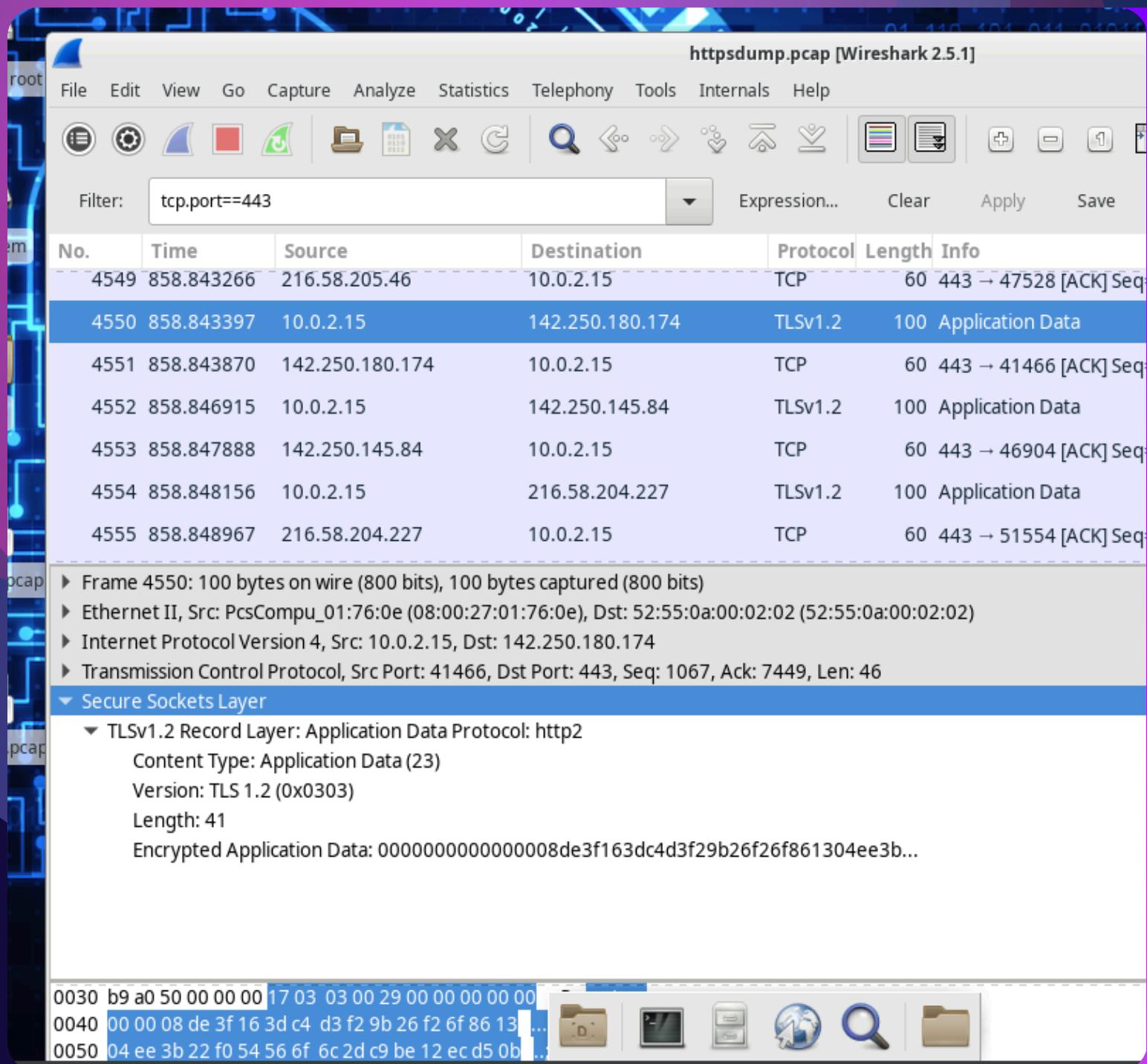
Frame 41: 708 bytes on wire (5664 bits), 708 bytes captured (5664 bits)
Ethernet II, Src: PcsCompu_01:76:0e (08:00:27:01:76:0e), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 65.61.137.117
Transmission Control Protocol, Src Port: 55352, Dst Port: 80, Seq: 502, Ack: 3246, Len: 654
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "uid" = "Admin"
Form item: "passw" = "Admin"
Form item: "btnSubmit" = "Login"



CATTURA E VISUALIZZAZIONE DEL TRAFFICO HTTPS

- Avviare `tcpdump` con il comando **sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap** per catturare il traffico HTTPS.
- Utilizzare il browser per accedere al sito www.netacad.com, che utilizza HTTPS.
- Accedere con le credenziali personali e chiudere il browser.
- Arrestare la cattura premendo **CTRL+C**.

```
Terminal - analyst@secOps:~/Desktop
File Edit View Terminal Tabs Help
[analyst@secOps Desktop]$ 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
^C4655 packets captured
4655 packets received by filter
0 packets dropped by kernel
[analyst@secOps Desktop]$
```



- Aprire il file **httpsdump.pcap** con **Wireshark**.
- Filtrare il traffico utilizzando il filtro **tcp.port==443** per isolare il traffico **HTTPS**.
- Analizzare i messaggi. Dopo la sezione **TCP**, si trova una sezione **Secure Sockets Layer (SSL/TLS)** che contiene i dati crittografati.
- Espandere la sezione **Dati applicazione crittografati**. Il payload risulta incomprensibile, confermando che il traffico **HTTPS è cifrato e protetto**.

Analisi con Wireshark



Conclusioni

Il laboratorio ha evidenziato le differenze sostanziali tra HTTP e HTTPS in termini di sicurezza:

- Con HTTP, i dati trasmessi sono visibili in chiaro, rendendoli vulnerabili a intercettazioni e attacchi di tipo man-in-the-middle.
- HTTPS protegge i dati attraverso la crittografia, rendendo il contenuto del traffico illeggibile senza le chiavi di decrittazione appropriate.

L'utilizzo di strumenti come tcpdump e Wireshark si è rivelato essenziale per comprendere la struttura dei pacchetti e per analizzare il traffico di rete. Questi strumenti sono fondamentali per gli analisti di sicurezza e gli amministratori di rete, sia per individuare vulnerabilità sia per monitorare l'attività sospetta.



Bonus 1

Esplorazione di Nmap

Di Carmine Malangone



INDICE

- 1. Introduzione**
- 2. Obiettivi del laboratorio**
- 3. Contesto e risorse**
- 4. Svolgimento del laboratorio**
 - **Parte 1: Esplorazione di Nmap**
 - **Parte 2: Scansione delle porte aperte**
- 5. Conclusioni**



Introduzione

Il traffico web è uno degli elementi fondamentali delle comunicazioni digitali moderne, reso possibile da protocolli come HTTP e HTTPS. HTTP (HyperText Transfer Protocol) è il protocollo più comune per la trasmissione di dati sul web, ma manca di qualsiasi meccanismo di protezione per i dati scambiati. HTTPS, d'altra parte, utilizza la crittografia per proteggere la confidenzialità e l'integrità delle informazioni trasmesse.

Questa relazione analizza le caratteristiche del traffico HTTP e HTTPS, evidenziandone le differenze attraverso la cattura e l'analisi dei pacchetti di rete. L'obiettivo del laboratorio è acquisire competenze pratiche nell'uso di strumenti come tcpdump e Wireshark per esaminare le comunicazioni su questi protocolli, comprendendo i rischi associati e il ruolo della crittografia.



Obiettivi

1. La scansione delle porte è una tecnica cruciale per l'analisi della sicurezza e il monitoraggio delle reti. Tra gli strumenti più popolari per questa attività, Nmap si distingue per la sua versatilità e potenza. Nmap (Network Mapper) è un'utilità open-source utilizzata per la scoperta di rete e l'audit di sicurezza.
2. Questa relazione descrive l'utilizzo di Nmap per esplorare una rete, identificare porte aperte, servizi attivi e sistemi operativi. Il laboratorio offre una comprensione pratica delle funzionalità principali dello strumento e delle sue applicazioni.

```
NMAP(1)          Nmap Reference Guide          NMAP(1)

NAME
nmap - Network exploration tool and security / port scanner

SYNOPSIS
nmap [Scan Type...] [Options] {target specification}

DESCRIPTION
Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key among that

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: li86-221.members.linode.com
Not shown: 995 closed ports
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 5.3p1 Debian 3ubuntu7 (protocol
| ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (
|_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 1dp
1720/tcp  filtered H.323/Q.931
```

Esplorazione di Nmap

- Avviare la macchina virtuale CyberOps Workstation e aprire un terminale.
- Eseguire il comando man nmap per accedere al manuale di Nmap.
- Identificare la descrizione generale di Nmap e la funzione degli switch principali, come -A per il rilevamento avanzato e -T4 per ottimizzare la velocità di scansione.
- Usare il comando /example per esplorare esempi pratici e navigare nei risultati utilizzando i tasti n e q.

Domande esplorative:

- Cos'è Nmap? Nmap è uno strumento per la scansione di rete e la scoperta di host e servizi attivi.
- A cosa serve l'interruttore -A? Abilita il rilevamento di sistema operativo, versioni di software, script e traceroute.
- A cosa serve l'interruttore -T4? Ottimizza la velocità della scansione riducendo i ritardi.



```
[analyst@secOps Desktop]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 09:22 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000033s 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 5
  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 12.13 seconds
[analyst@secOps Desktop]$
```

- Eseguire il comando `nmap -A -T4 localhost` per identificare le porte e i servizi attivi sul proprio host locale.
- Risultati: Porte aperte rilevate:
 - 21/tcp: FTP (vsftpd)
 - 22/tcp: SSH (OpenSSH)

Scansione del localhost



```
t@secOps Desktop]$ nmap -A -T4 network address/prefix
g Nmap 7.70 ( https://nmap.org ) at 2024-12-13 09:28 EST
to resolve "network".
to split netmask from target expression: "address/prefix"
: No targets were specified, so 0 hosts scanned.
ne: 0 IP addresses (0 hosts up) scanned in 0.49 seconds
t@secOps Desktop]$ nmap -A -T4 10.0.2.0/24
g Nmap 7.70 ( https://nmap.org ) at 2024-12-13 09:29 EST
an report for 10.0.2.15
  up (0.000049s latency).
wn: 998 closed ports
STATE SERVICE VERSION
open  ftp      vsftpd 2.0.8 or later
non: Anonymous FTP login allowed (FTP code 230)
--r--  1 0        0          0 Mar 26  2018 ftp_test
yst:
T:
erver status:
Connected to 10.0.2.15
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 5
vsFTPD 3.0.3 - secure, fast, stable
f status
open  ssh      OpenSSH 7.7 (protocol 2.0)
ostkey:
8 b4:91:f9:f9:d6:79:25:86:44:c7:9e:f8:e0:e7:5b:bb (RSA)
 06:12:75:fe:b3:89:29:4f:8d:f3:9e:9a:d7:c6:03:52 (ECDSA)
 34:5d:f2:d3:5b:9f:b4:b6:08:96:a7:30:52:8c:96:06 (ED25519)
Info: Host: Welcome

detection performed. Please report any incorrect results at https://nmap.org/su
ne: 256 IP addresses (1 host up) scanned in 20.85 seconds
t@secOps Desktop]$ █
```

- Determinare l'indirizzo IP della VM con il comando ip address.
- Eseguire nmap -A -T4 indirizzo_rete/prefisso per esplorare la LAN.
- Risultati:
 - Indirizzi IP rilevati: variabile a seconda della rete.
 - Servizi attivi sugli host: ad esempio, HTTP, SMB, ecc.

Scansione della rete locale



```
analyst@secOps Desktop]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2024-01-11 10:45 UTC
Nmap scan report for scanme.nmap.org (45.33.32.1)
Host is up (0.11s latency).
Other addresses for scanme.nmap.org (not scanned)
Not shown: 996 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu
           ssh-hostkey:
             1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34
               2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14
               256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:1
             - 256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:0
0/tcp    open  http         Apache httpd 2.4.7 (Ubuntu)
           _http-server-header: Apache/2.4.7 (Ubuntu)
           _http-title: Go ahead and ScanMe!
929/tcp   open  nping-echo  Nping echo
1337/tcp  open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux

Service detection performed. Please report any
issues at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.00 seconds
analyst@secOps Desktop]$
```

- Accedere al sito scanme.nmap.org per ottenere l'autorizzazione alla scansione.
- Eseguire il comando `nmap -A -T4 scanme.nmap.org`.
- Risultati: Porte aperte rilevate:
 - 22/tcp: SSH
 - 80/tcp: HTTP
 - 9929/tcp: ping-echo
 - 31337/tcp: tcpwrapped
- Sistema operativo rilevato: Ubuntu Linux.

Scansione di un server remoto



Conclusioni

Questo laboratorio ha evidenziato l'importanza di Nmap per la scoperta e l'analisi delle reti. Le principali osservazioni includono:

La scansione del localhost permette di identificare i servizi attivi sul proprio sistema.

La scansione di una rete locale consente di individuare host attivi e servizi esposti, fornendo informazioni critiche per l'audit di sicurezza.

La scansione di server remoti, come scanme.nmap.org, dimostra come Nmap possa essere utilizzato per testare la connettività e la configurazione di un sistema remoto.