

ANALISI AVANZATE APPROCCIO PRAATICO

INDICE

Windows PowerShell

- Accesso a PowerShell
- Comandi del CMD e PowerShell
- Cmdlet
- Comandi netstat in PowerShell
- Svuotare il cestino con PowerShell
- Riflessioni



OBIETTIVO

L'obiettivo del laboratorio è esplorare alcune delle funzioni di PowerShell, uno strumento potente per l'automazione e la gestione di sistemi Windows.

ACCESSO A POWERSHELL

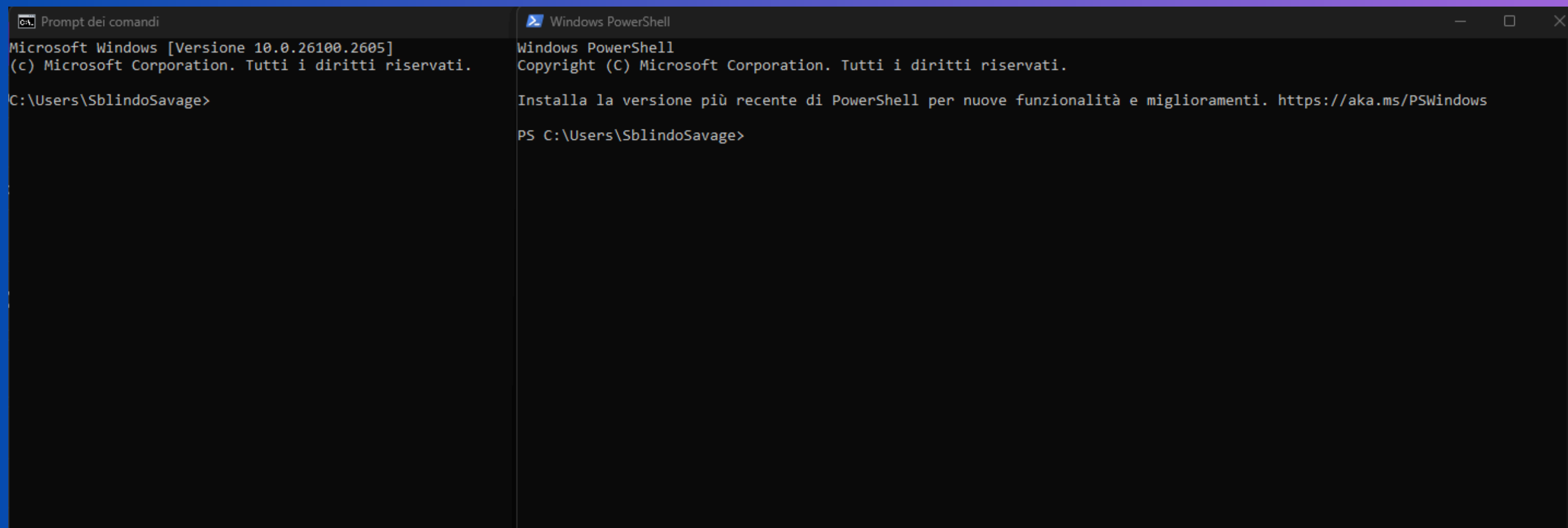
Windows PowerShell

Per accedere alla console di PowerShell:

- Fare clic su Start.
- Cercare e selezionare Windows PowerShell.

Per confrontare i comandi tra PowerShell e il Prompt dei comandi:

- Cercare e selezionare Prompt dei comandi.



The image shows two side-by-side terminal windows. The left window is titled 'Prompt dei comandi' and displays the standard Windows command prompt interface, including the version number 10.0.26100.2605 and the user path C:\Users\SblindoSavage. The right window is titled 'Windows PowerShell' and displays the PowerShell interface, including the copyright notice and a message about installing the latest version of PowerShell.

```
Prompt dei comandi
Microsoft Windows [Versione 10.0.26100.2605]
(c) Microsoft Corporation. Tutti i diritti riservati.
C:\Users\SblindoSavage>

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\SblindoSavage>
```

COMANDI CMD E POWERSHELL

Windows PowerShell

Comando dir:

- In entrambi gli ambienti, il comando dir restituisce un elenco di sottodirectory e file con informazioni come dimensioni, data e ora dell'ultima modifica. In PowerShell sono mostrati anche attributi/modalità dei file.

Windows PowerShell				Prompt dei comandi			
Mode	LastWriteTime		Length Name				
----	-----		-----	----			
d-----	16/05/2021	12:21	.Origin	18/10/2024	11:50	<DIR>	..
d-----	18/08/2024	13:57	.prefs	30/09/2024	13:54		182 .gitconfig
d-----	16/05/2021	12:21	.QtWebEngineProcess	16/05/2021	11:21	<DIR>	.Origin
d-----	12/12/2024	14:02	.VirtualBox	21/10/2024	09:28		184 .packettracer
d-----	12/10/2024	16:47	.vscode	18/08/2024	12:57	<DIR>	.prefs
d-r---	17/02/2021	20:28	3D Objects	16/05/2021	11:21	<DIR>	.QtWebEngineProcess
d-----	14/05/2021	14:18	ansel	12/12/2024	14:02	<DIR>	.VirtualBox
d-----	02/10/2024	10:37	Cisco Packet Tracer 8.0	12/10/2024	15:47	<DIR>	.vscode
d-r---	18/10/2024	18:24	Contacts	17/02/2021	20:28	<DIR>	3D Objects
d-r---	27/10/2024	16:45	Desktop	14/05/2021	13:18	<DIR>	ansel
d-r---	18/10/2024	18:24	Documents	02/10/2024	09:37	<DIR>	Cisco Packet Tracer 8.0
d-r---	12/12/2024	16:48	Downloads	18/10/2024	17:24	<DIR>	Contacts
d-r---	18/10/2024	18:24	Favorites	27/10/2024	16:45	<DIR>	Desktop
d-r---	18/10/2024	18:24	Links	18/10/2024	17:24	<DIR>	Documents
d-r---	18/10/2024	18:24	Music	12/12/2024	16:48	<DIR>	Downloads
dar--l	16/01/2023	16:48	OneDrive	18/10/2024	17:24	<DIR>	Favorites
d-r---	13/12/2024	09:18	Pictures	18/10/2024	17:24	<DIR>	Links
d-r---	18/10/2024	18:24	Saved Games	18/10/2024	17:24	<DIR>	Music
d-r---	18/10/2024	18:24	Searches	16/01/2023	16:48	<DIR>	OneDrive
d-----	18/08/2024	13:56	TheoTown	13/12/2024	09:18	<DIR>	Pictures
d-r---	13/12/2024	08:57	Videos	18/10/2024	17:24	<DIR>	Saved Games
d-----	10/12/2024	14:39	VirtualBox VMs	18/10/2024	17:24	<DIR>	Searches
d-----	07/01/2024	03:46	Zomboid	18/08/2024	12:56	<DIR>	TheoTown
-a----	30/09/2024	14:54	182 .gitconfig	13/12/2024	08:57	<DIR>	Videos
-a----	21/10/2024	10:28	184 .packettracer	10/12/2024	14:39	<DIR>	VirtualBox VMs
				07/01/2024	03:46	<DIR>	Zomboid
				2 File			366 byte
				25 Directory			76.158.894.080 byte disponibili
PS C:\Users\SblindoSavage>				C:\Users\SblindoSavage>			

Altri comandi:

- Comandi come ping, cd e ipconfig generano risultati simili in entrambi gli ambienti.

Windows PowerShell		Prompt dei comandi	
Stato supporto. : Supporto disconnesso Suffisso DNS specifico per connessione:		Stato supporto. : Supporto disconnesso Suffisso DNS specifico per connessione:	
Scheda Ethernet Ethernet 4:		Scheda Ethernet Ethernet 4:	
Suffisso DNS specifico per connessione: Indirizzo IPv6 locale rispetto al collegamento . : fe80::26ca:c663:f942:d470%15 Indirizzo IPv4 configurazione automatica : 169.254.56.158 Subnet mask : 255.255.0.0 Gateway predefinito :		Suffisso DNS specifico per connessione: Indirizzo IPv6 locale rispetto al collegamento . : fe80::26ca:c663:f942:d470%15 Indirizzo IPv4 configurazione automatica : 169.254.56.158 Subnet mask : 255.255.0.0 Gateway predefinito :	
Scheda LAN wireless Connessione alla rete locale (LAN)* 1:		Scheda LAN wireless Connessione alla rete locale (LAN)* 1:	
Stato supporto. : Supporto disconnesso Suffisso DNS specifico per connessione:		Stato supporto. : Supporto disconnesso Suffisso DNS specifico per connessione:	
Scheda LAN wireless Connessione alla rete locale (LAN)* 3:		Scheda LAN wireless Connessione alla rete locale (LAN)* 3:	
Stato supporto. : Supporto disconnesso Suffisso DNS specifico per connessione:		Stato supporto. : Supporto disconnesso Suffisso DNS specifico per connessione:	
Scheda LAN wireless Wi-Fi:		Scheda LAN wireless Wi-Fi:	
Suffisso DNS specifico per connessione: homenet.telecomitalia.it Indirizzo IPv6 locale rispetto al collegamento . : fe80::482f:82d:ca3b:5e5e%18 Indirizzo IPv4. : 192.168.1.35 Subnet mask : 255.255.255.0 Gateway predefinito : 192.168.1.1		Suffisso DNS specifico per connessione: homenet.telecomitalia.it Indirizzo IPv6 locale rispetto al collegamento . : fe80::482f:82d:ca3b:5e5e%18 Indirizzo IPv4. : 192.168.1.35 Subnet mask : 255.255.255.0 Gateway predefinito : 192.168.1.1	
PS C:\Users\SblindoSavage>		C:\Users\SblindoSavage>	

CMDLET

Windows PowerShell

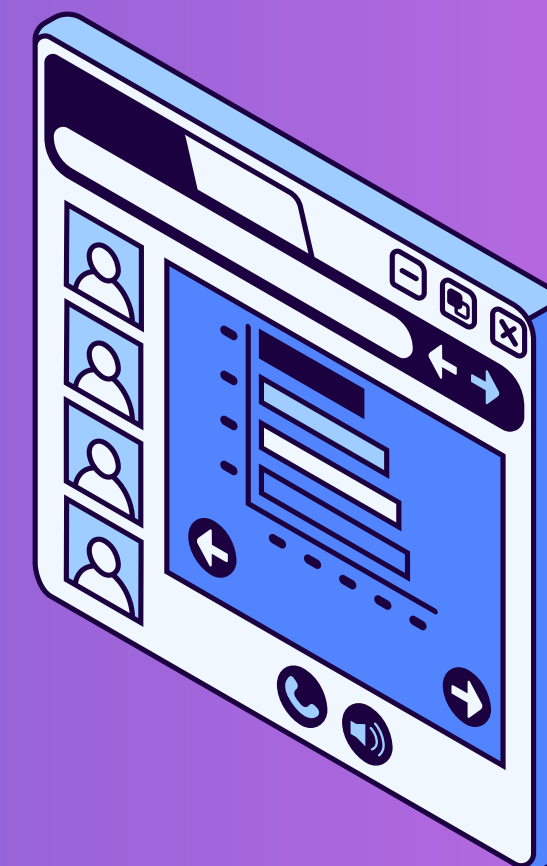
In PowerShell, i cmdlet seguono la sintassi verbo-nome.

Digitando Get-Alias dir, si scopre che il comando PowerShell equivalente è Get-ChildItem.

Approfondimento sui cmdlet:
I cmdlet offrono funzionalità estese rispetto ai comandi tradizionali del Prompt dei comandi. È possibile cercare una lista completa di cmdlet PowerShell sul sito ufficiale Microsoft.

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

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

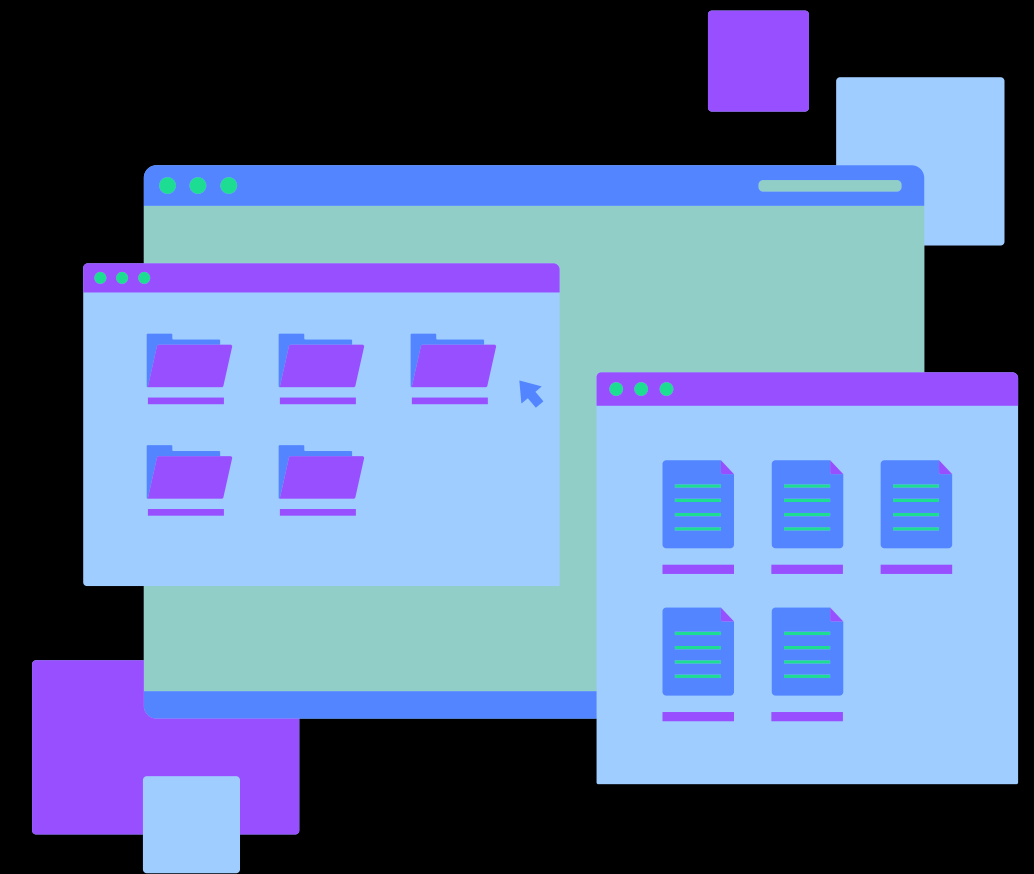


COMANDO NETSTAT IN POWERSHELL

Windows PowerShell

Il comando netstat permette di monitorare le connessioni di rete e la configurazione TCP/IP. Alcune delle opzioni principali includono:

- -a: Mostra tutte le connessioni e porte in ascolto.
- -h: Mostra le opzioni disponibili per il comando.
- -b: Mostra gli eseguibili associati alle connessioni.
- -r: Visualizza la tabella di routing.
- -n: Visualizza gli indirizzi IP e le porte in formato numerico, senza tentare la risoluzione DNS.
- -o: Include il PID (Process Identifier) per ogni connessione, consentendo di correlare le connessioni ai processi attivi.



COMANDO NETSTAT IN POWERSHELL

Windows PowerShell

Tabella di routing (netstat -r)

Utilizzando questo comando, è possibile visualizzare le rotte attive IPv4 e IPv6. Un esempio di output potrebbe includere:

- Rete di destinazione: Specifica l'indirizzo della rete remota.
- Gateway: Mostra l'indirizzo del router o gateway attraverso cui passa il traffico.
- Interfaccia: Indica l'indirizzo IP locale utilizzato per accedere alla rete remota.
- Metrica: Valore che determina la preferenza per una rotta (valori più bassi indicano percorsi preferiti).

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

=====
Elenco interfacce
16...98 ee cb cd 94 76 .....Realtek Gaming GbE Family Controller
15...0a 00 27 00 00 0f .....VirtualBox Host-Only Ethernet Adapter
 5...da f8 83 bb ba 3e .....Microsoft Wi-Fi Direct Virtual Adapter
20...d8 f8 83 bb ba 3f .....Microsoft Wi-Fi Direct Virtual Adapter #3
18...d8 f8 83 bb ba 3e .....Intel(R) Wi-Fi 6 AX201 160MHz
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   192.168.1.35    35
  127.0.0.0           255.0.0.0    On-link      127.0.0.1     331
  127.0.0.1           255.255.255.255 On-link      127.0.0.1     331
 127.255.255.255      255.255.255.255 On-link      127.0.0.1     331
 169.254.0.0          255.255.0.0  On-link      169.254.56.158 281
 169.254.56.158       255.255.255.255 On-link      169.254.56.158 281
 169.254.255.255       255.255.255.255 On-link      169.254.56.158 281
 192.168.1.0           255.255.255.0 On-link      192.168.1.35   291
 192.168.1.35          255.255.255.255 On-link      192.168.1.35   291
 192.168.1.255         255.255.255.255 On-link      192.168.1.35   291
 224.0.0.0             240.0.0.0    On-link      127.0.0.1     331
 224.0.0.0             240.0.0.0    On-link      169.254.56.158 281
 224.0.0.0             240.0.0.0    On-link      192.168.1.35   291
 255.255.255.255        255.255.255.255 On-link      127.0.0.1     331
 255.255.255.255        255.255.255.255 On-link      169.254.56.158 281
 255.255.255.255        255.255.255.255 On-link      192.168.1.35   291
=====
Route permanenti:
Nessuna

IPv6 Tabella route
=====
Route attive:
  Interf Metrica Rete Destinazione      Gateway
  1      331 ::1/128              On-link
 15      281 fe80::/64              On-link
 18      291 fe80::/64              On-link
 15      281 fe80::26ca:c663:f942:d470/128 On-link
 18      291 fe80::482f:82d:ca3b:5e5e/128 On-link
 1      331 ff00::/8                On-link
 15      281 ff00::/8                On-link
 18      291 ff00::/8                On-link
=====
Route permanenti:
Nessuna
PS C:\Users\SblindoSavage>
```

COMANDO NETSTAT IN POWERSHELL

Windows PowerShell

Connessioni attive (netstat -abno)

Una volta aperto PowerShell come Amministratore è possibile ottenere un’analisi dettagliata delle connessioni attive con questo comando.

Utile per monitorare attività di rete sospette o analizzare i processi che utilizzano specifiche porte di comunicazione.

```
Amministratore: Windows PowerShell
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  1504
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  7036
CDPSvc
[svchost.exe]
TCP    0.0.0.0:5426            0.0.0.0:0          LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:7680            0.0.0.0:0          LISTENING  2848
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49664           0.0.0.0:0          LISTENING  1120
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49665           0.0.0.0:0          LISTENING  812
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49666           0.0.0.0:0          LISTENING  2248
Schedule
[svchost.exe]
TCP    0.0.0.0:49667           0.0.0.0:0          LISTENING  2572
EventLog
[svchost.exe]
TCP    0.0.0.0:49668           0.0.0.0:0          LISTENING  3616
[spoolsv.exe]
TCP    0.0.0.0:49685           0.0.0.0:0          LISTENING  1092
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:52363           0.0.0.0:0          LISTENING  19268
[Spotify.exe]
TCP    0.0.0.0:57621           0.0.0.0:0          LISTENING  19268
[Spotify.exe]
TCP    127.0.0.1:6463          0.0.0.0:0          LISTENING  3224
[Discord.exe]
TCP    127.0.0.1:8097          0.0.0.0:0          LISTENING  19268
[Spotify.exe]
TCP    127.0.0.1:9100          0.0.0.0:0          LISTENING  4256
[lghub_updater.exe]
TCP    127.0.0.1:9180          0.0.0.0:0          LISTENING  4256
[lghub_updater.exe]
TCP    127.0.0.1:13333        0.0.0.0:0          LISTENING  10876
[RazerCortex.exe]
TCP    127.0.0.1:27060         0.0.0.0:0          LISTENING  8264
[steam.exe]
TCP    127.0.0.1:49669         0.0.0.0:0          LISTENING  4588
[VSSrv.exe]
TCP    127.0.0.1:49669         127.0.0.1:51765    ESTABLISHED  4588
[VSSrv.exe]
TCP    127.0.0.1:49670         0.0.0.0:0          LISTENING  4588
[VSSrv.exe]
TCP    127.0.0.1:49670         127.0.0.1:51761    ESTABLISHED  4588
[VSSrv.exe]
TCP    127.0.0.1:49684         0.0.0.0:0          LISTENING  4500
[GameManagerService3.exe]
TCP    127.0.0.1:49684         127.0.0.1:51910    ESTABLISHED  4500
[GameManagerService3.exe]
TCP    127.0.0.1:51760         0.0.0.0:0          LISTENING  2400
[RzTHX0529.exe]
TCP    127.0.0.1:51761         127.0.0.1:49670    ESTABLISHED  2400
```

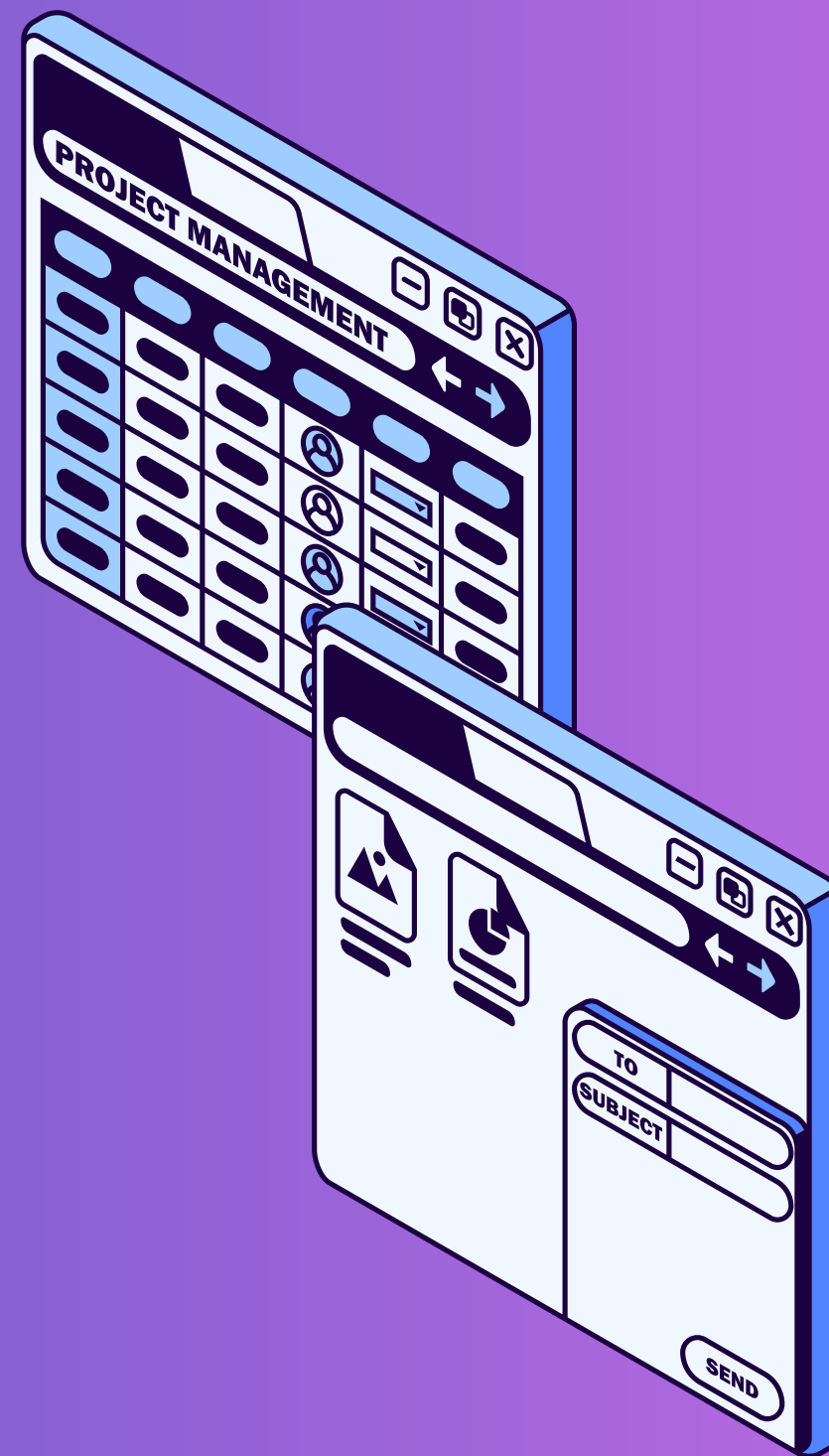

SVUOTARE IL CESTINO CON POWERSHELL

Windows PowerShell

Il cmdlet “Clear-RecycleBin” consente di svuotare il Cestino di Windows per uno o più utenti direttamente dalla console PowerShell. Questo comando è particolarmente utile per amministratori di sistema che vogliono automatizzare la pulizia del Cestino su macchine multiple, risparmiando tempo rispetto all’approccio manuale.

```
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>
```



PowerShell offre numerosi comandi utili per semplificare le attività di un analista della sicurezza. Esempi:

- Get-EventLog per analizzare i registri eventi.
- Test-Connection per verificare la connettività di rete.
- Get-Process per monitorare i processi attivi.
- Set-ExecutionPolicy per configurare le policy di esecuzione degli script.

Questi comandi possono essere combinati in script per automatizzare attività come il monitoraggio della rete, la verifica delle configurazioni di sicurezza o la risposta agli incidenti.

PowerShell è uno strumento potente e versatile per la gestione di sistemi e la sicurezza informatica. La sua conoscenza approfondita consente di migliorare l'efficienza operativa e di affrontare sfide complesse con strumenti avanzati di automazione e diagnostica.



ANALISI AVANZATE APPROCCIO PRACTICO

2

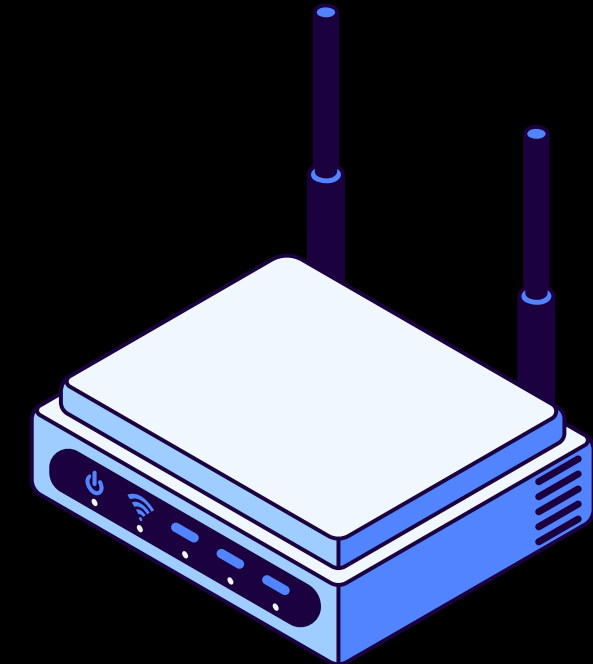
Cattura traffico HTTP/HTTPS

INDICE

Cattura HTTP/HTTPS



- Tcpdump
- Generazione traffico HTTP
- Analisi traffico HTTP con Wireshark
- Analisi traffico HTTPS con Wireshark
- Considerazioni finali



OBIETTIVO

L'obiettivo consiste nel catturare e analizzare il traffico HTTP/HTTPS utilizzando strumenti come tcpdump e Wireshark analizzando le differenze e comprendere le caratteristiche di sicurezza del protocollo HTTPS rispetto a HTTP.

TCPDUMP

Cattura HTTP/HTTPS

COS'È TCP DUMP

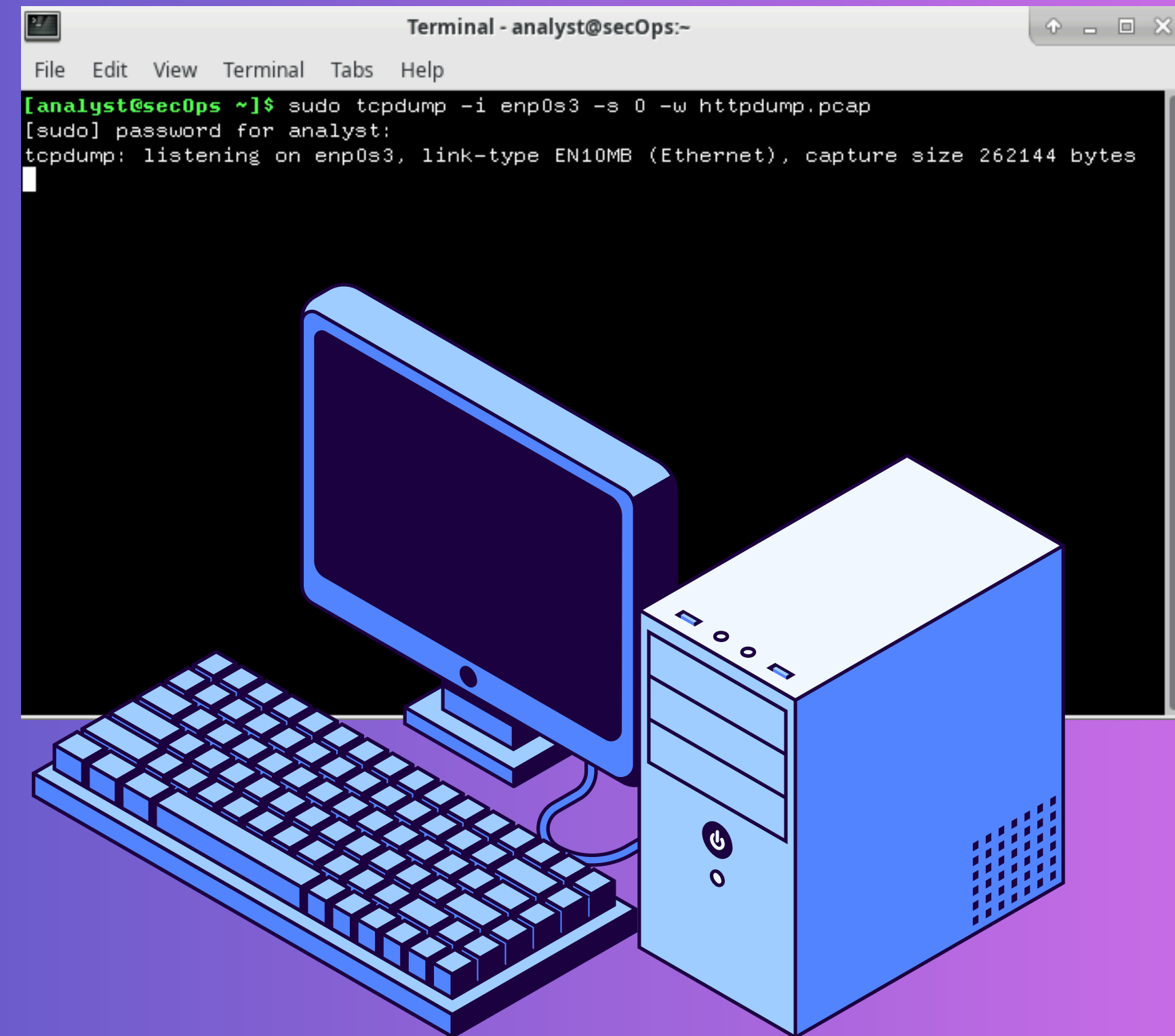
Tcpdump è uno strumento da riga di comando ideale per acquisire pacchetti di rete direttamente dal terminale, è particolarmente utile per configurazioni remote o analisi veloci

AVVIO TCPDUMP

Avviare tcpdump da terminale con il comando “sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap”

- **-i:** Specifica l'interfaccia.
- **-s:** Imposta la lunghezza dello snapshot (0 per catturare l'intero pacchetto).
- **-w:** Salva l'output in un file .pcap.

Eseguito il comando il terminale sarà in ascolto e in attesa di cattura del traffico che andremo a generare.



GENERAZIONE TRAFFICO HTTP

Cattura HTTP/HTTPS

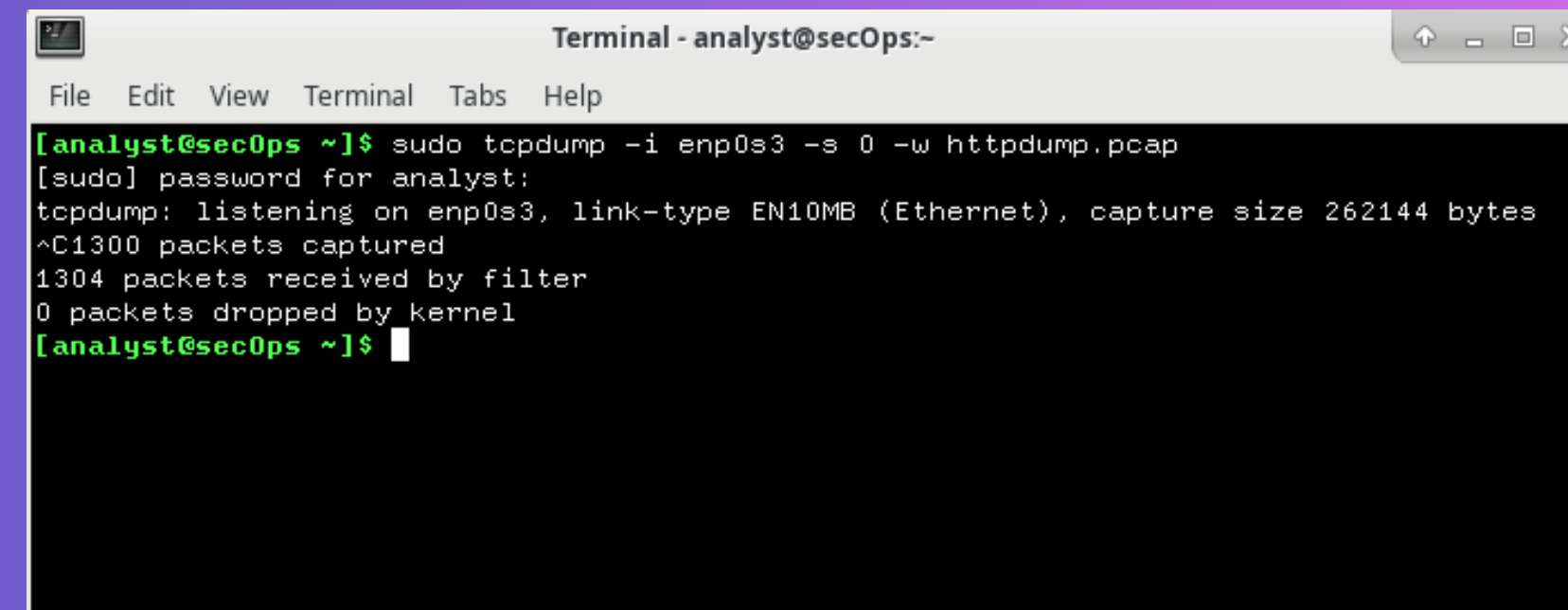
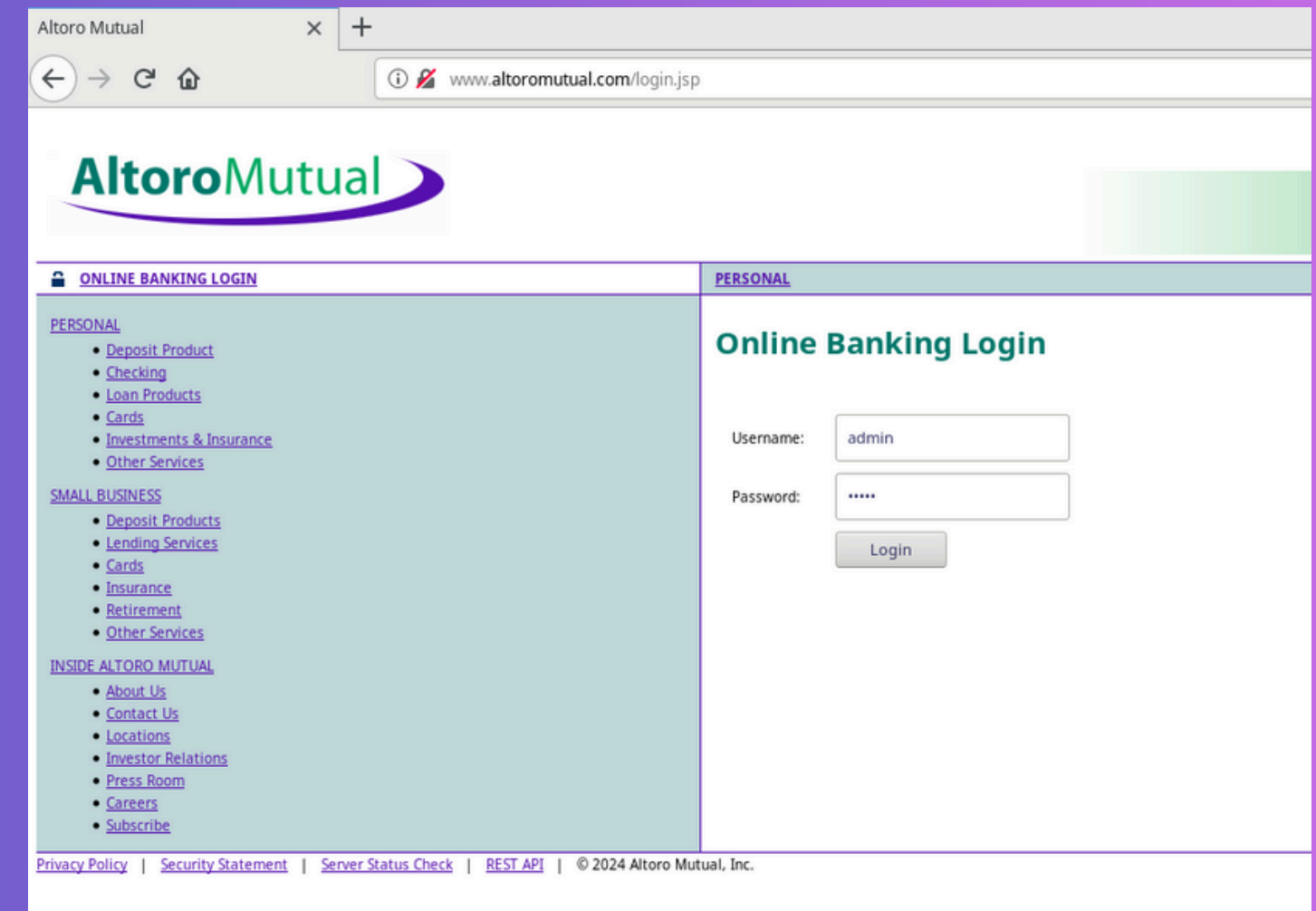
Il traffico **HTTP** (Hypertext Transfer Protocol) è il flusso di dati che avviene tra client (tipicamente un browser web) e server web, utilizzando il protocollo HTTP per la trasmissione di informazioni quindi non utilizzando crittografia avverrà in chiaro.

Utilizzare un browser per visitare
<http://www.altoromutual.com/login.jsp>.

Inserire le credenziali:

- Username: Admin
- Password: Admin

Chiudere il browser e interrompere la cattura premendo CTRL+C nel terminale.



ANALISI TRAFFICO HTTP

Cattura HTTP/HTTPS

Una volta interrotta la cattura verrà salvato un file “httpdump.pcap” che andremo ad analizzare con Wireshark.

Filtriamo i pacchetti http nel campo in alto e selezioniamo un messaggio POST, questo contiene i dati di login nascosti nel corpo del pacchetto che saranno visibili grazie alla mancanza di crittografia.

Esandere la sezione “HTML Form
URL Encoded per visualizzare:

- UID= admin
- PASSW= admin

No.	Time	Source	Destination	Protocol	Length	Info
603	2009.395641	65.61.137.117	10.0.2.15	HTTP	9534	HTTP/1.1 200 OK (JPEG JFIF image)
611	2009.541285	65.61.137.117	10.0.2.15	HTTP	1175	HTTP/1.1 200 OK (JPEG JFIF image)
613	2009.541405	65.61.137.117	10.0.2.15	HTTP	2451	HTTP/1.1 200 OK (GIF89a)
619	2009.640322	10.0.2.15	65.61.137.117	HTTP	408	GET /favicon.ico HTTP/1.1
620	2009.679769	10.0.2.15	65.61.137.117	HTTP	348	GET /favicon.ico HTTP/1.1
633	2010.195353	65.61.137.117	10.0.2.15	HTTP	7168	HTTP/1.1 404 Not Found (text/html)
637	2010.209093	65.61.137.117	10.0.2.15	HTTP	5788	HTTP/1.1 404 Not Found (text/html)
687	2013.848989	10.0.2.15	2.20.252.130	OCSP	485	Request
688	2013.849987	10.0.2.15	2.20.252.130	OCSP	485	Request
697	2014.372571	2.20.252.130	10.0.2.15	OCSP	943	Response
699	2014.376077	2.20.252.130	10.0.2.15	OCSP	943	Response
796	2035.858577	10.0.2.15	65.61.137.117	HTTP	589	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
802	2036.026171	65.61.137.117	10.0.2.15	HTTP	327	HTTP/1.1 302 Found
804	2036.250694	10.0.2.15	65.61.137.117	HTTP	607	GET /bank/main.jsp HTTP/1.1
812	2037.192333	65.61.137.117	10.0.2.15	HTTP	3622	HTTP/1.1 200 OK (text/html)
1010	2057.830370	10.0.2.15	192.229.221.95	OCSP	485	Request
1020	2057.832813	10.0.2.15	192.229.221.95	OCSP	485	Request
1021	2057.833124	10.0.2.15	192.229.221.95	OCSP	485	Request
1022	2057.833552	10.0.2.15	192.229.221.95	OCSP	485	Request
1023	2057.833846	10.0.2.15	192.229.221.95	OCSP	485	Request

▶ Frame 796: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits)

▶ Ethernet II, Src: PcsCompu_74:b5:6d (08:00:27:74:b5:6d), 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: 59062, Dst Port: 80, Seq: 1, Ack: 1, Len: 535

▶ Hypertext Transfer Protocol

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

- ▶ Form item: "uid" = "admin"
- ▶ Form item: "passw" = "admin"
- ▶ Form item: "btnSubmit" = "Login"

ANALISI TRAFFICO HTTPS



Cattura HTTP/HTTPS

Il traffico **HTTPS** (HyperText Transfer Protocol Secure) è una versione sicura di HTTP, che è il protocollo di base per la trasmissione di dati nel web. HTTPS protegge l'integrità e la riservatezza delle comunicazioni tra il client (un browser) e il server attraverso l'uso di un canale cifrato.

Faremo lo stesso procedimento di prima avviando tcpdump con il comando

“`sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap`” e mettendolo in ascolto.

Utilizzare un browser per visitare

`https://www.netacad.com` come già vediamo dall'url il sito utilizza il protocollo sicuro di HTTP (HTTPS) quindi dove prima vedevamo le credenziali in chiaro, su wireshark adesso vedremo che i dati sono criptati e non potremo vedere le credenziali inserite.

No.	Time	Source	Destination	Protocol	Length	Info
129	3.771743	10.0.2.15	34.120.5.221	TLSv1.2	231	Application Data
132	3.773656	10.0.2.15	34.120.5.221	TLSv1.2	92	Application Data
135	3.774297	34.120.5.221	10.0.2.15	TCP	60	443 → 47066 [ACK] Seq=3355 Ack=473 Win=65535 Len=0
136	3.774302	34.120.5.221	10.0.2.15	TCP	60	443 → 47066 [ACK] Seq=3355 Ack=511 Win=65535 Len=0
137	3.775540	10.0.2.15	34.120.5.221	TLSv1.2	248	Application Data
138	3.775955	10.0.2.15	34.120.5.221	TLSv1.2	85	Encrypted Alert
139	3.776164	10.0.2.15	34.120.5.221	TCP	54	47064 → 443 [FIN, ACK] Seq=521 Ack=3370 Win=37440 Len=0
140	3.777116	10.0.2.15	34.120.5.221	TLSv1.2	248	Application Data
141	3.777564	10.0.2.15	34.120.5.221	TLSv1.2	305	Application Data
142	3.777959	10.0.2.15	34.120.5.221	TLSv1.2	85	Encrypted Alert
143	3.778170	10.0.2.15	34.120.5.221	TCP	54	47062 → 443 [FIN, ACK] Seq=521 Ack=3355 Win=37440 Len=0

Filter: tcp.port==443

Expression... Clear Apply Save

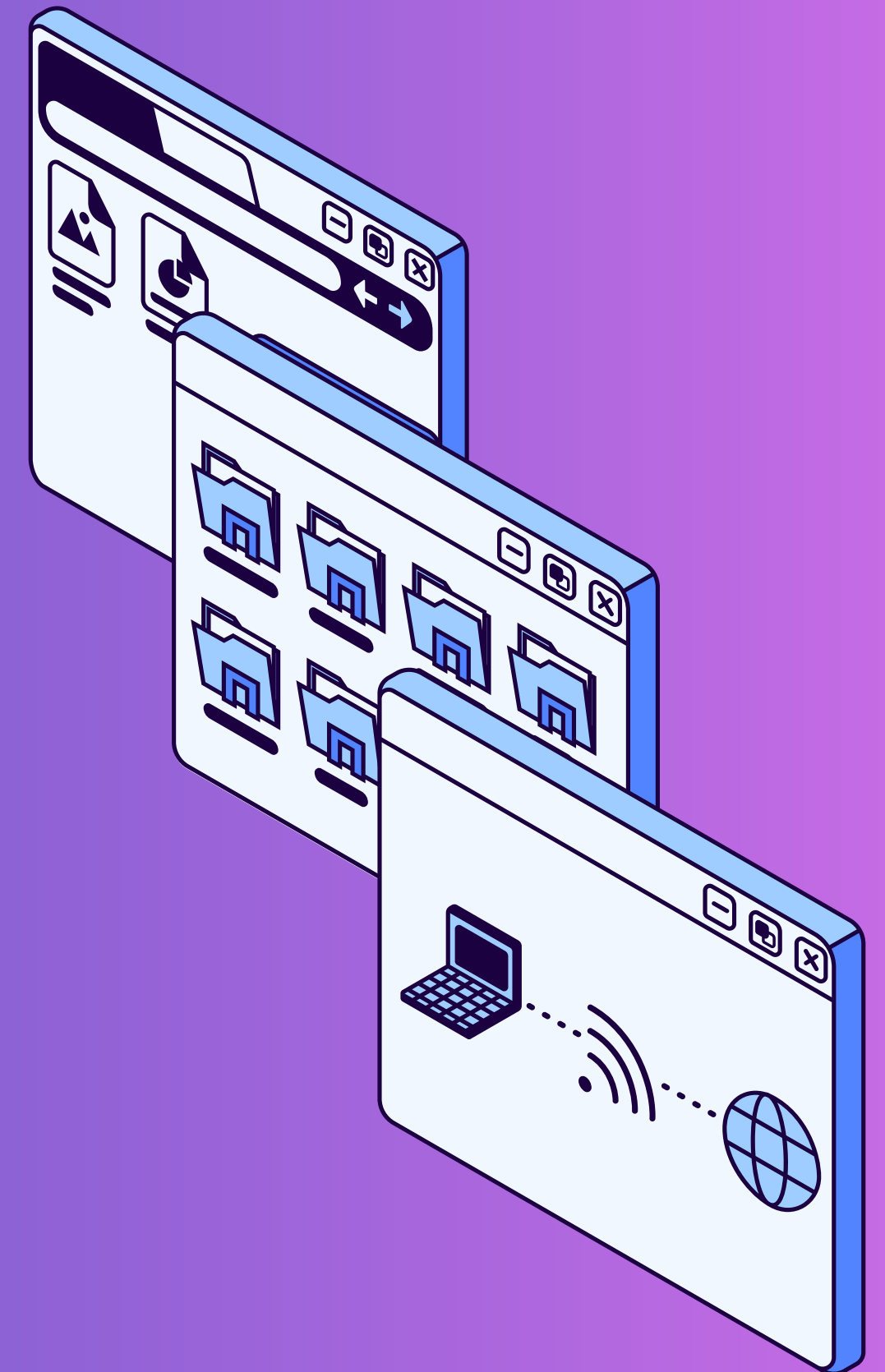
Frame 140: 248 bytes on wire (1984 bits), 248 bytes captured (1984 bits) on interface 0
Ethernet II, Src: PcsCompu_74:b5:6d (08:00:27:74:b5:6d), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 34.120.5.221
Transmission Control Protocol, Src Port: 47062, Dst Port: 443, Seq: 296, Ack: 3355, Len: 194
Secure Sockets Layer
TLSv1.2 Record Layer: Application Data Protocol: http2
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 189
Encrypted Application Data: 0000000000000000128d5c3e901949d02197399393f751e5a...

CONSIDERAZIONI FINALI

Cattura HTTP/HTTPS

L'esercitazione svolta ha messo in evidenza l'importanza della sicurezza nelle comunicazioni di rete, mostrando come il traffico HTTP, privo di crittografia, possa esporre dati sensibili a rischi significativi. Al contrario, HTTPS si è rivelato un protocollo fondamentale per garantire la riservatezza delle informazioni, sebbene non sia di per sé un indicatore di affidabilità del sito web. Attraverso l'uso di strumenti pratici come tcpdump e Wireshark, è stato possibile sperimentare metodi concreti di cattura e analisi del traffico di rete.

Questa esperienza ha permesso di acquisire competenze chiave nell'identificazione delle vulnerabilità associate alla trasmissione non protetta dei dati e di sviluppare una maggiore consapevolezza delle tecniche necessarie per monitorare e proteggere le reti in scenari reali.



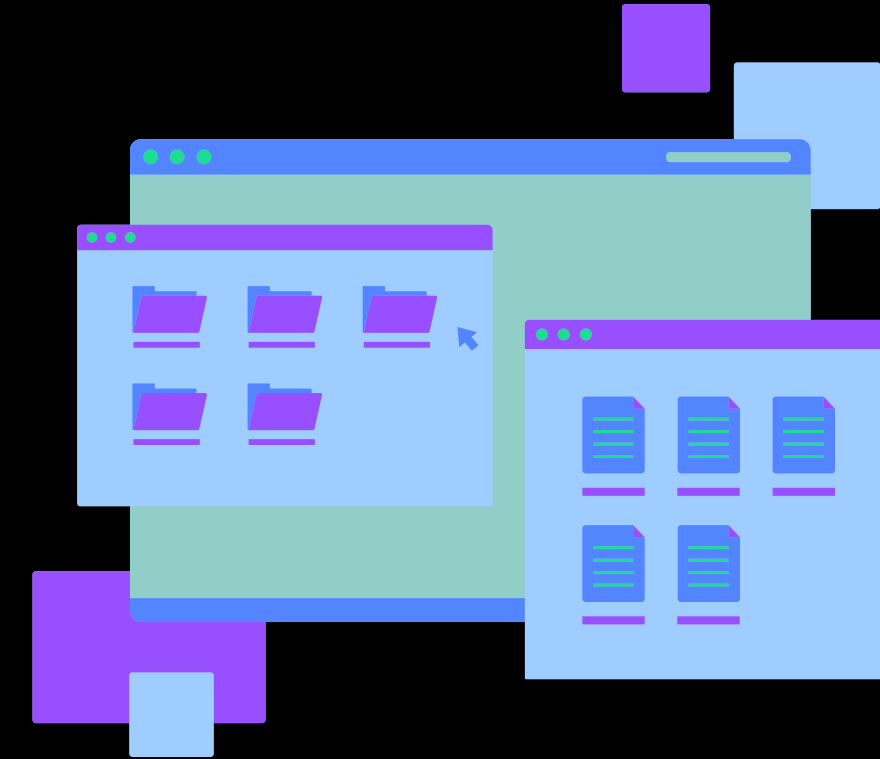
ANALISI AVANZATE APPROCCIO PRAATICO

INDICE

Bonus1 Nmap



- Cos'è Nmap?
- Man pages Nmap
- Port scanning
- PortScan su LocalHost
- PortScan in Lan
- PortScan su server remoto
- Considerazioni finali



OBIETTIVO

Mettere in pratica l'uso di Nmap per la raccolta di informazioni in modo strutturato, con una chiara comprensione dei rischi e delle possibili vulnerabilità che potrebbero essere sfruttate in base ai servizi attivi e alle loro vulnerabilità note.

COS'È NMAP?

Bonus1 Nmap

Nmap è un potente strumento open source utilizzato per la scansione e l'analisi di reti informatiche. È progettato per aiutare gli amministratori di sistema, gli esperti di sicurezza e i pentester a ottenere informazioni dettagliate sui dispositivi e sui servizi in una rete.

Le sue funzioni principali:

- **Scansione delle porte:**

Determina quali porte (TCP/UDP) sono aperte su un dispositivo target.

Indica i servizi che stanno utilizzando quelle porte (ad esempio, HTTP, FTP)

- **Identificazione dei servizi:**

Riconosce i servizi in esecuzione su una porta aperta

- **Rilevamento del sistema operativo:**

Tenta di identificare il sistema operativo del dispositivo target, insieme a informazioni come la versione del kernel o altre caratteristiche.

- **Scoperta di rete:**

Può identificare quali dispositivi sono attivi in una rete.

MAN PAGES NMAP

Bonus1 Nmap

Le man pages di Nmap sono i manuali integrati disponibili sui sistemi Unix/Linux che forniscono una documentazione completa e dettagliata sul funzionamento di questo strumento. Per accedere alle man pages di Nmap, si utilizza il comando:

“man nmap”

Le man pages sono particolarmente utili per approfondire le funzionalità avanzate di Nmap o quando si cerca di comprendere una specifica opzione.

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

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 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
9929/tcp  open  nping-echo   Nping echo
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.39
OS details: Linux 2.6.39
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
[Cut first 10 hops for brevity]
11  17.65 ms li86-221.members.linode.com (74.207.244.221)

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds

Manual page nmap(1) line 45 (press h for help or q to quit)
```

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

NMAP(1)                                Nmap Reference Guide                                NMAP(1)

NAME

nmap - Network exploration tool and security / port scanner

SYNOPSIS

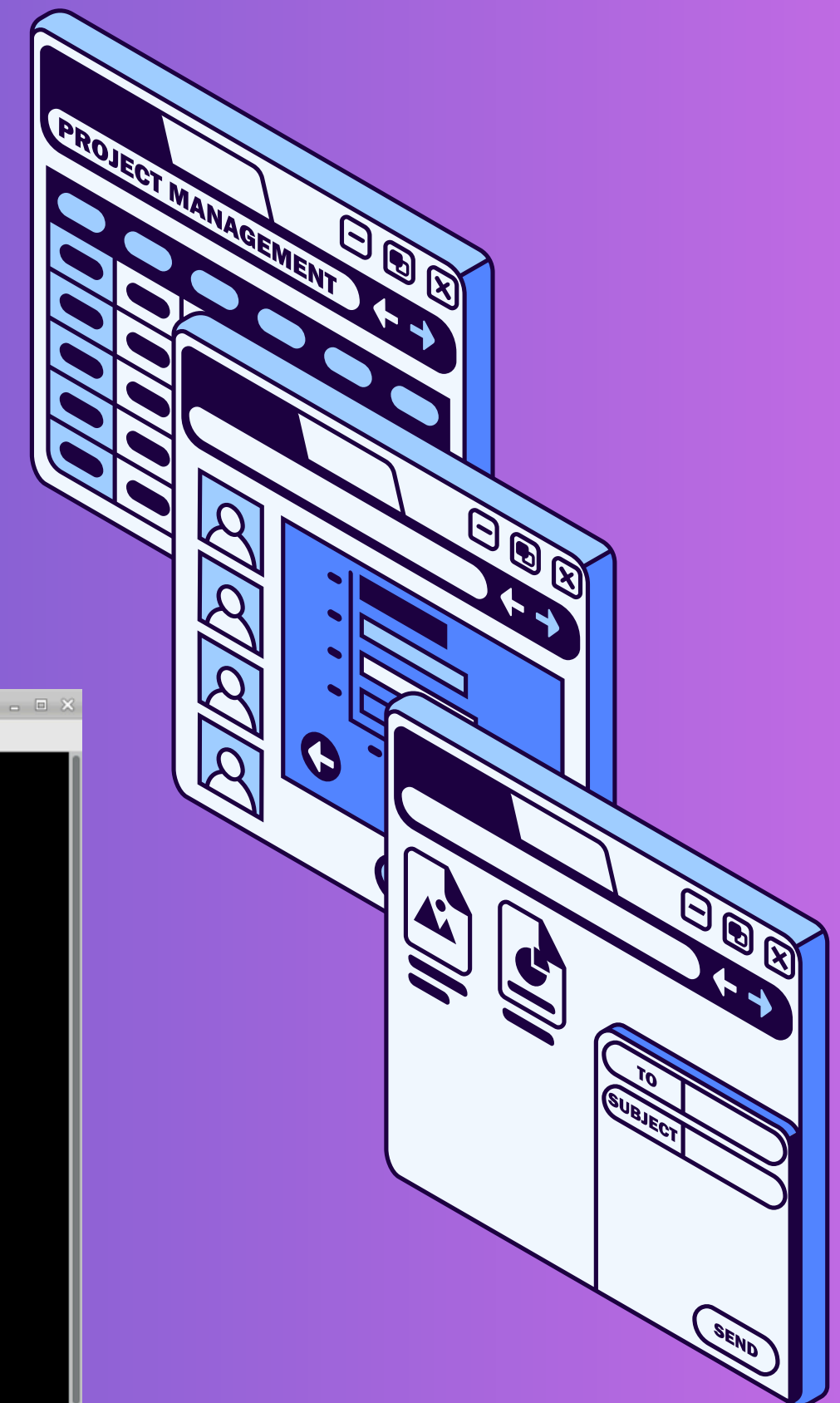
nmap [Scan Type...] [Options] {target specification}

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 information is the "interesting ports table". That table lists the port number and protocol, service name, and state. The state is either open, filtered, closed, or unfiltered. Open means that an application on the target machine is listening for connections/packets on that port. Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed. Closed ports have no application listening on them, though they could open up at any time. Ports are classified as unfiltered when they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or closed. Nmap reports the state combinations open/filtered and closed/filtered when it cannot determine which of the two states describe a port. The port table may also

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



PORT SCANNING

Bonus1 Nmap

Il **port scanning** è una tecnica utilizzata per identificare le porte di comunicazione aperte, chiuse o filtrate su un dispositivo di rete (ad esempio, un computer, un server o un dispositivo IoT). È un passo fondamentale per valutare la sicurezza di un sistema o per comprendere meglio la configurazione di una rete.

COSA È UNA PORTA?

Una porta è un punto di accesso logico che consente la comunicazione tra dispositivi in una rete. Le porte sono numerate da 0 a 65535, e ciascuna porta è associata a specifici servizi o protocolli.

Le porte che vanno da 0 a 1023 prendono il nome di **porte note**.

Queste porte sono utilizzate principalmente per identificare i servizi più comuni su Internet e nelle reti locali.



PORT SCAN SU LOCALHOST

Bonus1 Nmap

Comando: nmap -A -T4 localhost

Questo comando permette di eseguire una scansione approfondita sul proprio sistema (localhost). Nel contesto, "localhost" rappresenta il computer locale che esegue il comando. La scansione rileva porte aperte, servizi attivi e informazioni sul sistema operativo.

Porte aperte trovate e i relativi servizi attivi
Porta 21/tcp: FTP (vsftpd 2.0.8 o superiore)
Porta 22/tcp: SSH (OpenSSH)

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 09:28 EST
```

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 09:28 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000044s 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 6
|     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 12.19 seconds
[analyst@secOps ~]$
```

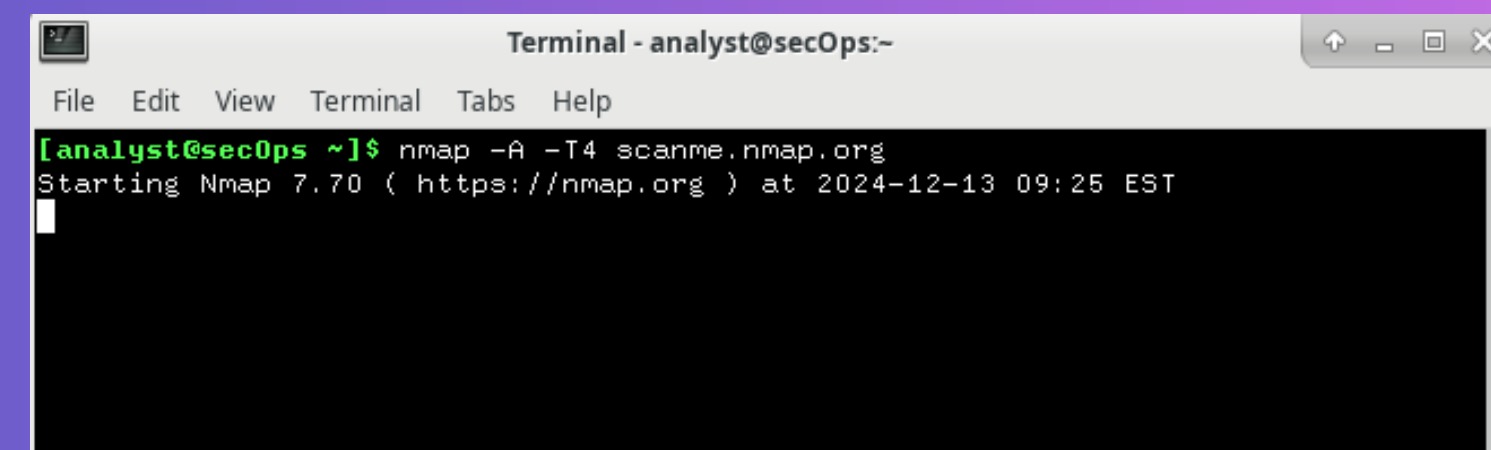

PORT SCAN SU SERVER REMOTO

Bonus1 Nmap

Con il comando **nmap -A -T4 scanme.nmap.org** si va a fare una scansione avanzata di Nmap su un server remoto, per raccogliere informazioni dettagliate, tra cui porte aperte, versioni dei servizi, e il sistema operativo del server. In questo caso il server di test **scanme.nmap.org**, server pubblico messo a disposizione da Nmap per scopi di test. Questo comando combina diverse opzioni di Nmap per ottenere informazioni dettagliate sul server.

-A: Attiva l'esecuzione di script avanzati e il rilevamento di sistema operativo e versioni dei servizi.
-T4: Imposta una scansione più veloce, con il rischio di essere rilevata più facilmente da sistemi di monitoraggio.

A destra possiamo vedere la foto del risultato della scansione.



```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org  
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 09:25 EST
```

```
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 10:36 EST  
Nmap scan report for scanme.nmap.org (45.33.32.156)  
Host is up (0.38s latency).  
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f  
Not shown: 996 filtered ports  
PORT      STATE SERVICE      VERSION  
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)  
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)  
|   256  96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)  
|_  256  33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)  
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))  
|_ http-server-header: Apache/2.4.7 (Ubuntu)  
|_ http-title: Go ahead and ScanMe!  
9929/tcp  open  nping-echo   Nping echo  
31337/tcp open  tcpwrapped  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 53.91 seconds  
[analyst@secOps ~]$
```

CONSIDERAZIONI FINALI NMAP

Bonus1 Nmap

Nmap è uno degli strumenti più potenti e utilizzati per l'analisi di reti e la sicurezza informatica, grazie alla sua capacità di eseguire scansioni dettagliate e di raccogliere informazioni vitali su un sistema remoto. Tuttavia, come qualsiasi strumento potente, va utilizzato con attenzione e in modo consapevole, soprattutto per evitare conseguenze indesiderate, come l'individuazione da parte dei sistemi di difesa.

Quando si esegue una scansione Nmap su una rete o su un dispositivo che non si possiede o non si ha il permesso di esaminare, si rischia di violare leggi relative all'accesso non autorizzato ai sistemi informatici. La scansione di porte senza consenso può essere vista come una forma di attacco di ricognizione.

