

Consegna 25 Ottobre

Laboratorio - Utilizzo di Wireshark per Esaminare il Traffico HTTP e HTTPS

Obiettivi

L'obiettivo del laboratorio è esplorare alcune funzioni di PowerShell.

Parte 1: Esplorazione dei Comandi di Command Prompt e PowerShell

- Esegui il comando `dir` in entrambe le console.

- **Output:** Entrambe le finestre mostrano una lista di sottodirectory e file. PowerShell fornisce anche gli attributi/mode.

```
Seleziona 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> dir

Directory: C:\Windows\system32

Mode                LastWriteTime         Length Name
----                -
d-----          07/05/2022    08:01             0409
d-----          07/05/2022    07:24      AdvancedInstallers
d-----          20/09/2024    16:36      AppLocker
d-----          10/10/2024    21:47      appraiser
d---s-          19/09/2024    18:13      AppV
d-----          19/09/2024    15:42      ar-SA
d-----          18/03/2024    08:47      bg-BG
d-----          10/10/2024    21:47      Boot
d-----          07/05/2022    07:24      Bthprops
d-----          18/03/2024    08:47      ca-ES
d-----          21/10/2024    18:17      CatRoot
d-----          22/10/2024    22:37      catroot2
d-----          19/09/2024    18:13      CodeIntegrity
d-----          21/09/2024    12:07      Com
d-----          24/10/2024    20:21      config
d---s-          07/05/2022    07:42      Configuration
d-----          16/07/2024    11:50      cs-CZ
d-----          16/07/2024    11:50      da-DK
d-----          28/05/2024    10:58      DDFs
d---s-          23/09/2024    09:13      de-DE
d---s-          21/09/2024    12:07      DiagSvc
d-----          21/09/2024    12:07      Dism
d-----          07/05/2022    07:24      downlevel
d-----          22/10/2024    18:55      drivers
d-----          07/05/2022    07:24      DriverState
d-----          22/10/2024    09:22      DriverStore
d-----          21/10/2024    14:35      DRVSTORE
d---s-          21/09/2024    12:07      dsc
d-----          16/07/2024    11:50      el-GR
d-----          16/07/2024    11:50      en
d-----          18/03/2024    08:47      en-GB
d---s-          21/10/2024    18:17      en-US
d---s-          23/09/2024    09:13      es-ES
d-----          18/03/2024    08:47      es-MX
d-----          18/03/2024    08:47      et-EE
```

- Esegui comandi come **ping**, **cd**, e **ipconfig** in entrambe le console.

- **Output:** L'output è simile in entrambe le finestre.

```
PS C:\Windows\system32\Boot> ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

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

Scheda Ethernet Ethernet 2:

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

Scheda Ethernet Ethernet 3:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::3b4b:3010:d70d:9c88%3
    Indirizzo IPv4. . . . . : 192.168.56.1
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . :

Scheda LAN wireless Wi-Fi 2:

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

Scheda LAN wireless Wi-Fi 5:

    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::6123:b75d:ff6e:5f61%11
    Indirizzo IPv4. . . . . : 192.168.194.144
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.194.234

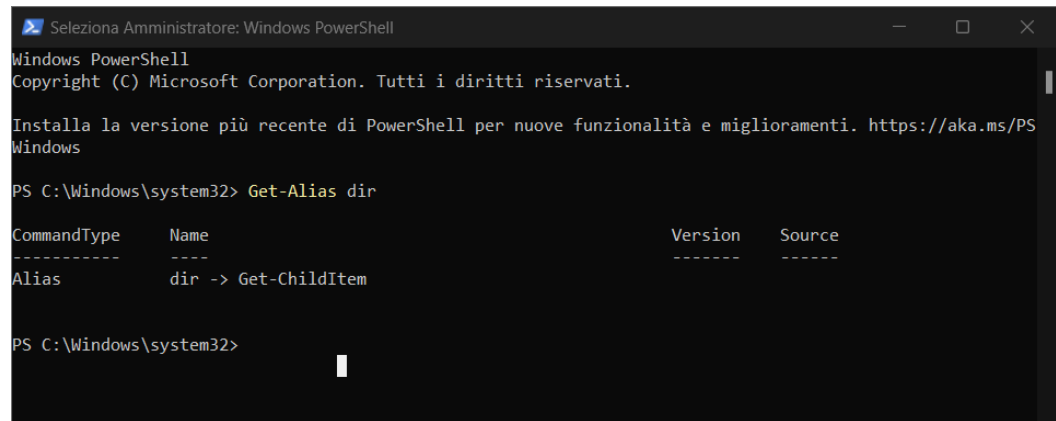
Scheda Ethernet Connessione di rete Bluetooth:

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

Parte 2: Esplorazione dei Cmdlets

- Usa `Get-Alias dir` per trovare il cmdlet PowerShell equivalente a `dir`.

- **Risultato:** Il comando PowerShell per `dir` è `Get-ChildItem`.



```
Seleziona 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> Get-Alias dir

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

PS C:\Windows\system32>
```

Parte 3: Esplorazione del Comando Netstat in PowerShell

- Usa `netstat -h` in PowerShell per vedere le opzioni disponibili.
- Esegui `netstat -r` per visualizzare la tabella di routing.

- **Output:** La tabella di routing IPv4 mostra i percorsi attivi; l'esempio usa un gateway IPv4 di 192.168.1.1.

```

Amministratore: Windows PowerShell

PS C:\Windows\system32> netstat -r

=====
Elenco interfacce
6...58 47 ca 78 68 61 .....Realtek PCIe 5GbE Family Controller
23...58 47 ca 78 68 60 .....Realtek PCIe 5GbE Family Controller #2
3...0a 00 27 00 00 03 .....VirtualBox Host-Only Ethernet Adapter
10...de 97 ba 6f f2 02 .....Intel(R) Wi-Fi 7 BE200 320MHz #2
9...dc 97 ba 6f f2 03 .....Intel(R) Wi-Fi 7 BE200 320MHz #5
11...dc 97 ba 6f f2 02 .....Intel(R) Wi-Fi 7 BE200 320MHz
4...dc 97 ba 6f f2 06 .....Bluetooth Device (Personal Area Network)
1.....Software Loopback Interface 1
61...00 15 5d 1e dd 51 .....Hyper-V Virtual Ethernet Adapter
=====

IPv4 Tabella route
=====
Route attive:
Indirizzo rete      Mask      Gateway      Interfaccia Metrica
0.0.0.0             0.0.0.0    192.168.194.234 192.168.194.144    50
127.0.0.0           255.0.0.0    On-link        127.0.0.1          331
127.0.0.1           255.255.255.255 On-link        127.0.0.1          331
127.255.255.255     255.255.255.255 On-link        127.0.0.1          331
172.30.240.0         255.255.255.255 On-link        172.30.240.1       5256
172.30.240.1         255.255.255.255 On-link        172.30.240.1       5256
172.30.255.255       255.255.255.255 On-link        172.30.240.1       5256
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
192.168.194.0        255.255.255.0 On-link        192.168.194.144    306
192.168.194.144      255.255.255.255 On-link        192.168.194.144    306
192.168.194.255      255.255.255.255 On-link        192.168.194.144    306
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        192.168.194.144    306
224.0.0.0            240.0.0.0    On-link        172.30.240.1       5256
255.255.255.255      255.255.255.255 On-link        127.0.0.1          331
255.255.255.255      255.255.255.255 On-link        192.168.56.1       281
255.255.255.255      255.255.255.255 On-link        192.168.194.144    306
255.255.255.255      255.255.255.255 On-link        172.30.240.1       5256
=====
Route permanenti:
Nessuna

IPv6 Tabella route
=====
Route attive:
Interf Metrica Rete Destinazione Gateway
1      331 ::1/128 On-link

```

- Avvia una seconda istanza di PowerShell come amministratore per visualizzare i processi associati alle connessioni TCP attive con `netstat -abno`.

- **Output:** Mostra connessioni attive, indirizzi locali/esterni, stato, e ID di processo (PID).

```

Amministratore: Windows PowerShell
Nessuna
PS C:\Windows\system32> netstat -abno

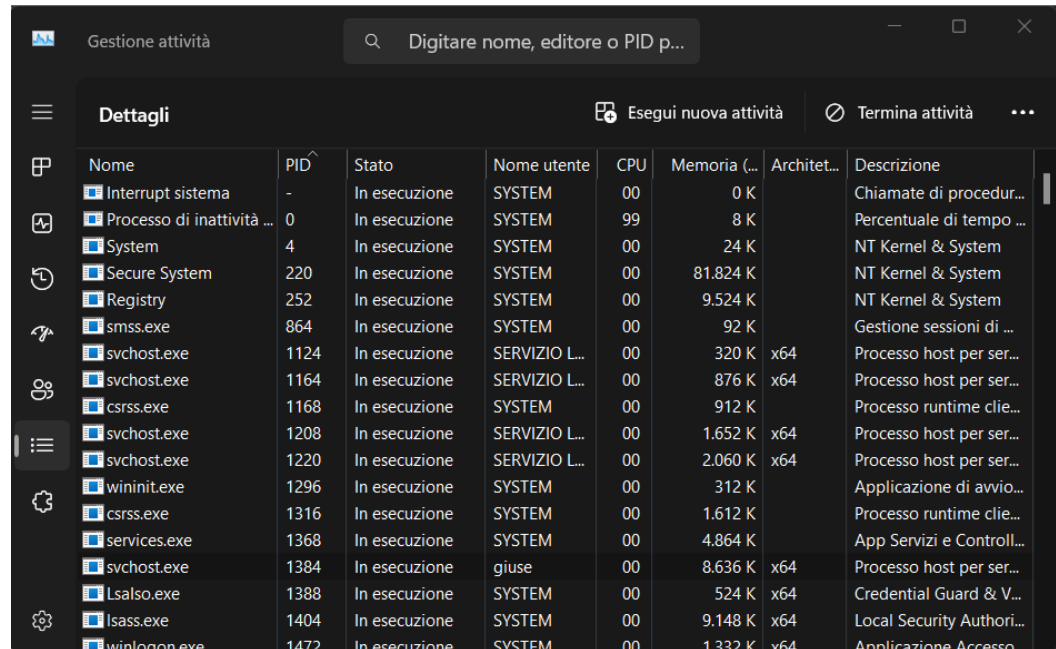
Connessioni attive

Proto Indirizzo locale      Indirizzo esterno    Stato      PID
-----
TCP    0.0.0.0:135             0.0.0.0:0            LISTENING  1772
RpcSs
[svchost.exe]
TCP    0.0.0.0:445             0.0.0.0:0            LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:3389            0.0.0.0:0            LISTENING  2028
TermService
[svchost.exe]
TCP    0.0.0.0:5040            0.0.0.0:0            LISTENING  8868
CDPSvc
[svchost.exe]
TCP    0.0.0.0:7680            0.0.0.0:0            LISTENING  9460
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49664           0.0.0.0:0            LISTENING  1404
[lsass.exe]
TCP    0.0.0.0:49665           0.0.0.0:0            LISTENING  1296
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49666           0.0.0.0:0            LISTENING  3492
Schedule
[svchost.exe]
TCP    0.0.0.0:49667           0.0.0.0:0            LISTENING  3936
EventLog
[svchost.exe]
TCP    0.0.0.0:49668           0.0.0.0:0            LISTENING  4208
SessionEnv
[svchost.exe]
TCP    0.0.0.0:49669           0.0.0.0:0            LISTENING  5072
[spoolsv.exe]
TCP    0.0.0.0:49670           0.0.0.0:0            LISTENING  1368
Impossibile ottenere informazioni sulla proprietà
TCP    127.0.0.1:6463          0.0.0.0:0            LISTENING  6696
[Discord.exe]
TCP    127.0.0.1:28385         0.0.0.0:0            LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP    127.0.0.1:28390         0.0.0.0:0            LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP    127.0.0.1:49350        0.0.0.0:0            LISTENING  9548
[esrv_svc.exe]
TCP    127.0.0.1:49351        0.0.0.0:0            LISTENING  7496
[esrv.exe]
TCP    127.0.0.1:50267        127.0.0.1:49350      TIME_WAIT  0
TCP    127.0.0.1:50268        127.0.0.1:49350      TIME_WAIT  0
TCP    127.0.0.1:50279        127.0.0.1:49350      TIME_WAIT  0

```

- In Task Manager, confronta uno dei PID dal comando `netstat` per identificare dettagli del processo associato.

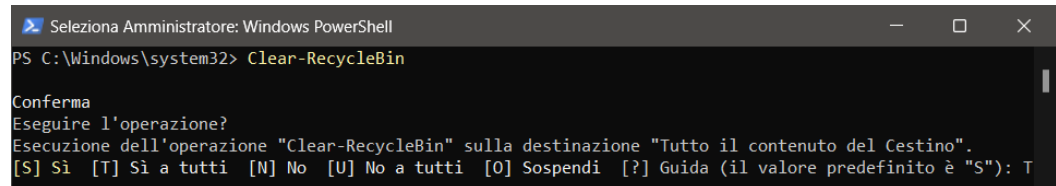
- **Esempio:** Il PID 1384 è associato a `svchost.exe`, con utente NETWORK SERVICE e 8636KB di memoria.



Nome	PID	Stato	Nome utente	CPU	Memoria (...)	Architet...	Descrizione
Interrupt sistema	-	In esecuzione	SYSTEM	00	0 K		Chiamate di procedur...
Processo di inattività ...	0	In esecuzione	SYSTEM	99	8 K		Percentuale di tempo ...
System	4	In esecuzione	SYSTEM	00	24 K		NT Kernel & System
Secure System	220	In esecuzione	SYSTEM	00	81.824 K		NT Kernel & System
Registry	252	In esecuzione	SYSTEM	00	9.524 K		NT Kernel & System
smss.exe	864	In esecuzione	SYSTEM	00	92 K		Gestione sessioni di ...
svchost.exe	1124	In esecuzione	SERVIZIO L...	00	320 K	x64	Processo host per ser...
svchost.exe	1164	In esecuzione	SERVIZIO L...	00	876 K	x64	Processo host per ser...
csrss.exe	1168	In esecuzione	SYSTEM	00	912 K		Processo runtime clie...
svchost.exe	1208	In esecuzione	SERVIZIO L...	00	1.652 K	x64	Processo host per ser...
svchost.exe	1220	In esecuzione	SERVIZIO L...	00	2.060 K	x64	Processo host per ser...
wininit.exe	1296	In esecuzione	SYSTEM	00	312 K		Applicazione di avvio...
csrss.exe	1316	In esecuzione	SYSTEM	00	1.612 K		Processo runtime clie...
services.exe	1368	In esecuzione	SYSTEM	00	4.864 K		App Servizi e Controll...
svchost.exe	1384	In esecuzione	giuse	00	8.636 K	x64	Processo host per ser...
Lsalso.exe	1388	In esecuzione	SYSTEM	00	524 K	x64	Credential Guard & V...
lsass.exe	1404	In esecuzione	SYSTEM	00	9.148 K	x64	Local Security Authori...
winlogon.exe	1472	In esecuzione	SYSTEM	00	1.332 K	x64	Applicazione Accesso...

Parte 4: Svuotamento del Cestino con PowerShell

- Verifica la presenza di file nel Cestino. Se vuoto, crea dei file e spostali nel Cestino.
- Esegui `clear-recyclebin` in PowerShell.
 - **Risultato:** I file nel Cestino vengono eliminati definitivamente.



```

Seleziona Amministratore: Windows PowerShell

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"): T
  
```