

S11L5

Laboratorio - Utilizzo di Windows PowerShell In questo laboratorio, esploreremo alcune delle funzioni di PowerShell .

<https://itexamanswers.net/3-3-11-lab-using-windows-powershell-answers.html>

Introduzione

Questo report documenta l'esecuzione del laboratorio "Utilizzo di Windows PowerShell", suddiviso in cinque parti principali. Lo scopo dell'attività è esplorare i comandi del Prompt dei comandi e di PowerShell, esaminare i cmdlet, utilizzare il comando netstat e gestire il Cestino tramite PowerShell.

Parte 1: Accesso alla console di PowerShell

1. Aperta la console di PowerShell tramite il menu Start.
2. Aperta la console di Prompt dei comandi (cmd) sempre tramite il menu Start.

PowerShell

Apps

Documents

Settings

People

Folders

Photos

M



ch

Windows PowerShell
em

Windows PowerShell ISE



Windows PowerShell (x86)



Windows PowerShell ISE (x86)



Postazioni sviluppatore
PowerShell



Consenti l'esecuzione di script
PowerShell locali senza firma



PowerShell-main.zip



Windows PowerShell

System



Open



Run as Administrator

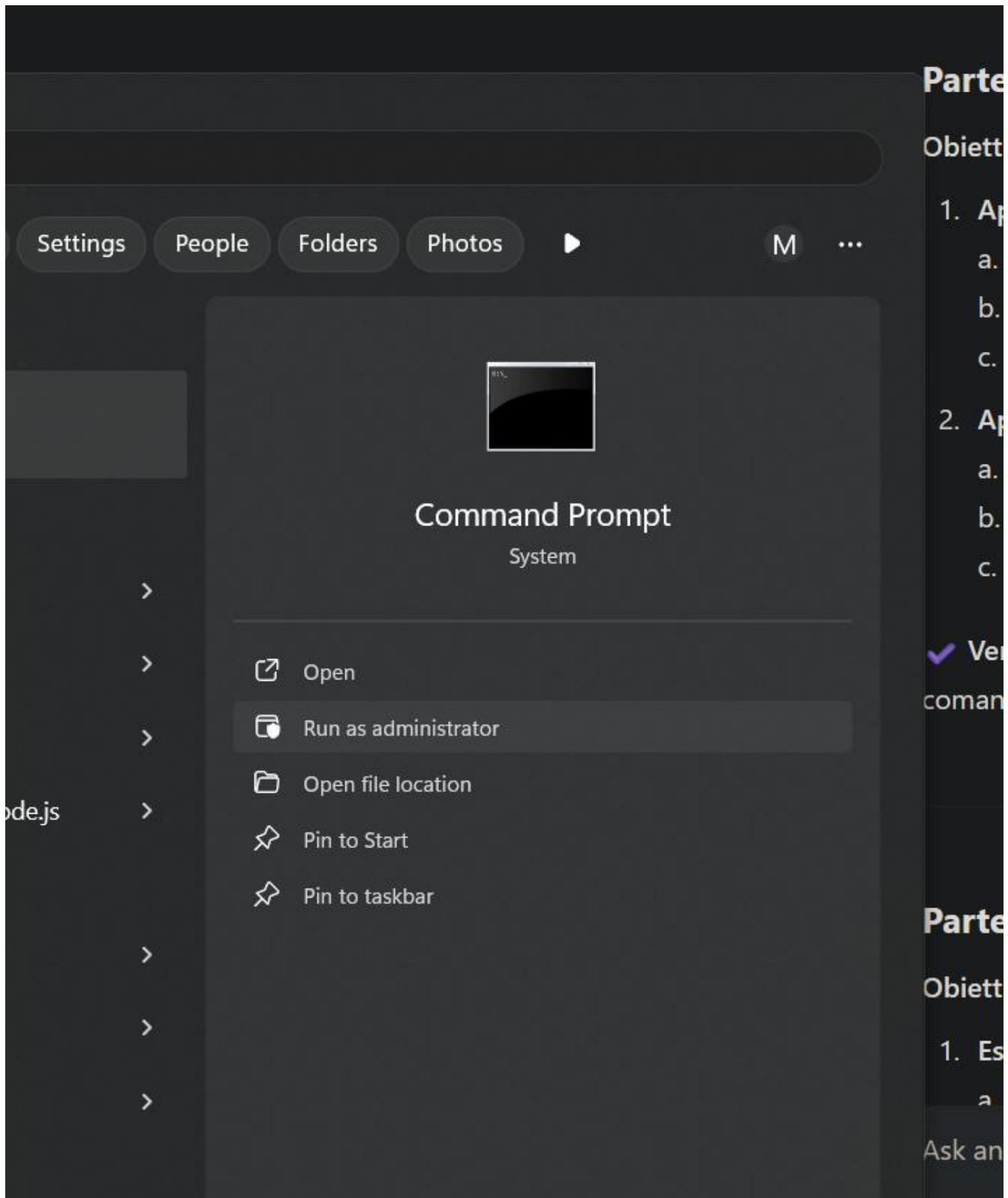


Run ISE as Administrator



Windows PowerShell ISE





Entrambe le console sono state avviate con successo.

Parte 2: Esplorazione dei comandi del Prompt dei comandi e di PowerShell

Obiettivo

Confrontare i comandi dir, cd, ipconfig tra Prompt dei comandi e PowerShell.

Procedura

1. Eseguito dir in entrambi gli ambienti.
2. Provati comandi comuni (cd .., ipconfig).
3. Osservato che alcuni comandi funzionano in entrambi gli ambienti, mentre PowerShell offre funzioni avanzate.

```
PS C:\WINDOWS\system32> cd ..
PS C:\WINDOWS> cd ..
PS C:\> dir

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
d-----         12/02/2025    12:17          [REDACTED]
d-----         02/11/2024     00:59          [REDACTED]
da----         24/02/2024     01:11          [REDACTED]
d-----         27/01/2025     00:09          [REDACTED]
d-----         11/07/2023    21:44          [REDACTED]
d-----         12/02/2025    12:31          [REDACTED]
d-----         08/01/2025    12:22          [REDACTED]
d-----         22/12/2024     00:26          [REDACTED]
d-----         24/06/2022    15:18          [REDACTED]
d-----         26/10/2024    16:19          [REDACTED]
d-----         01/04/2024     09:26          [REDACTED]
d-r---         14/02/2025    19:53      Program Files
d-r---         14/02/2025    17:17      Program Files (x86)
d-----         12/12/2024    11:18          [REDACTED]
d-----         23/01/2025    20:59      Python313
d-r---         03/10/2024    23:05      Users
d-----         19/02/2025    13:53      Windows
d-----         05/09/2024     01:13          [REDACTED]
-a----         26/10/2024     00:45          [REDACTED]
-a----         13/02/2025    14:41    12288 [REDACTED].log
```

Administrator: Command Prompt

C:\>dir

Volume in drive C has no label.
Volume Serial Number is 5BEB-E972

Directory of C:\

12/02/2025	12:17	<DIR>	\$WINDOWS.~BT
02/11/2024	00:59	<DIR>	.cache
24/02/2024	01:11	<DIR>	adb
27/01/2025	00:09	<DIR>	[REDACTED]
11/07/2023	20:44	<DIR>	[REDACTED]
25/10/2024	23:45		514 [REDACTED]
13/02/2025	14:41		12.288 [REDACTED]
12/02/2025	12:31	<DIR>	[REDACTED]
08/01/2025	12:22	<DIR>	[REDACTED]
22/12/2024	00:26	<DIR>	[REDACTED]
24/06/2022	14:18	<DIR>	[REDACTED]
26/10/2024	15:19	<DIR>	[REDACTED]
01/04/2024	08:26	<DIR>	Pe [REDACTED]
14/02/2025	19:53	<DIR>	Program Files
14/02/2025	17:17	<DIR>	Program Files (x86)
12/12/2024	11:18	<DIR>	Python312
23/01/2025	20:59	<DIR>	Python313
03/10/2024	22:05	<DIR>	Users
19/02/2025	13:53	<DIR>	Windows
05/09/2024	00:13	<DIR>	[REDACTED]
		2 File(s)	12.802 bytes
		18 Dir(s)	3.331.812.343.808 bytes free

C:\>

Administrator: Windows PowerShell

PS C:\> Get-Alias dir

CommandType	Name	Version	Source
Alias	dir -> Get-ChildItem		

PS C:\> Get-ChildItem

Directory: C:\

Mode	LastWriteTime	Length	Name
d----	12/02/2025 12:17		[REDACTED]
d----	02/11/2024 00:59		[REDACTED]
da----	24/02/2024 01:11		[REDACTED]
d----	27/01/2025 00:09		[REDACTED]
d----	11/07/2023 21:44		[REDACTED]
d----	12/02/2025 12:31		[REDACTED]
d----	08/01/2025 12:22		[REDACTED]
d----	22/12/2024 00:26		[REDACTED]
d----	24/06/2022 15:18		[REDACTED]
d----	26/10/2024 16:19		[REDACTED]
d----	01/04/2024 09:26		[REDACTED]
d-r---	14/02/2025 19:53		Program Files
d-r---	14/02/2025 17:17		Program Files (x86)
d----	12/12/2024 11:18		[REDACTED]
d----	23/01/2025 20:59		[REDACTED]
d-r---	03/10/2024 23:05		Users
d----	19/02/2025 13:53		Windows
d----	05/09/2024 01:13		[REDACTED]
-a----	26/10/2024 00:45	514	[REDACTED].txt
-a----	13/02/2025 14:41	12288	[REDACTED]

PS C:\>

Administrator: Windows PowerShell

```
-a----      26/10/2024      00:45      514 DriverInstall2024-10-26.txt
-a----      13/02/2025      14:41     12288 DumpStack.log
```

PS C:\> ipconfig

Windows IP Configuration

Unknown adapter VPI [REDACTED]

```
Connection-specific DNS Suffix . : [REDACTED]
IPv4 Address. . . . . : 192.168.178.205
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 0.0.0.0
```

Ethernet adapter vEthernet (Default Switch):

```
Connection-specific DNS Suffix . : [REDACTED]
Link-local IPv6 Address . . . . . : [REDACTED]
IPv4 Address. . . . . : 172.20.192.1
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . :
```

Ethernet adapter Ethernet 2:

```
Connection-specific DNS Suffix . : [REDACTED]
Link-local IPv6 Address . . . . . : [REDACTED]
IPv4 Address. . . . . : 192.168.88.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.88.1
```

Ethernet adapter Ethernet 5:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
```

Ethernet adapter Ethernet 4:

```
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::d746:3f23:49ab:ccfd%10
IPv4 Address. . . . . : 192.168.56.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

Wireless LAN adapter Connessione alla rete locale (LAN)* 2:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
```

Wireless LAN adapter Connessione alla rete locale (LAN)* 14:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
```

Wireless LAN adapter Wi-Fi 2:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
```

Ethernet adapter Connessione di rete Bluetooth 5:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
```

PS C:\>

```

Administrator: Command Prompt

2 File(s)      12.802 bytes
18 Dir(s)  3.331.812.343.808 bytes free

C:\>ipconfig

Windows IP Configuration

Unknown adapter VPNMarco:

    Connection-specific DNS Suffix  . : fritz.box
    IPv4 Address. . . . . : 192.168.88.24
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 0.0.0.0

Ethernet adapter vEthernet (Default Switch):

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::2f84:a0d6:9f6b:a386%40
    IPv4 Address. . . . . : 172.20.192.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::1111:caff:942f:1003%9
    IPv4 Address. . . . . : 192.168.88.24
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.88.1

Ethernet adapter Ethernet 5:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Ethernet adapter Ethernet 4:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::d746:3f23:49ab:ccfd%10
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Wireless LAN adapter Connessione alla rete locale (LAN)* 14:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Connessione alla rete locale (LAN)* 14:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Wi-Fi 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Ethernet adapter Connessione di rete Bluetooth 5:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\>

```

Il gateway trovato è il gateway della vpn a cui sono connesso, nascosto per privacy

Parte 3: Esplorazione dei cmdlet

Obiettivo

Esaminare i cmdlet di PowerShell e il loro utilizzo.

Procedura

1. Scoperto l'alias di dir usando Get-Alias dir.
2. Eseguito Get-ChildItem come alternativa a dir.
3. Utilizzato Get-Command per visualizzare l'elenco dei cmdlet disponibili.
4. Eseguito Get-Help Get-Process per visualizzare informazioni su un cmdlet specifico.

PowerShell fornisce una serie di cmdlet con funzionalità avanzate rispetto al Prompt dei comandi.

```
PS C:\> Get-Command
```

CommandType	Name	Version	Source
-----	----	-----	-----
Alias	Add-AppPackage	2.0.1.0	Appx
Alias	Add-AppPackageVolume	2.0.1.0	Appx
Alias	Add-AppProvisionedPackage	3.0	Dism
Alias	Add-MsixPackage	2.0.1.0	Appx
Alias	Add-MsixPackageVolume	2.0.1.0	Appx
Alias	Add-MsixVolume	2.0.1.0	Appx
Alias	Add-ProvisionedAppPackage	3.0	Dism
Alias	Add-ProvisionedAppSharedPackageContainer	3.0	Dism
Alias	Add-ProvisionedAppxPackage	3.0	Dism
Alias	Add-ProvisioningPackage	3.0	Provisioning
Alias	Add-TrustedProvisioningCertificate	3.0	Provisioning
Alias	Apply-WindowsUnattend	3.0	Dism
Alias	Disable-PhysicalDiskIndication	2.0.0.0	Storage
Alias	Disable-PhysicalDiskIndication	1.0.0.0	VMDirectStorage
Alias	Disable-StorageDiagnosticLog	2.0.0.0	Storage
Alias	Disable-StorageDiagnosticLog	1.0.0.0	VMDirectStorage
Alias	Dismount-AppPackageVolume	2.0.1.0	Appx
Alias	Dismount-MsixPackageVolume	2.0.1.0	Appx
Alias	Dismount-MsixVolume	2.0.1.0	Appx
Alias	Enable-PhysicalDiskIndication	2.0.0.0	Storage
Alias	Enable-PhysicalDiskIndication	1.0.0.0	VMDirectStorage
Alias	Enable-StorageDiagnosticLog	2.0.0.0	Storage
Alias	Enable-StorageDiagnosticLog	1.0.0.0	VMDirectStorage
Alias	Export-VMCheckpoint	2.0.0.0	Hyper-V
Alias	Export-VMCheckpoint	1.0.0.0	VMDirectStorage
Alias	Flush-Volume	2.0.0.0	Storage

```
PS C:\> Get-Help Get-Process
```

Do you want to run Update-Help?

The Update-Help cmdlet downloads the most current Help files for Windows PowerShell modules, and installs them on your computer. For more information about the Update-Help cmdlet, see <https://go.microsoft.com/fwlink/?LinkId=210614>.

[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): y

```
PS C:\> Get-Help Get-Process
```

Do you want to run Update-Help?

The Update-Help cmdlet downloads the most current Help files for Windows PowerShell modules, and installs them on your computer. For more information about the Update-Help cmdlet, see <https://go.microsoft.com/fwlink/?LinkId=210614>.

[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): y

NAME

Get-Process

SYNOPSIS

Gets the processes that are running on the local computer or a remote computer.

SYNTAX

```
Get-Process [[-Name] <System.String[]>] [-ComputerName <System.String[]>] [-FileVersionInfo] [-Module] [<CommonParameters>]
```

```
Get-Process [-ComputerName <System.String[]>] [-FileVersionInfo] -Id <System.Int32[]> [-Module] [<CommonParameters>]
```

```
Get-Process [-ComputerName <System.String[]>] [-FileVersionInfo] -InputObject <System.Diagnostics.Process[]> [-Module] [<CommonParameters>]
```

```
Get-Process -Id <System.Int32[]> -IncludeUserName [<CommonParameters>]
```

```
Get-Process [[-Name] <System.String[]>] -IncludeUserName [<CommonParameters>]
```

```
Get-Process -IncludeUserName -InputObject <System.Diagnostics.Process[]> [<CommonParameters>]
```

DESCRIPTION

The `Get-Process` cmdlet gets the processes on a local or remote computer.

Without parameters, this cmdlet gets all of the processes on the local computer. You can also specify a particular process by process name or process ID (PID) or pass a process object through the pipeline to this cmdlet.

By default, this cmdlet returns a process object that has detailed information about the process and supports methods that let you start and stop the process. You can also use the parameters of the `Get-Process` cmdlet to get file version information for the program that runs in the process and to get the modules that the process loaded.

RELATED LINKS

Online Version:

https://learn.microsoft.com/powershell/module/microsoft.powershell.management/get-process?view=powershell-5.1&WT.mc_id=ps-gethelp

Debug-Process

Get-Process

Start-Process

Stop-Process

Wait-Process

REMARKS

To see the examples, type: "get-help Get-Process -examples".

For more information, type: "get-help Get-Process -detailed".

For technical information, type: "get-help Get-Process -full".

For online help, type: "get-help Get-Process -online"

```
PS C:\> _
```

- `dir`: fornisce un output simile in entrambi gli ambienti.
- `ipconfig`: funziona correttamente in PowerShell e `cmd`.
- Alcuni comandi hanno alias in PowerShell.

Parte 4: Esplorazione del comando netstat utilizzando PowerShell

Obiettivo

Utilizzare netstat per monitorare le connessioni di rete.

Procedura

1. Eseguito netstat -h per elencare le opzioni disponibili.
2. Eseguito netstat -r per visualizzare la tabella di routing.
3. Avviata PowerShell come amministratore e eseguito netstat -abno.
4. Identificato un processo tramite il PID in **Gestione attività**.

Risultati

L'uso di netstat ha permesso di monitorare le connessioni e identificare i processi in ascolto sulla rete.

```
PS C:\> netstat -h
```

Socket Handle Count

PID	Count	Closing Count
22784	3	0
5124	4	0
7684	8	0
12808	1	0
6924	18	0
39436	2	0
16916	7	1
8216	11	0
6940	4	0
8476	1	0
22556	35	0
37660	19	6
26152	1	0
2348	4	0
4908	7	1
16176	2	0
30516	4	0
3128	2	0
8504	204	0
8512	6	0
2376	4	0
25672	75	0
9040	3	0
8792	2	0
25176	17	4
24924	2	0
26972	6	0
5220	2	0
9060	10	0
26468	1	0
2152	4	0
13672	4	1
5484	6	0
14956	7	0
8816	2	0
24180	4	0
3704	29	3
16252	8	0
2688	11	0
21376	33	0
7044	9	0
25732	1	0

PS C:\>

PS C:\> netstat -r

Interface List

```
77.....WireGuard Tunnel
40...00 15 5d 4c 01 00 .....Hyper-V Virtual Ethernet Adapter
9...fc 34 97 a6 b7 3b .....Intel(R) Ethernet Controller (3) I225-V
3...00 ff 0b 75 fb da .....TAP-Windows Adapter V9
10...0a 00 27 00 00 0a .....VirtualBox Host-Only Ethernet Adapter
14...68 54 5a 90 57 b9 .....Microsoft Wi-Fi Direct Virtual Adapter #5
30...6a 54 5a 90 57 b8 .....Microsoft Wi-Fi Direct Virtual Adapter #8
5...68 54 5a 90 57 b8 .....Intel(R) Wi-Fi 6 AX200 160MHz #2
19...68 54 5a 90 57 bc .....Bluetooth Device (Personal Area Network) #5
1.....Software Loopback Interface 1
```

IPv4 Route Table

Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	0.0.0.0	On-link	192.168.178.205	0
0.0.0.0	0.0.0.0	0.0.0.0	192.168.88.1	192.168.88.24	25
127.0.0.0	255.0.0.0	255.0.0.0	On-link	127.0.0.1	331
127.0.0.1	255.255.255.255	255.255.255.255	On-link	127.0.0.1	331
127.255.255.255	255.255.255.255	255.255.255.255	On-link	127.0.0.1	331
172.20.192.0	255.255.240.0	255.255.240.0	On-link	172.20.192.1	271
172.20.192.1	255.255.255.255	255.255.255.255	On-link	172.20.192.1	271
172.20.207.255	255.255.255.255	255.255.255.255	On-link	172.20.192.1	271
192.168.56.0	255.255.255.0	255.255.255.0	On-link	192.168.56.1	281
192.168.56.1	255.255.255.255	255.255.255.255	On-link	192.168.56.1	281
192.168.56.255	255.255.255.255	255.255.255.255	On-link	192.168.56.1	281
192.168.88.0	255.255.255.0	255.255.255.0	On-link	192.168.88.24	281
192.168.88.24	255.255.255.255	255.255.255.255	On-link	192.168.88.24	281
192.168.88.255	255.255.255.255	255.255.255.255	On-link	192.168.88.24	281
192.168.178.0	255.255.255.0	255.255.255.0	On-link	192.168.178.205	0
192.168.178.205	255.255.255.255	255.255.255.255	On-link	192.168.178.205	256
192.168.178.255	255.255.255.255	255.255.255.255	On-link	192.168.178.205	256
224.0.0.0	240.0.0.0	240.0.0.0	On-link	127.0.0.1	331
224.0.0.0	240.0.0.0	240.0.0.0	On-link	192.168.56.1	281
224.0.0.0	240.0.0.0	240.0.0.0	On-link	192.168.88.24	281
224.0.0.0	240.0.0.0	240.0.0.0	On-link	172.20.192.1	271
255.255.255.255	255.255.255.255	255.255.255.255	On-link	127.0.0.1	331
255.255.255.255	255.255.255.255	255.255.255.255	On-link	192.168.56.1	281
255.255.255.255	255.255.255.255	255.255.255.255	On-link	192.168.88.24	281
255.255.255.255	255.255.255.255	255.255.255.255	On-link	172.20.192.1	271

Persistent Routes:

Network	Address	Netmask	Gateway Address	Metric
0.0.0.0	0.0.0.0	0.0.0.0	100.127.255.254	1

IPv6 Route Table

Active Routes:

If	Metric	Network	Destination	Gateway
1	331	:::1/128		On-link
10	281	fe80::/64		On-link
9	281	fe80::/64		On-link
40	271	fe80::/64		On-link
9	281	fe80::1111:caff:942f:1003/128		

=====

Persistent Routes:

Network	Address	Netmask	Gateway Address	Metric
0.0.0.0		0.0.0.0	100.127.255.254	1

=====

IPv6 Route Table

=====

Active Routes:

If	Metric	Network	Destination	Gateway
1	331	::1/128		On-link
10	281	fe80::/64		On-link
9	281	fe80::/64		On-link
40	271	fe80::/64		On-link
9	281	fe80::1111:caff:942f:1003/128		On-link
40	271	fe80::2f84:a0d6:9f6b:a386/128		On-link
10	281	fe80::d746:3f23:49ab:ccfd/128		On-link
1	331	ff00::/8		On-link
10	281	ff00::/8		On-link
9	281	ff00::/8		On-link
40	271	ff00::/8		On-link

=====

Persistent Routes:

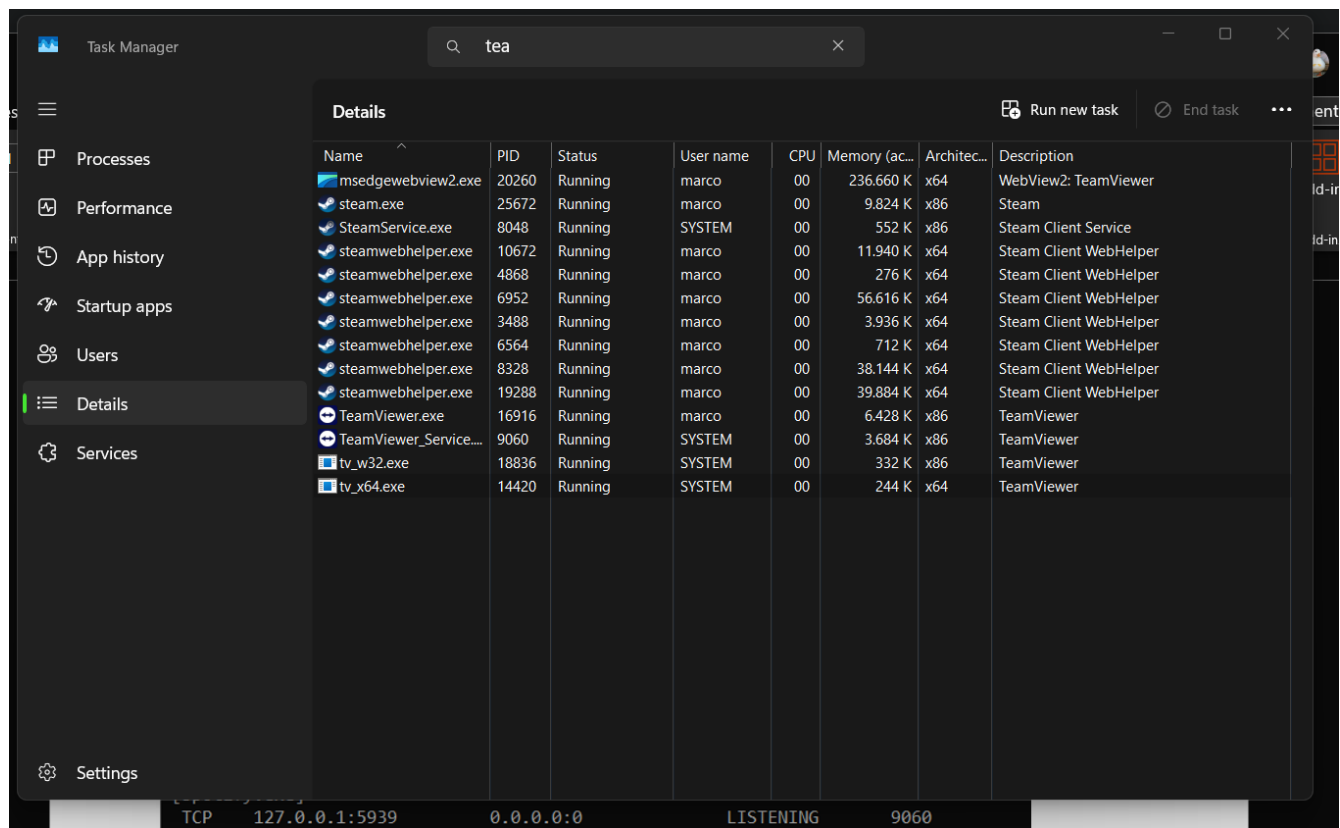
None

PS C:\>

```
PS C:\> netstat -abno
```

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	2688
RpcSs				
[svchost.exe]				
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
Can not obtain ownership information				
TCP	0.0.0.0:1716	0.0.0.0:0	LISTENING	25008
[kdeconnectd.exe]				
TCP	0.0.0.0:2179	0.0.0.0:0	LISTENING	5028
[vmms.exe]				
TCP	0.0.0.0:2869	0.0.0.0:0	LISTENING	4
Can not obtain ownership information				
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING	14956
CDPSvc				
[svchost.exe]				
TCP	0.0.0.0:7070	0.0.0.0:0	LISTENING	8360
[AnyDesk.exe]				
TCP	0.0.0.0:10020	0.0.0.0:0	LISTENING	3324
[G_Menu.exe]				
TCP	0.0.0.0:27036	0.0.0.0:0	LISTENING	25672
[steam.exe]				
TCP	0.0.0.0:47984	0.0.0.0:0	LISTENING	16252
[Sunshine.exe]				
TCP	0.0.0.0:47989	0.0.0.0:0	LISTENING	16252
[Sunshine.exe]				
TCP	0.0.0.0:47990	0.0.0.0:0	LISTENING	16252
[Sunshine.exe]				
TCP	0.0.0.0:48010	0.0.0.0:0	LISTENING	16252
[Sunshine.exe]				
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	2376
Can not obtain ownership information				
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	2152
Can not obtain ownership information				
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	3264
Schedule				
[svchost.exe]				
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	5124
EventLog				
[svchost.exe]				
TCP	0.0.0.0:49698	0.0.0.0:0	LISTENING	6940
[spoolsv.exe]				
TCP	0.0.0.0:49760	0.0.0.0:0	LISTENING	2348
Can not obtain ownership information				
TCP	0.0.0.0:57621	0.0.0.0:0	LISTENING	22556
[Spotify.exe]				
TCP	0.0.0.0:64343	0.0.0.0:0	LISTENING	22556
[Spotify.exe]				
TCP	127.0.0.1:5939	0.0.0.0:0	LISTENING	9060
[TeamViewer_Service.exe]				
TCP	127.0.0.1:5939	127.0.0.1:49825	ESTABLISHED	9060
[TeamViewer_Service.exe]				
TCP	127.0.0.1:6463	0.0.0.0:0	LISTENING	21376
[Vesktop.exe]				



Parte 5: Svuotamento del Cestino utilizzando PowerShell

Obiettivo

Svuotare il Cestino tramite PowerShell.

Procedura

1. Verificato il contenuto del Cestino.
2. Eseguito il comando Clear-RecycleBin.
3. Confermata l'operazione digitando Y.

Il Cestino può essere svuotato con successo tramite PowerShell.

```
PS C:\> Clear-RecycleBin

Confirm
Are you sure you want to perform this action?
Performing the operation "Clear-RecycleBin" on target "All of the contents of the Recycle Bin".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"):
```

Esercizio 2

Studiare questo link di anyrun e spiegare queste minacce in un piccolo report.

<https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281/>

L'analisi del file sospetto **Jvczfhe.exe** ha rivelato la creazione e l'interazione con diversi processi ed eseguibili nel sistema. Ecco un dettaglio specifico:

Processi ed eseguibili:

1. Processo principale:

- **Nome:** Jvczfhe.exe.bin.exe
- **Percorso:** C:\Users\admin\AppData\Local\Temp\Jvczfhe.exe.bin.exe
- **PID:** 6496
- **Descrizione:** Questo è il processo eseguibile principale avviato dall'utente. Si spaccia per "Microsoft Edge" con una versione dichiarata di 126.0.2592.113, ma opera da una directory temporanea, il che è atipico per applicazioni legittime.

[7492] Jvczfhe.exe C:\Users\admin\Downloads\Jvczfhe.exe

Threat Verdict

51

OUT OF 100

Suspicious

The score is an approximate value calculated by ANY.RUN algorithm based on process and user actions

Indicators:

Process information

Username: admin

SID: S-1-5-21-1693682860-607145093-2874071422-1001

IL: MEDIUM

Start: 22.10 s

File information

Company: Microsoft Corporation

Description: Microsoft Edge

Version: 126.0.2592.113

Command line

"C:\Users\admin\Downloads\Jvczfhe.exe"

Timeline of the process

0 s 22.10 s 62.16 s

11

22.10 s

Warning 3

Executes application which crashes

T1012 Query Registry (2)

Reads security settings of Internet Explorer

Checks Windows Trust Settings

T1059.003 Windows Command Shell (1)

Starts CMD.EXE for commands execution

Other 3

T1012 Query Registry (6)

Reads the software policy settings

Checks proxy server information

Reads Environment values

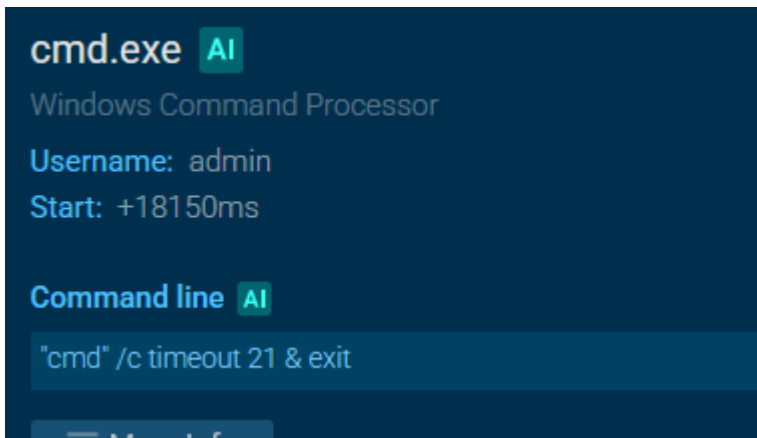
Reads the machine GUID from the registry

Reads the computer name

2. Processi secondari avviati:

○ cmd.exe

- **Comando:** "cmd" /c timeout 21 & exit
- **Percorso:** C:\Windows\SysWOW64\cmd.exe
- **PID:** 6680
- **Descrizione:** Il processo principale avvia il prompt dei comandi per eseguire il comando timeout, indicando una possibile tecnica di evasione o sincronizzazione temporale.



○ conhost.exe

- **Comando:** \??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1
- **Percorso:** C:\Windows\System32\conhost.exe
- **PID:** 6708
- **Descrizione:** Associato a cmd.exe, gestisce le finestre della console per le applicazioni della riga di comando.

○ timeout.exe

- **Comando:** timeout 21
- **Percorso:** C:\Windows\SysWOW64\timeout.exe
- **PID:** 6752
- **Descrizione:** Utilizzato per introdurre un ritardo di 21 secondi nell'esecuzione, spesso impiegato per sincronizzare attività o ritardare l'esecuzione di ulteriori comandi.

Esecuzione da percorso non standard: Il processo principale viene eseguito da una directory temporanea (AppData\Local\Temp), il che è insolito per applicazioni legittime come Microsoft Edge.

Uso di comandi della riga di comando: L'avvio di cmd.exe e l'esecuzione di timeout.exe suggeriscono tentativi di evasione o sincronizzazione, comuni nei comportamenti malevoli.

Falsificazione delle informazioni del file: Il processo principale dichiara di essere "Microsoft Edge" con dettagli come versione e descrizione corrispondenti, ma l'esecuzione da una directory temporanea e il nome del file sono sospetti.

Questi comportamenti indicano che **Jvczfhe.exe** potrebbe essere un eseguibile malevolo progettato per mascherarsi come un'applicazione legittima, eseguendo comandi di sistema per potenziali attività dannose.

Esercizio 3: è un banale esercizio di nmap

Esercizio 4: si tratta di un attacco SQL injection. Consiste in inserire istruzioni SQL in un sito web per ottenere una risposta dal database. Si può fare per alterare informazioni nel database o compiere azioni dannose. Viene fornito un file .pap e dall'http stream possiamo vedere che viene utilizzata la query 1=1 la prima volta e successivamente 1' or 1=1 union select database(), user()#) che permette di ottenere l'intero database e l'utente root localhost.

Viene poi usata la query 1' or 1=1 union select null, table_name from information_schema.tables# per Vedere tutte le tabelle del database, poi viene usata 1' or 1=1 union select user, password from user# che permette di ottenere le credenziali degli utenti. Nomi utente e password hashate. Si tratta di md5 di facile de-hashing