

Esercizio 1: Usare Windows PowerShell

Obiettivi

Accedere alla console PowerShell.

Esplorare i comandi del Prompt dei Comandi e di PowerShell.

Esplorare i cmdlet.

Esplorare il comando netstat usando PowerShell.

Svuotare il cestino usando PowerShell.

Macchine utilizzate: pfSense, Windows 10 pro.

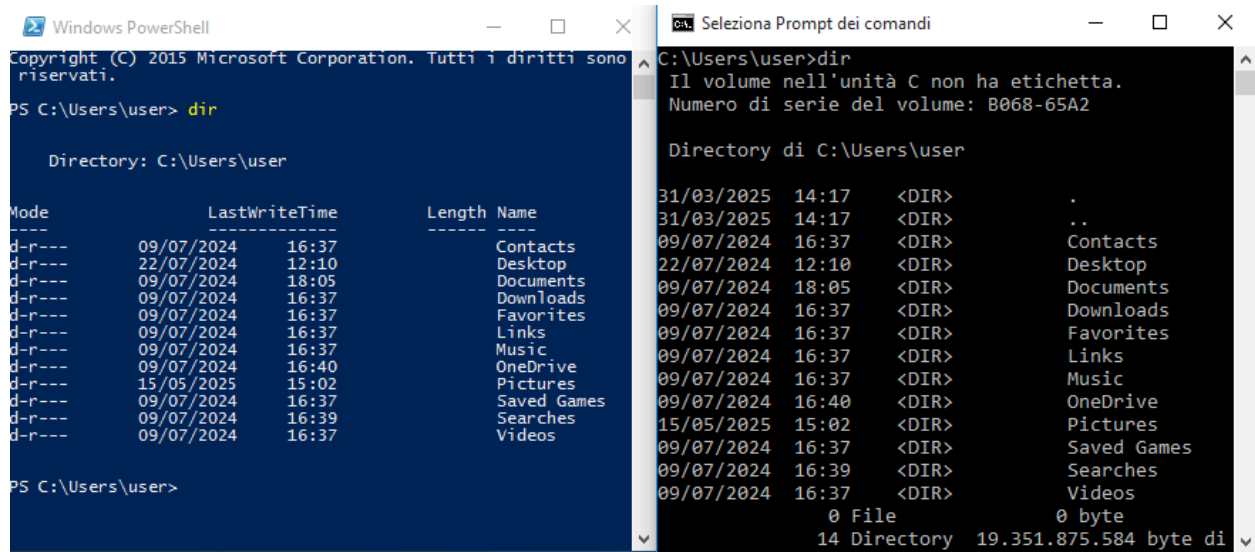
Configurazione della rete: La scheda di rete della macchina **Windows 10 pro** è stata impostata in rete interna, la stessa gestita da pfSense, che svolge la funzione di router in questo caso.

Per prima cosa, sono stati aperti **Windows PowerShell** e **Command Prompt** dal menù **Start**.

Successivamente, in entrambe le finestre, è stato utilizzato il comando **dir**.

Quali sono gli output del comando dir?

L'output è stato il seguente:



```
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

PS C:\Users\user> dir

Directory: C:\Users\user

Mode                LastWriteTime         Length Name
----                -
d-r---           09/07/2024   16:37             Contacts
d-r---           22/07/2024   12:10             Desktop
d-r---           09/07/2024   18:05             Documents
d-r---           09/07/2024   16:37             Downloads
d-r---           09/07/2024   16:37             Favorites
d-r---           09/07/2024   16:37             Links
d-r---           09/07/2024   16:37             Music
d-r---           09/07/2024   16:40             OneDrive
d-r---           15/05/2025   15:02             Pictures
d-r---           09/07/2024   16:37             Saved Games
d-r---           09/07/2024   16:39             Searches
d-r---           09/07/2024   16:37             Videos

PS C:\Users\user>
```

```
Seleziona Prompt dei comandi
C:\Users\user>dir
Il volume nell'unità C non ha etichetta.
Numero di serie del volume: B068-65A2

Directory di C:\Users\user

31/03/2025  14:17  <DIR>          .
31/03/2025  14:17  <DIR>          ..
09/07/2024  16:37  <DIR>          Contacts
22/07/2024  12:10  <DIR>          Desktop
09/07/2024  18:05  <DIR>          Documents
09/07/2024  16:37  <DIR>          Downloads
09/07/2024  16:37  <DIR>          Favorites
09/07/2024  16:37  <DIR>          Links
09/07/2024  16:37  <DIR>          Music
09/07/2024  16:37  <DIR>          OneDrive
09/07/2024  16:40  <DIR>          Pictures
15/05/2025  15:02  <DIR>          Saved Games
09/07/2024  16:39  <DIR>          Searches
09/07/2024  16:37  <DIR>          Videos
               0 File                0 byte
               14 Directory  19.351.875.584 byte di
```

Il comando mostra come output i file e le cartelle presenti nella Directory in cui ci troviamo.

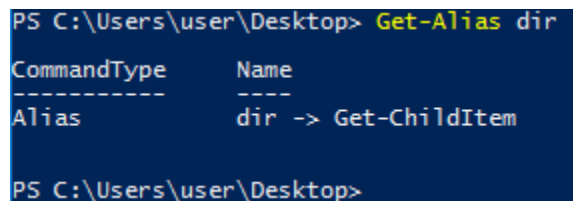
Sono state effettuate altre prove con comandi come **cd**, **ipconfig** e **ping**.

Quali sono i risultati?

L'output in questi casi è stato lo stesso.

La differenza nell'output quindi la si può trovare solo utilizzando comandi nativi di **PowerShell**, chiamati **cmdlet**.

E' stato inserito il comando **Get-Alias dir** sul prompt di PowerShell con il seguente output:



```
PS C:\Users\user\Desktop> Get-Alias dir

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

PS C:\Users\user\Desktop>
```

La struttura del comando **cmdlet** è quindi **<Verbo>-<Nome>**.

Qual è il comando PowerShell per dir?

In questo caso, possiamo utilizzare il comando **Get-ChildItem** per visualizzare i file e le cartelle presenti nella directory.

```
PS C:\Users\user\Desktop> Get-ChildItem

Directory: C:\Users\user\Desktop

Mode                LastWriteTime         Length Name
----                -
d-----          22/07/2024   12:09             Malware
d-----          22/07/2024   12:10             Programmi
                        per Malware
                        analisi
-a-----          22/07/2024   11:52             532 debug.log
-a-----          12/07/2024   13:07             1118 Icecast2
                        Win32.lnk
-a-----          12/07/2024   12:28             1091 tomcat.lnk

PS C:\Users\user\Desktop>
```

Esplorazione del comando **netstat**

Netstat viene utilizzato per mostrare informazioni riguardo la connessione di rete.

E' stato inserito nel Prompt di PowerShell il comando **netstat -h**. Ciò ci ha fornito un output contenente tutti i possibili comandi da poter effettuare insieme a netstat.

Per visualizzare la tabella di routing con le rotte attive, è stato inserito **netstat -r**.

L'output è stato il seguente:

```
PS C:\Users\user> netstat -r
=====
Elenco interfacce
4...08 00 27 d4 ce 85 .....Intel(R) PRO/1000 MT Desktop Adapter
1.....Software Loopback Interface 1
5...00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
3...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
=====

IPv4 Tabella route
=====
Route attive:
  Indirizzo rete      Mask      Gateway      Interfaccia  Metrica
  0.0.0.0             0.0.0.0    192.168.56.1  192.168.56.12  10
  127.0.0.0           255.0.0.0    On-link      127.0.0.1      306
  127.0.0.1           255.255.255.255  On-link      127.0.0.1      306
  127.255.255.255     255.255.255.255  On-link      127.0.0.1      306
  192.168.56.0        255.255.255.0   On-link      192.168.56.12  266
  192.168.56.12       255.255.255.255  On-link      192.168.56.12  266
  192.168.56.255      255.255.255.255  On-link      192.168.56.12  266
  224.0.0.0           240.0.0.0    On-link      127.0.0.1      306
  224.0.0.0           240.0.0.0    On-link      192.168.56.12  266
  255.255.255.255     255.255.255.255  On-link      127.0.0.1      306
  255.255.255.255     255.255.255.255  On-link      192.168.56.12  266
=====
Route permanenti:
  Nessuna

IPv6 Tabella route
=====
Route attive:
  InterF  Metrica  Rete Destinazione      Gateway
  5       306    ::/0                    On-link
  1       306    ::1/128                 On-link
  5       306    2001::/32               On-link
  5       306    2001:0:2851:782c:142b:1b3f:b0d1:ab0f/128
                                On-link
  4       266    fe80::/64                On-link
  5       306    fe80::/64                On-link
  5       306    fe80::142b:1b3f:b0d1:ab0f/128
                                On-link
  4       266    fe80::78df:8c7a:dc70:ca5f/128
                                On-link
  1       306    ff00::/8                 On-link
  4       266    ff00::/8                 On-link
  5       306    ff00::/8                 On-link
=====
Route permanenti:
  Nessuna
```

Qual è il Gateway IPv4?

Il Gateway IPv4 è 192.168.56.1, relativo alla configurazione della rete attuale.

E' stata aperta una seconda sessione di **PowerShell** con permessi di amministratore.

Qui è stato inserito **netstat -abno**.

Il comando fornisce in output i processi associati alle connessioni **TCP** attive.

Successivamente, è stato aperto il **Task Manager**, che mostra tutti i processi attivi.

Nella scheda dei Dettagli, è stato impostato PID in ordine cliccando su di esso.

Amministratore: Windows PowerShell

Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Tutti i diritti sono riservati.
PS C:\Windows\system32> netstat -abno

Connessioni attive

Proto	Indirizzo locale	Indirizzo esterno	Stato	PID
TCP	0.0.0.0:7	0.0.0.0:0	LISTENING	1880
[tcpvscs.exe]				
TCP	0.0.0.0:9	0.0.0.0:0	LISTENING	1880
[tcpvscs.exe]				
TCP	0.0.0.0:13	0.0.0.0:0	LISTENING	1880
[tcpvscs.exe]				
TCP	0.0.0.0:17	0.0.0.0:0	LISTENING	1880
[tcpvscs.exe]				
TCP	0.0.0.0:19	0.0.0.0:0	LISTENING	1880
[tcpvscs.exe]				
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	4
Impossibile ottenere informazioni sulla proprietà				
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	676
RpcSs				
[svchost.exe]				
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
Impossibile ottenere informazioni sulla proprietà				
TCP	0.0.0.0:1801	0.0.0.0:0	LISTENING	1864
[mqsvcs.exe]				
TCP	0.0.0.0:2103	0.0.0.0:0	LISTENING	1864
[mqsvcs.exe]				
TCP	0.0.0.0:2105	0.0.0.0:0	LISTENING	1864
[mqsvcs.exe]				
TCP	0.0.0.0:2107	0.0.0.0:0	LISTENING	1864
[mqsvcs.exe]				
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING	848
TermService				
[svchost.exe]				
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING	4
Impossibile ottenere informazioni sulla proprietà				
TCP	0.0.0.0:5432	0.0.0.0:0	LISTENING	2364
[postgres.exe]				
TCP	0.0.0.0:8009	0.0.0.0:0	LISTENING	2112
[tomcat7.exe]				
TCP	0.0.0.0:8080	0.0.0.0:0	LISTENING	2112
[tomcat7.exe]				
TCP	0.0.0.0:8443	0.0.0.0:0	LISTENING	4
Impossibile ottenere informazioni sulla proprietà				
TCP	0.0.0.0:49408	0.0.0.0:0	LISTENING	424
Impossibile ottenere informazioni sulla proprietà				
TCP	0.0.0.0:49409	0.0.0.0:0	LISTENING	864
Schedule				

Win32

Gestione attività

File Opzioni Visualizza

Processi Prestazioni Cronologia applicazioni Avvio Utenti Dettagli Servizi

Nome	PID	Stato	Nome ute...	CPU	Memoria (...)	Descrizione
Interrupt sistema	-	In esecuzione	SYSTEM	00	0 K	Chiamate di proced...
Processo di inattività...	0	In esecuzione	SYSTEM	99	4 K	Percentuale di temp...
System	4	In esecuzione	SYSTEM	00	7.696 K	NT Kernel & System
smss.exe	268	In esecuzione	SYSTEM	00	76 K	Gestione sessioni di ...
csrss.exe	348	In esecuzione	SYSTEM	00	464 K	Processo runtime cli...
svchost.exe	372	In esecuzione	SYSTEM	00	19.264 K	Processo host per se...
VBoxService.exe	420	In esecuzione	SYSTEM	00	688 K	VirtualBox Guest Ad...
wininit.exe	424	In esecuzione	SYSTEM	00	268 K	Applicazione di avvi...
csrss.exe	440	In esecuzione	SYSTEM	00	440 K	Processo runtime cli...
winlogon.exe	500	In esecuzione	SYSTEM	00	472 K	Applicazione Access...
services.exe	540	In esecuzione	SYSTEM	00	1.612 K	App Servizi e Contro...
lsass.exe	548	In esecuzione	SYSTEM	00	2.072 K	Local Security Auth...
svchost.exe	624	In esecuzione	SYSTEM	00	2.944 K	Processo host per se...
svchost.exe	676	In esecuzione	SERVIZIO ...	00	2.292 K	Processo host per se...
svchost.exe	848	In esecuzione	SERVIZIO ...	00	3.644 K	Processo host per se...
dwm.exe	856	In esecuzione	DWM-1	00	19.096 K	Gestione finestre de...
svchost.exe	864	In esecuzione	SYSTEM	00	9.588 K	Processo host per se...
svchost.exe	932	In esecuzione	SERVIZIO L...	00	896 K	Processo host per se...
svchost.exe	940	In esecuzione	SERVIZIO L...	00	6.728 K	Processo host per se...
svchost.exe	1056	In esecuzione	SERVIZIO L...	00	2.872 K	Processo host per se...
WmsSelfHealingSvc...	1268	In esecuzione	SYSTEM	00	356 K	WmsRepairService
WmsSvc.exe	1276	In esecuzione	SYSTEM	00	980 K	WmsService
cnool.exe	1508	In esecuzione	SYSTEM	00	940 K	Applicazione sottoc...

Meno dettagli

Termina attività

venerdì 13 giug...

E' stato selezionato un processo attivo come esempio, in questo caso **Tomcat** (essendo la macchina Metasploitable).

tomcat7.exe	2112	In esecuzione	SYSTEM	00	67.560 K	Commons Daemon ...
-------------	------	---------------	--------	----	----------	--------------------

E' stata aperta la pagina **Proprietà** relativa al processo.

Quali informazioni puoi ottenere dalla scheda Dettagli e dalla finestra di dialogo Proprietà per il PID selezionato?

Nella scheda **Dettagli**, si può vedere l'elenco completo dei processi attivi con le loro informazioni (**CPU** utilizzata dal processo e **RAM** utilizzata).

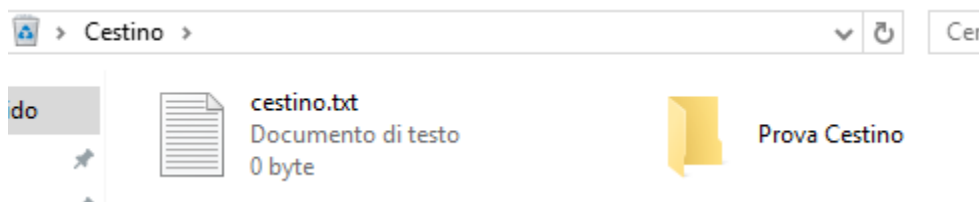
Nella scheda **Proprietà** invece, si può osservare il percorso del file, la sua dimensione e altri dettagli che riguardano la sua versione.

Generale	Compatibilità	Firme digitali
Sicurezza	Dettagli	Versioni precedenti

Si possono vedere inoltre i permessi del file e le firme digitali.

Svuotare il cestino usando PowerShell

La macchina utilizzata non aveva file nel cestino, quindi sono stati creati dei file di prova da eliminare e successivamente cancellati.



E' stato inserito il seguente comando sul Prompt di PowerShell:

```
PS C:\Users\user> clear-recyclebin
```

E con avvenuta conferma, il comando è stato eseguito.

Cosa è successo ai file nel Cestino?

I file nel cestino sono stati eliminati definitivamente.

Usando internet, ricerca comandi che potresti usare per semplificare i tuoi compiti come analista di sicurezza.

A ricerca effettuata, i comandi emersi come più importanti sono stati i seguenti:

Get-ChildItem -Recurse -Force -Hidden

Viene utilizzato per cercare file **nascosti** in tutte le sottocartelle.

Può essere utile per scovare **Malware**.

Get-Process, elenca tutti i processi attivi con **PID** e uso risorse.

Get-NetTCPConnection, mostra tutte le connessioni **TCP** attive, come **netstat**.

Stop-Process -Id <x> -Force

Sostituendo il numero del processo alla **x**, chiude il processo.

Altri comandi importanti possono essere:

query user, mostra utenti attivi, sessioni e terminali.

Get-LocalUser, elenca tutti gli utenti locali.

O comunque comandi per verificare file sospetti:

Get-FileHash "C:\percorso\file.exe", l'hash viene successivamente inviato a VirusTotal per verificarne la sicurezza.