S11/L5

1 Usare Windows PowerShell

Studente: Victor Rosati
Sistema Operativo: Windows 11 Home
Data: 20/02/26

Introduzione

L'obiettivo di questo laboratorio è esplorare le funzioni di PowerShell, confrontandole con il Prompt dei Comandi (CMD) e utilizzandole per compiti di amministrazione di sistema e analisi di rete.

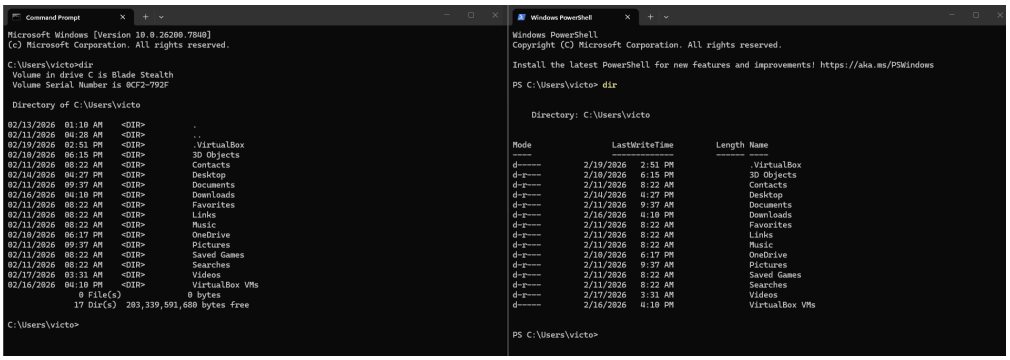
PowerShell è sia una console di comando che un linguaggio di scripting progettato per l'automazione.

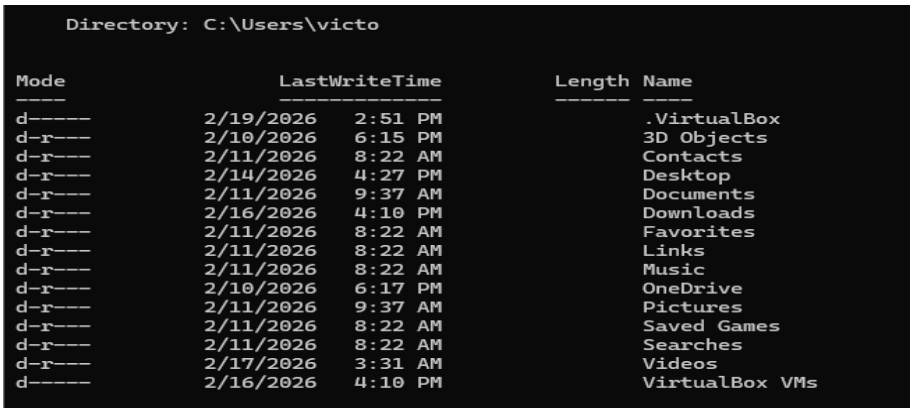
Parte 1 e 2: Esplorazione dei comandi base

In questa fase sono state aperte sia la console PowerShell che il Prompt dei Comandi per confrontare gli output.

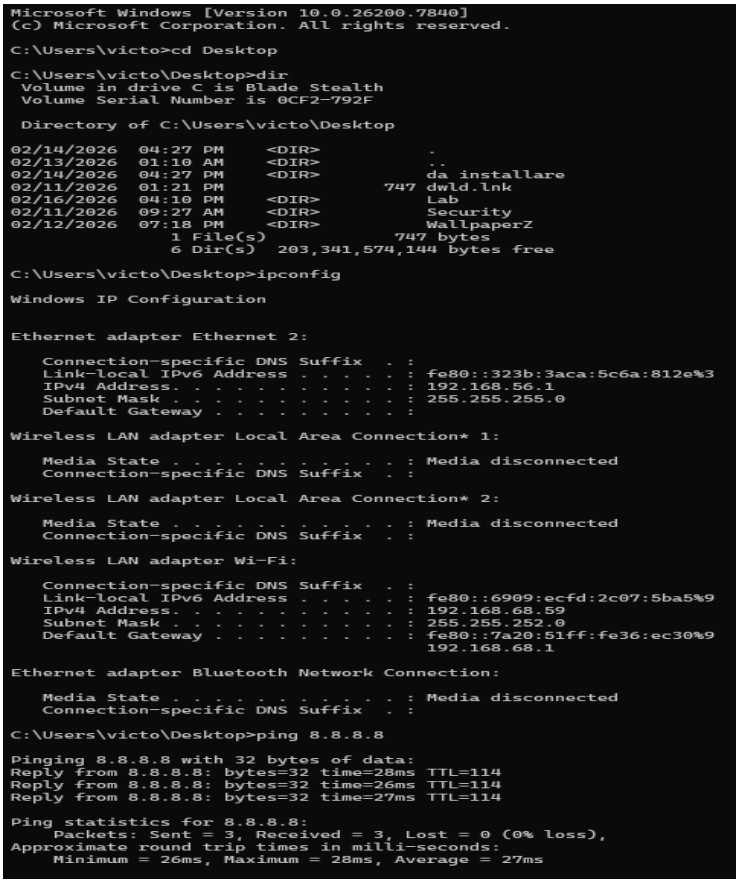
- **Confronto comando `dir`:** Nel **Prompt dei Comandi**, l'output è un elenco testuale che riporta data, ora, l'etichetta `<DIR>` e il nome.
    - In **PowerShell**, l'output è una tabella strutturata con colonne per `Mode`, `LastWriteTime`, `Length` e `Name`.
- **Comandi di rete:** Sono stati eseguiti i comandi `ipconfig`, `ping` e `cd`. I risultati mostrano la configurazione dell'adapter Wi-Fi e la raggiungibilità del server 8.8.8.8

Screenshot 1-2-3: *Output del comando dir nel Prompt dei Comand/PowerShelli:*





Screenshot 2: *Risultati dei comandi cd, ipconfig e ping:*



Parte 3: Esplorare i cmdlet

I comandi nativi di PowerShell sono chiamati **cmdlet** e seguono la struttura "verbo-nome".

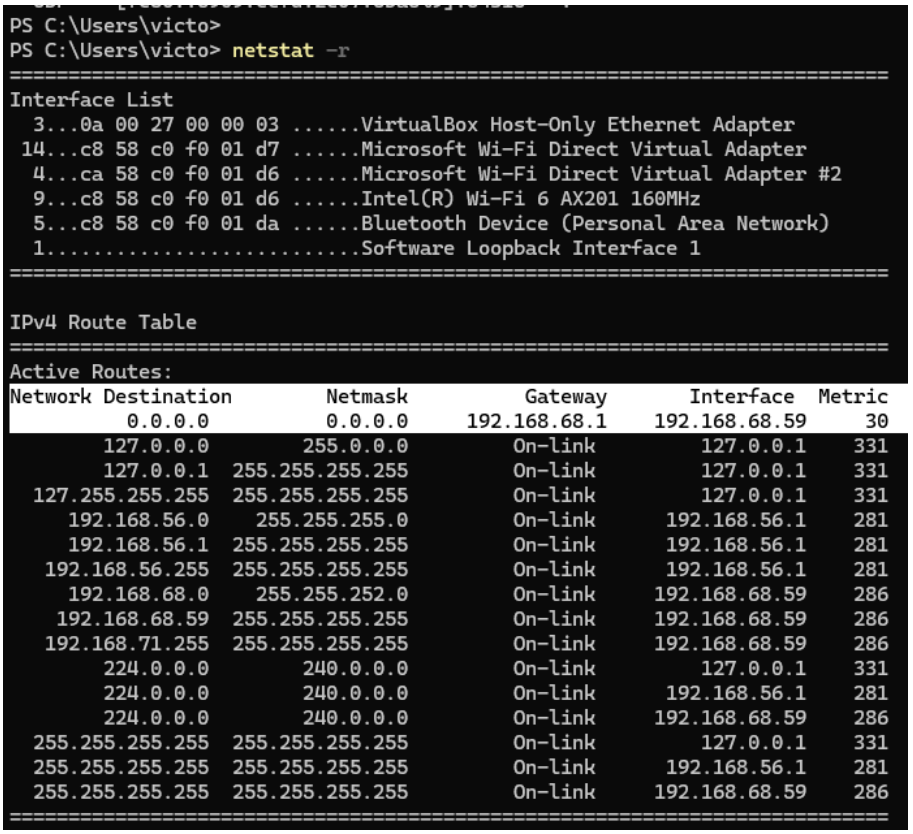
- Utilizzando il comando `Get-Alias dir`, è stato identificato che `dir` è un alias per il cmdlet **`Get-ChildItem`**.

Parte 4: Esplorare il comando netstat

È stata analizzata la tabella di routing del sistema utilizzando il comando `netstat -r`.

- **Identificazione Gateway:** Analizzando la tabella delle rotte attive per la destinazione `0.0.0.0`, è stato identificato il **Gateway IPv4:** 192.168.68.1.

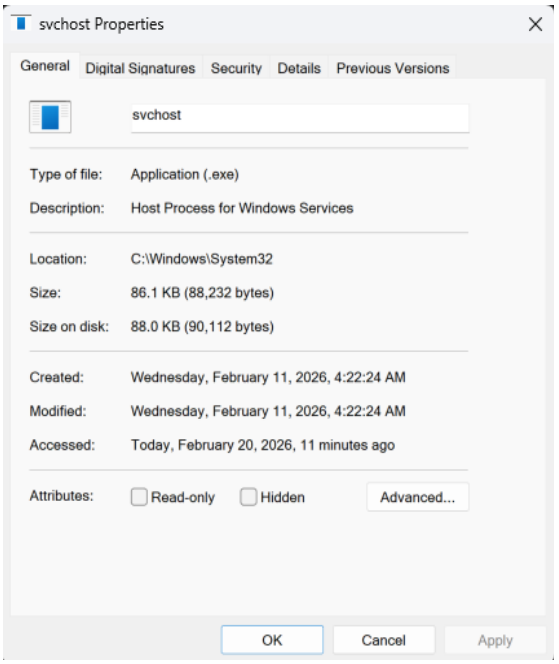
Screenshot 4: *Tabella di routing IPv4 e identificazione del Gateway.*

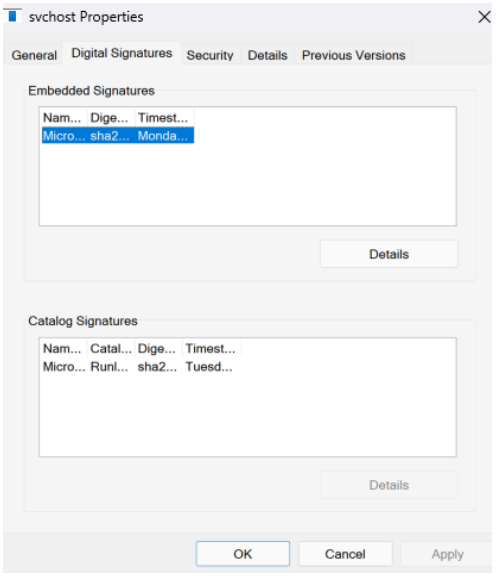


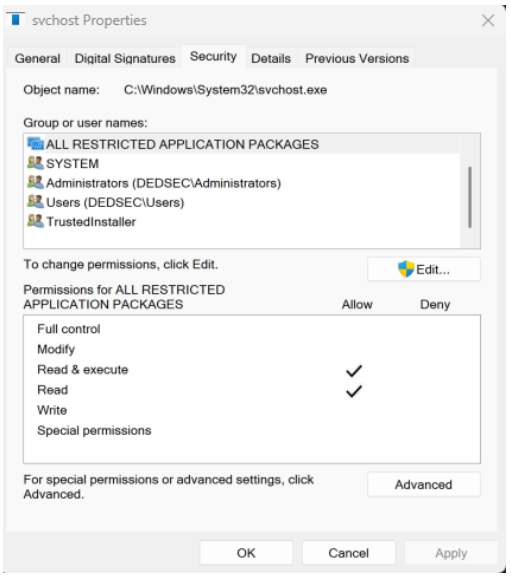
```
PS C:\Users\victo>
PS C:\Users\victo> netstat -r
===========================================================================
Interface List
  3...0a 00 27 00 00 03 ......VirtualBox Host-Only Ethernet Adapter
 14...c8 58 c0 f0 01 d7 ......Microsoft Wi-Fi Direct Virtual Adapter
  4...ca 58 c0 f0 01 d6 ......Microsoft Wi-Fi Direct Virtual Adapter #2
  9...c8 58 c0 f0 01 d6 ......Intel(R) Wi-Fi 6 AX201 160MHz
  5...c8 58 c0 f0 01 da ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.68.1    192.168.68.59     30
        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
     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
     192.168.68.0    255.255.252.0         On-link     192.168.68.59    286
    192.168.68.59  255.255.255.255         On-link     192.168.68.59    286
   192.168.71.255  255.255.255.255         On-link     192.168.68.59    286
        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     192.168.68.59    286
  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     192.168.68.59    286
===========================================================================
```

Successivamente, è stato analizzato il processo **svchost.exe** attraverso le proprietà del file (accessibili tramite il PID identificato con `netstat -abno`).

- **Informazioni ottenute:**
    - **Firme Digitali:** Conferma che il file è firmato da "Microsoft Windows", garantendone l'integrità.
    - **Sicurezza:** Elenco dei permessi per gli utenti (SYSTEM, Administrators, etc.).
    - **Generale:** Percorso del file (`C:\Windows\System32`) e dettagli sulle dimensioni.



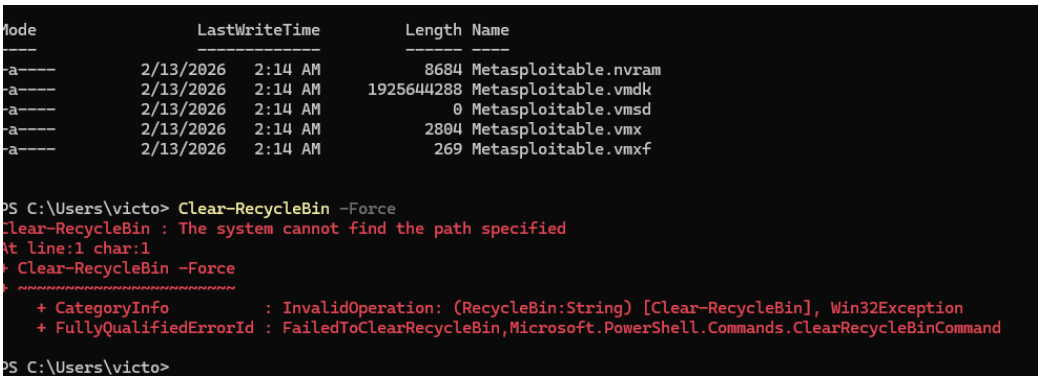




Parte 5: Svuotare il cestino tramite PowerShell

PowerShell permette di semplificare compiti amministrativi complessi con un singolo comando. È stato utilizzato il cmdlet `clear-recyclebin` per eliminare permanentemente i file dal Cestino.

- **Esito**: Nonostante un errore di sistema durante l'esecuzione (dovuto a volumi già vuoti o permessi specifici), l'operazione di pulizia è stata completata



Domanda di Riflessione

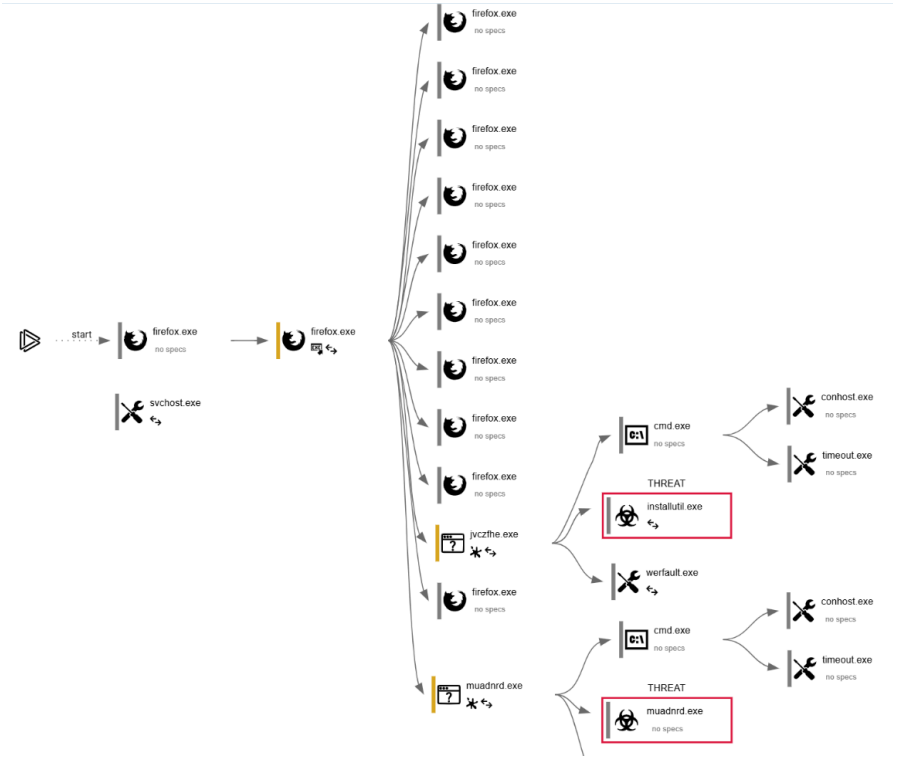
PowerShell è fondamentale per un analista di sicurezza. Comandi come `Get-WinEvent` (per i log) e `Get-FileHash` (per l'integrità dei file) sono strumenti essenziali per il monitoraggio e la risposta agli incidenti.

2 Studio Loc

1. Panoramica del Task

L'analisi riguarda l'esecuzione di un file sospetto all'interno di un ambiente controllato (Sandbox) per identificarne il comportamento malevolo.

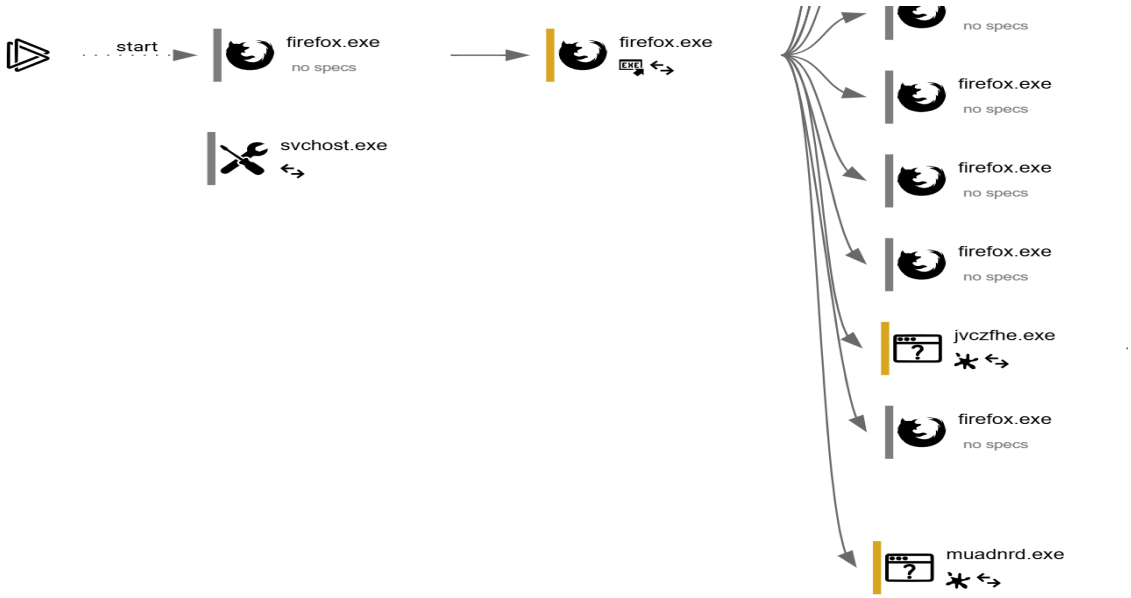
- **ID Analisi**: 9a158718-43fe-45ce-85b3-66203dbc2281.
- **Sistema Operativo**: Windows 10 Professional 64-bit.
- **Verdetto Finale**: Attività Malevola (Malicious Activity).



2. Catena di Infezione (Infection Chain)

Il malware non è stato eseguito direttamente dall'utente, ma è stato scaricato tramite un'applicazione legittima per eludere i controlli di sicurezza iniziali.

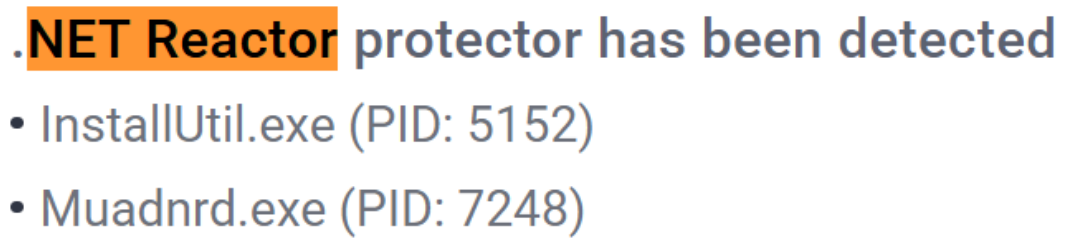
- **Processo Sorgente**: Firefox (PID 6596) è stato utilizzato per avviare la sessione di navigazione verso la risorsa malevola.
- **Vettore di Distribuzione**: Il payload è ospitato su un repository pubblico di GitHub (`https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe`).
- **Payload Identificato**: Il file scaricato ed eseguito è denominato **`Jvczfhe.exe`**.



3. Caratteristiche del Malware

L'analisi statica del file `Jvczfhe.exe` ha evidenziato l'uso di tecniche avanzate per nascondere il codice reale:

- **Offuscamento**: Il file è protetto da **.NET Reactor**, un software di protezione del codice utilizzato dagli attaccanti per impedire l'analisi del codice sorgente e il reverse engineering.
- **Compilazione**: Il binario è un eseguibile sviluppato in ambiente .NET.



4. Indicatori di Compromissione (IOC)

Durante l'esecuzione, sono state registrate attività anomale che confermano l'infezione:

- **Connessioni HTTP**: Il processo ha effettuato numerose richieste verso domini esterni per stabilire comunicazioni di Command & Control o scaricare componenti aggiuntivi.
- **Tattiche ATT&CK**: L'uso di piattaforme fimate (GitHub) per la distribuzione permette di bypassare i firewall che considerano il traffico verso tali domini come sicuro.

Conclusione Tecnica

Il sample analizzato rappresenta un classico esempio di **Loader** che sfrutta servizi cloud legittimi per la distribuzione. L'uso di offuscatori come .NET Reactor indica un tentativo deliberato di evadere le firme degli antivirus tradizionali, rendendo necessaria l'analisi dinamica (Sandbox) eseguita in questo task.

Conclusione Finale

L’utilizzo di PowerShell per il monitoraggio dell'integrità del sistema, integrato all'analisi in sandbox per smascherare malware offuscati che sfruttano servizi cloud legittimi, rappresenta una strategia di difesa completa ed essenziale contro le minacce moderne.