

Esercizio 1 Usare Windows PowerShell

Parte 2 Esplorare i comandi del Prompt dei Comandi e di PowerShell

- Inserisci dir al prompt in entrambe le finestre. **Quali sono gli output del comando dir?**
Gli output del comando dir nelle finestre di powershell e prompt dei comandi mostrano i file e le directory nell'unità C.

- Prova un altro comando che hai usato nel prompt dei comandi, come ping, cd e ipconfig. **Quali sono i risultati?**

Il comando ping mostra la connettibilità di rete tra il computer e un altro host su una rete IP.

La funzione del comando cd è di cambiare la directory corrente.

Il comando ipconfig mostra le configurazioni di rete del sistema e delle schede di rete.

Parte 3 Esplorare i cmdlet

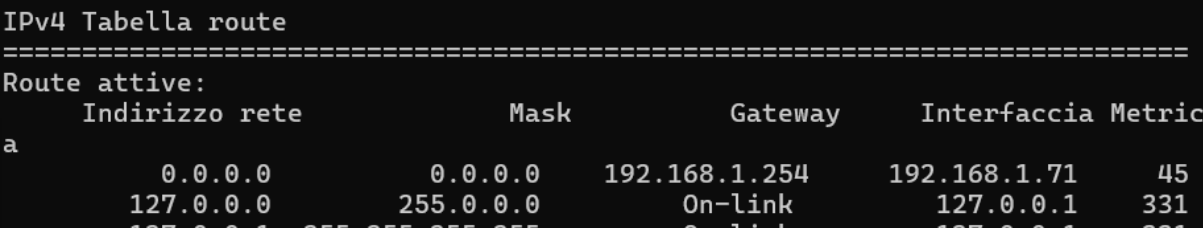
- Per identificare il comando PowerShell per elencare le sottodirectory e i file in una directory, inserisci Get-ChildItem al prompt di PowerShell. **Qual è il comando PowerShell per dir?**

Il comando PowerShell per dir è Get-ChildItem.

Parte 4 Esplorare il comando netstat usando PowerShell

- Per visualizzare la tabella di routing con le rotte attive, inserisci netstat -r al prompt. **Qual è il gateway IPv4?**

Il gateway IPv4 è 192.168.1.254 .



IPv4 Tabella route					
=====					
Route attive:					
	Indirizzo rete	Mask	Gateway	Interfaccia	Metrica
a	0.0.0.0	0.0.0.0	192.168.1.254	192.168.1.71	45
	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

- Individua il PID selezionato in Gestione Attività. Fai clic con il pulsante destro sul PID selezionato in Gestione Attività per aprire la finestra di dialogo Proprietà (Properties) per maggiori informazioni. **Quali informazioni puoi ottenere dalla scheda Dettagli e dalla finestra di dialogo Proprietà per il PID selezionato?**

Nella scheda Dettagli di Gestione Attività si ottengono informazioni sull'esecuzione in tempo reale del processo, mentre dalla finestra Proprietà del file eseguibile associato al PID si ottengono informazioni statiche e di configurazione relative al file stesso.

Parte 5 Svuotare il cestino usando PowerShell

- In una console PowerShell, inserisci `clear-recyclebin` al prompt. **Cosa è successo ai file nel Cestino?**

Eseguendo il comando `clear-recyclebin` in PowerShell i file nel cestino sono stati eliminati definitivamente.

Domanda di Riflessione

- PowerShell è stato sviluppato per l'automazione delle attività e la gestione della configurazione. Usando internet, ricerca comandi che potresti usare per semplificare i tuoi compiti come analista di sicurezza. Registra le tue scoperte.

Resolve-DnsName: esegue query DNS per risolvere nomi host in indirizzi IP e viceversa.

Utile per l'analisi di domini sospetti o per verificare la configurazione DNS.

Stop-Process -Name "nomeprocesso" / Stop-Process -Id PID: per terminare processi malevoli identificati.

Get-WinEvent -LogName Security -MaxEvents 100: per recuperare gli ultimi 100 eventi dal log di sicurezza.

Export-WinEvent: per esportare i log degli eventi in un file per un'analisi offline.

Get-ScheduledTask: Elenca le task programmate sul sistema. Il malware spesso usa task programmate per la persistenza.

Get-WmiObject Win32_Service: per ottenere dettagli più granulari sui servizi, incluso il percorso del binario e l'account con cui viene eseguito.

Esercizio 2: Studio loc

- Studiare questo link di anyrun e spiegare queste minacce in un piccolo report.
<https://app.any.run/tasks/9a15871843fe-45ce-85b366203dbc2281/>

Questo mostra un'analisi dinamica che analizza attività sospette dove firefox ha scaricato un file eseguibile direttamente da un repository GitHub non ufficiale, forte indicatore di un tentativo di consegna di un malware che sta scaricando ulteriori componenti e comunicando con domini esterni associati a servizi DNS dinamici. Queste attività indicano che il sistema analizzato è stato esposto a un software malevolo che tenta di stabilire persistenza, scaricare componenti aggiuntivi e comunicare con un'infrastruttura di Comando e Controllo per ricevere istruzioni o prendere dati.

In conclusione l'analisi rivela un'attività altamente sospetta e potenzialmente malevola. Il campione analizzato sembra essere un downloader o un componente di malware che scarica ulteriori payload da piattaforme legittime come GitHub per eludere il rilevamento e tenti di stabilire comunicazioni con un server di comando e controllo utilizzando servizi DNS dinamici, una tattica comune per la resilienza delle infrastrutture malevole.

Considerando che il malware si maschera da software legittimo per ingannare gli utenti e farsi installare potrebbe essere un trojan. Una volta all'interno, può avere diverse funzionalità malevole. Infatti i file scaricati da GitHub sono chiaramente dei Trojan Downloader, ovvero Trojan che servono a scaricare altro malware. Il "Trojan" è una macro-categoria che descrive il metodo di ingresso (inganno), mentre le funzionalità specifiche possono essere quelle di spyware, backdoor, ransomware, ecc. Spesso, i malware moderni sono di tipo

multi-funzionale, combinando caratteristiche di più categorie (ad esempio, un botnet può anche esfiltrare dati, agendo come spyware, o può essere aggiornato per diventare un cryptominer o lanciare ransomware). La presenza di C2 è un segno chiave di un controllo esterno sul sistema compromesso.

Raccomandazioni:

1. Isolamento: qualsiasi sistema su cui è stata osservata questa attività dovrebbe essere immediatamente isolato dalla rete per prevenire ulteriori compromissioni o la diffusione del malware.
2. Analisi Forense: effettuare un'analisi forense approfondita del sistema compromesso per identificare l'ambito dell'infezione, i dati esfiltrati e la presenza di altri malware.
3. Blocco Indicatori di Compromissione (IoC): bloccare a livello perimetrale i domini per prevenire ulteriori comunicazioni o infezioni.
4. Analisi del Payload: se possibile, recuperare e analizzare staticamente e dinamicamente il file per comprendere appieno le sue funzionalità malevole.
5. Sensibilizzazione Utenti: informare gli utenti sui rischi di cliccare su link sospetti o scaricare file da fonti non verificate, anche se apparentemente legittime.