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.

Comandi PowerShell utili per analisti di sicurezza

Comandi per la ricognizione e diagnostica di rete

- **`Get-NetIPConfiguration`** – Mostra dettagli sulla configurazione di rete, inclusi gli indirizzi IP e i server DNS. Utile per verificare configurazioni sospette o inconsistenze di rete.

- **`Test-NetConnection`** – Esegue test diagnostici su una destinazione (DNS, ping, porte aperte, ecc.). Ideale per verificare connettività o possibili porte vulnerabili.

Comandi per monitoraggio e analisi attività di sistema

- **`Get-Process`** – Elenca i processi in esecuzione; può essere filtrato per CPU o memoria per individuare attività sospette.

- **`Get-NetTCPConnection`** – Mostra connessioni TCP attive; utile per identificare traffico non autorizzato o connessioni persistenti.

Comandi per log ed eventi di sicurezza

- **`Get-EventLog`** – Accede ai log di sistema o sicurezza; fondamentale per investigare accessi falliti o eventi sospetti.

- **`Get-WinEvent`** – Permette un’analisi più avanzata dei log, filtrando per ID eventi come quelli relativi alla creazione di processi (per esempio 4688).

Comandi per controllo utenti e permessi

- **`Add-LocalGroupMember`** / **`Remove-LocalGroupMember`** – Modifica l’appartenenza degli utenti ai gruppi locali, ad esempio per revocare privilegi amministrativi.

- **`Get-Acl`** / **`Set-Acl`** – Visualizza o imposta permessi di file e directory per assicurare che non ci siano accessi inappropriati ai dati.

Comandi specifici per sicurezza del sistema e antivirus

- **`Get-MpComputerStatus`** – Mostra lo stato e le impostazioni di Microsoft Defender Antivirus su un endpoint.

- **`Start-MpScan`** – Avvia una scansione antivirus con varie opzioni (rapida, completa, personalizzata).

- **`Update-MpSignature`** – Aggiorna le definizioni di sicurezza usate dall’antivirus.

Comandi di automazione e best practice

- **`Get-Help`** – Mostra informazioni sui comandi (utile per documentarsi su cmdlet specifici).

- **`Set-ExecutionPolicy`** – Controlla le politiche di esecuzione degli script per mitigare rischi di script non autorizzati.

- **Remoting e automazione remota** – Permette l’esecuzione di script su più sistemi contemporaneamente (*es. PowerShell Remoting*).