Comandi di PowerShell per gli Analisti della Sicurezza

Come analista della sicurezza, PowerShell può essere uno strumento potente per automatizzare attività, investigare incidenti e raccogliere informazioni. Ecco alcune categorie di comandi ed esempi specifici che possono semplificare il tuo lavoro:

1. Raccolta di Informazioni di Sistema:

- `Get-ComputerInfo`: Recupera informazioni complete sul computer locale o remoto, inclusi dettagli del sistema operativo, configurazione hardware e software installato. Questo può essere utile per l'inventario degli asset e l'identificazione di potenziali vulnerabilità.
- `Get-WmiObject -Class Win32_OperatingSystem`: Fornisce informazioni dettagliate sul sistema operativo, come versione, numero di build e data di installazione.
- `Get-Service`: Elenca tutti i servizi in esecuzione sul sistema, insieme al loro stato (Running, Stopped), modalità di avvio e nome del servizio. Utile per identificare servizi insoliti o dannosi.
- `Get-Process`: Visualizza un elenco di tutti i processi in esecuzione, inclusi l'ID del processo (PID), l'utilizzo della CPU e il consumo di memoria. Utile per identificare processi sospetti o che consumano molte risorse.
- `Get-EventLog -LogName System -EntryType Error, Warning`: Recupera gli eventi di errore e avviso dal registro eventi di sistema, che possono indicare problemi di sistema o potenziali incidenti di sicurezza. Puoi specificare diversi nomi di registro (ad esempio, "Application", "Security") e tipi di voce.

2. Analisi di Rete:

- `Get-NetIPConfiguration`: Visualizza la configurazione di rete del sistema, inclusi indirizzi IP, subnet mask, gateway predefiniti e server DNS.
- `Get-NetTCPConnection`: Mostra le connessioni TCP attive, inclusi indirizzi locali e remoti, porte e stato della connessione. Utile per identificare connessioni di rete sospette.
- `Get-NetUDPEndpoint`: Visualizza i listener e le connessioni UDP attivi.
- `Test-NetConnection -ComputerName <Destinazione> -Port <Porta>`: Verifica la connettività di rete a un host e una porta specifici. Utile per verificare le regole del firewall e controllare se i servizi sono in ascolto.
- `Resolve-DnsName <NomeHost>`: Esegue ricerche DNS per risolvere i nomi host in indirizzi IP.

3. Analisi di File e Registro:

- `Get-ChildItem <Percorso>`: Elenca file e directory in un percorso specificato. Utile per esaminare l'attività del file system e identificare file sospetti. Puoi utilizzare parametri come `-Recurse`, `-Filter` e `-Attributes`.
- `Get-FileHash <Percorso> -Algorithm SHA256`: Calcola il valore hash di un file utilizzando un algoritmo specificato (ad esempio, SHA256, MD5). Utile per verificare l'integrità dei file e identificare file dannosi conosciuti.
- `Get-ItemProperty -Path <PercorsoRegistro>`: Recupera proprietà e valori da una chiave di registro specificata. Utile per esaminare la configurazione del sistema e identificare potenziali meccanismi di persistenza di malware.
- `Get-Acl <Percorso>`: Ottiene l'elenco di controllo degli accessi (ACL) per un file o una directory, mostrando le autorizzazioni per diversi utenti e gruppi. Utile per identificare potenziali problemi di autorizzazione.

4. Configurazione di Sicurezza e Audit:

- `Get-ExecutionPolicy`: Visualizza l'attuale policy di esecuzione degli script di PowerShell, che controlla se gli script possono essere eseguiti.
- `Get-LocalUser`: Elenca gli account utente locali sul sistema.
- `Get-LocalGroupMember -GroupName "Administrators"`: Elenca i membri del gruppo Administrators locale.
- `Get-WindowsFeature`: Elenca le funzionalità di Windows installate e disponibili.
- `Get-HotFix`: Visualizza un elenco degli aggiornamenti e degli hotfix installati.

5. Automazione e Scripting:

- La forza di PowerShell risiede nelle sue capacità di scripting. Puoi combinare questi cmdlet e la logica per automatizzare attività di sicurezza ripetitive come:

    - Raccolta e analisi dei log
    - Controlli dello stato del sistema
    - Audit degli account utente
    - Risposta automatizzata a determinati eventi di sicurezza
    - Script di threat hunting (caccia alle minacce)