Comandi PowerShell

Verifica delle Politiche di Esecuzione

PowerShell ha delle restrizioni sui tipi di script che possono essere eseguiti.

```
Get-ExecutionPolicy
```

Impostare una politica più restrittiva:

```
Set-ExecutionPolicy Restricted
```

Impedisce l'esecuzione di qualsiasi script PowerShell, utile per aumentare la sicurezza.

Consentire solo script firmati:

```
Set-ExecutionPolicy AllSigned
```

Controllo delle Connessioni di Rete

Visualizzare le connessioni attive:

```
Get-NetTCPConnection
```

Elencare i processi che utilizzano la rete:

```
Get-NetTCPConnection | Select-Object LocalAddress, LocalPort, RemoteAddress,
RemotePort, State, Ownin
```

Bloccare un IP sospetto tramite il firewall:

```
New-NetFirewallRule -DisplayName "Blocca IP sospetto" -Direction Inbound -Action
Block -RemoteAd
```

Monitoraggio dei Processi e Attività Sospette

Elencare i processi attivi:

```
Get-Process
```

Terminare un processo sospetto (sostituisci ID con il numero del processo):

```
Stop-Process -Id 1234 -Force
```

Controllo degli Eventi di Sicurezza

Analizzare i tentativi di accesso falliti:

```
Get-EventLog -LogName Security -InstanceId 4625 -Newest 10
```

Monitorare i cambiamenti nei privilegi utente:

```
Get-EventLog -LogName Security -InstanceId 4672 -Newest 10
```

Rilevamento di Malware Fileless

Controllare script sospetti in memoria:

```
Get-WmiObject Win32_Process | Where-Object { $_.CommandLine -like "bypass" }
```

Analizzare il registro alla ricerca di malware fileless:

```
Get-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run”
```

Controllo degli Account e dei Permessi

Elencare gli utenti locali:

```
Get-LocalUser
```

Controllare i membri del gruppo Administratori:

```
📝 Get-LocalGroupMember -Group "Administrators”
```

Disabilitare un utente sospetto:

```
📝 Disable-LocalUser -Name "utente_malevolo”
```