EVIL COMMANDS WINS

Obtener direcciones IP y configuración de red

```
ipconfig /all
```

Escaneo de archivos en windows (Búsqueda de credenciales):

```
findstr /SIM /C:"password" *.txt *.ini *.cfg *.config *.xml *.git *.ps1 *.yml
```

Escaneo de equipos en red que tienen conexion al PC:

```
for /L %a in (1,1,254) do @start /b ping 10.51.125.%a -w 100 -n 2 >nul
arp -a
```

Obtención de usuarios del sistema:

```
net user
```

Obtener información del sistema (detalles del equipo y el sistema operativo)

```
systeminfo
```

Comprobar políticas de seguridad de cuentas de usuario

```
net accounts
```

Listar procesos activos y servicios en ejecución

```
tasklist
```

Listar los servicios en ejecución

```
net start
```

Ver historial de conexiones RDP (Remote Desktop Protocol)

```
query user
```

Ver las redes Wi-Fi guardadas y sus contraseñas

```
netsh wlan show profile
```

```
netsh wlan show profile name="nombre_de_red" key=clear
```

Buscar credenciales en el Administrador de Credenciales (No muestra credenciales)

```
cmdkey /list
```