



OWASP

Open Web Application  
Security Project

# Windows-PrivEsc Audit Scripts

PowerUp PrivescCheck WindowsEnum

# whoami

Calvin Hansch

=====

Red Team Operator & Penetration Tester

BSc Applied Computer Science

working in IT since 2014

# Vectors checked

Script	PowerUp	PrivescCheck	WindowsEnum
=====	=====	=====	=====
AlwaysInstallElevated	X	✓	X
Ghost DLL-Injection	X	✓	X
DLL-Searchorder Hijacking	✓	X	X
User Privileges	X	✓	✓
Accessible SAM files (HiveNightmare aka. SeriousSAM)	X	✓	✓
Cached Credentials in Flat Files	✓	✓	✓
Modifiable Service Binaries	✓	✓	✓
Unquoted Service Path	✓	✓	✓

# PRACTICAL DEMONSTRATION

# THE TAKE AWAY

# Resources

- PowerUp:  
<https://github.com/PowerShellMafia/PowerSploit/blob/master/Privesc/PowerUp.ps1>
- PrivescCheck:  
<https://github.com/itm4n/PrivescCheck>
- WindowsEnum:  
<https://github.com/absolomb/WindowsEnum>