

# LOCAL PRIVILEGE ESCALATION

The attackers use a misconfiguration or vulnerability in local software to gain administrative access.

## DETECTION

---

Endpoint Analysis

Cyber Deception

Endpoint Security Protection Analysis

## TOOLS

---

Meterpreter Post-Exploitation Scripts

DLLHijackTest

PowerSploit:

- PowerUp

GhostPack:

- SharpUp

<https://github.com/slyd0g/DLLHijackTest>

<https://www.blackhillsinfosec.com/powershell-without-powershell-how-to-bypass-application-whitelisting-environment-restrictions>  
-av



PIVOT and ESCALATE

Created by: **BLACK HILLS** | Information Security