PowerSploit, Software S0194 | MITRE ATT&CK®

Archived: 2026-04-05 14:23:36 UTC

Enterprise T1134 Access Token Manipulation

PowerSploit's `Invoke-TokenManipulation` Exfiltration module can be used to manipulate tokens.[1][3]

Enterprise T1087 .001 Account Discovery: Local Account

PowerSploit's `Get-ProcessTokenGroup` Privesc-PowerUp module can enumerate all SIDs associated with its current token.[1][3]

Enterprise T1123 Audio Capture

PowerSploit's `Get-MicrophoneAudio` Exfiltration module can record system microphone audio.[1][3]

Enterprise T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

PowerSploit's `New-UserPersistenceOption` Persistence argument can be used to establish via the `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` Registry key.[1][3]

.005 Boot or Logon Autostart Execution: Security Support Provider

PowerSploit's `Install-SSP` Persistence module can be used to establish by installing a SSP DLL.[1][3]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

PowerSploit modules are written in and executed via PowerShell.[1][3]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

PowerSploit contains a collection of Privesc-PowerUp modules that can discover and replace/modify service binaries, paths, and configs.[1][3]

Enterprise T1555 .004 Credentials from Password Stores: Windows Credential Manager

PowerSploit contains a collection of Exfiltration modules that can harvest credentials from Windows vault credential objects.[1][3]

Enterprise T1005 Data from Local System

PowerSploit contains a collection of Exfiltration modules that can access data from local files, volumes, and processes.[1][3]

Enterprise T1482 Domain Trust Discovery

PowerSploit has modules such as `Get-NetDomainTrust` and `Get-NetForestTrust` to enumerate domain and forest trusts.[1][3]

Enterprise T1574 .001 Hijack Execution Flow: DLL

PowerSploit contains a collection of Privesc-PowerUp modules that can discover and exploit DLL hijacking opportunities in services and processes.[1][3]

.007 Hijack Execution Flow: Path Interception by PATH Environment Variable

PowerSploit contains a collection of Privesc-PowerUp modules that can discover and exploit path interception opportunities in the PATH environment variable.[1][3]

.008 Hijack Execution Flow: Path Interception by Search Order Hijacking

PowerSploit contains a collection of Privesc-PowerUp modules that can discover and exploit search order hijacking vulnerabilities.[1][3]

.009 Hijack Execution Flow: Path Interception by Unquoted Path

PowerSploit contains a collection of Privesc-PowerUp modules that can discover and exploit unquoted path vulnerabilities.[1][3]

Enterprise T1056 .001 Input Capture: Keylogging

PowerSploit's `Get-Keystrokes` Exfiltration module can log keystrokes.[1][3]

Enterprise T1027 .005 Obfuscated Files or Information: Indicator Removal from Tools

PowerSploit's `Find-AVSignature` AntivirusBypass module can be used to locate single byte anti-virus signatures.[1][3]

.010 Obfuscated Files or Information: Command Obfuscation

PowerSploit contains a collection of ScriptModification modules that compress and encode scripts and payloads.[1][3]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

PowerSploit contains a collection of Exfiltration modules that can harvest credentials using Mimikatz.[1][3]

Enterprise T1057 Process Discovery

PowerSploit's `Get-ProcessTokenPrivilege` Privesc-PowerUp module can enumerate privileges for a given process.[1][3]

Enterprise T1055 .001 Process Injection: Dynamic-link Library Injection

PowerSploit contains a collection of CodeExecution modules that inject code (DLL, shellcode) into a process.[1] [3]

Enterprise T1012 Query Registry

PowerSploit contains a collection of Privesc-PowerUp modules that can query Registry keys for potential opportunities.[1][3]

Enterprise T1620 Reflective Code Loading

PowerSploit reflectively loads a Windows PE file into a process.[1][3]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

PowerSploit's `New-UserPersistenceOption` Persistence argument can be used to establish via a Scheduled Task/Job.[1][3]

Enterprise T1113 Screen Capture

PowerSploit's `Get-TimedScreenshot` Exfiltration module can take screenshots at regular intervals.[1][3]

Enterprise T1558 .003 Steal or Forge Kerberos Tickets: Kerberoasting

PowerSploit's `Invoke-Kerberoast` module can request service tickets and return crackable ticket hashes.[4][5]

Enterprise T1552 .002 Unsecured Credentials: Credentials in Registry

PowerSploit has several modules that search the Windows Registry for stored credentials: `Get-UnattendedInstallFile`, `Get-Webconfig`, `Get-ApplicationHost`, `Get-SiteListPassword`, `Get-CachedGPPPassword`, and `Get-RegistryAutoLogon`.[6]

.006 Unsecured Credentials: Group Policy Preferences

PowerSploit contains a collection of Exfiltration modules that can harvest credentials from Group Policy Preferences.[1][3]

Enterprise T1047 Windows Management Instrumentation

PowerSploit's `Invoke-WmiCommand` CodeExecution module uses WMI to execute and retrieve the output from a PowerShell payload.[1][3]
