

Forum:[Hack Forums](#)

Thread: [./Dark Legion/PowerSploit: The Ultimate Weapon](#)

Dread.Reaper - March 31, 2023, 10:28 am

@Genuine@

PowerSploit: The Ultimate Weapon for Windows-Based Hacking.

Written By: Dread.Reaper - Dark Legion

Introduction:

The world of cybersecurity is constantly evolving, and it is essential to stay up to date with the latest tools and technologies. One such tool that has gained a lot of attention in recent years is the PowerShellMafia PowerSploit software. This open-source tool is designed to help hackers conduct reconnaissance, exploitation, and post-exploitation activities on Windows-based systems. In this essay, we will provide an expanded introduction to PowerSploit and delve into its functionality, installation, configuration, and usage.

PowerSploit is a powerful suite of PowerShell scripts that can be used to perform a range of tasks on Windows-based systems. This software is developed by the PowerShellMafia team, and it is constantly updated to keep up with the changing landscape of cybersecurity. The PowerSploit toolset is designed to provide hackers with a versatile set of tools that can be customized to suit their specific needs.

At its core, PowerSploit is a code execution framework that allows hackers to execute commands on target systems. The software provides a range of modules that can be used to perform various tasks, such as persistence, enumeration, and antivirus evasion. PowerSploit is designed to be flexible and can be adapted to suit the needs of different users.

One of the key features of PowerSploit is its flexibility. The software is written in PowerShell, which means that it can be customized using PowerShell scripts. This allows users to modify the toolset to suit their specific needs, making it a versatile and adaptable tool for cybersecurity professionals.

The PowerSploit toolset has gained a reputation for being a powerful and effective tool for hackers. However, it is important to note that the software can also be used for legitimate purposes, such as penetration testing and vulnerability assessments. When used responsibly, PowerSploit can be a valuable tool for securing Windows-based systems.

Functionality:

Code Execution:

PowerSploit's code execution functionality allows users to execute code on a target system. This feature can be used to perform various tasks, such as launching a reverse shell or executing arbitrary commands on the target system. PowerSploit provides a range of tools to help with code execution, such as Invoke-Shellcode and Invoke-ReflectivePEInjection.

Example:

To execute a PowerShell script on a target system, the following command can be used:

```
Invoke-Command -ScriptBlock {& "C:\path\to\script.ps1"}
```

Persistence:

PowerSploit's persistence functionality allows users to maintain persistence on a target system. This feature can be used to ensure that a hacker's access to the target system is not lost after a reboot or other changes to the system. PowerSploit provides a range of tools to help with persistence, such as Add-UserAutoLogon and Add-UserPermission.

Example:

To create a registry key that will run a script on user login, the following command can be used:

```
New-ItemProperty -Path "HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" -Name
```

"MyScript" -Value "C:\path\to\script.ps1" -PropertyType String -Force

Enumeration:

PowerSploit's enumeration functionality allows users to gather information about a target system. This feature can be used to identify vulnerabilities, locate sensitive data, and gain a better understanding of the target system's configuration. PowerSploit provides a range of tools to help with enumeration, such as Get-NetLocalGroup and Get-NetProcess.

Example:

To retrieve a list of all running processes on a target system, the following command can be used:

Get-Process

Antivirus Evasion:

PowerSploit's antivirus evasion functionality allows users to evade antivirus detection on a target system. This feature can be used to bypass antivirus software that may be installed on the target system and prevent it from detecting the hacker's activities. PowerSploit provides a range of tools to help with antivirus evasion, such as Invoke-Obfuscation and Out-EncryptedScript.

Example:

To obfuscate a PowerShell script to evade antivirus detection, the following command can be used:

Invoke-Obfuscation -ScriptBlock {& "C:\path\to\script.ps1"} -Command All

PowerSploit provides several configuration options that allow users to customize the software's behavior. In this section, we will provide a technical description of each of these configuration options and provide working examples of how they can be used.

ExecutionPolicy:

The ExecutionPolicy configuration option sets the PowerShell execution policy for the current session. The execution policy determines what scripts are allowed to run on the system.

PowerSploit recommends setting the execution policy to RemoteSigned, which allows locally created scripts to run and requires remotely created scripts to be digitally signed.

Example:

To set the execution policy to RemoteSigned, the following command can be used:

Set-ExecutionPolicy RemoteSigned

ScriptBlockLogging:

The ScriptBlockLogging configuration option enables or disables script block logging. Script block logging records the contents of PowerShell commands, including parameters and arguments, in the PowerShell event log. This can be used to track the activities of hackers or to troubleshoot issues with scripts.

Example:

To enable script block logging, the following command can be used:

Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\PowerShell\1\PowerShellEngine" -Name "ScriptBlockLogging" -Value "Enabled"

ModuleLogging:

The ModuleLogging configuration option enables or disables module logging. Module logging records information about the modules that are loaded in the current PowerShell session. This can be used to track the activities of hackers or to troubleshoot issues with scripts.

Example:

To disable module logging, the following command can be used:

Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\PowerShell\1\PowerShellEngine" -Name "ModuleLogging" -Value "Disabled"

Invoke-Expression:

The Invoke-Expression command executes a string as a PowerShell command. This command can be used to execute arbitrary commands on the target system.

Example:

To execute the command "ipconfig /all" on the target system, the following command can be used:

Invoke-Expression "ipconfig /all"

Invoke-Mimikatz:

The Invoke-Mimikatz command executes the Mimikatz tool on the target system. Mimikatz is a tool that can be used to extract plaintext passwords from memory, among other things.

Example:

To execute the Mimikatz tool on the target system, the following command can be used:

Invoke-Mimikatz

Get-NetUser:

The Get-NetUser command retrieves information about users on the target system. This command can be used to gather information about the users on the system, including their usernames, group memberships, and more.

Example:

To retrieve information about all users on the target system, the following command can be used:

Get-NetUser

Get-NetComputer:

The Get-NetComputer command retrieves information about computers on the target system. This command can be used to gather information about the computers on the system, including their names, IP addresses, and more.

Example:

To retrieve information about all computers on the target system, the following command can be used:

Get-NetComputer

Conclusion:

In conclusion, PowerSploit is a powerful tool for hackers and cybersecurity professionals alike. Its range of functionality, flexible configuration options, and versatile commands make it a must-have tool for any hacker looking to perform reconnaissance, exploitation, and post-exploitation activities on Windows-based systems.

From a hacker's perspective, PowerSploit's functionality is a game-changer. The toolset provides a range of modules that can be used to perform various tasks, including code execution, persistence, enumeration, and antivirus evasion. Each of these features is accompanied by a range of tools that can be customized to suit the specific needs of the user. PowerSploit's code execution feature allows hackers to execute arbitrary code on the target system, providing them with the access and control they need to achieve their goals. The persistence feature ensures that access to the target system is maintained, even after a reboot or other changes to the system. The enumeration feature allows hackers to gather information about the target system, identifying vulnerabilities, locating sensitive data, and gaining a better understanding of the target system's configuration. Finally, the antivirus evasion feature allows hackers to evade antivirus software installed on the target system, preventing detection of their activities.

From a technical perspective, PowerSploit's configuration options are equally impressive. The ExecutionPolicy option sets the PowerShell execution policy for the current session, allowing users to determine what scripts are allowed to run on the system. The ScriptBlockLogging option enables or disables script block logging, recording the contents of PowerShell commands in the PowerShell event log. The ModuleLogging option enables or disables module logging, recording information about the modules that are loaded in the current PowerShell session. These configuration options allow users to customize the behavior of PowerSploit to suit their specific needs.

PowerSploit's usage is equally impressive. The Invoke-Expression command executes a string as a PowerShell command, allowing users to execute arbitrary commands on the target system. The Invoke-Mimikatz command executes the Mimikatz tool on the target system, providing hackers with a powerful tool for extracting plaintext passwords from memory. The Get-NetUser command retrieves information about users on the target system, allowing hackers to gather information about the users on the system, including their usernames, group memberships, and more. The Get-NetComputer command retrieves information about computers on the target system, allowing hackers to gather information about the computers on the system, including their names, IP

addresses, and more.

In conclusion, PowerSploit is a valuable tool for hackers and cybersecurity professionals alike. Its range of functionality, flexible configuration options, and versatile commands make it an essential tool for performing reconnaissance, exploitation, and post-exploitation activities on Windows-based systems. With its powerful features and customization options, PowerSploit is a must-have tool for any hacker looking to gain access and control over Windows-based systems.

EOF