Manspider — инструмент для поиска файлов по SMB шарам

spy-soft.net/manspider-search-files-smb

30 сентября 2024 г.

Manspider — этот инструмент позволяет сканировать SMB-ресурсы для поиска файлов, содержащих чувствительную информацию. Он поддерживает поиск по содержимому файлов, используя регулярные выражения, что делает его отличным средством для сбора информации.

Еще по теме: Перечисление SMB ресурсов локальной сети

Установка Manspider через Docker

После обновления от 15 октября 2023 года установка Manspider через **pip** может вызвать проблемы из-за прекращения обновления библиотеки **textract**.

Рекомендуемый способ установки Manspider — через Docker:

```
1  docker run --rm -v ./manspider:/root/.manspider blacklanternsecurity/manspider --help
```

Для удобства запуска также доступен скрипт manspider.sh, который автоматически монтирует директории для хранения найденных файлов с конфиденциальной информацией и логов:

```
1  ./manspider.sh --help
```

Поддерживаемые форматы файлов:

- PDF
- DOCX
- XLSX
- PPTX
- Текстовые форматы и другие.

Manspider проверяет каждый ресурс на каждом целевом устройстве. Если указанные учетные данные не работают, он пытается подключиться как гость или через пустую сессию.

Для расширения функционала Manspider можно установить дополнительные зависимости:

Для обработки изображений (png, jpeg):

```
sudo apt install tesseract-ocr
```

Для работы с устаревшими форматами документов (.doc):

```
sudo apt install antiword
```

Установка Manspider через pipx:

```
pip install pipx pipx install git+https://github.com/blacklanternsecurity/MANSPIDER
```

Примеры использования Manspider

Поиск файлов по ключевым словам, связанным с учетными данными:

```
manspider 192.168.0.0/24 -f passw user admin account network login logon cred -d evilcorp -u bob -p Passw0rd
```

Поиск таблиц с паролями в названии файлов:

```
manspider share.evilcorp.local -f passw -e xlsx csv -d evilcorp -u bob -p Passw0rd
```

> Можно запустить несколько Manspider одновременно. Это удобно, если один экземпляр уже работает, и вы хотите искать в загруженных файлах. Для этого укажите ключевое слово loot как цель (manspider loot).

Поиск документов, содержащих пароли:

```
1 manspider share.evilcorp.local -c passw -e xlsx csv docx pdf -d evilcorp -u bob -p Passw0rd
```

Поиск файлов с интересными расширениями:

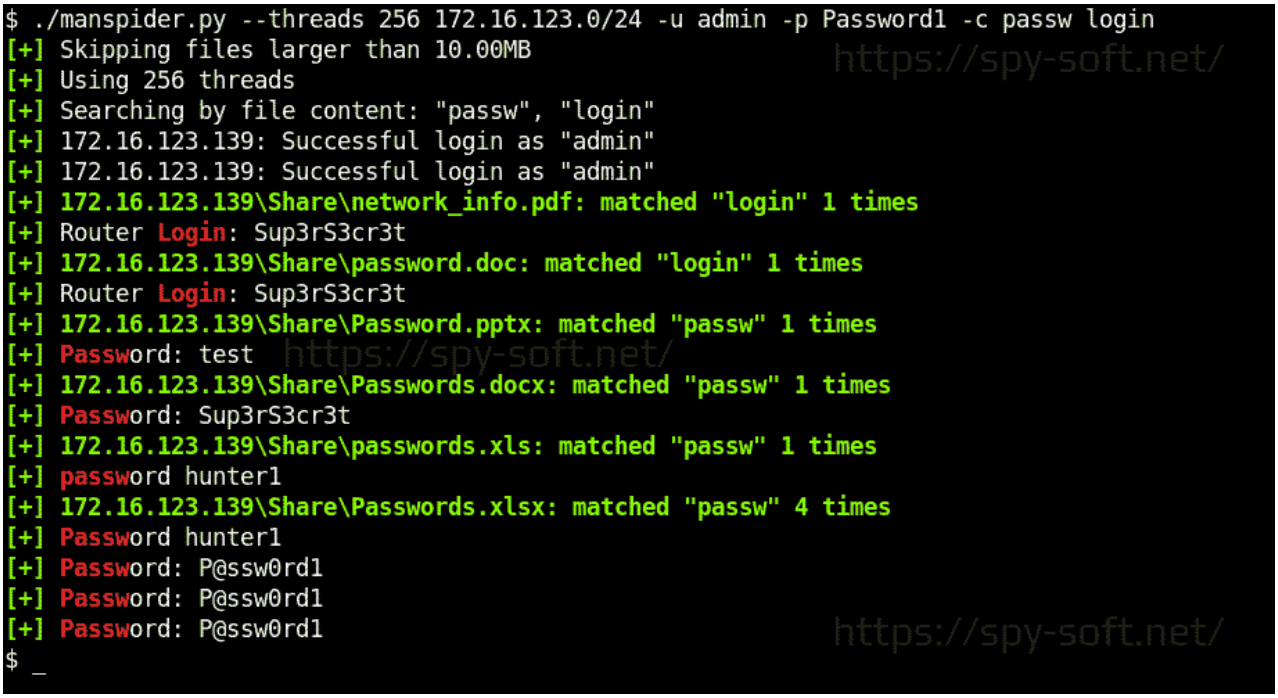
```
1 manspider share.evilcorp.local -e bat com vbs ps1 psd1 psm1 pem key rsa pub reg pfx cfg conf config vmdk vhd vdi dit -d evilcorp -u bob -p Passw0rd
```

Поиск файлов, связанных с финансами:

```
1 manspider share.evilcorp.local --dirnames bank financ payable payment reconcil remit voucher vendor eft swift -f '[0-9]{5,}' -d evilcorp -u bob -p Passw0rd
```

Поиск SSH-ключей по имени файла:

```
1 manspider share.evilcorp.local -e ppk rsa pem ssh rsa -o -f id_rsa id_dsa id_ed25519 -d evilcorp -u bob -p Passw0rd
```



Поиск файлов по SMB шарам используя Manspider

Поиск SSH-ключей по содержимому:

```
1 manspider share.evilcorp.local -e '' -c 'BEGIN .{1,10} PRIVATE KEY' -d evilcorp -u bob -p Passw0rd
```

Поиск файлов менеджеров паролей:

```
1 manspider share.evilcorp.local -e kdbx kdb 1pif agilekeychain opvault lpd dashlane psafe3 enpass bwdb msecure stickypass pwm rdb safe zps pmvault mywallet jpass pwmdb -d evilcorp -u bob -p Passw0rd
```

Поиск сертификатов:

```
1 manspider share.evilcorp.local -e pfx p12 pkcs12 pem key crt cer csr jks keystore key keys der -d evilcorp -u bob -p Passw0rd
```

Рекомендации

Тулза использует разумные значения по умолчанию для предотвращения длительной работы на одном ресурсе. Все эти параметры можно переопределить:

- Глубина по умолчанию: 10 (можно изменить с помощью -m)
- Максимальный размер файла: 10 МБ (можно изменить с помощью -s)
- Потоки по умолчанию: 5 (можно изменить с помощью -t)
- Исключенные ресурсы: C$, IPC$, ADMIN$, PRINT$ (можно изменить с помощью --exclude-sharenames)

Инструмент поддерживает различные типы целей:

- IP-адреса
- Имена хостов
- Подсети (формат CIDR)
- Файлы, содержащие цели
- Локальные папки с файлами

Пример указания нескольких целей одновременно:

```
1 manspider 192.168.1.250 share.evilcorp.local 192.168.1.0/24 smb_hosts.txt loot /mnt/share
```

Manspider — это полезный инструмент для поиска конфиденциальной информации на SMB-ресурсах. С помощью правильных фильтров и регулярных выражений можно эффективно находить важные файлы, что делает его незаменимым для тех, кто занимается информационной безопасностью и сисадминов.

ПОЛЕЗНЫЕ ССЫЛКИ: