Smbtakeover — захват порта 445 TCP на Windows при атаке NTLM Relay

spy-soft.net/smbtakeover

11 октября 2024 г.

Сегодня расскажу о технике Smbtakeover, которая позволяет освободить и снова привязать порт 445 TCP на Windows, не прибегая к загрузке драйвера, модуля в LSASS или перезагрузке целевой машины.

Еще по теме: Manspider — поиск файлов по SMB шарам

Захват порта 445 TCP на Windows

Эта техника значительно облегчает эксплуатацию NTLM relay через SMB, особенно в условиях работы с C2 (сервер для управления скомпрометированными устройствами). Технические детали были рассмотрены на презентации «Relay Your Heart Away: An OPSEC Concious Approach to 445 Takeover» на конференции x33fcon.

Перед применением техники следует учесть несколько моментов:

- Отключение служб, описанных ниже, временно лишает целевую машину возможности использовать namedpipes и серверную часть SMB-коммуникаций (например, CIFS). Важно понимать, для чего используется целевая машина, особенно если это критическая или производственная инфраструктура. После повторного включения службы их нормальная работа восстанавливается.
- Иногда может потребоваться отключить и другой набор служб. Это замечено на некоторых версиях Windows Server, а также при наличии установленных сторонних сетевых драйверов. Однако это не мешает использованию данной техники. Можно проследить зависимости служб от **srvnet** и при необходимости отключить дополнительные службы.

- Этот PoC не обязателен для эксплуатации данной техники! Вы можете использовать любое удобное средство для взаимодействия с диспетчером управления службами (Service Control Manager, SCM).
    Убедитесь, что выбранный инструмент использует **ncacn_ip_tcp** для транспорта RPC. Если он использует **ncacn_np** (named pipes), вы не сможете удаленно включить или отключить службы.

PoC написан на Python и в формате BOF (Beacon Object Files). Оба PoC используют RPC через TCP (ncacn_ip_tcp) в качестве транспорта при взаимодействии с удаленными машинами.

Для настройки Python-версии вам потребуется создать виртуальное окружение и установить пакет impacket:

```
1  git clone https://github.com/zyn3rgy/smbtakeover.git
2  cd smbtakeover
3  python3 -m virtualenv venv
4  source venv/bin/activate
5  python3 -m pip install impacket
6  python3 smbtakeover.py -h
```

Примеры использования Smbtakeover

Python:

```
1  python3 smbtakeover.py atlas.lab/josh:password1@10.0.0.21 check
2  python3 smbtakeover.py atlas.lab/josh:password1@10.0.0.21 stop
3  python3 smbtakeover.py atlas.lab/josh:password1@10.0.0.21 start
```

BOF:

```
1  bof_smbtakeover localhost check
2  bof_smbtakeover 10.0.0.21 stop
3  bof_smbtakeover localhost start
```

Эти команды позволяют проверять статус, останавливать и запускать необходимые службы на целевых машинах, как локально, так и удаленно.

- Атака SMB Relay и как от этого защититься
- Эксплуатация уязвимости CVE-2022-27228 и атака NTLM Relay