Пример атак Kerberoasting и AS-REP Roasting

spy-soft.net/kerberoasting-example-as-rep-roasting

2 апреля 2024 г.

В этой небольшой статье, в рамках прохождения уязвимой виртуальной машины Rebound с площадки Hack The Box, я продемонстрирую пример атаки Kerberoasting.

Еще по теме: Kerbrute для атаки на Active Directory

Итак, мы получили список пользователей и можем поспреить самые популярные пароли и проверив AS-REP Roasting.

Пример атаки AS-REP Roasting

Смысл атаки AS-REP Roasting в том, что атакующий отправляет на сервер аутентификации анонимный запрос для предоставления целевому пользователю доступа к какой-либо услуге. На что сервер имеет 3 разных ответа:

- предоставляет билет, откуда мы возьмем хэш;
- отвечает, что у этого пользователя не выставлен флаг PreauthNotRequired;
- говорит, что такого пользователя не существует в базе Kerberos.

Сделать это можно с помощью все того же CrackMapExec.

```
1  crackmapexec ldap rebound.htb -u users.txt -p '' --asreproast asreproast_hashes.txt
```

Результат проведения атаки AS-REP Roasting

Итак, в домене есть один пользователь, для которого не требуется предварительная аутентификации Kerberos, и мы получаем хеш его пароля. Для брута пароля в hashcat указываем режим **18200** (параметр -m) используя при этом словарь rockyou.txt.

```
1 hashcat -m 18200 asreproast_hashes.txt rockyou.txt
```

Перебор хеша с использование hashcat никаких результатов не дал.

Пример атаки Kerberoasting

Реализация протокола Kerberos в Windows использует имена участников службы (SPN) для определения того, какую учетную запись задействовать для шифрования билета службы. В Active Directory существует два варианта SPN: SPN на основе хоста и произвольные SPN. Первый вариант SPN связан с учетной записью компьютера домена, а второй обычно (но не всегда) — с учеткой пользователя домена (см. также Атака Kerberoasting).

Проще говоря, если запрошен билет, он шифруется паролем учетной записи, SPN которая его предоставила. Так, если мы получим билет, мы можем его просто пробрутить, чтобы получить пароль учетки! Хотя для этого и нужно пройти аутентификацию, но мы можем взять пользователя с прошлого этапа, для которого она не требуется. В этом варианте выполнить атаку можно с помощью Rubeus, для чего перейдем в виртуалку с Windows.

```
1 Rubeus.exe kerberoast /nopreauth:jjones /domain:rebound.htb /dc:10.10.11.231
  /spns:users.txt /ldaps /nowrap
```

Результат выполнения атаки Kerberoasting

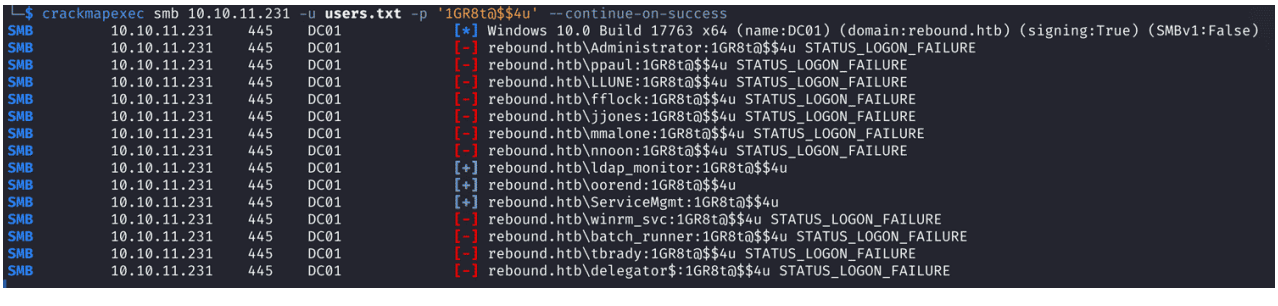
Получаем хеши пользователей ldap_monitor и delegator$, которые сразу отправляем на брут в hashcat.

```
1  hashcat -m 13100 kerberoasting_users.txt rockyou.txt
```

Результат взлома хешей

Получаем пароль для учетки ldap_monitor. Наш единственный пароль спреим по остальным учеткам и получаем еще одну валидную пару из логина и пароля — для пользователя oorend.

```
1  crackmapexec smb 10.10.11.231 -u users.txt -p '1GR8t@$$4u' --continue-on-
   success
```



Результат спрея пароля

Теперь перейдем к сбору данные для BloodHound.

ПОЛЕЗНЫЕ ССЫЛКИ:

- Создание стенда для атак на Active Directory
- Уклонение от Honeytoken при атаке Active Directory