Scénario 2 - Epreuve E4

Déploiement de certificats HTTPS

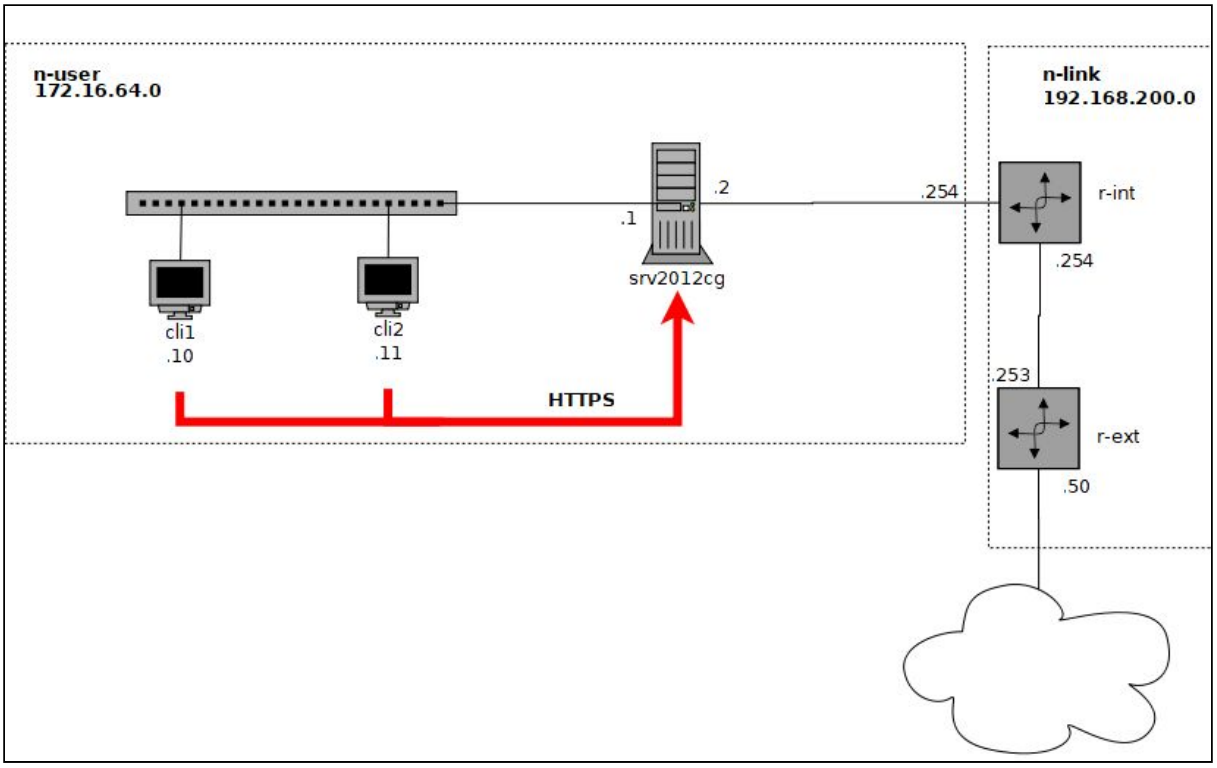
Objectif

Déployer des certificats HTTPS auto-signés sur des machines clientes Windows 7 par le biais de GPO (avec Windows Server 2012) dans un objectif de sécurisation d'un serveur web.

Choix effectués

- **Windows Server 2012 :** Gère les utilisateurs et leurs sessions, et déploie leurs certificats
- **IIS :** Serveur web Microsoft. Beaucoup plus simple à gérer sur un serveur Windows, car il est compatible avec celui-ci et configurable par interface graphique. L'utilisation d'un serveur web orienté Linux aurait pu générer davantage d'erreurs de configuration à corriger.
- **OpenVAS** : référence, de nombreux tests pour s'assurer que le système est suffisamment sécurisé.
- **Pare-feu Windows** : solution de référence sur Windows pour mettre en place de façon simplifiée un pare-feu. Les autres solutions sont plus compliqués à mettre en oeuvre.

Infrastructure à mettre en place

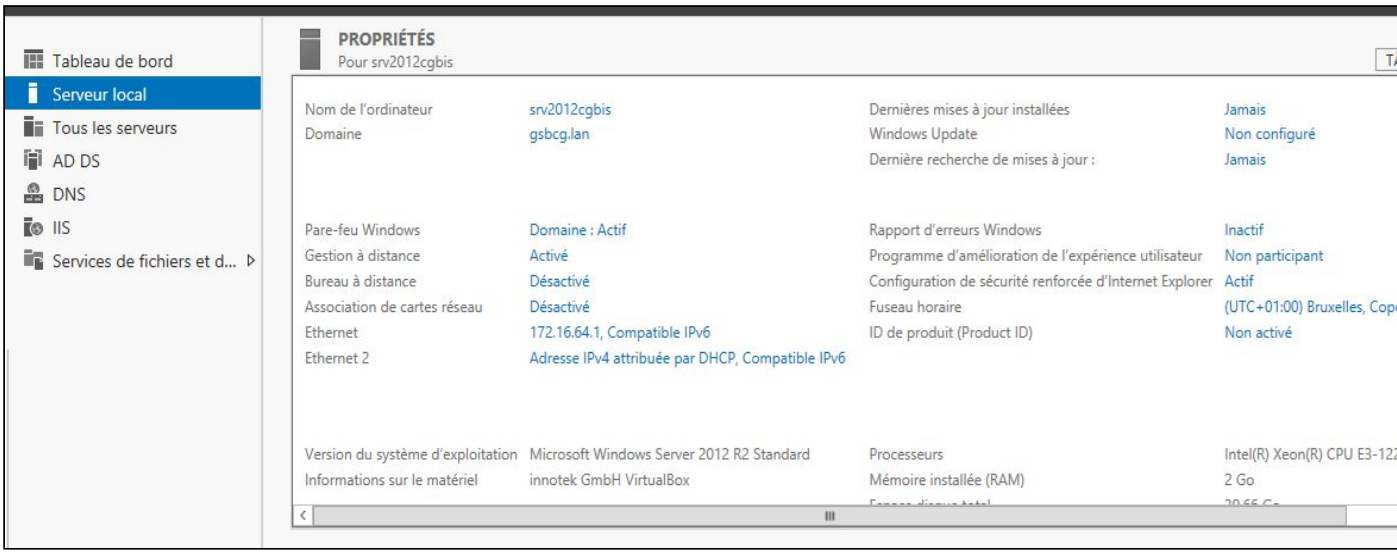


- srv2012cg : 3 cartes
  - pont
  - n-proxy : 172.16.64.2
  - n-user : 172.16.64.1

Tâches à effectuer

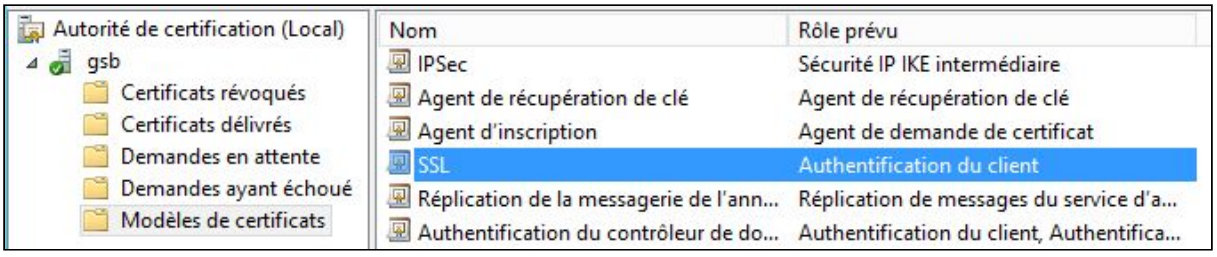
Mise en place des certificats auto-signés

- Installation du Windows Server 2012
  - Installation et configuration des différentes rôles : IIS, DHCP, DNS, AD DS (domaine), | AD CS (certificats Active Directory) (à faire après avoir promu le serveur en contrôleur de domaine)
  - Installation d'une machine cliente que l'on fait entrer dans le domaine et lui ajouter l'adresse du serveur (172.16.64.1)
  - Désactiver le mode protégé d'Internet Explorer via le gestionnaire de serveurs
  - Ajouter une étendue DHCP
  - Créer un utilisateur



- Création des certificats
    - Lors de la configuration de AD CS, création d'un certificat identifiant la machine en renseignant son nom de domaine sous forme canonique.
    - Ouvrir une console MMC, ajouter le composant "Certificats". Sélectionnez "Un compte d'ordinateur" > "L'ordinateur local"
    - Ouvrir le menu "Certificats" > "Autorités de certification racines de confiance " > "Certificats". Le certificat créé plus haut devrait apparaître. Clic droit > Toutes les tâches > Exporter. Sélectionner "au format X509 .cert", et indiquer le chemin où enregistrer le certificat (par défaut dans les documents du compte courant)

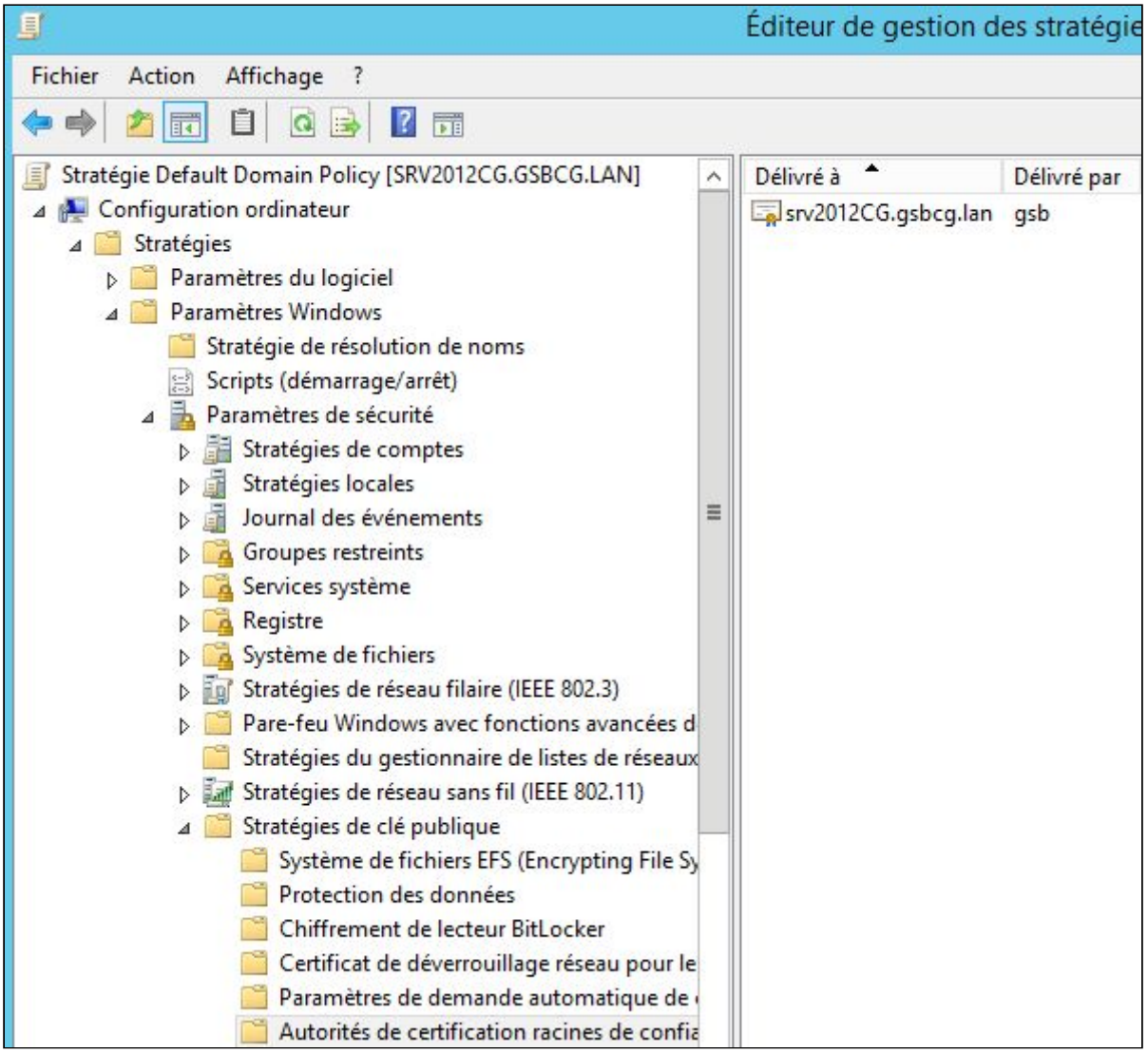
- Création d'un modèle de certificat
    - Gestionnaire de serveurs > Outils > Autorité de certification > nom de l'autorité (ici gsb) > Modèles de certificat [Clic droit] > Gérer
    - Clic Droit sur le modèle "Serveur Web" > "Dupliquer"
    - Sur le nouveau modèle créé, clic droit > "Propriétés >"Sécurité" et modifier les autorisations des "utilisateurs authentifiés". Cocher "Inscrire" et "Inscription automatique" pour qu'ils puissent demander des certificats (inscriptions).



    - Lancer gpudpate pour mettre à jour la stratégie de l'ordinateur

- Modification de la stratégie de groupe afin d'y inclure le certificat
    - Gestionnaire de serveurs > Outils > Gestionnaire de la stratégie de groupe

- Sélectionner le bon domaine, “Objets de stratégie de groupe”, “Default Domain Policy” [Clic droit] > “Modifier”
- Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies de clé publique**Autorités de certification racine de confiance**
- Clic droit dans la zone à droite contenant les certificats > “Importer”
- Lancer gpudpate pour mettre à jour la stratégie de l’ordinateur



Ajout du certificat dans Firefox

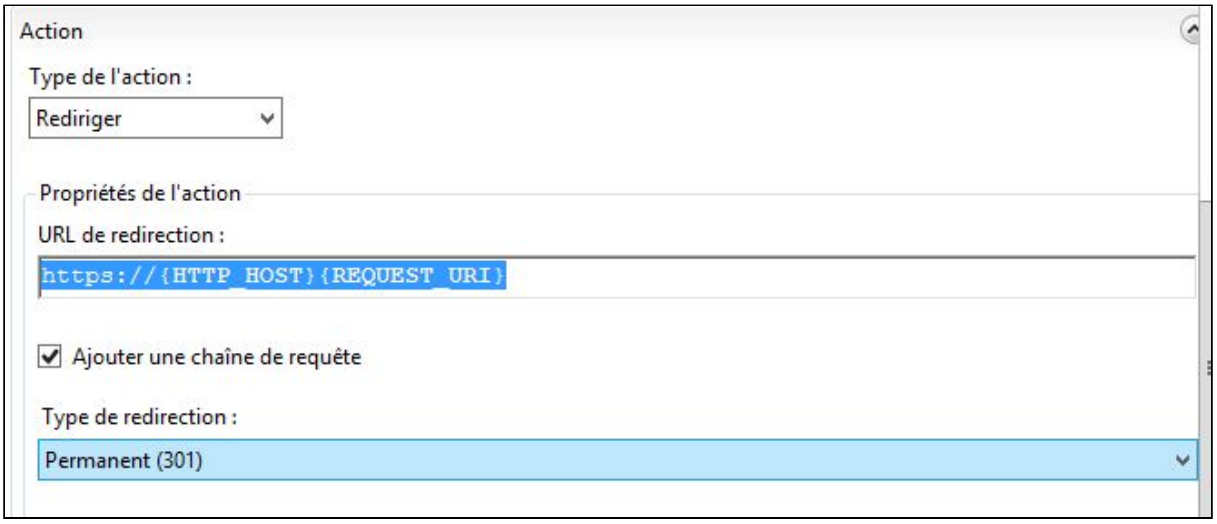
https://www.dhimyotis.com/tuto/Navigateur/Firefox/importation_certificat_firefox.pdf

- Outils > Options > Avancé > Certificats > Afficher les certificats
- Lancer le programme "certmgr.msc" > "Autorités de certification racines de confiance” > “Certificats". Exporter les certificats srv2012cg et gsb.
- Dans “Serveurs”, ajouter le certificat srv2012cg.
- Dans “Autorités de certification”, ajouter le certificat gsb, et lui donner les 3 droits.

Mise en place de la redirection HTTPS

Au niveau de IIS (Gestionnaires de serveurs > Outils > Gestionnaire Internet (IIS)) :

- Sélectionner le site (“Default Web Site”) et cliquer sur “Liaisons” dans le menu à droite. Ajouter une liaison : “https”, “443”, et indiquer le chemin du certificat utilisé.
- Télécharger le module réécriture d’url (https://www.microsoft.com/fr-fr/download/details.aspx?id=7435)
- Default Web Site > Réécriture d’URL > Ajouter une règle puis suivre http://www.jppinto.com/2010/03/automatically-redirect-http-requests-to-https-on-iis7-using-url-rewrite-2-0/



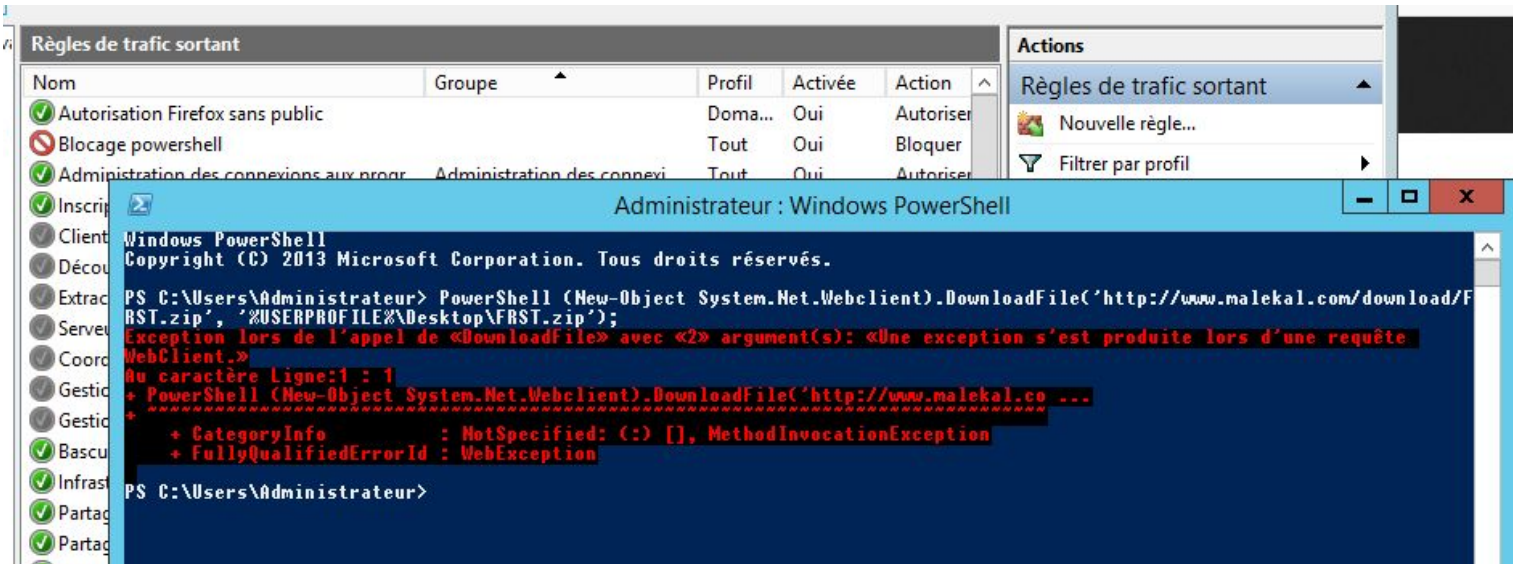
Après ajout de la règle

Mise en place du pare-feu Windows

Tutoriels utilisés afin de se documenter

- https://www.malekal.com/tutoriel-pare-feu-avance-windows/

Stratégie



- Blocage des instances Powershell que plusieurs programmes malicieux pourraient utiliser pour exécuter du code (ex : https://www.youtube.com/watch?v=013gKja_I6U&feature=youtu.be).

- Blocage des scripts wscript en ajoutant une règle adaptée dans le pare-feu.
- Blocage d'explorer (C:\Windows\explorer.exe), sauf pour les partages réseau (une règle autorise le port 445 pour le SMB (port distant dans les options) pour ce programme, une autre interdit tous les ports)

Tests à effectuer

Redirection HTTPS

- Connexion en HTTP pour tester la redirection effective
- Connexion en HTTPS pour tester le fonctionnement du site et son accessibilité.

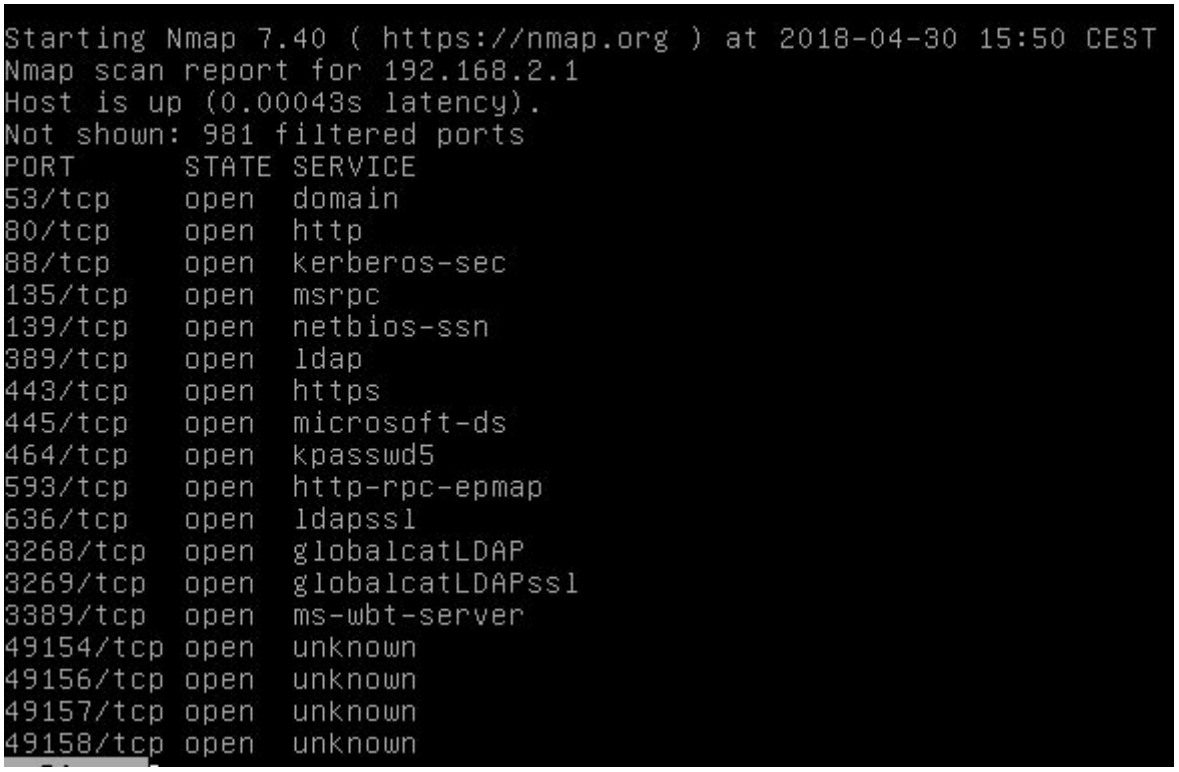
Déploiement du certificat sur le client

- Lancer le programme "certmgr.msc" > "Autorités de certification racines de confiance" > "Certificats".
- Connexion au site par son **nom de domaine**, celui-ci étant attaché au certificat utilisé

Vérification de la sécurité mise en place

Effectuée depuis une Debian 9 (2 Go de mémoire, 12 Go de stockage) avec docker et un conteneur OpenVAS

- Lancement d'un nmap pour vérifier les ports ouverts, qui peuvent être des vulnérabilités crédibles.



```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-04-30 15:50 CEST
Nmap scan report for 192.168.2.1
Host is up (0.00043s latency).
Not shown: 981 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
443/tcp   open  https
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
49154/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
```

- Lancement du programme OpenVAS afin de lister les failles de sécurité présentes.
  - `Documentation :` https://github.com/mikesplain/openvas-docker
  - `curl depl/inst-docker|sh`
  - ~~`docker run -d -p 443:443 --name openvas mikesplain/openvas`~~
  - `docker run -d -p 443:443 -p 9390:9390 --name openvas mikesplain/openvas`
  - ~~`docker run mikesplain/openvas`~~
  - Si on a besoin d'intervenir sur le conteneur : `docker exec -it openvas bash` ou `docker run -i -t mikesplain/openvas /bin/bash`
  - Modifier `/etc/hosts` pour ajouter l'adresse de la machine openvas et pouvoir la contacter grâce à son nom (`openvas`)
  - Se connecter au tableau de bord d'OpenVAS grâce à l'adresse suivante : `192.168.0.27` (statique; `admin/admin`)
  - Cliquer sur "`Scans`" > "`Tasks`", puis sur l'icône violet en haut à gauche, en forme de baguette magique.
  - Entrer l'IP de la machine à tester (192.168.0.46 (statique)) puis attendre le résultat des tests.
  - Cliquer sur "`Scans`" > "`Reports`", puis cliquer sur le rapport en question.
  - Pour chaque vulnérabilité, une solution est proposée :

Vulnerability Detection Result

'Vulnerable' cipher suites accepted by this service via the SSLv3 protocol:

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

Solution

Solution type: Mitigation

The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.

Please see the references for more resources supporting you with this task.

- La plupart des failles proviennent du support des différentes versions obsolètes de TLS et SSL il faut désactiver des versions obsolètes de SSL et TLS . Pour ce faire modification des clés du registres.
- Sources : (https://www.kinamo.fr/fr/support/faq/comment-desactiver-ssl-2-0-et-ssl-3-0-sur-microsoft-iis, https://basics.net/2015/10/06/iis-7-5-how-to-enable-tls-1-1-and-tls-1-2/)

Vulnerability		Severity	QoD	Host	Location	Ac
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS		5.0 (Medium)	98%	192.168.0.46	443/tcp	
DCE/RPC and MSRPC Services Enumeration Reporting		5.0 (Medium)	80%	192.168.0.46	135/tcp	
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)	98%	192.168.0.46	3389/tcp	
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)	98%	192.168.0.46	3269/tcp	
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)	98%	192.168.0.46	636/tcp	
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)	98%	192.168.0.46	443/tcp	
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection		4.3 (Medium)	98%	192.168.0.46	3269/tcp	
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)		4.3 (Medium)	80%	192.168.0.46	3269/tcp	
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection		4.3 (Medium)	98%	192.168.0.46	636/tcp	
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)		4.3 (Medium)	80%	192.168.0.46	636/tcp	
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection		4.3 (Medium)	98%	192.168.0.46	443/tcp	
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)		4.3 (Medium)	80%	192.168.0.46	443/tcp	
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability		4.0 (Medium)	80%	192.168.0.46	3389/tcp	
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability		4.0 (Medium)	80%	192.168.0.46	3269/tcp	

Vulnerability		Severity
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS		5.0 (Medium)
DCE/RPC and MSRPC Services Enumeration Reporting		5.0 (Medium)
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)		4.3 (Medium)
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection		4.3 (Medium)
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)		4.3 (Medium)
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection		4.3 (Medium)
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)		4.3 (Medium)
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection		4.3 (Medium)
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability		4.0 (Medium)
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability		4.0 (Medium)
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability		4.0 (Medium)
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability		4.0 (Medium)
TCP timestamps		2.6 (Low)
(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70)		

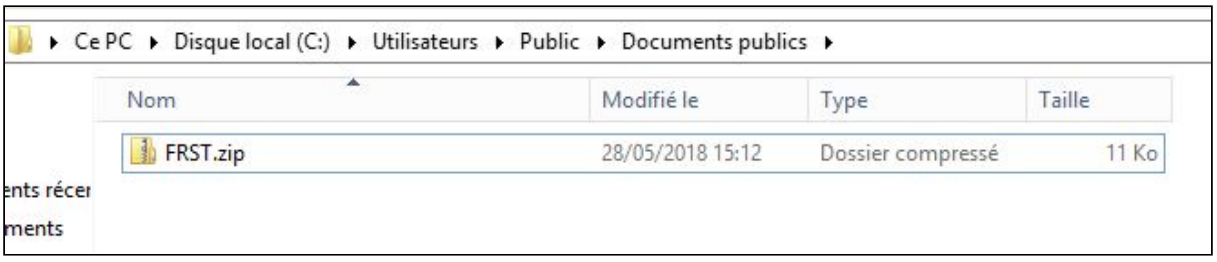
Avant la correction des failles

Vulnerability		Severity
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS		5.0 (Medium)
DCE/RPC and MSRPC Services Enumeration Reporting		5.0 (Medium)
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability		4.0 (Medium)
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability		4.0 (Medium)
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability		4.0 (Medium)
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability		4.0 (Medium)
TCP timestamps		2.6 (Low)

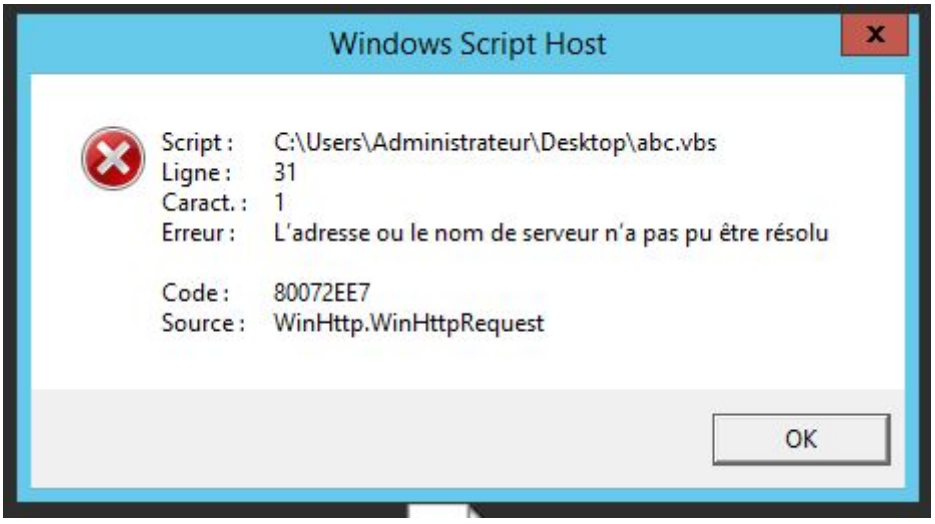
Après la correction des failles

Vérification d'une partie des règles du pare-feu

- Test avec un script permettant de télécharger un programme sous forme de fichier zip.



Avant le blocage



Après le blocage

Améliorations possibles

- **Appliquer toutes les solutions préconisées par OpenVAS afin de sécuriser davantage le serveur web.**

Sources

- https://www.informatiweb-pro.net/admin-systeme/win-server/15--windows-server-2012-2012-r2-creer-une-autorite-de-certification-racine-d-entreprise-root-ca.html