Rapport de Stage

Théo TURLETTI

Stage de 6 semaines réalisé dans l’entreprise Fortinet

Du 16 mai au 24 juin 2022

Adresse : 905 Rue ALBERT EINSTEIN
06560 VALBONNE

Type de présence : Présentiel : 5/5

Test d’authentification Kerberos, NTLM et LDAP et automatisation de génération d’architecture Active Directory

Remerciements

Avant tout développement, je tiens à remercier particulièrement Monsieur Emmanuel Lety, mon maître de stage, qui m'a formé et accompagné tout au long de ce stage avec patience et pédagogie. Je remercie également l'ensemble des employés de Fortinet pour les conseils qu'ils ont pu me prodiguer au cours de ces 6 semaines.

1. Contexte du travail

1.1. L'entreprise Fortinet

Fortinet est une multinationale américaine spécialisée en cyber-sécurité. Elle commercialise des produits et services orientés dans la prévention et la défense contre les intrusions. Son ambition est d'apporter une sécurité numérique globale sur l'ensemble des services et terminaux informatiques.

Ayant acquis la confiance de plus de 500 000 clients et commercialisé à ce jour plus de 7 Millions de produits, le chiffre d'affaires de Fortinet a atteint plus de 3 milliard d'euros en 2021[1]. Son siège social est situé à Sunnyvale en Californie et elle dispose de bureaux locaux dans le monde entier.

Fondée en 2000 par Xen Xie, Fortinet subit une forte croissance depuis 2 ans avec la crise du coronavirus et la révolution digitale. En effet, nos habitudes changent en matière d'utilisation du numérique, les entreprises ont tendance à favoriser le télétravail et l'utilisation de l'Internet des objets (IoT) se généralise. Tout cela crée de forts besoins dans le domaine de l'IA pour gérer la masse de données supplémentaire mais aussi dans le domaine de la cyber-sécurité pour gérer toutes les nouvelles menaces qui découlent de ce changement de paradigme[2].

1.2 Fonctionnement de l'entreprise

Il paraît important de noter, dans un premier temps, que l'entreprise a fait le choix d'une gestion par zone géographique. Ces zones sont EMEA pour Europe Middle-East Africa, APAC - Asie-Pacifique - et Amérique. Ce choix de découpage permet théoriquement une meilleure gestion économique notamment grâce à la limite de distance qu'il impose ainsi qu'à l'homogénéité des fuseaux horaires. Le découpage par continent apparaît inadapté face au faible potentiel de vente du continent Africain et de l'Océanie.

Situé au cœur de la première technopole d'Europe, j'ai effectué un stage au sein de l'équipe Tiger/Core-Tech au centre de Fortinet de Sophia-Antipolis. Cette équipe d'experts est spécialisée dans le produit cœur de l'entreprise, le Fortigate. C'est un pare-feu nouvelle génération qui propose une plateforme large et automatisée pour les entreprises, filtre le trafic réseau et les protège des menaces internes et externes. Sa différence avec les pare-feux traditionnels repose sur des fonctions avancées qui permettent l'identification des assaillants et des nouveaux malwares. Régulièrement mis à jour, il offre une protection évolutive indispensable pour les entreprises soucieuses de leur sécurité.

---

[1] Pour consulter les données financières liées à Fortinet :
https://www.zonebourse.com/cours/action/FORTINET-INC-60103137/fondamentaux

[2] Cf. YUVAL NOAH HARRARI, *Homo Deus* ; KLAUS SCHWAB, *La 4ème révolution industrielle* et *La Grande Réinitialisation*

L'équipe Tiger/Core-Tech s'occupe des pré-ventes des Fortigates sur la région EMEA. Ses membres, les Tigers, sont des Consultant System Engineers (CSE). Leur objectif est de présenter les fonctionnalités avancées du Fortigate et de s'assurer des bonnes conditions de déploiement du Fortigate. Les CSE ne sont pas en contact direct avec le client, ce sont les SE (System Engineers) qui agissent comme intermédiaires et contactent régulièrement les Tigers lorsqu'ils ont des questions précises sur les fonctionnalités ou la configuration du Fortigate chez un client. L'équipe Core-Tech n'est pas la seule équipe composée de CSE, les membres de l'Enhanced-Tech ont les mêmes tâches mais sont spécialisés sur les autres produits vendus par Fortinet.

Le centre de Fortinet de Sophia-Antipolis est aussi composé d'une équipe Support qui s'occupe de l'après-vente. Son rôle est d'aider les clients qui ont des problèmes dans la configuration de leurs nouveaux équipements. L'équipe Support propose même des services où un ingénieur expert peut travailler sur place chez le client plusieurs jours.

De grandes salles dans le centre sont réservées pour les Fortinet Executive Briefing Center (EBC). Les EBC sont des évènements importants qui ont lieu généralement une fois par mois, c'est le moment où le client vient en personne visiter le centre avant de conclure un achat. Les vendeurs qui s'occupent du marketing sont présents, tout comme les SE et les CSE. Les clients visitent également le lab du centre, un grand espace très impressionnant où sont regroupés les serveurs et les produits physiques vendus et testés par Fortinet.

1.3 Concept clé de la commercialisation des produits

Accès Zero-Trust (ZTA)

L'accès Zero-Trust est une approche qui permet de sécuriser l'accès au réseau par l'identification et le contrôle de tous les dispositifs et des utilisateurs. Cette philosophie affirme qu'on ne doit donner sa confiance à personne à l'intérieur ou en dehors du réseau tant qu'une authentification approfondie n'ait été effectuée.

Elle repose sur les concepts suivants :

- L'authentification multi-facteur (MFA) vérifie l'identité des utilisateurs en utilisant différentes formes d'authentification. Celle qui est la plus utilisée se base sur ce que l'utilisateur connaît (authentification par mot de passe). À cela, on peut rajouter une vérification utilisant ce que l'utilisateur a (clé usb, SMS via mobile) ou ce que l'utilisateur est (empreinte digitale, reconnaissance faciale) afin d'accroître la fiabilité de l'authentification.
- La micro-segmentation implique la création de zones dans le réseau pour isoler les éléments qui pourraient contenir des informations sensibles. Une barrière est ensuite placée autour de cette zone grâce à un pare-feu qui bloque les menaces potentielles.
- L'accès privilège minimum (Least-privilege Access) consiste à accorder l'accès à une ressource uniquement aux employées qui en ont absolument besoin. C'est un outil supplémentaire pour limiter les points d'entrées aux informations sensibles.
- L'accès réseau Zero-Trust (ZTNA) est un élément du ZTA qui permet le contrôle d'accès aux applications à distance. La révolution numérique et la crise sanitaire ont

grandement affecté nos comportements; le télétravail commence à s'implanter de manière durable par exemple. Le ZTNA vise à sécuriser l'accès au réseau indépendamment de la localisation de l'utilisateur. Ainsi, la politique de sécurité est la même pour un employé qui travaille à distance que pour un employé en présentiel. Les entreprises préfèrent utiliser le ZTNA plutôt que la connexion par VPN à distance, le ZTNA étant très simple d'utilisation. Au-delà de l'aspect sécurité et transparence, le ZTNA cache les applications derrière un proxy, ce qui les rends inaccessibles directement depuis internet.

Produits correspondants : Fortigate, FortiOS, FortiNAC, FortiClient, FortiToken, FortiAuthenticator[3].

2. Description du travail réalisé

2.1 Objectif du Stage

L'objectif de ce stage consiste à mettre en place un environnement virtualisé afin de mettre en œuvre des tests d'authentification LDAP, NTLM et Kerberos. Ces protocoles ont fait l'objet d'une étude approfondie. Ensuite, afin d'aider Monsieur Emmanuel Lety, j'ai développé des scripts powershell et python afin d'automatiser à la fois la génération d'architecture Active Directory et la configuration du Fortigate avec l'API REST[4].

La suite de ce rapport comporte une présentation des différents protocoles d'authentification puis d'une description du travail réalisé en suivant la logique temporelle.

2.2 Authentification

Identification, Authentification et Autorisation

Il est bon, tout d'abord, de souligner la différence entre ces concepts. L'identification consiste à décliner son identité, elle se fait simplement par le biais d'un identifiant. L'authentification utilise un ou plusieurs moyens pour prouver que la personne est bien celle qu'elle prétend être. Trois modes d'authentification seront présentés dans la suite du

[3] Les informations sur les différents produits sont disponibles ici : https://www.fortinet.com/fr/products
[4] La documentation pour l'API REST de Fortigate : https://fndn.fortinet.net

rapport, LDAP, NTLM et Kerberos. Enfin, on vérifie ses droits d'accès, c'est l'autorisation. LDAP est le protocole qui gère l'autorisation mais l'extension PAC (Privileged Attribute Certificate) de Kerberos peut être une alternative intéressante puisqu'elle intègre l'autorisation dans les tickets d'authentification Kerberos.

Prenons un cas concret pour illustrer ces trois notions, un contrôle de police. Dans un premier temps, le gendarme vous demande votre carte d'identité. Suite à cette identification, il va vérifier que vous êtes bien la personne sur la carte en comparant votre visage à celui de la photo, c'est l'authentification. Enfin, pour l'autorisation, le gendarme va vérifier dans ses fichiers que vous n'êtes pas recherché par ses services.

LDAP

Lightweight Direct Access Protocol est un protocole permettant d'interroger des services d'annuaires, on l'utilisera, dans notre environnement, pour interroger l'Active Directory présent sur le Windows Server. Les requêtes LDAP circulent grâce au protocole TCP/IP sur le réseau.

Pour comprendre le fonctionnement de LDAP, il est nécessaire de s'intéresser à son modèle de nommage. Chaque entrée a un identifiant unique appelé le Distinguished Name (DN), son chemin absolu. Le DN est composé de différents attributs :

- un nom commun ou numéro d'utilisateur (cn ou uid)
- une ou plusieurs unités d'organisations (ou)
- un ou plusieurs "domain components" (dc) qui est généralement le nom de domaine de l'arbre de l'annuaire.

Exemple de DN pour un utilisateur présent dans l'Active Directory : cn = bob, ou = users, dc = eldemo1, dc = com
D'après ce DN, l'utilisateur bob est présent dans l'unité d'organisation "users" du domaine "eldemo1.com".

Le protocole LDAP est capable de gérer à la fois l'authentification et l'autorisation. L'authentification se fait grâce à l'opération bind qui envoie l'identifiant et le mot de passe de l'utilisateur qui s'authentifie en clair au serveur. Si les identifiants et mots de passe correspondent à une entrée dans l'annuaire, alors l'authentification est validée. Le mot de passe circulant en clair, il devient nécessaire de sécuriser la connexion par TLS. Deux moyens sont possibles pour établir cette connexion sécurisée. Soit l'on utilise le protocole non standard LDAPS sur un autre port, ce qui nécessite de fermer la session à chaque fois que l'on souhaite passer d'une connexion sécurisée à une connexion non-sécurisée, soit l'on démarre une connexion sécurisée directement sur le port 389 avec l'opération StartTLS.
Pour l'autorisation, on vérifie si l'utilisateur authentifié est membre d'un groupe ayant les droits d'accès grâce à l'opération search.

NTLM

New Technology LAN Manager est un protocole d'authentification Microsoft challenge-réponse. Il fournit aux utilisateurs un accès par authentification unique (Single Sign-On) en trois étapes : Négociation, Stimulation et Authentification. Dans un premier temps, le client établit une connexion avec le serveur et envoie un message de négociation contenant une liste des fonctionnalités qu'il prend en charge. Le serveur répond ensuite par un challenge. Ce dernier consiste en une opération à appliquer sur le "hash" du mot de passe. Un hash est le résultat d'une fonction de hachage cryptographique, une fonction qui transforme une entrée, ici le mot de passe, en une suite de caractères avec lesquelles il est théoriquement impossible de retrouver le mot de passe. C'est la résolution de ce défi par le client qui permet de valider l'authentification NTLM.

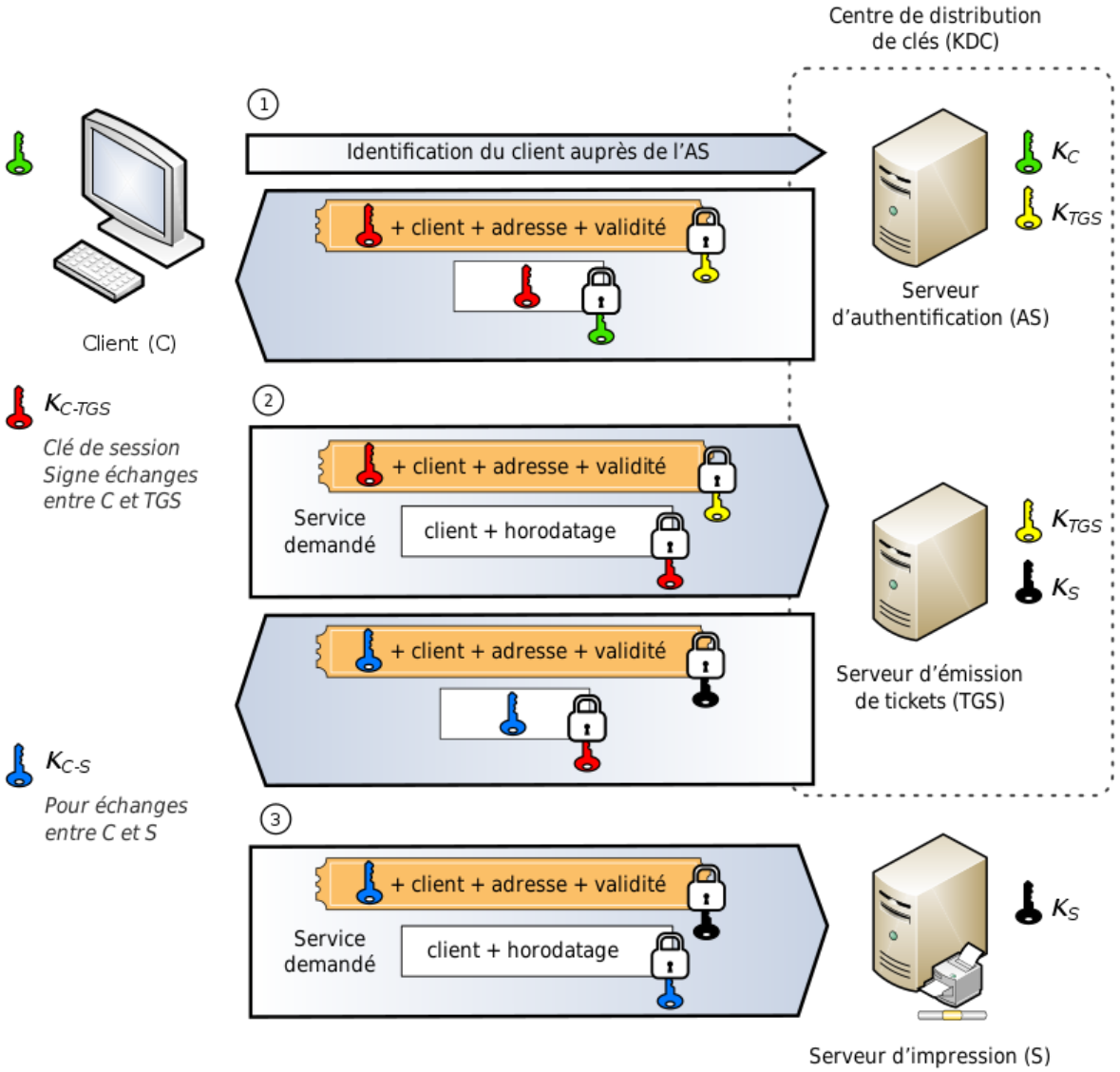
Kerberos

Kerberos est un protocole d'authentification mis en œuvre pour éviter l'interception de mot de passe en clair. Son mécanisme se base sur une communication avec une tierce partie, le Key-Distribution-Center (KDC), qui utilise le chiffrement asymétrique et l'échange de tickets afin d'authentifier l'utilisateur. Le mot de passe utilisé comme clé de chiffrement n'est ainsi jamais transmis sur le réseau. Kerberos suppose que tous les utilisateurs sont dignes de confiance, ainsi si un agent malveillant réussit à accéder au centre de distribution de clé (KDC), c'est tout le système d'authentification kerberos qui est compromis.

Le KDC comprends deux serveurs :

- Serveur d'authentification
- Serveur d'émission de Ticket - Ticket Granting Server (TGS)

Principe de fonctionnement de kerberos :



(1) https://fr.wikipedia.org/wiki/Kerberos

Ce schéma issu de Wikipédia expose clairement les trois étapes de l'authentification Kerberos :

- Phase 1 : Le client commence par envoyer une requête au serveur d'authentification dans laquelle il s'identifie et demande un ticket (TGT - Ticket Granting Ticket) pour accéder au TGS. Le serveur répond en envoyant un ticket ainsi que la clé de session pour communiquer avec le TGS. Cette clé de session est chiffrée asymétriquement avec la clé du client et son mot de passe. Ainsi, l'authentification sera validée de manière implicite lorsque le client déchiffrera la clé de session avec sa propre clé.

- Phase 2 : A chaque fois que le client souhaite accéder à un serveur cible, il doit s'authentifier au TGS en envoyant le ticket TGT reçu précédemment et une requête avec identifiant et date d'émission. Pour valider l'authentification, cette requête doit être chiffrée avec la clé de session déchiffrée dans l'étape 1. Le TGS émet ensuite

un ticket d'accès au serveur qu'il envoie accompagné de la clé de session client-serveur que le client authentifié pourra déchiffrer.

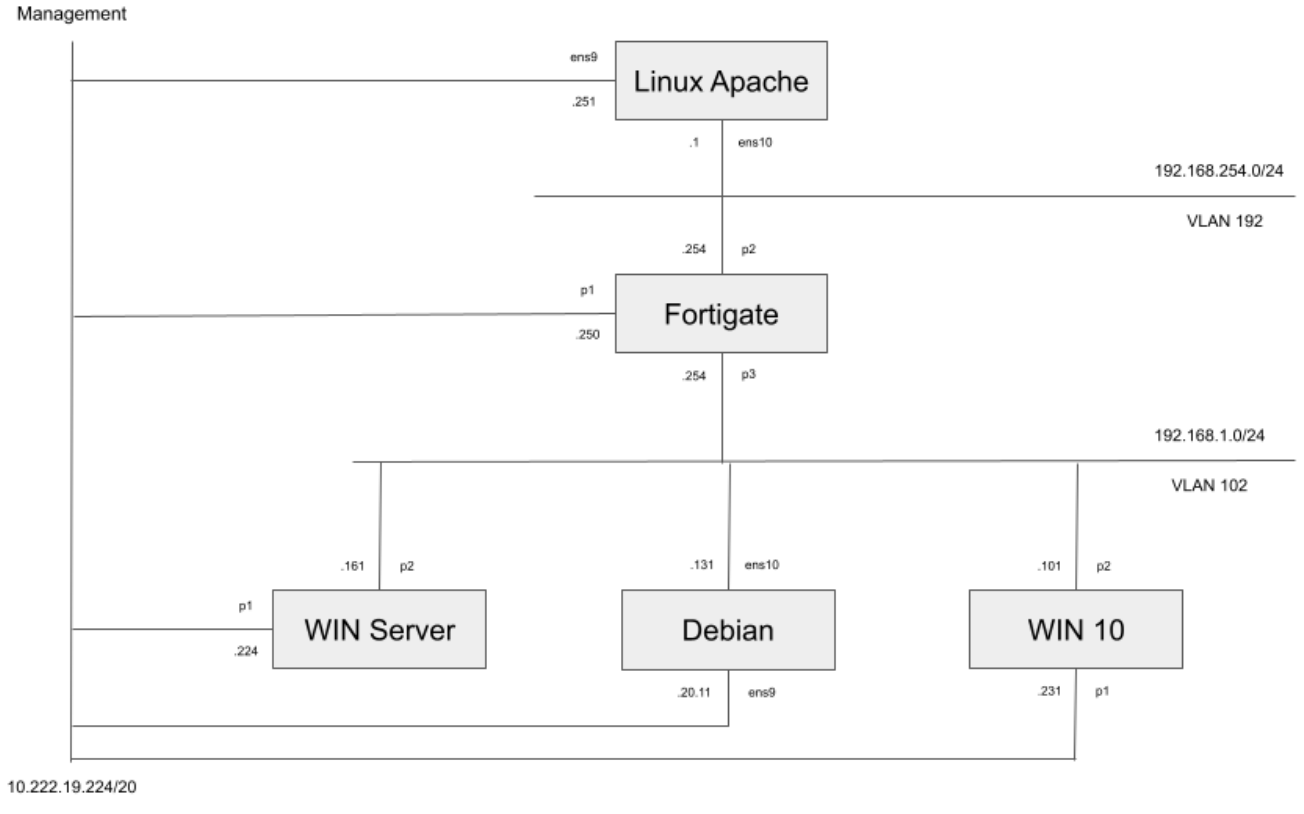
- Phase 3 : Dans cette dernière étape, le client tente d'accéder au serveur. Il lui communique le ticket d'accès provenant du TGS ainsi que son identifiant qu'il chiffre avec la clé de session client-serveur. Le serveur vérifie que tout est correct puis autorise l'accès.

2.3 Programme NSE (Network Security Expert)

Fortinet propose des formations gratuites en cybersécurité pour encourager l'émergence de nouveaux experts[5]. Ce programme est aussi une bonne introduction à tous les produits vendus par l'entreprise. Tous les employés de Fortinet sont ainsi dans l'obligation de le valider en entier et un certain niveau est généralement demandé aux professionnels du secteur pour accéder à certaines présentations de l'entreprise. J'ai ainsi passé le début de la première semaine de stage à valider les 3 premiers niveaux de certification de ce programme[6].

2.4 Mise en place de l'environnement virtuel

L'architecture du réseau sur lequel porte le stage est la suivante:



Toutes les machines présentes sont virtuelles, on y accédera par le réseau Management 10.222.16.0/20 depuis le wifi de l'entreprise. Les deux sous-réseaux virtuels VLAN 102 et VLAN 192 connectent les différentes machines.

L'objectif est de connecter puis d'authentifier les deux clients (Windows 10 et Debian) au serveur apache situé sur la machine Linux derrière le Fortigate. Le Windows Server joue à la fois le rôle de serveur Domain Name System (DNS), d'Active Directory et de Key Distribution Center (KDC) pour l'authentification Kerberos.

Le Fortigate, lui, agit comme pare-feu et explicit-proxy. Son rôle est donc double, bloquer les requêtes non autorisées en interrogeant le windows server et être un intermédiaire pour accéder au subnet de la machine Linux sur lequel est configuré le serveur Apache.

2.5 Configuration des différentes entités

Configuration réseau

Une configuration des sous-réseaux est nécessaire. Il faut dans un premier temps connecter toutes les machines entre elles. Cela se fait en leur attribuant à chacune d'entre elles une adresse ip statique puis en y définissant des routes. Une fois que toutes les machines sont correctement rattachées à leurs sous-réseau respectifs, on peut s'assurer du bon fonctionnement en effectuant des requêtes ICMP (Internet Control Message Protocol) avec la commande ping suivie de l'adresse ip de la machine cible.

Configuration du Windows Server

Ensuite, un serveur DNS (Domain Name System) doit être déployé sur le Windows Server. Son rôle va être de traduire à tous les membres du réseau les noms de domaines en adresse ip et inversement. Une fois le DNS correctement configuré, les clients pourront faire des requêtes DNS au Windows Server à chaque fois qu'ils ont besoin de retrouver une adresse ip.

L'étape suivante dans la configuration du Windows Server est le déploiement d'une forêt Active Directory et d'un contrôleur de domaine. La création d'une forêt et d'un domaine permet d'éviter de placer les utilisateurs et les ordinateurs dans le modèle Groupe De Travail (WORKGROUP) qui est le modèle par défaut de Windows. Constitué d'une base d'utilisateur locale et lourd en administration, il apparaît vite inadapté pour les entreprises. Le passage à un domaine Active Directory sous Windows Server permet entre autres d'avoir une architecture et une administration des utilisateurs et des groupes centralisés ainsi qu'une synchronisation de l'annuaire lorsque plusieurs contrôleurs de domaine sont présents dans la forêt.

Configuration du serveur apache

Ensuite, un serveur apache a été déployé sur la machine debian située derrière le fortigate. Apache HTTP server est le serveur HTTP le plus utilisé d'internet. Une fois déployé, il est possible de coder une page web personnalisée en HTML/CSS/JS.

Pour accéder à cette page web, il suffira pour un client d'entrer l'adresse ip de la machine debian dans un navigateur web. Il est possible d'ajouter l'adresse ip de la machine debian dans le serveur DNS du Windows Server 2016. Cela permet d'accéder à la page web directement à partir du nom de domaine en .com.

Configuration du Fortigate

Le cœur de la configuration se situe sur le Fortigate. Il va falloir dans un premier temps configurer des règles de pare-feu pour laisser passer les paquets entre les deux sous réseaux virtuels.

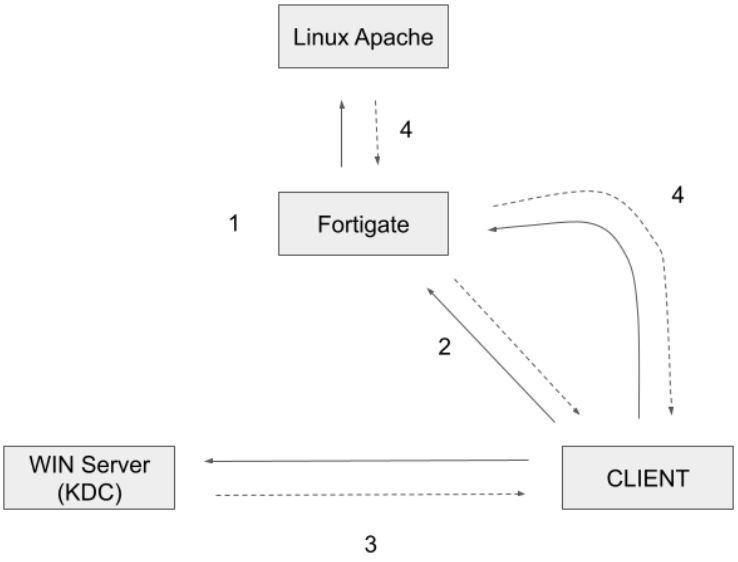
Ensuite la mise en place d'un explicit-proxy permettra au Fortigate de s'occuper de l'autorisation et de l'authentification des clients qui se connectent au serveur Apache. Ce sera donc le Fortigate qui jouera le rôle d'intermédiaire du serveur apache de manière transparente. Ainsi, si un client qui n'a pas d'autorisation tente d'accéder à la page web, le Fortigate, par le biais de son proxy, lui bloquera l'accès.

Configuration du Client Win 10

Ici, la configuration est assez simple. Il faut dans un premier temps changer le modèle par défaut de Windows WORKGROUP et se connecter sur cette machine avec les identifiants d'un utilisateur présent dans le domaine Active Directory accessible depuis le Windows Server.

Puis, il suffit de spécifier, dans les paramètres du navigateur, que l'on souhaite accéder au web depuis le proxy présent sur le Fortigate.

2.6 Simulation d’authentification kerberos dans l’environnement virtuel avec Fortigate



Etape 1 :

Dans un premier temps, une table de clé (keytab) doit être configurée sur le fortigate. Le keytab est un fichier contenant une liste cryptée des principaux et de leur clé respective, dans notre cas, on crée un seul principal, le fortigate. La table de clés permet de décrypter un ticket Kerberos afin de valider ou non l’authentification des utilisateurs. Elle correspond pour le fortigate, agissant comme proxy, à la troisième phase du schéma de fonctionnement de Kerberos[7].

Etape 2 :

Le client tente d'accéder au serveur apache, le fortigate lui bloque l’accès et demande une authentification kerberos.

Etape 3 :

Le client va s’authentifier au serveur d’authentification du KDC présent sur le Windows Server s' il ne l’était pas précédemment, puis va demander un ticket pour valider l’accès par le fortigate au Serveur d’impressions de Ticket (TGS). C’est la phase 1 et 2 de Kerberos.

Etape 4 :

[7] Cf. 2.2 Authentification Kerberos

Le client muni de son ticket peut enfin l'envoyer au fortigate. Le fortigate, grâce à sa clé présente dans le keytab, pourra déchiffrer ce ticket et approuver l'authentification de l'utilisateur. Il fera ensuite une requête HTTP au serveur apache afin de récupérer les données de la page web pour les envoyer au client.

2.7 Automatisation configuration Fortigate

Une partie de ce stage fut consacrée à l'automatisation de la configuration du Fortigate. Le but est de faciliter le travail de mon maître de stage qui doit souvent répéter les mêmes configuration à chaque nouvelle simulation d' environnement client. Les deux automatisations ci-dessous se font grâce à l'API REST du Fortigate, une méthode qui utilise 4 requêtes HTTP - GET, POST, PUT et DELETE - et permet ainsi d'accéder et de modifier les paramètres du Fortigate sans nécessairement passer par son interface (Graphique ou CLI).

Ajout du keytab Kerberos

Le code développé ici permet tout d'abord de générer une table de clés sur le Windows Server. Une fois générée, il faut la déchiffrer et récupérer uniquement la donnée qui nous intéresse, la clé. Un fichier JSON contenant cette clé et d'autres informations comme le nom de domaine du serveur LDAP est ensuite envoyé sur le Fortigate par une requête HTTP "POST" pour finaliser la configuration.[8]

Ajout de groupe pour l'autorisation

La deuxième automatisation est ciblée sur la sélection de groupes pour le firewall du Fortigate. L'objectif est de coder un script qui facilitera la sélection des groupes qui se fait habituellement sur l'interface graphique du Fortigate grâce à des requêtes LDAP[9]. Ces groupes sélectionnés permettent de mettre en place une politique d'autorisation qui bloquera l'accès à tous les groupes non-autorisés.

2.8 Génération d'architecture Active Directory

[8] Code pour la configuration kerberos :
https://github.com/TheoTurletti/Fortinet/tree/main/kerberos_configuration
[9] Code pour la sélection de groupe :
https://github.com/TheoTurletti/Fortinet/tree/main/group_configuration

La génération d'architecture Active Directory fait partie des principaux objectifs de ce stage. Les CSE ont souvent besoin, lorsqu'un client fait face à un problème, de tester certaines fonctionnalités dans un environnement similaire. Les scripts codés permettront aux ingénieurs d'avoir des fonctions pour générer groupes et utilisateurs et d'une base de code documentée qui pourra être facilement enrichi.

Deux scripts ont été envoyés à mon tuteur de stage. Le premier est un script simple en powershell qui permet de générer des architectures Active Directory en prenant en compte trois paramètres : le nombre de groupes, le nombre d'utilisateur par groupe, et le pourcentage d'utilisateur activé.

Le second script est codé en python et utilise la librairie pyad qui permet d'accéder, créer et modifier les divers éléments présents dans l'AD. Lorsque le script est lancé, 5 choix de génération d'architecture Active Directory sont possibles. Les deux premiers choix sont des générations uniformes. Chaque groupe aura x uniques users ou inversement. La création sera symétrique.

La génération du choix 1 forme de nombreux groupes où chaque utilisateur est associé à plusieurs groupes, ces utilisateurs étant les seuls membres de ces groupes.

Pour le choix 2, c'est l'inverse, à chaque groupe est associé plusieurs utilisateurs qui sont uniquement présents dans ce groupe.

Le troisième choix demande le nombre d'utilisateurs, le nombre de groupes et le nombre de groupes par utilisateur. Chaque utilisateur aura ici un nombre fixe de groupes mais l'attribution des groupes aux utilisateurs se fait de manière aléatoire. Ainsi, un groupe peut avoir 0 membres alors qu'un autre plusieurs.

Les quatrièmes et cinquièmes choix sont des générations de groupes de type "nested", où des groupes peuvent être membres d'autres groupes. J'ai fait le choix de créer et d'agencer ces groupes sous forme d'arbre.

Le choix 4 demande le type d'arbre et le nombre de groupes. Choisir le type d'arbre 1 créera une chaîne, 2 un arbre binaire, etc. La profondeur dépendra de ces deux paramètres.

Le choix 5 demande la hauteur et le type d'arbre. Ici c'est le nombre de groupes qui variera en fonction des paramètres.

2.9 Difficultés rencontrées

La configuration du client debian m'a posé plusieurs problèmes. L'objectif était d'intégrer cette machine linux dans l'Active Directory pour ensuite essayer différentes méthodes d'authentification. L'intégration d'une machine linux dans un environnement windows nécessite l'utilisation de samba, un logiciel d'interopérabilité entre système Windows-Unix.

L'intégration dans le domaine AD fut source de nombreux bugs mais c'est l'authentification kerberos qui me posa le plus de problèmes. Pour faire fonctionner kerberos sous linux, il est nécessaire de configurer manuellement un fichier de configuration où sont stockés tous les paramètres internes. J'ai passé plusieurs journées à essayer de faire fonctionner cette authentification en vain. Le manque de documentation et le grand nombre

d’erreurs rencontrées ont fait que j’ai préféré laissé de côté cette partie, le client debian ne fut donc pas totalement configuré à l’issue du stage.

Apports en expérience

Au cours de ces six semaines, j’ai acquis de nombreuses notions en cybersécurité, particulièrement en réseau, qui me seront sans aucun doute utiles dans ma future vie professionnelle. J’ai également accumulé des compétences en powershell et en python à travers le développement des différents scripts.

Ce stage m’a permis d’avoir un bon aperçu du métier d’ingénieur expert réseau. Cela m'a également conforté dans le choix de ma spécialité pour la cinquième année, la cybersécurité.

Enfin, il fut l’occasion de découvrir le fonctionnement d’une grande entreprise en cybersécurité de renommée mondiale, ses méthodes d’organisation et la manière dont travaillent les équipes.

Planning

16 mai - 19 mai 2022 : NSE Certification
20 mai - 1er juin 2022 : Mise en place et configuration de l’environnement / Test d’authentification
2 juin - 6 juin 2022 : Configuration de Kerberos sur Debian
6 juin - 8 juin 2022 : Génération d’Architecture Active Directory avec Powershell
9 juin - 14 juin 2022 : Automatisation configuration du Fortigate
15 juin - 21 juin 2022 : Génération d’Architecture Active Directory avec Python
22 juin - 24 juin 2022 : Rapport de Stage

Conclusion

Ce stage fut l’occasion de découvrir et de travailler sur de nombreux concepts réseaux. J’ai maintenant, grâce aux différents tests d’authentification effectués, un large aperçu des méthodes d’authentification les plus utilisées dans les entreprises. J’ai également acquis, grâce à la configuration du Windows Server et les scripts développées,

de bonnes compétences en administration Windows. Les certifications Fortinet passées au début du stage m'ont apporté un large aperçu des produits et concepts de commercialisation de l'entreprise. De plus, c'est une réelle valeur ajoutée dans un CV.

Ces six semaines dans l'entreprise Fortinet furent une excellente expérience d'immersion dans le monde de la cybersécurité et des réseaux.

Summary

This internship was an opportunity to work on many network concepts. Thanks to the various authentication tests carried out, I now have a large overview of the most used authentication methods in companies. I also acquired, thanks to the configuration of the Windows Server and the developed scripts, good skills in Windows administration. Fortinet certifications I took at the start of the internship brought me a large overview of the company's marketing products and concepts. In addition, it is a real value to add in a CV.

These six weeks in the Fortinet company were an excellent immersion in the world of cybersecurity and networks.

ANNEXE

FORTINET
Training Institute

This acknowledges that

Theo Turletti

successfully completed the course

Information Security Awareness

Rob Rashotte
Vice President, Global Training &
Technical Field Enablement at Fortinet

Date: May 16, 2022

FORTINET
Training Institute

This acknowledges that

Theo Turletti

successfully completed the course

The Evolution of Cybersecurity

Rob Rashotte
Vice President, Global Training &
Technical Field Enablement at Fortinet

Date: May 17, 2022

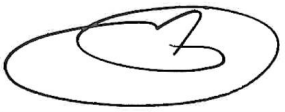
FORTINET
Training Institute

This acknowledges that

Theo Turletti

successfully completed the course

Fortinet Product Awareness



Rob Rashotte
Vice President, Global Training &
Technical Field Enablement at Fortinet

Date: May 30, 2022