Rapport de stage

PREMIÈRE SEMAINE

Lundi —— 27 MAI

Une fois arrivée, on m'a présenté l'équipe puis les locaux qui nous intéresse pour le stage

Présentation des applications importantes pour leur travail:
GLPI : qui est leur moyen de résoudre les demande des membre de l'hopital

Avec un membre de l'équipe, on a réglé un problème de droit dans l'Active Directory. Une personne n'avait pas accès à un dossier partagé.

Ils m'ont montré comment ils ont organisé leur Vlan par exemple:
Le Vlan 200 est pour les personnes dans l'informatique
Le Vlan 10 est pour les médecin en réanimation

J'ai déployé quelques PC sur le réseau de l'hôpital

Mardi —— 28 MAI

Je me suis familiarisé avec le site Cyberwatch qui permet de savoir si dans le domaine il y a des vulnérabilité

J'ai demandé quel type de switch et de routeur ils avaient, donc un membre de l'équipe m'a montré leurs switchs Aruba

Mercredi —— 29 MAI

On m'a demandé sur une kali linux de trouver sur le réseau de l'entreprise les Active Directory

A l'aide de "*nmap*" j'ai pu trouver leurs AD:
"Nmap -sP" m'a permis de trouver leurs 3 AD:
leurs IP et avec la commande "*Nmap -sV*" j'ai trouvé leur nom AD1, AD2 et ADHC3

Avec la commande *"nmap -O"* j'ai pu trouver les OS des 3 AD : deux Windows server 2019 et une Windows server 2022

Après ça, on m'a demandé de trouver le nom de domaine des AD, donc avec la commande "*crackmapexec smb +IP cible"* j'ai pu le trouver.

Jeudi —— 30 MAI

On m'a demandé de continuer le projet de la veille.

Cette fois, il fallait pour entrer dans l'un des active directory que je trouve un identifiant ainsi qu'un mot de passe d'un membre du domaine.

Premièrement, j'ai voulu faire une attaque Man in the middle avec l'outil kali "*Ettercap*"
Mais je n'ai pas réussi

Puis avec Wireshark, j'ai capturé des trames et dans la barre de recherche j'ai mis le protocole *Kerberos* qui m'a permis de trouver un identifiant "980186"

Je n'ai pas eu le temps de pouvoir trouver le mot de passe de l'utilisateur

J'ai trouvé ça compliqué, j'ai du faire énormément de recherche et demander de l'aide (mais les aides étaient très vagues)

Vendredi —— 31 MAI

J'ai continué le projet, mais je n'ai pas réussi à trouver le mot de passe.

J'ai essayé de faire une attaque par brute force à l'aide de crunch
" cruch [minilenght] [maxilenght] mixalpha-numeric-all-space -o > fichier.txt"
Comme leur politique de mot de passe est renforcée, lorsque j'ai essayé, le fichier prenais trop de place donc faisait cracher la machine donc j'ai abandonné l'idée.

Avec hydra, j'ai aussi essayé mais en vain car mon fichier de mot de passe (qui était celui de Crunch n'avait pas été finalisé)

Comme au bout de quelque temps je n'y arrivais pas, j'ai demandé de l'aide mais il ne voyait pas non plus comment faire. Donc j'ai réessayé une attaque man in the middle avec "*Ettercap*" qui n'a rien donné.

On a eu ensuite une idée, trouver un PC sur le domaine et voir si les port du protocole sbm sont ouvert, ce qui permettra de voir les dossier partagés
Mais, les accès étaient refusés donc je n'avais aucune information.

Rapport de stage

DEUXIÈME SEMAINE

Lundi ——— 3 JUIN

Toujours à la recherche d'avoir un identifiant avec un mot de passe pour pouvoir accéder à l'active directory.

J'ai recherché sur internet ce que je pourrai faire, et j'ai appris la connaissance d'une attaque c'est l'Attaque Kerberoasting.

J'ai essayé de la faire mais comme d'habitude, il me faut un mot de passe (ce qui me bloque).

Avec Wireshark, j'ai essayé de capturer des identifiants et des mots de passe sur internet en http avec comme filtre :"http.request.method= "Post (ou GET)""

Mais je n'ai rien trouvé.

Mardi ——— 4 JUIN

Avec un des membres de l'équipe, on a cherché comment résoudre le problème du mot de passe.
Mais toujours en vain.

On a trouvé un serveur SSH à l'aide de Nmap.
Avec ce serveur j'ai essayé de trouver une vulnérabilité à l'aide de Metasploit et de l'exploiter, pour ça je me suis grandement aidée de vidéos et de sites internet.
Mais encore une fois je n'ai pas réussi car leur infrastructure est bien sécurisé.

Après de nombreuses tentatives encore et encore en vain, il m'a donné une nouvelle mission en attendant qu'il trouve une réponse pour que je puisse continuer.

Il faut à présent que je trouve le mot de passe pour me connecter au réseau grâce au Wifi.

Pour ça j'essaie avec "Fern_Wifi_Cracker"

Mais l'application ne parvient pas à trouver l'adresse MAC d'une personne qui utilise ce Wifi.

Mercredi ——— 5 JUIN

Toujours pour le même projet, j'ai utilisé l'outil kali "Wifite", ça permet de faire la liste de tous les wifi à proximité et de pouvoir faire un brute force.

J'ai dézippé le fichier "RockYou.txt" car c'est une bibliothèque de mot de passe.

Sur ceux où "Wifite" fonctionnait (seulement si il y avait une "Handshake Capture, cela nous donnait un fichier en .cap), j'ai essayé le brute force avec la commande "aircrack-ng (le lien en .cap) -w /usr/share/wordlists/rockyou.txt"

Mais, ça n'a pas abouti car dans la liste, il n'y avait pas de mot de passe correspondant.

Je me suis rendue compte qu'il me manquait deux outils pour l'outil "Wifite" sont:
-hcxdumptool
-hcxpcapngtool

Mais pour les avoir, il me faut un moyen d'accéder à internet.

Jeudi ——— 6 JUIN

Après plusieurs heures de recherche et plusieurs tests qui n'ont pas fonctionné, on a utilisé une clé wifi "tp-link"et je l'ai connecté au hotspot de l'hôpital, avec la commande "nmcli device wifi connect HOPITAL-HOTSPOT".

Une fois connecté, j'ai pu télécharger les outils qu'il me manquait tout en suivant une vidéo Youtube car l'installation est complexe.

https://www.youtube.com/watch?v=oWgfqOC0Hlo

Vendredi ——— 7 JUIN

Il fallait que je trouve le moyen de changer sur "Wifite" la bibliothèque de mot de passe par défaut.
"Sudo wifite --wpa --dict /usr/share/wordlists/rockyou.txt --kill".

Durant plusieurs heures, j'ai procédé à plusieurs tests de nombreux réseaux wifi mais comme c'était vraiment long et prenaient toutes les performance de la kali j'ai arrêté.
Ceux que j'ai plutôt réussi n'ont pas fonctionné car même avec le brute force, ça n'a pas trouvé le mot de passe.

Comme la liste des mots de passe ne m'a pas fait réussir, j'en ai installé une avec plus de mot:
"Crackstation.txt" avec plus de 1,493,677,782 mots

Au départ, je voulais le fichier "Rockyou2021.txt" (c'est la plus grandes liste de mot de passe) mais elle était trop volumineuse pour le PC qui m'a été mis à disposition.

Mais, je n'ai pas eu le temps de tester la liste.

Rapport de stage

TROISIÈME SEMAINE

Lundi —— 10 JUIN

Après demande de faire du réseau, il m'ont dit qu'on commencera Mardi.

Donc je me suis informé sur ce qu'était un Bastion, un UTM et comment fonctionnait SCCM.
J'en ai donc fais des fiches, car c'est un bon moyen mnémotechnique par exemple avec des schémas.

J'ai demandé à ce qu'on me donne les droit sur SCCM pour que je puisse regarde comment ça fonctionne et à quoi ça ressemble exactement. On m'a expliqué rapidement mais je n'ai pas vraiment compris.

Puis on m'a donné un lien pour accéder à leur bastion, j'ai mis mon compte admin. Mais ils m'ont laissé sans explications, j'ai fais des recherches mais je n'ai non plus pas compris.

Mardi —— 11 JUIN

On m'a donné comme première mission de copier une configuration sur un switch HP de tout copier dessus en urgence.

J'ai procédé à la réinitialisation du switch en supprimant la configuration du switch afin de pouvoir copier la nouvelle configuration.

Ensuite, j'ai copié la configuration sur un fichier puis réinitialisé 10 switch HP car ils n'en n'ont plus l'utilité, parce que maintenant ils ont des Aruba.

J'ai appris de nouvelles commandes qui sont propre à HP tel que:
-display current-config -> ça permet de voir la configuration que le switch utilise.
-display startup -> montre le fichier de la sauvegarde de la configuration
-delete fichier.cfg

Mercredi —— 12 JUIN

J'ai réinitialisé le reste des switch (environ une dizaine), c'était long car les switch étaient vieux et lents.

Puis l'après-midi, j'ai du aller dans l'atelier de l'hôpital pour récupérer la configuration d'un switch qu'ils veulent changer.

Puis avec la configuration du switch HP, je devais la mettre sur leur nouveau Switch Aruba.

Certaines commandes étaient comme celle de Cisco.

Par exemple, j'ai appris une commande : "spannig-tree bpdu-gard" -> ça empêche les boucles entre plusieurs switch.

J'ai seulement eu le temps de configurer les vlan.

Jeudi —— 13 JUIN

J'ai continué à configurer le switch Aruba.

J'ai eu un problème, dès que j'allais sur PuTTy puis en serial avec le port Com adapté, cela me mettait des signes étranges.
J'avais oublié de changer le débit en bauds, il fallait mettre 115200.

Sur la configuration du HP, il y avait plein de commande que je ne comprenais pas donc j'ai fais des recherches.

J'ai réussi à configurer la plupart des interfaces avec l'aide d'un membre de l'équipe et des recherches internet.

J'ai configuré les routes par défaut avec la commande : "ip route 0.0.0.0/Masque +une ip"

Vendredi —— 14 JUIN

J'ai continué à configurer le switch.
J'ai fini de configurer les interfaces, j'ai essayer à l'aide d'autres configurations Aruba de faire ce que je ne connaissait pas.
Par exemple, j'ai appris ce qu'était le AAA(Authentification Autorization Accounting) qui permet de vérifier les utilisateurs qui se connectent peut importe où ils sont dans le réseau . Pour ça, il faut utiliser un serveur d'authentification. Dans la configuration, on a utilisé Radius, Tacacs et j'ai essayé aussi Clearpass. Grâce à ces serveur, les utilisateurs serons placés automatiquement dans le vlan attribué en fonction de leur travail/fonction dans l'entreprise. Mais si un utilisateur n'est pas connu, sont accès sera soit refusé, soit il sera placé dans un vlan dit "poubelle"

J'ai configuré à l'aide d'un autre Aruba le server SNMP, ce qui permet d'analyser les éléments du réseau.

Mais je ne pouvais pas faire quelque commande à cause de la version de l'OS du switch.

Ensuite, pour le Clearpass, j'ai configuré les "Port-access role +nom_du_role". Cela permet d'associer des rôles à tous les clients, authentifiés et non authentifiés et appliqués à chaque session utilisateur.

Rapport de stage

QUATRIÈME SEMAINE

Lundi —— 17 JUIN

On m'a aidé a finalisé le switch, car il y avait des commande qui ne fonctionnaient pas en fonction de l'OS des Aruba.

On est allé débrancher l'ancien switch de l'atelier afin de mettre le nouveau.

Puis on est allé dans la salle des serveurs, il y a deux cœur de réseau : un pour les switch HP (qu'il faut tous changer) et un autre pour les switch Aruba.
Donc comme l'ancien était un HP et le nouveau était un Aruba, on a donc du modifier la topologie afin que le nouveau switch soit dans le cœur de réseau Aruba.

Puis l'après midi, ils devaient faire une réunion pour les procédures en cas de cyber attaques. Ils m'ont donc demandé de venir et me posaient des questions sur ce dont je pensais de la procédure et si j'avais des idées de comment faire.

Mardi —— 18 JUIN

La matin, j'ai demandé ce que je pouvais faire, mais ils ne savaient pas quoi.

Après de nombreuses demandes, on m'a fait tester le switch que j'ai configuré pour savoir si il convenait à la procédure de cyber attaque.

Après ça, un stagiaire a demandé si on pouvait faire un AD. Donc moi j'ai voulu essayé de faire une machine physique Windows server 2022 avec une iso que le stagiaire avait déjà sur clé.

Mercredi —— 19 JUIN

La machine n'avait aucun pilote et je n'avais aucune carte réseau.

Après des recherches, je suis tombé sur le bon driver et j'avais enfin une carte réseau.

Mais quand on essayé de la branché sur le réseau, ça ne le détectait pas.

Alors avec deux employés, on a cherché comment faire. Mais, on y arrivait toujours pas. Alors j'ai trouvé une iso plus récente de Windows server 2022 et cette fois ci avec la carte réseau déjà installé.

Mais le problème était toujours là.

Jeudi —— 20 JUIN

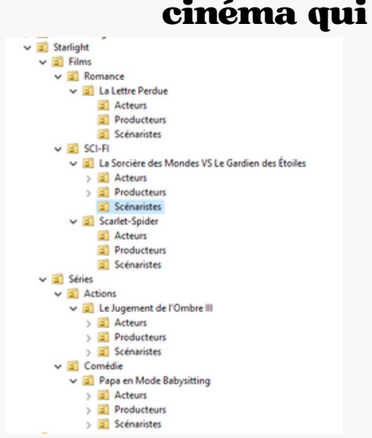
Finalement, comme le problème persistait et on ne trouvait pas de solution, on m'a dit de passer sur une VM.

Comme les PC de l'hôpital n'avait assez de mémoire RAM, je n'arrivais pas à lancer la VM Windows server 2022.

Donc, je suis passée sur une Windows server 2019 (j'ai mis 2048MB) et une Windows 11, comme ce que l'on avait fait en cours.

J'ai ajouté le rôle d'active directory, DNS et DHCP.

J'ai voulu crée un Active Directory pour une entreprise de cinéma qui ressemble à peu près à ça:



Vendredi —— 21 JUIN

J'ai continué mon AD, j'y ai inscrit les utilisateurs et les groupes.
Par exemple: Le groupe Producteur qui est avec un utilisateur que j'ai placé dans l'UO producteurs

Ensuite, j'ai commencé à créer les GPO:
-Augmenter les exigences de mots de passe (minimum 15 caractères)
-Durée de vie minimal d'1 mdp : 1j -> 5j
-Durée de vie maximal d'1 mdp : 42j -> 30j
-Durée de vie minimal d'1 mdp : 5j

J'ai des des Stratégie de verrouillage du compte :
-Seuil verrouillage : 0 -> 5
-Durée de verrouillage des comptes : 0-> 10min
-Réinitialiser le compteur de verrouillage du compte : 0-> 10min
Ainsi que d'autres GPO que l'on a vu en cours comme interdiction d'accès au panneau de configuration,...

On m'a demandé de faire du Tiering. Avec l'aide d'un salarié, on à récupérer un script PowerShell pour que ça nous créer les GPO, Groupes, UO et quelques utilisateurs pour avoir des compte T0,T1 et T2.

Rapport de stage

CINQUIÈME SEMAINE

Lundi —— 24 JUIN

Dans l'AD, j'ai créé les répertoires personnels des utilisateurs ainsi que le répertoire de leur profil.

Ensuite, j'ai fait une GPO pour les fond d'écran (1 pour chaque rôle).

Après ça, j'ai créé mes compte T0,T1 et T2 par exemple :
"Adminlucy -t0"
Puis je leur ai mis des droits en les associant à des groupe qui sont soumis à des GPO qui ont été installés avec le tiering.

Après cela, on m'a demandé à ce que seul les comptes T0 (qui sont des comptes pour l'accès à l'active directory) aient accès à l'AD.

J'ai créé une GPO et autorisé l'accès au bureau à distance depuis l'AD.

À cause du tiering, on ne peut pas établir une connexion bureau à distance avec l'IP mais il faut mettre le nom de la machine de l'AD.

Mardi —— 25 JUIN

J'ai continué à créer des GPO, j'ai voulu :

-mettre en place un message d'avertissement avant la connexion de l'utilisateur

-prévenir l'utilisateur qu'il doit changer son mot de passe avant qu'il n'expire 0 -> 3j

-limite d'inactivité de l'ordinateur: 0 ->120 s (2min)

Je crée une nouvelle AD (AD-Sunshine) pour pouvoir faire un domaine d'approbation
Domaine : AD-Sunshine.local

J'ai configuré le DNS pour que les deux machines se connaissent puis j'ai pu faire la relation d'approbation.

Puis pour voir si cela marchait, je devais utilisé un compte utilisateur de l'AD-Sunshine depuis ma machine windows 11.

J'ai donc créer une GPO dans laquelle, j'autorise tout le monde a pouvoir se connecter localement.

Mercredi —— 26 JUIN

J'ai créé une machine Windows10 afin de l'inscrire dans l'AD Sunshine.

Avec un compte inscrit sur l'AD Lucy, grâce à la relation d'approbation, j'ai pu m'identifié avec la machine Windows10.

Sur l'AD-Sunshine, j'ai continué la création de comptes et de groupes.

J'ai ensuite créé une machine Windows Server 2022. Cet AD ci, sera un domaine enfant de la forêt AD-Lucy.local.

Pour ça, dans le DNS de chaque machine, j'ai inscrit chaque AD pour qu'elles puissent se reconnaître.

Pour essayer si ça avait bien marché, je me suis connecté à la Windows11 inscrite dans L'AD-Lucy avec un compte de l'AD-Storm (Windows server 2022)

Jeudi —— 27 JUIN

Préparation des Switch pour les donner à l'école (ainsi qu'a moi même) puis des nouveaux claviers.

Il y a eu la venue des professeurs, où l'un des employé à expliqué ce que j'avais fait durant le stage.

J'ai fait signé la fiche d'attestation de fin de stage car mon tuteur est en télétravail le vendredi.

Puis, j'ai commencé à créer un serveur GLPI avec une VM Debian.

Lors de l'installation, le miroir ne voulait pas fonctionnait.

J'ai créé la machine plusieurs dizaines de fois car je pensais avoir mal crée la machine. Mais en vain.

Puis, chez moi j'ai installé la machine sans aucun problème de miroir.

Vendredi —— 28 JUIN

J'ai apporté des cookies que j'avais fait pour leur remercier de s'être occupé de moi.

J'ai continué le serveur GLPI, à l'aide de ce site :
https://www.it-connect.fr/installation-pas-a-pas-de-glpi-10-sur-debian-12/

J'ai eu une erreur lors de l'installation de GLPI, il y avait un problème de droit d'écriture.

J'ai ensuite trouvé l'erreur, un des fichier que j'avais crée s'est supprimé et j'avait fais une erreur dans un des autres fichiers.

Après avoir corrigé, j'ai pu installé normalement GLPI.

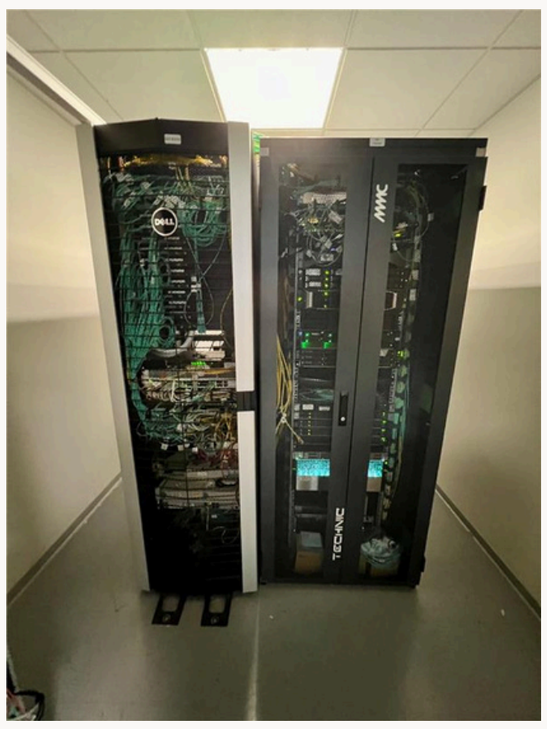
Puis, j'ai changé le mot de passe de base du compte : glpi/glpi en glpi/123AZEqsd!

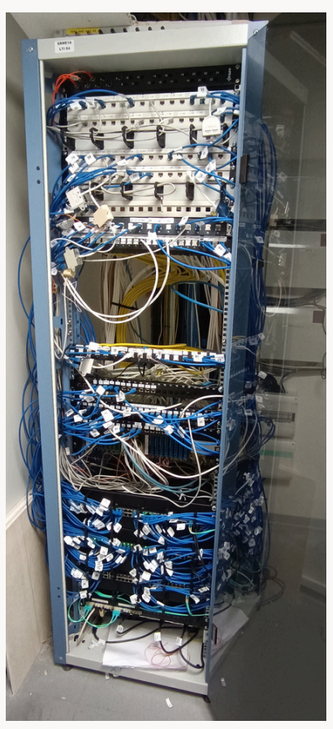
Comme c'était la fin de la journée, je suis allée prendre des photos des serveur pour mon rapport

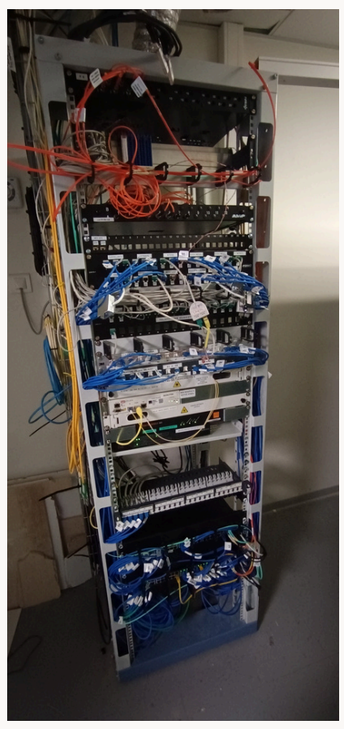
Pour finir, je suis allée rendre les clefs des locaux.

Rapport de stage

PHOTOS ANNEXES

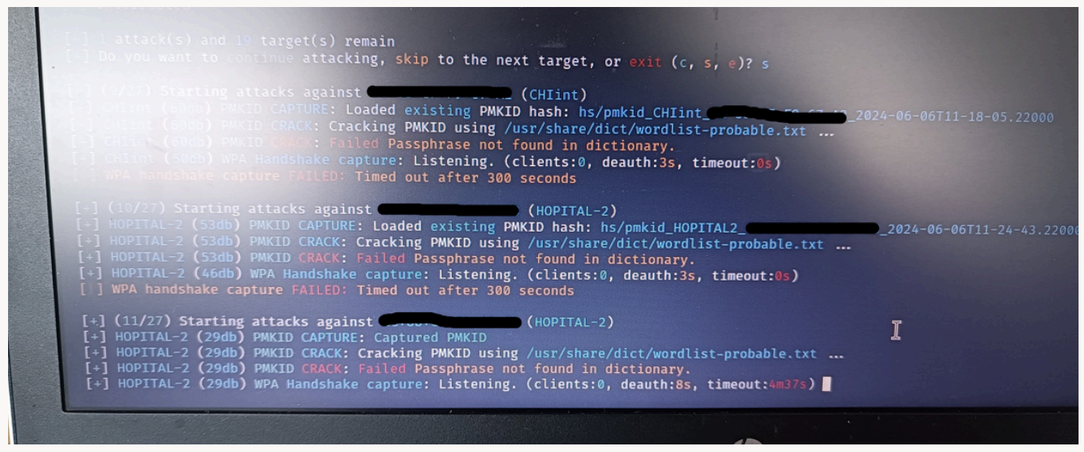






← **Ce sont les baies de serveur de l’hôpital**

Tentative de craquage de mot de passe d’un wifi avec l’outil Wifite →



Trouver les AD à l’aide de l’outil “Nmap” →

C’est une partie des Switch que j’ai réinitialisé.

↓

C’est le Switch de l’atelier que j’ai configuré puis remplacé

↓