Rapport de Stage

Table des Matières :

Semaine 1

Lundi 05 janvier

Lors de cette première journée de stage, j'ai pris en charge des demandes via l'outil GLPI, principalement des tickets d'incident. Je me suis déplacé auprès des utilisateurs. De mon temps libre, j'ai commencé à avancer sur mon portfolio en mettant à jour certaines informations.

Mardi 06 janvier

Durant cette journée, j'ai poursuivi le traitement des demandes sur GLPI en gérant différents tickets d'incident. Je suis également intervenu directement auprès des utilisateurs. J'ai continué à travailler sur mon portfolio afin de le compléter progressivement.

Mercredi 07 janvier

J'ai de nouveau traité des tickets d'incident via GLPI et aidé les utilisateurs en me déplaçant sur site. J'ai configuré et déployé des switchs Aruba. Je me suis connecté aux équipements à l'aide de l'outil PuTTY afin d'accéder à la ligne de commande en y précisant une vitesse de 115200 . J'ai vérifié la version du système avec la commande show version, puis monté une clé USB à l'aide de usb mount et vérifié son contenu avec show usb file-system. J'ai copié la nouvelle image avec copy usb:/... secondary, puis défini l'image de démarrage avec la commande boot system secondary.

Jeudi 08 janvier

Cette journée a été similaire à la précédente concernant le traitement des tickets GLPI et l'assistance aux utilisateurs. En complément, j'ai découvert le pentesting sur une machine Parrot. J'ai réalisé une analyse d'empreintes numériques à partir des réseaux sociaux. Pour cela, j'ai utilisé plusieurs outils tels que nslookup afin de trouver l'adresse IP du serveur, whois afin d'en savoir plus sur le nom de domaine, sublist3r pour énumérer les sous-domaines et dnsrecon pour collecter des informations sur une infrastructure DNS afin d'identifier des sous-domaines, des enregistrements DNS. J'ai également effectué une analyse des ports à l'aide de l'outil nmap.

Vendredi 09 janvier

J'ai finalisé le travail qui m'avait été confié concernant le pentest. J'ai notamment utilisé l'outil theHarvester afin de collecter des informations. J'ai également continué à gérer certains des tickets d'incident via GLPI et j'ai avancé sur mon portfolio de mon temps libre.

Semaine 2

Lundi 11 janvier

J’ai fini de déployer des switchs Aruba 6300M en mettant à jour les drivers dans le gestionnaire de périphériques. Pour trouver les bons composants, j’ai effectué des recherches au préalable sur Reddit. Une fois les drivers installés, j’ai terminé le travail en installant la dernière image système sur ces switchs afin qu'ils soient totalement à jour.

Mardi 12 janvier

Je me suis occupé de la mise à jour de cinq firewalls Fortinet. Comme on ne peut pas passer directement à la dernière version, j’ai dû avancer petit à petit en installant les versions antérieures les unes après les autres pour respecter le chemin de mise à jour. Pour finir, j'ai appliqué une configuration de base sur l'un des firewalls.

Mercredi 14 janvier

J’ai continué ma mission sur le pentest en me branchant directement sur un port réseau protégé par un NAC. Cette manipulation m'a permis d'accéder au premier contrôleur de domaine (AD) du réseau. Cependant, je suis resté bloqué car je ne pouvais ni lister les unités d'organisation (UO), ni voir les classes d'objets à cause des sécurités en place.

Jeudi 15 janvier

À cause d'un problème de Wi-Fi dans la matinée, j’ai dû préparer et déployer 2 ou 3 machines. Je me suis ensuite davantage renseigné sur l’utilisation de l’outil Metasploit, déjà vu en première année. Enfin, j'ai utilisé nslookup pour trouver un AD en haute disponibilité, puis nmap pour lister les ports ouverts et les numéros de version des logiciels.

Vendredi 16 janvier

En me branchant sur un port NAC, j'ai analysé les trames avec Wireshark pour observer une connexion entre un employé et une imprimante. J'ai ensuite utilisé un module de Metasploit Auxiliary Konica Minolta Password Extractor pour tenter d'extraire les mots de passe d'une centaine d'imprimantes. J’ai configuré les options RHOSTS, RPORT et le SSL, mais les machines ont répondu par une erreur car “la connexion s'est brutalement interrompue”.

Semaine 3

Lundi 19 janvier

J'ai commencé par créer des machines virtuelles avec VirtualBox. J'ai installé un serveur pour gérer le réseau (AD) et un autre pour la messagerie (Exchange). J'ai aussi préparé des nouveaux PC.

Mardi 20 janvier

J'ai fait les mises à jour Windows et j'ai installé Exchange. Malheureusement, j'ai vu trop tard que je n'avais pas assez de place sur le disque dur.

Mercredi 21 janvier

Pour régler mon problème de place, j'ai tout réinstallé sur des vrais ordinateurs au lieu du virtuel. J'ai relié trois machines entre elles grâce à un switch. J'ai aussi préparé une clé USB avec Rufus pour installer les systèmes sur des PC Dell.

Jeudi 22 janvier

J'ai eu un problème d'écran bleu sur un PC. J'ai dû utiliser une image système de l'hôpital et changer de machine pour que ça marche enfin. J'ai aussi continué à préparer des ordinateurs.

Vendredi 23 janvier

La connexion était très lente, donc les mises à jour ont mis 4 heures. Heureusement, j'avais téléchargé les outils à l'avance. J'ai réussi à finir mes serveurs AD et Exchange.

Semaine 4

Lundi 26 janvier

J'ai fini de configurer la messagerie Exchange avec un nom de domaine. Pour la sécurité, j'ai installé CrowdSec afin de protéger mon serveur.

Mardi 27 janvier

J'ai commencé l'installation d'un serveur SCCM sur une nouvelle machine pour apprendre à gérer un parc informatique.

Jeudi 29 janvier

Après avoir promu le serveur en windows server 2016, j'ai donc dû promouvoir les autres serveurs en tant que windows server 2016. Suite à ça, je n'avais plus aucun fichier de configuration, j'ai dû tout recommencer à zéro. J'ai réussi à terminer mon serveur Echange. J'ai transformé ma machine physique en machine virtuelle (P2V).

j'ai été à la journée des portes ouvertes le mercredi 28 janvier pour l'iut de sophia-antipolis ainsi que la licence avec Nathan.
Pour des raisons médicales, j'ai été absent le vendredi 30 janvier. Vous trouverez ci-dessous le justificatif de mon absence.

Semaine 5

Lundi 2 février

J'ai commencé en travaillant sur un serveur de déploiement SCCM. Cependant, au cours de mes recherches, j'ai décidé de changer de stratégie pour m'orienter vers une solution plus directement intégrée à l'Active Directory. J'ai donc opté pour la mise en place d'un serveur WDS.

Mardi 3 février

J'ai procédé au déploiement du serveur WDS et à l'intégration d'une image Windows 11. Pour cela, j'ai récupéré les fichiers install.wim et boot.wim en montant l'iso, afin de permettre le déploiement de postes clients sur le réseau, qu'ils soient en mode UEFI ou en Boot. J'ai ensuite, à l'aide d'un script ajouté des classes de fournisseurs à l'aide de scripts trouvés sur le site de IT-Connect. J'ai également envisagé d'installer l'outil MDT, mais j'ai constaté qu'il n'était plus disponible à l'installation.

Mercredi 4 février

J'ai, par la suite, déployé un serveur de supervision Zabbix. Une fois installé, j'ai configuré et installé les agents Zabbix sur le superviseur lui-même, ainsi que sur le serveur Exchange et l'Active Directory.

Jeudi 5 février

J'ai d'abord tenté de créer une machine virtuelle sous VirtualBox, mais j'ai rencontré un problème : la présence d'Hyper-V sur mon poste empêchait le lancement de la VM. Pour éviter de désinstaller l'Hyper-V où je comptais seulement appliquer les serveurs virtualisés, j'ai décidé d'intégrer directement le serveur d'inventaire OCS Inventory sur la machine existante du superviseur. J'ai ensuite déployé l'agent OCS sur le serveur AD, puis je l'ai appliqué à toutes les machines de ce réseau via une GPO au démarrage. Cela m'a permis d'automatiser l'inventaire des nouvelles machines dès leur connexion au domaine.

Vendredi 6 février

J'ai fini la semaine par le déploiement de GLPI. Après une première installation en version 10.0.16, j'ai rencontré un problème de compatibilité avec le plugin OCS Inventory NG. J'ai donc dû installer GLPI en version 11.0.0 et recréer la base de données. Grâce à cette mise à jour, j'ai réussi l'installation du plugin ainsi que la synchronisation entre OCS et GLPI. Enfin, j'ai lié GLPI à l'annuaire Active Directory pour permettre l'authentification des utilisateurs, après avoir configuré les règles de pare-feu nécessaires. J'ai donc essayé de me connecter avec un compte avec peu de privilèges sur GLPI simulant un problème technique sur un des pc du réseau pour qu'une personne du service un informatique du réseau (compte avec de hauts privilèges) puisse s'en occuper.

Semaine 6

Lundi 9 février

Déploiement d'un serveur de sauvegarde et de restauration Veeam Backup & Replication. Après l'installation de Veeam, j'ai procédé au déploiement des agents Veeam sur chaque machine du parc, qu'il s'agisse des serveurs sous Windows ou des serveurs Debian.

Mardi 10 février

J'ai consacré cette journée à la mise en place d'un bastion Apache Guacamole afin de sécuriser et faciliter les accès distants à mon réseau. Je me suis donc appuyé sur les procédures vues en cours. Le bastion n'est cependant pas accessible à distance. Je n'ai pas ajouté de pare-feu quelconque.

Mercredi 11 février

Dans la continuité des travaux précédents, j'ai finalisé la configuration de la solution Veeam en initiant la virtualisation de l'ensemble des machines au sein de l'hyperviseur Hyper-V de Windows Server. Cette étape était cruciale pour consolider l'infrastructure. Une fois les machines virtuelles opérationnelles et stabilisées sous Hyper-V, j'ai configuré et lancé les premières sauvegardes complètes dans Veeam Backup. Cela m'a permis de vérifier l'intégrité des données et de m'assurer que les points de restauration étaient correctement créés pour chaque serveur critique.

Jeudi 12 février

J'ai procédé au déploiement de huit firewalls Fortinet. J'ai dû monter progressivement dans les mises à jour (6.4.7 à 7.2.9) . Pour réaliser une configuration de base plus rapidement, j'ai utilisé la ligne de commande afin de configurer l'interface 2 avec l'adresse IP 192.168.254.254/24. J'ai également appliqué la commande set allowaccess ping https ssh stp pour définir les protocoles d'administration autorisés.

Vendredi 13 février

j'ai effectué un redéploiement complet de l'ensemble des machines utilisées durant mon stage.