Du 24 mai au 25 juin 2021

Note de synthèse

Jordan HAYAT
BTS SIO SISR

Table des matières

REMERCIEMENTS

Je souhaite remercier dans un 1er temps mon corps enseignant, puis la direction de mon établissement ORT Montreuil pour leur accompagnement dans ma recherche de stage.

J'aimerai également remercier Hadi El-Khoury, mon tuteur, qui m'a permis de réaliser mes 5 semaines de stage au sein de son entreprise. Grâce à lui, j'ai pu découvrir le monde de la start-up. Il s'est montré patient et très pédagogue envers moi, a fait preuve de bienveillance, et m'a permis d'acquérir de nouvelles connaissances tout au long de ce stage.

Je suis également très reconnaissant envers Arthur Duchet-Suchaux, le CEO de la société et Léo Dupouy, le CTO, qui, malgré la distance, m'ont partagé leurs compétences et leurs sages explications.

Enfin, je tiens à saluer cordialement l'ensemble des personnes qui ont pu m'aider, de près ou de loin pendant mon séjour, ainsi que pour l'accueil et le temps qu'ils m'ont consacré.

I) CONTEXTE

A) Présentation de l'entreprise

Knock Knock est une start-up spécialisée dans le pentesting (test d'intrusion) à destination des entreprises. Elle a été créée en mars 2020 par 2 associés. Le groupe est immatriculé à Bordeaux au sein de La Cité Numérique. Il possède aussi des locaux au Plessis-Robinson dans l'espace de coworking « La Canotière ». La start-up dispose également d'un site internet.

Locaux de Knock Knock, Le Plessis-Robinson, France.

B) Présentation du service

Knock Knock offre à ses clients une évaluation de la sécurité de leur système d'information, d'une application, d'un objet connecté etc désigné comme cible en effectuant des pentests (penetration testing), en français tests d'intrusion. Cette technique consiste à se mettre dans la peau de la menace, c'est-à-dire de l'attaquant.e, à tenter de s'introduire sur la cible et d'arpenter les chemins à même de conduire la « menace » vers les données qu'elles convoitent et/ou vers les niveaux de privilège qui lui permettraient de perturber le fonctionnement de la cible et des processus / activités métiers qu'elle sous-tend. Un test d'intrusion est conduit par un « pentester », une personne qui dispose des compétences et de la structure mentale lui permettant de se projeter dans la peau de la menace.

C) Présentation du projet

Tout au long de mon stage, j'ai eu pour mission de trouver à l'entreprise l'outil de simulation de SI/réseaux correspondant le plus à leurs attentes. Afin d'y parvenir, j'ai donc eu à réaliser un certain nombre de tâches.

D) Présentation de l'équipe

La start-up Knock Knock se compose de 3 équipiers :

Arthur : PDG de la start-up.
Léo : Directeur des Nouvelles Technologies et développeur spécialisé dans l'intelligence artificielle (IA).
Hadi : Directeur produit.

Arthur et Léo sont basés à Bordeaux. Seul Hadi est au Plessis-Robinson.

Durant ma période de stage, d'autres stagiaires étaient présents et s'occupaient de la partie développement informatique de la start-up.

II) EXPRESSIONS DES BESOINS

A) Description de l'existant

L'entreprise n'utilise actuellement aucun logiciel de simulation de réseau.

B) Liste des besoins

Avec les nombreux tests d'intrusion dans les SI (pentests) que réalisent l'entreprise, cette dernière a noté la nécessité/besoin d'utiliser des outils de simulation de réseaux. J'ai donc été amené à leur trouver l'outil qui correspond le plus à leurs attentes à travers la réalisation d'une veille et recherches.

C) Contraintes à respecter

Fonctionnelles : Sachant que l'outil doit pouvoir être malléable selon les besoins de l'entreprise, il nécessite donc d'être open source et gratuit.

Techniques : Le logiciel devra répondre à tous les critères techniques imposés par l'entreprise.

Ergonomiques : L'outil devra être le plus simple et agréable possible. Facile à utiliser. Je devrai donc éliminer les outils complexe d'utilisation.

D) Définition des ressources matérielles et logicielles

Au cours de mon stage, je disposais des ressources matérielles et logicielles suivantes :

- **Mon ordinateur portable personnel** fonctionnant sous macOS 11.2.3.

- **Slack** : C'est une plateforme de travail collaborative qui permet de rassembler les personnes, les informations pertinentes et les outils nécessaires à la réalisation de projets.

- **Packet Tracer** : Cisco Packet Tracer est un programme complet d'enseignement et de formation sur les technologies réseaux. Il offre une combinaison unique de simulations et de visualisations réalistes, d'évaluations, de fonctions pour la création d'activités et de possibilités de collaboration et de compétition multi-utilisateur.

- **Google Drive** : Service de stockage et de partage de fichiers dans le cloud lancé par la société Google.

- **Microsoft Excel** : Logiciel tableur de la suite bureautique Microsoft Office développé et distribué par l'éditeur Microsoft.

- **Microsoft Word** : Logiciel de traitement de texte publié par Microsoft.

- **Google Meet** : Google Meet est un service de visioconférence professionnel sécurisé développé par Google.

- **GitHub** : C'est un service web d'hébergement et de gestion de développement de logiciels. GitHub permet aux développeurs de stocker et de partager, publiquement ou non, le code qu'ils créent.

III) ANALYSE

A) Problème rencontré

La start-up n'utilisant pas encore de logiciel de simulation de réseaux/SI actuellement, elle cherche donc à trouver lequel est le plus adapté à son activité qui est le pentesting.

B) Description de la solution envisagée

De nos jours, il existe une multitude d'outils permettant la simulation de matériels réseau. Chaque entreprise spécialisée dans ce domaine en utilise un précis qui correspond à leurs attentes. Dans le cas de mon entreprise ils n'en n'ont pas encore. Afin de remédier à cela, j'ai donc été chargé, après de longues recherches et analyses, de leur présenter le logiciel qui leur conviendrait le mieux.

IV) RÉALISATION

A) Description des tâches

Dans le but d'arriver à l'objectif escompté, j'ai dû réaliser un grand nombre de tâches données par mon maître de stage.

Tâche 1 : Veille des outils de simulation de réseau

Ma première mission consistait à faire une veille regroupant tous les outils/logiciels de simulation de SI/réseau et leur description dans un tableur Excel. Pour y parvenir, j'ai donc utilisé le logiciel Microsoft Excel et réalisé de nombreuses recherches approfondies sur Internet.

A
Logiciel
Packet Tracer
GNS3
NetSim
Filius
SopiremInfoSR3
Simulateur de réseau local
Network-In!
Marionnet
EdrawMax
Huawaï eNSP
EVE-NG
Microsoft Visio
Junosphère Cloud
Cytra
Mininet

Tableur des différents logiciels de simulation de réseau

Tâche 2 : Ajout de critères

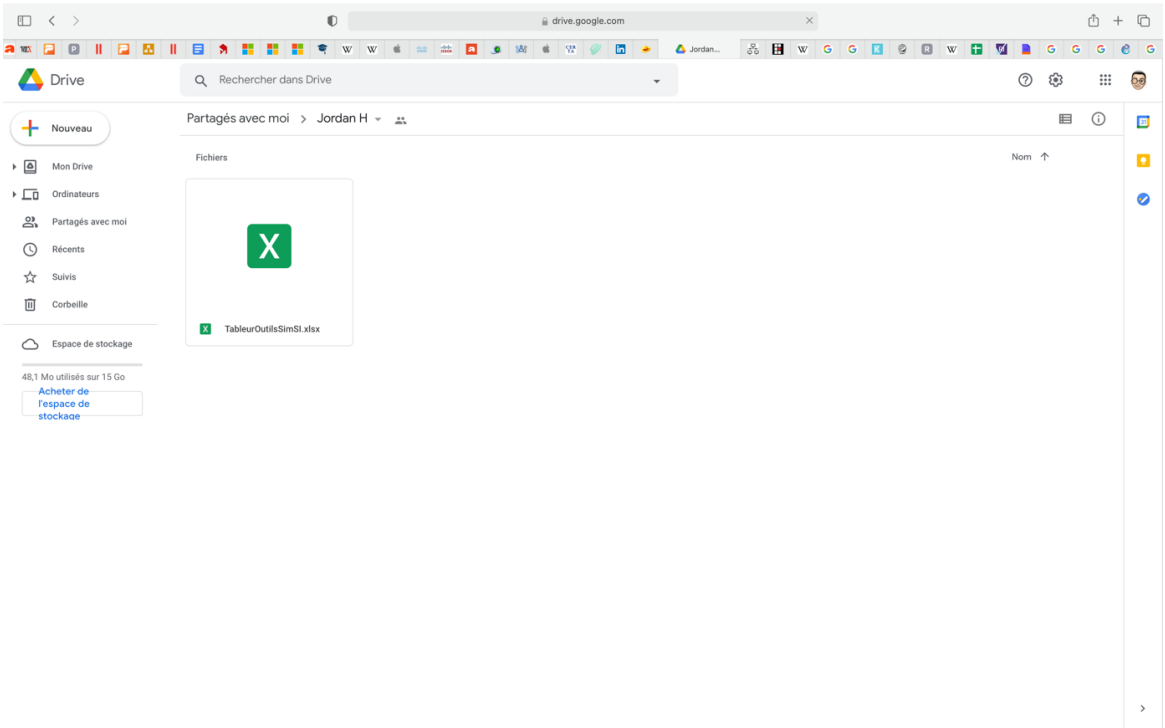
Ensuite, afin d'être le plus exhaustif possible j'ai dû ajouter certains critères tels que la raison sociale, l'origine, le prix, le type de licence pour les logiciels gratuits et un lien renvoyant vers chaque outil.

Logiciel	Raison sociale	Pays d'origine	Gratuit/Payant	Licence	Lien
Packet Tracer	Cisco Systems	Californie, USA	Gratuit	Licence propriétaire	https://www.netacad.com/fr/courses/packet-tracer
GNS3	GNS3 Technologies	Californie, USA	Gratuit	Usage commercial, modification	https://docs.gns3.com/docs/
NetSim	Boson Holdings	Nashville, USA	Payant		https://www.boson.com/netsim-cisco-network-simulator
Filius	University of Siegen	Haiger, DE	Gratuit	Licence GNU/GPL	https://em12d.ac-bordeaux.fr/disciplines/sti-college/2019/09/25/filius-un-logiciel-de-simulation-de-reseau-simple-et-acces
SopiremInfoSR3	SopiremInfo Dolata	Amiens, FR	Payant		http://www.sopireminfo.com
Simulateur de réseau local	Réseau CERTA	Dijon, FR	Gratuit	Licence non permissive	https://www.reseaucerta.org/?q=content/simulateur-de-réseau
Network-In!	Verdon Corp	FR	Gratuit	Licence GNU/GPL	http://network-in.vverdon.fr/index.php
Marionnet	Jean-Vincent Loddo	Paris, FR	Gratuit	Licence GNU/GPL	https://www.marionnet.org/site/index.php/fr/
EdrawMax	Wondershare Technology	Shenzen, CN	Payant		https://www.edrawsoft.com/fr/edraw-max/
Huawai eNSP	Huawei Technologies Co.Ltd.	Shenzen, CN	Gratuit	Licence non-connue	https://forum.huawei.com/enterprise/fr/4-raisons-pour-lesquelles-vous-devriez-utiliser-huawei-ensp/thread/610818-1003
EVE-NG	EVE-NG Ltd	Londres, UK	Payant		https://www.eve-ng.net
Microsoft Visio	Microsoft Corporation	Washington, USA	Payant		https://support.microsoft.com/fr-fr/office/vidéo-créer-un-diagramme-de-réseau-a2360cd9-5c9d-4839-b4f6-17b485e02262
Junosphère Cloud	Juniper Networks Inc.	Californie, USA	Payant		https://www.juniper.net/documentation/en_US/junosphere3.0/information-products/pathway-pages/junosphere/index.htm
Cytra	Beware Cyberlabs	Bordeaux, FR	Payant		https://beware-cyberlabs.eu/cytra-3/
Mininet	Mininet Project Contributors	USA	Gratuit	Licence BSD Open Source permissive	http://mininet.org

Élargissement du tableau avec l'ajout de critères

Tâche 3 : Partage sur le Drive

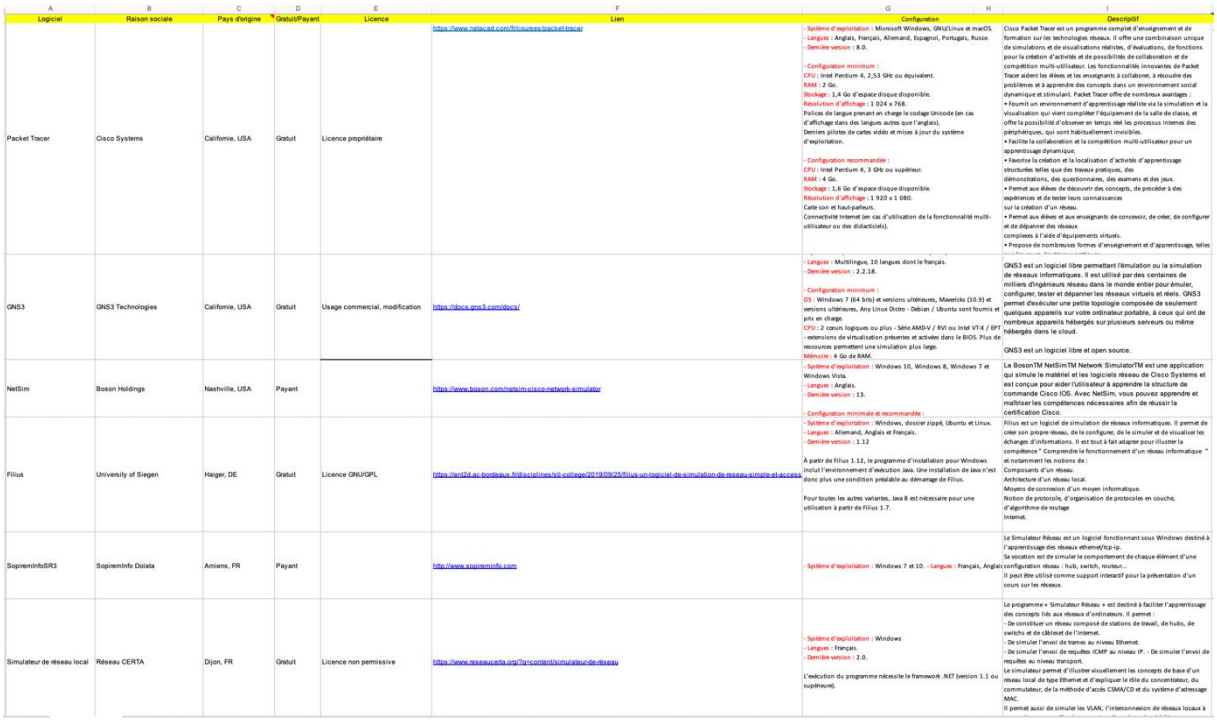
Une fois la mise en page des outils en tableur Excel perfectionnée, je l'ai partagée à mon tuteur grâce au logiciel Google Drive pour vérification.



Travail partagé sur Google Drive

Tâche 4 : Configuration et descriptif des outils

J'ai ensuite continué mon analyse des différents outils de simulation de réseaux sur tableur Excel en rajoutant une colonne « Configuration » qui va permettre de savoir quels sont les prérequis nécessaires afin de pouvoir utiliser l'outil et une colonne « Descriptif » présentant ce dernier. Toutes ces informations vont bien évidemment permettre à l'entreprise de savoir quel outil est le plus adapté à leurs besoins.



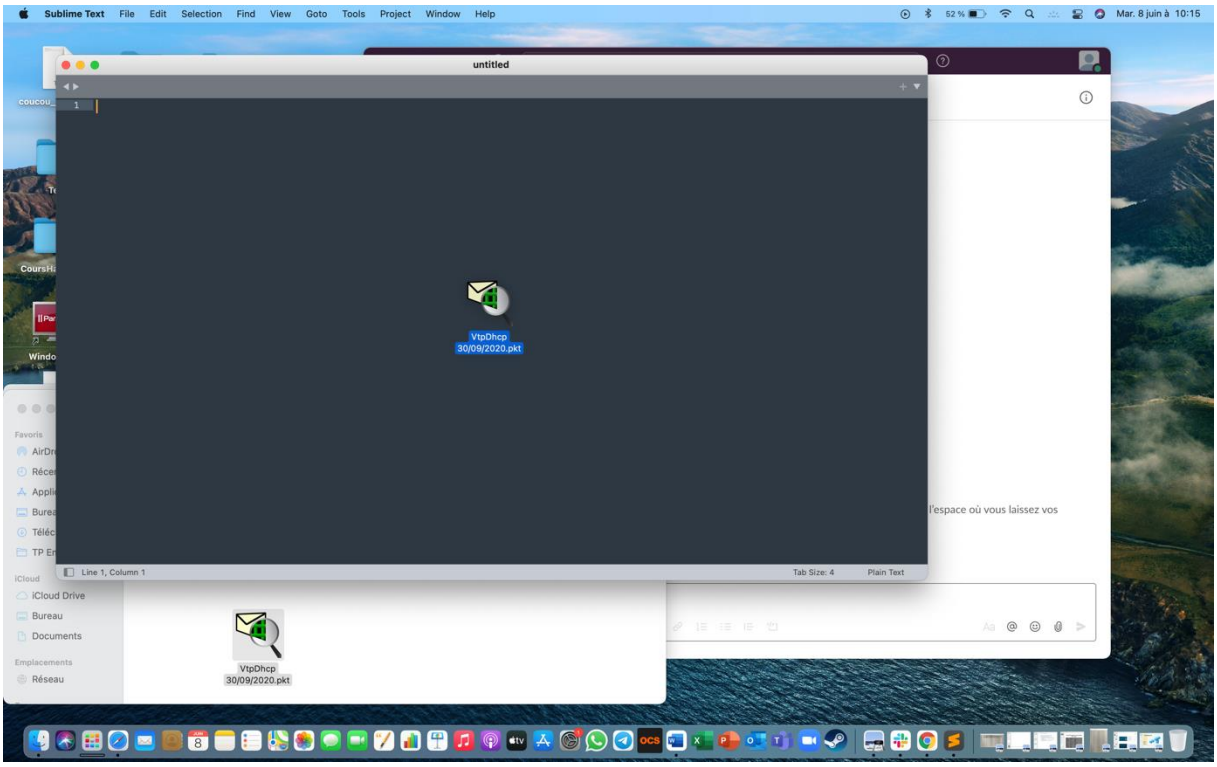
Logiciel	Raison sociale	Pays d'origine	Gratuit/Payant	Licence	Lien	Configuration	Descriptif
Packet Tracer	Cisco Systems	Californie, USA	Gratuit	Licence propriétaire	https://www.netacad.com/fr/courses/packet-tracer	- Système d'exploitation : Microsoft Windows, GNU/Linux et macOS. - Langues : Anglais, Français, Allemand, Espagnol, Portugais, Russe. - Dernière version : 8.0. - Configuration minimum : CPU : Intel Pentium 4, 2,53 GHz ou équivalent. RAM : 2 Go. Stockage : 1,4 Go d'espace disque disponible. Résolution d'affichage : 1 024 x 768. Polices de langue prenant en charge le codage Unicode (en cas d'affichage dans des langues autres que l'anglais). Derniers pilotes de cartes vidéo et mises à jour du système d'exploitation. - Configuration recommandée : CPU : Intel Pentium 4, 3 GHz ou supérieur. RAM : 4 Go. Stockage : 1,6 Go d'espace disque disponible. Résolution d'affichage : 1 920 x 1 080. Carte son et haut-parleurs. Connectivité Internet (en cas d'utilisation de la fonctionnalité multi-utilisateur ou des didacticiels).	Cisco Packet Tracer est un programme complet d'enseignement et de formation sur les technologies réseaux. Il offre une combinaison unique de simulations et de visualisations réalistes, d'évaluations, de fonctions pour la création d'activités et de possibilités de collaboration et de compétition multi-utilisateur. Les fonctionnalités innovantes de Packet Tracer aident les élèves et les enseignants à collaborer, à résoudre des problèmes et à apprendre des concepts dans un environnement social dynamique et stimulant. Packet Tracer offre de nombreux avantages : • Fournit un environnement d'apprentissage réaliste via la simulation et la visualisation qui vient compléter l'équipement de la salle de classe, et offre la possibilité d'observer en temps réel les processus internes des périphériques, qui sont habituellement invisibles. • Facilite la collaboration et la compétition multi-utilisateur pour un apprentissage dynamique. • Favorise la création et la localisation d'activités d'apprentissage structurées telles que des travaux pratiques, des démonstrations, des questionnaires, des examens et des jeux. • Permet aux élèves de découvrir des concepts, de procéder à des expériences et de tester leurs connaissances sur la création d'un réseau. • Permet aux élèves et aux enseignants de concevoir, de créer, de configurer et de dépanner des réseaux complexes à l'aide d'équipements virtuels. • Propose de nombreuses formes d'enseignement et d'apprentissage, telles
GNS3	GNS3 Technologies	Californie, USA	Gratuit	Usage commercial, modification	https://docs.gns3.com/docs/	- Langues : Multilingue, 10 langues dont le français. - Dernière version : 2.2.18. - Configuration minimum : OS : Windows 7 (64 bits) et versions ultérieures, Mavericks (10.9) et versions ultérieures, Any Linux Distro - Debian / Ubuntu sont fournis et pris en charge. CPU : 2 cœurs logiques ou plus - Série AMD-V / RVI ou Intel VT-X / EPT - extensions de virtualisation présentes et activées dans le BIOS. Plus de ressources permettent une simulation plus large. Mémoire : 4 Go de RAM.	GNS3 est un logiciel libre permettant l'émulation ou la simulation de réseaux informatiques. Il est utilisé par des centaines de milliers d'ingénieurs réseau dans le monde entier pour émuler, configurer, tester et dépanner les réseaux virtuels et réels. GNS3 permet d'exécuter une petite topologie composée de seulement quelques appareils sur votre ordinateur portable, à ceux qui ont de nombreux appareils hébergés sur plusieurs serveurs ou même hébergés dans le cloud. GNS3 est un logiciel libre et open source.
NetSim	Boson Holdings	Nashville, USA	Payant		https://www.boson.com/netsim-cisco-network-simulator	- Système d'exploitation : Windows 10, Windows 8, Windows 7 et Windows Vista. - Langues : Anglais. - Dernière version : 13. - Configuration minimale et recommandée :	Le BosonTM NetSimTM Network SimulatorTM est une application qui simule le matériel et les logiciels réseau de Cisco Systems et est conçue pour aider l'utilisateur à apprendre la structure de commande Cisco IOS. Avec NetSim, vous pouvez apprendre et maîtriser les compétences nécessaires afin de réussir la certification Cisco.
Filius	University of Siegen	Haiger, DE	Gratuit	Licence GNU/GPL	https://ent2d.ac-bordeaux.fr/disciplines/sti-college/2019/09/25/filius-un-logiciel-de-simulation-de-reseau-simple-et-access	- Système d'exploitation : Windows, dossier zippé, Ubuntu et Linux. - Langues : Allemand, Anglais et Français. - Dernière version : 1.12 À partir de Filius 1.12, le programme d'installation pour Windows inclut l'environnement d'exécution Java. Une installation de Java n'est donc plus une condition préalable au démarrage de Filius. Pour toutes les autres variantes, Java 8 est nécessaire pour une utilisation à partir de Filius 1.7.	Filius est un logiciel de simulation de réseaux informatiques. Il permet de créer son propre réseau, de le configurer, de le simuler et de visualiser les échanges d'informations. Il est tout à fait adapter pour illustrer la compétence " Comprendre le fonctionnement d'un réseau informatique " et notamment les notions de : Composants d'un réseau. Architecture d'un réseau local. Moyens de connexion d'un moyen informatique. Notion de protocole, d'organisation de protocoles en couche, d'algorithme de routage Internet.
SopireminfoSR3	SopireminfoDolata	Amiens, FR	Payant		http://www.sopireminfo.com	- Système d'exploitation : Windows 7 et 10. - Langues : Français, Anglais	Le Simulateur Réseau est un logiciel fonctionnant sous Windows destiné à l'apprentissage des réseaux ethernet/tcp-ip. Sa vocation est de simuler le comportement de chaque élément d'une configuration réseau : hub, switch, routeur... Il peut être utilisé comme support interactif pour la présentation d'un cours sur les réseaux.
Simulateur de réseau local	Réseau CERTA	Dijon, FR	Gratuit	Licence non permissive	https://www.reseauxcerta.org/?q=content/simulateur-de-reseau	- Système d'exploitation : Windows - Langues : Français. - Dernière version : 2.0. L'exécution du programme nécessite le framework .NET (version 1.1 ou supérieure).	Le programme « Simulateur Réseau » est destiné à faciliter l'apprentissage des concepts liés aux réseaux d'ordinateurs. Il permet : - De constituer un réseau composé de stations de travail, de hubs, de switchs et de câbleset de l'Internet. - De simuler l'envoi de trames au niveau Ethernet. - De simuler l'envoi de requêtes ICMP au niveau IP. - De simuler l'envoi de requêtes au niveau transport. Le simulateur permet d'illustrer visuellement les concepts de base d'un réseau local de type Ethernet et d'expliquer le rôle du concentrateur, du commutateur, de la méthode d'accès CSMA/CD et du système d'adressage MAC. Il permet aussi de simuler les VLAN, l'interconnexion de réseaux locaux à

Ajout d'une colonne configuration et descriptif

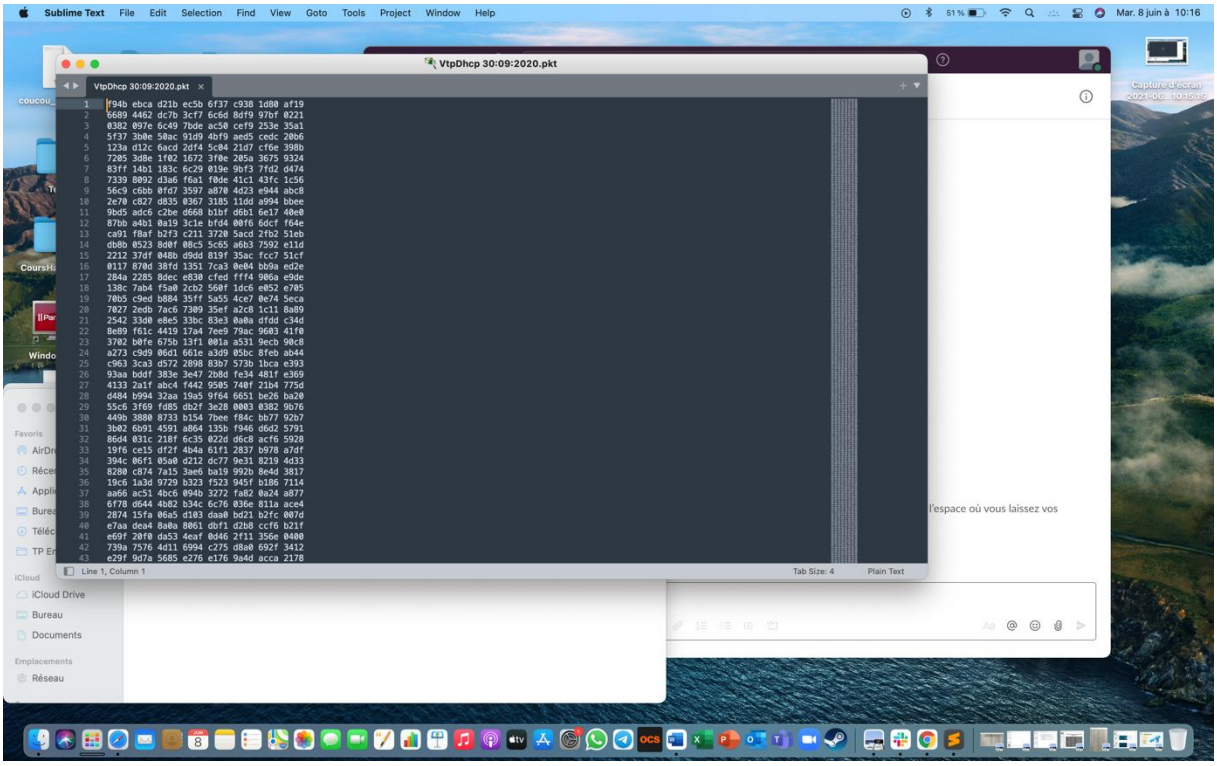
Tâche 5 : Interopérabilité des outils

La start-up souhaite utiliser un logiciel qui est interopérable, c'est-à-dire la capacité que possède un produit ou un système, dont les interfaces sont intégralement connues, à fonctionner avec d'autres produits ou systèmes existants ou futurs et ce sans restriction d'accès ou de mise en œuvre. Ce processus passe par plusieurs étapes :
1) Voir sous quelle forme ces outils enregistrent les topologies de réseaux.
2) Est-ce que l'outil donne accès à ces fichiers ? Dans l'affirmative, sous quel format lisible (xml, ...) ?
3) Et comment sont-ils structurés ?

J'ai donc dû faire des tests et recherches approfondies sur le Web pour en savoir plus.

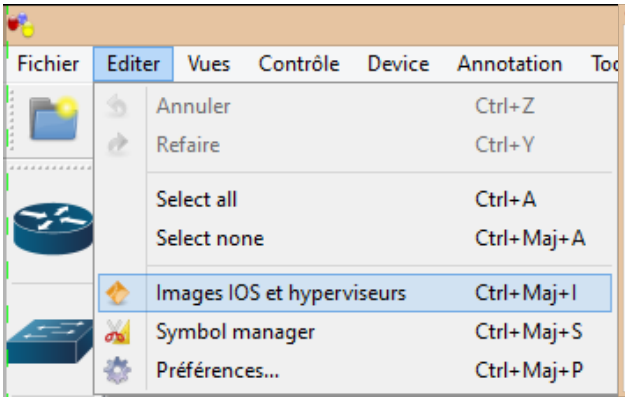


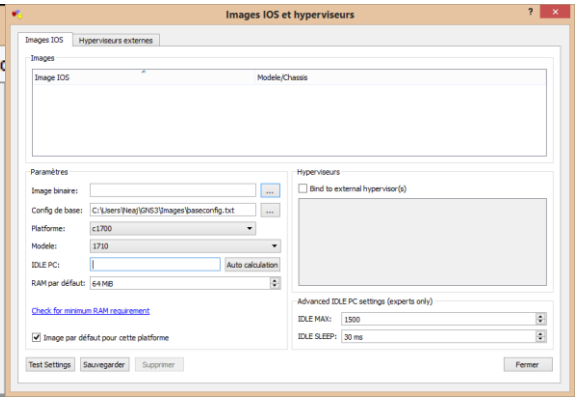
Test d'interopérabilité du logiciel Packet Tracer dans un éditeur de texte (ici Sublime Text).



Données du ficher illisibles donc le logiciel Packet Tracer n'est pas interopérable.

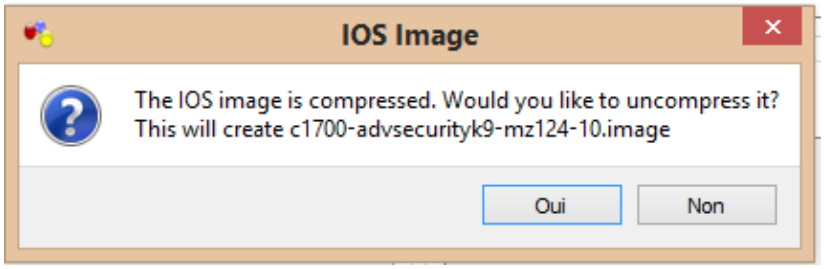
Test d'interopérabilité du logiciel GNS3 avec une IOS Cisco :



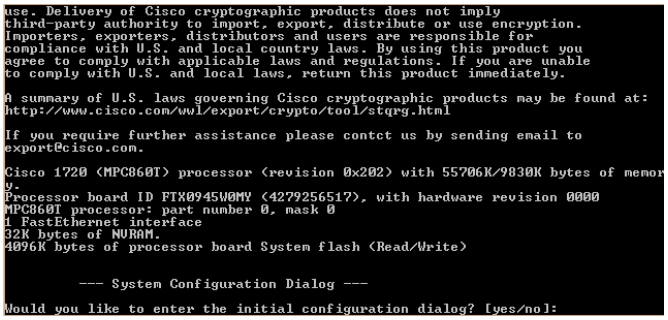


Paramétrage des images IOS

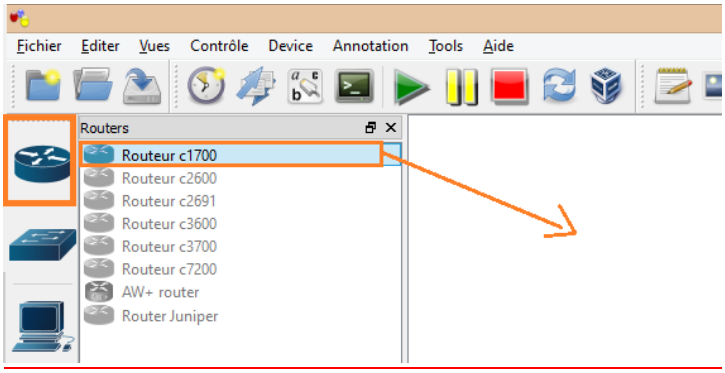
Fenêtre permettant de gérer les IOS Cisco



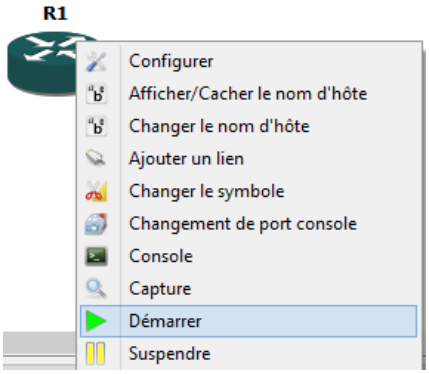
Demande de décompression de l'image IOS



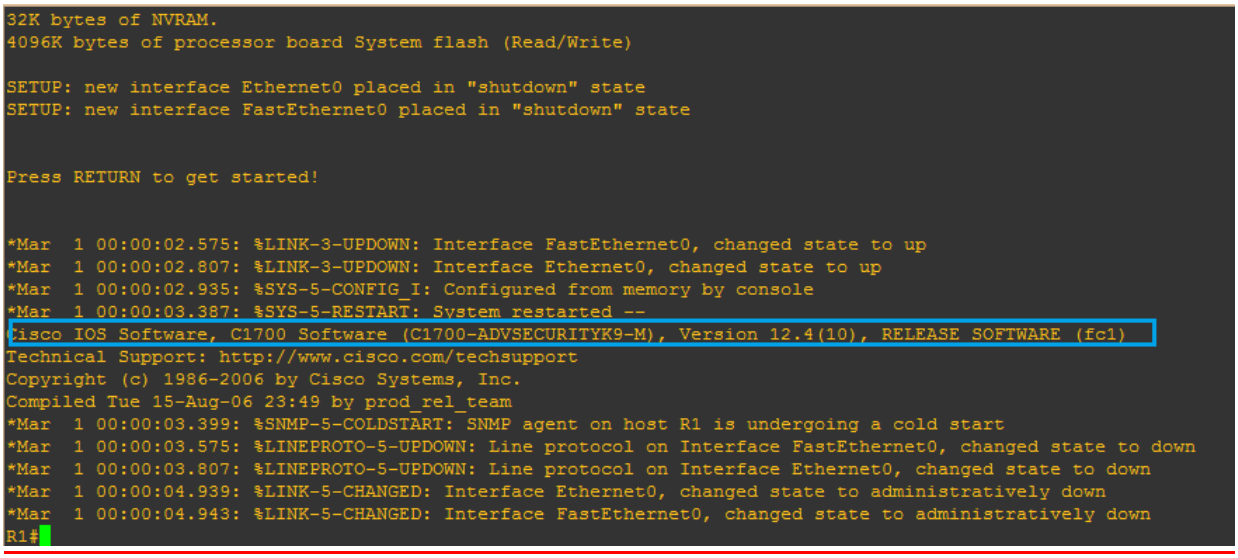
Démarrage test de
l'image IOS Cisco importée



Intégration d'un routeur dans le schéma du réseau virtuel GNS3



Démarrage du
routeur virtuel

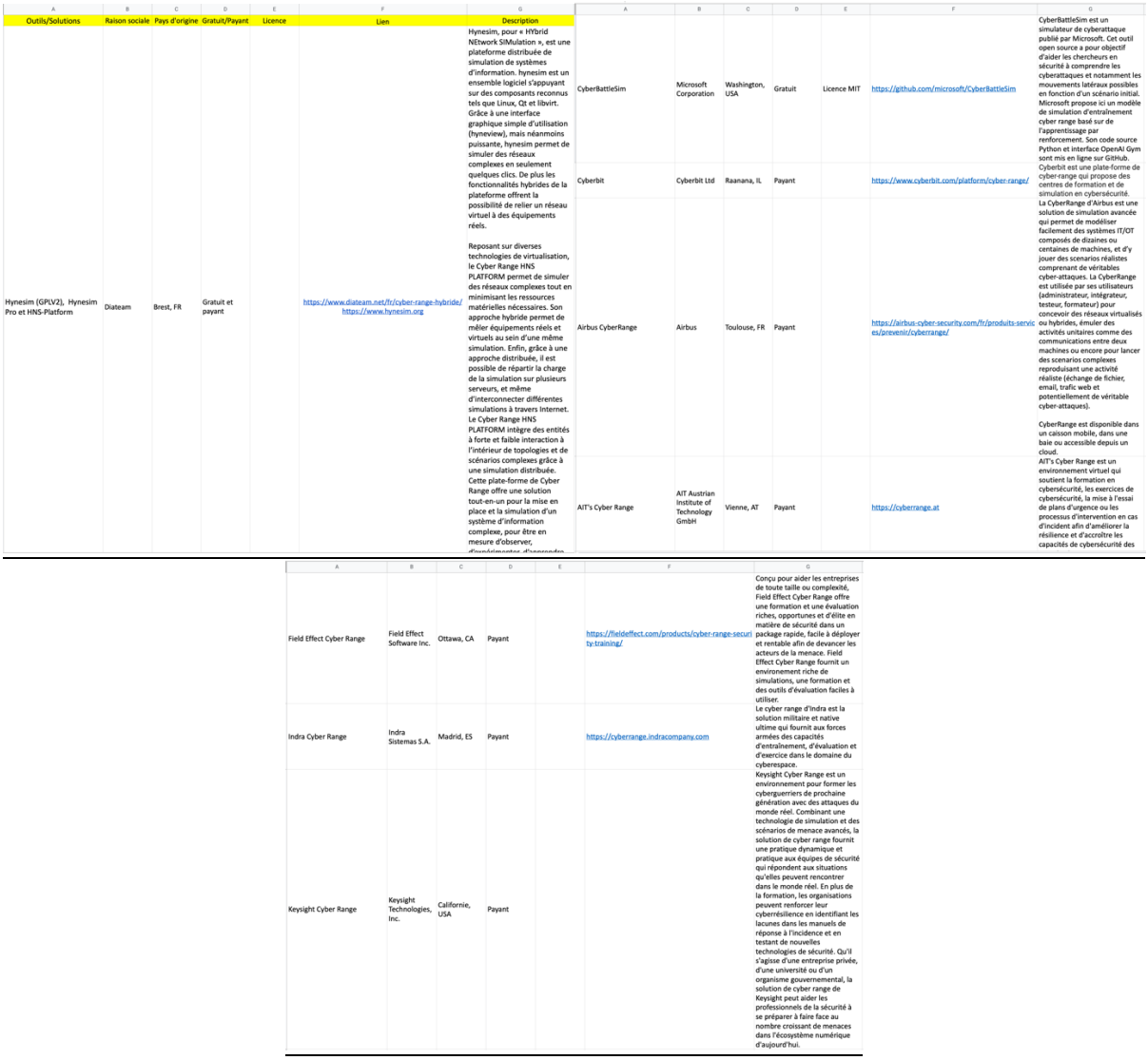


Vue terminale du routeur démarré

Le logiciel de simulation réseau GNS3 est donc interopérable.

Tâche 6 : Benchmark des outils de cyber-range

À la suite de mon travail sur les logiciels de simulation réseau, j'ai eu à réaliser un benchmark aux outils de cyber-range.
Qu'est-ce que le cyber-range ?
Un Cyber Range est un environnement virtuel qui permet aux organisations et plus précisément aux équipes de sécurité informatique d'une entreprise de simuler des entraînements aux combats cyber en jouant des scenarios réalistes comprenant de véritables cyber-attaques. De plus, le Cyber Range facilite le développement, les tests et l'évaluation des solutions systèmes/réseaux.



Outils/Solutions	Raison sociale	Pays d'origine	Gratuit/Payant	Licence	Lien	Description
Hynesim (GPLV2), Hynesim Pro et HNS-Platform	Diateam	Brest, FR	Gratuit et payant		https://www.diateam.net/fr/cyber-range-hybride/ https://www.hynesim.org	Hynesim, pour « HYbrid NEtwork SIMulation », est une plateforme distribuée de simulation de systèmes d'information. hynesim est un ensemble logiciel s'appuyant sur des composants reconnus tels que Linux, Qt et libvirt. Grâce à une interface graphique simple d'utilisation (hyneview), mais néanmoins puissante, hynesim permet de simuler des réseaux complexes en seulement quelques clics. De plus les fonctionnalités hybrides de la plateforme offrent la possibilité de relier un réseau virtuel à des équipements réels. Reposant sur diverses technologies de virtualisation, le Cyber Range HNS PLATFORM permet de simuler des réseaux complexes tout en minimisant les ressources matérielles nécessaires. Son approche hybride permet de mêler équipements réels et virtuels au sein d'une même simulation. Enfin, grâce à une approche distribuée, il est possible de répartir la charge de la simulation sur plusieurs serveurs, et même d'interconnecter différentes simulations à travers Internet. Le Cyber Range HNS PLATFORM intègre des entités à forte et faible interaction à l'intérieur de topologies et de scénarios complexes grâce à une simulation distribuée. Cette plate-forme de Cyber Range offre une solution tout-en-un pour la mise en place et la simulation d'un système d'information complexe, pour être en mesure d'observer,
CyberBattleSim	Microsoft Corporation	Washington, USA	Gratuit	Licence MIT	https://github.com/microsoft/CyberBattleSim	CyberBattleSim est un simulateur de cyberattaque publié par Microsoft. Cet outil open source a pour objectif d'aider les chercheurs en sécurité à comprendre les cyberattaques et notamment les mouvements latéraux possibles en fonction d'un scénario initial. Microsoft propose ici un modèle de simulation d'entraînement cyber range basé sur de l'apprentissage par renforcement. Son code source Python et interface OpenAI Gym sont mis en ligne sur GitHub.
Cyberbit	Cyberbit Ltd	Raanana, IL	Payant		https://www.cyberbit.com/platform/cyber-range/	Cyberbit est une plate-forme de cyber-range qui propose des centres de formation et de simulation en cybersécurité.
Airbus CyberRange	Airbus	Toulouse, FR	Payant		https://airbus-cyber-security.com/fr/produits-services/prevenir/cyberrange/	La CyberRange d'Airbus est une solution de simulation avancée qui permet de modéliser facilement des systèmes IT/OT composés de dizaines ou centaines de machines, et d'y jouer des scenarios réalistes comprenant de véritables cyber-attaques. La CyberRange est utilisée par ses utilisateurs (administrateur, intégrateur, testeur, formateur) pour concevoir des réseaux virtualisés ou hybrides, émuler des activités unitaires comme des communications entre deux machines ou encore pour lancer des scenarios complexes reproduisant une activité réaliste (échange de fichier, email, trafic web et potentiellement de véritable cyber-attaques). CyberRange est disponible dans un caisson mobile, dans une baie ou accessible depuis un cloud.
AIT's Cyber Range	AIT Austrian Institute of Technology GmbH	Vienne, AT	Payant		https://cyberrange.at	AIT's Cyber Range est un environnement virtuel qui soutient la formation en cybersécurité, les exercices de cybersécurité, la mise à l'essai de plans d'urgence ou les processus d'intervention en cas d'incident afin d'améliorer la résilience et d'accroître les capacités de cybersécurité des
Field Effect Cyber Range	Field Effect Software Inc.	Ottawa, CA	Payant		https://fieldeffect.com/products/cyber-range-security-training/	Conçu pour aider les entreprises de toute taille ou complexité, Field Effect Cyber Range offre une formation et une évaluation riches, opportunes et d'élite en matière de sécurité dans un package rapide, facile à déployer et rentable afin de devancer les acteurs de la menace. Field Effect Cyber Range fournit un environement riche de simulations, une formation et des outils d'évaluation faciles à utiliser.
Indra Cyber Range	Indra Sistemas S.A.	Madrid, ES	Payant		https://cyberrange.indracompany.com	Le cyber range d'Indra est la solution militaire et native ultime qui fournit aux forces armées des capacités d'entraînement, d'évaluation et d'exercice dans le domaine du cyberespace.
Keysight Cyber Range	Keysight Technologies, Inc.	Californie, USA	Payant			Keysight Cyber Range est un environnement pour former les cyberguerriers de prochaine génération avec des attaques du monde réel. Combinant une technologie de simulation et des scénarios de menace avancés, la solution de cyber range fournit une pratique dynamique et pratique aux équipes de sécurité qui répondent aux situations qu'elles peuvent rencontrer dans le monde réel. En plus de la formation, les organisations peuvent renforcer leur cyberrésilience en identifiant les lacunes dans les manuels de réponse à l'incidence et en testant de nouvelles technologies de sécurité. Qu'il s'agisse d'une entreprise privée, d'une université ou d'un organisme gouvernemental, la solution de cyber range de Keysight peut aider les professionnels de la sécurité à se préparer à faire face au nombre croissant de menaces dans l'écosystème numérique d'aujourd'hui.

Tableur détaillé des outils et solutions de cyber-range.

B) Solution choisie

L’outils de simulation qui a donc été retenu est GNS3. Ce-dernier répond le plus aux attentes de l’entreprise car c’est un logiciel complet qui possède de nombreux avantages :

- Gratuit et open source.
- Installation simple et rapide.
- Interopérable.
- Facile d’utilisation.
- Pas de frais de licence mensuels ou annuels.
- Aucune limitation du nombre d'appareils pris en charge.
- Peut être exécuté avec ou sans hyperviseurs.
- Simulation réseau en temps réel pour les tests de prédéploiement sans avoir besoin de matériel réseau.
- Se connecte à n'importe quel réseau réel.
- Permet de tester et estimer, dans des conditions quasi réelles et sans avoir à financer le matériel, les configurations et réseaux avant de les mettre en place physiquement.

V) RÉUNIONS

Pendant mon stage, j'ai eu l'occasion d'assister à plusieurs réunions toutes en visioconférence traitant de différents sujets en rapport avec l'activité de la start-up. Pour cela, l'entreprise utilise Google Meet.

A) Réunion de présentation

Lors de mon 1er jour au sein de la start-up, mon tuteur a organisé une réunion avec ces 2 autres associés afin de me présenter l'entreprise, son activité etc. Cela a été l'occasion pour moi de me familiariser avec le vocabulaire de base.

1/ Le pentest

L'objectif d'un pentest est d'évaluer le niveau de sécurité d'une infrastructure, d'un service web ou encore d'un site e-commerce. Pour cela, l'auditeur (ou communément appelé pentester ou ethical hacker), va tester la cible en simulant des attaques réelles.

On distingue 2 modes de pentest :

Externe : Ce type d'audit peut être réalisé sur des cibles externes de l'entreprise (sites web accessibles sur internet, API publiques…). Le pentester réalise ses tests à distance, depuis une simple connexion internet. Il simulera des attaques d'acteurs malveillants, de manière anonyme.

Interne : Il peut être aussi réalisé en interne, depuis les locaux de l'entreprise. Dans ce contexte, le pentester simulera des actions malveillantes depuis l'intérieur de l'entreprise. Le but est de mesurer le risque de compromission par un collaborateur, un partenaire ou un prestataire de l'entreprise.

2/ Approches de pentest

Lors d'un audit de sécurité, trois approches sont possibles. Elles correspondent à différents niveaux d'information et d'accès fournis aux pentesters.

Black Box : Une approche « Black Box » ou « Boîte Noire » consiste à évaluer le niveau de sécurité de la cible **en ne disposant d'aucune information**, tel un hacker découvrant pour la première fois ce système. Dans un tel contexte, l'auditeur se positionne comme n'importe quel acteur malveillant. Ce type d'approche nécessite de la méthodologie et du temps pour explorer la cible.

Grey Box : Une approche « Grey Box » ou « Boîte Grise » consiste, quant à elle, **à tenter de s'introduire dans le système d'informations en disposant d'un nombre limité d'informations** sur l'organisation et son système. Ce cas permet de vérifier les failles d'un système en se positionnant soit en tant que collaborateur de l'entreprise ayant accès en interne à quelques informations, soit en tant que point de départ d'un hacker qui aurait réussi à avoir accès à un compte utilisateur au sein de l'organisation.

White Box : Une approche « White Box » ou « Boîte Blanche » se traduit par le fait que **le pentester a accès à la totalité des informations concernant le système.** Le testeur travaille dans ce cas en collaboration avec les équipes techniques de l'organisation afin de récupérer un maximum d'informations utiles. Il a accès à tout ce dont il a besoin **afin de détecter un maximum de vulnérabilités.**

Schéma illustrant le principe des 3 approches de pentest

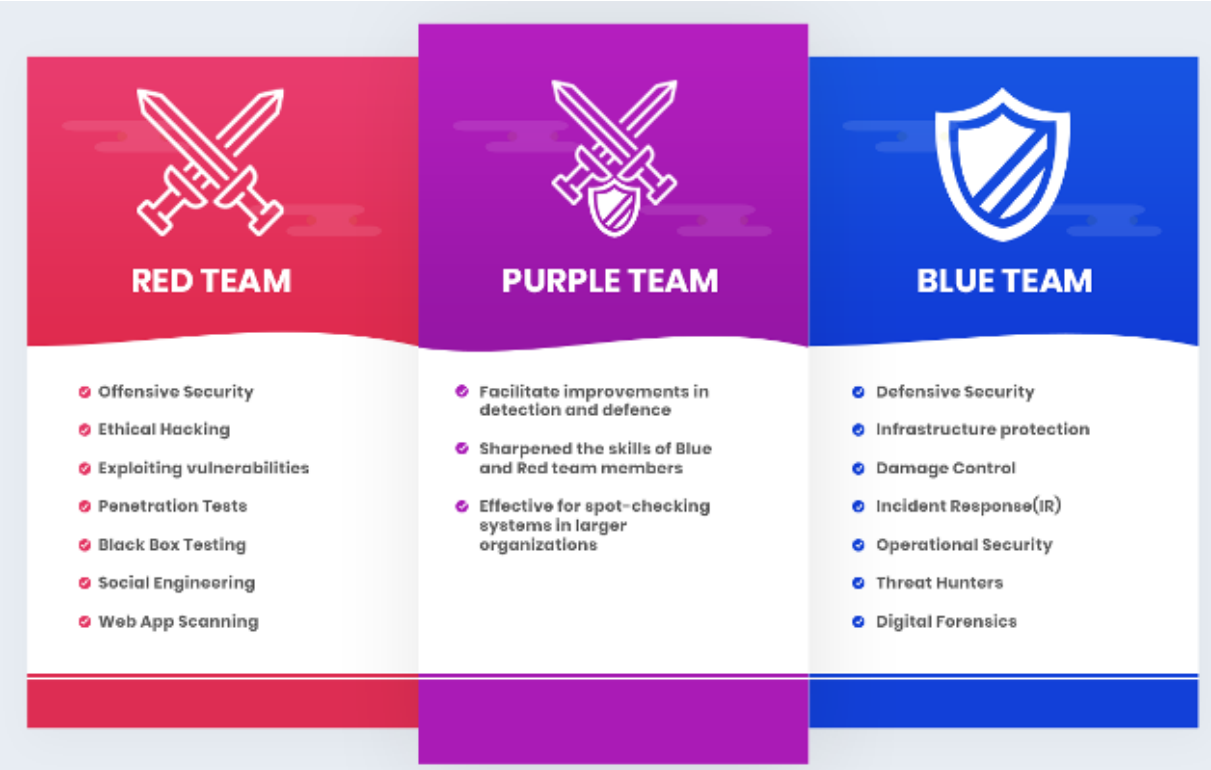
3/ Les 3 types d'équipe

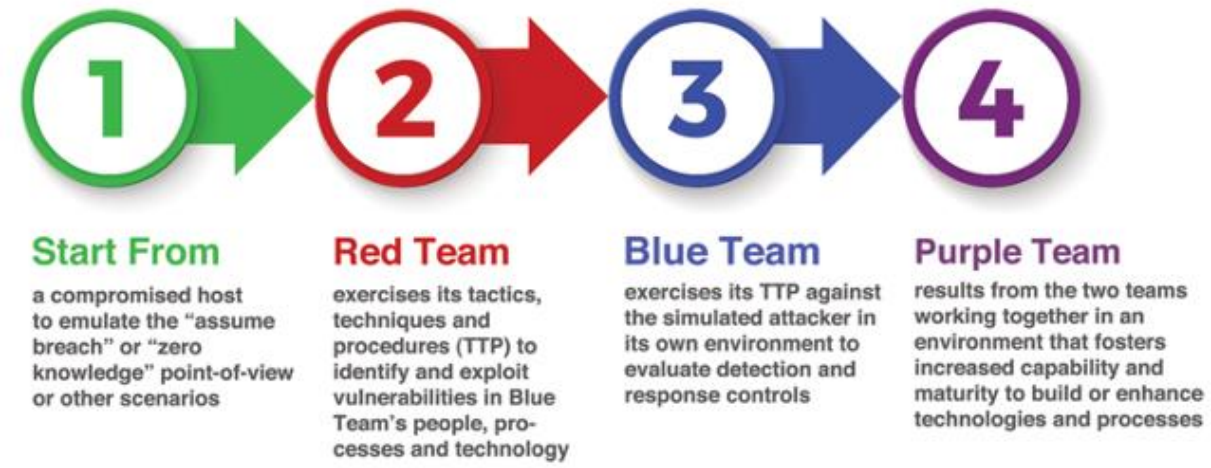
Les tests d'intrusion sont généralement limités dans le temps. C'est pourquoi il faut monter 3 équipes pour minimiser le temps des tests tout en maximisant les compétences de chacun.

Red Team : La « Red Team » ou « Équipe Rouge » a pour objectif de simuler le scénario où un pirate souhaiterait pénétrer le système d'information d'une entreprise ou d'une institution sans limite de temps, ni de périmètre. Leur but est de détecter, prévenir et éliminer les vulnérabilités. Les tests red team se déroulent sur une période de temps plus longue qu'un test d'intrusion normal (2 à 3 mois, contre 1 à 2 semaines) et n'ont pas de périmètre précis défini par le commanditaire (le testeur démarre avec uniquement le nom de l'entreprise). Nous sommes donc dans une approche offensive.

Blue Team : La « Blue Team » ou « Équipe Bleu » effectue une analyse des systèmes d'information pour assurer la sécurité, identifier les failles de sécurité, vérifier l'efficacité de chaque mesure de sécurité et veiller à ce que toutes les mesures de sécurité continuent d'être efficaces après leur mise en œuvre. Elle se doit de réagir face aux attaquants. Nous sommes donc ici dans une approche défensive.

Purple Team : La « Purple Team » ou « Équipe Violette » est le résultat de la collaboration entre la Blue Team et la Red Team. Elle consiste à aligner les objectifs Red Team et Blue Team pour améliorer la défense du SI en créant une coopération vertueuse. Elle conduit des tests d'intrusions de type Red Team dans le but de favoriser l'entrainement de l'équipe Blue Team. Elle a ses propres objectifs et vise à améliorer les capacités de détection de l'équipe Blue Team.





Fonctionnement des 3 types d'équipe

B) Réunions hebdomadaires

Tous les lundis, les 3 dirigeants de la start-up ont l'habitude de faire une réunion de 1h30 en moyenne. Celle-ci a pour but de faire le point sur la semaine passée (debriefing) et celle à venir (briefing) à travers une synchronisation du plan d'action. Ce dernier récapitule étape par étape l'avancée des tâches exécutées et à exécuter pour chaque domaine entourant la start-up (marketing, comptabilité, informatique, légal, etc). Cette réunion est aussi importante pour moi car elle me permet de faire le point sur ma semaine passée, mes tâches accomplies, et définir celles à accomplir lors de la prochaine semaine.

C) Réunion fiche de vulnérabilité

Au cours de cette réunion de 1h, il m'a été présenté une fiche de vulnérabilité réalisée par la start-up elle-même. Pour des raisons de confidentialité la fiche n'étant pas encore disponible publiquement, je ne peux donc pas l'inclure ici. Cette fiche était centrée sur une vulnérabilité particulière : le Cross-site scripting.

Cross-site scripting

1/ Qu'est-ce que c'est ?

Le cross-site scripting (abrégé XSS) est un type de faille de sécurité des sites web permettant d'injecter du contenu dans une page, provoquant ainsi des actions sur les navigateurs web visitant la page. Les possibilités des XSS sont très larges puisque l'attaquant peut utiliser tous les langages pris en charge par le navigateur (JavaScript, Java...) et de nouvelles possibilités sont régulièrement découvertes notamment avec l'arrivée de nouvelles technologies comme HTML5. Il est par exemple possible de rediriger vers un autre site pour de l'hameçonnage ou encore de voler la session en récupérant les cookies

2/ Principe

Le principe est d'injecter des données arbitraires dans un site web, par exemple en déposant un message dans un forum, ou par des paramètres d'URL. Si ces données arrivent telles quelles dans la page web transmise au navigateur (par les paramètres d'URL, un message posté…) sans avoir été vérifiées, alors il existe une faille : on peut s'en servir pour faire exécuter du code malveillant en langage de script (du JavaScript le plus souvent) par le navigateur web qui consulte cette page.

La détection de la présence d'une faille XSS peut se faire par exemple en entrant un script Javascript dans un champ de formulaire ou dans une URL :

```
<script>alert('bonjour')</script>
```

Si une boîte de dialogue apparaît, on peut en conclure que l'application Web est sensible aux attaques de type XSS.

3/ Risques

L'exploitation d'une faille de type XSS permettrait à un intrus de réaliser les opérations suivantes :
- Redirection (parfois de manière transparente) de l'utilisateur (souvent dans un but d'hameçonnage).
- Vol d'informations, par exemple sessions et cookies.
- Actions sur le site faillible, à l'insu de la victime et sous son identité (envoi de messages, suppression de données…).
- Rendre la lecture d'une page difficile (boucle infinie d'alertes par exemple).

Nous avons aussi abordé les notions de « User Story » (US) ou « Récit utilisateur » et « Evil User Story » (EUS).

User Story : Un récit utilisateur, ou « User Story » (US) en anglais, est une description simple d'un besoin ou d'une attente exprimée par un utilisateur et utilisée dans le domaine du développement de logiciels et de la conception de nouveaux produits pour déterminer les fonctionnalités à développer. Généralement, la story est rédigée par le Product Owner, le responsable produit ou le responsable de programme avant d'être soumise pour revue.

Evil User Story : Une Evil User Story (EUS) décrit la réalisation d'un scénario de risque à travers l'identification d'une source de risque (attaquant externe / collaborateur malveillant), exploitant une vulnérabilité, occasionnant un impact sur la valeur métier. Elles sont rédigées par les équipes sécurité.
Pour chaque EUS, des mesures de sécurité (Security User Stories) permettant de mitiger les risques sont identifiées et intégrées au backlog.

Les **User Stories** sont les exigences logicielles **centrées sur la valeur** exprimées en **conversation** par les utilisateurs	*« En tant que **(rôle utilisateur)**, je veux **(activité)**, afin de **(valeur métier)** »*
	« En tant qu'**utilisateur**, je veux **renseigner mes identifiants**, afin **de me connecter à l'application**»
Les **Evil User Stories** mettent en évidence l'impact métier d'une activité malveillante ciblant le produit	*« En tant que **(utilisateur malveillant)**, je veux **(activité malveillante)**, afin de **(impact métier)** »*
	« En tant qu'**attaquant**, je veux **essayer de deviner le mot de passe d'un utilisateur** en envoyant de très nombreuses requêtes d'authentification en parallèle **pour me connecter à sa session** »
Les **Security User Stories** décrivent les mesures de sécurité à implémenter pour mitiger les risques.	*« En tant que **(rôle squad)**, je veux **(activité)**, afin de **(éviter qu'un evil user story se produise)** »*
	« En tant que **développeur**, je veux **mettre en place un mécanisme de blocage des comptes utilisateurs** après 5 tentatives **pour éviter les attaques par bruteforce**

Tableau explicatif des notions de User Story et Evil User Story

Ces notions sont importantes et fondamentales dans le cadre de la relation qu'entretient la start-up envers ses clients. En effet, elles permettent de savoir quels sont les besoins de ces derniers, leurs attentes et aussi d'exprimer les intentions d'un utilisateur malveillant.

D) Réunion définition du besoin de virtualisation/simulation

Lors de cette réunion, nous avons étudié en détail les objectifs à remplir grâce à la virtualisation/simulation. Nous en avons relevé plusieurs : le clonage de SI clients, la récupération d'environnements de simulation / pré-prod déjà implémentés dans des outils équivalents, la validation de la performance des outils de pentest, la montée en compétence manuelle sur les outils de hacking etc. Parmi tous les objectifs étudiés, nous en avons priorisé certains. Puis, afin d'arriver à atteindre ces objectifs, 2 axes à travailler ont été défini :

- La diversité et la représentativité des SI simulés.
- L'interopérabilité des outils.

CONCLUSION

Cette première expérience dans le monde de l'entreprise a été très enrichissante pour moi et m'a permis de découvrir plus en profondeur le domaine de l'informatique après 1 an d'apprentissage. J'ai pu en apprendre plus sur le secteur que j'affectionne tout particulièrement : le réseau et la cybersécurité.

Tout au long de mon stage j'ai dû faire face à certaines difficultés qui ne m'étaient pas venu à l'esprit de prendre en considération. Des difficultés que je n'avais jamais rencontrées auparavant en classe. Cela m'a donc permis de comprendre plus en détail certaines notions avec lesquelles je n'étais pas familiarisé.

Ce stage a été également l'occasion pour moi de travailler en équipe ainsi qu'en toute autonomie afin de parvenir aux objectifs visés. J'ai pu acquérir de nouvelles connaissances et compétences et aussi partager les miennes au sein de l'entreprise.

De plus, grâce à ce stage j'ai pu ressentir une certaine responsabilité du fait de la petite taille de l'entreprise.

Enfin, cette expérience m'a permis de mieux cibler mes futures appétences professionnelles. Travailler dans une start-up comme Knock-Knock me conviendrait en tout point. Les tâches que j'ai eu à réaliser m'ont conforté dans l'idée que j'aimerai travailler dans le domaine du réseau et de la cybersécurité.