

# Projet Annuel

## **Botnet**

ESGI - BACHELOR SÉCURITÉ INFORMATIQUE (3JSI)

### **Groupe :**

- Nicolas TORRES-SANNIER
- Julien DELAUNAY
- Alexy DA COSTA

# Table des matières

<b>Table des matières</b>	<b>2</b>
<b>Présentation du projet</b>	<b>4</b>
Contributeurs	4
Contexte	4
Livrable	4
Objectifs	5
<b>Contraintes</b>	<b>6</b>
Techniques	6
Architecture réseau	6
Logiciel	8
Légales	8
<b>Users stories</b>	<b>9</b>
<b>Schémas</b>	<b>19</b>
Maquette du site web	19
Connexion	19
Accueil	20
Attaque x	21
Consultation des données collectées	22
Consultation des statistiques	23
Base de données	24
MCD	24
MLD	25
Infrastructure réseaux	26
Schéma Logique	26
Schéma Technique (Infra de test)	26
Schéma Technique (condition réelle minimum d'une infrastructure)	27
Processus	27
Légende	27
Choisir une attaque	28
Consultation des données collectées	28
Dashboard statistiques	29
Accès CLI (Reverse Shell)	29
Mise à jour des zombies	30
Suppression des traces	30
Collecte d'informations	31

Bomb Fork	31
Vidéo/son faisant peur	32
Brute Force	32
Relayage de phishing/spam	33
Minage de cryptomonnaie	33
Cookie Jacking	34
<b>Référentiels</b>	<b>34</b>
Liens	34
Ressources	35
Risques	36
Organisation du temps	36
Répartition du travail	37
Rôles	37
Tâches	38
Feuille de route Jira	39
Backlog de l'épic "Remise à niveau des connaissances"	40

## Présentation du projet

### Contributeurs

- Nicolas TORRES
- Julien DELAUNAY
- Alexy DA COSTA

### Contexte

Ce projet représente notre Projet Annuel du Bachelor Sécurité Informatique de l'ESGI.

Tous passionnés par la SI et souhaitant approfondir de façon significative nos connaissances en :

- Programmation
- Réseaux
- Système
- Cybersécurité

Nous avons trouvé judicieux de choisir de réaliser un Botnet de A à Z, majoritairement from scratch. Cela, car pour y parvenir nous aurons besoin d'un panel de connaissances large touchant à ses 4 domaines.

### Livrable

Botnet comportant :

1. Une application web (C&C) permettant d'envoyer une demande d'instruction sur des zombies (réseau de machines distantes infectés), de visualiser un Dashboard de statistiques, ainsi que de consulter les données volées
2. Un Malware installé sur chaque zombies permettant d'attaquer les zombies ainsi que des victimes tiers

## Objectifs

1. **Délai** : Respecter les délais de chaque Sprint, Epic
2. **Qualité** : Rendre un code propre/fonctionnel, un site web intuitif et une infrastructure réseau relativement sécurisée
3. **Personnel** : Augmenter de façon significative nos compétences en programmation, réseaux, système et cybersécurité, ainsi qu'en méthodologie/gestion de projet.

## Méthodologie utilisée

La méthodologie que nous utilisons est Scrum.

## Contraintes

## Techniques

### Architecture réseau

Hostname	Nom réseau	Services	OS	IP
pc-attaquant	Réseau Attaquant		Ubuntu	172.16.0.1
pfsense1	Réseau Attaquant	HTTPS, Packet Filter	PfSense	LAN : 172.16.0.254  WAN : 172.16.10.1
pfsense2	Réseau Attaquant	HTTPS, Packet Filter	PfSense	LAN : 172.16.20.2  WAN : 172.16.30.1
serveur-c&c	Réseau Attaquant	HTTPS, SFTP, MySQL, PhpMyAdmin	Arch Linux	LAN : 172.16.10.2  WAN : 172.16.20.1
routeur1	Réseau Attaquant		Arch Linux	LAN : 172.16.30.2  WAN : 10.10.0.1

routeur2	Réseau Zombies		Arch Linux	LAN : 10.10.0.254  WAN : 10.10.0.2
routeur3	Réseau Victimes		Arch Linux	LAN : 192.168.0.254  WAN : 10.10.0.3
zombie1	Réseau Zombies		Windows 10	10.0.0.1
zombie2	Réseau Zombies		Windows 10	10.0.0.2
zombie3	Réseau Zombies		Windows 10	10.0.0.3
victime1	Réseau Victime		Windows 10	192.168.1.1

## Logiciel

Nom du logiciel	Architecture	Langages	Spécificité
Serveur C&C	MVC	HTML, Bootstrap, Python, Django, D3.js, MySQL	Programmation haut niveau web, répartie et réseau
Malware	C : fichiers .h include dans fichiers .c, procédural  Python : Héritage, séparation par module	C et/ou Python, PowerShell	C : Programmation bas niveau, répartie et réseau  Python : Programmation haut niveau, répartie et réseau

## Légales

1. Interdiction de partager le code source en public ou en privé.
2. Interdiction d'utiliser le Botnet dans un environnement autre que celui de test.



## Users stories

Fonction	Connexion
En tant que	Attaquant
Je veux	Me connecter au C&C
Afin de	Naviguer sur le C&C
Contraintes	Site responsive, UX Design user friendly
Niveau de priorité	1

Fonction	Déconnexion
En tant que	Attaquant
Je veux	Me déconnecter du C&C
Afin de	Fermer ma session
Contraintes	Site responsive, UX Design user friendly
Niveau de priorité	1

Fonction	Choisir une attaque
En tant que	Attaquant
Je veux	Consulter ce que je peux exécuter comme attaque
Afin de	Attaquer une machine zombie, cible ou groupe de machines
Contraintes	Site responsive, UX Design user friendly
Niveau de priorité	1

Fonction	Consultation des données collectées
En tant que	Attaquant
Je veux	Consulter les données collectées sur un ou des zombies
Afin de	Faire de l'espionnage, chantage, récolter l'information
Contraintes	Site responsive, UX Design user friendly

Niveau de priorité	1
--------------------	---

Fonction	Dashboard Statistiques
En tant que	Attaquant
Je veux	Consulter les statistiques du C&C
Afin de	Avoir une vision globale de ce qui se passe sur les zombies/victimes, ainsi que de mes performances
Contraintes	Site responsive, UX Design user friendly
Niveau de priorité	1

Fonction	Mise à jour des zombies
En tant que	Attaquant
Je veux	Pouvoir mettre à jour le Malware présent sur les machines zombies
Afin de	Pouvoir utiliser les dernières versions des attaques, appliquer les correctifs applicatifs

Contraintes	Référence des MAJ dans la BD, TCP
Niveau de priorité	1

Fonction	Suppression des traces
En tant que	Attaquant
Je veux	Pouvoir supprimer mes traces sur les machines zombies
Afin de	Diminuer les chances de me faire détecter
Contraintes	Niveau de suppression élevé des fichiers temporaires et permanent, automatisation
Niveau de priorité	1

Fonction	DDOS
En tant que	Attaquant
Je veux	Lancer des requêtes intensives depuis mes zombies

Afin de	Altérer la disponibilité d'un service ou d'une machine
Contraintes	Persistance du DDOS, polymorphisme
Niveau de priorité	1

Fonction	Collecte d'informations
En tant que	Attaquant
Je veux	Pouvoir collecter de l'information sur les machines infectées ou cibles (hash de mot de passe, photos, vidéos, dossiers persos, historique navigateur, identifiants...)
Afin de	Faire du renseignement, chantage
Contraintes	Cacher le processus
Niveau de priorité	1

Fonction	Bomb Fork
En tant que	Attaquant
Je veux	Pouvoir exécuter une bombe fork sur un zombie
Afin de	Faire un déni de service
Contraintes	Cacher le processus
Niveau de priorité	1

Fonction	Vidéo / Son faisant peur
En tant que	Attaquant
Je veux	Pouvoir lancer une vidéo ou un son faisant peur
Afin de	Augmenter la probabilité du paiement de la rançon, stresser la victime

Contraintes	Cacher le processus, ne pas pouvoir sortir de la fenêtre, son au maximum
Niveau de priorité	1

Fonction	Brute Force
En tant que	Attaquant
Je veux	Récupérer le mot de passe d'une machine ou d'un compte
Afin de	Avoir un accès à une machine ou un compte
Contraintes	Polymorphisme
Niveau de priorité	1

Fonction	Relayage de phishing/spam ciblé ou en masse
En tant que	Attaquant

Je veux	Relayer des campagnes de phishing/spam en masse
Afin de	Récupérer des identifiants/mots de passes, faire de l'activisme
Contraintes	À partir d'un fichier au format json
Niveau de priorité	1

Fonction	Minage de cryptomonnaie
En tant que	Attaquant
Je veux	Miner de la cryptomonnaie sur les machines infectés
Afin de	Gagner de l'argent virtuel (crypto monnaies)
Contraintes	Cacher le processus
Niveau de priorité	2



Fonction	Cookie Jacking
En tant que	Attaquant
Je veux	Récupérer des cookies de sessions
Afin de	Se connecter à un compte
Contraintes	Cacher le processus (alternate data stream)
Niveau de priorité	2

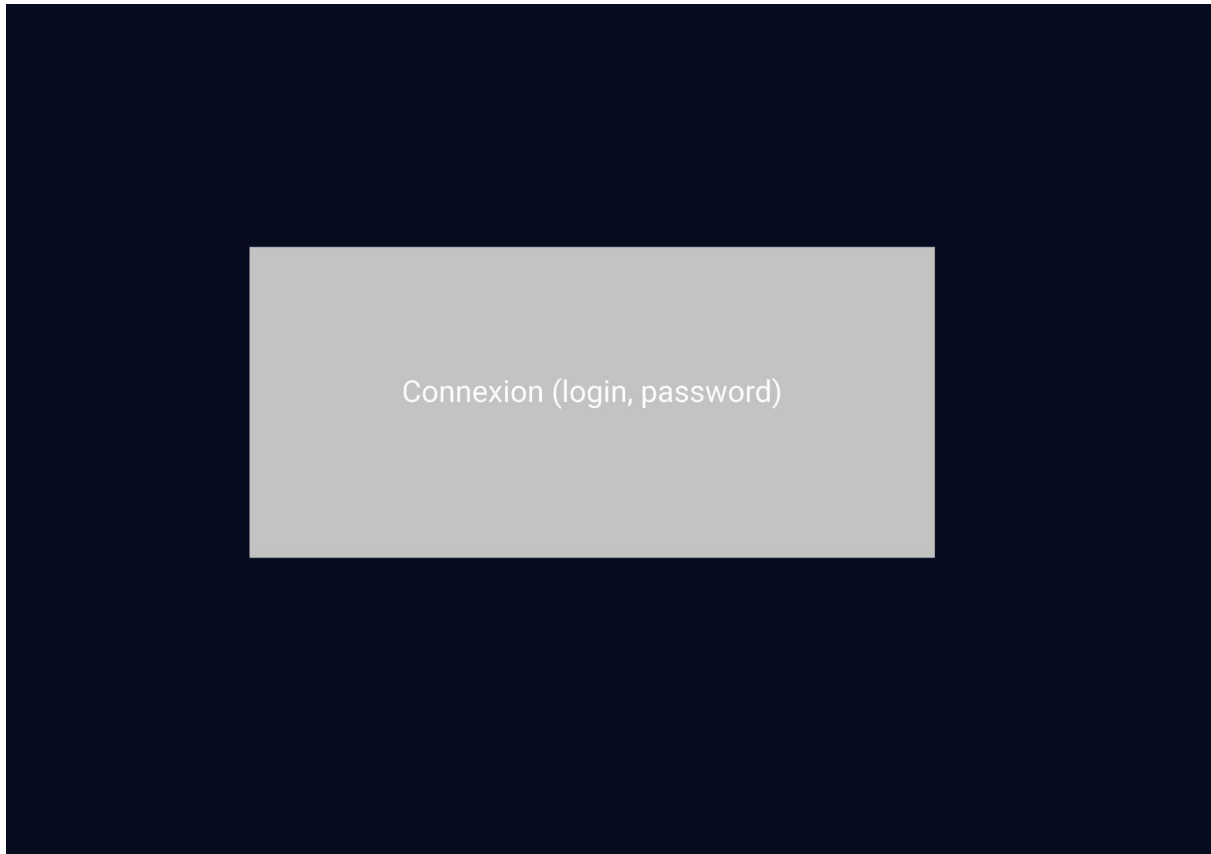
Fonction	Accès CLI (reverse shell) sur le C&C avec choix d'attaques critiques prêtes à l'emploi
En tant que	Attaquant
Je veux	Avoir un accès CLI sur un zombie via le C&C
Afin de	Exécuter des commandes spécifiques
Contraintes	Site responsive, UX Design user friendly

Niveau de priorité	2
--------------------	---

## Schémas

### Maquette du site web

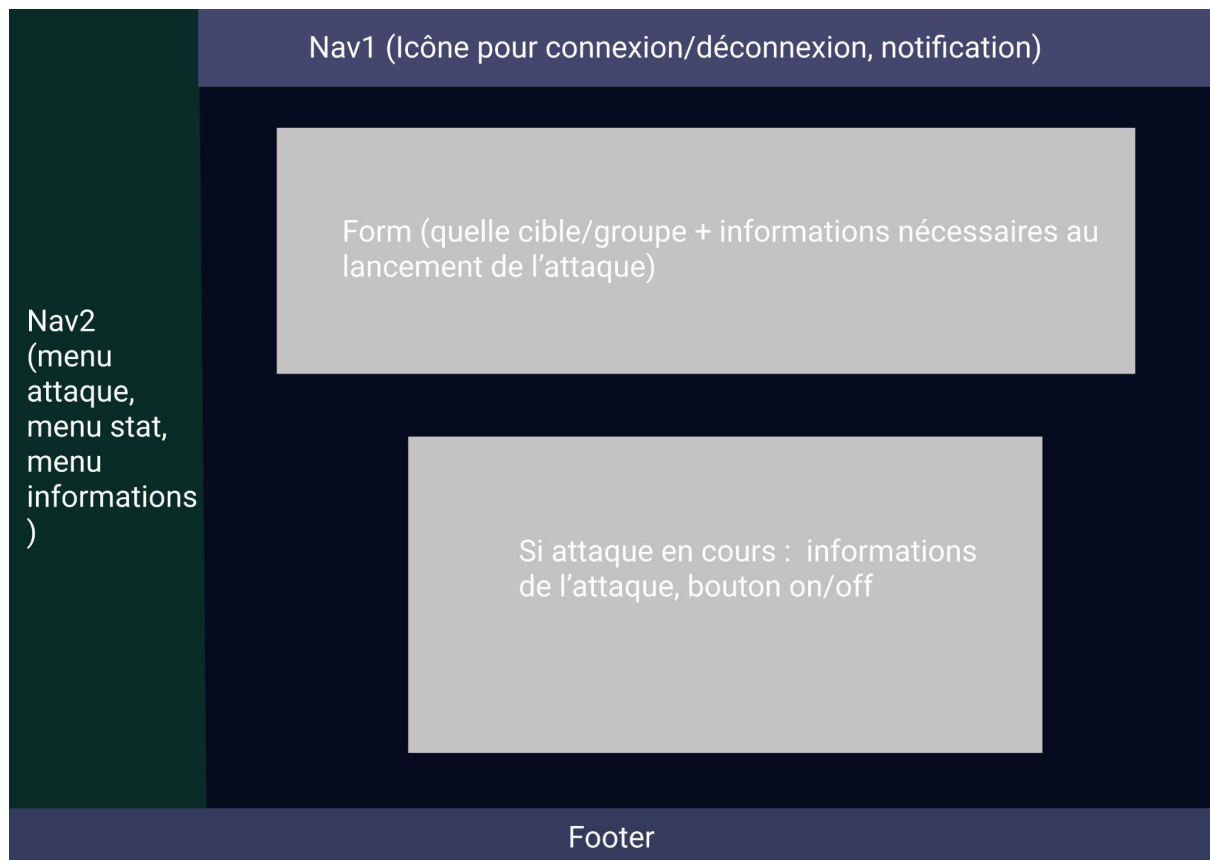
#### Connexion



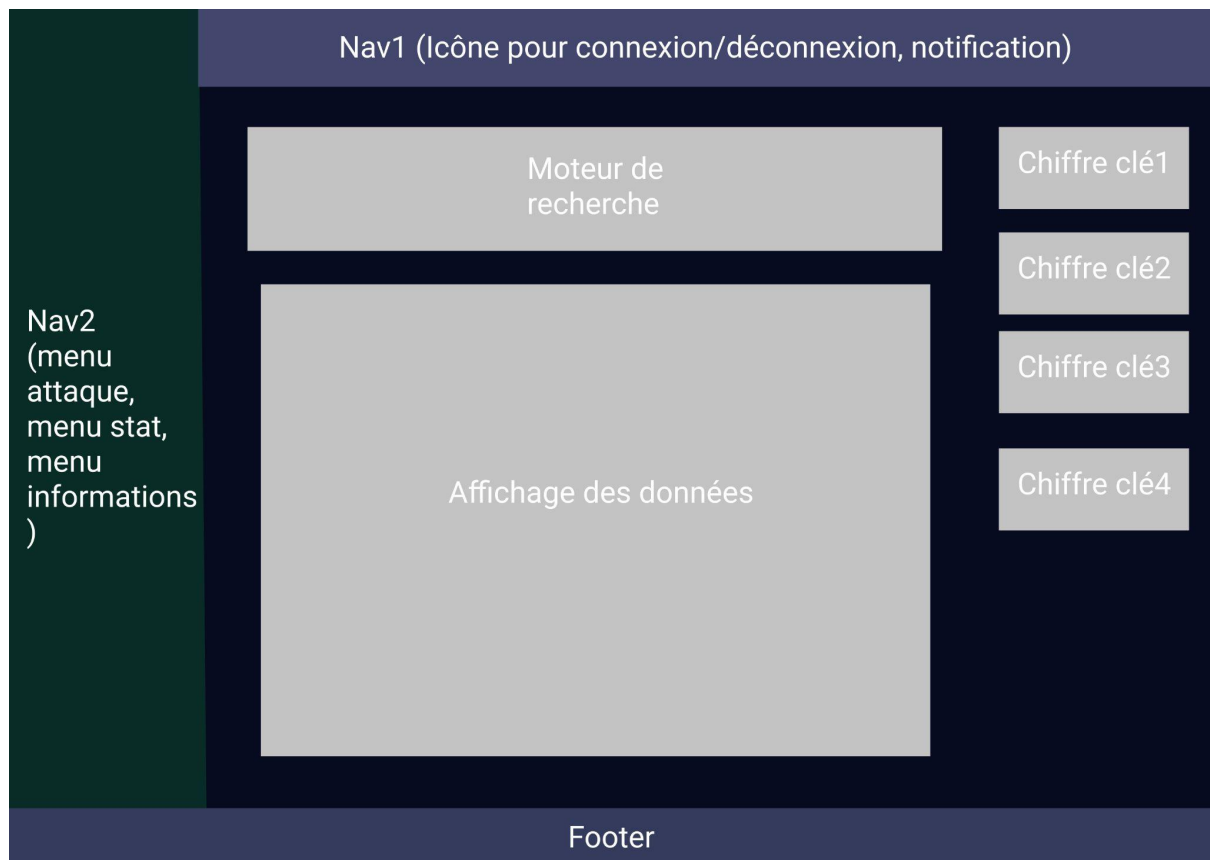
## Accueil



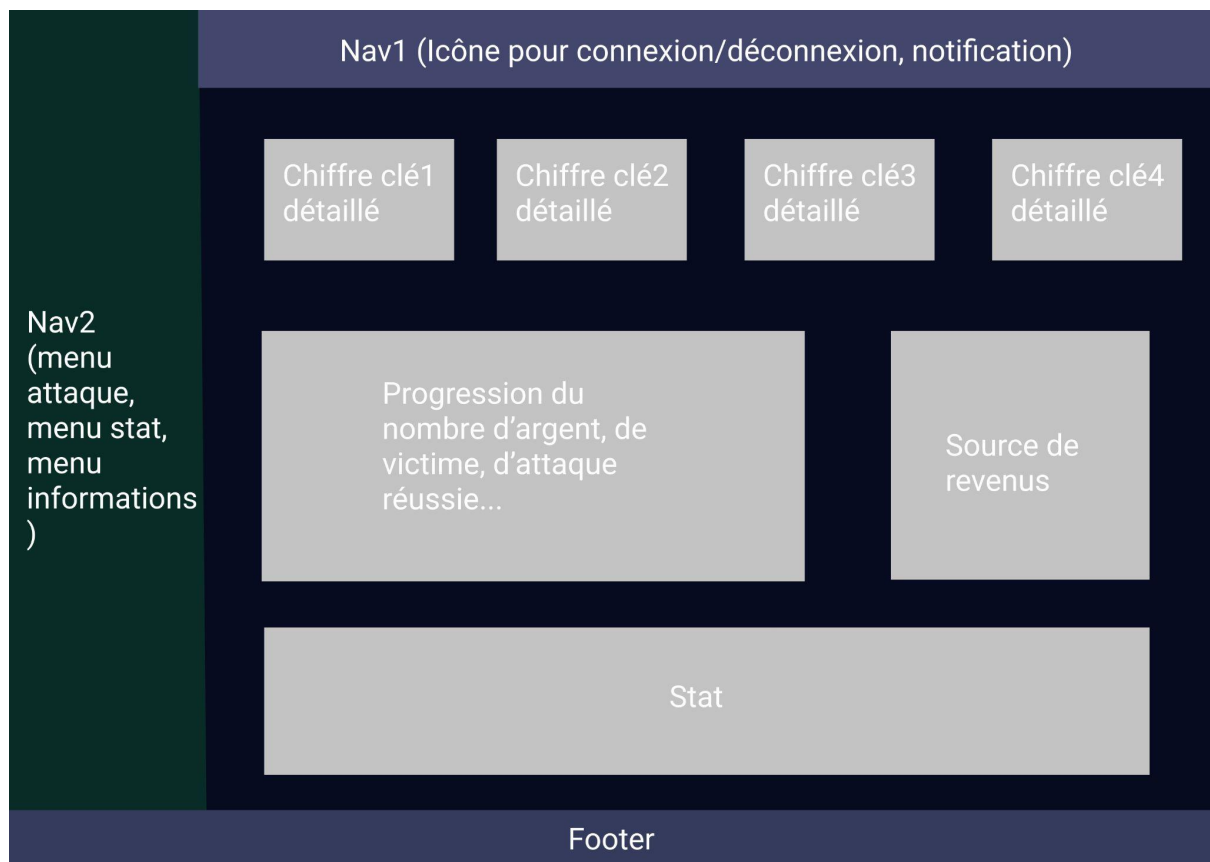
## Attaque x



## Consultation des données collectées

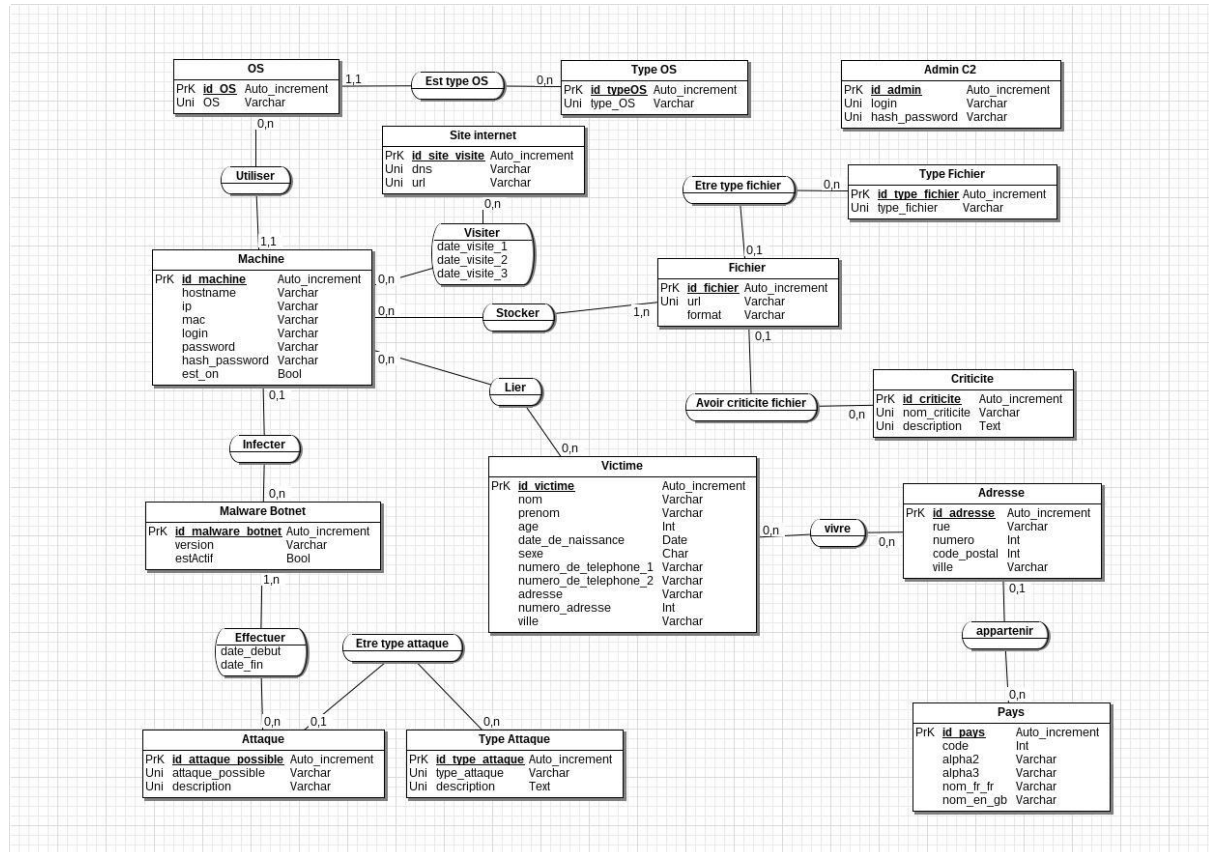


## Consultation des statistiques



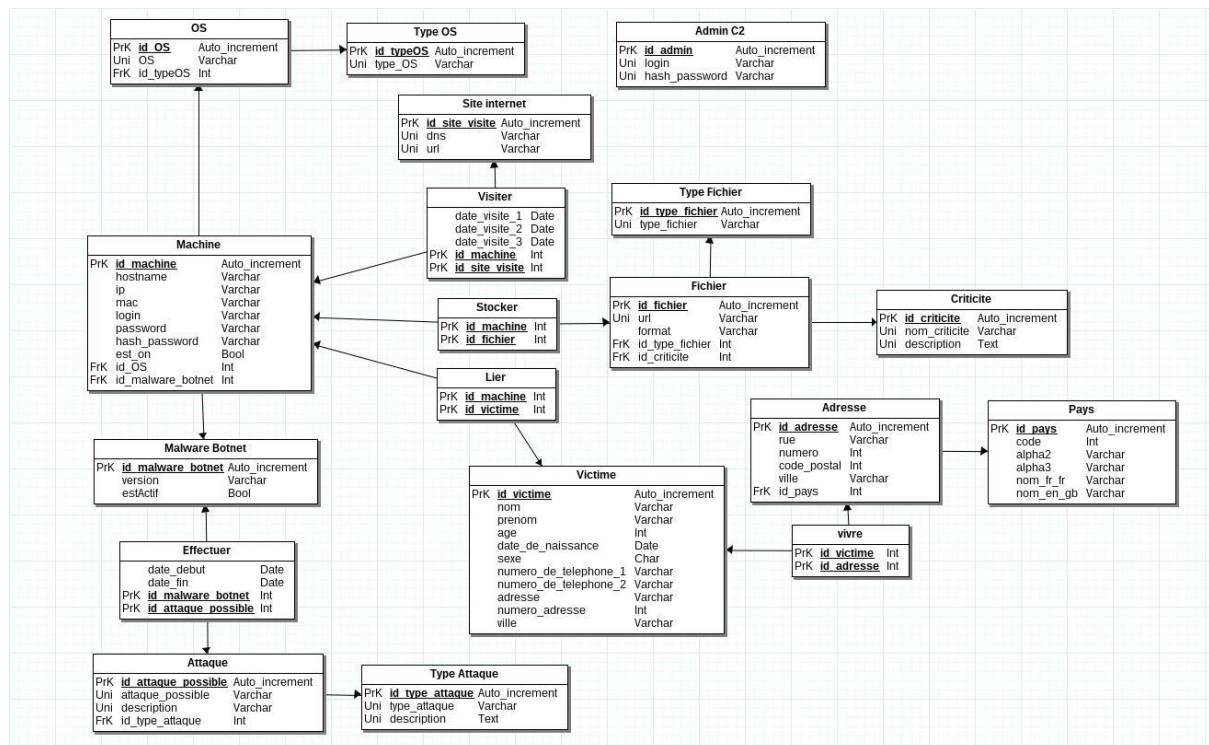
# Base de données

## MCD



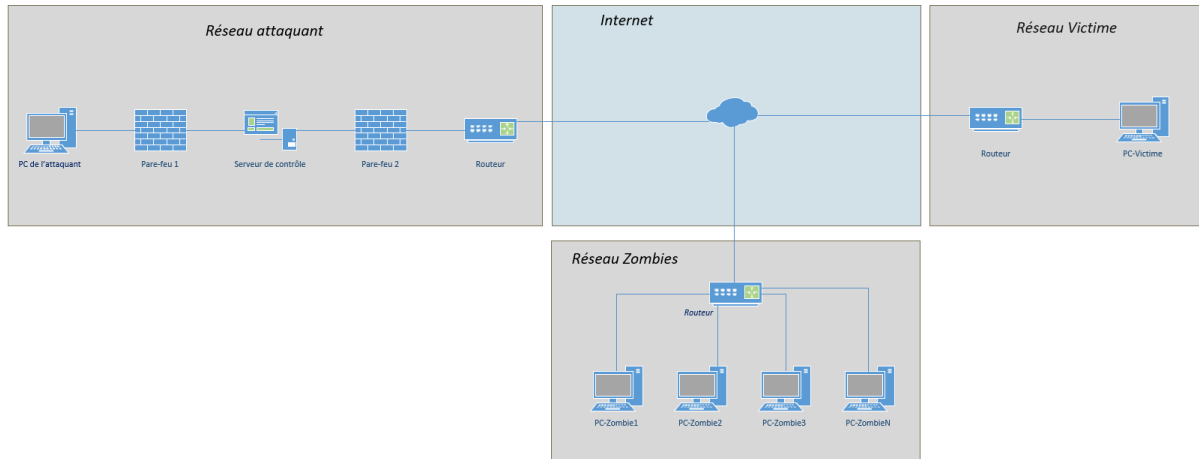


# MLD

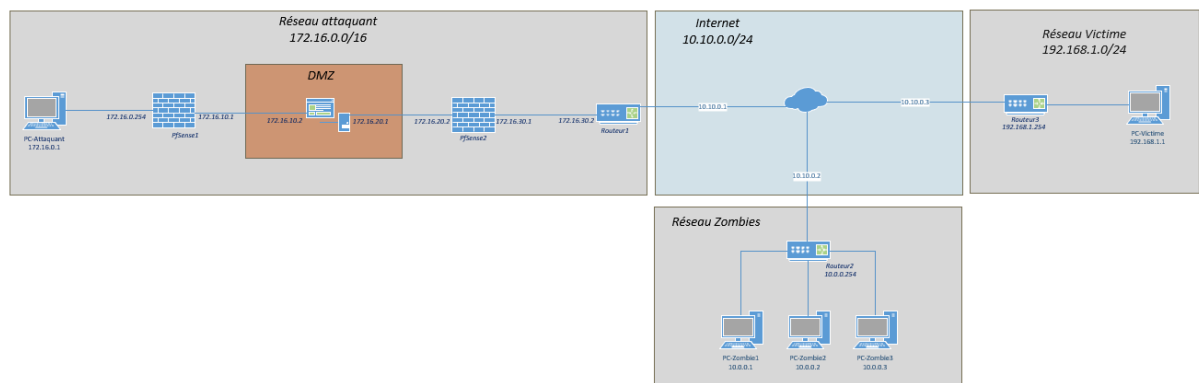


# Infrastructure réseaux

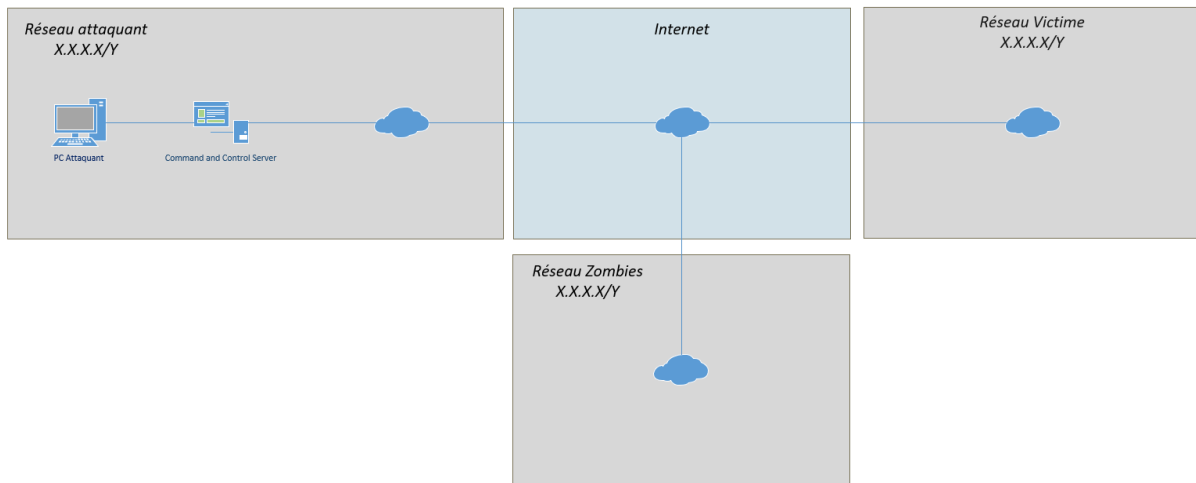
## Schéma Logique



## Schéma Technique (Infra de test)

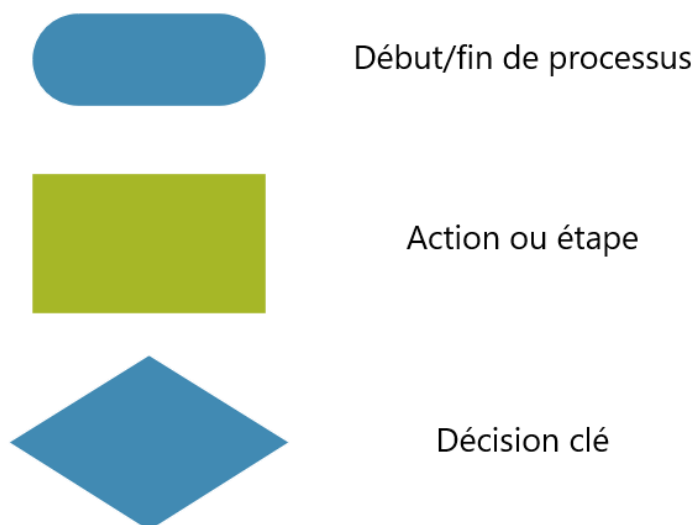


## Schéma Technique (condition réelle minimum d'infrastructure)

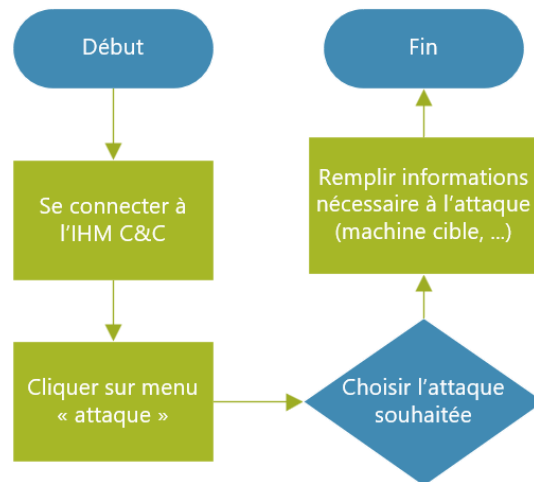


## Processus

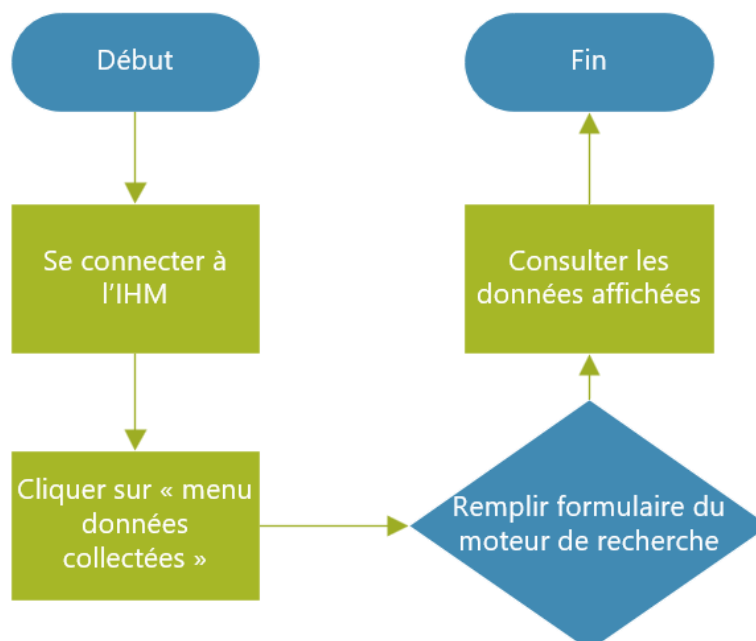
### Légende



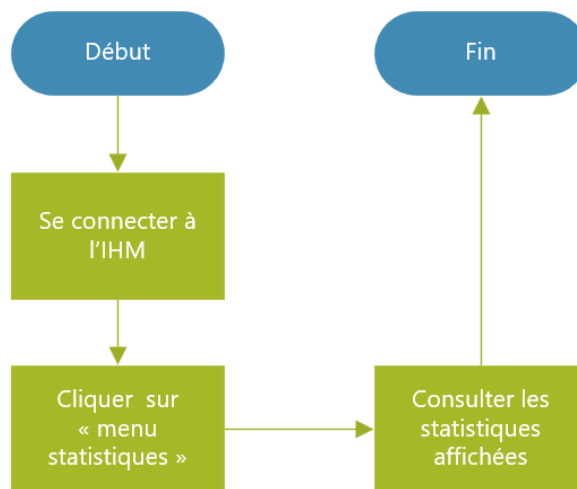
## Choisir une attaque



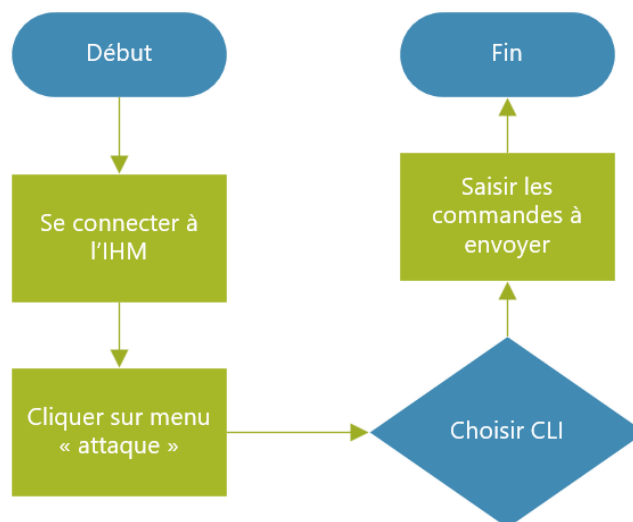
## Consultation des données collectées



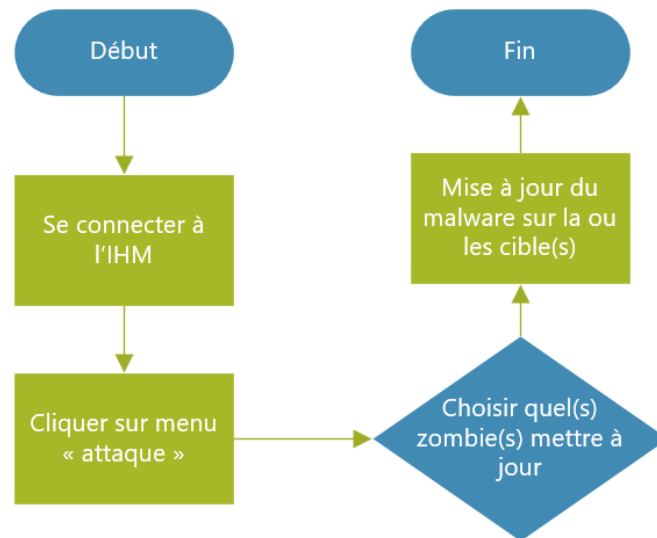
## Dashboard statistiques



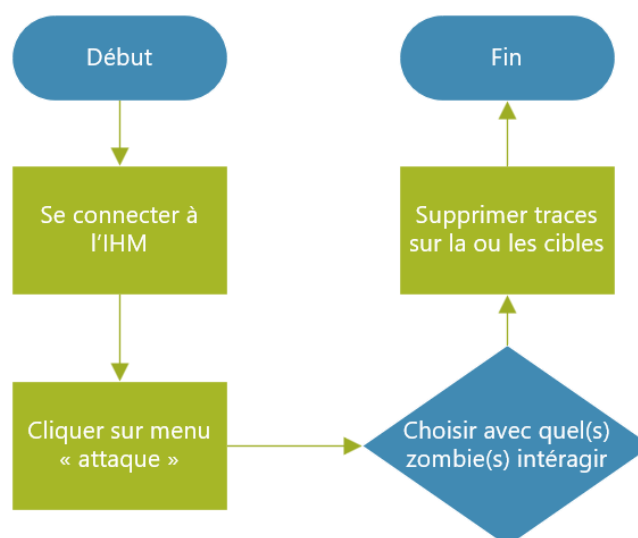
## Accès CLI (Reverse Shell)



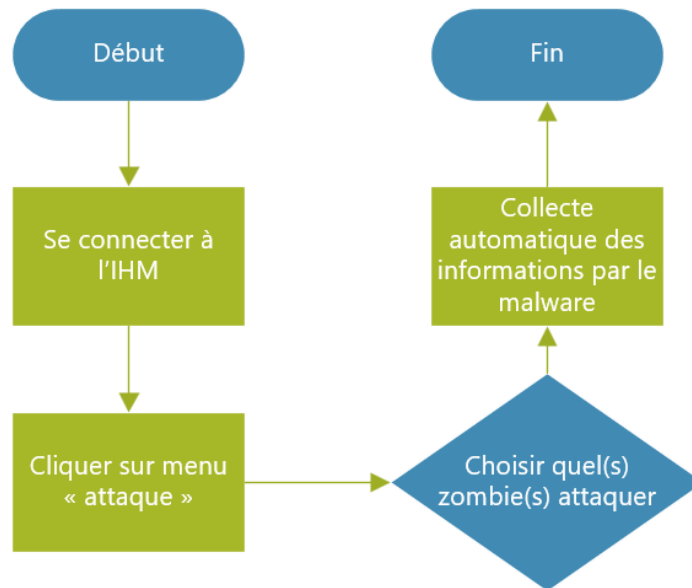
## Mise à jour des zombies



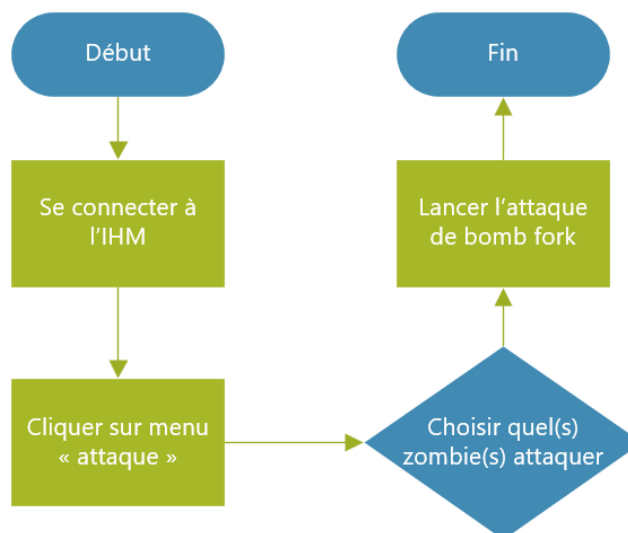
## Suppression des traces



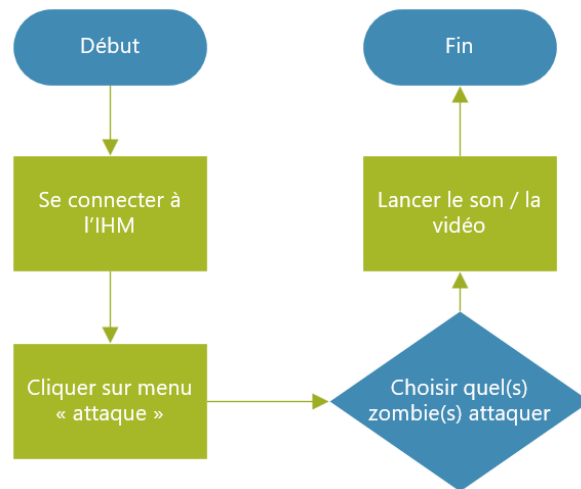
## Collecte d'informations



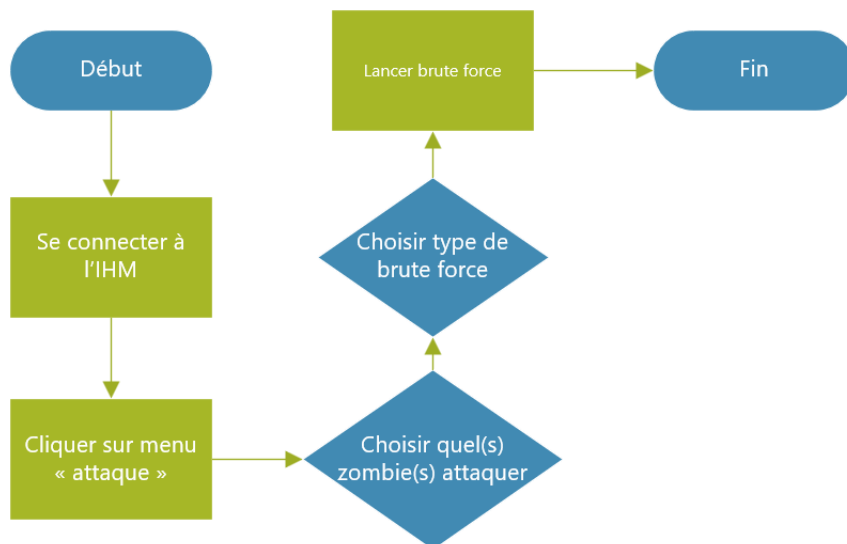
## Bomb Fork



## Vidéo/son faisant peur

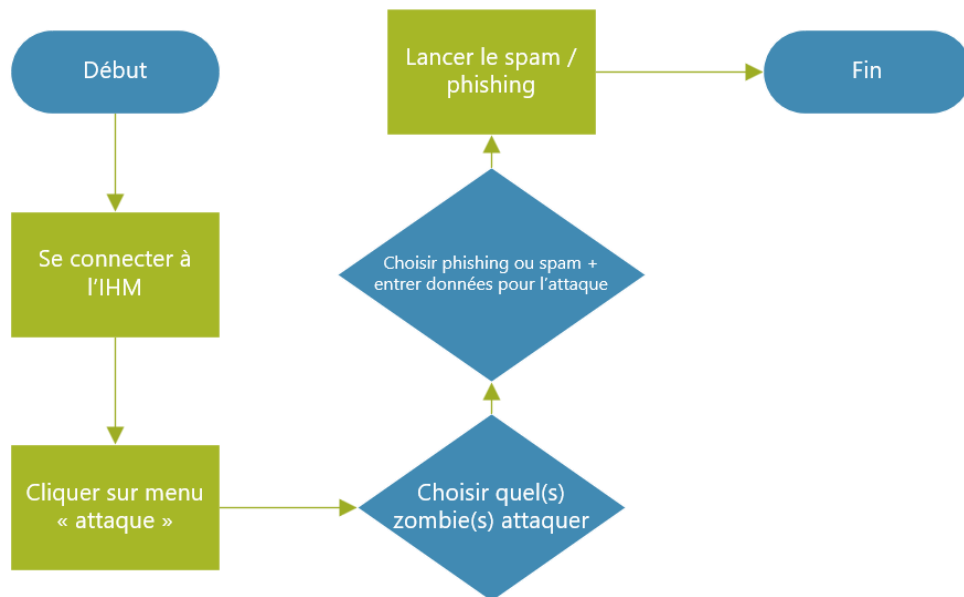


## Brute Force

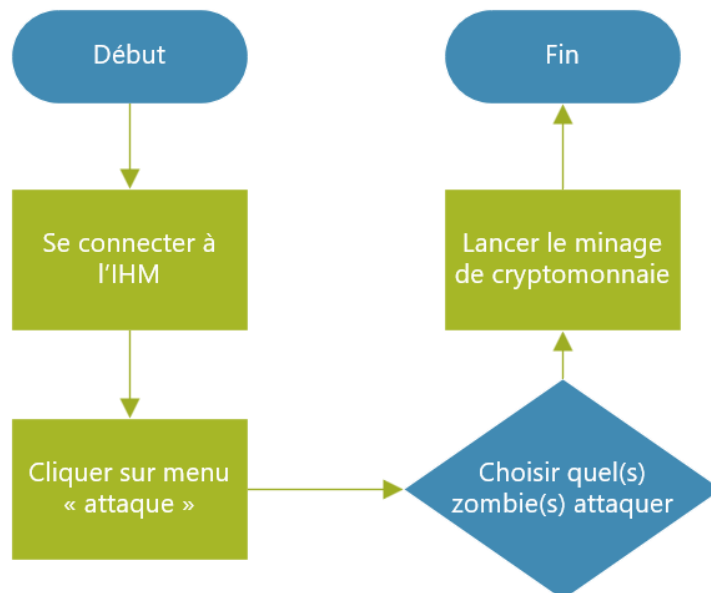




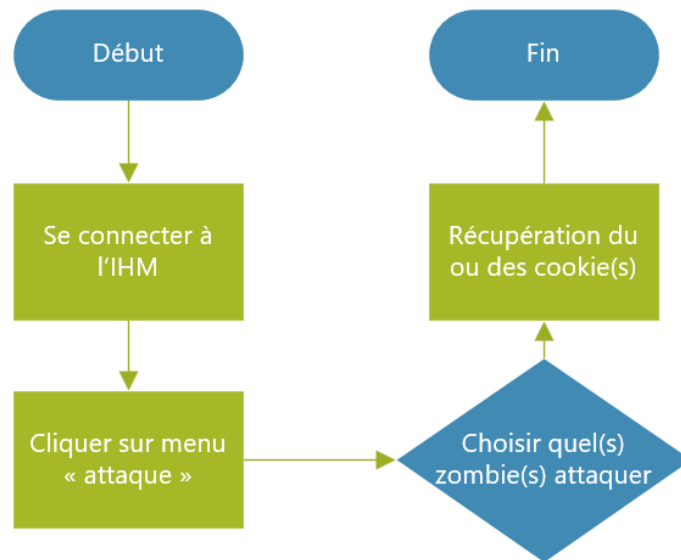
## Relayage de phishing/spam



## Minage de cryptomonnaie



## Cookie Jacking



## Référentiels

### Liens

- [Jira Confluence](#)
- [Jira Software](#)
- [GitHub](#)
- [Google Drive](#)

## Ressources

Ressource	Type	Description	Rôle
<a href="#"><u>Jira Confluence</u></a>	Matérielle	Création, modification et stockage collaboratif de documents dans le Cloud	Centraliser les documents du projet Botnet
<a href="#"><u>Jira Software</u></a>	Matérielle	Outil de méthodologie scrum pour le développement de logiciel	Gérer les user story, tâches à faire et bugs à corriger avec des informations associées (responsable, deadline etc)
<a href="#"><u>GitHub</u></a>	Matérielle	GitHub est une plateforme de stockage, versionning et partage de code en ligne	Upload le code du Botnet C2 et Botnet Malware, pour travailler en équipe
<a href="#"><u>VMWare</u></a>	Matérielle	VMWare est une plateforme de virtualisation de machines et d'infrastructure	Mise en place de l'infrastructure (machines, serveurs, pare-feu, zombies etc)
<a href="#"><u>Discord</u></a>	Matérielle	Discord est un outil de communication textuel, audio et vidéo	Communiquer au sein de l'équipe
<a href="#"><u>Google Drive</u></a>	Matérielle	Google Drive, est un service de stockage et de partage de fichiers dans le cloud lancé par la société Google.	Stockage de nos fichiers, utilisé en tant que solution de backup
<a href="#"><u>Étudiants ESGI</u></a>	Humaine	Ensemble d'étudiants participant au projet annuel "Botnet"	<p>Réaliser le projet en respectant les délais et la qualité.</p> <p>Échanger nos connaissances afin d'harmoniser les compétences.</p> <p><b>Spécialisation technique au début du projet :</b></p> <ul style="list-style-type: none"> <li>- Alexy et Julien (Réseau et système)</li> <li>- Nicolas (Programmation full-stack, Base de données, Méthodologie agile)</li> </ul>

Évaluation des risques										
N1	Risque identifié	Effets	Catégorie	Probabilité	Gravité	Criticité %	Criticité	Mesure(s)	Probabilité (nb)	Gravité (nb)
1.	Perte de donnée.	Devoir refaire le travail perdu.	Technique	1 - Nul (rare)	5 - Très élevée	20%	Élevé	Backup une fois par semaine et récupération de mot de passe sur Google Drive, Jira, GitHub.	1	5
2.	Manque de connaissance de certaines technologies.	Perte de productivité.	Humain	4 - Élevé (probable)	3 - Moyenne	48%	Élevé	Apprendre les technologies en amont et s'échanger les connaissances.	4	3
3.	Relations conflictuelles entre les membres participant au projet.	Relation humaine dégradé, productivité ralenti, retard sur le rendu des tâches.	Humain	3 - Moyenne (possible)	4 - Élevé	48%	Élevé	Se former à la méthodologie, planifier une discussion de groupe, comprendre le point de vue de chaque partie et réfléchir à une solution viable pour les deux parties.	3	4
4.	Estimation du temps erronée.	Délai sur les tâches, et éventuellement sur le rendu final.	Délai	3 - Moyenne (possible)	3 - Moyenne	36%	Élevé	Être réaliste, donner son maximum lors des sprints pour respecter les deadlines puis si besoin, accorder un délai de temps supplémentaire à consacrer aux tâches.	3	3
5.	Problème de santé, maladie ou situation imprévue.	Incapacité de travailler sur le projet pendant une certaine durée.	Humain	2 - Faible (improbable)	3 - Moyenne	24%	Moyen	Estimer une période de récupération et prévoir du temps à certains endroits.	2	3
6.	Inaptitude à évaluer ou/et prévoir certains risques.	Perte de temps et de contrôle au niveau de la gestion de projet.	Humain	4 - Élevé (probable)	2 - Faible	32%	Élevé	Examiner autant de risques que possible avec tous les intervenants concernés par le projet.	4	2
7.	Dysfonctionnement du matériel de travail ou connexion internet.	Rendu différé de tâches. Inaccessibilité des ressources de travail.	Technique	1 - Nul (rare)	4 - Élevé	16%	Moyen	Prévoir une solution de secours (partage de connexion, deuxième machine de travail).	1	4
7.	Dysfonctionnement du matériel de travail ou connexion internet.	Rendu différé de tâches. Inaccessibilité des ressources de travail.	Technique	1 - Nul (rare)	4 - Élevé	16%	Moyen	Prévoir une solution de secours (partage de connexion, deuxième machine de travail).	1	4
8.	Incompréhension sur l'objectif et/ou le résultat attendu d'une tâche.	Gaspillage de temps, production de fonctionnalités erronés.	Humain	2 - Faible (improbable)	2 - Faible	16%	Faible	Être le plus clair possible au sujet de la description d'une tâche et communiquer autant qu'il faut.	2	2

## Organisation du temps

- Durée de sprint : 3 semaines
- Réunions :
  1. **Début de sprint** : 1er Lundi du sprint à 20h30 (durée de ~2h)
  2. **Inter-sprint** : Lundi et Jeudi à 20h30 (durée de ~30min)
  3. **Fin de sprint** : Samedi (durée de ~1h)

## Répartition du travail

### Rôles

Rôle	Personne(s)
Tech lead Dev	@Nicolas Torres
Tech lead S&R	@Julien Delaunay @DA COSTA Alexy
Développeur	@Nicolas Torres @DA COSTA Alexy @Julien Delaunay
Architecte S&R	@Julien Delaunay @DA COSTA Alexy @Nicolas Torres
Scrum Master	@Nicolas Torres (puis amené à changer)

## Tâches














Nous allons tous travailler sur chaque brique du projet afin d'élargir, approfondir nos connaissances dans chaque domaine.

La répartition des tâches se fera à chaque début de sprint sous forme de ticket Jira.

Partie	Personne(s)	Livrable	Répartition
<b>C&amp;C</b>	<a href="#">@Nicolas Torres</a> <a href="#">@Julien Delaunay</a> <a href="#">@DA COSTA Alexy</a>	Code source	Par fonctionnalité
<b>Malware</b>	<a href="#">@Nicolas Torres</a> <a href="#">@Julien Delaunay</a> <a href="#">@DA COSTA Alexy</a>	Code source	Par fonctionnalité
<b>Infra</b>	<a href="#">@Nicolas Torres.</a> <a href="#">@Julien Delaunay</a> <a href="#">@DA COSTA Alexy</a>	Fichiers des configurations des VM	Par machine puis fonctionnalité
<b>Méthodologie</b>	<a href="#">@Nicolas Torres</a> <a href="#">@Julien Delaunay</a> <a href="#">@DA COSTA Alexy</a>	Cahier des charges et liens annexes	<a href="#">@Nicolas Torres</a> (User Stories, contraintes logiciels, Maquette du C&C, MCD/MLD/script BD, schéma réseaux, présentation du projet, initialisation du Git et Jira, mise en forme du cahier

















			des charges, Scrum Master)  <a href="#">@Julien Delaunay</a> (User Stories, schéma réseaux, processus, contraintes techniques de l'infra)  <a href="#">@DA COSTA Alexy</a> (User Stories, schéma réseaux, référentiel des ressources et risques, feuille de route)
--	--	--	--

## Feuille de route Jira

Epic	MARS	AVR. – JUIN	JUIL. – SEPT.	OCT. – DÉC.
> <a href="#">BOTNET-40 Méthodologie/Préparation</a>				
 BOTNET-56 Remise à niveau des connaissances				
 BOTNET-42 Création de l'infrastructure réseau				
 BOTNET-44 Création du C&C				
 BOTNET-43 Création du Malware				
 BOTNET-54 Enrichissement de notre Malware				
 BOTNET-55 Préparation du rendu				

## Backlog de l'épic "Remise à niveau des connaissances"

*Note : Le responsable de chaque ticket de cet épic est la personne spécialisée dans la technologie (ex : C). Elle s'assurera que le ou les membre(s) de l'équipe affectée(s) à cette tâche de remise à niveau, ont bien acquis les compétences requises. De plus, il sera disponible pour répondre (si besoin) aux questions.*

<input checked="" type="checkbox"/> BOTNET-59	Remise à niveau HTML	 2	À FAIRE ▾	 N
<input checked="" type="checkbox"/> BOTNET-60	Remise à niveau Bootstrap	 2	À FAIRE ▾	 N
<input checked="" type="checkbox"/> BOTNET-65	Remise à niveau SQL	 2	À FAIRE ▾	 N
<input checked="" type="checkbox"/> BOTNET-61	Remise à niveau POO	 3	À FAIRE ▾	 N
<input checked="" type="checkbox"/> BOTNET-62	Remise à niveau Django	 4	À FAIRE ▾	 N
<input checked="" type="checkbox"/> BOTNET-58	Remise à niveau en C	 5	À FAIRE ▾	 N
<input checked="" type="checkbox"/> BOTNET-63	Remise à niveau Système	 3	À FAIRE ▾	 DA
<input checked="" type="checkbox"/> BOTNET-64	Remise à niveau Réseaux	 4	À FAIRE ▾	 JD