Projet Annuel

**Botnet**

ESGI - BACHELOR SÉCURITÉ INFORMATIQUE (3JSI)

**Groupe :**

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

# Table des matières

[**Table des matières**](#_pqohjy2ojxpa) **2**

[**Présentation du projet**](#_6zl16ugb59f8) **4**

[Contributeurs](#_8xgutrja3gyo) 4

[Contexte](#_dnz9jxlklapp) 4

[Livrable](#_ym2qw882kp6e) 4

[Objectifs](#_1v10i5pxj1j0) 5

[**Contraintes**](#_gc2wk18exxm9) **6**

[Techniques](#_uszdbzza3t6m) 6

[Architecture réseau](#_uusvitmevanh) 6

[Logiciel](#_akmi0b901rbc) 8

[Légales](#_yyikvkmp9nw1) 8

[**Users stories**](#_ow0x7evftm6j) **9**

[**Schémas**](#_izxyg8ntbkdu) **19**

[Maquette du site web](#_u3s5o79ujgd) 19

[Connexion](#_qwart17evs7r) 19

[Accueil](#_xru7zfq12a4y) 20

[Attaque x](#_gyd1sq235g3q) 21

[Consultation des données collectées](#_238bkg9cfbta) 22

[Consultation des statistiques](#_7bsg5msn6f4r) 23

[Base de données](#_fouwr5ykbjvy) 24

[MCD](#_8otcqudx1yxi) 24

[MLD](#_vr6erarkl5jw) 25

[Infrastructure réseaux](#_sk8bo1z0rp95) 26

[Schéma Logique](#_kwgxt8ah0k4f) 26

[Schéma Technique (Infra de test)](#_ytvvcduj17my) 26

[Schéma Technique (condition réelle minimum d’une infrastructure)](#_gmb38ou7nif0) 27

[Processus](#_loa64tzb9sun) 27

[Légende](#_3adf9p2111j7) 27

[Choisir une attaque](#_nysbnz8y7kvv) 28

[Consultation des données collectées](#_rylsqpkqbhnr) 28

[Dashboard statistiques](#_novnkjubkc37) 29

[Accès CLI (Reverse Shell)](#_6983chbgtsxi) 29

[Mise à jour des zombies](#_2dflno77vitm) 30

[Suppression des traces](#_76nzpiz9i3a3) 30

[Collecte d’informations](#_fucuzjg8hy78) 31

[Bomb Fork](#_ms5nllku403e) 31

[Vidéo/son faisant peur](#_n5xnd22vfoxt) 32

[Brute Force](#_sptn3e39a78r) 32

[Relayage de phishing/spam](#_d9z0qq93ai6r) 33

[Minage de cryptomonnaie](#_u6ynism7omkx) 33

[Cookie Jacking](#_m4mi7xunfg1j) 34

[**Référentiels**](#_oye2d5ardht5) **34**

[Liens](#_54nnxhbg7jsp) 34

[Ressources](#_ott6ye4uwj6l) 35

[Risques](#_vfdsztpsjuol) 36

[Organisation du temps](#_b2nzuvv3cgr6) 36

[Répartition du travail](#_7gl0vu82599a) 37

[Rôles](#_ezd01mavj034) 37

[Tâches](#_ae4wpt98vq5n) 38

[Feuille de route Jira](#_uov8sv4nabn) 39

[Backlog de l’épic “Remise à niveau des connaissances”](#_dmom0go8mm9g) 40

# 

# 

# 

# 

# :mag: Présentation du projet

## :busts_in_silhouette: Contributeurs

* Nicolas TORRES
* Julien DELAUNAY
* Alexy DA COSTA

## :compass: 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.

## :truck: 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

## :trophy: 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.

## :compass: Méthodologie utilisée

La méthodologie que nous utilisons est Scrum.

# :lock: Contraintes

## :man_technologist: 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 |

## :man_judge: 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.

# :thought_balloon: 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 |

# :triangular_ruler: Schémas

## Maquette du site web

### Connexion

### 

### 

### 

### 

### 

### Accueil

### 

### 

### 

### 

### 

### 

### 

### 

### Attaque x

### 

### 

### 

### 

### 

### 

### 

### 

### Consultation des données collectées

### 

### 

### 

### 

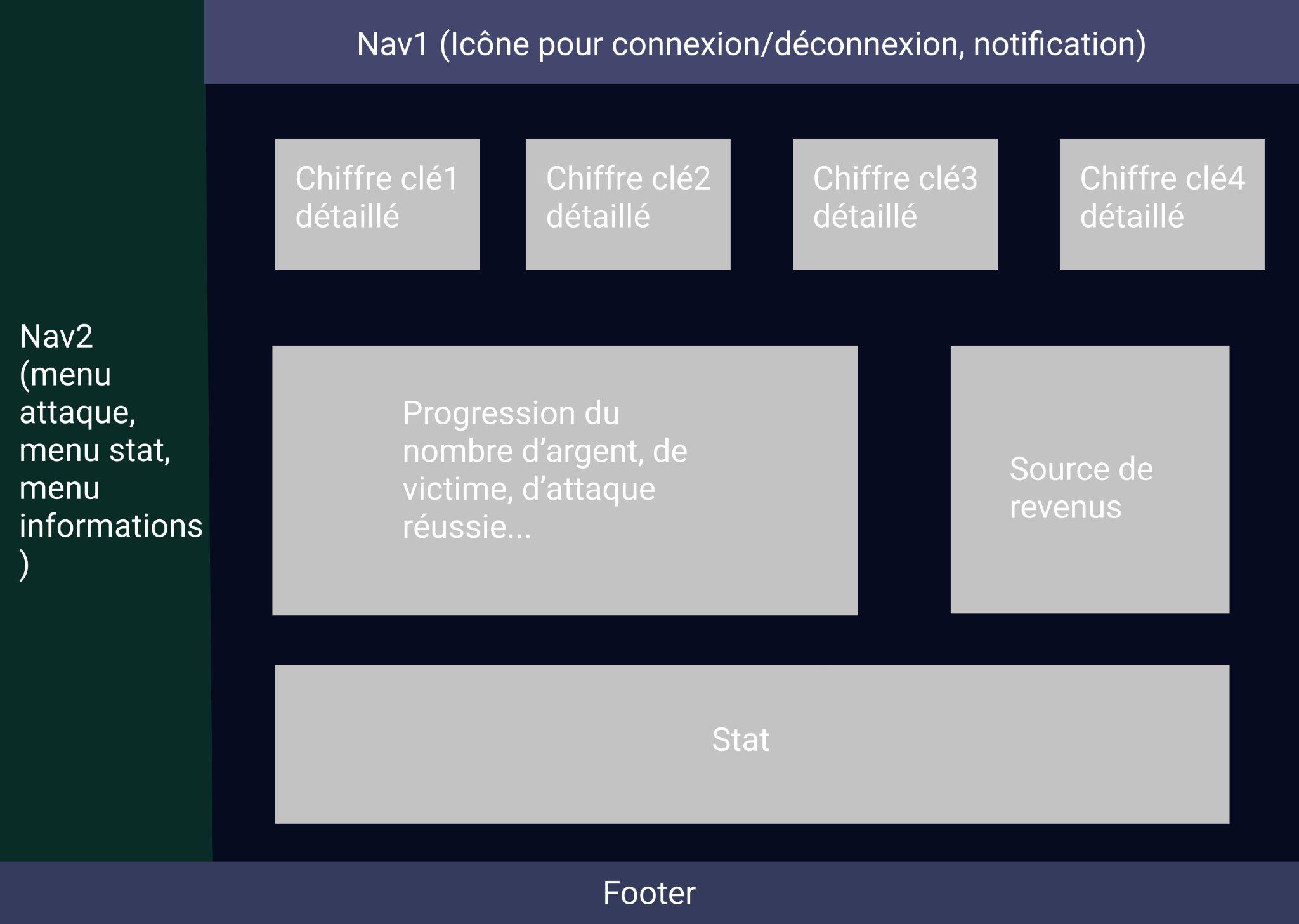
### 

### 

### 

### 

### Consultation des statistiques



## 

## 

## 

## 

## Base de données

### MCD

### 

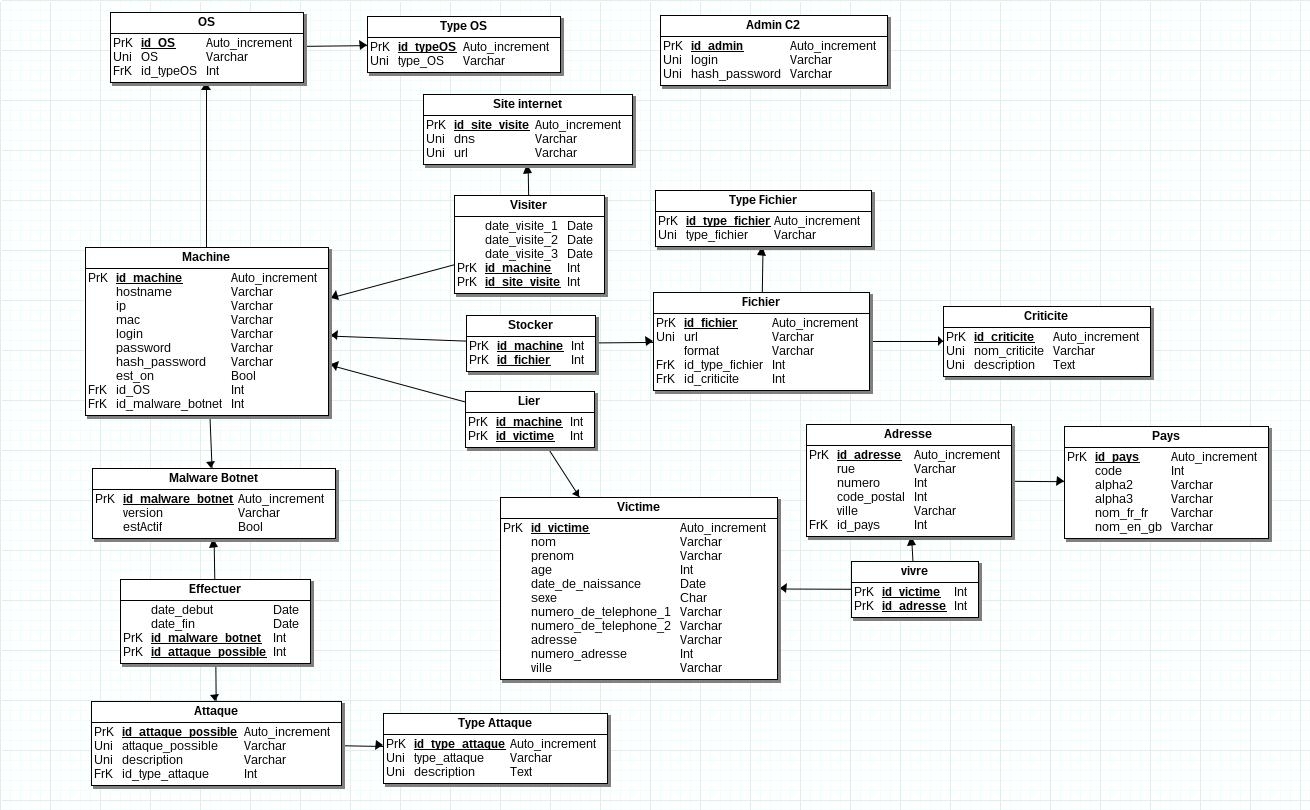
### 

### 

### 

### 

### MLD



## Infrastructure réseaux

### Schéma Logique

### Schéma Technique (Infra de test)

### 

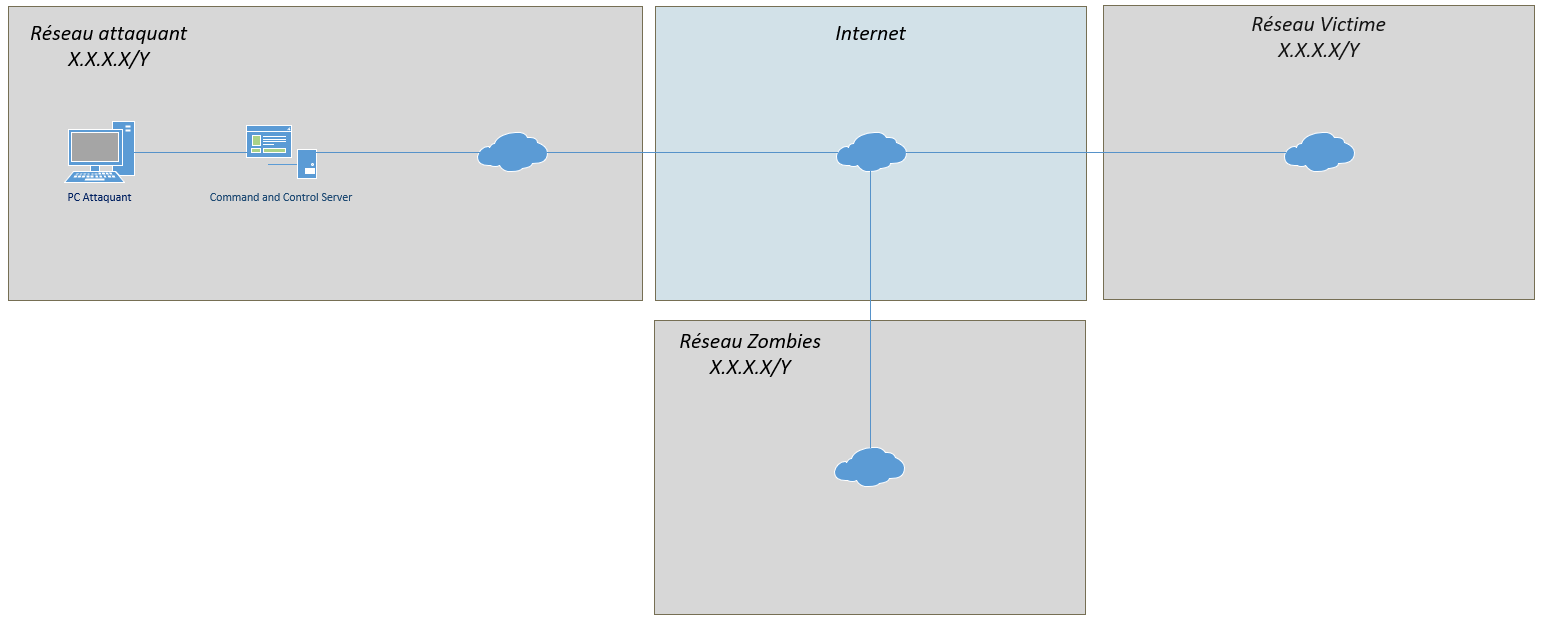
### 

### 

### 

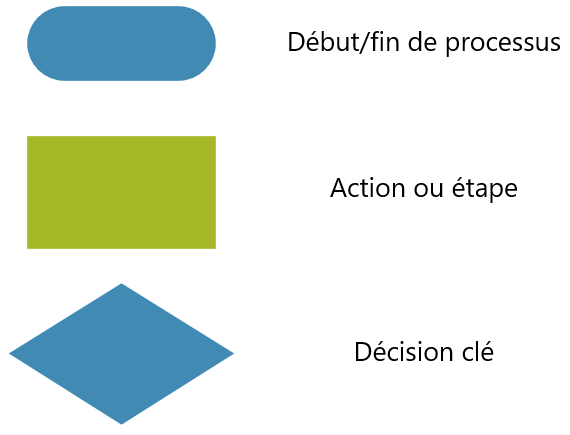
### 

### Schéma Technique (condition réelle minimum d’une infrastructure)



## Processus

### Légende



### Choisir une attaque

### 

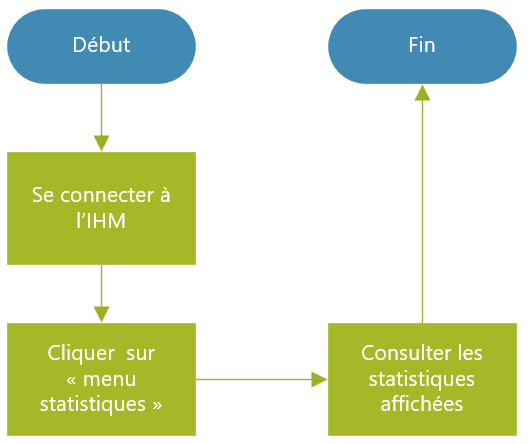
### 

### Consultation des données collectées

### 

### 

### Dashboard statistiques



### 

### Accès CLI (Reverse Shell)

### 

### 

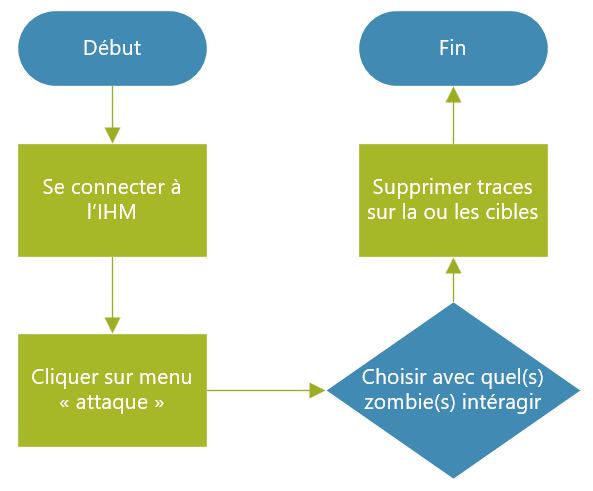
### Mise à jour des zombies

### 

### 

### 

### Suppression des traces



### Collecte d’informations

### 

### Bomb Fork

### 

### 

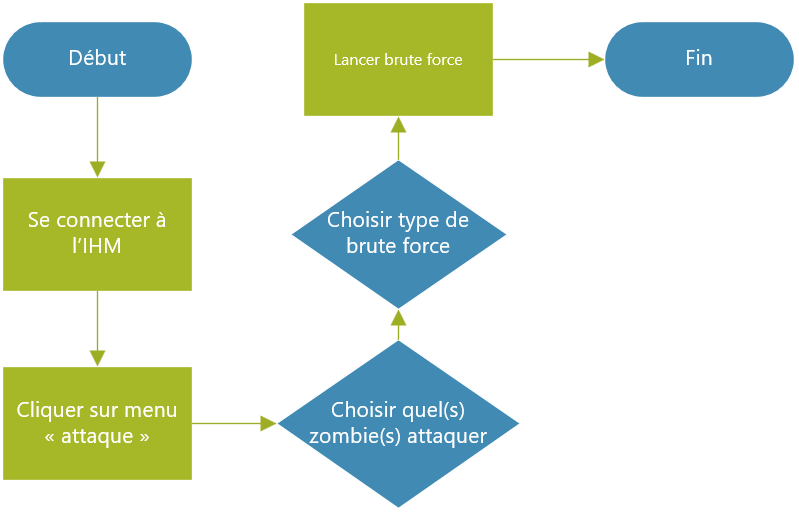
### 

### Vidéo/son faisant peur

### 

### 

### Brute Force



### 

### 

### Relayage de phishing/spam

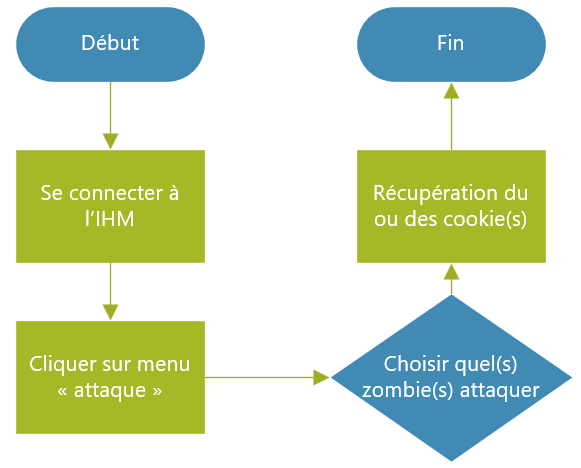
### 

### Minage de cryptomonnaie

### 

### 

### Cookie Jacking



# :pushpin: Référentiels

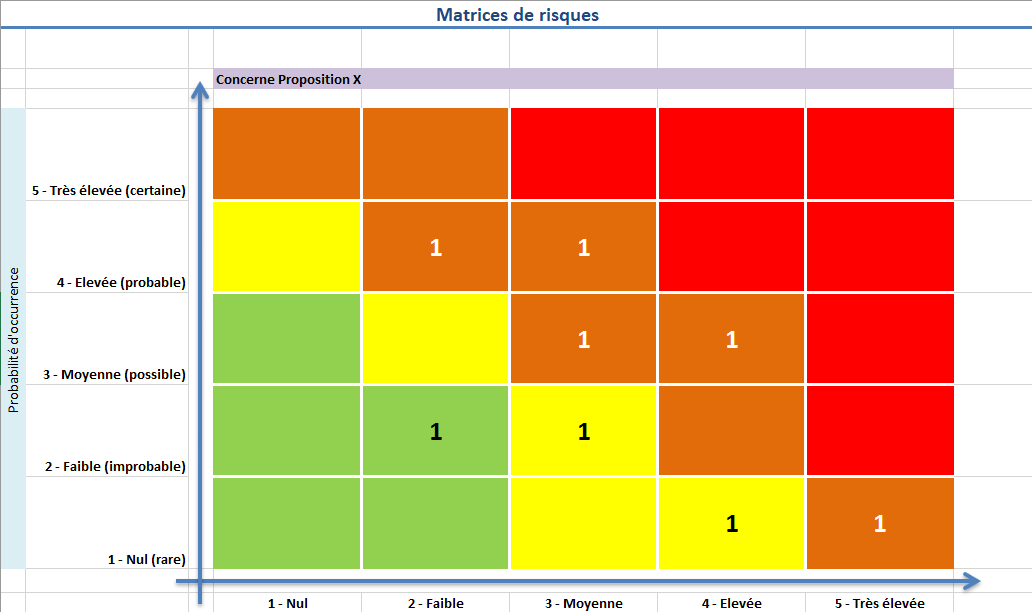
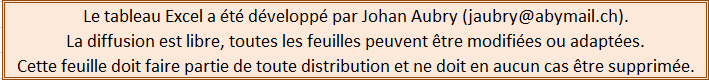
## :link: Liens

* [Jira Confluence](https://botnet3si.atlassian.net/wiki/spaces/BOTNET3JSI/pages)
* [Jira Software](https://botnet3si.atlassian.net/jira/projects?selectedProjectType=software)
* [GitHub](https://github.com/Nicolas-Torres/Botnet)
* [Google Drive](https://drive.google.com/drive/folders/1T4WEzPE3GCgzG6y0TM1W_h14OAh11zPh)

## :muscle: Ressources

| **Ressource** | **Type** | **Description** | **Rôle** |
| --- | --- | --- | --- |
| Jira Confluence | Matérielle | Création, modification et stockage collaboratif de documents dans le Cloud | Centraliser les documents du projet Botnet |
| Jira Software | 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) |
| GitHub | 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 |
| VMWare | Matérielle | VMWare est une plateforme de virtualisation de machines et d’infrastructure | Mise en place de l’infrastructure (machines, serveurs, pare-feu, zombies etc) |
| Discord | Matérielle | Discord est un outil de communication textuel, audio et vidéo | Communiquer au sein de l'équipe |
| Google Drive | 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 |
| Étudiants ESGI | Humaine | Ensemble d'étudiants participant au projet annuel “Botnet” | Réaliser le projet en respectant les délais et la qualité.  Échanger nos connaissances afin d’harmoniser les compétences.  **Spécialisation technique au début du projet :**  **-** Alexy et Julien (Réseau et système)  - Nicolas (Programmation full-stack, Base de données, Méthodologie agile) |

## :shield: Risques



## :alarm_clock: 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)

## :busts_in_silhouette: 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) |

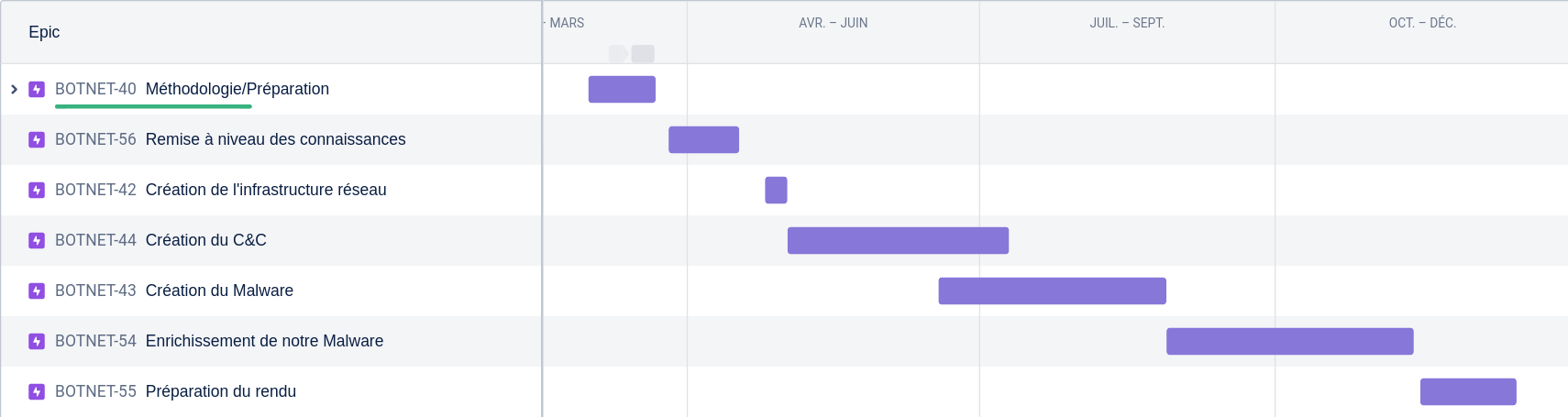
### Tâches

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** |
| --- | --- | --- | --- |
| **C&C** | @Nicolas Torres  @Julien Delaunay  @DA COSTA Alexy | Code source | Par fonctionnalité |
| **Malware** | @Nicolas Torres  @Julien Delaunay  @DA COSTA Alexy | Code source | Par fonctionnalité |
| **Infra** | @Nicolas Torres.  @Julien Delaunay  @DA COSTA Alexy | Fichiers des configurations des VM | Par machine puis fonctionnalité |
| **Méthodologie** | @Nicolas Torres  @Julien Delaunay  @DA COSTA Alexy | Cahier des charges et liens annexes | @Nicolas Torres (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)  @Julien Delaunay (User Stories, schéma réseaux, processus, contraintes techniques de l’infra)  @DA COSTA Alexy (User Stories, schéma réseaux, référentiel des ressources et risques, feuille de route) |

## :telescope: Feuille de route Jira



## 

## :telescope: 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.*

