

|  |
| --- |
| PROJET 2SU  CTF IoT |
| Ce rapport explore l'univers captivant des CTF, des compétitions informatiques immersives visant à tester et améliorer les compétences en sécurité. Plongeant dans le monde de l'IoT, nous découvrirons comment ces challenges peuvent mettre en lumière les vulnérabilités et défis uniques présentés par les objets connectés, tout en offrant une plateforme d'apprentissage stimulante pour les passionnés de sécurité informatique. |
| 2023-2024  INSA Centre-Val-de-Loire  Créé par : PARVEDY Raphael, GENY Yanis, ALQARH Jannate |



Table des matières

[I. Introduction 3](#_Toc155164365)

[Contexte du projet de CTF avec l'IoT 3](#_Toc155164366)

[Objectifs spécifiques de votre initiative 3](#_Toc155164367)

[Mise en avant du scénario élaboré 3](#_Toc155164368)

[II. Activité 1: Piratage WiFi 4](#_Toc155164369)

[Description détaillée de l'activité 4](#_Toc155164370)

[Méthodologie pour simuler un réseau WiFi 4](#_Toc155164371)

[Attaque du réseau Wifi 4](#_Toc155164372)

[III. Activité 2: Redirection du Flux Vidéo de la Caméra 5](#_Toc155164373)

[Contextualisation de l'activité 5](#_Toc155164374)

[Méthodologie pour simuler une caméra de surveillance 5](#_Toc155164375)

[Attaque du réseau de caméras simulé 5](#_Toc155164376)

[IV. Activité 3: Piratage de Carte d'Accès 6](#_Toc155164377)

[Explication détaillée du scénario 6](#_Toc155164378)

[Méthodologie pour simuler une carte d'accès 6](#_Toc155164379)

[Attaque de carte d’accès 6](#_Toc155164380)

[V. Activité 4: Création d'un Keylogger 7](#_Toc155164381)

[Présentation de l'activité 7](#_Toc155164382)

[Processus de création du scénario de keylogging 7](#_Toc155164383)

[VI. Activité 5: Onde radio 8](#_Toc155164384)

[Présentation de l'activité 8](#_Toc155164385)

[Processus de récupération du flag 8](#_Toc155164386)

[Processus de création du scénario de brouilleur radio 8](#_Toc155164387)

[VII. Analyse Transversale des Activités 9](#_Toc155164388)

[Comparaison des différentes activités en termes de complexité 9](#_Toc155164389)

[Points forts et points faibles de chaque activité 9](#_Toc155164390)

[Considérations sur la variété des compétences testées 9](#_Toc155164391)

[VIII. Conclusion 10](#_Toc155164392)

[Récapitulation des points forts du projet 10](#_Toc155164393)

[Perspectives futures et continuité du projet 10](#_Toc155164394)

# I. Introduction

## Contexte du projet de CTF avec l'IoT

Dans l'univers en constante évolution de la sécurité informatique, la simulation de scénarios de cyberattaques devient une méthode inestimable pour tester et améliorer les compétences des professionnels et des passionnés. Ce rapport retrace notre exploration dans le monde des Capture The Flag (CTF) en combinant la complexité de l'Internet des Objets (IoT) avec une touche ludique et taquine.

## Objectifs spécifiques de votre initiative

Notre projet se déroule dans le cadre unique d'une simulation d'attaque contre la salle des 4AS, la seconde section de notre école. Dans une ambiance de rivalité amicale, cette initiative vise à mettre à l'épreuve nos compétences en sécurité tout en ajoutant une dimension ludique à nos interactions quotidiennes. Nous avons imaginé et créé un scénario de CTF basé sur des attaques réalistes visant le WiFi, les caméras de surveillance, les cartes d'accès, l'installation d'un keylogger, et même la création d’un brouilleur. Chacune de ces activités a été minutieusement conçue pour tester nos connaissances, stimuler notre créativité, et surtout, renforcer notre compréhension des défis de la sécurité IoT.

## Mise en avant du scénario élaboré

Au fil des pages qui suivent, plongeons dans les détails de notre projet, explorons les activités captivantes que nous avons mises en place, et découvrons les enseignements que nous avons tirés de cette expérience unique. Notre objectif n'était pas seulement de défier les compétences techniques, mais aussi de favoriser un environnement d'apprentissage dynamique et amusant au sein de notre communauté éducative

# II. Activité 1: Piratage WiFi

L'acte initial de notre simulation de CTF s'est déroulé dans l'enceinte de notre salle de classe, où trône notre propre boîtier WiFi, soigneusement configuré par nos soins. Ce premier défi visait à évaluer notre aptitude à percer les défenses d'un réseau sans fil, en mettant en lumière la nécessité d'une sécurité robuste dans le monde connecté qui nous entoure.

## Description détaillée de l'activité

Dans un souci de réalisme, nous avons instigué une attaque ciblée sur notre réseau WiFi local. La configuration de la box que nous avons utilisée a été délibérément pensée pour refléter les paramètres d'un environnement réel.

Les participants seront confronté à la tâche ardue de percer le mot de passe de notre réseau Wifi. Notre équipe avait préalablement modifié ce dernier, adoptant un schéma bien défini, mêlant majuscules, minuscules et chiffres.

Cette méthodologie vise à tester non seulement la capacité de nos participants à contourner les protections, mais également leur perspicacité à déchiffrer des modèles de mots de passe en connaissant le paterne du mot de passe.

## Méthodologie pour simuler un réseau WiFi

## Attaque du réseau Wifi

# III. Activité 2: Redirection du Flux Vidéo de la Caméra

L'exploration de la sécurité IoT a pris une dimension concrète avec notre deuxième activité, centrée sur la simulation d'une caméra de surveillance connectée. Pour ce faire, nous avons opté pour une approche pratique en utilisant une Raspberry Pi, équipée d'un module caméra, créant ainsi une véritable caméra de surveillance. Cette activité avait pour objectif de tester notre habileté à contourner les dispositifs de sécurité associés aux objets connectés.

## Contextualisation de l'activité

Nous avons orchestré un réseau simulé composé d'une caméra de surveillance unique. La Raspberry Pi, agissant comme une caméra réelle, étant équipée de LEDs servant à signaler la détection de présence et les éventuels problèmes de connexion avec la caméra.

Les participants seront vu confier la mission de détourner le flux vidéo en direct de la caméra.

La Raspberry Pi, en continu, transmet le flux vidéo vers le routeur(une seconde Raspberry), et les LEDs sont programmées pour refléter différentes conditions, ajoutant une couche de réalisme au scénario.

Les participants devront rediriger ce flux vidéo sans se faire repérer.

## Méthodologie pour simuler une caméra de surveillance

## Attaque du réseau de caméras simulé

# IV. Activité 3: Piratage de Carte d'Accès

Pour la troisième étape de notre Capture The Flag IoT, nous avons mis en scène une attaque simulée sur les systèmes de sécurité physique en simulant le piratage d'une carte d'accès. Cette activité a été conçue pour évaluer notre aptitude à comprendre et à exploiter les mécanismes de sécurité physiques, un aspect souvent négligé dans le monde de la cybersécurité.

## Explication détaillée du scénario

Les participants seront chargés de comprendre le fonctionnement des cartes d'accès, en identifiant les vulnérabilités potentielles dans le système.

Le scénario a inclus la possession d'une carte d'accès d'un ancien élève dont le mot de passe était connu, mais dont l'identifiant était désactivé, empêchant ainsi l'accès physique aux locaux, et une Raspberry servant avec un lecteur de carte servant à simuler un véritable système de carte d’accès.

Les participants devront élaborer des stratégies pour contourner cette restriction en explorant la façon dont les cartes d'accès étaient vérifiées et validées. Ils seraient alors possible d’opté pour des attaques de type relais, ou encore exploité des faiblesses dans le processus de désactivation des cartes.

## Méthodologie pour simuler une carte d'accès

## Attaque de carte d’accès

# V. Activité 4: Création d'un Keylogger

Au cœur de notre quête pour explorer les vulnérabilités IoT, nous avons introduit une activité mettant en scène la création et le déploiement d'un keylogger. Cette tâche délicate vise à évaluer la compréhension des participants quant aux menaces liées à l'enregistrement des frappes, et comment ils pourraient se défendre contre de telles attaques.

## Présentation de l'activité

Les participants seront chargés de mettre en place un keylogger depuis une Raspberry, un outil sournois capable d'enregistrer les frappes effectuées sur un clavier. Le scénario simule la nécessité d'accéder discrètement aux identifiants d'élève à l'insu de ces derniers, soulignant ainsi les risques associés à la compromission de la sécurité des systèmes d'information.

## Processus de création du scénario de keylogging

# VI. Activité 5: Onde radio

Dans le cadre de notre exploration des vulnérabilités des objets connectés (IoT), nous avons introduit une activité axée sur la conception et le déploiement d'un brouilleur radio. Cette tâche complexe vise à évaluer la compréhension des participants concernant les menaces associées à ces dispositifs, contre lesquelles il est difficile de se défendre.

## Présentation de l'activité

Les participants seront tout d'abord invités à se familiariser avec l'utilisation d'une antenne TNT depuis leurs ordinateurs, ainsi qu'avec des outils tels que SdrSharp. Ceci se fera à travers un petit Capture The Flag (CTF) où nous émettrons le drapeau sur une onde radio, et les participants devront le déchiffrer.

Après avoir acquis des connaissances sur la réception des ondes radio, ils seront ensuite sollicités pour émettre en créant un brouilleur radio. Ils disposeront d'une Raspberry Pi et d'un câble de 20 à 30 cm.

## Processus de récupération du flag

Chaque jour, nous sommes exposés à la radio, que ce soit chez nous, dans notre voiture, sur notre téléphone, etc. C'est pourquoi nous avons pensé qu'un petit CTF portant sur ce sujet serait intéressant.

Nous utilisons une Raspberry Pi équipée d'un câble d'une vingtaine de centimètres pour simuler notre propre station de radio. Lorsque nous trouvons la fréquence de notre station, comme pour une station réelle (NRJ, Skyrock, etc.), nous pouvons visualiser le nom de la station et un texte radio (souvent le nom de la chanson diffusée). Bien sûr, nous pouvons également entendre la musique ou le son diffusé. Cette partie peut être réalisée depuis un ordinateur, un téléphone portable ou une voiture. Les participants trouveront un drapeau chiffré dans le texte radio, avec une clé de chiffrement qu'ils n'ont pas encore. Mais comment la trouver ?



Figure : Photo de la station que l’on créé

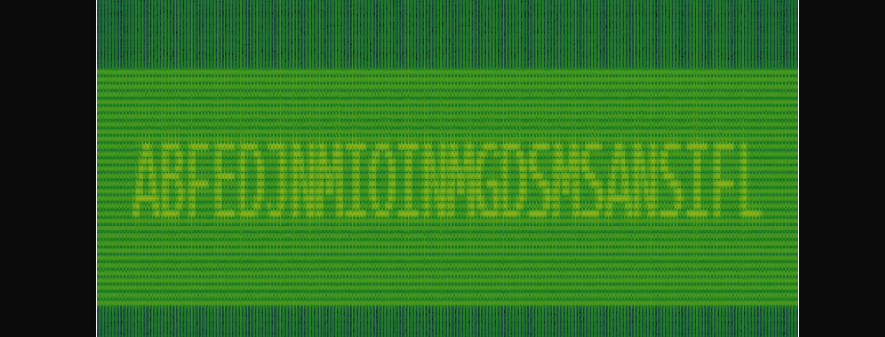
La deuxième partie concerne la stéganographie, un processus consistant à cacher une image dans un son. Le drapeau sera dissimulé dans le son diffusé sur notre station de radio, et les participants devront récupérer ce son et l'analyser avec des outils tels que Sonic Visualiser pour retrouver la clé de chiffrement.

Figure : Photo du spectre de notre son

Nous utilisons le code fourni part <https://github.com/solusipse/spectrology> pour encoder un fichier image en données audio, de sorte que le message visuel est incorporé dans le signal sonore.

Enfin, les participants devront comprendre l'algorithme de chiffrement, dont ils disposeront du fichier source, afin de déchiffrer le drapeau.

## Processus de création du scénario de brouilleur radio

Après avoir compris comment recevoir une onde radio, les participants devront étudier la manière d'émettre une onde radio. Ils auront à leur disposition une Raspberry Pi ainsi qu'un câble de 20 à 30 cm qui servira d'antenne.

De nombreux exemples sont disponibles sur des référentiels publics GitHub, dont ils pourront s'inspirer. Cependant, voici les étapes principales pour la création d'un brouilleur radio à partir d'une Raspberry Pi. :

 **Raspberry Pi Configuration :** Configurez la Raspberry Pi

 **Ajout d'un Module Émetteur :** Intégrez un module émetteur radio fréquence (RF) compatible avec la Raspberry Pi.

 **Antenne :** Connectez une antenne au module émetteur pour diffuser le signal sur une certaine distance. L'antenne doit être adaptée à la fréquence de fonctionnement.

 **Réglage de la Fréquence :** Paramétrez la fréquence d'émission du brouilleur radio

 **Programmation :** Élaborez un programme sur la Raspberry Pi pour contrôler le module émetteur et régler la fréquence d'émission.

Un exemple de brouilleur radio est disponible sur notre GitHub :

<https://github.com/yanistvg/CTF-IOT-Project/tree/main/radio/fm_transmitter-master>



Figure : Photo de notre brouilleur radio

# VII. Analyse Transversale des Activités

Cette phase d'analyse transversale offre une perspective holistique sur les différentes activités de notre Capture The Flag (CTF) IoT, mettant en évidence les similitudes, les disparités et les enseignements transposables à l'ensemble du projet.

## Comparaison des différentes activités en termes de complexité

En évaluant la complexité des activités, nous constatons que le piratage WiFi peut être perçu comme l'étape initiale, tandis que la création d'un keylogger comme plus avancée. Cette comparaison souligne la nécessité de comprendre progressivement les nuances de la sécurité IoT, en commençant par des concepts fondamentaux avant de progresser vers des défis plus élaborés.

## Points forts et points faibles de chaque activité

L'analyse détaillée de chaque activité révèle des points forts et des points faibles spécifiques.

Par exemple, le piratage de cartes d'accès a mis en évidence des vulnérabilités potentielles dans les mécanismes physiques de sécurité, tandis que la redirection de flux vidéo a souligné des risques associés à la confidentialité.

Cette compréhension fine permettra d'identifier les domaines où les compétences des participants se sont particulièrement distinguées et ceux qui nécessitent davantage d'attention.

## Considérations sur la variété des compétences testées

Les activités ont mis à l'épreuve une gamme diversifiée de compétences, allant de la programmation et de l'analyse réseau à la compréhension des vulnérabilités physiques. Cela souligne l'importance d'une approche holistique de la sécurité IoT, exigeant des participants qu'ils combinent des connaissances techniques avec des compétences en ingénierie sociale et en éthique pour réussir l'ensemble des défis.

Cette analyse transversale vise à dévoiler des tendances récurrentes et à fournir des informations exploitables pour orienter les futures itérations du CTF IoT. Elle souligne également l'importance de concevoir des scénarios diversifiés pour garantir une évaluation complète des compétences des participants dans le domaine complexe et en constante évolution de la sécurité des objets connectés.

# VIII. Conclusion

## Récapitulation des points forts du projet

En récapitulant les points forts de ce projet de Capture The Flag (CTF) dédié à l'Internet des objets (IoT), il est clair que notre démarche a permis de mettre en lumière la diversité des compétences nécessaire à un ingénieur STI et de renforcer la compréhension des défis complexes liés à la sécurité IoT. Parmi les réalisations notables, la conception de scénarios réalistes a stimulé notre créativité.

## Perspectives futures et continuité du projet

Quant aux perspectives futures et à la continuité du projet, nous envisageons d'approfondir notre exploration des tendances émergentes en matière de sécurité IoT. Cette expérience ne marque pas la fin, mais plutôt le début d'une trajectoire continue visant à éduquer, à sensibiliser et à préparer les professionnels de la cybersécurité aux défis dynamiques de notre monde de plus en plus connecté.

Les perspectives à venir incluent l'exploration approfondie des évolutions technologiques, l'intégration de nouveaux scénarios et la consolidation des leçons tirées de cette expérience.

Ainsi, cette conclusion ne marque pas la clôture, mais plutôt l'ouverture de portes vers de nouvelles opportunités d'apprentissage, de recherche et d'innovation en matière de sécurité IoT. L'avenir de ce projet s'inscrit dans une démarche dynamique d'adaptation constante aux évolutions du paysage de la cybersécurité, avec pour objectif ultime de former des professionnels aguerris et prêts à relever les défis complexes à venir.