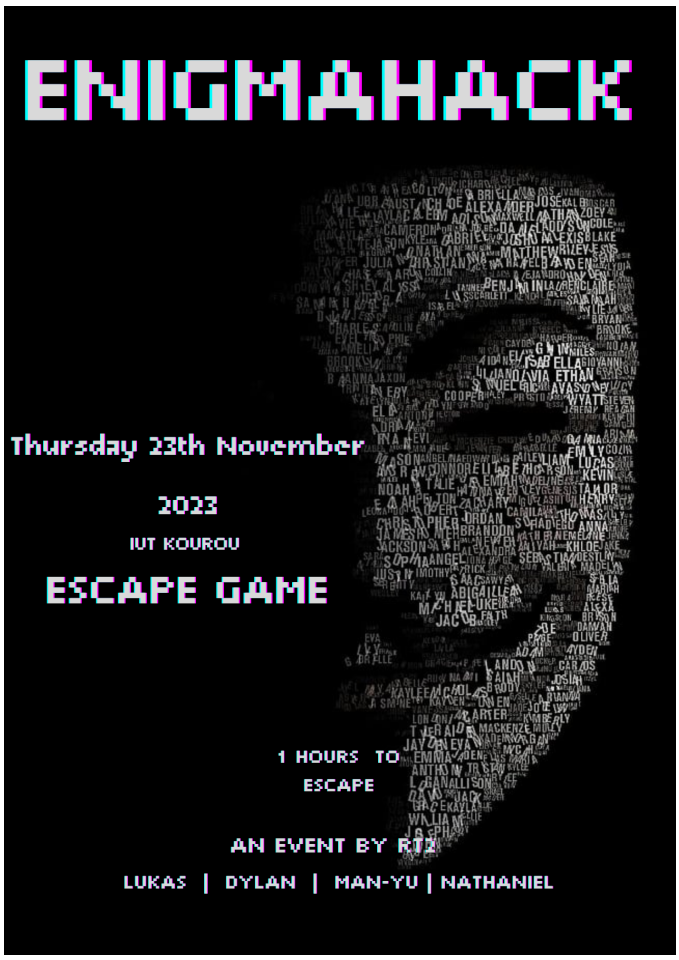
COMPTE RENDU FINAL ENIGMAHACK

Mettre en oeuvre un système de transmission sans fil



GARCIA DYLAN, LING MAN YU, BORDES NATHANIEL & STANKOWICH LUKAS

21/12/2023

Réseaux & Télécommunication 2

INTRODUCTION

Au cours de la SAE 31, notre équipe de quatre membres composée de Nathaniel, Dylan, Man Yu et Lukas a entrepris le défi captivant de concevoir un escape game innovant. L'objectif principal de cette SAE était de nous immerger dans de nouvelles méthodes de transmission de données sans fil, explorant des technologies telles que la radio et l'infrarouge.

Ce compte rendu détaillera notre aventure à travers cette SAE, mettant en évidence les découvertes faites, les défis relevés et les résultats obtenus au cours de cette exploration fascinante des moyens de communication modernes.

Découverte des Technologie :

Dans cette première phase de notre SAE, chaque membre de l'équipe s'est plongé dans l'univers fascinant des technologies de communication sans fil. Individuellement, nous avons exploré divers domaines, élargissant notre compréhension des moyens innovants de transmission de données. Voici un aperçu des technologies découvertes :

Radio :

- Nous avons exploré les principes fondamentaux de la communication radio, comprenant les différentes fréquences et les applications possibles dans le contexte de notre escape game.

Infrarouge :

- La technologie infrarouge a captivé notre attention, offrant des possibilités uniques pour des interactions sans fil, en particulier dans des environnements restreints.

Ultrasons :

- Nous avons étudié l'utilisation d'ondes ultrasonores pour la transmission de données, en particulier dans des scénarios nécessitant une détection précise.

Électroaimant :

- La manipulation des champs magnétiques à l'aide d'électroaimants a été explorée, ajoutant une dimension interactive à notre projet.

Raspberry Pi avec Radio Pirate :

- L'intégration de Raspberry Pi avec une radio pirate a ouvert des possibilités de communication sophistiquées, élargissant notre compréhension des solutions matérielles.

Matrice LED avec Arduino :

- Nous avons expérimenté la création de visuels dynamiques en utilisant des matrices LED avec Arduino, enrichissant ainsi le volet visuel de notre escape game.

RFID/NFC :

- Les technologies RFID (Radio-Frequency Identification) et NFC (Near-Field Communication) ont été examinées pour leurs applications potentielles dans la gestion des épreuves.

Écrans Arduino :

- L'utilisation d'écrans Arduino a été explorée pour afficher des informations cruciales et créer une expérience immersive pour les participants.

Élaboration du Plan de Jeu :

Dans cette phase collaborative, l'équipe s'est réunie pour concevoir un escape game immersif qui guiderait les participants à travers un fil conducteur tout en permettant certaines épreuves en parallèle. La réflexion conjointe a abouti à la création de dix épreuves captivantes, intégrant diverses technologies découvertes lors de la phase précédente. Voici un aperçu détaillé des épreuves planifiées, chacune contribuant à l'expérience globale :

1. Keyless Access (Lukas) :

- Ici les participants devaient trouver une carte RFID dans la salle qui leur permettrait de déverrouiller le pc de jeux (épreuve abandonnée pour cause de non fonctionnement).

2. Enigahack (Lukas):

- Une épreuve dans laquelle le flag est caché dans le site web ou les joueurs entre les flags.

3. SAFE Chest (Man yu) :

- Un calcul mathématique était inscrit au tableau, son résultat nous donne le code d'un cadenas à 3 chiffres. Le cadenas verrouille un coffre-fort, coffre-fort que les candidats doivent trouver dans la salle.

4. Switch Access (Nathaniel):

- Une épreuve de réseau dans laquelle il devait accéder à une interface de configuration d'un switch.

5. Look Around (Dylan) :

- Ici une matrice led avec un smiley qui sourit et dans la salle qui donne accès au mode de configuration du switch

6. 94.3MHz (Dylan) :

- La radio nous a donné un audio qui permettait d'entendre une IP d'un serveur.

7. SSH crackme (Dylan):

- Avec l'IP donnée précédemment on initialise une connexion ssh et on crack le mot de passe.

8. Terminal ./prgm.py (Lukas) :

- Ici un programme python teste la connexion ping avec l'extérieur pour savoir si la configuration a été bien faite.

9. You Can Do It (Man yu):

- Sur le compte "crackme" se trouve un jeu de mémoire que les candidats

devront résoudre afin d’obtenir un code morse et le décoder.

10. Stéganographie (Dylan) :
    - La dernière épreuve engage les participants dans une analyse Stéganographie, les poussant à explorer les éléments de l'escape game sous un nouvel angle.

Chaque épreuve a été soigneusement sélectionnée pour contribuer à l'intrigue générale tout en mettant en avant les différentes technologies et compétences apprises au cours de notre cursus R&T. Cette phase de planification a jeté les bases d'un escape game stimulant et diversifié.

Programmation Arduino :

Pour notre escape game, nous avons initialement envisagé l'utilisation de deux programmes Arduino. Cependant, suite à l'abandon du RFID, nous avons consolidé nos efforts sur un seul programme, élaboré par Dylan. Ce programme a pour objectif d'afficher un smiley sur une matrice LED 16x16, utilisant les bibliothèques Neomatrix et NeoPixel.

Une difficulté majeure à laquelle nous avons fait face était l'alimentation de la grande matrice. Pour résoudre ce problème, nous avons décidé d'utiliser deux cartes Arduino en tandem. Un autre défi était le mappage de la matrice, et pour résoudre cela, j'ai collaboré avec Lukas pour créer un fichier Excel détaillant le mappage, où chaque cellule correspond à une LED avec ses coordonnées.

Concernant la partie programmation, nous développé un code utilisant la matrice pour allumer spécifiquement certaines LED afin de former le visage souriant. L'utilisation des bibliothèques Neomatrix et NeoPixel a grandement facilité cette tâche, permettant une gestion efficace de l'éclairage de chaque LED.

L'un des enseignements importants de cette expérience a été la nécessité de coordonner l'alimentation de la matrice avec précision, en utilisant deux cartes Arduino de manière synchronisée. De plus, le mappage précis de la matrice à l'aide d'un fichier Excel a simplifié le processus de programmation, assurant un affichage cohérent du smiley.

Dans l'ensemble, cette réalisation témoigne de notre capacité à résoudre des problèmes complexes, à collaborer efficacement et à utiliser les ressources disponibles pour concrétiser notre vision dans le cadre de notre escape game.

Réalisation de la radio Pirate :

Tout d'abord, j'ai mis en place une radio pirate en utilisant un Raspberry Pi 4, qui utilise le logiciel PiFmRds qui permet d'émettre sur une fréquence que nous avons choisie avec la commande suivant :

$ pi_fm_rds -ps PiRateFM -audio adresseIP.wav -freq 94.3M

Le programme propose plusieurs options. Il y a quelques fichiers d'exemple

fournis, dont un fichier st´er´eo (st´er´eo 44100.wav) qui alterne un message `a droite

et à gauche. Les options sont :

-freq freq : la fréquence d'´émission ;

-audio fichier : le fichier audio jou´e ;

-pi picode : le picode identifie la radio, ;

-ps texte : Le nom de la station sur huit caract`eres ;

-rt texte : diffusion de texte, comme le nom du morceau de musique ;

-ctl fifo : fichier fifo permettant de contrˆoler l'émission ;

-ppm : dans certains cas, si le récepteur ne reçoit pas le signal RDS, il faut

calibrer l"émetteur.

Cette commande nous a permis d'attribuer à la fréquence 94.3Mhz un audio qui donnait une adresse IP.

Réalisation cracking SSH :

Les participants de l'escape game ont dû réaliser une attaque par dictionnaire sur le compte crackme avec la commande hydra suivante :

hydra -l crackme -P rockyou.txt ssh://10.102.64.64

Cette commande nous donne le mot de passe du compte crackme qui nous permettait d'avancer dans le jeu.

Troll:

Un code Morse a été mis au tableau afin de faire perdre du temps au Participant, le but de ce code morse était de faire monter les participant au premier étage ou il ont trouvé un message .

Programmation du Jeu en C++ :

Bonjour Bonjour… !

Le programme se lance avec la commande ./compile (qui lui lance la commande de compilation g++ en bash.)

Le jeu est codé en objet et composé de plusieurs sous-programmes qui s'incluent ensemble. (ex : map.cpp s'occupe de l'affichage de la carte, tile.cpp s'occupera lui des cases du tableaux et pgrm.cpp fait le liens entre l'input de l'utilisateur et le jeu, etc)

Quand le jeu est terminé, le programme lance un script qui utilise la commande speaker-test. Cette commande permet de créer du son à la fréquence et au temps voulu. Le script pourra ainsi jouer le flag en code morse.

Réalisation du Réseau :

Switch Access

Cette épreuve consistait, elle a accédé à un switch sécurisé par un mot de passe console ainsi qu'un mot de passe enable qui permet un accès privilégié afin de pouvoir effectuer différentes modifications au sein de la configuration du switch (VLAN, gestion des ports) et rétablir la communication des appareils du réseau local et l'accès à Internet via le réseau de l'IUT auquel le switch était interconnecté. Pour parvenir à cela, il faut donc disposer d'un PC doté d'un connecteur série afin de brancher le câble console qui permet la gestion du switch, sur ce même ordinateur, il faut avoir l'application PuTTY qui nous sert de

terminal de configuration. Dans le cadre de cette épreuve, nous avions caché le câble console et le mot de passe console dans un coffre qui devait être trouvé dans un coffre dans une épreuve précédente. Pour la configuration de ce switch, nous avons éteint tous les ports du switch ensuite nous avons attribué au vlan ESCAPEGAME les ports sur lesquels les ordinateurs devaient être connectés afin de communiquer.

Commandes à utiliser :

Conf t (afin d'accéder au terminal de configuration)

Int range fa 0/1-24 (commandes qui permet de configurer un groupe d'interfaces en même temps, ici nous avons sélectionné toutes les interfaces)

No shutdown (commandes qui permet de réactiver toutes les interfaces)

Vlan "numéro du vlan" (commande permettant de créer un vlan)

Name (afin d'attribuer un nom au vlan)

Switchport mode Access (afin de configurer un port en mode d'accès et pouvoir l'affecter à un vlan)

Switch port Access vlan "numéro du vlan" (commande qui permet d'affecter le port au vlan désirer)

Réalisation du Site Web :

Dans cette étape cruciale de notre projet, la création du site web avait un double objectif. Tout d'abord, il devait collecter les flags découverts par l'équipe tout au long de l'escape game. De plus, grâce à une interface administrateur, nous pouvions analyser le temps que chaque équipe mettait pour terminer l'ensemble du jeu.

1. Objectif de Collecte des Flags et Suivi du Temps :

- Le site web avait pour première mission de collecter les flags trouvés par

l'équipe et de fournir, via une interface admin, des informations sur le temps mis par chaque équipe pour résoudre l'ensemble des épreuves.

2. Gestion Fluide des Équipes et des Challenges :

- Pour assurer une expérience fluide, j'ai mis en place un système où chaque utilisateur créant une équipe voyait automatiquement les défis liés à sa formation ajoutés à une base de données. Chaque challenge était associé à un ID défini dans l'ordre croissant, facilitant ainsi la progression linéaire.

3. Technologies Employées :

- Le site web a été développé en utilisant PHP et JavaScript pour la gestion des messages dynamiques. La sécurité a été renforcée grâce à une base de données avec des flags et des mots de passe hashés, garantissant la confidentialité des informations.

4. Base de Données et Gestion des Challenges :

- La base de données comprenait une table pour les challenges, stockant l'ID et le hash du challenge. Les flags côté utilisateur étaient hachés avec un salt et comparés au hash en base de données. En cas de succès, la table ChallengeTeam était mise à jour, passant la variable associée au challenge à 2, indiquant ainsi de passer au challenge suivant.

5. Implication dans la Réalisation :

- La réalisation du site web et de la base de données a été menée exclusivement par moi-même, mettant à profit mes compétences acquises au cours du cursus R&T.

6. Design Inspiré de la Culture Hacker :

- Pour le design, j'ai puisé dans l'esthétique associée à la culture hacker, optant pour une palette de couleurs verte et noire simple. L'utilisation de tableaux a permis une présentation claire des données.

7. Synchronisation Automatique des Challenges :

- La synchronisation des épreuves se faisait de manière automatique par le biais de rafraîchissements. Lorsqu'un flag correct était soumis, le système passait naturellement au challenge suivant.

8. Absence de Problèmes lors de la Première Édition :

- À la première édition du jeu, aucune difficulté majeure n'a été rencontrée, témoignant de l'efficacité de la conception du site web et de sa mise en œuvre.

9. Utilisation des Compétences Acquises au Cours du Cursus :

- Aucune technologie externe n'a été utilisée dans la réalisation du site web. Les compétences acquises au cours du cursus R&T ont été suffisantes pour répondre aux besoins.

10. Retours Positifs des Utilisateurs :

- Les retours des utilisateurs ont souligné une ergonomie appréciée, un site simple et une expérience sans problème, ce qui a contribué à la réussite globale de cette composante interactive de l'escape game.

Mode d'Emploi du Jeu :

Partie Admin

Etape 1 : accéder au site web

Etape 2 : accéder a la page administrateur caché du site

Etape 3 : créer un compte admin et se connecter

Etape 4 : créer un nouveau challenge et ajouter les indices nécessaire à la réalisation de l'épreuve

Partie Participants

Etape 1 : accéder au site web

Etape 2 : Créer une team et choisir la formation puis se connecter

Etape 3 : vous arrivez sur la page d'accueil du site ou vous avez le nom de l'épreuve, les indice et le flags à rentrer

Etape 4 : vous pouvez commencer a vous tenter de vous échapper

Les tutos installations des différentes épreuves ont été déposés sur un github .

Solutions aux Énigmes avec Explications :

1. Enigahack (Lukas):
    - Afin de compléter cette épreuve vous devez inspecter le code source de la page
    - FLAG = H7mL_I5_N0t3_53cUR3!!!
3. SAFE Chest (Man yu) :
    - Ici un calcul mathématique était inscrit dans la salle et devait être résolue afin d'avoir un code d'un cadenas à 3 chiffres.
    - FLAG = L3_C0D3_3T_977!!
4. Switch Access (Nathaniel):
    - Pour cette épreuve un câble console avec un mot de passe étaient caché dans le coffre de l'épreuve safe chest ce code permet d'accéder au switch

via l’interface série du PC

- FLAG = S3Ri4l_1sn’7_UsEl3s5!!!

5. Look Around (Dylan) :

- Ici une matrice led avec un smiley qui sourit a été disposée dans la salle et il suffit de trouver le smiley afin de découvrir le flag qui est juste à côté.
- FLAG = Sm1L3

6. 94.3MHz (Dylan) :

- Il faut allumer sa radio sur la fréquence 94.3Mhz et écouter le message.
- FLAG = 10.102.64.64

7. SSH crackme (Dylan):

- Dans les indices de l'escape game on donne le nom du compte qui est crackme .Avec l’IP donnée précédemment on initialise une connexion ssh et on crack le mot de passe avec la commande Hydra suivante:
- commande : hydra -l crackme -P rockyou.txt ssh://10.102.64.64
- FLAG = pokemon

8. Terminal ./prgm.py (Lukas) :

- Ici une fois l’épreuve switch access réussi les PC sont capable de communiquer entre eux, pour vérifier la connexion nous effectuons un ping pour lequel le résultat sera analysé dans un programme en bash et qui renvoie le flag ci-dessous si le ping est réussi
- Flag = ICmP_1s_@n_G0od_pR07oC0Le

9. You Can Do It (Man yu):

- Après avoir cracké le mot de passe du compte “crackme” et s’y être connecté en SSH, la nouvelle épreuve est un programme en C++. Il s’agit d’un mémory où les participants devront matcher les paires de cases dans une grille de 4 x 4.
- A la fin du jeu, un code morse sera joué et ce seront aux candidats de le

déchiffrer afin de trouver le flag.

- Flag = C0DEDBYRTINC

10. Stéganographie (Dylan) :

- Le dernier flag est caché dans l'image de l'escape game qui apparaît après avoir rentré le flag précédent.Grâce à la commande suivante les participants ont donc le dernier flag et on termine le jeu et peuvent maintenant sortir de ENIGMAHACK.
- Commande : steghide extract -sf image.jpg
- Flag = W3LL_D0N3_Y0U_w1n!!!

Conclusion :

En conclusion, le projet ENIGMAHACK a été une exploration réussie des technologies de transmission sans fil à travers la création d'un escape game innovant. Notre équipe a appliqué diverses technologies, surmonté des défis techniques, et obtenu des retours positifs des utilisateurs. En résumé, ENIGMAHACK représente un accomplissement significatif dans notre parcours académique et professionnel.

Annexe :

Liens gitHub : https://github.com/shadowfr97/Escape-Game.