الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne démocratique et populaire

وزارة التعليم العالي و البحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة سعد دحلب البليدة
Université SAAD DAHLAB de BLIDA

كلية التكنولوجيا
Faculté de Technologie

قسم الإلكترونيك
Département d'Électronique

Mémoire de Master

Filière Télécommunications
Spécialité Réseaux & Télécommunications

présenté par

ABDELAZIZ Mounira

&

BOUANANI Hiba

Techniques de sécurité des objets connectés contre les attaques réseaux

Proposé par : Mr. KABIR Yacine

Année Universitaire 2022-2023

Remerciements

Ce travail a été effectué au sein du Département d'électronique de l'Université de Blida1,

En premier lieu nous remercions DIEU tout puissant de nous avoir donné la patience, la santé et la volonté pour achever ce travail

Nous remercions nos parents pour leurs sacrifices et l'aide pour que nous réussissions, de nous avoir donné l'importance, de prendre toujours soin de nous, de nous faire confiance et de toujours nous démontrer l'amour que vous nous portez.

Nous adressons nos sincères remerciements à notre professeur Mr KABIR Yacine pour avoir consacré son temps précieux et avoir accepté de nous encadrer, pour tous les efforts et l'importance qu'il nous a donnée.

Nous remercions Les membres de jury pour avoir accepté d'examiner notre modeste travail.

ملخص: في هذه الرسالة بعنوان الأمان التقني للكائنات المتصلة ضد هجمات الشبكة ، اعتمدنا على دراسة نقاط ضعف الكائنات من خلال تقديم مفاهيم الكائنات المتصلة والبروتوكولات المستخدمة وهجمات الشبكة الشائعة ESP32 المتصلة على منصة بالإضافة إلى أحدث ما توصلت إليه التقنية فيما يتعلق بأمن الكائنات المتصلة واستكشفنا إبراز نقاط الضعف المحددة ، وصفنا مع تحليل نتائجهم ، ومناقشة .Wireshark و Kali Linux التجربة من خلال تغطية تكوين بيئة الاختبار واستخدام أدوات مثل نقاط الضعف التي تم تحديدها واقتراح التدابير الأمنية المقابلة.

كلمات المفاتيح: الاجهزة المتصلة: IoT, ESP32, Kali Linux, Wireshark, Attaque réseau

Résumé : dans ce mémoire qui est intitulé technique de sécurité des objets connectés contre les attaques réseaux , on a basé sur l'étude de vulnérabilités des objets connectés sur la plateforme ESP32 en présentant les concepts des objets connectés, les protocoles utilisés et les attaques réseau courantes ainsi que l'état de l'art sur la sécurité des objets connectés et explorés mettant en évidence les vulnérabilités spécifiques, on a décrit l'expérimentation en couvrant la configuration de l'environnement des tests et l'utilisation des outils tels que Kali Linux et Wireshark. Avec leurs résultats analysés, discutant les vulnérabilités identifiées et proposant des mesures de sécurité correspondants.

Mots clés :IoT, ESP32, Kali Linux, Wireshark,.Attaque réseau

Abstract: in this dissertation, which is entitled technical security of connected objects against network attacks, we have based on the study of vulnerabilities of connected objects on the ESP32 platform by presenting the concepts of connected objects, the protocols used and the common network attacks as well as the state of the art on the security of connected objects and explored highlighting the specific vulnerabilities, we described the experimentation by covering the configuration of the test environment and the use of tools such as Kali Linux and Wireshark. With their results analyzed, discussing the identified vulnerabilities and proposing corresponding security measures.

Keywords : IoT, ESP32, Kali Linux, Wireshark, Network Attack.

Liste des acronymes et abréviations

CERP-IoT: Cluster des Projets Européens de Recherche sur l'Internet des Objets.

Cmd: Windows Command Prompt.

CoAP: Constrained Application Protocol.

DOS: Denial Of Service.

GPS: Global Positioning System

GSM: Global System for Mobile Communications

HTTP : HyperText Transfer Protocol

IdO : Internet des Objets.

IoT: Internet of Things.

IP: Internet Protocol

IPV4 : Internet Protocol Version 4

IPV6 : Internet Protocol Version 6

LoRa: Low Range

LWPAN: Low-Power Wide-Area Network

MitM: Man-in-the-Middle

MQTT: Message Queue Telemetry Transport.

M2M: Machine To Machine.

OC: Objet Connecté.

TCP: Transmission Control Protocol

UDP: User Datagram Protocol.

WIFI: WIreless FIdelity

XML: Extensible Markup Language

XMPP: Extensible Messaging and Presence Protocol

Table des matières

Liste des figures

Introduction générale

L'avènement de l'Internet des objets (IoT) a ouvert la voie à une nouvelle ère de connectivité où les Objets du quotidien deviennent intelligents et interconnectés. Cependant, Cette révolution Technologique soulève des préoccupations majeures en matière de sécurité. Les objets connectés, tels Que les dispositifs basés sur ESP32, sont devenus des cibles privilégiées pour les attaquants cherchant à exploiter leurs vulnérabilités et à perturber notre vie quotidienne.

Dans ce contexte, cette étude se concentre sur les techniques de sécurité visant à protéger les objets Connectés contre les attaques réseau. Son objectif est de comprendre les défis et les risques auxquels Sont confrontés les dispositifs IoT, En mettant particulièrement l'accent sur les objets connectés basés Sur ESP32. En analysant en profondeur les vulnérabilités spécifiques à ces dispositifs, nous cherchons à identifier les failles potentielles et à proposer des mesures de sécurité efficaces pour renforcer leur Résilience face aux attaques.

Cette étude s'appuie sur une combinaison d'expertise en sécurité informatique, En réseaux et en objets Connectés. Elle vise à combler le fossé entre le monde de la sécurité et celui des objets connectés, en Fournissant des recommandations pratiques et des solutions concrètes pour améliorer la protection des Dispositifs IoT. En explorant les protocoles couramment utilisés dans les objets connectés, en Analysant les vulnérabilités les plus fréquemment rencontrées et en menant des tests de sécurité Approfondis, nous espérons contribuer à l'élaboration de normes de sécurité solides pour l'ensemble de L'écosystème IoT.

L'importance de cette étude ne se limite pas seulement à la sécurité des objets connectés basés sur ESP32, mais elle a également des répercussions plus larges sur la confiance et l'adoption de l'IoT dans Notre société. En renforçant la sécurité des objets connectés, nous contribuons à préserver la vie privée Des utilisateurs, à protéger les données sensibles et à éviter les conséquences potentiellement Dommageables des attaques sur les infrastructures critiques.

En conclusion, cette étude sur les techniques de sécurité pour les objets connectés contre les attaques Réseau représente une étape cruciale pour assurer un développement durable et sécurisé de l'IoT. En Combinant une compréhension approfondie des vulnérabilités spécifiques à ces dispositifs, une Analyse rigoureuse des résultats des tests de sécurité et des recommandations pratiques, nous aspirons à promouvoir un environnement IoT plus sûr et plus fiable. Il est impératif d'agir dès maintenant pour Garantir que les bénéfices des objets connectés ne soient pas compromis par des failles de sécurité, et Pour que notre avenir connecté soit véritablement sûr et protégé.

Chapitre 1 Etat de l'art sur la sécurité des objets connectés

1.1 Introduction

En raison de plusieurs facteurs notamment l'utilisation des réseaux informatiques pour la transmission des données vers les objets connectés à des risques d'accès et de manipulation des données par des personnes non autorisées d'un façon accidentelle ou bien intentionnelle sont apparus et par conséquent les attaques et les actes de malveillance informatique sont devenus plus fréquents et plus dangereux.

A travers ce projet nous allons voir comment une personne malveillante peut attaquer un objet connecté avec un réseau informatique et puis on va faire des traitements de protection contre ces attaques.

Ce chapitre présente des définitions globales des schémas explicatifs, des explications…et à la fin des techniques et méthodes des protections qui sont nécessaires à la mise en place d'une politique de sécurité des réseaux d'entreprise.

1.2 Les objets connectés

1.2.1Définition

Les objets connectés, également appelés Internet des objets (IdO), sont des dispositifs physiques qui intègrent des capteurs, des logiciels et des technologies de communication pour se connecter à un réseau. Ils peuvent collecter des données, interagir avec leur environnement et prendre des décisions autonomes ou être contrôlés à distance. Ces objets utilisent des technologies sans fil pour se connecter, tels que le Wi-Fi ou le Bluetooth. Ils peuvent être des appareils domestiques, des véhicules connectés, des dispositifs médicaux ou des infrastructures urbaines intelligentes. Les objets connectés collectent des données grâce à des capteurs, qui sont ensuite traitées localement ou transmises à des serveurs distants.

Le groupe de travail Internet of Things Global Standards Initiative (IOT-GSI),Piloté par l'international Télécommunication Union (ITU), considère l'IOT comme **«** une infrastructure mondiale au service de la société de l'information » permettant d'offrir des services évolués en interconnectant des objets

(physiques et virtuels) grâce à l'interopérabilité de technologies de l'information et de la communication Existantes ou en évolution de son côté, l'IEEE définit l'IOT comme un « réseau d'éléments chacun muni de capteurs qui sont connectés à Internet »[1]

Le CERP-IOT « Cluster des projets européens de recherche sur l'Internet des Objets » définit l'Internet des Objets comme : « une infrastructure dynamique d'un réseau global. Ce réseau global a des capacités d'auto-configuration basée sur des standards et des protocoles de communication interopérables. Dans ce réseau, les objets physiques et virtuels ont des identités, des attributs physiques, des personnalités virtuelles et des interfaces intelligentes, et ils sont intégrés au réseau d'une façon transparente » [2]

1.2.2Domaines d'application

Plusieurs domaines d'application sont touchés par l'IOT, Parmi ces principaux domaines nous citons : le domaine de la sécurité, le domaine du transport, l'environnement et l'infrastructure et les services publics…etc. Nous allons maintenant détailler ces secteurs :[3]

Figure 1 domaine d'application de l'IoT

a. *Transport*

Depuis la création de l'IOT en 1999, le nombre des véhicules intelligents sont en croissance, presque Tous les véhicules vendus aujourd'hui dans le monde renferment déjà des capteurs et de moyens de communication pour traiter la congestion du trafic, la sécurité, la pollution et le transport efficace des marchandises, etc.

L'objectif est qu'une voiture soit capable de communiquer de façon autonome avec d'autres véhicules ou une centrale de surveillance pour prévenir les accidents et réduire les coûts d'assurance.[3]

b. *La santé*

Le secteur de la santé a connu un très grand nombre d'applications permettant à un patient et à son docteur de recevoir des informations, parfois même en temps réels, qu'il aurait été impossible de connaître avant l'apparition d'IOT. Par exemple, (Porteuse Digital Health) qui est le premier

médicament connecté sur le marché grâce à un capteur directement intégré dans l'être humain qui permet après ça le suivi des patients à distance.[3]

c. *La domotique*

La domotique regroupe l'ensemble des technologies permettant l'automatisation des équipements d'un habitat. Elle vise à apporter des fonctions de confort : commandes à distance, gestion d'énergie (optimisation de l'éclairage et du chauffage… etc.), sécurité (comme les alarmes) et de communication (contacts et discussion avec des personnes extérieures)

Les services offerts par la domotique couvrent 3 domaines principaux :

- Assurer la protection des personnes et des biens en domotique par la prévenir des risques d'accident (incendie, fuite de gaz, etc.).
- Confort de la vie quotidienne surtout pour les personnes âgées ou handicapées.
- Faciliter les économies d'énergie grâce à la réactivité maîtrisée d'une maison intelligente.[3]

d. *L'agriculture*

L'agriculture intelligente a pour objet de renforcer la capacité des systèmes agricoles, de contribuer à la sécurité alimentaire en intégrant le besoin d'adaptation et le potentiel d'atténuation dans les stratégies de développement de l'agriculture durable. Cet objectif a été atteint enfin par l'utilisation des nouvelles technologies, telles que l'imagerie satellitaire et l'informatique, les systèmes de positionnement par satellite de comme GPS, aussi par l'utilisation des capteurs qui vont s'occuper de récolter les informations utiles sur l'état du sol, taux d'humidité, taux des sels minéraux, etc. et envoyer ces informations au fermier pour prendre les mesures nécessaires garantissant la bonne production. [3]

1.2.3Qu'est-ce qu'un réseau IoT ?

Un réseau IOT sert à doter des objets d'une connectivité à Internet pour permettre la remontée d'informations. Différents protocoles de communication sont disponibles sur le marché pour effectuer cela. Tous n'ont pas les mêmes caractéristiques. Pour les entreprises qui se lancent dans IOT, choisir le réseau de communication le plus adapté à leurs usages peut ainsi devenir un casse-tête chinois. Deux grandes catégories de réseaux existent sur le marché :

- **Les réseaux longue portée :** on distingue les réseaux basse consommation dits LWPAN comme Sigfox, LoRa, des technologies cellulaires (GSM, 2G, 3G, 4G, 5G). Ces deux types de réseaux longue portée sont capables de faire transiter des data d'un appareil à l'autre sur de vastes distances. Ils sont utilisés par les entreprises qui veulent connecter des kilomètres d'infrastructures à Internet ou dans des projets de smart citées par exemple.

- **Les réseaux à courte portée :** comme le Wifi, le Z-Wave, le ZigBee, ou encore le Bluetooth Low Energy, permettent de transférer des données sur de faibles distances. Ils sont utilisés dans la domotique.

Avant de se pencher dans le détail sur les fonctionnalités techniques de chaque réseau, il faut donc déterminer si ses objets connectés seront ou non situés loin du portail de réception de leurs données. [4]

1.3 Les protocoles des objets connectés

1.3.1COAP (Constrained Application Protocol)

COAP (Constrained Application Protocol) est un protocole de transfert Web Optimisé pour les périphériques et réseaux contraints utilisés dans les réseaux de capteurs sans fil pour former l'Internet des objets. Basé sur le style architectural REST, il permet de manipuler au travers d'un modèle d'interaction client-serveur les ressources des objets communicants et capteurs identifiées par des URI en S'appuyant sur l'échange de requêtes-réponses et méthodes similaires au protocole HTTP. [5]

1.3.2MQTT (Message Queue Telemetry Transport)

MQTT est un protocole standardisé reposant sur TCP/IP. Il est particulièrement utilisé pour transporter des données des objets connectés sur le cloud. Son processus se divise en quatre étapes distinctes : connexion, authentification, communication, terminaison. MQTT permet la gestion des déconnexions et des reconnexions de devises de manière simplifiée. La taille maximale d'un message envoyé avec MQTT est de 256 Mo.

La Qualité de Service (QOS) est ainsi une caractéristique clé du protocole MQTT. Il s'agit d'un accord qui définit la garantie de livraison d'un message spécifique et le type d'authentification utilisé. Il y a trois niveaux de QOS dans MQTT : plus une fois, au moins une fois et exactement une fois. Les deux côtés d'un message envoyé sont à prendre en compte : la remise du message du client au broker et le message du broker au client abonné. Le client qui publie le message sur le broker définit le niveau de QoS du message lorsqu'il envoie le message au broker. Le courtier transmet ce message aux clients abonnés, tout en utilisant le niveau de QoS que chaque client abonné définit au cours du processus d'abonnement. Si le client abonné définit une qualité de service "inférieure" à celle du client, le broker transmet le message avec un QoS inférieur. La QoS donne ainsi au client le pouvoir de choisir un niveau de service correspondant à la fiabilité de son réseau ainsi qu'à sa logique d'application. [6]

1.3.3XMPP (Protocole de messagerie et de présence extensible)

Le protocole XMPP (Extensible Messaging and Présence Protocol) désigne un protocole de communication à code source ouvert conçu pour la gestion des listes de contacts, les intergiciels orientés messages, la maintenance des listes de contacts et la messagerie instantanée (MI).

Il est basé sur XML (Langage de balisage extensible) et offre des fonctionnalités au-delà de la messagerie instantanée typique. L'architecture de XMPP est similaire à celle du courrier électronique. XMPP utilise des technologies et des mécanismes de cryptographie tels que la Messagerie Confidentielle (OTR) pour assurer les plus hauts niveaux de sécurité. [7]

1.4 Le protocole MQTT

1.4.1Définition

MQTT (Message Queuing Telemetry Transport) est un protocole applicatif de messagerie sur le web, dont l'efficacité est de plus en plus approuvée dans de célèbres applications comme la messagerie sur le réseau social Facebook. Avec un mécanisme de communication suffisamment simple pour mieux répondre aux fortes contraintes des réseaux de capteurs connectés à Internet. Un protocole Publish/Subscribe asynchrone qui fonctionne avec TCP. C'est un protocole M2M (Machine to Machine) largement utilisé dans l'IOT. Le protocole MQTT est un protocole à message extrêmement léger. C'est pour cette raison qu'il est adopté dans l'écosystème IOT. Presque toutes les plates formes IOT prennent en charge le protocole MQTT pour envoyer et recevoir des données à partir des objets intelligents. Trois niveaux de qualité de service sont prévus pour la transmission des messages

- Fire and Forget : le message est envoyé une fois et aucun acquittement n'est exigé.
- Delivered at least once : le message est envoyé au moins une fois et un acquittement est exigé.
- Delivered exactly once : un mécanisme en quatre temps assure la délivrance du message une seule et unique fois. [8]

1.4.2Les avantages de protocole MQTT

Il est idéal pour répondre aux besoins suivants :

- Protocole ouvert, simple, léger et facile à mettre en œuvre.
- Idéal pour l'utilisation sur les réseaux sans fils.
- Particulièrement adapté pour utiliser une très faible bande passante.
- Faible consommateur en énergie.
- Très rapide, il permet un temps de réponse supérieur aux autres standards du web actuel.
- Permet une forte fiabilité si nécessaire.

- Nécessite peu de ressources processeurs et de mémoires. [8]

1.4.3Fonctionnement

MQTT est un service de publication/abonnement TCP/IP simple et extrêmement léger. Il fonctionne sur le principe client/serveur. Le serveur, nommé broker, va collecter des informations que les Publisher (les Objet communicants) vont lui transmettre. Certaines informations collectées par le broker seront renvoyées à certains Publisher ayant préalablement fait la demande au broker. Le principe d'échange est très proche de celui de Twitter. Les messages sont envoyés par les Publisher sur un canal appelé topic. Ces messages peuvent être lus par les subscribers (abonnés). Les topics (ou canaux d'informations) peuvent avoir une hiérarchie qui permet de sélectionner finement les informations que l'on désire. Les messages envoyés par les objets communications peuvent être de toutes sortes mais ne peuvent excéder une taille de 256 Mo. [8]

1.4.4Les différents brokers MQTT

- Activemq qui permet d'ajouter MQTT à un serveur Web Apache (Développé par la fondation Apache).
- Jorammq pour l'intégration de MQTT en Java.
- Mosquitto, le broker open-source le plus utilisé dans les projets DIY soutenu par la fondation eclipse.org.
- Rabbitmq, un projet open source disponible également avec un support commercial.
- EMQTT, un projet développé en Erlang/OTP disponible pour Windows, Mac Os X et Linux. [8]

Conçu pour recevoir de très nombreuses connexions (jusqu'à 1 million par serveur). Il est possible de créer un cluster (réseau de serveur) pour accroitre les nombres de connexions simultanées. ActiveMQ et JoramMQ sont des brokers assez spécifiques. Rabbit est plus orienté entreprise avec son offre commerciale.

1.5 La sécurité informatique

Un réseau informatique est un ensemble d'équipement informatique il protégé l'intégrité des technologies de l'information contre les accès non autorisés.

1.5.1Les notions de base de la sécurité

La sécurité informatique a plusieurs définitions pour les objectifs de la sécurité mais on trouve cinq principaux services les plus connus sont :

a. La confidentialité

Permet de protéger les informations sauvegardées ont transmise sur le réseau, c'est-à-dire l'autorisation d'accéder aux données est uniquement pour les personnes autorisées.

b. L'intégrité

C'est-à-dire assurer la transmission des données de façon correcte sans détruite de manière accidentelle ou bien intentionnelle.

c. L'authentification

C'est une procédure qui permet de certifier l'identité d'une personne ou d'un ordinateur et de la légitimité de la demande d'accès faite par une entité.

d. Non-répudiation

Permet à l'expéditeur d'utiliser une clé secrétée pour chaque signature ce qui empêcher le récepteur de simuler une transmission à la place de l'émettre.

e. Disponibilité

Cet objectif permet d'accéder aux données dans des bonnes conditions c'est à dire que le temps d'attente et les temps de service sont raisonnables.

1.6 Les soucis de la sécurité informatique

Les problèmes de cyber sécurité nous concernent tous, quelle que soit l'utilisation que nous faisons d'Internet, ou notre importance sur le web. Particuliers, entreprises, organisations ou associations, nous sommes tous plus ou moins exposés à ces différents problèmes de sécurité informatique, qu'il est important de connaître afin d'employer les mesures de protection les plus adaptées. Voici 3 de ces problèmes de cyber sécurité les plus courants, ainsi que nos conseils pour les résoudre.

1.6.1Le vol de mot de passe

Vous souhaitez vous connecter à votre espace personnel sur une boutique en ligne sur laquelle vous aimez réaliser vos achats, ou pour accéder à votre profil sur votre réseau social préféré, pour autant, un message d'erreur apparaît constamment. Ce message d'erreur vous informe que votre mot de passe est erroné, et, malgré vos essais, aucune des méthodes proposées ne semble pouvoir vous aider à en récupérer l'accès. Ce type de problème peut signifier que vous avez été victime du vol de mot de passe, et qu'un cybercriminel est maintenant en possession de votre compte et des informations privées qui peuvent y être stockées.

1.6.2Les malwares

Il s’agit du type de menace le plus courant sur Internet, auquel vous avez peut-être déjà été confronté. Les malwares, ou logiciels malveillants, ont pour but d’accéder à vos informations personnelles, de bloquer votre accès à certains contenus ou programmes, ils peuvent supprimer certains de vos fichiers ou encore se servir d’une voie d’accès pour propager un virus à de nombreux appareils.

1.6.3Les attaques de ransomware

Le ransomware, ou rançongiciel, est développé par les pirates informatiques dans le but de récupérer vos informations sensibles, qui seront ensuite chiffrées pour vous en interdire l’accès. Pour retrouver ces données, vous devrez accepter la rançon proposée par le cybercriminel, qui pourrait s’avérer particulièrement élevée dans le cas de vidéos privées, ou lorsqu’il s’agit d’informations sensibles concernant le fonctionnement de certaines entreprises, ou leur base de données client. Le cybercriminel peut aussi vous menacer de divulguer ces données au plus grand nombre si vous ne réglez pas la rançon demandée dans les délais impartis. [9]

1.7 Les problèmes de sécurité

Contraintes techniques de l’IdO L’évolution d’internet vers l’Internet des Objets se fait grâce à l’intégration des systèmes complexes, des objets communicants, localisables et mobiles les rendent de plus en plus autonomes. Ceci indique que l'IoT va fournir des bases pour lancer bientôt une nouvelle phase technologique (estimé en 2020), qui exposera de nouveaux moyens et d’opportunités dans notre vie quotidienne. En raison de ses vastes applications, l‟IoT a été ciblé et de nouvelles idées ont été proposées à cet égard par de nombreux chercheurs au cours de ces dernières années. Cette section analyse les contraintes techniques liées à la normalisation, limitations matérielles, problèmes de middleware, gestion de base de données, problèmes de sécurité et de confidentialité.

1.7.1Problème d'adressage et de détection

Dans l'IdO, chaque objet en environnement temps réel, est une chose vivante ou non- vivante, devait être adressée par une identité unique. Plusieurs chercheurs ont analysé et détecté les problèmes dans la perspective de l'IdO tels qu’adaptation IPv6. En utilisant les réseaux de capteurs, il est évident d'avoir un grand nombre de nœuds qui doivent être adressable séparément.

D'autre part, le problème est le nombre d'objets qui est beaucoup plus grand que le schéma d'adressage IPv4.Les estimations futures prédit que le nombre d'appareils ou d'objets augmentera au lieu de diminuer. B. Stockebrand a affirmé qu'IPv4 était déjà en infériorité numérique et toutes les adresses IP étaient occupées. Par conséquent, IPv6 a été défini par le moyen de 128 bits qui remplira les demandes d'adresses IP en constante augmentation.

1.7.2Problème de mise en réseau

En réseau, les protocoles jouent un rôle critique pour la connexion transformation de données. Le protocole réseau agit en tant que pilier d'acheminement des données entre le monde extérieur et les capteurs. L'Internet actuelle utilise le protocole TCP pour la transmission des données, ce qui n'est pas réalisable pour lido en raison de ses limites. Il y a beaucoup de protocoles existants en fonction des différents critères pour les réseaux mobiles, mais tous ont des inconvénients qui les rendent impraticables pour l'IdO. Alors il existe un besoin de protocole pour une gestion efficace en traitement des données. Plusieurs chercheur sont analysé les principaux problèmes liés au protocole TCP, qu'on peut classer comme suit :

a. Configuration de la connexion

Le protocole TCP crée une connexion d'abord avant toute transmission de données. Il faut beaucoup de temps pour créer cette connexion. Il semble que c'est un gaspillage de temps inutile dans le cas de l'IdO parce que la quantité de données et le temps de connexion sont très courts. De plus, une connexion est créée entre deux terminaux dont l'énergie est très limitée, donc ce n'est pas faisable.

- **Contrôle de congestion**

Le protocole TCP est responsable d'effectuer un contrôle de congestion sur les deux terminaux pendant la transmission des données, ce qui n'est pas réalisable dans le cas de l'IdO en raison de sa nature hétérogène. La plupart du temps, les données qui doivent être transférées sont de petite taille et le contrôle de la congestion dans ce cas est une surcharge. De plus, la communication se fait entre différents types de réseaux et de supports sans fil, le contrôle de la congestion dans ce scénario diminuera les performances. Ainsi, le contrôle de congestion TCP avec son état existant est peu pratique dans la perception de l'IdO.

- **Mise en mémoire tampon des données**

Le protocole TCP stocke les données à la fois dans les terminaux pour assurer la transmission sécurisée des données.

Par la suite en cas de dommage ou de perte au cours de la transmission des données, ces données peuvent être renvoyées, ce qui nécessite des tampons sur les deux terminaux pour stocker les données qui seront très coûteuses en terme de l'énergie et de stockage pour les appareils qui sont petits avec faible capacité de stockage et la durée de vie de la batterie très limitée.

- **Problème de contrôle du trafic et de surcharge**

Contrôle du trafic dans L'IdO est une autre tâche difficile liée à la mise en réseau. Il est une transmission facile en termes de contrôle de la circulation quand il est seulement entre les nœuds de

capteurs dans le réseau sans fil. Mais il devient compliqué lorsque les capteurs font partie de l'ensemble du réseau ayant des buts hétérogènes. En machine à machine (M2M), le contrôle du trafic est totalement différent que la communication homme à machine.

1.7.3Problème de protocole de routage

M2M est une clé facilitateur pour les villes intelligentes. Avec l'avancement des technologies, le M2M nécessitera le routage des données en raison de la nécessité de débits de données élevés. C'est une clé défi de créer un protocole de routage fiable ayant une haute vitesse de transmission et délai de livraison réduit. [8]

1.8 Les types des attaques

1.8.1Attaques par déni de service (DoS) et par déni de service distribué (DDoS)

Une attaque par déni de service submerge les ressources d'un système afin que ce dernier ne puisse pas répondre aux demandes de service. Une attaque DDoS vise elle aussi les ressources d'un système, mais elle est lancée à partir d'un grand nombre d'autres machines hôtes infectées par un logiciel malveillant contrôlé par l'attaquant.

À la différence des attaques conçues pour permettre à un attaquant d'obtenir ou de faciliter des accès, le déni de service ne procure pas d'avantage direct aux attaquants. Le déni de service est une satisfaction en soi pour certains pirates. Cependant, si la ressource attaquée appartient à un concurrent, l'avantage pour l'attaquant est alors bien réel. Une attaque DoS peut aussi avoir pour but de mettre un système hors ligne afin de pouvoir lancer un autre type d'attaque.

a. ***Attaque TCP SYN flood***

Un attaquant exploite l'utilisation de l'espace tampon lors du handshake d'initialisation de session TCP. La machine de l'attaquant inonde de demandes de connexion la petite file d'attente de traitement du système cible, mais elle ne réagit pas lorsque le système cible répond à ces demandes. Le système cible se met alors à temporiser en attendant la réponse de la machine de l'attaquant, ce qui fait planter le système ou le rend inutilisable lorsque la file d'attente de connexion se remplit.

b. ***Attaque Tear drop***

Cette attaque provoque le chevauchement des champs de longueur et de décalage de fragmentation des paquets séquentiels du protocole Internet (IP) au niveau de l'hôte attaqué ; au cours de ce processus, le système attaqué tente de reconstruire les paquets mais échoue. Le système cible s'embrouille et plante.

c. *Attaque Smurf*

Cette attaque implique d'usurper une adresse IP et d'utiliser l'ICMP pour saturer de trafic un réseau cible. Cette méthode d'attaque utilise des demandes d'écho ICMP ciblant des adresses IP de diffusion. Ces demandes ICMP proviennent d'une adresse usurpée. Si, par exemple, l'adresse de la victime choisie est 10.0.0.0 l'attaquant simule une demande d'écho ICMP de 10.0.0.0. à l'adresse de diffusion 10.255.255.255 Cette demande est envoyée à toutes les adresses IP de la plage, et toutes les réponses sont renvoyées à 10.0.0.0 submergeant ainsi le réseau. Ce processus est répétable et peut être automatisé en vue de générer des encombrements considérables sur le réseau.

d. *Ping of death*

Ce type d'attaque pingée un système cible avec des paquets IP dont la taille est supérieure au maximum de 65 535 octets. Les paquets IP de cette taille ne sont pas autorisés, le pirate les fragmente donc. Lorsque le système cible réassemble les paquets, il peut subir des débordements de tampon et d'autres plantages.

Les attaques Ping de la mort peuvent être bloquées à l'aide d'un pare-feu qui vérifie la taille maximale des paquets IP fragmentés.

e. *Botnets*

Les botnets sont des réseaux constitués de millions de systèmes infectés par des logiciels malveillants et contrôlés par des pirates informatiques afin d'effectuer des attaques DDoS. Ces bots ou systèmes zombies sont utilisés pour effectuer des attaques contre les systèmes cibles, souvent en submergeant leur bande passante et leurs capacités de traitement. Ces attaques DDoS sont difficiles à tracer.

1.8.2Attaque de l'homme au milieu (MitM)

Une attaque de l'homme du milieu est un pirate qui s'insère dans les communications entre un client et un serveur. Voici quelques types courants d'attaques de l'homme du milieu :

a. *Détournement de session*

Dans ce type d'attaque MitM, un attaquant détourne une session entre un client de confiance et un serveur réseau. L'ordinateur attaquant substitue son adresse IP au client de confiance pendant que le serveur poursuit la session, croyant qu'il communique avec le client. Par exemple, l'attaque pourrait se dérouler ainsi :

- Un client se connecte à un serveur.
- L'ordinateur de l'attaquant prend le contrôle du client.

- L'ordinateur de l'attaquant déconnecte le client du serveur.
- L'ordinateur de l'attaquant remplace l'adresse IP du client par sa propre adresse IP et son propre nom de domaine et usurpe les numéros de séquence du client.
- L'ordinateur de l'attaquant poursuit le dialogue avec le serveur, le serveur croit qu'il communique toujours avec le client.

b. ***Usurpation d'IP***

Un pirate peut utiliser l'usurpation d'adresse IP pour convaincre un système qu'il communique avec une entité connue et fiable afin de lui donner accès au système. Le pirate envoie à un hôte cible un paquet contenant l'adresse IP source d'un hôte connu et fiable au lieu de sa propre adresse IP source. Il est possible que l'hôte cible accepte le paquet et agisse en conséquence.

1.8.3Attaques phishing et spear phishing

L'hameçonnage consiste à envoyer des e-mails qui semblent provenir de sources fiables dans le but d'obtenir des informations personnelles ou d'inciter les utilisateurs à faire quelque chose. Cette technique combine ingénierie sociale et stratagème technique. Elle peut impliquer une pièce jointe à un e-mail, qui charge un logiciel malveillant sur votre ordinateur. Elle peut également utiliser un lien pointant vers un site Web illégitime qui vous incite à télécharger des logiciels malveillants ou à transmettre vos renseignements personnels.

1.8.4Attaque par Drive by Download

Les attaques par téléchargement furtif sont une méthode courante de propagation des logiciels malveillants. Les pirates recherchent des sites Web non sécurisés et insèrent un script malveillant dans le code HTTP ou PHP de l'une des pages. Ce script peut installer des logiciels malveillants directement sur l'ordinateur d'un visiteur du site, ou rediriger celui-ci vers un site contrôlé par les pirates. Des téléchargements furtifs peuvent survenir lors de la visite d'un site Web ou de l'affichage d'un e-mail ou d'une fenêtre pop-up. À la différence de nombreux autres types d'attaques informatiques, un téléchargement furtif ne nécessite pas qu'un utilisateur déclenche activement l'attaque – nul besoin de cliquer sur un bouton de téléchargement ou d'ouvrir une pièce jointe malveillante pour être infecté. Un téléchargement furtif peut profiter d'une application, d'un système d'exploitation ou d'un navigateur Web contenant des failles de sécurité dues à des mises à jour infructueuses ou à une absence de mise à jour.

1.8.5Attaque par mot de passe

Les mots de passe étant le mécanisme le plus couramment utilisé pour authentifier les utilisateurs d'un système informatique, l'obtention de mots de passe est une approche d'attaque courante et efficace. Le

mot de passe d'une personne peut être obtenu en fouillant le bureau physique de la personne, en surveillant la connexion au réseau pour acquérir des mots de passe non chiffrés, en ayant recours à l'ingénierie sociale, en accédant à une base de données de mots de passe ou simplement en devinant. Cette dernière approche – deviner – peut s'effectuer de manière aléatoire ou systématique :

1.8.6Attaque par injection SQL

L'injection SQL est devenue un problème courant qui affecte les sites Web exploitant des bases de données. Elle se produit lorsqu'un malfaiteur exécute une requête SQL sur la base de données via les données entrantes du client au serveur. Des commandes SQL sont insérées dans la saisie du plan de données (par exemple, à la place du nom d'utilisateur ou du mot de passe) afin d'exécuter des commandes SQL prédéfinies. Un exploit d'injection SQL réussi peut lire les données sensibles de la base de données, modifier (insérer, mettre à jour ou supprimer) les données de la base de données, exécuter des opérations d'administration de la base de données (par exemple la fermer), récupérer le contenu d'un fichier spécifique, et, dans certains cas, envoyer des commandes au système d'exploitation.

1.8.7Attaque XSS (Cross-site scripting)

Les attaques XSS utilisent des ressources Web tierces pour exécuter des scripts dans le navigateur Web de la victime ou dans une application pouvant être scriptée. Plus précisément, l'attaquant injecte un JavaScript malveillant dans la base de données d'un site Web. Lorsque la victime demande une page du site Web, le site Web transmet la page à son navigateur avec le script malveillant intégré au corps HTML. Le navigateur de la victime exécute ce script, qui envoie par exemple le cookie de la victime au serveur de l'attaquant, qui l'extrait et l'utilise pour détourner la session. Les conséquences les plus graves se produisent lorsque XSS sert à exploiter des vulnérabilités supplémentaires. Ces vulnérabilités peuvent non seulement permettre à un attaquant de voler des cookies, mais aussi d'enregistrer les frappes de touches et des captures d'écran, de découvrir et de collecter des informations réseau et d'accéder et de contrôler à distance l'ordinateur de la victime.

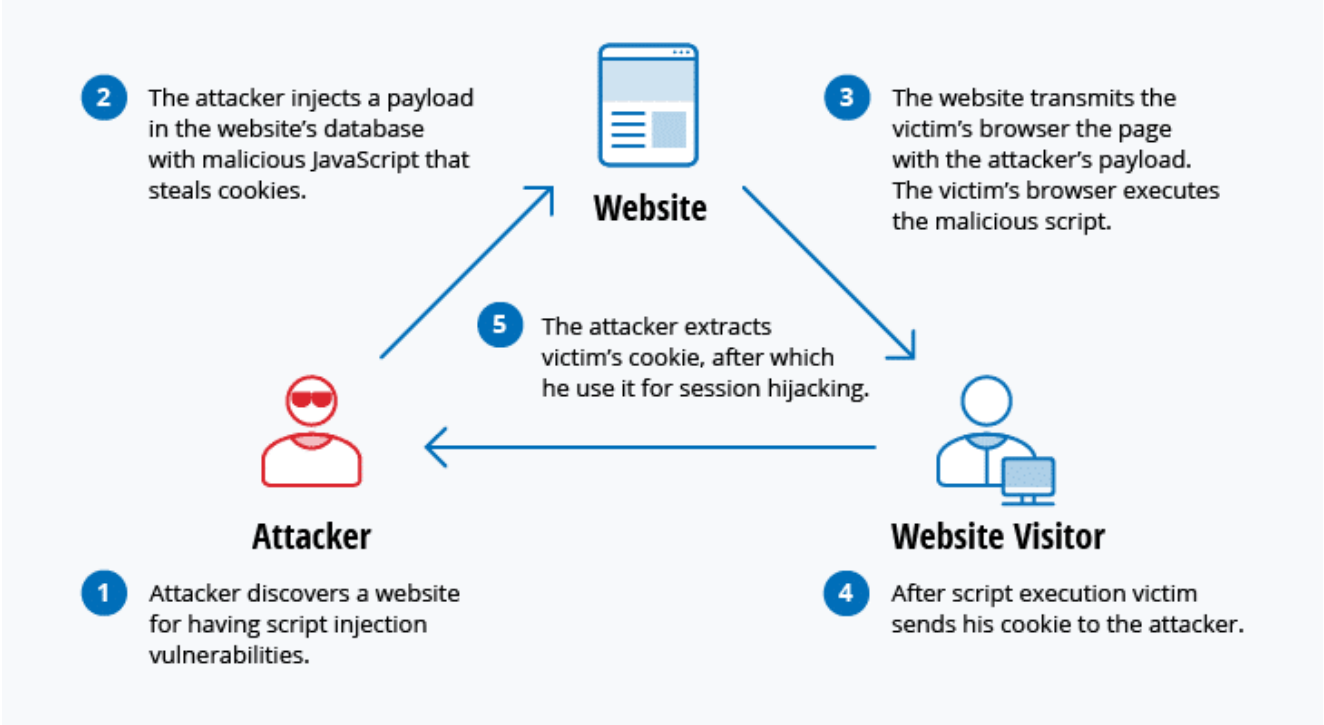

Figure 2 attaque XSS

1.8.8Attaque par écoute illicite

Les écoutes clandestines sont le résultat d'une interception du trafic réseau. Elles permettent à un attaquant d'obtenir des mots de passe, des numéros de carte bancaire et d'autres informations confidentielles qu'un utilisateur envoie sur le réseau. Elles peuvent être passives ou actives :

- Écoute clandestine passive – Un pirate détecte des informations en écoutant la transmission de messages sur le réseau.
- Écoute clandestine active – Un pirate s'empare activement d'informations en se faisant passer pour une unité amie et en envoyant des requêtes aux transmetteurs. On appelle cela sonder, scanner ou saboter.

Il est souvent plus important de détecter des écoutes passives que des écoutes actives, car ces dernières exigent de l'attaquant qu'il apprenne à connaître les unités amies en effectuant préalablement des écoutes passives.

1.8.9Attaque d'anniversaire

Les attaques des anniversaires sont lancées contre les algorithmes de hachage qui vérifient l'intégrité d'un message, d'un logiciel ou d'une signature numérique. Un message traité par une fonction de hachage produit une synthèse du message de longueur fixe, indépendante de la longueur du message entrant ; cette synthèse caractérise de façon unique le message. L'attaque des anniversaires fait référence à la probabilité de trouver deux messages aléatoires qui génèrent la même synthèse lorsqu'ils sont traités

par une fonction de hachage. Si un attaquant calcule la même synthèse pour son message que l'utilisateur, il peut tout à fait remplacer le message de l'utilisateur par le sien, et le destinataire ne sera pas en mesure de détecter le remplacement, même s'il compare les synthèses. [10]

1.9 Vulnérabilités courants des objets connectés

1.9.1Manque d'authentification et d'autorisation

Un système d'authentification et d'autorisation est un élément essentiel de tout réseau, qu'il s'agisse d'un réseau informatique traditionnel ou d'un dispositif IoT. Sans authentification et autorisation appropriées, n'importe qui peut potentiellement accéder à des données ou des dispositifs sensibles.Cela pourrait conduire à une violation de données, à une activité malveillante ou simplement à l'utilisation non autorisée de ressources. Un système d'authentification et d'autorisation bien conçu devrait être en mesure d'empêcher tout accès non autorisé tout en permettant aux utilisateurs légitimes d'accéder au système. Malheureusement, de nombreux systèmes sont soit mal conçus, soit mal mis en œuvre, ce qui peut entraîner de graves problèmes de sécurité.

1.9.2Communications non sécurisées

À notre époque, il est important d'être conscient des dangers des communications non sécurisées. Avec l'essor de l'IoT, de plus en plus d'appareils sont connectés à l'internet, et beaucoup d'entre eux sont équipés de capteurs en tout genre et de caméras. Cela signifie que si vos communications ne sont pas correctement sécurisées, elles pourraient être interceptées par des acteurs malveillants. Les communications doivent être cryptées de bout en bout, afin que seuls les destinataires prévus puissent les lire. En outre, toutes les communications doivent être signées au moyen d'une signature numérique afin de garantir qu'elles n'ont pas été altérées.

1.9.3Mots de passe non sécurisés

La mauvaise sécurité des mots de passe est l'un des plus grands défis de la cyber sécurité des dispositifs IoT. Malheureusement, peu d'appareils IoT sont protégés par mot de passe, et même lorsqu'ils le sont, les utilisateurs ont généralement tendance à utiliser des mots de passe par défaut, ce qui rend ces appareils vulnérables aux violations.

De plus, de nombreux appareils IoT, tels que les montres connectées, s'appuient sur la vérification d'identité à l'aide de systèmes biométriques. Bien que ceux-ci puissent être plus sécurisés que l'utilisation de mots de passe faciles à deviner, les données de vérification doivent être stockées et gérées de manière plus sécurisée.

Comme la plupart des appareils personnels, les appareils IoT sont livrés avec des paramètres par défaut codés en dur pour une configuration simple. Ces paramètres deviennent prévisibles au fil du temps et sont très peu sûrs.

1.9.4Manque de mises à jour et logiciels obsolètes

Les mises à jour sont essentielles pour maintenir la sécurité des appareils IoT. Ils doivent être mis à jour immédiatement après la découverte de nouvelles vulnérabilités. Les smartphones et les ordinateurs reçoivent généralement des mises à jour fréquemment ce n'est malheureusement souvent pas le cas pour les appareils IoT. Ces appareils manquent souvent d'un processus établi pour les mises à jour et les correctifs de sécurité. Les fabricants d'appareils IoT ne donnent souvent pas la priorité à la cyber sécurité lors de la conception de leurs produits. Cela conduit à la production d'appareils plus vulnérables aux cyberattaques. Par conséquent un appareil IoT qui était sécurisé lorsqu'un client l'a acheté pour la première fois devient non sécurisé et facilement accessible pour les pirates.

1.9.5Absence de plan de réponse aux incidents

Les cyberattaques causent souvent des dégâts considérables aux entreprises qui peuvent même conduire jusqu'à leur faillite. Il est important de considérer ce risque surtout que les cyberattaques ont augmenté de plus de 28% en 2022 par rapport à 2021.Le nombre d'objet connecté ne cesse d'augmenter, faisant ainsi augmenter les chances de cyberattaques. Le besoin de plans d'intervention en cas d'incident ne peut que devenir plus urgent. Malheureusement, beaucoup d'entreprises attendent d'être au milieu d'une situation d'urgence pour commencer à réfléchir à une réponse. À ce moment-là, il est généralement trop tard. Si vous voulez être prêt pour la prochaine grande attaque, prenez le temps de développer un plan de réponse aux incidents dès maintenant. Cela pourrait faire la différence entre être une victime et être un survivant. [11]

1.10 Mécanisme de sécurité

Les mécanismes de sécurité sont des mécanismes conçus pour détecter, empêcher ou récupérer suite à une attaque de sécurité :

- **La certification** est un moyen sûr de confirmer la véritable identité des deux parties qui communiquent entre elles. D'où en utilisant l'infrastructure à clé publique, il est possible d'obtenir l'authentification forte par clé publique bidirectionnelle pour prévenir l'authenticité et la confidentialité du système IOT.
- **Sécurité des données** La sécurité des données et l'exploration des données doivent figurer en tête de la liste des caractéristiques de sécurité de l'IoT à travers la cryptographie. Il s'agit de la première étape pour empêcher tout accès non authentifié aux

appareils du réseau IoT. Une architecture en couches doit être utilisée dans le système de sécurité des données. Par conséquent, toute violation du niveau de sécurité initial n'expose pas toutes les données. Elle doit plutôt alerter les auto- rites sur les menaces potentielles et la violation du niveau de sécurité initial.

- **Contrôle d'accès** Le contrôle d'accès est un autre mécanisme qui sécurise l'environnement de l'IoT en limitant le contrôle d'accès aux machines, objets ou personnes qui n'ont pas le droit d'accéder aux ressources.
- **Cloud Comptine** Le "cloud" est un nom qui désigne une capacité de stockage de données énorme, des performances élevées à un coût abordable. Dans le fonctionnement essentiel de l'ITO, c'est-à-dire le grand nombre de nœuds de capteurs qui collectent et analysent une énorme quantité de données, le stockage et le traitement des données où l'informatique dans les nuages peut être utilisée très efficacement. [12]

1.11 Conclusion

Dans ce chapitre on a démontré les différentes attaques informatiques qui perturbe la sécurité des réseaux et quelques définitions de ses concepts des bases, Puis on a parlé de l'internet des objets sa définition ses protocoles et ses domaines d'application, Et on a terminé par ses contraintes techniques les plus connues.

Chapitre 2 Etude des vulnérabilités des objets connectés basés sur ESP32

2.1 Introduction

Les objets connectés basés sur ESP32 ont pris une place prépondérante dans le domaine de l'Internet des objets (IDO). Ces dispositifs physiques, connectés au réseau, permettent L'échange de données et d'informations avec d'autres systèmes et appareils. L'une plateforme matérielle open-source, s'est imposée comme une solution populaire pour le développement d'objets connectés grâce à sa puissance de traitement, sa connectivité sans fil (Wi-Fi et Bluetooth), sa faible consommation d'énergie et ses capacités de programmation polyvalentes.

Ce chapitre propose une exploration approfondie de ces objets connectés basés sur ESP32. Nous commencerons par analyser l'architecture et les fonctionnalités de l'mettant en évidence les éléments essentiels qui en font une plateforme adaptée aux objets connectés. Cette compréhension préliminaire est essentielle pour appréhender les enjeux liés à la sécurité et aux vulnérabilités des objets connectés, qui seront examinés plus en détail par la suite.

En outre, nous aborderons les avantages et les défis liés à l'utilisation de l'ESP32 dans le développement d'objets connectés, tout en explorant les opportunités qu'il offre pour

L'innovation dans ce domaine en pleine expansion.

2.2 La carte ESP 32

L'ESP32 est une plateforme matérielle populaire utilisée dans le développement d'objets Connectés Comprendre son architecture et ses fonctionnalités est essentiel pour exploiter, tout son potentiel. Cette recherche approfondie se penche sur l'ESP32, mettant en évidence son architecture interne, ses composants clés et ses fonctionnalités principales.

2.2.1Architecture de la carte ESP32

Dans l'architecture de la carte ESP32 on a plusieurs composants mais on va concentrer sur les suivants qui sont mentionnés sur la figure :

a. ***Antenne wifi***

L'antenne Wi-Fi de l'ESP32 est un composant intégré qui permet à la carte de se connecter à des réseaux sans fil. Elle émet et reçoit des signaux radiofréquences dans la plage de fréquences du Wi-Fi (2,4 GHz et/ou 5 GHz). Elle permet à l'ESP32 d'établir des connexions sans fil avec des points d'accès Wi-Fi, d'accéder à Internet et d'échanger des données avec D'autres appareils compatibles Wi-Fi. L'emplacement et l'orientation de l'antenne sont importants pour optimiser la qualité de la connexion Wi-Fi.

b. ***Microcontrôleur ESP32***

Ce processeur fonctionne à une fréquence d'horloge de 240 MHz. Il possède une mémoire RAM de 520 kB, EEPROM de 448 kB et aussi une mémoire Flash de 4000 kB (pour la programmation et l'enregistrement de données).

Le microcontrôleur possède une puce Wifi permettant de se connecter au réseau local, de créer un serveur ou de créer son propre réseau afin que d'autres appareils s'y connectent. Le microcontrôleur possède une puce Bluetooth qui lui permet d'interagir avec d'autres appareils.

c. ***Mémoire***

L'ESP32 est équipé de différents types de mémoire, notamment une mémoire flash intégrée pour le stockage du programme et des données, ainsi qu'une mémoire RAM pour L'exécution des applications.

d. ***Coprocesseurs spécialisés***

L'ESP32 dispose de plusieurs coprocesseurs spécialisés pour gérer des tâches spécifiques telles que la gestion de la connectivité Wi-Fi et Bluetooth, le chiffrement matériel, la gestion de l'énergie, etc.

Et le rôle des autres composants est mentionné sur la figure suivante :

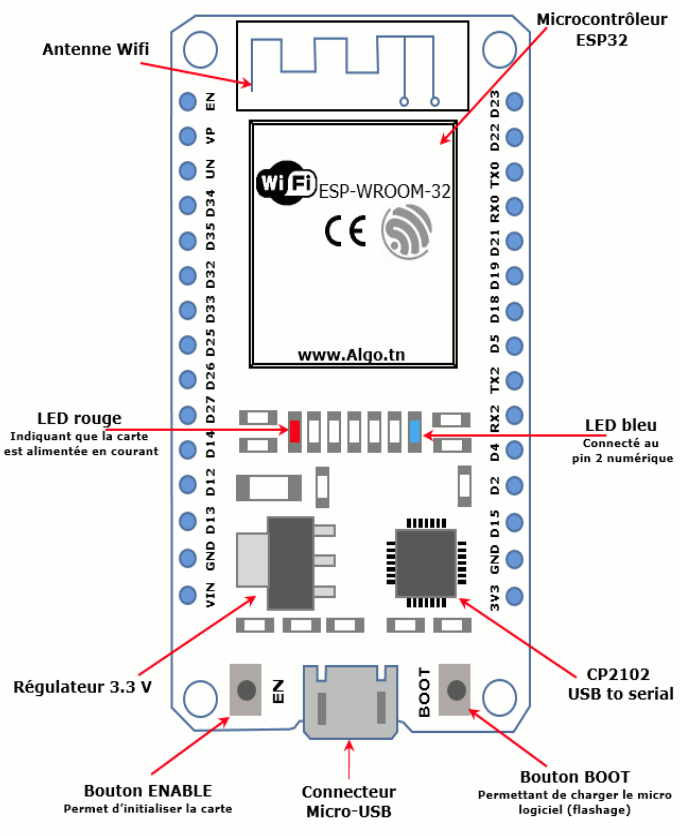

Figure 3 L'Architecture de la carte ESP32[13]

2.2.2 Caractéristiques :

- Alimentation :

  - 5 Vcc via micro-USB

  - 3,3 Vcc via broches Vin

- Microcontrôleur : ESP32
- Microprocesseur : Tensilica LX6 Dual-Core
- Fréquence : 240 MHz
- Mémoire SRAM : 512 kB
- Mémoire Flash : 4 Mb
- E/S disponibles :
  - 15 E/S digitales dont 10 compatibles PWM
  - 2 x sorties analogiques (DAC)
  - 15 x entrées analogiques (ADC)
- Interfaces: I2C, SPI, 2 x UART
- Interface Wi-Fi 802.11 b/g/n 2,4 GHz
- Bluetooth: Classique / BLE

- Antenne intégrée
- Température de service: -40 à 125 °C
- Dimensions: 48 x 26 x 11,5 mm [14]

2.3 Sécurité des objets connectés

2.3.1 Les vulnérabilités courantes des objets connectés basés sur ESP32

Les objets connectés basés sur ESP32, tout comme tout autre dispositif IOT, peuvent présenter différentes vulnérabilités courantes. Voici quelques exemples de vulnérabilités souvent observées dans les objets connectés basés sur ESP32 :

a. ***Mauvaise gestion des identifiants et des mots de passe***

Les objets connectés peuvent être livrés avec des identifiants et des mots de passe par défaut préconfigurés, souvent largement connus et disponibles sur Internet. Si les utilisateurs ne changent pas ces informations d'identification, les appareils deviennent vulnérables aux attaques par force brute et aux compromissions.

b. ***Manque de chiffrement des communications***

Les objets connectés peuvent transmettre des données sur des réseaux non sécurisés sans utiliser de chiffrement adéquat. Cela peut permettre à des attaquants de capturer et de lire ces données, compromettant la confidentialité et l'intégrité des informations.

c. ***Absence de mises à jour de sécurité***

Les fabricants peuvent ne pas fournir de mises à jour régulières pour les objets connectés, les laissant vulnérables aux failles de sécurité connues. Sans mises à jour appropriées, les vulnérabilités restent exploitables, même si des correctifs sont disponibles.

d. ***Manque de contrôles d'accès robustes***

Certains objets connectés peuvent ne pas mettre en œuvre de mécanismes de contrôle d'accès suffisamment solides. Cela peut permettre à des attaquants de compromettre les appareils en contournant les restrictions d'accès et en exécutant des actions non autorisées.

e. ***Injection de code***

Si les objets connectés ne valident pas correctement les entrées utilisateur, ils peuvent être vulnérables à des attaques d'injection de code, telles que les attaques par injection SQL ou par injection de commandes. Ces attaques peuvent permettre aux attaquants d'exécuter du code malveillant sur l'appareil.

f. ***Défauts de conception matérielle***

Certains objets connectés peuvent présenter des vulnérabilités au niveau de leur conception matérielle, telles que des interfaces non sécurisées ou des mécanismes de stockage non protégés. Ces vulnérabilités peuvent être exploitées par des attaquants pour obtenir un accès non autorisé à l'appareil ou aux données qu'il contient.

2.4 Méthodologie des tests des vulnérabilités des objets connectés

La méthodologie des tests de vulnérabilités pour les objets connectés peut varier en fonction des spécificités de chaque dispositif, mais voici une méthodologie générale qui peut être utilisée :

2.4.1Reconnaissance

Cette phase consiste à collecter des informations sur l'objet connecté, tels que son modèle, sa version du frimaire, les protocoles de communication utilisés, les interfaces disponibles, etc. Cela peut être réalisé en consultant la documentation, en analysant le trafic réseau ou en effectuant des recherches en ligne.

2.4.2Analyse des vulnérabilités connues

Dans cette étape, vous devez rechercher des vulnérabilités déjà connues associées à l'objet connecté spécifique. Vous pouvez consulter des bases de données de vulnérabilités, des bulletins de sécurité ou des ressources en ligne pour identifier les problèmes de sécurité connus.

2.4.3Évaluation des interfaces de communication

Examinez les protocoles de communication utilisés par l'objet connecté, tels que le Wi-Fi, le Bluetooth, les interfaces filaires, etc. Cherchez des vulnérabilités telles que l'absence de chiffrement, les faiblesses d'authentification ou les problèmes de gestion des sessions.

2.4.4Analyse du firmware

Analysez le firmware de l'objet connecté pour identifier les éventuelles vulnérabilités liées à sa conception ou à son implémentation. Cela peut inclure la recherche de faiblesses de sécurité, l'analyse

des bibliothèques tierces utilisées, l'extraction des clés de chiffrement ou la détection de back Doors potentielles.

2.4.5Tests d'injection de code

Effectuez des tests d'injection de code pour évaluer la résistance de l'objet connecté aux attaques telles que l'injection SQL, l'injection de commandes ou l'injection de code HTML. Vérifiez si les entrées utilisateur sont correctement validées et si les mécanismes de sécurité appropriés sont en place pour prévenir ces attaques.

2.4.6Tests d'authentification et d'autorisation

Testez les mécanismes d'authentification et d'autorisation de l'objet connecté pour déterminer si des faiblesses existent. Cela peut inclure des tests d'authentification par force brute, des tests d'accès non autorisés ou des tests d'escalade de privilèges.

2.4.7Test de résistance

Évaluez la résistance de l'objet connecté aux attaques courantes telles que les dénis de service, les tentatives de contournement de sécurité ou les attaques de manipulation de données. Cela permet de vérifier la stabilité et la robustesse de l'objet connecté face à des situations hostiles.

2.4.8Rapport de vulnérabilités

Documentez toutes les vulnérabilités identifiées, en fournissant des détails précis sur chaque problème découvert, son impact potentiel et les recommandations pour le corriger. Organisez les vulnérabilités par ordre de priorité en fonction de leur sévérité.

2.5 Méthodologie d’expérimentation

L'objectif de cette étude est d'analyser la sécurité de la carte ESP32 en identifiant les vulnérabilités potentielles et en évaluant la robustesse de ses mécanismes de sécurité. Les principaux objectifs sont :

- Identifier les vulnérabilités courantes de la carte ESP32.
- Évaluer la robustesse des mécanismes d'authentification et d'autorisation.
- Tester la résistance de la carte ESP32 aux attaques courantes.
- Fournir des recommandations pour améliorer la sécurité de la carte ESP32.

Et pour atteindre ces objectifs on va passer par les étapes suivantes :

- Installation du logiciel Arduino IDE et programmation d'un serveur web sur la carte ESP32.
- Tester la connectivité au serveur de la carte ESP32.
- Installation de kali linux.
- Analyse du trafic réseau et des ports ouverts.
- Faire des pentests avec kali linux sur le serveur de la carte ESP32.
- Mettre des recommandations pour renforcer la sécurité des objets connectés basés sur ESP32.

2.6 Arduino IDE

Les créateurs d'Arduino ont développé un logiciel pour que la programmation des cartes arduino soit visuelle, simple et complète à la fois. C'est ce que l'on appelle une IDE, qui signifie Integrated Développent Environnent Environnement de Développement « Intégré » en français (donc EDI). L'IDE Arduino est le logiciel qui permet de programmer les cartes Arduino. L'IDE affiche une fenêtre graphique qui contient un éditeur de texte et tous les outils nécessaires à l'activité de programmation. On peut donc saisir votre programme, l'enregistrer, le compiler, le vérifier, le transférer sur une carte arduino…A la date de rédaction de cette page, la version la plus récente de l'IDE Arduino est la 1.8.10. L'aspect est à peu près identique sur chaque plate-forme (Windows, Mac et Linux). L'image suivante montre l'écran initial qui apparaît au lancement de l'IDE.[15]

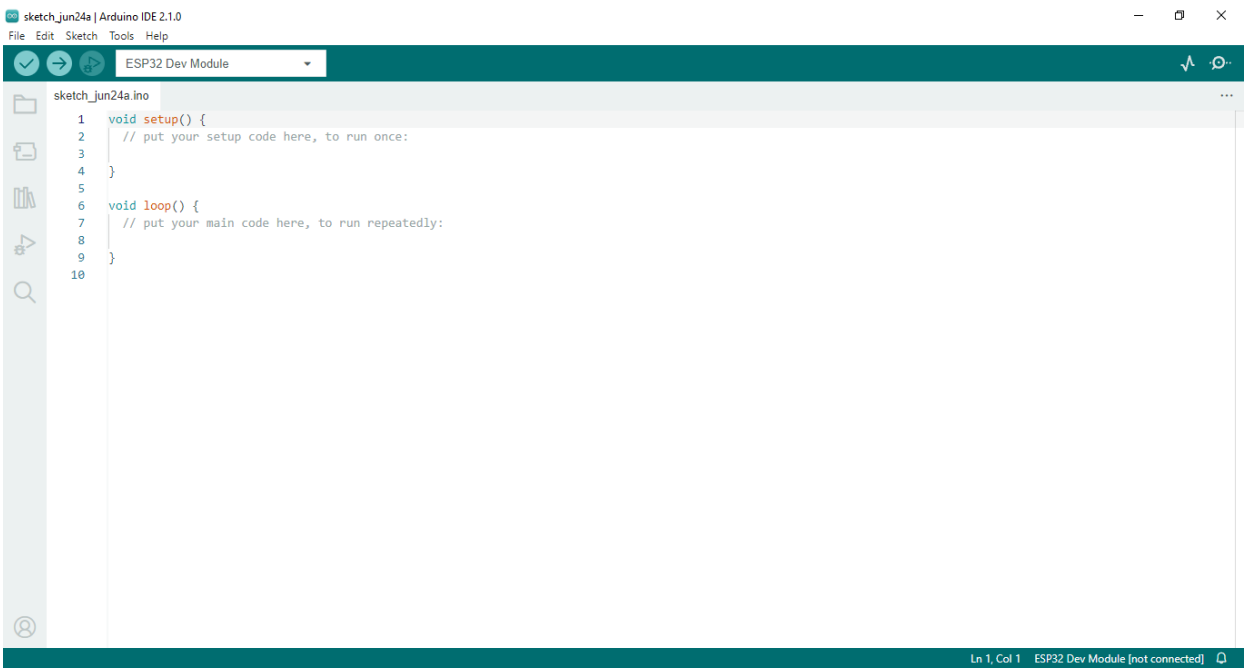

Figure 4 L'interface graphique d'Arduino

2.7 Kali linux

Kali Linux est une distribution GNU/Linux basée sur Debian sortie en 2013. Cette dernière fait suite à Back rack, qui était-elle basée sur Ubuntu.

L’objectif de cette suite de logiciels est de regrouper les outils nécessaires aux tests de sécurité d’un système informatique : test d’intrusion, sniffing, reverse engineering, crack de mot de passe, recherche de vulnérabilité, etc.[16]

Figure 5 l'interface graphique de kali linux

2.8 Conclusion

Ce chapitre a porté sur l'étude des vulnérabilités des objets connectés basés sur ESP32. Nous avons présenté la plateforme ESP32, identifié les vulnérabilités spécifiques à ESP32, et élaboré une méthodologie d'expérimentation pour les analyser. La méthodologie comprend des étapes telles que la reconnaissance, l'analyse du firmware, l'analyse du trafic réseau, les tests d'injection de code, les tests d'authentification et d'autorisation, ainsi que les tests de résistance. Ces informations nous permettront de renforcer la sécurité des objets connectés ESP32 en identifiant et en remédiant aux vulnérabilités découvertes.

Chapitre 3 Expérimentation et tests de sécurité

3.1 Introduction

Comme nous l'avons mentionné dans le chapitre précédent les vulnérabilités des objets connectés sont nombreuses. Et malheureusement ces failles peuvent causer des risques de sécurité par exemple vol des données mauvaise communication …etc. et pour cela il faut sécuriser et protéger le réseau et les objets connectés.

Dans ce chapitre on se concentre sur l'expérimentation et les tests de sécurités des objets connectés ; nous aborderons les différentes étapes nécessaires pour mettre en place un enlisement de test approprie ; Ainsi que les outils spécifiques utilisés pour évaluer les sécurités de ses dispositifs.

Dans ce chapitre on va faire une étude qui est basée sur :

- La programmation et le test de la carte ESP32.
- Le contrôle de la carte ESP32 à distance.
- Des tests de vulnérabilité sur la carte ESP32 et l'analyse en détails de tout le trafic.

Pour résoudre notre problématique et atteindre notre objectif on a suivi enchainement des étapes suivantes :

- La documentation : tout d'abord ; on doit faire une étude complétée sur les concepts théoriques de la communication à distance avec la carte ESP32
- Le test : après l'étude de la carte ESP32 on peut sélectionner les vulnérabilités et faire des tests avec kali linux pour les étudier.
- La capture : pour assurer que le test des vulnérabilités a bien marché on doit utiliser un analyseur de paquet open source.
- Wireshark : qui permet de capturer ; analyser et capturer le trafic réseau sur plusieurs protocoles.

3.2 Matériel utilisé

On a réalisé notre travail dans un environnement ouvert ; un réseau local connecté à internet. On fait les expériences sures :

- Un ordinateur portable acer avec un processeur Intel (R) core (TM) ; 3-3217UCPU@ 1.80 GHz avec une RAM 4.00 Go.
- Un ordinateur portable HP avec un processeur avec une RAM 4.00 Go.
- Système d'exploitation Windows 10.
- Système d'exploitation kali linux.
- Carte ESP32 W-ROOM.

Dans notre recherche on utilise les logiciels suivants :

- Wireshark version.
- Arduino IDE version 2.1.0
- LOIC : Low orbit ION Cannon 1.0.8

3.3 Environnement

3.3.1Architecture de travail

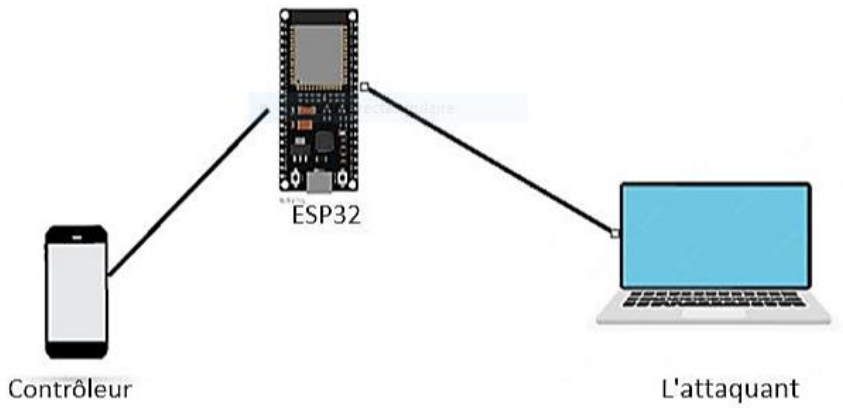

Figure 6 Architecture de travail partie pratique

La figure ci-dessus nous montre l'architecture de notre travail :

- La carte ESP32 : on a programmé la carte pour connecter avec elle à distance par un site web (on l'utilise comme un objet connecté).

- Le téléphone portable : on l'utilise pour accéder au site web de la carte ESP32 et la contrôler à distance.
- Le pc portable : c'est un pc attaquant contient de système d'exploitation kali linux pour analyser et contrôler les vulnérabilités de l'ESP32.

3.4 Programmation de la carte ESP32

3.4.1Test de contrôle à distance l'ESP32

Pour contrôler un ESP32 à distance il faut passer aux étapes suivantes :

a. ***Etape 1 : programmer le wifi de l'ESP32***

Assuré que l'ESP32 est fonctionnel avec un firmware installé et équipé du wifi

- Ensuite, on a connecté notre ESP32 à l'ordinateur à l'aide d'un câble USB
- Et puis, on a ouvert logiciel Arduino IDE et télécharger la bibliothèque de l'ESP32, après le téléchargement de bibliothèque on a sélectionné le port série correct.
- Après les étapes précédentes ; on a tapé le programme suivant :[17]

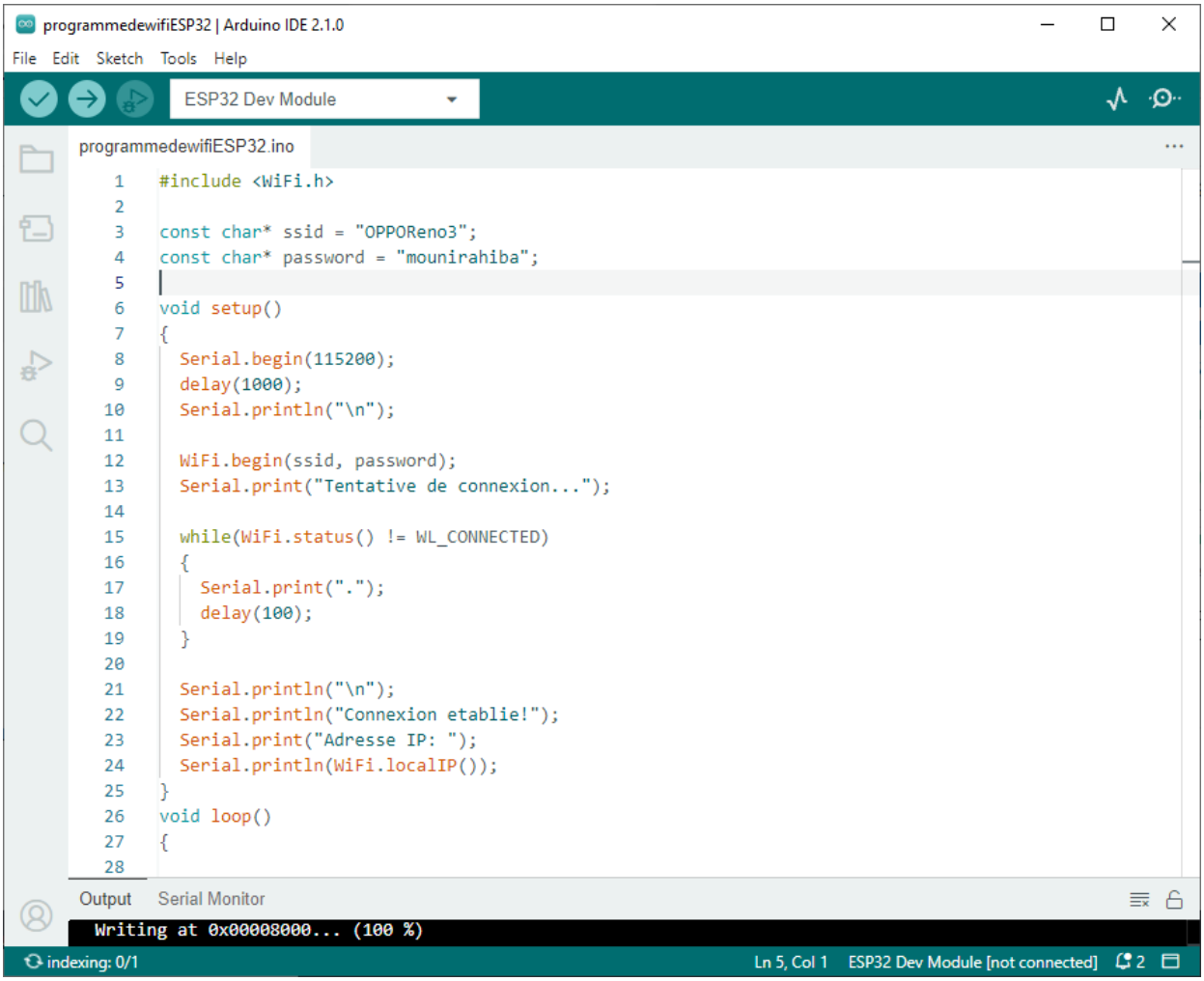

Figure 7 capture de code Arduino (wifi)

- **Explication des commandes de code**

Ce code Arduino utilise la bibliothèque wifi.h pour configurer la connexion Wifi de l'ESP32 voici la fonctionnalité de chaque commande :

- SSID : pour saisir le nom de réseau.
- Password : pour saisir le mot de passe de réseau.
- Serial. Begin (115200) : pour voir les messages de débogages sur le moniteur série de l'IDE Arduino.
- Delay (1000) : pour permettre à l'ESP32 de s'initialise à un délai d'une seconde.
- While : une boucle est utilisée pour attendre que la connexion soit établie.
- Wifi. Local IP () : quand la connexion est établie ; cette commande affiche l'adresse IP attribué à l'ESP32.

b. *Etape 2 : code de serveur de la carte ESP32*

Après la programmation de Wifi de la carte ESP32 on a créé un autre programme de serveur pour contrôler la carte à distance voici notre programme :

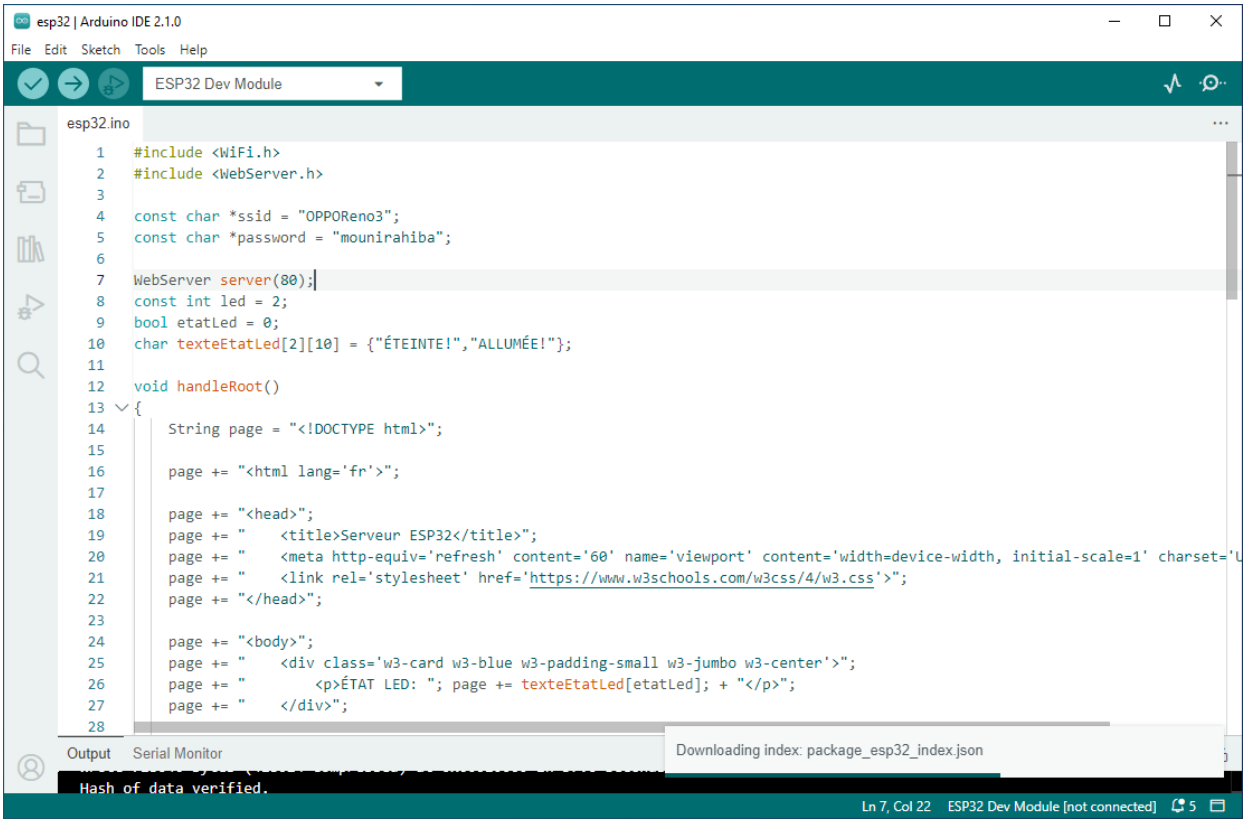

Figure 8 capture de code esp32

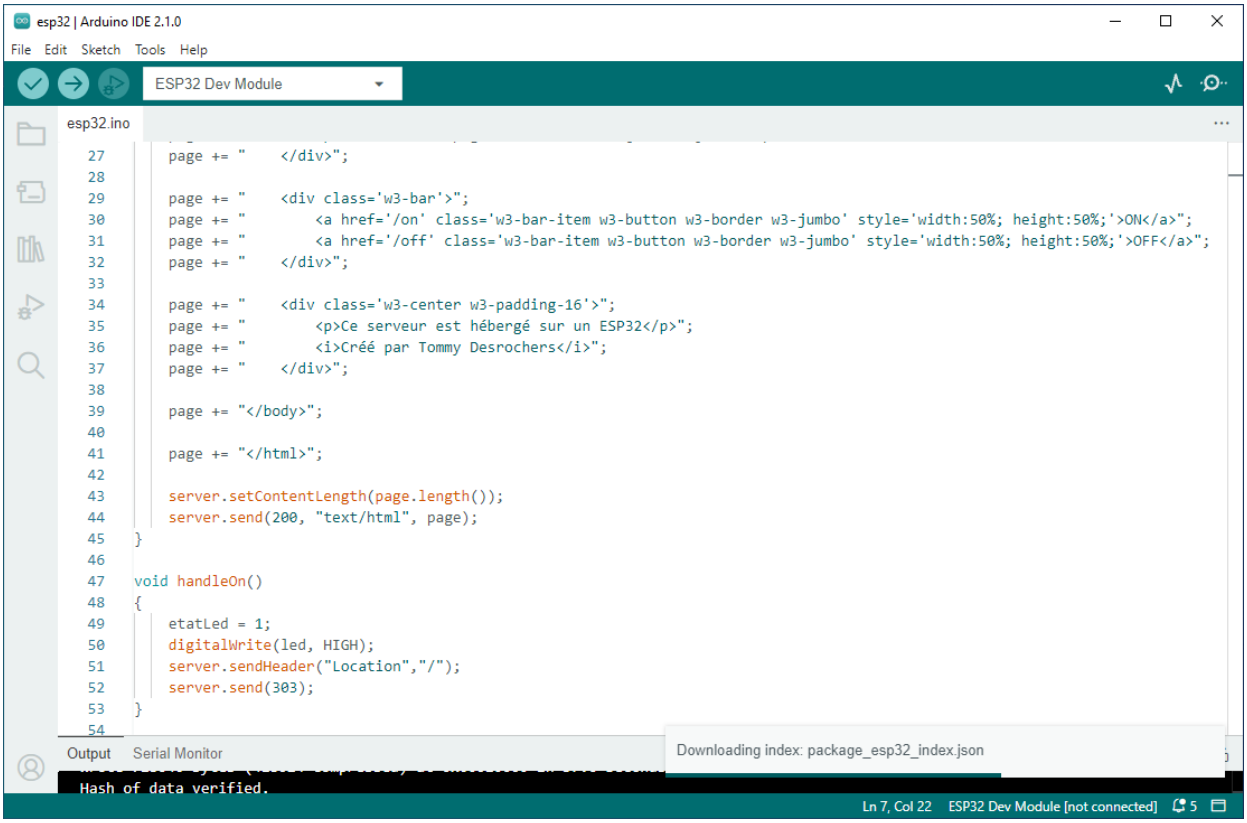

Figure 9 capture de code Arduino (ESP32)

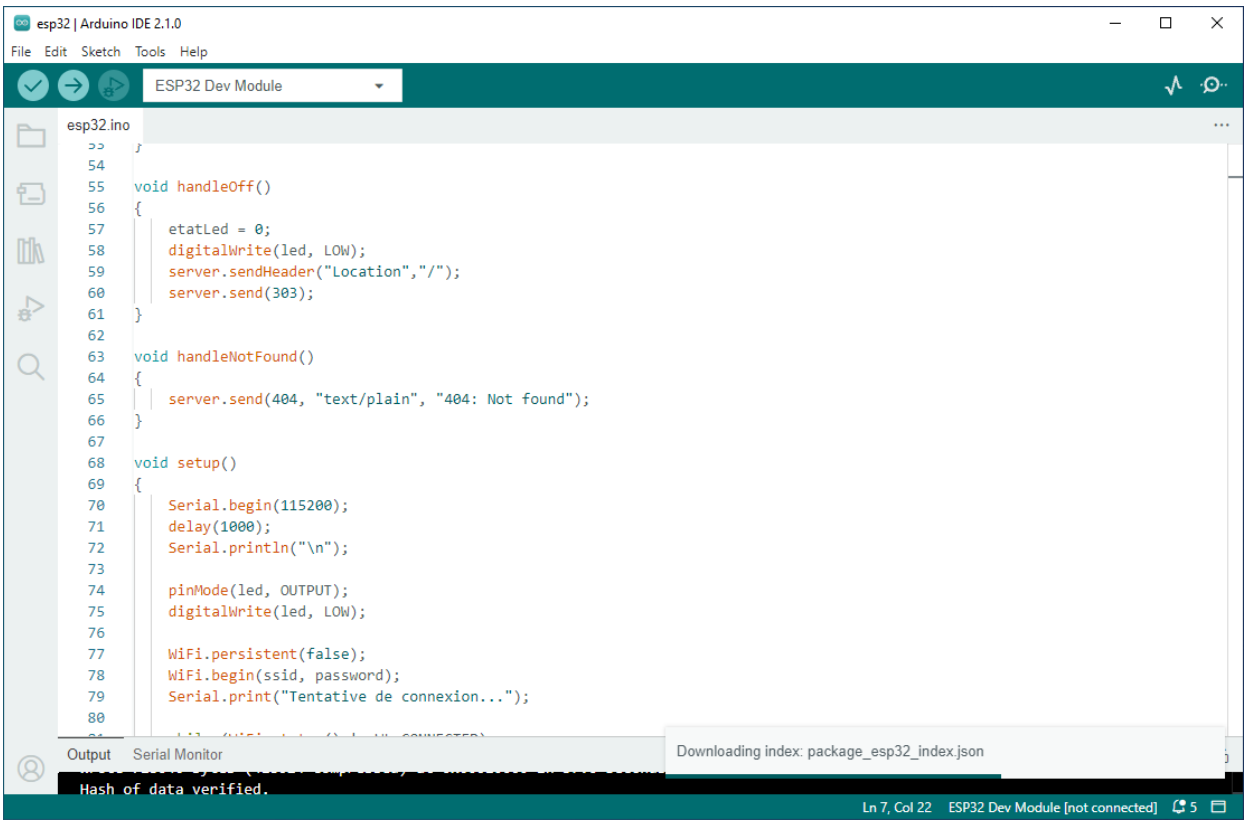

Figure 10 capture de code Arduino (ESP32)

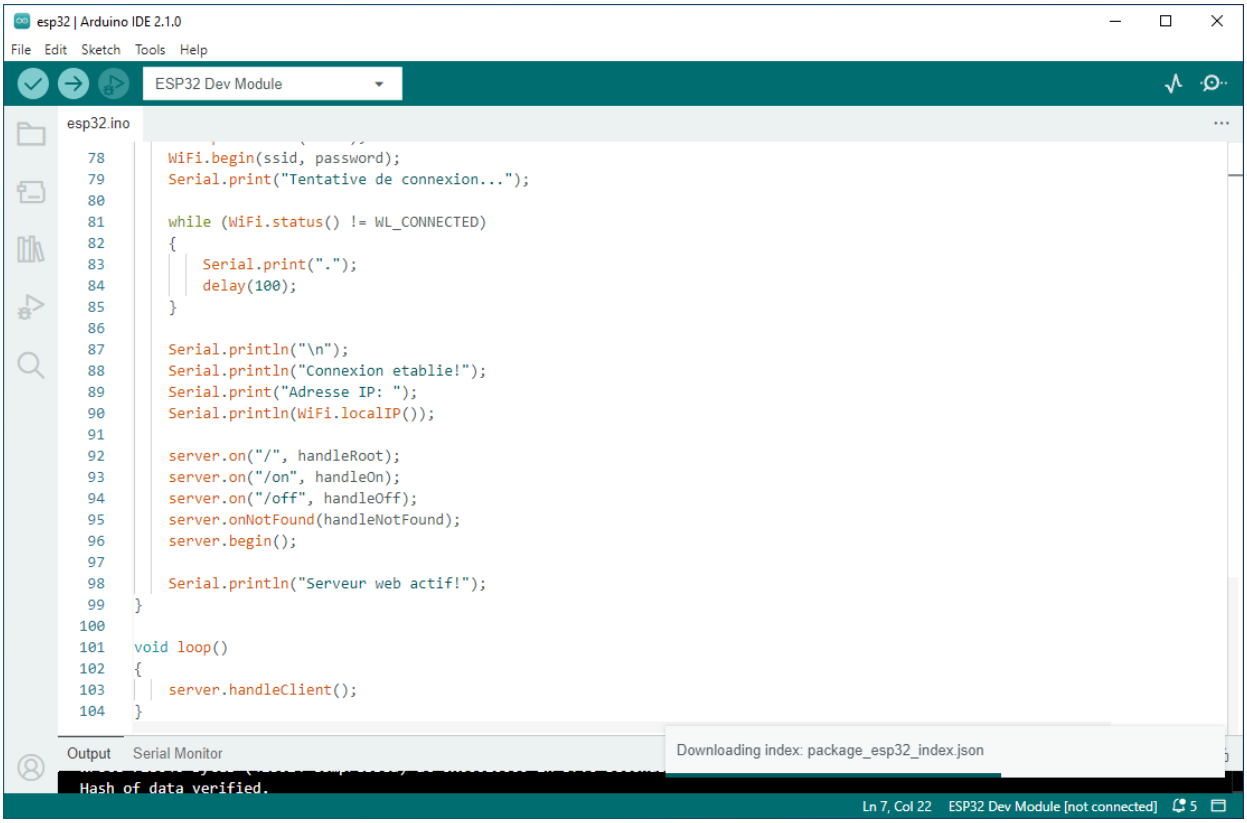

Figure 11 capture de code arduino (ESP32)

- **Explication des commandes de code**

Ce code Arduino utilise les bibliothèques Wifi.h et webserver.h pour créer un serveur web sur la carte ESP32. Notre serveur web permet de contrôler l'état de LED connecté au pin 2 l'ESP32 avec HTTP.

- Webserver server (80) : pour créer une instance de la classe webserver sur le port (80)
- Const int led =2 : la led connecté au pin 2 de l'ESP32.
- Etat led : variable booléenne son rôle est suivre l'état de LED.
- Handle root () : elle géré la page principale du suivre web.
- Handle on () et handle off () : sont définies pour gérer les requêtes HTTP vers les URL.
- Handle not found () : si une URL inconnue est demandé ; cette commande renvoi une réponse 404.
- Server. Handle client () : pour gérer les requêtes de clients.

c. *Etape 3 : test de contrôle à distance par le serveur créé*

Après la compilation des codes précédents on a obtenu l'adresse IP de notre carte ESP32 192.168.43.182 on a écrit l'adresse sur le navigateur ; on a obtenu cette page.

Et voilà les résultats ; on a bien contrôle l'état de LED de notre ESP32.

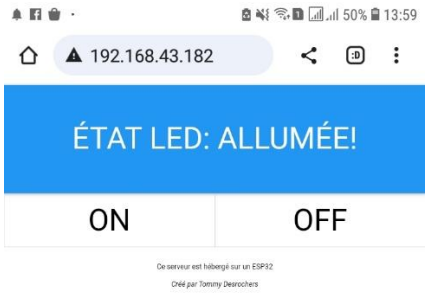

Figure 12site web de la carte ESP32

La figure précédente représente le site web créé pour contrôler l'ESP32.

Figure 13Résultat de contrôle la LED à distance

La figure précédente représente le résultat de contrôle la LED de l'ESP32 à distance.

3.5 Les pentests des vulnérabilités sur kali linux

Pour tester les vulnérabilités de la carte ESP32, on a choisi le système d'exploitation kali linux car il contient de plusieurs outils de pin tests sécurisés et fiables. On a téléchargé le kali linux gratuitement parce qu'il est open source.

Pour débuter notre pin tests on a fait des recherches des attaques contre les serveurs. On a trouvé deux attaques connues DOS et DDOS. La déférence entre ces deux dernières c'est que DOS (deny of service) fait par une seule machine mais DDOS fait par plusieurs machines zombies (botnets).

Et pour cela, on a choisi plusieurs outils pour découvrir et tester les failles de notre carte. On a les mentionné comme suivant :

3.5.1GoldenEye

a. *Définition*

Goldeneye est un outil gratuit et open source disponible sur GitHub. Nous pouvons effectuer une attaque par déni de service à l'aide de cet outil. C'est un framework écrit en .NET Core. Cet outil fournit de nombreuses classes de base et extensions à utiliser dans notre travail quotidien. Cet outil permet à une seule machine de mettre hors service le serveur web d'une autre machine en utilisant du trafic HTTP parfaitement légitime. Il établit une connexion TCP complète, puis n'a besoin que de quelques centaines de requêtes à intervalles réguliers et à long terme. En conséquence, l'outil n'a pas besoin d'utiliser beaucoup de trafic pour épuiser les connexions disponibles sur un serveur. [18]

b. *Utilisations de Goldeneye*

- Goldeneye utilise du trafic HTTP parfaitement légitime.
- Une attaque par déni de service peut être exécutée à l'aide de Goldeneye en générant un trafic important à partir de botnets.
- Goldeneye envoie plusieurs requêtes à la cible, ce qui génère un trafic important à partir de botnets.
- Goldeneye peut être utilisé pour effectuer des attaques DDoS sur n'importe quel serveur web.

c. *Test de GoldenEye*

Après avoir l'utilité de cette commande on a décidé de travailler avec elle

- Tout d'abord ; on a installé Goldeneye avec le lien suivant :

git clone https://github.jseidl/GoldenEye.git

- Et pour changer le répertoire de kali linux on a écrit sur la ligne des commandes « cd Goldeneye pour pointer vers le répertoire Goldeneye ce qui permet d'accéder aux fichiers qui s'y trouvent
- ls : cela signifie une tentative de liste des fichiers et répertoires.
- "http://192.168.43.182/" est l'URL de la cible sur laquelle l'attaque sera effectuée.
- "-s 10" spécifie que 10 threads seront utilisés pour l'attaque. Cela signifie que l'attaque sera simultanée et utilisera plusieurs connexions pour augmenter l'impact.
- "-m random" indique que le mode de sélection des requêtes sera aléatoire. Cela signifie que les requêtes seront générées de manière aléatoire, ce qui rendra l'attaque plus difficile à détecter et à contrer.

Dans la pratique des captures précédentes le serveur a été bloqué. On n'a pas pu accéder au site web de la carte.

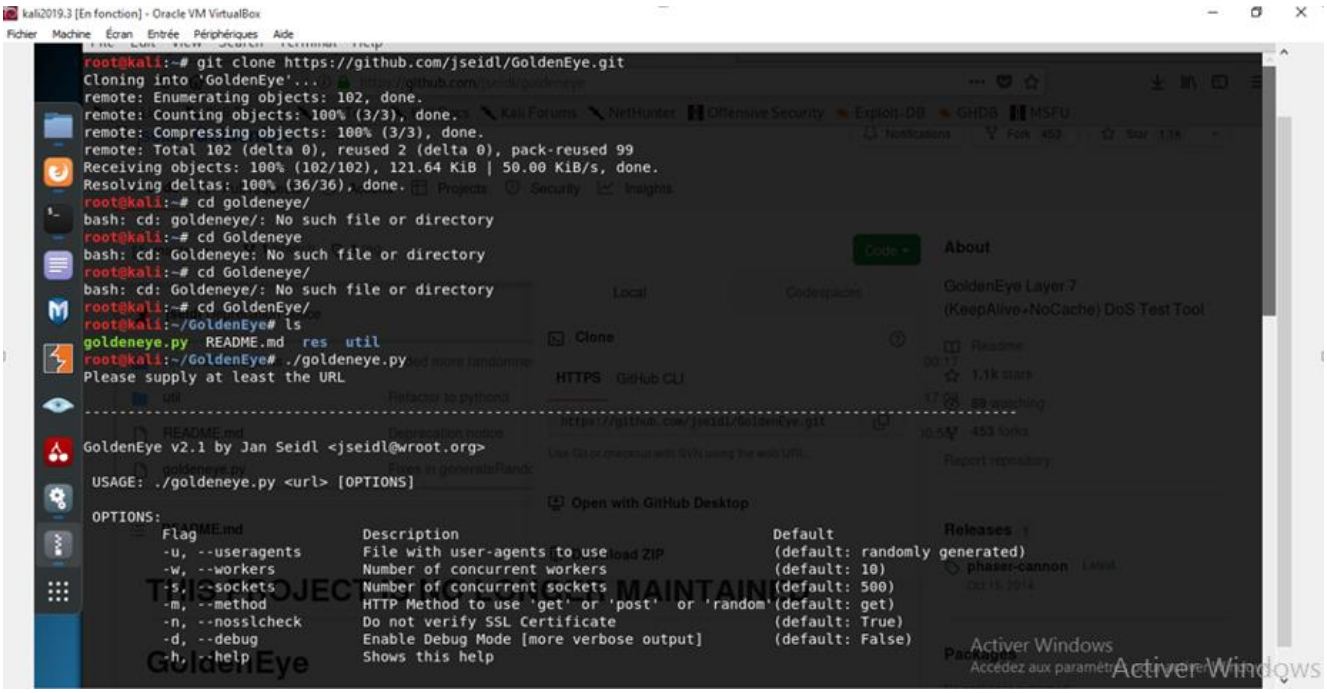

Figure 14 capture de test commande GoldenEye

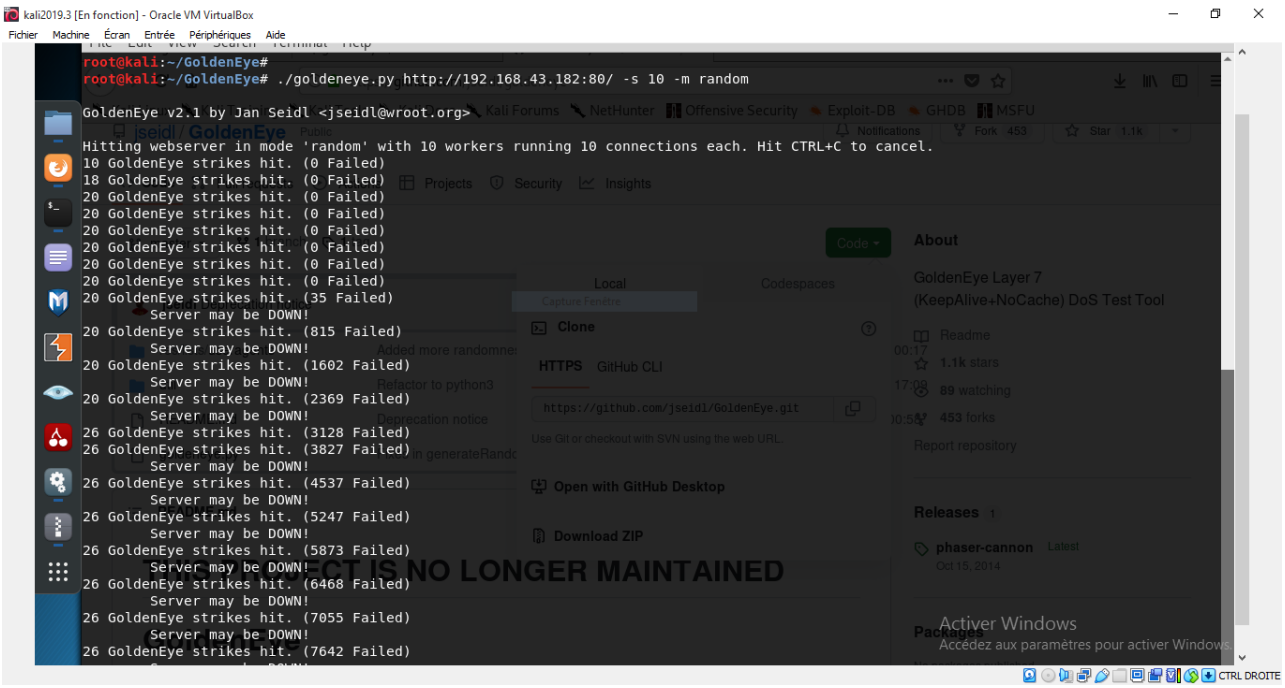

Figure 15 capture de test commande GoldenEye

3.6 Test de LOIC

3.6.1low orbit ion cannon (LOIC)

Low orbit ion cannon est un logiciel open-source développé en programme C par l'équipe Praetox Technologies. Il est à la base utilisée dans le but d'effectuer du « network stress testing » Qui est un type de test, dont le but va être de pousser le service à l'extrême, jusqu'à Ses limites. Il permet de soumettre aux serveurs une charge massive de trafic réseau Afin de pouvoir le diagnostiquer. Au fil du temps et des mises à jour, il a été modifié, Popularisé et utilisé comme un outil DDOS notamment par le mouvement hacktiviste Anonymous.

Au travers de ce logiciel on peut donc très simplement mettre en place une attaque DOS/DDOS. Il nous permet de surcharger des serveurs de requêtes TCP, UDP ou http jusqu'à ce qu'ils ralentissent, voir dans le pire des cas, ne répond plus. En effet, IL est effrayamment très simple à prendre en main et ne nécessite pas de grandes connaissances en informatique. Bien évidemment, la majorité des services actuels sont un minimum protégé contre ce type d'attaque. Par conséquent, une attaque DOS ne générerait pas assez de requêtes pour aboutir à ses fins. En revanche, une attaque DDOS serait envisageable au travers de ce logiciel. Il suffirait que plusieurs milliers d'utilisateurs se coordonnent et lancent l'attaque sur un même réseau au même moment pour que l'attaque fonctionne.

3.6.2Attaque (Exploitation)

- La première étape à faire pour mettre en place l'attaque DOS/DDOS au travers du logiciel Low orbit ion cannon est évidemment de télécharger le programme. Etant donné que ce logiciel contient des utilitaires pour falsifier les différents paquets (TCP/UDP/HTTP), qui vont être envoyés massivement sur la victime. Ceux-ci seront certainement identifiés comme un virus par votre anti-virus, mais il s'agira en réalité d'un faux positif. Pour y remédier, il suffit de faire accepter le programme LOIC dans les paramètres de votre antivirus. Une fois téléchargé et dézipper, il faudra lancer le programme « LOIC.EXE » et une interface utilisateur fera son apparition.

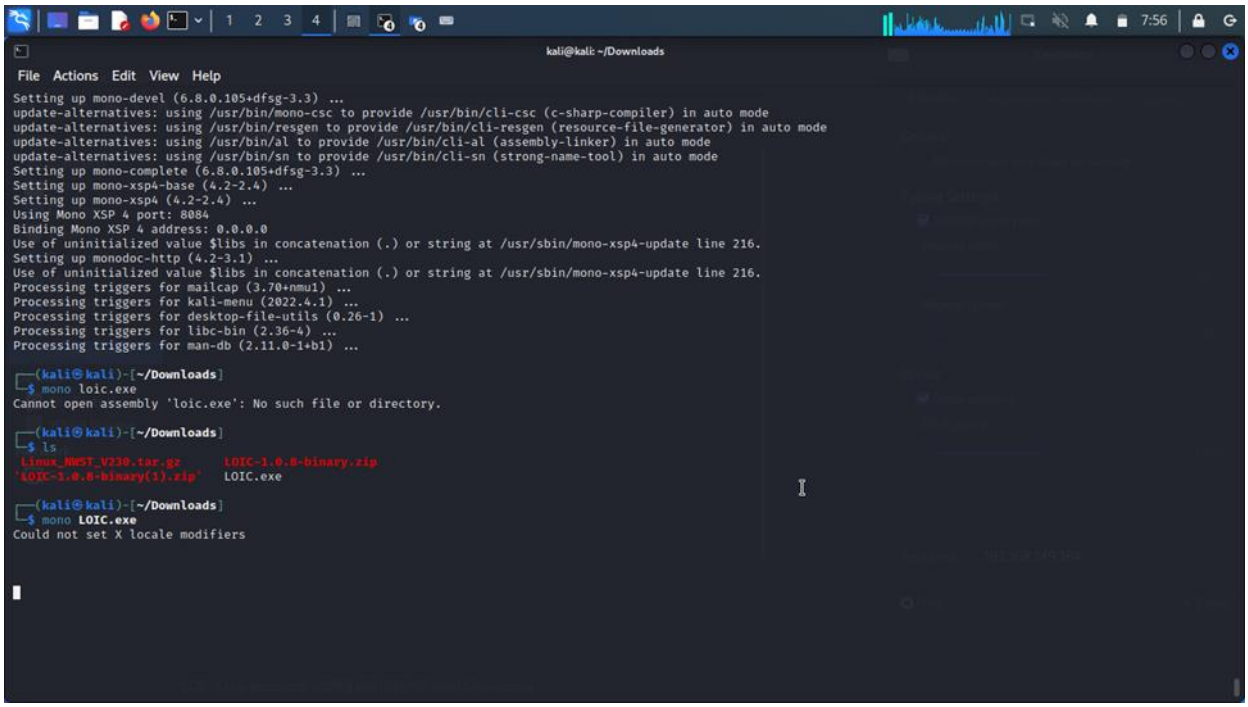

Figure 16 capture de lancement application LOIC

- L'interface utilisateur de Low Orbit Ion Cannon est plutôt explicite. Tout d'abord, nous devons rentrer l'adresse IP ou l'url de notre victime dans la section « Select your target » et cliquer sur le bouton « lock on ». Suite à cela, l'adresse IP ou le lien de la victime devrait s'afficher en grand dans la section « Selected target ». Ensuite, dans la section « Attack options », nous pouvons paramétrer notre attaque DOS/DDOS. En effet, plusieurs options sont possibles. C'est notamment dans cette section que nous allons indiquer la méthode ainsi que le port que nous allons attaquer. Nous pouvons également gérer la vitesse d'envoi des paquets. Pour finir, il ne reste plus qu'à lancer l'attaque.

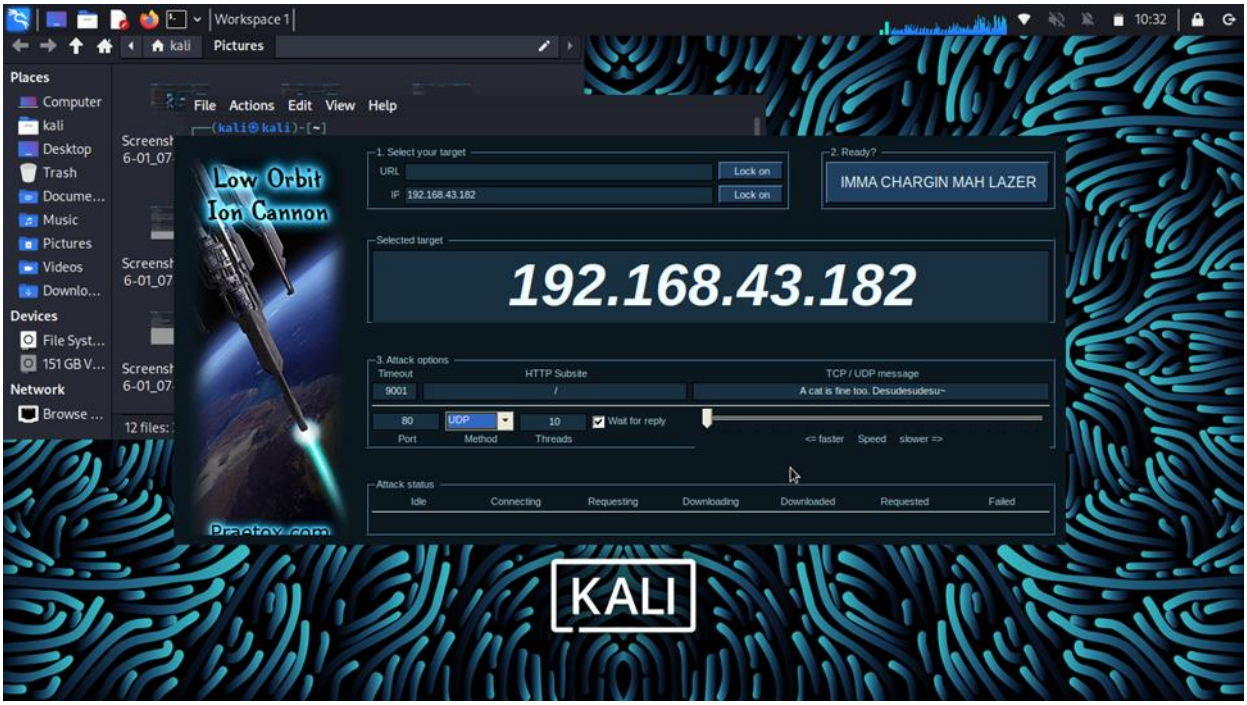

Figure 17 Application LOIC

- Pour ce faire, il suffit de cliquer sur le bouton « IMMA CHARGIN MAH LAZER » dans la section « Ready ? ». L'affichage du détail de l'attaque se fera dans la section « Attack status » où nous pouvons notamment apercevoir le nombre de requêtes envoyées. Au travers de l'invite de commande.

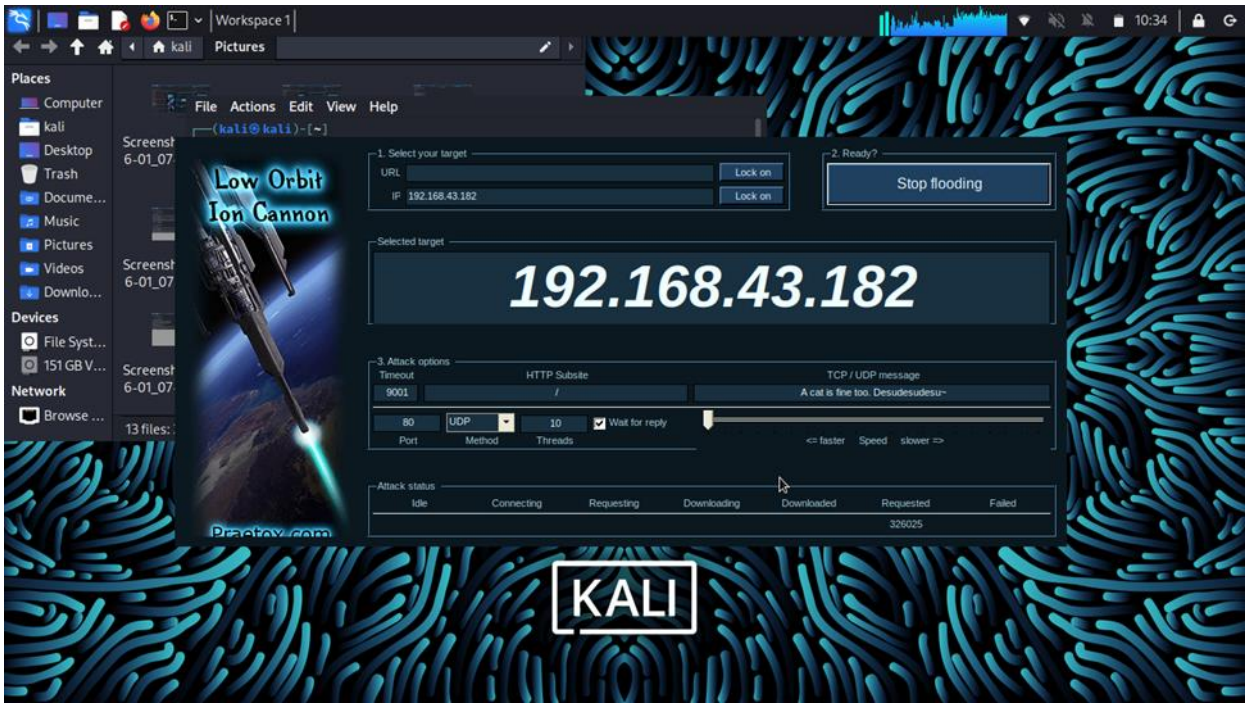

Figure 18 test de l'application LOIC

- Un ping au serveur web a été fait afin de pouvoir évaluer l'impact que possède le programme LOIC sur celui-ci. Nous pouvons constater qu'en temps normal, avant que l'attaque soit lancée, le temps de réponse est constant et tourne autour des 2 millisecondes ce qui est très rapide. Suite

au lancement du programme Low Orbit Ion Cannon, nous pouvons constater un temps de réponse qui augmente considérablement allant jusqu'à atteindre 314 millisecondes ce qui est anormal étant donné que l'appareil est situé en local. Lors de l'arrêt du programme, nous remarquons que le temps de réponse revient à la normale en se rapprochant de nouveau de 2 millisecondes. Malgré un échec lors de l'exécution du ping, nous pouvons voir un ralentissement du temps de réponse mais pas un arrêt complet du service. Comme expliqué précédemment, les attaques DOS sont souvent insuffisantes pour faire tomber un service, car le nombre de requêtes envoyées ne sont pas suffisantes. Il aurait fallu lancer ce programme sur diverses machines différentes (botnet ou machines zombies), au même moment afin d'exécuter une attaque DDOS pour espérer faire tomber le service. [19]

3.7 Wireshark

3.7.1 Introduction à wireshark

Wireshark est un analyseur de paquets open source (GNU) populaire. Ses "dissectors" ou décodeurs de protocoles permettent d'interpréter le trafic du réseau. Conçu en 1997-1998 par Gerald Combes sous le nom historique de "Ethereal", il est repris en 2006 sous le nom moderne de "Wireshark". En 2008, Wireshark sort en version 1.0 et en 2015 en version 2.0 avec une nouvelle interface graphique.

3.7.2 Fonctionnalités de wireshark

Les fonctionnalités principales de Wireshark sont

- Disponibles pour les systèmes UNIX et Windows.
- Capturer les paquets de données en "live" qui passent en live sur les interfaces à partir de n'importe quel type de supports : Ethernet, Wi-Fi, Bluetooth, Frame-Relay, ATM, HDLC, USB, … Voir Network Média.
- Ouvrir des fichiers de captures de paquets réalisés avec tcpdump/Win Dump, Wireshark et bien d'autres programmes.
- Importer des paquets venant de fichiers texte contenant les charges en hexa de paquets de données.
- Display packets with very detailed protocol information.
- Enregistrer des paquets de données capturés.
- Exporter certains ou tous les paquets capturés dans différents formats.
- Filtrer les paquets sur base de différents critères.
- Rechercher des paquets sur base de différents critères.
- Coloriser des paquets sur base de différents critères.

- Créer différentes statistiques.[20]

Et voilà les captures suivantes montrent comment on ouvre wireshark pour avoir les listes des paquets transmises et ses source et destination.

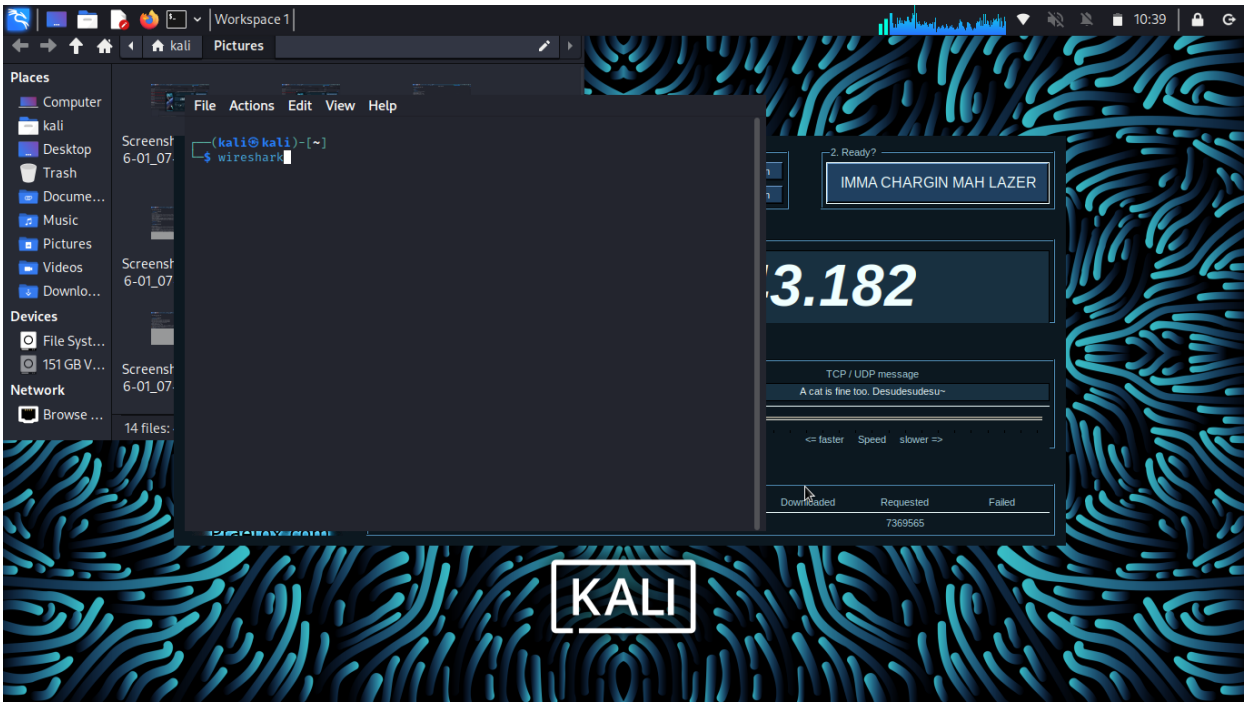

Figure 19 wireshark

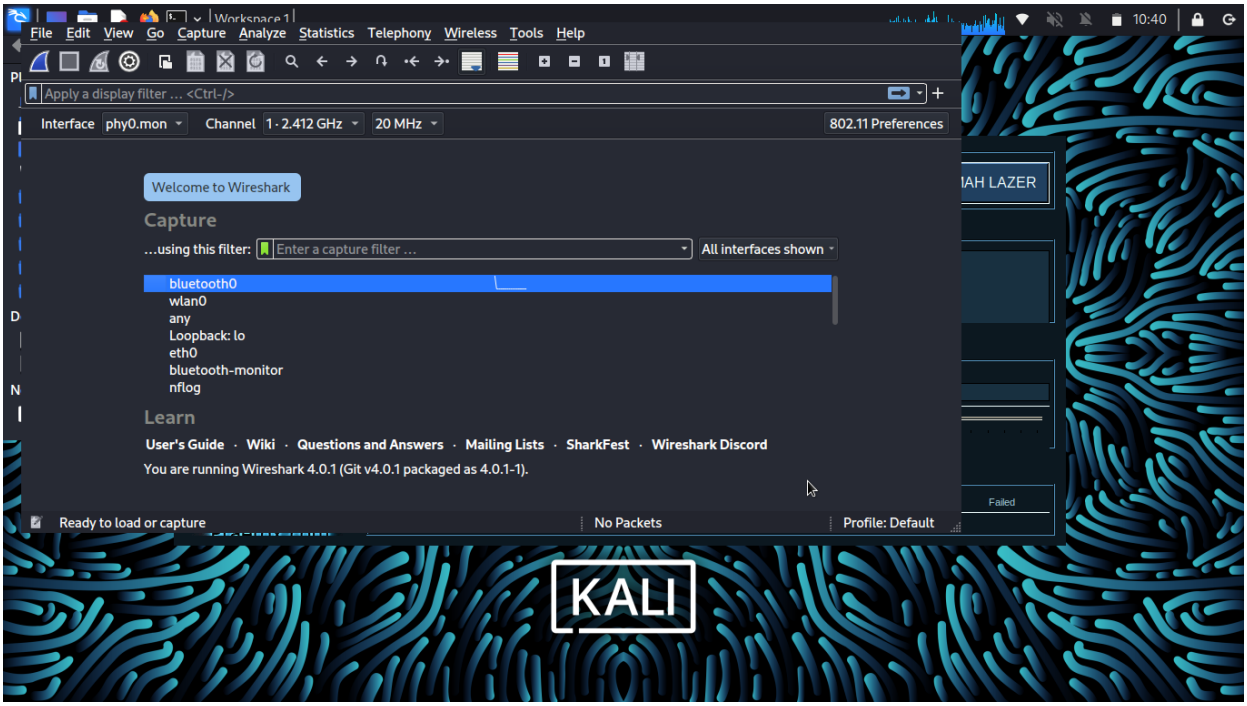

Figure 20 réglage des paramètres de wireshark

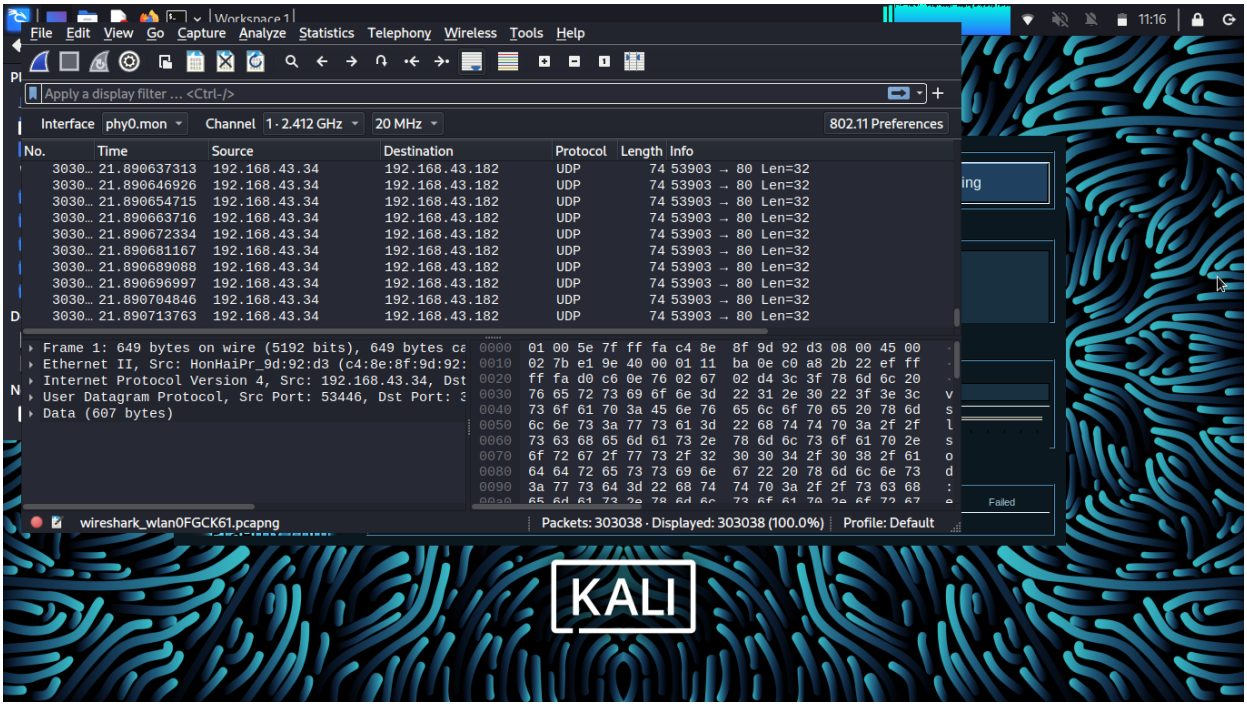

Figure 21 résultats obtenus de wireshark

3.8 Mise en place de broker MQTT

Le principe de broker MQTT c'est d'envoyer les requêtes entre le subscriber et le publish comme intermédiaire entre les deux.

Pour tester le broker MQTT, On a téléchargé le Mosquitto sur ce site https://mosquitto.org/download/ et puis on a terminé les étapes de l'installation de fichier sur le pc. Pour démarrer le Mosquitto on a ouvert une commande CMD au tant qu'administrateur pour accéder à Mosquitto.et voilà la figure qui montre la fenêtre de commande cmd suivante :

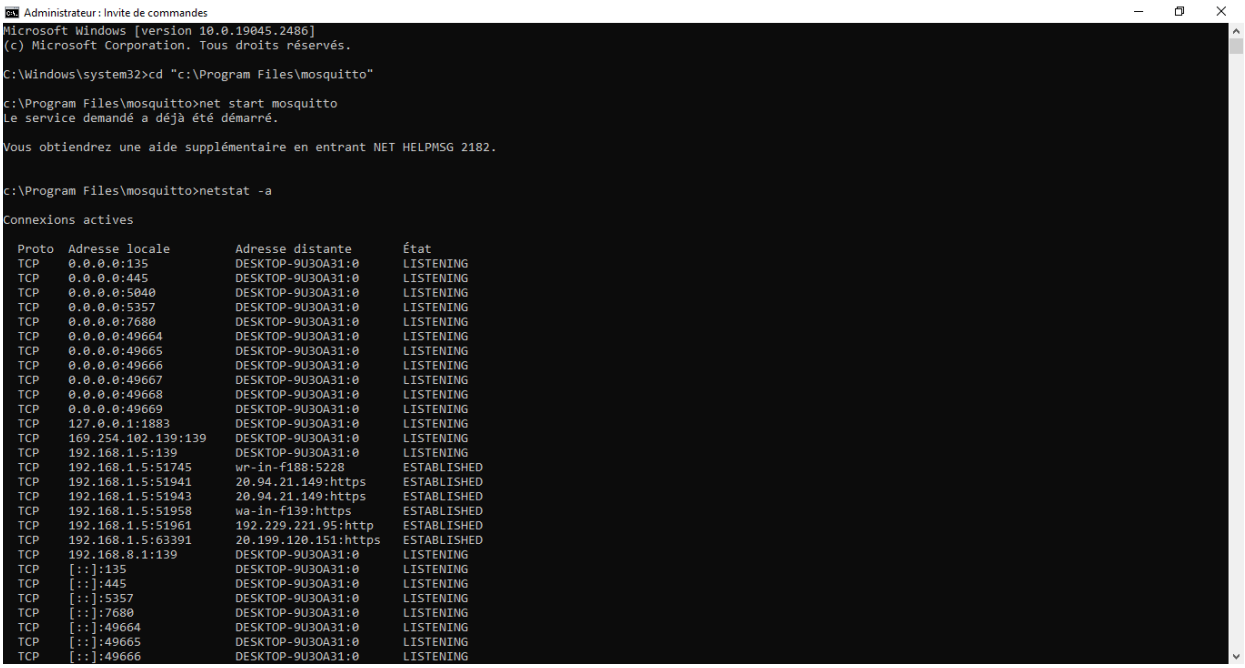

Figure 22 Démarrage de Mosquitto

La figure précédente montre le démarrage de mosquitto et les connexions actives du pc avec les autres adresses IP avec des requêtes.

Et pour tester la fonctionnalité de ce Mosquitto, on a le placé entre deux invites de commandes sur un même pc. Une invite de commande cmd pour le Publisher et l'autre pour subscriber.la figure suivante montre les deux fenêtres :

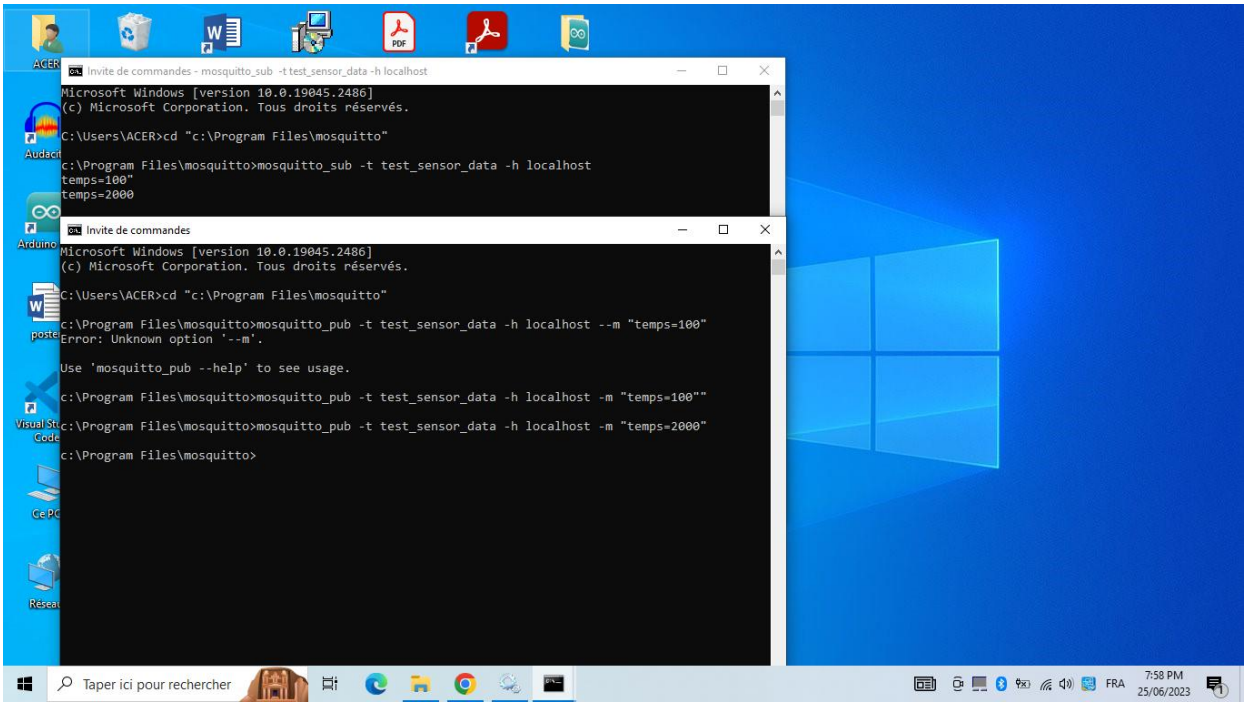

Figure 23 les fenêtres (subscriber & Publisher)

On a fait un pentest avec logiciel LOIC sur le broker Mosquitto avec une attaque DDOS, l'attaque a marché mais elle n'a pas bloqué le Mosquitto. Car le Mosquitto a une architecture de protection qui bloque les requêtes fragmentées. Voilà la figure suivante montre le pentest :

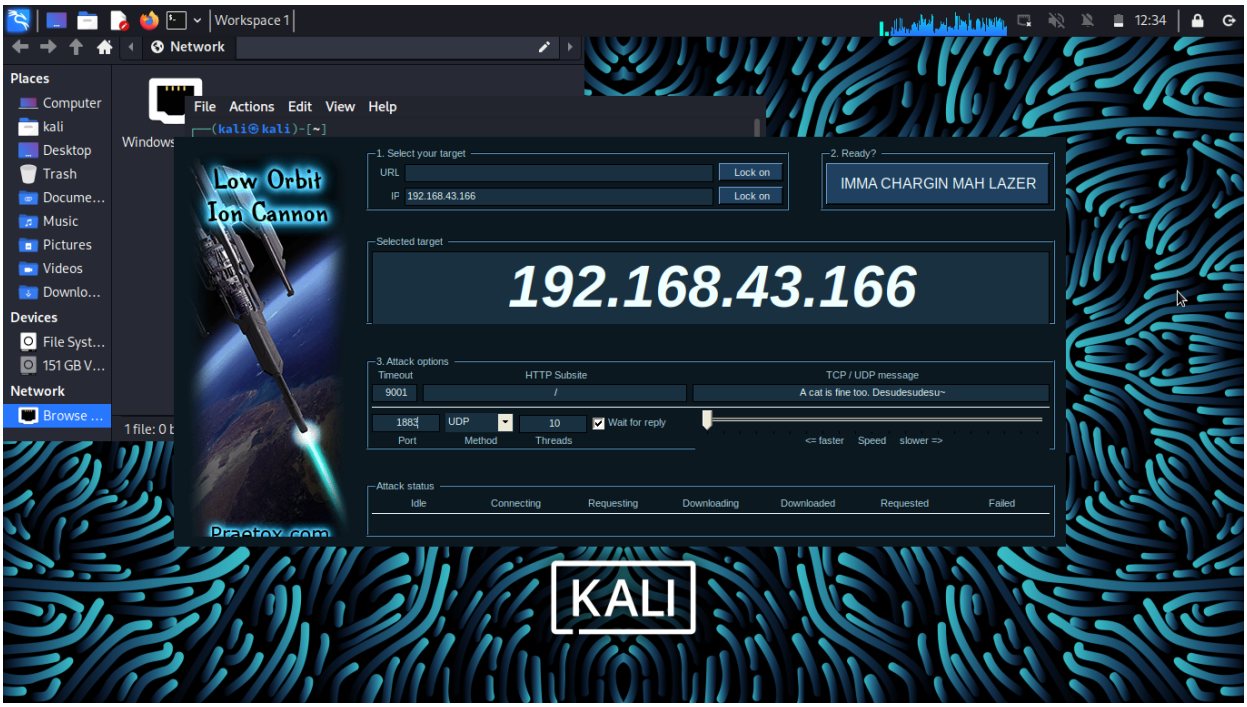

Figure 24 pentest de Mosquitto

3.9 Conclusion

En conclusion, ce chapitre souligne l'importance de l'expérimentation et des tests de sécurité dans la protection des systèmes et des réseaux. La configuration d'un environnement de test adéquat et l'utilisation des outils de test de Kali Linux offrent des moyens efficaces d'évaluer la sécurité d'un système et d'identifier les zones à risque. Grâce à ces tests, il est possible de mettre en place des mesures de sécurité appropriées pour renforcer la résilience des infrastructures informatiques.

Chapitre 4 Résultats, discussion et recommandations

4.1 Introduction

La mission du chercheur consiste à effectuer plusieurs tests tout au long de son travail scientifique afin d'obtenir des résultats plus précis et réduire les erreurs. Par conséquent, ce chapitre sera abordé de manière professionnelle en exposant les différents tests réalisés au cours de notre recherche dans le domaine de vulnérabilités des objets connectés.

Ensuite, nous examinerons chaque résultat obtenu en évaluant tous les critères pertinents pour cette étude, tout en cherchant à identifier les problèmes qui ont contribué à l'augmentation des erreurs et à la diminution des performances des modèles de classification.

En conclusion, nous interpréterons les résultats obtenus afin d'aboutir à une conclusion pertinente pour notre étude, en prenant en compte tous les aspects qui contribuent à la construction de la structure de notre recherche scientifique.

4.2 Analyse des résultats des tests de sécurité

Comme indiqué dans le chapitre précédent, nous avons manipulé les données d'entrée en utilisant deux méthodes différentes afin d'obtenir différents types d'informations à traiter. C'est pourquoi nous aurons donc deux résultats distincts à évaluer.

Chaque résultat obtenu comportera des images à visualiser et à commenter, en observant les différentes caractéristiques qu'elles présentent. Nous aborderons les deux types de classification de la même manière, en accompagnant chaque méthode de manipulation des données de commentaires explicatifs.

4.2.1GoldenEye

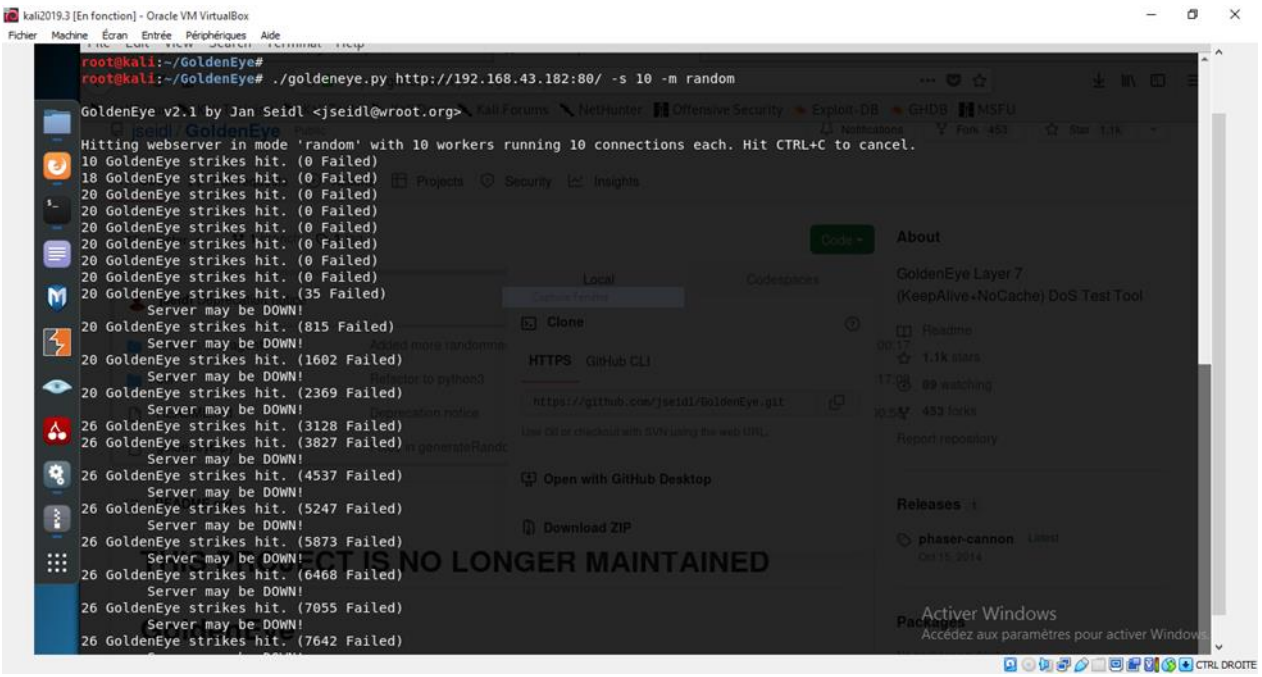

Figure 25 test de commande de GoldenEye

Commentaires

- Avant de lancer l'attaque GoldenEye, le serveur web de la carte ESP32 était au cours de fonctionnement.
- Quand on a lancé l'attaque, on a vu les lignes de terminal indique ce message (server may be down) cela signifie que le serveur victime peut être hors de fonctionnement.
- Et pour confirmer le message obtenu sur le terminal on a testé la connectivité de serveur.
- Les premiers temps après l'attaque, le serveur a était bloqué.
- Mais quand on a essayé une autre fois cet attaque, le serveur a bien marché donc l'attaque a fonctionné une seule fois pas plus.

4.2.2LOIC (Low Orbit Ion Cannon)

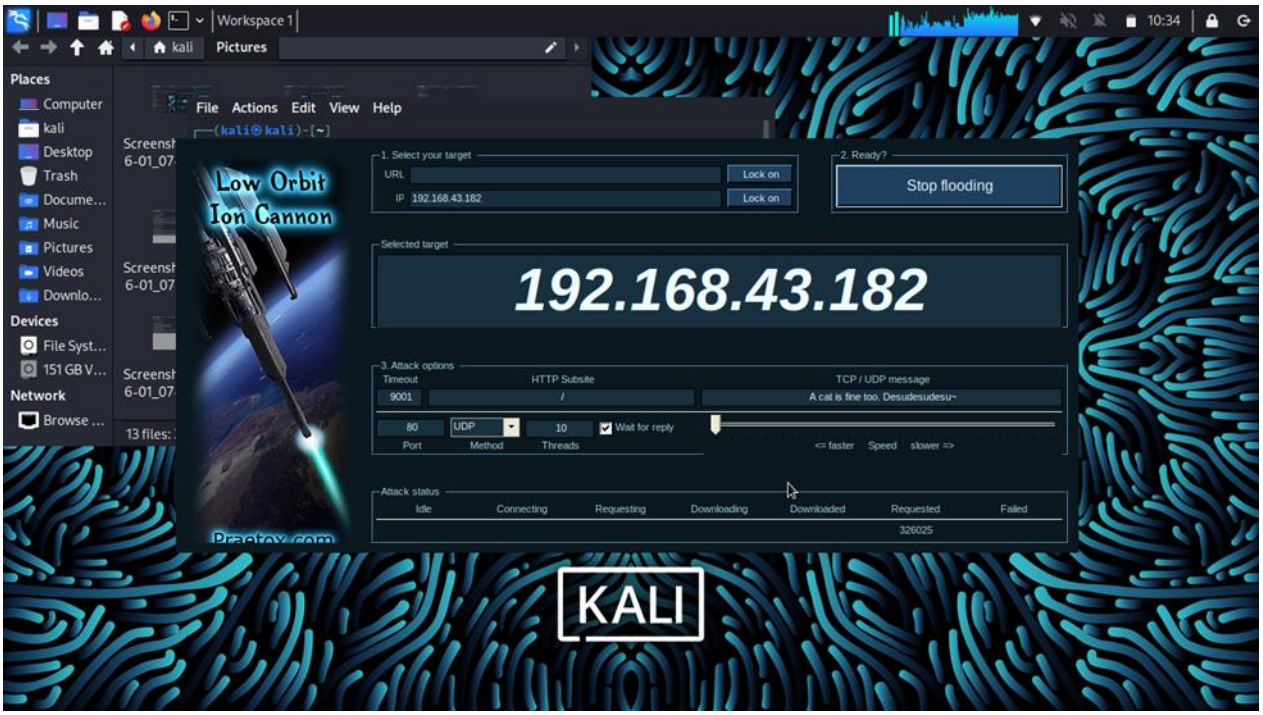

Figure 26 test de l'application LOIC

Commentaires

- Après l'installation de LOIC on obtient la fenêtre précédente, on a choisi le Protocol TCP et l'adresse de la carte ESP32 victime.
- Et puis on a cliqué sur le bouton (IMMA CHARGIN MAH LAZER) pour débuter l'attaque DDOS.
- Quand l'attaque a débuté, on a vu le des requêtes augmente rapidement dans quelques secondes.
- Le rôle des requêtes transmises est la saturation de la bande passante de serveur de la carte ESP32.et pour cela on n'a pas pu accéder au serveur durant que l'attaque se déroulai.
- L'avantage de cette application LOIC est la facilité d'utilisation et la fiabilité de l'attaque.

4.3 Discussions des résultats

La commande GoldenEye et l'application LOIC (Low Orbit Ion Cannon) sont deux outils utilisés dans le domaine des tests de pénétration et des attaques par déni de service (DDoS). Bien qu'ils aient des objectifs similaires, il existe des différences significatives entre ces deux outils en termes de

fonctionnalités, d'efficacité et d'utilisation. Cette étude comparative vise à évaluer les avantages et les limitations de chaque outil afin de déterminer lequel est préférable dans certaines situations.

4.3.1GoldenEye

La commande GoldenEye est un outil basé sur Python qui permet de mener des attaques DDoS en envoyant un grand nombre de requêtes à une cible spécifique. Il offre des fonctionnalités telles que la personnalisation des requêtes, le choix du type d'attaque (GET, POST, etc.) et la possibilité d'utiliser des proxies pour masquer l'origine des attaques. GoldenEye est souvent utilisé pour tester la résilience d'un système face à une attaque DDoS simulée.

a. *Avantages de GoldenEye*

- Personnalisation des requêtes : GoldenEye permet de modifier les paramètres des requêtes, ce qui peut rendre les attaques plus sophistiquées et difficiles à détecter.
- Utilisation de proxy : L'utilisation de proxy permet de cacher l'adresse IP de l'attaquant et de rendre les attaques plus difficiles à tracer.
- Flexibilité : GoldenEye offre une flexibilité dans la configuration des attaques, ce qui peut être utile pour des scénarios spécifiques.

b. *Limitations de GoldenEye*

- Niveau de sophistication : Bien que GoldenEye offre des fonctionnalités de personnalisation, il peut ne pas être aussi puissant ou sophistiqué que d'autres outils plus avancés sur le marché.
- Détection : GoldenEye peut être plus facilement détecté par les systèmes de défense contre les DDoS en raison de ses caractéristiques spécifiques.

4.3.2LOIC (Low Orbit Ion Cannon)

LOIC est une application largement utilisée pour mener des attaques DDoS. Contrairement à GoldenEye, LOIC est une application graphique qui permet à l'utilisateur de spécifier la cible et de lancer l'attaque en appuyant simplement sur un bouton. LOIC utilise des requêtes HTTP ou UDP pour inonder la cible de trafic et la submerger.

a. Avantages de LOIC

- Facilité d'utilisation : LOIC est très convivial et ne nécessite pas de compétences techniques avancées pour être utilisé.
- Accessibilité : LOIC est largement disponible en téléchargement gratuit sur Internet, ce qui le rend facilement accessible pour les utilisateurs.

b. Limitations de LOIC

- Puissance limitée : LOIC peut ne pas générer autant de trafic ou être aussi efficace que d'autres outils plus avancés dans le domaine des attaques DDoS.

- Détectabilité : En raison de sa popularité et de sa simplicité, LOIC est souvent facilement détectable et peut être bloqué par des mesures de sécurité appropriées.

L'attaque par LOIC repose sur le principe d'inonder la cible avec un grand nombre de requêtes. LOIC peut utiliser des requêtes HTTP ou UDP pour générer un trafic excessif vers le système cible. Cette surcharge de requêtes et de trafic entraîne une saturation des ressources disponibles, ce qui peut rendre les services du système cible inaccessibles aux utilisateurs légitimes.

La commande GoldenEye, quant à elle, fonctionne en envoyant un grand nombre de requêtes personnalisées à la cible. Ces requêtes peuvent être modifiées pour cibler des vulnérabilités spécifiques ou pour simuler différentes méthodes d'attaque. L'objectif est de submerger la cible avec un flux constant de requêtes, épuisant ainsi les ressources disponibles et provoquant un déni de service.

Dans les deux cas, l'attaque par déni de service exploite la limite des capacités du système cible à gérer un volume élevé de trafic ou de requêtes. Cela peut entraîner une surcharge des ressources du système, telles que la bande passante, la mémoire, le processeur ou les connexions réseau. En conséquence, le système peut devenir indisponible pour les utilisateurs légitimes, ce qui peut causer des perturbations importantes et des dommages financiers pour les organisations ciblées.

4.4 Recommandations pour renforcer la sécurité des objets connectés basés sur ESP32

Il est beaucoup plus simple de gérer une attaque par déni de services plutôt qu'une attaque par déni de service distribuée. En effet, si l'attaque provient d'une seule adresse IP telle que pour l'attaque DOS, nous pouvons facilement l'identifier et la bloquer. En revanche, quand l'attaque est dite distribuée, les adresses IP sont multiples et par conséquent, sont plus difficilement gérables. Malgré tout, il existe tout de même certaines techniques pour essayer de contrecarrer les attaques par déni de services distribuées afin d'éviter au maximum que les services soient totalement indisponibles. En voici quelques exemples

4.4.1Les systèmes d'alertes automatiques

Mettre en place des systèmes d'alertes automatiques qui vont permettre d'effectuer les premières interventions. En cas de trafic anormal sur le réseau, son rôle est d'avertir les administrateurs afin qu'ils puissent dès le début de l'attaque, essayer de prendre le contrôle de celle-ci et de limiter les dégâts. Les administrateurs doivent donc connaître parfaitement le système afin de différencier l'état « normal » des événements spéciaux.

- Exemple d'outil/application :

Cloudflare : Service assurant à un site web de la performance, fiabilité et de la sécurité contre les attaques malveillantes notamment contre les attaques DDOS où des systèmes d'alertes automatiques sont mis en place.

IPS/IDS : Snort, Bro ou encore surricata par exemple, sont des systèmes de prévention d'intrusion qui avertissent en temps réel lorsqu'il y a du trafic anormal sur le réseau.

4.4.2Évaluation automatique régulière

Évaluation automatique régulière des fichiers logs afin de détecter toutes les éventuelles anomalies présentes sur le système. Notamment au niveau du réseau de l'entreprise, il est important de suivre l'évolution du trafic de l'entreprise. En plus de la détection d'anomalie, cela permet à l'entreprise d'être au courant de l'évolution des visiteurs sur leurs plateformes.

- Exemple d'outil/application :

Nagios : Jugé comme l'un des meilleurs outils disponibles sur le marché, il s'agit d'un analyseur de réseaux puissants permettant notamment de détecter des menaces de sécurité. Les administrateurs système ont des vues en temps réel de la santé du réseau de l'entreprise.

Ntopng : Analyseur réseau à grande vitesse, il permet de surveiller la fréquentation du réseau en temps réel de façon très performante. Il est compatible avec tout type de système d'exploitation tel que Unix, Windows ou MacOs.

4.4.3Mettre en place un plan d'urgence

Mettre en place un plan d'urgence afin de limiter le temps d'indisponibilité des services. Effectuer une analyse des risques complète avec les différentes mitigations pour chacun des risques. Imaginer et prévoir les pires scénarios possibles et mettre en place des solutions pour réduire l'impact des dégâts dans le cas où ils arriveraient. Ce qui comprend également la formation des différents collaborateurs impliqués.

- Exemple d'outil/application :

Méhari : Méthode harmonisée d'analyse de risque suivant une logique d'amélioration continue passant notamment par l'analyse des enjeux majeurs, étude des vulnérabilités, mitigation de la gravité des risques ainsi que le pilotage de la sécurité de l'informations.

Ebios :Outil d'analyse de risque de l'agence nationale de la sécurité des systèmes d'information française passant par l'expression des besoins et l'identification des objectifs de sécurité.

4.4.4Mise en place d’un pare-feu ou/et d’un système de prévention d’intrusion (IPS)

Les pares feux et les IPS d’aujourd’hui assurent un certain niveau de défense contre les attaques DDOS. Certains des pares feux actuels NGFW (Next Generation Firewall) intègrent déjà des services IPS et DDOS.

- Exemple d’outil/application :

Snort : Système de détection d’intrusion open source permettant de configurer des règles et d’être averti en temps réel lorsque celles-ci ne sont pas respectées.

Cisco Firepower : Pare-feu de type NGFW disponible de plusieurs formes assurant la sécurité d’une organisation. La fonctionnalité NGFW est capable de détecter et bloquer les logiciels malveillants circulant sur le réseau.

4.4.5Filtrer les adresses IP

Si l’attaque provient d’un petit nombre d’adresses. En effet, depuis le routeur ou le pare-feu, il est possible de bloquer ces adresses IP. Évidemment, cette technique est faisable dans le cas d’une attaque DOS ou si les nombres d’adresses IP émises lors de l’attaque ne sont pas volumineuses.

4.5 Conclusion

En conclusion, l'analyse des résultats des tests de sécurité effectués sur les objets connectés basés sur ESP32 a révélé plusieurs vulnérabilités importantes. Ces vulnérabilités mettent en évidence les risques potentiels auxquels ces dispositifs sont exposés lorsqu'ils sont connectés à un réseau. Il est essentiel de comprendre et de prendre en compte ces vulnérabilités afin de renforcer la sécurité des objets connectés.

Il est impératif de reconnaître que la sécurité des objets connectés est un défi constant et évolutif. Les attaques réseau se perfectionnent continuellement, et il est donc essentiel de mettre en place des mesures de sécurité solides pour protéger les objets connectés et les utilisateurs qui les utilisent. En suivant les recommandations fournies dans ce chapitre, il est possible d'améliorer significativement la sécurité des objets connectés basés sur ESP32 et de réduire les risques liés aux attaques réseau.

Conclusion générale

En conclusion, cette étude a exploré les techniques de sécurité pour les objets connectés contre les attaques réseau, en mettant l'accent sur les dispositifs basés sur ESP32. Tout au long de ce travail, nous avons identifié les vulnérabilités courantes des objets connectés, analysé en détail les failles spécifiques à ESP32 et mené des tests de sécurité approfondis pour évaluer leur résistance face aux attaques.

L'analyse des résultats a révélé l'existence de vulnérabilités significatives au sein des objets connectés basés sur ESP32, mettant en évidence les risques auxquels ces dispositifs sont exposés lorsqu'ils sont connectés à un réseau. Ces vulnérabilités concernent notamment l'authentification, l'autorisation, la confidentialité des données et l'intégrité du système. Cependant, grâce à une approche méthodique et à l'utilisation d'outils de test avancés, nous avons pu identifier ces vulnérabilités et proposer des mesures de sécurité correspondantes pour les atténuer.

Les recommandations formulées dans ce travail visent à renforcer la sécurité des objets connectés basés sur ESP32. Elles comprennent la mise en œuvre de mécanismes d'authentification robustes, l'utilisation de protocoles de communication sécurisés, la gestion rigoureuse des autorisations, la mise à jour régulière des micrologiciels pour corriger les failles connues, ainsi que l'éducation des utilisateurs sur les bonnes pratiques en matière de sécurité. En suivant ces recommandations, il est possible d'améliorer la sécurité des objets connectés et de réduire les risques liés aux attaques réseau.

Il est important de souligner que la sécurité des objets connectés est un défi constant et évolutif. Les attaquants cherchent constamment de nouvelles façons de compromettre la sécurité des dispositifs IoT, et il est donc essentiel de rester vigilants et de continuer à développer des solutions de sécurité robustes. La collaboration entre les acteurs de l'industrie, les chercheurs en sécurité et les utilisateurs finaux est essentielle pour faire face à ces défis et garantir un environnement IoT sûr et fiable.

En conclusion, cette étude représente une contribution significative à la compréhension des techniques de sécurité pour les objets connectés contre les attaques réseau. En renforçant la sécurité des objets connectés basés sur ESP32, nous sommes en mesure de protéger la vie privée des utilisateurs, de prévenir les perturbations potentielles des infrastructures critiques et de favoriser une adoption confiante de l'Internet des objets. Il est essentiel de poursuivre les efforts de recherche et de développement dans ce domaine pour garantir un avenir connecté sécurisé pour tous.

Bibliographie

[1] Christophe Baland, Damien Cauquil, Thomas Gayet, Julia Juvigny, Renaud Lifchitz, Nha-Khanh Nguyen , la sécurité de l‟Internet des Objets, livre blanc.

[2] Cluster of European Research Projects on the Internet of Things, “Vision and Challenges 74 for Realising the Internet of Things”, March 2010.

[3] https://wikimemoires.net/2019/09/domaines-d-applications-de-l-iot/ consulté 11 septembre 2019

[4] David Hanes et al., "IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things", 1st Edition, Cisco Press, June 2017.

[5] C. Bormann, A. P. Castellani et Z. Shelby, « CoAP: An Application Protocol for Billions of Tiny Internet Nodes », IEEE Internet Computing, vol. 16, no 2, 1er mars 2012, p. 62–67.

[6] Gerardus Blokdyk, "Message Queue Telemetry Transport A Clear and Concise Reference" Paperback, July 6, 2022.

[7] Peter Saint-Andre, Kevin Smith, Remko Tronçon, "XMPP: The Definitive Guide: Building Real-Time Applications with Jabber Technologies", 1st Edition, O'Reilly Media, June 2009.

[8] MOULAI MOSTEFA sakina, LARBI chaimaa, "Conception D’un Système D’acquisition Des Données En Temps Réel A Base De IOT En Utilisant Le Protocole MQTT", Mémoire de Master, UNIVERSITE YAHIA FARES DE MEDEA, 2021.

[9] Flavien ROUX, "LES 5 PROBLÈMES DE SÉCURITÉ INFORMATIQUE LES PLUS COURANTS ET COMMENT LES RÉSOUDRE", Journal du Freenaute, Mai 5, 2022, consulté le 15 mai 2023, https://www.journaldufreenaute.fr/les-5-problemes-de-securite-informatique-les-plus-courants-et-comment-les-resoudre/

[10] Pierre-Louis Lussan, "Les 10 types de cyberattaques les plus courants", netwrix, 17 octobre 2022, consulté le 20 mai 2023, https://blog.netwrix.fr/2018/07/04/les-10-types-de-cyberattaques-les-plus-courants/

[11] Faker Skandrani,"Cyberattaques : Top 6 des vulnérabilités", consulté le 01 juin 2023, https://iotindustriel.com/cybersecurite/cyberattaques-iot-top-6-des-vulnerabilites/

[12] Younes ABBASSI, Habib BENLAHMER, "Un aperçu sur la sécurité de l'internet des objets (IOT)", Colloque sur les Objets et systèmes Connectés - COC'2021, IUT d'Aix-Marseille, Mar 2021, MARSEILLE, France.

[13] http://algo.tn/esp32/introduction/, consulté le 10 juin 2023.

[14] https://www.gotronic.fr/art-module-nodemcu-esp32-28407.htm, consulté le 05 juin 2023.

[15] Massimo Banzi, "Getting Started with Arduino (Make: Projects)"; First Edition, Make: Books, October 15, 2008.

[16] https://www.funinformatique.com/kali-linux-cest-quoi/, consulté le 10 juin 2023.

[17] https://youtu.be/zqwnYuOLvsE/consulé le 24 janvier 2020

[18] https://stacklima.com/outil-goldeneye-ddos-dans-kali-linux/, consulté le 10 juin 2023.

[19] Gomes Michael, "Analyse de cyberattaques et proposition de solution au travers du pentesting", Mémoire de bachelor: Haute école de gestion de Genève, 2021.

[20] François Goffinet, "Introduction à Wireshark", sip, consulté le 12 juin 2023, https://sip.goffinet.org/wireshark/introduction-wireshark/