Lightning Malware

Morgane REYNAUD – Yamyna RENAI

Table des matières

Introduction

Objectif du projet

Le projet "Lightning Malware" vise à développer une plateforme en ligne capable d'analyser et de détecter les menaces potentielles présentes dans les fichiers et les adresses IP/URL. Notre objectif principal est de fournir aux utilisateurs un outil intuitif et efficace pour évaluer la sécurité de leurs données et de leurs connexions en ligne.

Contexte et justification

Dans un monde numérique en constante évolution, et face à une augmentation significative des attaques de logiciels malveillants, il est impératif de développer des solutions innovantes pour protéger les données et garantir la sécurité en ligne. Inspiré par des initiatives telles que "VirusTotal", une référence dans le domaine de la sécurité informatique, le projet "Lightning Malware" propose une plateforme de détection des menaces, contribuant ainsi à renforcer la sécurité numérique de ses utilisateurs. En offrant une solution accessible, notre objectif est de fournir aux utilisateurs les outils nécessaires pour identifier et contrer les menaces potentielles, assurant ainsi la protection de leurs données et de leurs activités en ligne.

Planification et Gestion de Projet

Planification du projet

Pour la planification du projet, nous avons mis en place une méthodologie rigoureuse afin de garantir une progression efficace et coordonnée les différentes étapes du projet.

Pour une répartition claire des responsabilités et une gestion efficace des tâches, nous avons élaboré une matrice RACI (Responsibility Assignment Matrix) en planification projet SI. Cette matrice nous permet de déterminer qui est Responsable, qui est Actif, qui doit être Consulté et qui doit être Informé pour chaque activité du projet. Ainsi, chacun des membres de l'équipe sait exactement quelles sont ses responsabilités et à qui il doit rendre compte.

La voici :

	RBS		
		Yamyna	Morgane
WBS	Création interface graphique		
	Création du nom	R	A,C,I
	Création du style css	R	A,C,I
	Uploader les fichiers	R	A,C,I
	Uploader les IP/URL	R	A,C,I
	Infrastructure réseaux/sécurité		
	Acheter un serveur	A,C,I	R
	Acheter un domaine	R	A,C,I
	Avoir un certificat ssl/sshd	R	A,C,I
	Changer le port par défaut	A,C,I	R
	Bloquer la connexion avec l'utilisateur root	A,C,I	R
	Héberger le site sur le serveur	R	A,C,I
	Développement des fonctionnalités		
	Analyser les fichiers avec des anti-virus	R	A,C,I
	Analyser les URL/ip avec des API	A,C,I	R
	Analyser le comportement du fichier	A,C,I	R
	Analyser les fichiers "Keylogger" avec un code	A,C,I	R
	Améliorations supplémentaires du projet		
	Améliorer l'interface graphique si besoin	R	A,C,I
	Analyser un autre type de virus	R,C,I	R,A,C,I

Gestion de projet

Nous avons créé un référentiel GitHub dédié au projet "Lightning Malware", où nous gérons l'ensemble de nos travaux. Ce référentiel est structuré avec un template spécifique pour les projets logiciels, ainsi que des issues qui sont attribuées aux membres du groupe en fonction de leurs compétences et de leur disponibilité.

En combinant ces outils, nous nous assurons que le projet avance de manière organisée. La collaboration et la communication au sein de l'équipe sont facilitées, ce qui favorise la résolution rapide des problèmes et permet d'atteindre nos objectifs dans les délais impartis.

Conception visuelle

Création de l’interface graphique

Pour la conception visuelle de notre projet "Lightning Malware", nous nous concentrons sur la création d'une interface graphique accessible. Notre équipe accorde une attention particulière à chaque détail afin de rendre l'expérience utilisateur aussi facile et agréable que possible. Cela se traduit par :

La création d'une interface graphique conviviale, où chaque élément est soigneusement conçu pour faciliter la navigation et l'interaction des utilisateurs. Nous offrirons également la possibilité d’ajuster le style en fonction des préférences, notamment avec un mode nuit et un mode jour.

La conception d'un nom de projet qui capturent l'essence de "Lightning Malware", signifiant "mettre en lumière les virus". Notre objectif est de fournir aux utilisateurs les outils nécessaires pour lutter contre les virus potentiels.

Le développement d'un style CSS simple mais esthétique, garantissant une présentation harmonieuse sur l'ensemble du site web.

L'intégration de fonctionnalités d'upload des fichiers et des adresses IP/URL, afin d’offrir aux utilisateurs la possibilité de soumettre leurs données pour analyser de manière pratique et sécurisée.

En mettant l'accent sur l'accessibilité et la facilité d'utilisation, notre objectif est de fournir aux utilisateurs une expérience visuelle facile d’utilisation et agréable lorsqu'ils interagissent avec "Lightning Malware".

Infrastructure et Sécurité

Pour garantir la sécurité de notre projet "Lightning Malware", nous accordons une attention particulière à l'infrastructure réseau et à la sécurité. Voici les fonctionnalités que nous allons mettre en place :

Achat d'un serveur : Nous investirons dans l'acquisition d'un serveur dédié, assurant ainsi une performance optimale et un contrôle total sur notre environnement d'hébergement.

Achat d'un domaine : Nous sécuriserons un nom de domaine pour "Lightning Malware", offrant aux utilisateurs un accès facile et une identification claire de notre plateforme.

Obtention d'un certificat SSL/TLS : Pour garantir la confidentialité et l'intégrité des données échangées entre le serveur et les utilisateurs, nous installerons un certificat SSL/TLS. Cela assurera une connexion sécurisée et cryptée, renforçant ainsi la confiance des utilisateurs dans notre plateforme.

Changement du port par défaut : Par mesure de sécurité, nous modifierons le port par défaut utilisé par les services réseau, réduisant ainsi la surface d'attaque potentielle et renforçant la sécurité de notre infrastructure.

Blocage de la connexion avec l'utilisateur root : Pour prévenir les attaques par force brute et limiter les risques d'accès non autorisés, nous configurerons notre système pour bloquer la connexion directe avec l'utilisateur root, imposant ainsi l'utilisation de comptes utilisateurs.

Hébergement du site : Nous mettrons en place un système d'hébergement fiable et sécurisé pour notre site web "Lightning Malware", garantissant une disponibilité maximale et une résistance aux attaques potentielles en le plaçant sur notre serveur sécurisé.

En intégrant ces fonctionnalités dans notre infrastructure réseau et de sécurité, nous nous engageons à offrir à nos utilisateurs un environnement fiable, sécurisé et performant pour accéder à "Lightning Malware" en toute confiance.

Développement et Fonctionnalités

Pour le développement des fonctionnalités de notre projet, nous mettons l'accent sur la mise en place d'outils efficaces pour analyser les menaces potentielles. Voici les fonctionnalités clés que nous allons développer :

Analyse des fichiers avec des anti-virus : Nous intégrerons des moteurs d'analyse antivirus pour inspecter les fichiers téléchargés par les utilisateurs. Cette analyse permettra d'identifier les éventuelles signatures de logiciels malveillants et de protéger les utilisateurs contre les menaces potentielles.

Analyse des URL/IP avec des API : Nous utiliserons des interfaces de programmation (API) pour interroger des bases de données de réputation en ligne, permettant ainsi d'analyser les adresses URL et IP fournies par les utilisateurs. Cette analyse nous permettra de détecter les liens vers des sites malveillants ou des adresses IP suspectes.

Analyse des fichiers "Keylogger" avec un code : Nous développerons des algorithmes spécifiques pour détecter les signatures et les comportements associés aux enregistreurs de frappe (keyloggers) dans les fichiers soumis par les utilisateurs. Cette analyse approfondie permettra d'identifier les logiciels potentiellement dangereux et de protéger les utilisateurs contre les tentatives de vol d'informations sensibles.

En intégrant ces fonctionnalités de développement, nous visons à fournir une plateforme robuste et efficace pour analyser et détecter les menaces de sécurité informatique, offrant ainsi une protection maximale aux utilisateurs de "Lightning Malware".

Amélioration et Perspectives

Pour continuer à améliorer notre projet "Lightning Malware" et à répondre aux besoins évolutifs de nos utilisateurs, nous envisageons plusieurs améliorations supplémentaires, à condition que les fonctionnalités existantes soient déjà bien établies et offrent une expérience utilisateur de qualité :

Amélioration de l'interface graphique si nécessaire : Nous resterons attentifs aux retours des utilisateurs (étudiants, professeurs) et aux évolutions des tendances en matière de design et d'expérience utilisateur. Si nécessaire, nous apporterons des améliorations à l'interface graphique pour garantir une expérience utilisateur fluide, intuitive et esthétique.

Analyse d'autres types de virus : Nous élargirons notre champ d'action en analysant d'autres types de virus et de logiciels malveillants. En explorant de nouveaux vecteurs d'attaque et en intégrant des technologies de détection avancées, nous renforcerons la capacité de "Lightning Malware" à protéger les utilisateurs contre une gamme encore plus large de menaces potentielles.

Conclusion

En conclusion, le projet "Lightning Malware" que nous envisageons pour notre 3ème année en sécurité informatique vise à répondre à l'ensemble des exigences énoncées dans notre cahier des charges. Notre objectif est de créer une plateforme sécurisée qui réponde aux besoins des utilisateurs.

Ce projet annuel résume bien notre parcours en sécurité informatique. Il nous offre l'opportunité de consolider nos connaissances en matière de sécurité des sites web, d'analyse antivirus et de gestion sécurisée des serveurs.

En travaillant sur "Lightning Malware", nous nous préparons à relever les défis complexes liés à ce projet. Il nous permettra d'acquérir une expérience pratique et précieuse, ainsi que de développer des compétences essentielles dans ce domaine.

En résumé, le projet "Lightning Malware" constitue un jalon important dans notre parcours académique et professionnel en cybersécurité.