Cégep du Vieux Montréal

25 mai 2021

Ver informatique

Sprint 3 – Rapport de Projet

Réalisé par

Karl Boulais

Présenté à

Pierre-Paul Monty

Dans le cadre du cours

Projet synthèse

420-B65-VM gr. 00001



Table des matières

[Table des matières 2](#_Toc72598544)

[Le projet 3](#_Toc72598545)

[Retour général 3](#_Toc72598546)

[Résumé du développement 3](#_Toc72598547)

[Problèmes 3](#_Toc72598548)

[Manque de temps 3](#_Toc72598549)

[Fonctionnalités 3](#_Toc72598550)

[Parfaitement fonctionnel 3](#_Toc72598551)

[Semi fonctionnel 3](#_Toc72598552)

[Non fonctionnel 3](#_Toc72598553)

[Abandonné 3](#_Toc72598554)

[Amélioration possible 4](#_Toc72598555)

[Auto-évaluation 4](#_Toc72598556)

Le projet

Retour général

Le but de ce projet était de créer un ver informatique qui se transmettrait et se reproduirait par ses propres moyens d’un système Windows Server 2016 à un autre en abusant de la faille de sécurité Eternal Blue (MS17-010).

Nous voulions aussi ajouter une composante de centre de contrôle qui aurait permit d’avoir une base de données des serveurs infectés ainsi qu’une interface par laquelle nous pourrions contrôler une de ces machines.

Résumé du développement

Problèmes

Manque de temps

Fonctionnalités

Parfaitement fonctionnel

* La reproduction

Semi fonctionnel

* La communication TCP

Non fonctionnel

* Intégration du module Metasploit

Abandonné

* Interface graphique
* Utilisation de Ansible
* Interface graphique

Amélioration possible

Ajouter une interface graphique et la possibilité de recevoir plusieurs connexion TCP en utilisant le module threading de python.

Auto-évaluation

Je crois que la planification de ce projet était bonne. Malheureusement, l’exécution laisse fortement à désirer et qu’avoir à refaire ce projet, je planifierais plus de temps. En ce qui concerne la note, je dirais «A» pour l’intention et «C» pour l’exécution.