Compte rendu n°01

15/03/2017

BOUTANT Thomas
SALMAN Alexandre

Encadrant
CHARMET Fabien
BLANC Grégory

Cette semaine : Un nouvel encadrant et un nouveau projet

- *Réunion le 13/03/2017. Nouvel objectif principal : participation à RESSI 2017*
- *Le projet "Amélioration de la plateforme de génération d'épreuves CTF" devient secondaire*

RESSI 2017 :

https://ressi2017.sciencesconf.org/

du mercredi 17 mai au vendredi 19 mai 2017, à Grenoble

TODO : Création d'un challenge réaliste

Règle du jeu : des équipes auront accès à un site web possédant plusieurs vulnérabilités. Elles devront les trouver et les corriger. En parallèle, des attaques sur ces sites vont avoir lieu, exploitant les vulnérabilités créées. L'équipe qui sécurisera le mieux le site, et par extension gagnera le plus d'argent avec sa plateforme de e-commerce remportera le challenge.

Durée : 3h

Sur le site web : 10 à 15 vulnérabilités

Ce qui a été fait cette semaine :

1 - *Recherche et installation d'une VM : Ubuntu Server*
Fichiers : *./ressources/CassioRessiVM.vdi*
Avancement : *100%*
Remarques :
- *login : cassioressi*
- *password = wordpresse*

Réflexions :
- *A la place de Ubuntu Server : Lubuntu, Xubuntu ? (mais présence d'une interface graphique)*

2 - Création d'un site de e-commerce
Fichiers : *./ressources/wordpress/*
Avancement : *95%*
Remarques :
- Le site est un wordpress
- Un catalogue de 4 articles est disponible
- Le paiement par chèque permet de simuler les échanges (la monnaie devient "virtuelle")

Spécificités :
- *Achat de produits, connexion au site, sélection du moyen de paiement (chèque)*

3 - Installation d'Apache sur la VM
Avancement : 30% (en cours)
Remarques :
- *Tutoriels trouvés. Nous en avons testé un qui n'a pas été concluant.*

II - Autres

Formation/Résolution de challenges

Scores	Thomas	Alexandre
RootMe	**Challenges :** 405 Points 37/245 **Place :** 5729/46045	**Challenges :** 170 Points 18/245 **Place :** 11636/46045
NewbieContest	**Points :** 262 **(+6)** **Position :** : 3533 / 43482	**Points :** 108 **Position :** 8540 / 43482
HackThisSite	**391 Points (+391)**	
OverTheWire	**Bandit - level 12**	
W3Challs	**Position : 3056 / 19284** **Points : 2 (+2)**	

Ce que nous comptons faire d'ici une semaine :

- *réussir à utiliser le site web avec la VM*
- *créer un script qui achète périodiquement les produits (création d'un bash et utilisation d'un "curl" sur la page d'achat)*
- *lire et extraire les informations utiles des revues M.I.S.C prêtées*
- *créer une liste des vulnérabilités connues que l'on pourrait implémenter*

Réflexions d'amélioration :

- *Système de bonus lorsqu'une vulnérabilité est trouvée ? (vulnérabilité empêchant l'affichage d'un produit dans la boutique par exemple ?)*

Ancien drive :
https://drive.google.com/drive/folders/0B3LMkUOD2uVTZE5xODNaTWJleG8?usp=sharing

Drive actuel :
https://drive.google.com/drive/folders/0B3LMkUOD2uVTRDU3ZlpGSzRiQ2M?usp=sharing