Compte rendu n°04

20/04/2017

BOUTANT Thomas
SALMAN Alexandre

Encadrants
CHARMET Fabien
BLANC Grégory

Il y a deux semaines :

(la semaine dernière était une semaine de vacances et nous n'avions pas assez de matière pour faire un compte-rendu)

- *Création d'une backdoor*
- *Enumération de vulnérabilités connues pour Wordpress*
- *Installation de quelques plugins et découverte de WP Rollback*

Ce qui a été fait cette semaine :

1 - *Création d'un scoreboard*

Les fichiers :

- */Ressources/Scoreboard/script_table.html*
- */Ressources/Scoreboard/script_lampe.html*
- */Ressources/Scoreboard/script_canape.html*
- */Ressources/Scoreboard/scoreboard.py*
- */Ressources/Scoreboard/readme_SELENIUM.txt*

Avancement : 80%

Installation : suivre les consignes du readme_SELENIUM.txt

Remarques :

- *script_table.html est le script d'achat du produit "Table" que nous avions fait précédemment, auquel nous avons ajouté deux lignes : une pour stocker dans une variable le prix total d'achat, puis une pour l'afficher dans la console (avec un echo).*
- *Les deux autres scripts permettent d'acheter les deux autres produits restants, à savoir la lampe et le canapé. A noter que pour script_lampe.html nous avons implémenté une condition d'existence : si nous sommes connectés avec le compte "admin/faible", l'achat est moins rentable.*
- *Installation aussi d'un plugin pour Sélénium : FileLogging. Il permet de récupérer les résultats des commandes effectuées sur Sélénium dans un fichier texte. Ainsi, nous obtiendrons le prix de la commande dans notre fichier texte avec la commande "echo".*
- *scoreboard.py est un programme qui va récupérer tous les prix dans le fichier texte obtenu grâce à FileLogging, puis va afficher et actualiser le graphe du score (=somme des prix) en fonction du temps.*
- *Avec ces deux fichiers, chaque participant pourra voir son score. Il ne reste plus qu'à rassembler tous les scoreboards de chaque participant pour les comparer en temps réels, et à faire une appli web python pour afficher le tout.*

2 - Amélioration de la backdoor

Les fichiers :

- */Ressources/Backdoor/test_backdoor_serveur.py*
- */Ressources/Backdoor/test_backdoor_client.exe*
- */Ressources/Backdoor/test_backdoor_client.py*

Avancement : 100%

Remarques :

- *Création d'une nouvelle backdoor permettant de s'affranchir de l'adresse IP de l'attaquant. Comme pour la précédente, elle s'ouvre automatiquement à partir des crontab. En revanche, elle est à présent visible en scannant les ports de la VM, donc moins discrète, et elle requiert les droits d'administrateur pour s'exécuter, ce qui peut-être gênant. Elle ne requiert plus l'utilisation de paramiko, et un exécutable a été créé pour Windows.*
- *Elle utilise le port 443 du serveur Web*

3 - Création d'une vidéo de présentation d'une minute pour un autre projet Cassiopée
La vidéo : https://youtu.be/MjahLijhy_Q
Avancement : 100%
Remarque :

- *Une des équipes des projets Cassiopée a pour rôle de mettre en avant, valoriser ces projets. Pour cela, les deux étudiants de cette équipe ont demandé (sur Facebook) un peu avant les vacances une vidéo "de 30s à 1 min" pour présenter notre projet. D'où l'existence de cette vidéo, assez minimaliste dans son contenu.*

II - Autres

Formation/Résolution de challenges

Scores	Thomas	Alexandre
RootMe	**Points :** 465 **(+0)** **Challenges :** 40/251 **Place :** 5244/48696	**Points :** 240 **(+0)** **Challenges :** 23/251 **Place :** 9197/48696
NewbieContest	**Points :** 268 **(+0)** **Position :** : 3426 / 43594	**Points :** 108 **(+0)** **Position :** 8540 / 43482
HackThisSite	**391 Points**	
OverTheWire	**Bandit - level 12**	
W3Challs	**Position : 3056 / 19284** **Points : 2**	

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

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

Le scénario :
https://hackmd.io/OwNgLAHAzBwEwFoCMBOADAEwWMAzAxggIZGwICsARsAKZjCUazBJA===