Compte rendu n°05

27/04/2017

BOUTANT Thomas
SALMAN Alexandre

Encadrants
CHARMET Fabien
BLANC Grégory

La semaine dernière :

- *Création d'un scoreboard*
- *Amélioration de la backdoor*

Ce qui a été fait cette semaine :

1 - *Scoreboard - appli web*

Les fichiers :

- */Ressources/Scoreboard/ (pas présent actuellement car pas fini)*

Avancement : 90%

Remarques :

- L'appli web est opérationnelle, il reste à faire en sorte que le temps affiché sur le graphe concorde avec le temps de l'achat et non de l'actualisation

2 - Les deux backdoors

Les fichiers :

- */Ressources/Backdoor/**

Avancement : 90%

Remarques :

- *Il reste à implémenter le fait que la backdoor se lance au démarrage, avec des privilèges sudo, et le fait de convertir le script python en C pour pouvoir générer un exécutable, ce qui sera moins visible.*

3 - Des tentatives : openssh-server et switch Ethernet

Fichiers :

- */Tutoriels/Tutoriel OpenSSH (liens des deux tutoriels trouvés)*

Avancement : 20%

Remarque :

- **Openssh-server (Thomas)**
  - Ce qui a été fait :
    - sudo apt-get install openssh-server : fait
    - modification de quelques paramètres de /etc/ssh/sshd_config
    - création de ~/.ssh/authorized_keys avec les droits qu'il faut
    - génération de clefs et partage des clefs entre host et guest
  - Problème :
    - en faisant "ssh -vvv cassioressi@10.0.0.2 -p 22222" (j'ai choisi comme port 22222), il y a une connexion avec la VM, puisque j'arrive à voir la bannière de /etc/issue.net. Mais, ensuite : "Permission denied (publickey)".
- **Switch Ethernet**

4 - Analyse de checkout.js et du système des coupons

Fichiers :

- */Ressources/Scoreboard/script_coupon_unlimited.html*
- */Ressources/Scoreboard/script_canape_coupon.html*

Avancement : 40%

Remarques :

- dans /wp-content/plugins/woocommerce/assets/js/frontend/, j'ai regardé 2 fichiers : **checkout.js** et **cart.js**, sans résultat pour l'instant.
- dans /wp-content/plugins/woocommerce/includes/, j'ai modifié (mis des "//") **class-wp-coupon.wp** pour les fonctions testant la validité du coupon
  On passe maintenant le passage Cart → Checkout.
  Problème : dans Checkout, cliquer sur "Place Order" renvoie le message *"Coupon usage limit has been reached"*. Il faut donc sûrement modifié un autre fichier. Mais lequel ?...
- *script_coupon_unlimited.html* → permet de (re)-mettre le coupon de code "qwerty" en quantité infinie
- *script_canape_coupon.html* permet d'acheter un canapé avec une réduction (utilisation d'un coupon de réduction)

5 - Divers

Avancement : 100%

Remarques :

- Implémentation d'un compte sudoer sur la VM et d'un compte admin sur wordpress avec des mots de passe faibles.

Cette semaine :

- **Entretien téléphonique le 25/04/2017**
  Objectif : faire un bilan de ce qu'il reste à faire;
  Priorité donnée au bon fonctionnement de la connexion wifi entre participants

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===