Compte rendu n°06

04/05/2017

BOUTANT Thomas
SALMAN Alexandre

Encadrants
CHARMET Fabien
BLANC Grégory

La semaine dernière :

- *Scoreboard - appli web*
- *Les deux backdoors*
- *Des tentatives : openssh-server et switch Ethernet*
- *Analyse de checkout.js et du système des coupons*

Ce qui a été fait cette semaine :

1 - *Scoreboard - appli web*

Les fichiers :

- */Ressources/Scoreboard/serveur.py (le mettre dans le même dossier que scoreboard.py et log.txt)*

Avancement : 95%

Remarques :

- *TODO - Avoir sur un même graphe tous les scores des candidats.*
- *L'exe ne semble pas fonctionner pour une raison inconnue*

2 - Les deux backdoors

Les fichiers :

- */Ressources/Backdoor/**

Avancement : 90%

Remarques :

- *Il reste toujours 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.*
- *Je n'ai pas encore regardé en détail la nouvelle version envoyée par M. Nicomette, je le ferais dans le courant de la semaine prochaine.*

3 - Routeur Wifi : Pineapple Nano

Fichiers :

- */Tutoriels/Tutoriel Pineapple Nano*

Avancement : 60%

Remarque :

- *Il reste à tester la connection d'une dizaine d'appareils*
- *La connection était très lente, le fait d'avoir update la route semble avoir résolu le problème… (à re-tester)*
- *Il faut modifier dans les paramètres de WP (Settings -> General) l'URL pour que l'IP colle avec l'IP attribuée par le routeur. Cela devra être fait le jour J pour chaque participant.*

4 - Exploitation du système des coupons

Fichiers :

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

Avancement : 70%

Remarques :

- dans /wp-content/plugins/woocommerce/includes/ : modification de **class-wp-coupon.wp** : on peut ainsi utiliser un coupon à l'infini tant qu'il existe, et le script *script_coupon_limited.html* le re-crée/met à jour.

Cette semaine :

- *Peaufiner la configuration du routeur Wi-Fi*
- *Réunion le 10/05 à 17h45*
- *Regarder les vulnérabilités SSH et celles ajoutées par M. Nicomette*
- *Faire un snapshot de la machine en état stable*
- *Voir si on peut faire encore plus de dégâts dans* /wp-content/plugins/woocommerce/includes/ : modification du prix au dernier moment par exemple

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===