Compte rendu n°03

06/04/2017

BOUTANT Thomas
SALMAN Alexandre

Encadrants
CHARMET Fabien
BLANC Grégory

Il y a deux semaines :

(la semaine dernière a été dédiée au Challenge Projet d'Entreprendre)

- *Installation de LAMP sur la VM*
- *Utiliser le site wordpress sur la VM*
- *Création d'un script avec Sélénium pour acheter automatiquement les produits*

Ce qui a été fait cette semaine :

1 - *Création d'une backdoor*
Avancement : 95%
Remarque :

- *Fonctionnelle, mais possède plusieurs inconvénients. L'IP de l'attaquant doit figurer dans le client de la backdoor, sur la VM, ce qui implique de la modifier au dernier moment. Sous certaines circonstances détaillées dans le readme, le client peut s'arrêter avec un message d'erreur, ce qui est peu discret.*
- *La backdoor ne donne pas de privilèges administrateurs, mais l'attaque peut être réalisée sans, simplement en utilisant la commande shutdown*
- *La backdoor s'active automatiquement toutes les 15 minutes et reste ouverte pendant 2 minutes, rendant la détection plus difficile*
- *Un moyen de la détecter est par exemple de regarder la liste des processus (python 2.7 /etc/calendar.config semble louche)*

2 - Enumération de vulnérabilités connues
Fichier : ~/Idées, choses à retenir/Liste vulnérabilités
Avancement : 30% (on ne pourra pas toutes les lister)
Remarques :

- *Pour wordpress, LA référence : https://wpvulndb.com/*

3 - Installation de plugins et découverte de WP Rollback
Avancement : 40%
Remarques :

- *pour installer/uploader un plugin, un identifiant FTP est demandé. En utilisant http://www.techrepublic.com/blog/smb-technologist/how-to-create-an-ftp-server-on-an-ubuntu-1204-virtual-machine/, je n'en ai pas eu besoin. Une idée de vulnérabilité : uploader un plugin défaillant qui sera dans la VM sous forme .zip, ce qui donnera une nouvelle porte pour de futures attaques.*
- *WP Rollback permet de faire revenir les plugins dans leurs versions antérieures. Associé à la liste donnée sur ce site (https://wpvulndb.com/), il peut être très utile.*

Des événements :

- *04/04/2017 : Réunion pour faire l'état de l'avancée du projet et discuter du scénario*
- *05/04/2017 : Réunion montrant le fonctionnement de la backdoor et pour fournir une image de la VM*
- *06/04/2017 : point Challenge RESSI avec l'équipe RENAvisio*
  (cf ~/06/04/2017 - Entretien téléphonique n°2)

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===