FeedBack Attaque SERE H4413

ONO Lucas - RAQUIN Etienne (H4412)

Installation de Vagrant et des Machines Virtuelles :

* L’installation se passe sans soucis et est rapide
* Elle prend beaucoup de place sur le disque, prévoir de prévenir l’utilisateur
* Le chemin d’accès pour script.php se trouve home/scripts ce qui ne correspond pas au chemin d’accès dans les slides

Premières questions :

* On trouve que le shell courant en tapant cmd=whoami est www-data qui correspond à un shell utilisateur
* Pour le système d’opération on tape cmd=uname et on trouve linux

Configuration du Proxy

* La configuration s’est bien passée
* Envisager de mettre en valeur, sur les slides, les modifications à réaliser
* On upload notre script, cela permet bien de contourner la nouvelle sécurité de vérification du type MIME
* Spécifier d’arrêter le proxy, avant d’essayer d’accéder au script
* Corriger le chemin affiché : « restrict-uploads » est faux, il faut indiquer : « restricted-uploads »
* On accède au script uploadé

Création du PayLoad :

* On génère le code de notre PayLoad
* On créé notre programme python : trojan.py
* On upload notre trojan

Écoute de la connexion de la victime

* On utilise MetaSploit

Exécution du PayLoad :

* On lance notre trojan
* On accède à la machine de la victime
* On voit que l’on est connecté en tant que « www-data »

Augmentation de privilèges :

* Dans le fichier « exploit.c », on modifie la ligne « system(‘’/bin/sh’’) », en « system(‘’python trojan.py’’) »
* On compile ce programme
* On upload l’exécutable généré
* On n’arrive pas à exécuter notre programme, car notre programme n’a pas les droits d’exécution
* On fait donc un chmod
* On arrive à exécuter notre programme
* On voit que l’on est connecté en tant que « root »