Compte rendu projet YDAYS du 21 octobre

Lors de ce premier jour de Ydays, le chef de projet nous a bien expliqué ses attentes. J'ai donc décidé de m'attaquer à la compromission de machines virtuelles. La machine la plus abordable selon notre chef de projet est metasploitable 2, j'ai donc voulu m'adonner à celle-ci pour ce premier jour. Je me suis donc rendu sur le site root-me.fr qui propose de s'attaquer à celle-ci à distance, ce qui permet d'éviter de télécharger les machines directement sur son ordinateur.

Etant donné qu'il est interdit de faire fuiter les résultats sur internet, je vais juste expliquer comment j'ai fait pour attaquer la machine Metasploitable et non les commandes exactes utilisées. Je prendrais le risque de dévoiler les commandes utilisées uniquement au chef de projet et à sa demande.

Pour lancer la partie de capture the flag, il suffit de se rendre sur la partie dédiée aux capture the flag dans root-me et de se rendre dans une salle, de sélectionner une machine et de lancer la partie.

Début de la partie :

Une fois l'environnement virtuel démarré et kali linux lancé, il faut récupérer l'adresse de l'environne ment virtuel (exemple : `ctf01.root-me.org`).

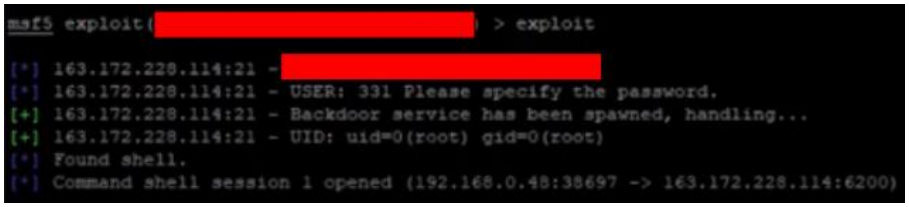
Il faut analyser par la suite les ports de la machine pour voir par lesquels on peut essayer de la pénétrer. J'ai personnellement utilisé nmap pour toutes mes attaques. Il faut spécifier certains arguments dans notre commande pour pouvoir affiner notre recherche.

En parallèle de l'analyse nmap, pour exploiter les failles, il faut utiliser Metasploit (d'où le nom de la machine).

Une fois l'analyse nmap terminée, on va utiliser Metasploit et chercher si une faille est disponible avec les ports ouverts listés par nmap. Un port retient mon attention, celui qui permet de gérer le flux de contrôle pour le transfert de fichiers.

Il faut utiliser le nom de version de cette faille sur Metasploit avec la commande ‘search nomDeLaFaille’. Par chance metasploit la connait, on va donc l’utiliser avec la commande ‘use nomDeLaFaille’. Il faut remplir un champ avant de lancer l’exploit qui est RHOSTS, qui correspond à l’adresse IP de la machine attaquée avec la commande ‘set RHOST adresseIP’.

Ceci fait, il faut lancer l'exploit en tapant `exploit`.



Ensuite, il faut exécuter la commande `shell` puis `ls` et le fichier `passwd` sera listé. Il faut donc l'ouvrir et le mot de passe se trouve à l'intérieur.

J’ai réussi 4 fois cette attaque et je pense l’essayer à nouveau avec une approche différente.

Résultats	Nom	Nombre de tentative(s)	Nombre de compromission(s)
✔	Metasploitable 2	12	4