Rapport intermédiaire SécuRT

Tout d’abord, nous avons décidé de travailler sur la catégorie “exploit” exclusivement pour le moment même si nous avons pensé à mêler d’autres catégories comme la stéganographie.

Au lieu de faire directement des défis root me ou autre, nous avons décidé de nous exercer sur des machines virtuelles.

Tout d’abord, nous avons installé une machine “metasploitable” (metasploitable 2 et 3) et une VM kali linux. En utilisant metasploit et nmap, nous avons scanné la machine afin de lister toutes les vulnérabilités et les points d’entrée possibles sur celle-ci, tout cela dans le but de nous donner des idées de défis en regardant comment les différentes vulnérabilités sur les applications se caractérisent.

Nous avons ensuite fait de même sur une VM Windows 7 et 8.

Voici les niveaux auxquels nous avons pensés :

### **Niveau facile : Récupérer un mot de passe via FTP**

Nous allons télécharger une version vulnérable de ProFTPD, qui est un serveur FTP open-source linux. L’attaquant devra utiliser Metasploit afin d’exploiter la backdoor présentes dans cette version de logiciel. Il devra par la suite exécuter des commandes sur le serveur afin de récupérer un fichier avec le mot passe pour valider l’épreuve. La CVE utilisée sera la CVE-2010-4221.

### **Niveau difficile : Exploitation de Windows avec EternalBlue (MS17-010).**

Sur une machine Windows server 2008, nous allons configurer la version 1 de SMB contenant la faille EternalBlue. L’attaquant devra utiliser Metasploit et nmap pour scanner les ports disponibles et trouver celui correspondant à SMB. Pour plus de difficultés, nous pensons changer le port de base de SMB vers la plage de ports privés. De plus, le mot de passe à trouver dans le niveau sera caché dans une des images d’un dossier du serveur. Cela mélange donc exploit et stéganographie.

Nous avons déjà commencé le niveau 1 mais, nous sommes seulement en train de configurer le service FTP.

Pour la répartition des tâches, nous travaillons en même temps car nous sommes plus efficaces avec cette méthode.

Entraînement effectué :

**Antonin**

Pour approfondir ma formation sur les exploits, j'ai travaillé sur une vulnérabilité connue : vsftpd 2.3.4 dans l’environnement Metasploitable 2.

Scan avec Nmap :

J'ai débuté par un scan de la machine Metasploitable avec **Nmap** pour identifier les services ouverts et qui pouvaient être vulnérables. Ce scan a révélé plusieurs services, dont le service **FTP** sur le port 21**.** Après avoir identifié la version du serveur FTP, j’ai effectué des recherches et trouvé que **vsftpd 2.3.4** contenait une **backdoor** connue, exploitable pour obtenir un accès au système.

Exploitation avec Metasploit :J’ai ensuite utilisé **Metasploit** pour exploiter cette faille. Voici les commande que j’ai utilisée pour lancer Metasploit et rechercher le module à utiliser :  
msfconsole

search vsftpd

Le module trouvé était exploit/unix/ftp/vsftpd\_234\_backdoor.

J’ai configuré ce module en indiquant l’adresse IP cible et le port (21) :

use exploit/unix/ftp/vsftpd\_234\_backdoor

set RHOSTS @IP

set RPORT 21

exploit

En lançant l’exploit, cela à ouvert une session avec les droits d’utilisateur non privilégiés..

**Julien**

Pour approfondir ma formation en exploitation de vulnérabilités, j'ai travaillé sur un point d’entrée de la machine **Metasploitable 2** : le service **Telnet**. Cette machine virtuelle comporte un service Telnet mal sécurisé, car il accepte un compte par défaut qui permet un accès à distance non autorisé.

J'ai commencé par scanner la machine Metasploitable avec **Nmap** pour identifier les services ouverts :  
Le scan a révélé que le port **23** était ouvert et que le service **Telnet** y était actif.

Après avoir identifié le port Telnet ouvert, j’ai recherché des informations spécifiques sur ce service dans Metasploitable 2. Il est connu que le compte par défaut msfadmin:msfadmin est souvent laissé activé dans cet environnement, permettant ainsi un accès au shell.

J’ai ensuite utilisé un client Telnet pour tenter de me connecter à la machine cible en utilisant ces identifiants par défaut :  
  
telnet @IP

Au prompt, j’ai entré :

* Nom d'utilisateur : msfadmin
* Mot de passe : msfadmin

La connexion a été établie, me donnant un accès au shell de la machine.

Une fois connecté, j’ai pu naviguer dans les fichiers du système de la machine Metasploitable et accéder à des informations système, ce qui m’a confirmé l'accès non autorisé.