TP1: Introduction

Exercice 1 : Questions

1. Citer 5 métiers de la cybersécurité.

2. Citer 3 états-nations en pointe dans le domaine du malware et citer les récentes attaques qui leur sont attribuées.

3. Quelle est la forme de malware la plus répandue actuellement, et pourquoi ? donner un exemple récent accompagné des chiffres clés correspondants.

4. Citer et expliquer brièvement quelques attaques sur des systèmes industriel, et chercher les impacts de ces attaques.

5. Donner un exemple concret de chaque type de vulnérabilité (vulnérabilité au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation d'un bien)

6. Chercher sur Internet une des vulnérabilités les plus exploitées par des attaquants.

7. Chercher une vulnérabilité sur BASH avec un score CVSS le plus élevé, puis expliquer la dangerosité de cette vulnérabilité et enfin expliquer comment ce score a été obtenu.

8. Une faille de sécurité sur OpenSSL est restée plus de 2 ans avant d'être découverte. Sans pour autant renier le modèle "open source" et la licence GPL, qu'est-ce que cette situation montre, en termes de niveau de sécurité, pour les logiciels open-source ? Quelles implications en entreprise ?

9. Qu'est-ce qu'une APT ? donner un exemple réel.

10. Argumenter pour ou contre l'utilisation d'un Gestionnaire de mot de passe, rechercher des exemples.

Exercice 2 : Demarche d'un attaquant

L'objectif de cet exercice est de comprendre la démarche d'un attaquant afin de s'introduire dans un système et faire une escalade de privilège. Pour cela nous avons besoin d'une machine virtuelle vulnérable. Nous allons choisir la VM *metasploitable* qui est un bon départ pour ce genre d'exercice.

1. Télécharger la VM Metasploitable (*https://sourceforge.net/projects/metasploitable/files/Metasploitable2/*)

Lancer cette machine. Vous pouvez constater que vous n'avez pas l'accès root à cette machine. L'objectif est de trouver une vulnérabilité qui nous permet d'avoir le droit root sans pour autant connaitre le mot de passe root !

2. Configurer la carte réseau en mode host-only. Lancer la machine.

3. En toute logique, vous n'allez pas scanner les quatre milliards d'adresse IP possibles pour trouver la bonne adresse IP de votre VM car ceci n'est ni performant ni légal. Comment faire alors pour trouver le bon préfixe réseau à scanner ? Donner un nom à cette étape.
4. Une fois le bon préfixe trouvé, utiliser un outil de scan réseau pour identifier l'adresse IP de votre VM. Quel est le type de scan utilisé ?
   Comment rendre le scan plus furtif ?
5. Quels sont les services lancés sur cette machine ? quels sont les versions exactes des services lancés ? qu'appelle-t-on cette étape ?
   D'après vous, comment fonctionne concrètement cette découverte ?
6. Chercher sur google une vulnérabilité sur le serveur FTP présent sur cette machine. Quelle est le type de cette vulnérabilité ?
   Exploiter cette vulnérabilité afin d'avoir un accès root à la VM.
7. Google est bien pour hacker, mais il y a mieux : les outils d'analyse de vulnérabilité. Installer un outil d'analyse de vulnérabilité de votre choix, ou utiliser simplement les outils sur Kali. Lancer une analyse sur votre VM.
   Donner deux autres vulnérabilités qui vous permettent d'avoir un accès distant à votre VM.
8. Exploiter une vulnérabilité peut être délicat. Heureusement il y a l'outil Metasploit. Cet outil permet d'automatiser l'exploitation des vulnérabilités. Chercher dans Metasploit un ***exploit*** d'une des vulnérabilités que vous avez trouvées sur la VM metasploitable (une vulnérabilité sur Bash ou SSL par exemple), puis lancer automatiquement cet exploit.