Récapitulatif D1

Généralités de hacking

Il est toujours possible d'attaquer sur deux fronts : technique et/ou social.

Il faut différencier une attaque ciblée sur une personne, presque impossible à éviter lorsqu'elle est bien exécutée, d'une attaque sur un système entier.

Lorsqu'une seule personne est ciblée, certaines techniques deviennent accessibles pour avoir accès à une donnée :

- Chantage
- Vol
- Installation de keylogger
- Enregistrement vidéo de la frappe au clavier
- Phishing bien pensé
- Soirée alcoolisée
- …

En revanche, pour un système entier, il faut se reposer soit sur l'exploitation des privilèges d'un employé de la société mainteneuse, soit sur une faille technique.

Les failles techniques les plus connues sont aussi les plus courantes. On en retrouve la liste dans l'OWASP 10 ou le SANS top 25.

Faille XSS

Une faille XSS (Cross-Site Scripting) est le fait d'insérer un script (le plus souvent Javascript) dans une page qui n'est pas pensée pour.

Cette faille est rendue exploitable par le fait que le site ne vérifie pas les entrées utilisateur avant de les afficher.

Il y a deux types de failles XSS : L'XSS réfléchie et l'XSS permanente.

Quand elle est simplement réfléchie, la page web ne fait qu'afficher une entrée utilisateur pour la personne qui a fait l'injection. Cela est souvent anodin, mais est souvent en fait associé à une faille permanente. À première vue, ce n'est pas un problème grave parce que l'utilisateur peut seulement injecter du code dans ses propres pages. Cependant, avec un peu d'ingénierie sociale, un attaquant peut convaincre un utilisateur de suivre une URL piégée qui injecte du code dans la page de résultat, ce qui donne à l'attaquant tout contrôle sur le contenu de cette page. L'ingénierie sociale étant requise pour l'exploitation de ce type de faille (et du précédent), beaucoup de programmeurs ont considéré que ces trous n'étaient pas très importants.

On parle d'une XSS permanente quand celle-ci est stockée sur le site web, comme un message de forum est stocké sur celui-ci. La faille XSS est donc utilisée chez tous les clients visitant la page.

Il est possible de s'en protéger soit en utilisant des fonctions telles que htmlspecialchars() ou htmlentities(), ou en utilisant un framework web templaté digne de ce nom.

S'entrainer à exploiter des failles XSS : http://xss-game.appspot.com/

Dans tous les cas, exploiter ces failles sans autorisation préalable est hautement illégal et relève du tribunal pénal. Les peines sont lourdes et la justice n'est pas tendre.

Les seuls hackers qui s'en sortent vendent leurs services aux entreprises qu'ils hackent ou font des travaux de recherche.

Challenges newbie contest

Client side

Il faut ici manipuler le browser pour trouver des informations. Regarder le code source reçu, le modifier en l'inspectant, etc…

Crackme

Chaque épreuve est un binaire exécutable à analyser. On conseillera un afficheur d'hexadécimal ou un désassembleur pour faire ces exercices.

Lien utile : https://zestedesavoir.com/articles/97/introduction-a-la-retroingenierie-de-binaires/

Cryptographie

Peu de code ici. Il faut se renseigner sur les techniques de chiffrement existantes et sur comment les casser.

Lien utile : https://zestedesavoir.com/articles/54/cest-toute-une-histoire-la-cryptographie-partie-1-3/

Hacking

Ici encore il faut manipuler le browser. Changer les URL, changer le contenu des cookies, la requête http, tout est bon pour passer outre un filtre.

Logique

Pas de code du tout ici. Seulement des suites logiques et/ou mathématiques. Les challenges se ressemblent peu.

Programmation

Il faut créer un programme qui fait des appels réseau et agit en fonction. La difficulté au début est d'arriver à faire une requête correctement, en arrivant à passer le cookie de session. Vu en cours, rapprochez-vous de vos camarades si vous ne voyez pas comment faire.

Stéganographie

L'art de cacher une information dans une autre. Ici le but n'est pas, comme en cryptographie, de chiffrer un message pour le rendre illisible à quiconque n'aurait pas un mot de passe, ici le fait que l'on passe un message est caché. Texte en blanc sur blanc, caché dans les pixels d'une image, …

Stéganographie & Forensics

Ces catégories seront couvertes en D4.