Projet de synthèse

Le projet de synthèse du parcours SSI comporte deux étapes. La première étape consiste à développer et à déployer un site Web dont certaines informations manipulées sont classées comme sensibles. C'est pourquoi, si le déploiement doit naturellement être particulièrement sécurisé, le développement doit également faire l'objet de la plus grande attention. La deuxième étape consiste à jouer simultanément deux rôles : celui de l'attaquant, et celui du défenseur. Dans le rôle de l'attaquant, il s'agit de déployer toute l'inventivité et l'opiniâtreté nécessaires à la réalisation d'exploits sur les sites Web des autres groupes. Mais parallèlement, votre propre site Web fait naturellement l'objet d'attaques qu'il faut surveiller. Et si l'une d'entre elle réussit, il faut réagir de la meilleure manière. Dans les paragraphes suivants, nous décrivons les spécifications du site Web, ainsi que les « règles du jeu » que doivent respecter attaquants et défenseurs.

Etape 1 : site Web

Wikimedia est un logiciel très connu aujourd'hui, sur lequel est naturellement bâtie l'encyclopédie Wikipedia, mais énormément d'autres wikis. Même si c'est un outil très populaire, la création, la rédaction, l'historisation d'un article peuvent paraître un peu ardues pour le commun des internautes (demandez à votre grand-mère de créer un article!). Nous vous demandons de construire une application Web pour faciliter cette gestion des articles.

Bien sûr, vous éviterez de polluer Wikipédia en installant votre propre wiki. Il faudra évidemment l'installer pour garantir sa sécurité et sa disponibilité au mieux. Il faudra éviter qu'il soit défiguré (defacing), et que le contenu des articles soit de bonne tenue (pas de vocabulaire "inapproprié").

Votre application Web sera développée indépendamment. Les fonctionnalités attendues sont plus précisément :

- S'authentifier sur l'appli, ou s'inscrire si c'est la première utilisation. Hormis cette phase de login qui peut être en https, **tout le reste de l'application doit être en http !**
- La rédaction d'un nouvel article avec une ergonomie basique mais très simple d'utilisation (c'est le but de l'appli!);
- L'affichage de ses articles (la liste complète de tous les articles et l'affichage complet d'un article);
- La synchronisation d'un article, c'est-à-dire l'envoi sur le wiki de l'article sélectionné dans l'appli web. Il n'y a pas de problème d'antériorité si l'article vient d'être créé dans l'appli web. Mais lorsqu'il s'agit d'une version chargée depuis le wiki (voir ci-dessous), il se peut qu'il y ait un conflit de version (comme dans un système de versionnage). Vous proposerez une solution simple à ce problème;
- Le chargement de la dernière version d'un article depuis le wiki, c'est-à-dire qu'un article créé et synchronisé à l'instant t, va évoluer au gré des modifications des internautes sur le wiki. Le chargement consiste à récupérer la version de l'article à l'instant t', laquelle est bien sûr liée à la version de l'instant t;
- Modifier la dernière version d'un article.

Vous avez entière liberté dans le choix des OS, SGBD, langages de programmation ou CMS. Mais, dans tous les cas, vous devrez obligatoirement laisser au moins une vulnérabilité (mais une vulnérabilité complexe à exploiter, quand même), afin que les autres groupes puissent avoir l'opportunité de réaliser au moins un exploit sur votre site.

Etape 2 : attaques/défenses

L'objectif de cette étape correspond clairement à son intitulé : attaquer le site des autres groupes, et défendre le sien. Mais, pour que cette étape se déroule correctement, dans le bon esprit, quelques règles doivent être respectées.

1. Pas d'attaque physique : même si toutes les machines sont situées dans un local indépendant et quasi inaccessible, toute manipulation directe d'une machine d'un autre groupe est proscrite (pas de keylogger, de clé USB avec ophcrack, etc.)
2. Le site doit être accessible en permanence, y compris quand vous n'êtes pas dans la salle (n'allumer la machine que quelques minutes par jour est déloyal)

3. Pas de trahison, ni de corruption ! (on ne dit rien à son copain ou sa copine de l'autre groupe… On ne se laisse pas acheter non plus avec des boissons ou des barres chocolatées,…). Vous êtes membre d'un groupe, et devez respecter la confidentialité qui entoure nécessairement le travail de votre groupe, ainsi que la loyauté envers les autres membres du groupe.

Calendrier

Le projet de synthèse se déroule tout au long de l'année et nécessite tout le temps que vous pourrez y consacrer. Cependant, tous les jeudis après-midi sont bloqués dans l'emploi du temps. Ces créneaux serviront, entre autre, à présenter régulièrement l'avancée de vos travaux pendant l'étape 1, et les compte-rendu de vos attaques/défenses pendant l'étape 2. Certaines dates sont d'ores et déjà bloquées pour présenter certains livrables :

3 octobre 2013 : présentation du projet (par les encadrants…)

24 octobre 2013 : présentation du cahier des charges fonctionnel (maquette des écrans, navigation, contraintes fonctionnelles, etc.). Cette présentation est générale (devant toute la promo). Une planification du projet doit être présentée, ainsi que les risques. Le cahier des charges fonctionnel est un document rédigé qui devra être remis avant la présentation.

14 novembre 2013 : présentation du cahier des charges technique (choix des environnements, des solutions techniques, etc.). Cette présentation se fera par groupe. Le cahier des charges technique est un document rédigé qui devra être remis avant la présentation.

19 décembre 2013 : démonstration du site en production. Cette présentation est générale.

16 janvier 2014 : présentation de la démarche d'attaque et des outils. Cette présentation se fera par groupe.

20 mars 2014 : bilan général des attaques/défenses. Un rapport rédigé, remis avant la présentation, devra consigner l'ensemble des attaques entreprises (y compris celles qui n'ont pas abouties) avec leur analyse. De même, les réactions aux attaques subies devront être décrites.

A chaque présentation, vous devrez présenter le planning à jour, en justifiant éventuellement les retards. Vous devez également réévaluer les risques (les risques maîtrisés, et ceux qui apparaissent).

Notation

Dès qu'une attaque a été réussie, le groupe attaquant doit réaliser un document synthétique expliquant le principe de l'attaque, les outils utilisés et la preuve du succès de l'attaque. Vous communiquerez ce document par mail aux encadrants (Francine et moi). Lorsque nous aurons pris connaissance de ce document, nous enverrons un accusé de réception et vous pourrez révéler les information au groupe attaqué. Le groupe attaqué rédigera à son tour un rapport d'incident dans lequel l'analyse de l'incident est donnée, ainsi que les actions menées pour éviter qu'elle ne se reproduise.

Dès qu'une attaque a été bloquée (même si elle n'a pas réussi), le groupe attaqué procédera de la même manière en rédigeant un rapport de tentative d'attaque dans lequel figureront les preuves de l'attaque et l'analyse du comportement de votre système (pour notre information), et éventuellement des actions que vous avez entreprises face à cette tentative.

Essayez de formaliser ces documents dans un modèle structuré avec des noms, des numéros (Rapport d'attaque n°x, ...) et une forme propre (pas des quelques lignes en vrac avec une copie d'écran).

La note du projet de synthèse est composée de plusieurs critères d'évaluation :

- Qualité du développement
- Qualité de la démarche de sécurisation
- Qualité des présentations
- Qualité des rapports
- Qualité des attaques
- Qualité des réactions