Projet de synthèse

Etape 1 : audit de code et déploiement

Vous êtes l'équipe sécurité d'une grande entreprise. Un service de cette entreprise a acheté une application web à une société tierce (une société de service par exemple). Cette application est un site Web d'achat d'articles en ligne. En tant que responsable de la sécurité, vous devez vous assurer que cette application est conforme à votre politique de sécurité. C'est pourquoi, si le déploiement doit naturellement être particulièrement sécurisé, la qualité du code doit être préalablement méticuleusement évaluée (robustesse, sécurité, architecture...). En fonction de cette analyse, vous devrez définir l'environnement sécurisé sur lequel vous déploierez cette application. Vous pourrez même, selon vos découvertes, modifier le site (mais pas le réécrire naturellement).

Pour le déploiement et la mise en production, il vous est demandé d'installer et de configurer une machine avec un serveur web, avec tous les services nécessaires. Il vous faudra notamment un accès pour configurer la machine à distance (ssh), un accès pour mettre les pages web à jour (ftp), un accès pour modifier la base de données (ex. mysql) et enfin un accès web. Le système d'exploitation et les différents outils ne sont pas imposés mais vous devez justifier vos choix.

Ce système devra être protégé par un firewall. Les règles du firewall devront changer au fur et à mesure des détections réalisées par ELK (bien sûr ceci doit se faire de façon automatique). Dans un premier temps, nous vous demandons de ne pas installer de WAF pour laisser plus d'opportunités d'attaques. A la fin du projet, vous aurez à activer le WAF de votre choix et chaque groupe devra répéter ses attaques et constater celles qui réussissent et celles bloquées. En revanche dès le début de votre projet, vous devrez installer le SIEM ELK. Ce système devra vous avertir si une tentative d'intrusion est en cours (qu'elle soit un échec ou une réussite).

Elaboration d'un CTF

Enfin, on vous demande de choisir, parmi les outils précités (l'application, le serveur http, le serveur de bases de données, ou autre), une faille dont vous expliquerez le fonctionnement, de faire une preuve de concept et de configurer votre site de façon que cette vulnérabilité reste présente une fois votre site mis en ligne. Mais surtout, cette vulnérabilité devra faire l'objet d'un CTF. C'est-à-dire que la découverte de cette faille fera l'objet d'un jeu de piste constitué d'une suite d'indices délibérément éparpillés dans les différents composants de votre projet.

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 physique, de clé USB avec ophcrack, etc.). Si, dans un autre groupe, une session est restée ouverte par étourderie, n'en profitez pas ! (si vous prenez une photo et exercez un chantage pour avoir une tournée de croissants, nous n'y voyons aucun inconvénient)
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, etc.). 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.

Mise en péril réseau

Vous devez créer des applications permettant de réaliser les tâches suivantes :

- Définir la « signature » réseau du serveur en récoltant les informations suivantes
  - Version du système d'exploitation,
  - Version de tous les services installés sur le serveur.
- Trouver un moyen pour « casser » les mots de passes suivants :
  - Administration à distance
  - Mise à jour des pages web
  - Et des autres services installés si besoin.
- Tout faire pour saturer le serveur (envoi de paquets) sans se faire repérer.
- Prendre la place du serveur sur le réseau (usurpation d'identité)
  - En profiter pour retenir les logins des utilisateurs, pour détourner les liaisons d'administration et retenir les mots de passe des administrateurs du site.

Défacement des sites

- S'arranger pour afficher un texte sur les pages web du site. Ce texte prouvera que vous avez modifié le site sans en être l'administrateur officiel.
- S'arranger pour que le site officiel redirige vers une autre page.
- S'arranger pour que le site exécute un code non autorisé.
- Forcer le site à afficher une page qui ne devrait pas s'afficher en temps normal (comme par exemple la liste d'un répertoire).

Détournement d'informations

Créer des outils permettant de faire les opérations suivantes :

- Récupérer le site pour en faire un double. Le double servira à piéger les utilisateurs.
- Récupérer les informations des utilisateurs
- Récupérer les comptes administrateurs.

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 mardis après-midi sont bloqués dans l'emploi du temps. Ces créneaux serviront, entre autres, à présenter régulièrement l'avancée de vos travaux. Certaines dates sont d'ores et déjà bloquées pour présenter certains livrables :

17 septembre 2021 - 11h00 : présentation du projet

4 novembre 2021 - 9h00 : présentation par groupe du code revu et corrigé, déployé et testé en local

17 novembre 2021 - 13h30 : présentation par groupe de l'architecture de sécurité et présentation du CTF et maquettage de l'infrastructure (Avec Yvon BOUTRY)

15 décembre 2021 - 13h30 : présentation globale des sites en production, et du SIEM. Si besoin résolution des problèmes liés aux accès distants

12 janvier 2022 - 9h00 : présentation globale des défacements de sites + Dénis de service et signatures collectées

26 janvier 2022 - 9h00 : présentation globale des spoofing

9 février 2022 - 9h00 : présentation globale des cassages des mots de passe

23 février 2022 - 13h30 : présentation globale des CTF

9 mars 2022 - 13h30 : présentation globale du fonctionnement du projet avec WAF

23 mars 2022 - 13h30 : présentation globale de tout le projet

D'autres créneaux seront susceptibles d'être programmés en fonction des circonstances.