TP Sécurité informatique

Pour la réalisation de ces travaux pratiques, vous disposez d'une machine pendant 4 semaines sur laquelle vous pourrez travailler pendant les heures de TP en présence d'un enseignant et en dehors sur des créneaux laissés libre par votre emploi du temps. Afin de profiter au mieux des travaux pratiques, il est conseillé d'effectuer les tâches fastidieuses (téléchargement et compilation de logiciels) en dehors des séances. Un certain nombre de travaux, décrits ci-dessous vous sont demandés ; il s'agit avant tout d'une orientation de travail. En fonction de vos thèmes d'intérêts, d'autres aspects peuvent être abordés et mis en œuvre. A l'issu des 4 semaines, un rapport vous sera demandé résumant le travail effectué, les difficultés rencontrées, les mesures de sécurité prises sur la machine dont vous aviez la responsabilité, les outils mis en œuvre en précisant leur fonctionnalité et ce qu'ils vous ont permis de faire, les fichiers de configuration pertinents ainsi que les éventuelles vulnérabilités découvertes ou recommandations sur la machine cible de test. **Ce rapport est à rendre impérativement au plus tard une semaine après la fin de vos séances de travaux pratiques.**

Travail à réaliser :

1) Installation d'une distribution Linux: une distribution Mandrake 10 est mis à disposition mais vous pouvez installer la distribution de votre choix. N'oubliez pas d'inclure les packages de développement, les documentations et de tester la configuration de la carte graphique. Les paramètres réseaux sont définis sur l'étiquette appliquée sur les machines.

2) Sécurisation des machines après l'installation (détection et fermeture des éventuels services inutiles, test des droits d'écriture sur votre disque, …).

3) Installation des services de base :
   - serveur sshd : http://www.openssh.org http://www.openssl.org
   (installer le serveur *sshd* comme un service avec le démon *xinetd* afin que le service soit actif après chaque redémarrage de la machine ; attention à la compilation du serveur sshd: lors du configure, il faut spécifier que les mots de passe seront cryptés avec l'algorithme md5 et que le démon sshd sera lancé par xinetd).
   - serveur www : http://www.apache.org
   Compiler le serveur avec l'option ssl afin d'offrir un service http et https (la génération de certificats est explicitée en annexe). Un fichier de démarrage sera créé pour que le serveur www soit actif après chaque redémarrage de la machine.
   …

4) Installation et prise en main d'outils de sécurisation :

   a. sniffers (tcpdump,Ethereal, …)

Quelques exemples de tests : détecter toutes les demandes de connexion sur votre machine, détecter les trames pour lesquelles les bits non utilisés des flags dans l'entête tcp sont positionnés, …

b. scanners :
   nmap : tester les différentes options possibles
   nessus : tester quelques machines et analyser les résultats
   ….

c. installation d'un nids : snort pour intercepter les activités douteuses (scans, …). Définir des règles intéressantes et automatiser la mise en forme des résultats au format html.

d. Filtrage des données sous linux (iptables) : limiter l'accès de certains services sur votre machine, …

e. …

5) Procéder à des scénarios attaques/défenses : scanner la machine d'un autre binôme sans vous faire remarquer et détecter toute tentative de scan et/ou intrusion sur votre machine.

6) Un fichier de log réalisé sur un « honeypot » est disponible à l'adresse *http://www.ducrot.org/tpsecurite/snort.log.gz*. Copier ce fichier et analysez- le avec les outils installés (tcpdump, ethereal, snort) et essayez de répondre aux questions suivantes :

   1. Quelle est l'adresse IP de destination et celle de l'attaquant ?
   2. Quel outil de scan a été utilisé pour analyser l'honeypot ?
   3. Pouvez-vous identifier quels types de scans ont été mis en œuvre pour tester l'honeypot ?
   4. Quels ports ont été trouvés ouverts sur l'honeypot ?
   5. Quel était le système d'exploitation de l'attaquant

7) Vous trouverez à l'adresse *http://www.ducrot.org/tpsecurite/serverbuf.c* le code source d'un petit logiciel serveur. Ce programme comporte t'il une vulnérabilité ? Dans l'affirmative essayez d'écrire le code correspondant permettant d'exploiter la vulnérabilité.

8) Faites une analyse détaillée sur la sécurité de la machine cible.ecole.ensicaen.fr

Annexe: Configuration d'un serveur apache https

1) Le serveur apache doit avoir été configuré avec l'option - - enable-ssl

2) Le package *openssl* doit être installé

3) Génération d'un certificat:
   a. **openssl genrsa –des3 –out server.key 1024**
      i. Le fichier server.key contient la clé privée
      ii. Il ne faut pas oublier la phrase de génération
   b. **openssl req –new –key server.key –out server.csr**
      i. Cela génère le certificat qu'il faut maintenant faire signer par un tiers de confiance.
      ii. Pour sauter cette étape, nous allons devenir notre propre tiers de confiance pour signer notre certificat
   c. **openssl genrsa –des3 –out ca.key 1024**
      i. Génération de la clé privée du tiers de confiance
   d. **openssl req –new –x509 –days 365 –key ca.key –out ca.crt**
      i. Création d'un certificat autosigné valide de 365 jours
   e. **sign.sh server.csr**
      i. Signature du certificat par le tiers de confiance grâce au script *sign.sh* présent dans le package *mod_ssl*, répertoire *pkg.contrib*. Ce package doit être téléchargé à partir du site *http://www.apache.org*.

4) Placé les certificats (*server.key* et les fichiers *.csr*) dans les bons répertoires d'apache (se référer au fichier *ssl.conf* pour les déterminer).

5) Retirer la phrase de génération au lancement du serveur apache:

   a. **cp server.key server.key.org**
   b. **openssl rsa –in server.key.org –out server.key**

6) Supprimer les droits de lecture sur les fichiers .key:
   a. **chmod 400 server.key server.key.org**

7) Lancer le serveur apache:
   a. **/usr/local/apache2/bin/apachectl startssl**