ÉCOLE
POLYTECHNIQUE
MONTRÉAL

INF4420A – Sécurité Informatique

Travail Pratique 2

Automne 2019

Sommaire

Directives

Tous les travaux devront être remis avant 23h55 le jour de la remise sur le site Moodle du cours. À moins que cela ne soit explicitement demandé dans le sujet, vous ne devez remettre qu'un fichier PDF nommé selon le format *TPX-matricule1-matricule2.pdf*. Vous pouvez inclure des annexes dans votre rapport si vous jugez que cela améliore la lisibilité (code source, …)

- Voir la date de remise du rapport de ce laboratoire dans le plan du cours.
- Le travail devra être fait par équipe de deux. Toute exception (travail individuel, équipe de trois) devra être approuvée au préalable par le professeur.
- L'orthographe et la forme seront prises en compte pour chaque question.
- Indiquez toutes vos sources d'information, qu'elles soient humaines ou documentaires.

NOTE : POUR TOUTES LES QUESTIONS, VOUS DEVEZ MONTRER COMMENT VOUS AVEZ OBTENU LES RÉPONSES, INCLUANT DANS VOTRE RAPPORT LES CAPTURES D'ÉCRAN MONTRANT LES COMMANDES UTILISÉES ET LEUR SORTIE.

Question 1 - Accès physique = *Game Over* [/2.5]

Scénario

Vous êtes un pirate informatique et vous avez réussi à pénétrer dans un local de Omnisoft, une compagnie lavalloise qui se spécialise dans le domaine du multimédia interactif. Ceci est une prise de taille, car si vous mettez la main sur le code source de leur tout dernier jeu, vous pourriez gagner gros en vendant des copies pirates avant la date de lancement. Le local contient deux machines sans aucune protection physique.

Dans cet exercice vous allez voir certaines techniques permettant d'obtenir les droits administrateur sur une machine à laquelle vous avez accès physiquement. Les machines virtuelles **LocalOwnLinux** et **LocalOwnWin** se trouvent dans le répertoire `/home/INF4420a/TP2`.

Machine LocalOwnLinux

Phase de reconnaissance

1. Démarrer la machine virtuelle (VM) et essayer de vous connecter à une session. Que constatez-vous ?
2. Redémarrez la VM et au démarrage appuyez sur `F2` pour rentrer dans le BIOS. Que se passe-t-il ?
3. Appuyez sur `Echap` pour continuer le boot de la machine. A l'écran de Grub (fond violet), appuyer sur une touche quelconque (sauf `Entrée`). Cet écran présente les différentes options de boot pour la machine, dans notre cas il n'y a qu'une seule ligne correspond au système Gentoo Linux. Habituellement il est possible d'éditer la ligne de commande correspondante en appuyant sur la touche `e`.
4. Est-ce possible dans notre cas ? Sinon, pourquoi ?

Réalisation de l'attaque

1. La configuration du BIOS est conservée lorsque l'ordinateur est éteint grâce à une pile présente sur la carte mère. Si la pile est retirée pendant quelques secondes, le BIOS est réinitialisé et donc les mots de passe sont supprimés. (NB : il est aussi possible de le faire grâce à un jumper présent sur la plupart des cartes mères…). L'équivalent pour une VM est la suppression du fichier *.nvram dans le répertoire de la VM (de votre linked clone).

   Supprimez ce fichier et entrez dans le BIOS de la machine. Dans le menu `Boot` faites passer le lecteur CD-ROM au-dessus du disque dur dans la séquence de boot. Appuyez sur `F10` pour quitter et sauvegarder les changements.

2. Insérez un livecd de Backtrack dans le lecteur CD : dans vmware, dans le menu VM → Settings, dans les paramètres du lecteur CD/DVD, cochez « Connected » et « Connectat power on » puis sélectionnez « Use ISO image » et indiquer le chemin vers le fichier `BT5R3-KDE-32.iso` qui se trouve dans le même dossier que les VMs.

3. Redémarrez la VM. Lorsque « boot : » s'affiche appuyez sur `Entrée`, puis encore une fois pour sélectionner « BackTrackText ».

4. A ce stade, de nombreuses options sont possibles pour obtenir l'accès root sur la machine :

   - utiliser John the Ripper pour trouver les mots de passe.
   - modifier le fichier shadow directement.
   - faire un « chroot » et changer le mot de passe root avec la commande `password`.

   Cependant, nous allons juste supprimer le mot de passe de Grub afin de vous montrer ce qu'on peut faire si Grub n'est pas protégé.

   Montez la partition de boot en entrant les commandes suivantes :

   ```
   mkdir /mnt/tmp
   mount /dev/sda1 /mnt/tmp
   ```

   Ouvrez le fichier grub/grub.conf qui est sur cette partition. Supprimez la ligne commençant par `password`. Redémarrez la VM sans booter sur le livecd.

5. A l'écran de grub appuyez sur `e` pour éditer la commande. Sélectionnez la ligne commençant par `kernel` et appuyer sur `e`. Ajoutez `init=/bin/bash` à la fin de la ligne. Appuyez sur `Entrée` puis `b`.

6. Vous arrivez sur une invite de commande root (Appuyez une fois sur `Entrée` si nécessaire). Utilisez la commande suivante pour remonter la partition root avec tous les droits :

   ```
   mount -o remount,rw /
   ```

   Puis utilisez la commande `passwd` pour changer le mot de passe root.

7. Redémarrer la machine et ouvrez une session root.

Machine LocalOwnWin

1. Refaites les mêmes manipulations que pour LocalOwnLinux afin de booter sur le livecd de BackTrack.
2. À l'invite de commande lancer l'interface graphique avec la commande `startx`. Répondez `Yes` si une fenêtre s'ouvre concernant la carte son.
3. (Optionnel) Vous pouvez augmenter la résolution en cliquant sur l'icône de BackTrack en bas à gauche puis sur `Settings → System Settings`, puis `Display Monitor`.
4. Cliquer sur l'icône de Dolphin puis sur le disque dur dans la partie gauche de la fenêtre. Cela a pour effet de monter la partition automatiquement. Fermer la fenêtre.
5. Cliquez sur l'icône de BackTrack en bas à gauche puis
   `BackTrack → PrivilegeEscalation → PasswordAttacks → Offline Attacks → chntpw`.
6. Entrer la commande :
   `./chntpw /media/disk/Windows/System32/config/SAM –i`
7. Expliquez à quoi sert ce fichier SAM.
8. Utilisez le menu interactif de chntpw pour effacer le mot de passe de l'utilisateur « admin » (qui est dans le groupe administrateur).
9. Redémarrez la VM sous Windows et ouvrez la session de l'utilisateur « admin ».

Question 2 - Exploitation des vulnérabilités [/2.5]

Dans cet exercice, vous aurez la possibilité de vous familiariser avec le Framework Metasploit d'exploitation de vulnérabilité des logiciels et des systèmes d'exploitation.

Démarrez les machines virtuelles **Quebec**, **Ottawa** et **Sherbrook.**

Phase de reconnaissance

1. Comme vous l'avez fait pour la question 1, démarrez le livecd de BackTrack à partir de **LocalOwnLinux** ou **LocalOwnWin** et lancez l'interface graphique.
2. Les machines que vous voulez attaquer sont dans la plage d'adresse 195.34.45.0/24. BackTrack prendra automatiquement une adresse privée dans le 192.168.0.0/16. Normalement, pour que deux réseaux ayant un sous-réseau différent communiquent ensemble, nous devons passer par un routeur. À défaut d'avoir un routeur, nous allons tricher et changer l'adresse IP de BackTrack pour une adresse IP publique dans le même sous-réseau que les machines que nous désirons infecter. Assignez donc l'adresse IP statique suivante dans BackTrack : 195.34.45.208.
   Entrez la commande suivante pour changer l'adresse IP :
   `ifconfig eth0 195.34.45.208`
3. Avec la commande `ping`, testez que vous pouvez effectivement communiquer avec les machines dans le réseau (testez avec 195.34.45.7).
4. Expliquez en quoi la modification effectuée en 2. ne serait pas nécessaire si vous étiez dans votre sous-sol chez votre mère en train de vouloir hacker les serveurs Québec, Ottawa et Sherbrooke ?
5. Cliquez sur l'icône de BackTrack en bas à gauche puis
   `BackTrack → Exploitation Tools → Network Exploitation Tools → Metasploit Framework → armitage`.
6. Cliquez sur « Connect » puis répondre « Yes » pour démarrer le serveur Metasploit RPC.
7. Lorsqu'une fenêtre vous demande l'adresse IP de la machine attaquante ouvrez un terminal et tapez `ifconfig` pour la connaître. Entrez-la dans Metasploit.
8. Scannez le réseau pour trouver des machines cibles :
   `Hosts → Nmap Scan → Quick Scan (OS detect)`
   Indiquer le sous-réseau de la machine attaquante.
9. Quel est le résultat ? Expliquer. (Indice : à quoi sert Nmap ?)
10. Rechercher les exploits applicables aux machines cibles :
    `Attacks → FindAttacks`
    Maintenant si vous faites un clic-droit sur une des cibles vous avez accès à un menu « Attack ».

Exploitation de failles de sécurité connues

1. Comme vous le savez, le système d'exploitation Windows 2000 est relativement vieux. Plusieurs failles de sécurité ont été découvertes dans ce système d'exploitation. Dans le cas du système installé sur les machines de ce TP, nous avons remarqué que, sur une d'elle, le service **rpcdcom** écoute par défaut sur le port 135. Quelle est cette machine ?
2. Utilisez l'exploit ms03_026_dcom sur cette machine. Cet exploit profite d'une faille de sécurité dans le service **rpcdcom**. Quel est le résultat ? Quelles sont les nouvelles possibilités avec cette machine cible ?
3. Grâce à l'exploit précédent ajoutez un utilisateur "h4x0r" avec le mot de passe "toto" sur la machine cible et créez un répertoire "owned" sur le bureau de l'utilisateur inf44201 (C:\Documents and Settings\inf44201\Bureau). Vous devez donner un listing des commandes que vous avez utilisées, une explication de votre démarche et une preuve des résultats (captures d'écran).
4. Une autre faille a aussi été détectée sur la même machine. Cette faille concerne le service WarFTPD et elle exploite le débordement de tampon dans la commande PASS de la version 1.65 de cette application. Comme vous le savez, WarFTPD est un serveur FTP utilisant par défaut le port 21. Trouvez cet exploit et utilisez-le afin de créer un répertoire sur la machine cible. Pour qu'il s'affiche il faut changer le « Exploit Rank » à « Poor » dans le menu « Armitage » et relancer la recherche des exploits.

   Donnez le nom du module utilisé ainsi que les différentes commandes que vous avez exploitées, une explication de votre démarche et une preuve des résultats.
5. Trouver un exploit utilisable sur l'autre machine Windows et créer un répertoire « owned2 » sur le bureau de l'utilisateur inf44201. Vous devez donner un listing des commandes que vous avez utilisées, une explication de votre démarche et une preuve des résultats.
6. RPC (RemoteProcedure Call) est un protocole permettant de faire des appels de procédures sur un ordinateur distant à l'aide d'un serveur d'applications. Ce protocole est utilisé dans le modèle client-serveur et permet de gérer les différents messages entre ces entités. Sur la machine que vous jugez vulnérable, vous allez arrêter le service **rpcdcom**. Pour cela, suivez les instructions suivantes :

   Clic-droit sur Poste de Travail → Gérer → Services et applications → Services

   Ensuite, dans les propriétés du service « Appel de procédure distante (RCP) » choisissez le type de démarrage « Désactivé ». Redémarrez la machine.

   Vérifier que l'exploit n'est plus réalisable (capture d'écran).
7. Une version mise à jour de l'application WarFTPD est disponible à l'adresse http://195.34.45.30/update. A partir de la machine **Quebec**, démarrez l'installation, et choisissez « Upgrade from 1.6* or previous version » au moment où le setup le propose. L'installation présente sur la machine se trouve dans le répertoire C :\warftpd.

   Redémarrez la machine et vérifier que l'exploit n'est plus réalisable (capture d'écran).

Question 3 - Site web PHP vulnérable [/2.5]

Scénario

L'association PolyVideo loue des DVD aux étudiants de Poly à un tarif réduit. Pour se faire connaître, l'association a mis en place un site web qui permet aux membres de gérer leurs informations personnelles et de voir la liste des films qui sont disponibles. Les étudiants qui ont construit le site ont un principe : d'abord la fonctionnalité et ensuite la sécurité. Le site est maintenant en ligne mais la sécurité n'a jamais été mise en balance.

Pour voir le site de PolyVideo qui est hébergé sur la machine **Sherbrooke**, ouvrez un navigateur sur la machine **Québec** et naviguez vers l'adresse suivante : http://195.34.45.30.

Injection de SQL (SQLi)

Vous soupçonnez que le site de PolyVideo est vulnérable à une attaque d'injection de SQL. En faisant du social engineering avec l'administrateur du site web, vous avez réussi de récupérer le bout de code qui authentifie les utilisateurs. Il a suffi de dire à l'admin que vous voulez développer un site qui implémente une authentification et il vous a gentiment donné le code de la page login2.php du site de PolyVideo.

```
1    extract($_POST);
2    $req = "select mem_codefrom MEMBRES wheremem_login = '$login' and mem_pwd = '$pass'";
3    $result = mysql_query($req) or
4    die ("Error : the SQL request<br><br>".$req."<br><br>is not valid: ".mysql_error());
5    list($mem_code) = mysql_fetch_array($result);
6    if (empty($mem_code))        { //verifier que la requete a retourne une reponse positive
```

1. Proposez une façon de vous loguer sur le site web avec le compte : gigi
2. Proposez une façon pour passer à travers de la partie identification du site en supposant que vous ne connaissez aucun nom de compte.
3. Quelles failles dans le code avez-vous utilisées pour l'attaque 1 ? Et pour l'attaque 2 ?
4. Corrigez les failles dans le code que l'admin de PolyVideo vous a envoyé et mettez le code corrigé dans le rapport.

Cross Site Scripting (XSS)

En allant plus loin avec les attaques d'injection SQL, vous avez réussi à copier votre propre page web sur le site. La page est disponible à l'adresse http://195.34.45.30/hacked.html. Pour montrer à vos amis que vous avez réussi à pirater le site de PolyVideo, vous allez faire en sorte que tout utilisateur qui se connecte sur le site de PolyVideo soit redirigé automatiquement vers la page de hacked.html.

Une manière de rediriger un navigateur vers une autre page dans html est la suivante :

```
<script type="text/javascript">document.location.href="autre_page.html"</script>
```

1. Comment avez-vous effectué l'attaque ?
2. Quelles ont été les failles que vous avez utilisées ? Comment les corriger ?

Question 4 - Hacking « facile » [/1]

Pour répondre à cette question, démarrez uniquement la machine virtuelle **Bufferoverflows**. Ouvrez la session **Invité** et allez sur la page http://192.168.242.3.

Vous devez trouver comment entrer dans le système suivant, sans trouver les noms d'usagers et les mots de passe (qui sont évidents dans ce cas-ci, puisqu'ils sont en texte clair dans le programme). Il faut utiliser une attaque basée sur un problème de sécurité dans le programme. Vous devez vous baser uniquement sur ce code et non supposer qu'il y a des trous de sécurité dans d'autres composantes du système (comme des injections SQL). Votre seule manière d'interagir avec le système est donc d'envoyer et de recevoir des caractères au programme. Si votre attaque est un succès, vous n'aurez entré aucun des mots de passe de la liste puis le programme écrira "Bienvenu sur ce système ..." et terminera correctement (il ne doit pas y avoir de faute système).

Le fichier exécutable Windows et le code source en C sont disponibles dans le dossier « hack1 » de l'archive « Fichiers TP2 » sur le site Moodle (utilisez le fichier exécutable fourni et non pas une version que vous avez compilée).

1. Donnez la séquence exacte de caractères à entrer. Expliquez brièvement comment votre « hack » fonctionne.
2. Que faudrait-il changer dans le programme pour enlever ce problème de sécurité?

Question 5 - Hacking « difficile » [/1.5]

Pour répondre à cette question, démarrez uniquement la machine virtuelle **Bufferoverflows**. Ouvrez la session **Invité** et lancez Putty.

Ouvrez une session sur l'hôte 192.168.242.3, sur le port 9999. Le mot de passe est « pass ».

C'est le même problème que la Question 4, mais avec un programme différent. Ce programme permet de gérer des fichiers (lister, afficher) mais si l'on veut *uploader* un fichier le programme demande un user/password. Le but est de contourner l'authentification qui apparaît quand on veut *uploader* un fichier. Ce programme est beaucoup moins facile à « hacker » correctement (si vous êtes débutants dans ce genre de chose). Si votre attaque est un succès, vous n'aurez entré aucun des mots de passe de la liste puis le programme écrira "Bienvenu sur l'interface d'upload de fichier" et terminera correctement (il ne doit pas y avoir de faute système).

Le fichier exécutable Windows et le code source en C sont disponibles dans le dossier « hack2 » de l'archive « Fichiers TP2 » sur le site Moodle (utilisez le fichier exécutable fourni et non pas une version que vous avez compilée).

1. Expliquez en détail comment vous effectuez votre hack.
2. Que faudrait-il changer dans le programme pour enlever ce problème de sécurité?

Références

- Nmap
  http://www.insecure.org/nmap/
- Protocole RCP
  http://en.wikipedia.org/wiki/Remote_procedure_call
- Vulnerabilité RPCDCom
  http://osvdb.org/show/osvdb/2100
- Metasploit Framework
  http://www.metasploit.com/
- Buffer overflow
  http://en.wikipedia.org/wiki/Buffer_overflow#Basic_example
- Stack buffer overflow
  http://en.wikipedia.org/wiki/Stack_buffer_overflow
- Smashing The Stack For Fun and Profit
  http://phrack.org/issues/49/14.html
- Putty User Manual
  http://the.earth.li/~sgtatham/putty/0.58/htmldoc/