UQAR

Université du Québec à Rimouski

300, allée des Ursulines, C. P. 3300, succ. A
Rimouski (Québec) G5L 3A1, CANADA
www.uqar.ca

Département de mathématiques, d'informatique et de génie

Sécurité Informatique
Devoir 2 — Énoncé

SIGLE : INF36207
TITRE : Sécurité Informatique
GROUPE : 06
PROFESSEUR : Steven Pigeon
K-212
steven_pigeon@uqar.ca

DATE DE REMISE : 18 Mars 2016, avant minuit

Modalités. Vous devez faire le devoir en équipes de deux. Comme le devoir demande de créer une machine virtuelle, nous ne pouvez pas tout envoyer par courriel. Par contre, assemblez dans un .zip (ou tout autre type d'archive) les fichiers que vous avez crées ou modifiés avec une indication d'où ils se trouvent dans le système (c'est-à-dire que si vous avez un fichier `.machin`, il faut savoir d'où il vient, par exemple `/etc/truc/.machin`), et les outputs demandés. Joignez un court rapport des étapes nécessaires à la résolution des n° qui suivent. Et, oui, il se peut que vous ayez à installer des choses sur la machine virtuelle fraîchement créée, et, oui, vous devez en tenir compte pour le rapport.

Questions :

1. **Machine Virtuelle**. 2 pts.

   Créez une machine virtuelle Ubuntu Linux Desktop 15.10 (32 ou 64 bits ; au choix, ou même une autre saveur de Linux). Vous pouvez la télécharger à l'adresse suivante : http://www.ubuntu.com/download/desktop.

2. **Firewall & routage**. 7 pts.

   2a) 3 pts. Configurez SSH pour recevoir les connexions venant de l'extérieur sur un port différent de 22 (disons 49876 [1]). Montrez le résultat avec les commandes IPtables (mais vous avez le choix d'utiliser IPtables directement ou un *front-end* qui modifie les règles IPtables pour vous).

   2b) 2 pts. Configurez SSH pour le *forwarding* automatique des connexions X ; côté client et coté serveur.

   2c) 2 pts. Écrivez un court script qui crée un tunnel SSH pour un service, disons `identd` (ou un autre service dont vous pouvez facilement prouver la fonctionnalité à travers le tunnel).

3. **Découverte du réseau**. 6 pts.

   4a) 4 pts. Grâce à `netdiscover` et `zenmap`, construisez une carte *détaillée* du réseau autour de vous (plus la location au moment de l'expérience est intéressante, plus le résultat sera intéressant : évitez donc votre chambre et votre réseau local personnel), avec les ordinateurs au même niveau que vous, les routeurs, les voisins des routeurs si vous en trouvez, et quelques serveurs un peu plus loin sur l'intranet et Internet. Conservez toutes les traces de vos détections (à remettre), et montrez une carte crée par `zenmap`.

   Note : Si vous voulez répondre à la question bonus, quel type de scan `nmap` *allez vous utiliser ?*

   4b) 2 pts. Si vous êtes dans un café, que remarquez vous comme différence principale entre disons, le réseau de l'université et celui du café ?

4. **Bonus**. 2 pts.

   Parmi les ordinateurs voisins que vous aurez trouvés au n° 4, est-ce qu'ils semblent tous configurés adéquatement en terme de sécurité réseau ? Pourquoi ? Quel système d'exploitation utilisent-ils ? Sont-il à jour, pensez vous ? Pourquoi ?

1. Les ports en haut de 49152 sont habituellement réservés pour les connexions dynamiques, donc pas utilisées pour les services