INF4420A – Sécurité Informatique

Travail Pratique 4

01/09/2022

Sommaire

Directives

LIRE ATTENTIVEMENT LES DIRECTIVES SUR LE RAPPORT À REMETTRE SOUS PEINE DE PERDRE DES POINTS OU LA TOTALITÉ DES POINTS.

Tous les travaux devront être remis avant 23h59 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 la professeure.
- L'orthographe et la forme seront prises en compte pour chaque question.
- Indiquez toutes vos sources d'information, qu'elles soient humaines ou documentaires.

Mise en situation

Votre grand ami Bob est un amateur de l'informatique et apprend à faire usage des logiciels libres en lisant des tutoriels. Il veut se servir de l'informatique comme passe- temps pour publier ses passions sur Internet.
Toutefois, voyant régulièrement dans les journaux le fait que de nombreuses compagnies, petites comme grandes, soient victimes de piratage, Bob est craintif. Il se demande si la sécurité de son système est adéquate.
Sachant que vous êtes un étudiant du cours INF4420a – Sécurité Informatique, votre ami Bob vous approche pour évaluer la sécurité de son serveur. Voulant mettre à l'épreuve les notions apprises durant votre cours, vous acceptez avec empressement et un accord d'autorisation écrit.

Votre mandat

Bob vous fournit alors un fichier OVA de machine virtuelle qui est situé dans `/home/INF4420a/A2022/TP4/`.

Votre mandat est donc le suivant : vous devez utiliser Kali Linux et tout outil à votre disposition, téléchargeable dans Kali, pour hacker le serveur, à distance par le réseau local (aucune tentative par un accès direct à la machine virtuelle en elle-même n'est acceptée). Votre objectif, comme celui des hackers, est de prendre le contrôle administratif total du serveur : devenir root.

Étapes suggérées

- Téléchargez et installez un logiciel de virtualisation tel que VirtualBox ou VMWare
- Téléchargez une image virtuelle de la distribution Kali Linux
- Téléchargez l'image virtuelle de l'ordinateur de Bob
- Importez les deux machines dans votre logiciel de virtualisation
- Configurez les deux machines virtuelles pour que les paramètres correspondent à 'host only' dans VMWare ou 'réseau interne' dans VirtualBox (voir Figure 1 et 2 dans Annexe)
- Retrouvez l'IP de la machine de Bob en utilisant l'utilitaire `netdiscover`. Si vous avez besoin d'accéder à Internet à partir de Kali, vous devez soit changer de configuration à chaque fois ou ajouter une interface réseau de type NAT.
- Vous allez ensuite utiliser la machine Kali pour attaquer la machine vulnérable de Bob.

Rapport à remettre en PDF

Chaque action doit être mentionnée accompagnée d'une capture d'écran. Votre explication de la démarche doit inclure toutes les étapes depuis le scan du réseau jusqu'à l'obtention du privilège root sur la machine. La découverte, l'exploitation et les outils utilisés doivent figurer dans votre rapport.

Pour chaque vulnérabilité identifiée, veuillez proposer des recommandations à appliquer afin de la corriger. Vous trouverez dans l'annexe 2, une méthodologie d'audit.

Bon hacking et ayez du plaisir!

Barème

- Reconnaissance [/2]
- Modélisation de la menace [/2]
- Exploitation [/8]
- Escalade de privilèges [/4]
- Recommandations [/3]
- Clarté générale du rapport [/1]

Total : [/20]

Vous devez laisser des traces de votre raisonnement et de vos manipulations, ainsi que des captures d'écran des étapes importantes.

Annexe 1 : Configuration réseau

Configuration de réseau interne sur les paramètres de la machine virtuelle.

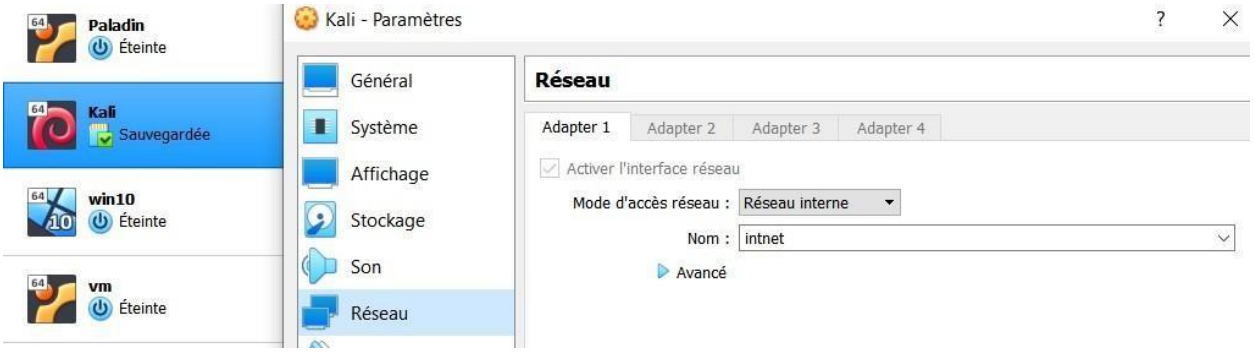

Figure 1 Configuration réseau interne sur VirtualBox Configuration host-only sur les paramètres de la machine virtuelle.

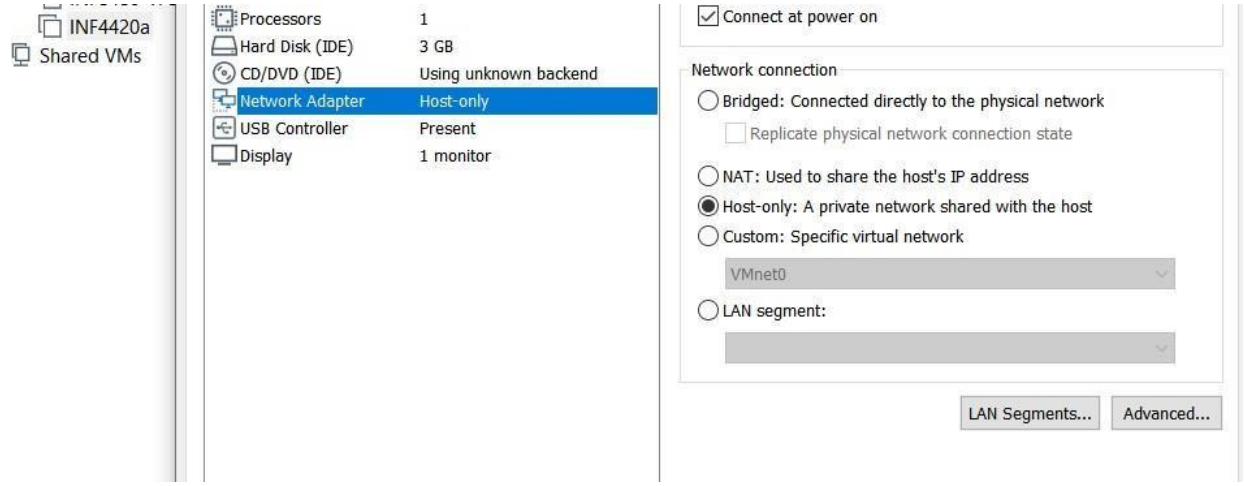

Figure 2 Configuration réseau host-only sur Vmware

Annexe 2 : Éléments de Méthodologie

Ce TP est une simulation d'audit de sécurité, ou *pentesting.* Il existe plusieurs processus de *pentesting*. Les étapes qui nous intéressent sont :

2.1 **Planification** : cette étape correspond à la détermination du domaine de *pentesting*. En lisant le mandat conféré, vous allez pouvoir délimiter ce que vous devez faire, ce que vous ne devez pas faire. Vous allez également préparer votre environnement d'audit en fonction des informations que vous avez.

Cette étape consistera ici à configurer votre VM Kali Linux et configurer les différents paramètres réseau nécessaires à la communication avec votre cible, la VM de l'ordinateur de Bob.

2.2 **Reconnaissance** : Cette étape consiste à recueillir le plus d'information sur la victime afin de déterminer les principaux vecteurs d'attaques. Elle peut être passive ou active. Nous nous intéresserons aux méthodes actives à savoir le balayage de port, l'énumération de répertoires, etc.

Votre VM Kali possède déjà une panoplie d'outils pour faire de la reconnaissance.

nmap : pour le balayage de port et la découverte de services.

Exemple : `nmap -sC -sV -oN sauvegarde.txt 192.x.x.x.`

dirbuster : application pour la découverte de répertoires sur des serveurs Web. Cet outil permet de faire des attaques par dictionnaire/ brute force sur des serveurs web et de découvrir les sous répertoires existants. Dans votre VM Kali, vous pouvez trouver des dictionnaires dans *usr/share/dirbuster/wordlists/.* Ils vous permettront de trouver des sous répertoires intéressants.

2.3 **Modélisation de la menace / Threat modeling** : Dans cette phase, vous allez définir les différents processus/services/assets qui peuvent être attaqués. Vous avez trouvé lors de la phase de reconnaissance des vecteurs d'attaques. Vous pouvez compléter cette phase avec une analyse de risque pour déterminer les potentiels agents de menace.

2.4 **Exploitation :** Durant cette phase, vous allez rechercher des vulnérabilités sur les applications que vous avez trouvées. Vous allez tenter d'en prendre le contrôle.

Il existe des scanneurs de vulnérabilité dans Kali. Par exemple, si vous avez un site Wordpress, vous pouvez utiliser wpscan pour en scanner les vulnérabilités

wpscan: outil de test pour application Wordpress, peut énumérer les plugins installés. *https://tools.kali.org/web-applications/wpscan*

Exemple: `wpscan --url site_wordpress --enumerate p`

searchsploit : outil de recherche dans la base de données d'exploits exploitdb. Vous pouvez chercher localement des exploits sur un service donné

Exemple: `searchsploit woocommerce`

metasploit : Après avoir trouvé un exploit dans exploitdb, vous pouvez tester cet exploit sur Metasploit. La commande *search* permet de chercher dans la liste d'exploits disponibles.

Si vous essayez un exploit sur metasploit et qu'il ne fonctionne pas, en dernier recours vous pouvez essayer d'exploiter la vulnérabilité manuellement. Si c'est le cas, référez-vous au document sur l'exploitation manuelle sur Moodle.

2.5 **Escalade de privilèges :** L'exploitation donne rarement accès directement à un super utilisateur/administrateur du système ciblé. Il faut faire une ou plusieurs escalades de privilège pour passer devenir root/Administrateur. Il y a plusieurs méthodes pour faire une escalade de privilège en fonction du cas. La première des actions à mener est de vérifier les privilèges donnés par le 1er utilisateur acquis (whoami). Ensuite, il faut mener une énumération des fichiers / répertoires auxquels on a accès, à la recherche d'indices, d'identifiants. Parmi les fichiers sensibles, nous avons les fichiers de configuration du service exploité, les configurations ssh, */etc/passwd, /etc/shadow.*

hashcat : outil pour cracker des *hash.* Il utilise par défaut le GPU, mais l'option --force permet d'utiliser le CPU. Il est préférable de se connecter aux machines de Poly pour avoir accès à une plus grosse puissance de calcul.

-m permet de choisir le type de hash, à déterminer en consultant le manuel (man hashcat), -a détermine le mode d'attaque. Le dictionnaire utilisé est rockyou. Sur Kali, il faut d'abord le décompresser avec *gunzip*.

Indice : Si vous trouvez un hash à cracker, il sera entièrement composé de chiffres. Vous pouvez adapter l'attaque pour ne considérer que les nombres dans le dictionnaire rockyou. Il aura aussi une longueur maximale de 7 caractères.

sudo : Vous pouvez déterminer les privilèges que vous avez en utilisant les paramètres de cette commande. Cela peut vous permettre de découvrir des commandes que vous pouvez lancer avec des privilèges plus élevés, *suid.*

2.6 **Post Exploitation :** Cette étape consiste à maintenir la persistance sur le système audité, exfiltrer des données, etc. Elle est en dehors du domaine du TP, mais une fois root, vous pouvez pratiquement tout faire.

2.7 **Rapport :** Cette étape est la partie la plus importante du TP et aussi la raison pour laquelle une méthodologie est nécessaire. C'est à travers le rapport d'audit que vous communiquez vos trouvailles. Vous devez donc dans ce rapport énoncé clairement le domaine de vos tests, les risques (services vulnérables et potentiellement attaquables), idéalement les recommandations. Vous devez munir de captures d'écran commentées toutes les différentes étapes de votre rapport. Vous devez à la fois justifier que l'attaque est possible, montrer une preuve de l'attaque, et pour ce TP, montrer que vous êtes celui qui a réalisé l'attaque.