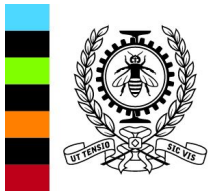
INF8430- Investigation numérique en informatique

Étape initiale à la préparation du travail de session et mesures de sécurité

Séance donnée par Nedra Hamouda



POLYTECHNIQUE MONTRÉAL

Plan de la séance

1. Hyperviseur
2. Réalisation d’une attaque
3. Système d’exploitation
4. Configuration du réseau

Vous trouverez à la fin des liens utiles et autres.

Le reste de la période sera réservé pour vous familiariser avec les outils et pour votre projet de session.

Sondage

1. Combien ont déjà suivi les cours :
    a. INF4420a - Sécurité Informatique (José M. Fernandez)
    b. INF8402 - Sécurité des réseaux fixes et mobiles (Alejandro Quintero)

2. Êtes-vous familier avec l'usage d'hyperviseurs?

3. Avez-vous déjà participé à des compétitions de sécurité?

1 - Hyperviseur

Qu’est-ce qu’un hyperviseur

Le fait d’exécuter un système d’exploitation par le biais d’un logiciel. Un tel logiciel est communément appelé un hyperviseur .

L’hyperviseur permet de virtualiser une “machine” sur une autre machine hôte.

2- Réalisation d'une attaque

Conseil

Je vous conseille d'utiliser **VirtualBox** car c'est un hyperviseur *open source* gratuit à 100% et est facile d'installation.

Lien pour le téléchargement :

https://www.virtualbox.org/wiki/Downloads

Étapes d’une attaque (kill chain simplifié)

1. Reconnaissance
   - Analyse, social engineering, etc...
2. Balayage
   - Exemple : Scannage de ports et de systèmes (nmap)
3. Exploitation
   - Attaquer la cible Exemple d’outils : Metasploitable, John the Ripper, Wireshark
4. Post exploitation
   - Maintenir l’accès, créer une backdoor (Ncat, Rootkits)

Pour votre projet de session, vous devez…

1. Effectuer une revue de littérature
2. Configurer les machines virtuelles
3. Avant l'attaque :
    3.1. Prélèvement des mémoires *RAM*
    3.2. Base de registres
    3.3. Processus en cours
    3.4. Image judiciaire des VMs
4. Effectuer l'attaque
5. Suite à l'attaque :
    5.1. Prélèvement des mémoires *RAM*
    5.2. Base de registres
    5.3. Processus en cours
    5.4. Image judiciaire des VMs
6. Analyser les traces de l'attaque

3 - Système d'exploitation (*OS*)

Comment choisir?

- Le choix dépend de l'attaque que vous allez effectuer pour votre projet.

- Listez les avantages et les désavantages d'utiliser un système plus que l'autre.

- Soyez conscient des limitations de chaque système.

Linux Kali

- Nouvelle version de BackTrack
- Regroupe plusieurs outils de **reconnaissance**, de **balayage**, d'**exploitation** et de **post exploitation**.

Une image de Linux Kali pour VirtualBox :

https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/

Metasploitable II

- Il s’agit d’une machine virtuelle Linux déjà vulnérable

Metasploitable II peut être téléchargé ici :

http://sourceforge.net/projects/metasploitable/files/Metasploitable2/

Exemples de vulnérabilités exploitables sur Metasploitable II

- Backdoor

- Services web vulnérables
  - SQL Injection
  - JavaScript Injection
  - JSON Injection
  - Cross site scripting
  - Phishing

- Mots de passes faibles

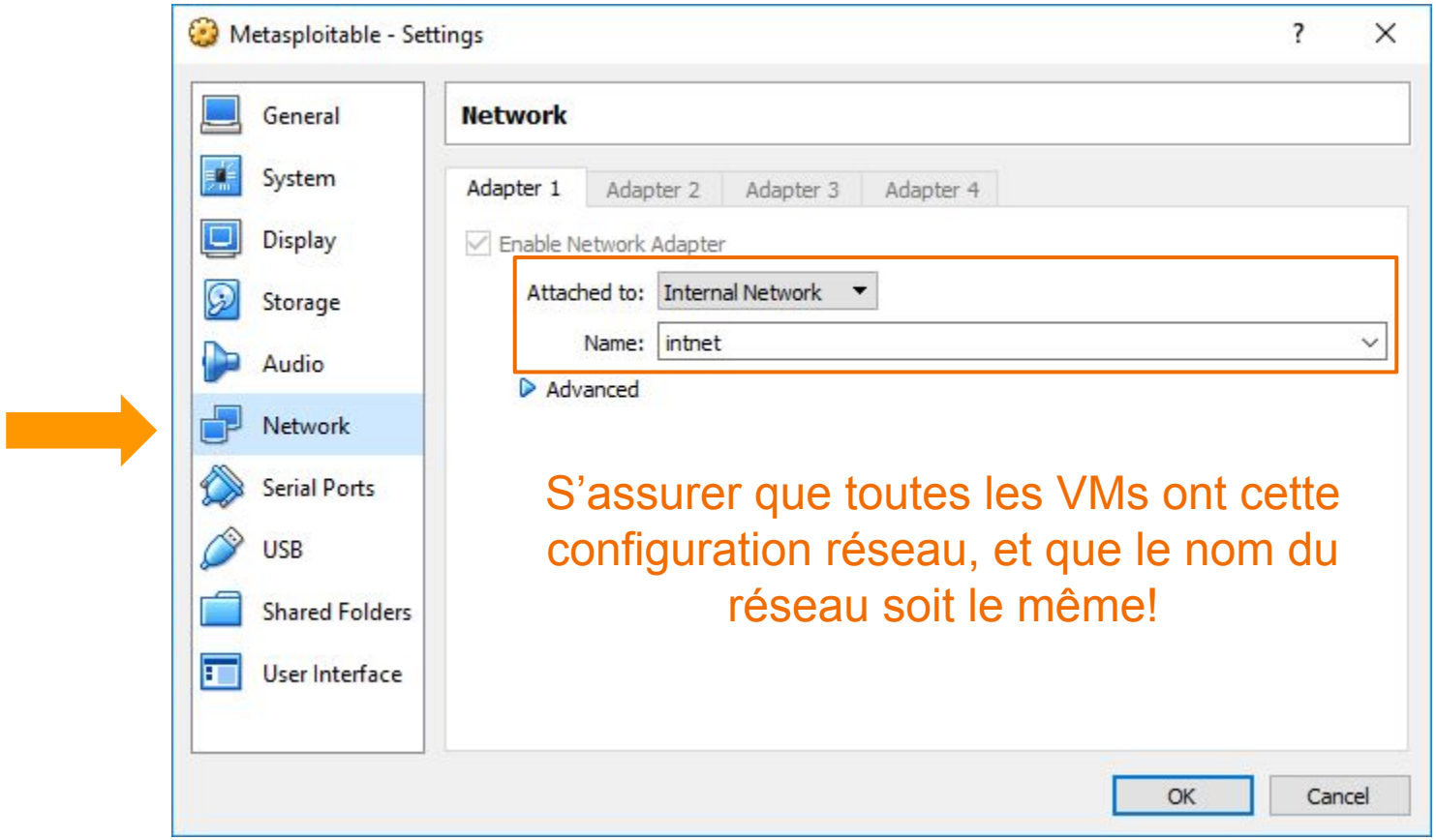
4- Configuration du réseau

Isolation d'Internet

Il faut s'assurer de créer un **réseau local interne**. C'est un réseau local et privé sur la machine hôte. Les machines virtuelles connectées à ce réseau auront la possibilité de communiquer entre elles. Il est impossible d'envoyer ou de recevoir du trafic avec le réseau local de la machine hôte ou Internet.

NB : Par défaut, Linux Kali est configuré avec un NAT. Plusieurs tutoriels existent expliquant comment le changer.

Configuration du réseau pour chaque VM



Précautions à prendre

- Assurez-vous de ne jamais pouvoir accéder au réseau externe à partir des machines virtuelles
- Testez la configuration une première fois tout en prenant des notes afin de la refaire proprement pour ne pas laisser des traces inutiles sur les machines virtuelles.
- Prendre des *snapshot* des états initiaux ou avant toute manipulation dont vous n'êtes pas certains.

Liens utiles

Liste de ports logiciels : https://fr.wikipedia.org/wiki/Liste_de_ports_logiciels

Tutoriels :

- Wireshark : https://wiki.wireshark.org/
- Nmap : https://nmap.org/
- Metasploitable II : https://community.rapid7.com/docs/DOC-1875/

PolyHack : http://polyhack.org/wp-content/uploads/2013/08/Cheminement_General_1.2.pdf

Pour les intéressés

Voici quelques sites de challenge

- http://vulnhub.com/
- https://google-gruyere.appspot.com/
- http://captf.com/practice-ctf/
- https://xss-game.appspot.com/

N’oubliez pas de signer la feuille avant de quitter!

Travail sur le Labo #1 et rencontre pour votre travail de session