Laboratoire N^o 2

Cours : Sécurité des réseaux informatiques

1 Rappel important

Il est complètement interdit de pratiquer les techniques vues dans ce cours sur un réseau ou une machine qui ne vous appartient pas, y compris le réseau de l'université et les machines qui ne sont pas dans le laboratoire prévu pour cette fin. Vous risquez la prison et ni votre professeur, ni votre université ne peuvent vous protéger. La loi c'est la loi !
Le piratage (Hacking), c'est criminel. Principalement, la loi définit comme crimes informatiques : L'accès illégal aux ordinateurs et à leurs données (cc.342.1) ; le vols de données informatiques (cc.342.1) ; le méfaits aux données (cc.430). Pour plus de détails sur le code criminel : laws-lois.justice.gc.ca/PDF/C-46.pdf

2 Objectif

L'objectif de ce travail est de permettre à l'étudiant de se familiariser avec quelques outils de *scan* et de *footprinting*.

3 Description du réseau utilisé

À part la machine hôte, nous utilisons pour ce laboratoire la machine virtuelle Kali configurée avec la même adresse que nous vous avons attribuée lors du premier laboratoire ainsi que la machine M110 du premier TP.

4 Travail demandé

Dans le même esprit que le premier laboratoire, ce travail consiste à faire certaines opérations décrites dans les étapes qui suivent et de prendre des copies d'écrans montrant vos résultats. Les étapes pour lesquelles vous devez prendre des copies d'écrans sont indiquées par le signe suivant :

1. Personnaliser le prompt de votre machine Kali avec la commande suivante en remplaçant `Nom` et `Prenom` par votre nom et votre prénom :

   ```
   PS1="${debian_chroot:+($debian_chroot)}\[\033[01;32m\]\u@\h Prenom Nom \[\033[00m\]:\[\033[01;34m\]\w\[\033[00m\]#"
   ```

   Remarque : Toutes vos captures d'écran doivent montrer soit votre nom (sur un interpréteur de commandes) soit l'adresse IP de votre machine Kali.
2. Connecter Kali à Internet, la mettre à jour (`apt-get update`), puis la redémarrer (`reboot`).
3. Mettre la carte réseau de Kali dans le mode host-only.
4. Lancer M110 et mettre sa carte réseau dans le mode host-only. N'essayez pas de rentrer des noms d'utilisateur ou des mots de passe sur M110.
5. (2.5pts) nmap : l'outil de scan le plus utilisé :
   a) (0.25pt) Via la commande `ping`, vérifiez si vous pouvez joindre M110 à partir de Kali. Donner une copie d'écran montrant à la fois la commande utilisée et le résultat obtenu.
   b) (0.25pt) À partir de Kali et en utilisant `nmap` et le mode TCP-Connect, trouver tous les ports TCP ouverts sur M110. Donner une copie d'écran montrant à la fois la commande utilisée et le résultat obtenu.
   c) (0.25pt) À partir de Kali et en utilisant `nmap` et le mode TCP-Syn, scanner tous les ports TCP de M110, et ce, tout en fixant le port TCP source à 25 (protocole SMTP). Donner une copie d'écran montrant à la fois la commande utilisée et le résultat obtenu.
   d) (0.25pt) À partir de Kali et en utilisant `nmap` et le mode TCP-Syn, scanner tout le réseau 192.168.1.0 excluant la machine Kali. Donner une copie d'écran montrant à la fois la commande utilisée et le résultat obtenu.
   e) (0.25pt) À partir de Kali et en utilisant `nmap`, trouver les ports UDP, parmi les plus utilisés, ouverts sur M110. Donner une copie d'écran montrant à la fois la commande utilisée et le résultat obtenu.

f) (0.25pt) ☞ À partir de Kali et en utilisant `nmap`, trouver le service qui se cache derrière le port 21 de la machine M110 ainsi que sa version (votre commande ne doit pas montrer des informations relatives à des ports autres que 21). Donner une copie d'écran montrant à la fois la commande utilisée et le résultat obtenu.

g) (0.25pt) ☞ Via `nmap`, déterminer le nom et la version du système d'exploitation de la machine M110. Donner une copie d'écran montrant à la fois la commande utilisée et le résultat obtenu.

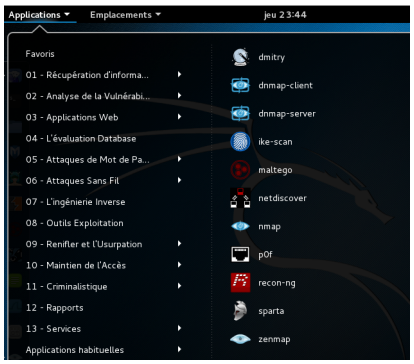
h) (0.25pt) ☞ À partir de Kali et en utilisant les scripts de `nmap`, vérifier si M110 admet un service qui permet une connexion FTP anonyme. Donner une copie d'écran montrant à la fois la commande utilisée et le résultat obtenu.

```
root@kali:~# nmap --script ftp-anon.nse 192.168.1.110 -p 21
```

i) (0.25pt) ☞ À partir de Kali et en utilisant le script sshv1.nse de `nmap`, vérifier si M110 admet la version sshv1 obsolète et peu sécuritaire du service SSH . Donner une copie d'écran montrant à la fois la commande utilisée et le résultat obtenu.

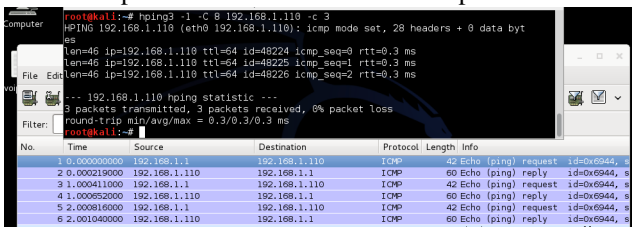
j) (0.25pt) ☞ À partir de Kali et en utilisant le script `vuln` de `nmap`, vérifier si M110 admet des services vulnérables. Donner une copie d'écran montrant à la fois la commande utilisée et le résultat obtenu.

k) (0.25pt) ☞ Via `Zenmap` (nmap avec une interface graphique), vous faites un SYN scan sur les ports de 20 à 440. Donner une copie d'écran montrant à la fois la commande utilisée et le résultat obtenu. `Zenmap` est accessible à partir du menu suivant :



6. (1pt) Hping3 : un autre outil de scan redoutable
   Pour visualiser les options de *hiping3*, taper *hping3 -h*

a) (0.25 pt) ☞ En utilisant *hping3*, envoyer trois ICMP de type 8 (Echo Request) à la machine M110 et prendre une copie d'écran montrant à la fois la commande tapée et le trafic Wireshark correspondant.



b) (0.25 pt) ☞ En utilisant *hping3*, trouver l'heure (timestamp) sur la machine M110. Donner une copie d'écran montrant à la fois la commande utilisée et le trafic Wireshark correspondant.

c) (0.25 pt) ☞ En utilisant *hping3*, envoyer un paquet SYN/FIN sur le port 80 de la machine M110 et prendre une copie d'écran montrant à la fois la commande tapée et le trafic Wireshark correspondant.

d) (0.25 pt) ☞ En utilisant *hping3*, scanner le port UDP 53 tout en remplaçant (spoofing) l'adresse source par 192.168.1.254. Donner une copie d'écran montrant à la fois la commande utilisée et le trafic Wireshark correspondant.

7. (0.1pt) Autres outils

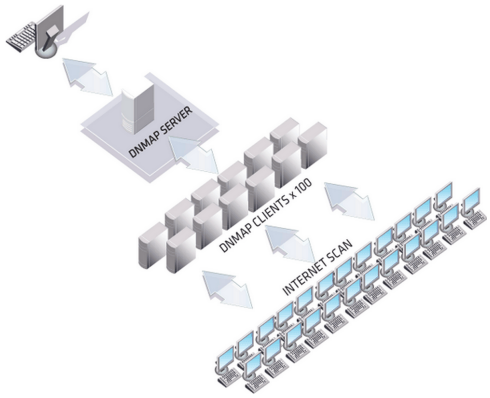
a) (0.25pt) ☞ Netcat (commande `nc`) est l'un des outils les plus utiles lors de différentes étapes d'une attaque (c'est une sorte d'un couteau suisse). Pour avoir de l'aide sur netcat, taper la commande `nc -help`. À partir de Kali et en utilisant

Netcat, avec les options "-v" et "-z", scanner tous les ports TCP entre 10 et 100 de la machine M110. Donner une copie d'écran montrant à la fois la commande utilisée et le résultat obtenu.

b) (0.25pt) ☞ À partir de Kali et en utilisant Netcat, scanner tous les ports UDP entre 1 et 1054 de la machine M110. Donner une copie d'écran montrant à la fois la commande utilisée et le résultat obtenu.

c) (0.5pt)☞ À partir de Kali, utiliser PackETH pour construire une trame permettant de faire un scan de type TCP FIN sur le port 23 de la machine M110. Donner une copie d'écran montrant à la fois la commande utilisée et le trafic Wireshark correspondant.

8. (0.75pt) *dnmap* (distributed namp) permet de distribuer un scan d'un réseau sur plusieurs clients et d'envoyer le résultat à un seul serveur central comme le montre le schéma suivant :

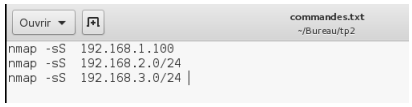


source : http ://www.tripwire.com/state-of-security/vulnerability-management/distributed-nmap-port-scanning-dnmap-megacluster/

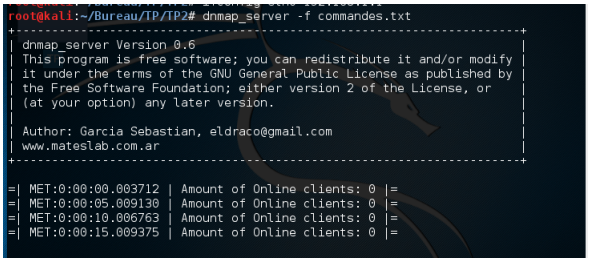
a) Comprendre le fonctionnement de dnmap : http ://www.mateslab.com.ar/dnmap-the-distributed-nmap.html

b) Utiliser kali, pour lancer un serveur et un client dnmap pour scanner la machine M110 (un syn scan des ports les plus célèbres) et prenez des copies d'écran montrant votre démarche et vos résultats. Les étapes suivantes sont données à titre indicatif :

– Créer le fichier de commandes.

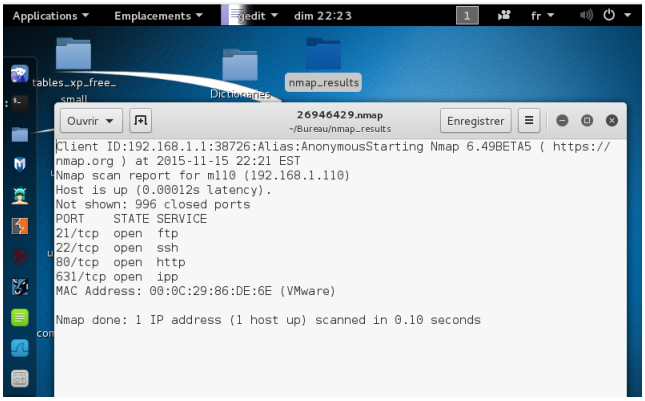


– Lancer le serveur.

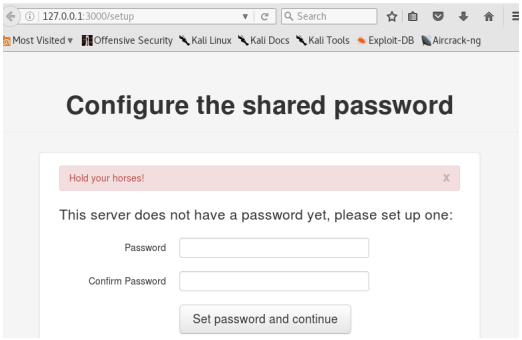


– (0.25pt)☞ Lancer le client et le connecter au serveur.

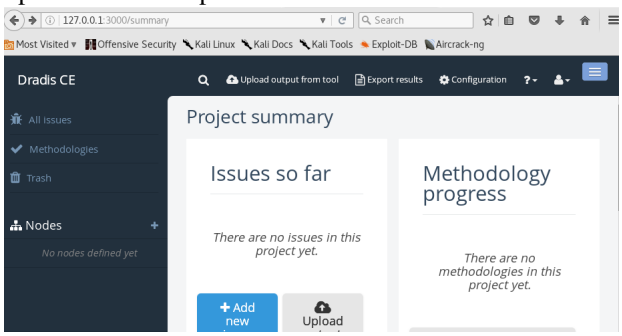
– (0.5pt)☞ Récupérer le résultat dans le répertoire *nmap_results*



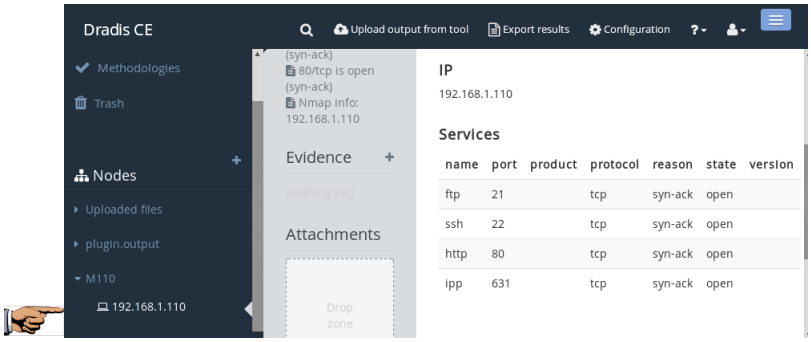
9. (0.75pt) Génération et partage des résultats d'un scan.
   L'analyse d'un réseau devrait toujours s'accompagner d'un rapport montrant les résultats. Parmi les outils utiles permettant de faciliter la rédaction et le partage de ce genre de rapport via le web, nous trouvons `Dradis` (*http ://dradisframework.org/*).
   – La version courante de Dadis sur Kali présente certains problèmes. Pour télécharger et installer la dernière version, connecter Kali à Internet et suivre les étapes suivantes :
     – *apt-get install libsqlite3-dev*
     – *apt-get install mysql-server mysql-client libmysqlclient-dev*
     – *apt-get install redis-server*
     – *redis-server*
     – *git clone https ://github.com/dradis/dradis-ce.git*
     – *cd dradis-ce*
     – *./bin/setup*
     – *bundle install*
     – *./bin/setup*
   – Démarrer dradis via la commande suivante : *bundle exec rails server* à partir du répertoire */dradis-ce*
   – Lancer l'interface web du dradis via le menu `Applications->Rapports->dradis` et choisir un mot de passe (exemple *toor*).



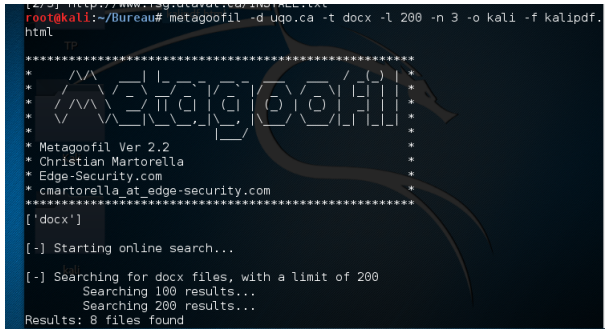
   En cas de problèmes, ouvrez votre navigateur et tapez http ://127.0.0.1 :3000/setup
   – Choisir un nom d'utilisateur et taper votre mot de passe.



   – Sur un terminal lancer nmap sur M110 tout en demandant que le résultat soit sauvegardé dans le fichier nmapM110.xml selon format XML.
   – (0.75pt) Une fois connecté, créer un noeud M100 dans lequel vous importer les résultats du fichier nmapM110.xml. Prenez une copie d'écran du résultat.
   – Sous Dradis, ajouter un noeud M110 dans lequel vous importez le contenu du fichier nmapM110.xml.



10. Connecter Kali à Internet
11. (1pt) Utilisation de l'outil *maltego* (Kali : `Applications->Récupération d'informations->maltegoce`) pour une collecte d'informations. Pour mieux comprendre le fonctionnement *maltego*, consultez la documentation disponible sur le site web *www.paterva.com*.
    a) (0.5pt) À partir de votre machine Kali et en utilisant l'outil *maltego*, trouver les serveurs courriels, les serveurs DNS et les intervalles d'adresses IP de l'université Laval. Prendre des copies d'écran montrant vos résultats.
    b) (0.5pt) Utiliser les transformateurs (Transformers) de *maltego* pour voir ce qu'il peut dévoiler comme information sur vous : à partir de votre nom et prénom, essayez de voir si *maltego* peut trouver vos adresses courriel, vos comptes liés aux réseaux sociaux, vos photos, vos numéros de téléphone, etc. Prendre des copies d'écran montrant vos résultats.
12. (0.5pt) *Metagoofil* est un outil pertinent permettant de collecter des données (nom d'utilisateurs, courriels, version de logiciels, etc.) à partir des métadonnées des fichiers (PDF, PPT, etc.).
    – Utiliser la commande suivante pour installer *metagoofil* :
    ```
    pip install requests
    rm -rf /usr/share/metagoofil/
    git clone https://github.com/WiReD-/metagoofil.git /usr/share/metagoofil
    ```
    – Taper `metagoofil -h` pour comprendre les options de cet outil.
    – Comprendre et lancer la commande suivante :



    metagoofil -d owasp.org -t pdf,doc,ppt -l 200 -n 5 -o /root/Bureau/metagoofil/ -f /root/Bureau/metagoofil/result.html
    – (0.5pt) Afficher les utilisateurs et les versions de logiciels découverts par la commande précédente :

5 Remarques

1. Le travail est individuel.
2. Le barème (total =7.5) indiqué est à titre indicatif.

6 À remettre

Utilisez le site web du cours pour déposer un fichier PDF ou Word contenant les copies d'écrans demandées, et ce, tout en gardant le même ordre et les mêmes numérotations.

7 Échéancier

Le 31 octobre 2016 avant 00h00. **À noter que les TPs remis en retard ne seront pas acceptés.**