

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 vol de données informatiques (cc.342.1); le méfait 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 du *footprinting* et du *scanning*.

3 Description du réseau utilisé

À part la machine hôte, nous utilisons la machine Kali et la machine M110. La machine Kali garde la même adresse utilisée lors du premier TP.

4 Travail demandé

Dans le même esprit que le premier TP, ce travail consiste à manipuler certains outils 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 :



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 : Pour ne pas perdre vos points, toutes vos captures d'écran doivent montrer soit votre nom (sur un interpréteur de commandes) soit l'adresse IP de votre machine Kali.

4.1 Footprinting

- I) (0.3pt) En utilisant *whois*, en ligne de commandes, trouver l'intervalle d'adresses IP du domaine `microsoft.com` selon les étapes suivantes :
 - a) Utiliser *whois* pour trouver des serveurs de noms du domaine en question.
 - b) Utiliser *dig* pour trouver l'adresse IP du premier serveur trouvé dans l'étape précédente.
 - c) Utiliser l'adresse IP précédente et *whois* pour trouver l'intervalle d'adresses en question.
- II) (0.3pt) Prendre une copie d'écran montrant la commande et le résultat pour chacune des questions suivantes :
 - a) Utiliser *host* pour demander au serveur DNS du domaine `zonetransfer.me` un transfert de zone.
 - b) Utiliser *dig* pour demander à google (8.8.8.8) l'adresse IPv6 de `www.ulaval.ca`
 - c) Utiliser *nslookup* pour afficher l'enregistrement SOA du domaine `ulaval.ca`
- III) (0.25pt) Utiliser une requête raffinée de Google, pour trouver des fichiers de configuration de serveur VPN (fichiers de type `pccf`) contenant une clé de connexion. Donner une copie d'écran montrant la commande utilisée et une autre montrant un résultat donnant la clé permettant d'accéder à un serveur VPN.

```

GroupName=Staff
GroupPwd=
enc_GroupPwd=4DA72563626066B87D78836E93086F1973343B803A6981BE6AF4F50776E08D7F35D
EnableISPConnect=0
ISPConnectType=0
ISPConnect=

```

IV) (0.65pt) Utilisation de *maltego* (Kali : Applications->Récupération d'informations->maltego) pour une collecte d'informations. Pour mieux comprendre le fonctionnement de cet outil, consultez la documentation disponible sur le site web www.paterva.com.

- (0.4pt) À partir de 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.
- (0.25pt) Utiliser les transformateurs (Transformers) de *maltego* pour voir ce qu'il peut dévoiler comme informations 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.

V) (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* :

```
apt-get install metagoofil
```

- Taper `metagoofil -h` pour comprendre les options de cet outil.
- Comprendre et lancer la commande suivante :

```

root@kali:~/Bureau# metagoofil -d uqo.ca -t docx -l 200 -n 3 -o kali -f kalipdf.html
Metagoofil Ver 2.2
* Christian Martorella
* Edge-Security.com
* cmartorella_at_edge-security.com
[ 'docx' ]
[.] Starting online search...
[.] Searching for docx files, with a limit of 200
    Searching 100 results...
    Searching 200 results...
Results: 0 files found

```

`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 :



4.2 Scanning

1. Lancer M110 sans essayer de rentrer un nom d'utilisateur ou un mot de passe.
2. (2.5pts) nmap : l'outil de scan le plus utilisé :
 - a) (0.25pt) 🖱️ À partir de Kali et en utilisant nmap faire un scan rapide (Fast scan) sur 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 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.
3. (1pt) Hping3 : un autre outil de scan redoutable.
Pour visualiser les options de hping3, taper `hping3 -h`

```
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 (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) 🖱️ À partir de Zenmap (nmap avec une interface graphique), faire 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 Applications → Récupération d'Informations du Kali.

```
root@kali:~# hping3 -h
usage: hping3 host [options]
-h --help show this help
-V --version show version
-c --count packet count
-i --interval wait (uX for X microseconds, for example -i u1000)
--fast alias for -i u1000 (10 packets for second)
--faster alias for -i u1000 (100 packets for second)
--flood sent packets as fast as possible. Don't show replies.
-n --numeric numeric output
-q --quiet quiet
-I --interface interface name (otherwise default routing interface)
-V --verbose verbose mode
-D --debug debugging info
-Z --bind bind ctrl+z to ttl (default to dst port)
-Z --unbind unbind ctrl+z
-b --beep beep for every matching packet received

Mode
default mode TCP
-0 --rawip RAW IP mode
-1 --icmp ICMP mode
-2 --udp UDP mode
-8 --scan SCAN mode.
Example: hping -s -s -s -s -s www.target.host
```

- 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 utilisée et le trafic Wireshark correspondant.

```
root@kali:~# hping3 -I 0 -c 3 192.168.1.110
HPING 192.168.1.110 (eth0 192.168.1.110): icmp mode set, 28 headers + 0 data byt
len=46 ip=192.168.1.110 ttl=64 id=48224 icmp_seq=0 rtt=0.3 ms
len=46 ip=192.168.1.110 ttl=64 id=48225 icmp_seq=1 rtt=0.3 ms
len=46 ip=192.168.1.110 ttl=64 id=48226 icmp_seq=2 rtt=0.3 ms
root@kali:~#
```

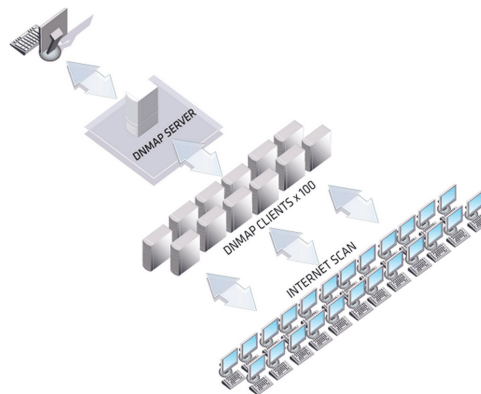
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.1	192.168.1.110	ICMP	42	Echo (ping) request id=0x6944, s
2	0.000219000	192.168.1.110	192.168.1.1	ICMP	60	Echo (ping) reply id=0x6944, s
3	1.000411000	192.168.1.1	192.168.1.110	ICMP	42	Echo (ping) request id=0x6944, s
4	1.000630000	192.168.1.110	192.168.1.1	ICMP	60	Echo (ping) reply id=0x6944, s
5	2.000818000	192.168.1.1	192.168.1.110	ICMP	42	Echo (ping) request id=0x6944, s
6	2.001040000	192.168.1.110	192.168.1.1	ICMP	60	Echo (ping) reply id=0x6944, s

- 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 utilisée et le trafic Wireshark correspondant.
- d) (0.25 pt) 🖱️ En utilisant *hping3*, scanner le port UDP 53, et ce, 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.

4. (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) (0.25pt) 🖱️ À partir de Kali et en utilisant Netcat, déterminer la version du serveur *ftp* de la machine M110 en faisant une analyse de bannière. Donner une copie d'écran montrant à la fois la commande utilisée et le résultat obtenu.
- d) (0.25pt) 🖱️ À partir de Kali, utiliser *PACKET* 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.

5. (0.5pt) *dnmap* (distributed nmap) 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://mateslab.weebly.com/dnmap-the-distributed-nmap.html>
- b) Une version améliorée de dnmap, s'appelle dnmapR se trouve sur <https://github.com/opsdisk/dnmapR>
- c) 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 :

- i) Télécharger et décompresser les fichiers de dnmapR dans un répertoire de votre choix.

```
root@kali:~/Bureau/dnmapR-master# ls
dnmapR_client.py dnmapR_server.py LICENSE README.md README.orig server.pem
root@kali:~/Bureau/dnmapR-master#
```

- ii) Créer le fichier de commandes.

```
commands.txt
Fichier Édition Rechercher Options Aide
nmap -sS 192.168.1.0/24
nmap -sS 192.168.2.0/24
nmap -sS 192.168.3.0/24
```

- iii) Lancer le serveur (l'adresse IP doit être celle de votre machine Kali).

```

root@kali: ~/Bureau/dnmapR-master
Fichier Édition Affichage Rechercher Terminal Aide
root@kali:~/Bureau/dnmapR-master# python dnmapR_server.py -f commands.txt -i 192.168.1.1
[*] dnmapR server version 1.0
[*] Listening for connections on: 192.168.1.1:46001
[*] Log file location: ./dnmapR_server.log
[*] MET:0:00:00.002486 | Online clients: 0 |=
[*] MET:0:00:05.007590 | Online clients: 0 |=

```

iv) (0.25pt) 🖱️ Lancer le client et le connecter au serveur (l'adresse IP doit être celle de votre machine Kali).

```

root@kali: ~/Bureau/dnmapR-master
Fichier Édition Affichage Rechercher Terminal Aide
root@kali:~/Bureau/dnmapR-master# python dnmapR_client.py -s 192.168.1.1
[*] Client started...
[*] Nmap output files stored in 'nmap_output' directory...
[*] Attempting connection to server
[*] Client connected successfully...waiting for more commands.
[*] No -oA argument, adding it to keep results. Added -oA 89870313
[*] Executed command: nmap -sS 192.168.1.0/24 -oA 89870313
[*] Sending output to the server...
[*] Waiting for more commands...

```

v) (0.25pt) 🖱️ Récupérer le résultat dans le répertoire *nmap_results*

```

Ouvrir 89870313.nmap Enregistrer
~/Bureau/dnmapR-master/nmap_results
Client ID:192.168.1.1:36154:Alias:anonymousStarting Nmap 7.50 ( https://nmap.org ) at 2017-07-11
13:29 EDT
Nmap scan report for 192.168.1.110
Host is up (0.00040s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
631/tcp   open  ipp
MAC Address: 08:00:27:6A:EB:C3 (Oracle VirtualBox virtual NIC)

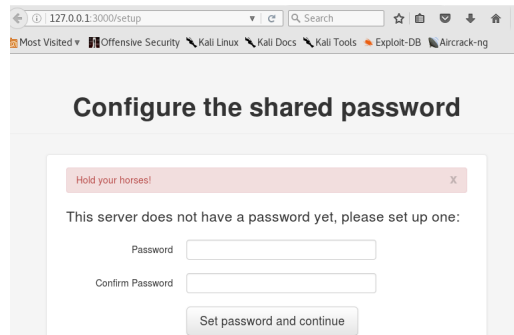
Nmap scan report for 192.168.1.1
Host is up (0.0000030s latency).
All 1000 scanned ports on 192.168.1.1 are closed
Nmap done: 256 IP addresses (2 hosts up) scanned in 8.81 seconds

```

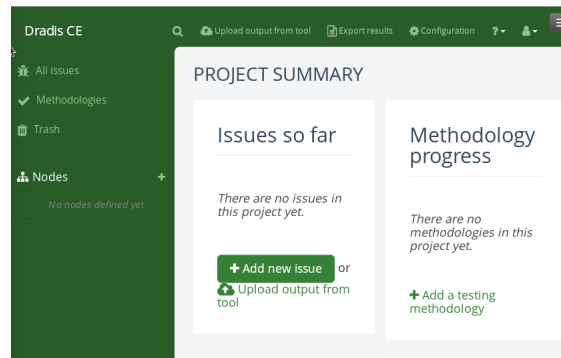
6. (0.5pt) Génération et partage des résultats d'un scan.

L'analyse d'un réseau devrait toujours s'accompagner d'un rapport montrant les résultats. Parmi les outils permettant de faciliter la rédaction et le partage de ce genre de rapport via le web, nous trouvons Dradis (<http://dradisframework.org/>).

a) Lancer l'interface web du dradis via le menu Applications->Rapports->dradis et choisir un mot de passe (exemple *toor*).

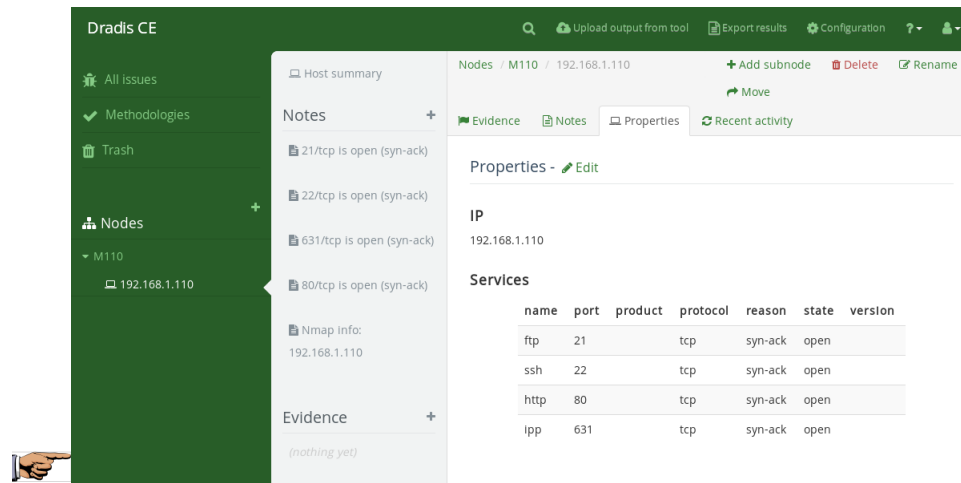


b) Choisir un nom d'utilisateur et taper votre mot de passe.



c) Sur un terminal lancer nmap sur M110 tout en demandant que le résultat soit sauvegardé dans le fichier nmapM110.xml selon format XML.

d) (0.5pt) Une fois connecté, créer un noeud M110 dans lequel vous importez les résultats du fichier nmapM110.xml. Prenez une copie d'écran du résultat.



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 30 octobre 2018 avant 14h00. Le maximum autorisé pour un retard est deux jours (48 heures), et ce, avec les pénalités suivantes : pour moins que 24 heures de retard, l'étudiant aura 70% de sa note. Entre 24 et 48 heures de retard, il aura 40% de sa note. Plus que 48 heures de retard, il aura 0.