Chapitre 3
Installation du lab d'exploitation

1. Rappel sur l'éthique des tests

En France, les tests d'intrusion sont encadrés par un cadre légal relativement important. En effet, plusieurs articles du Code pénal mettent en évidence les délits informatiques à l'encontre des systèmes de traitements automatisés de données (STAD).

Code pénal, art. 323-1 :

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un STAD est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.

« **Frauduleusement** » est le terme le plus important au sein de cette phrase. En effet, avant la réalisation des tests d'intrusion, client et auditeur doivent se mettre d'accord sur le périmètre à auditer ainsi que sur les actions à faire ou ne pas faire (cf. chapitre Introduction aux tests d'intrusion, section Quelles sont les différentes phases d'un test d'intrusion ?).

Ainsi, **le mandat d'autorisation** est l'élément permettant à l'auditeur de se dégager de toute responsabilité vis-à-vis de l'audit de sécurité. En effet, s'il y a autorisation, il ne peut y avoir fraude.

Le lecteur curieux pourra également s'intéresser aux articles 323-2 et 323-3 du Code pénal.

En France, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a également mis en place la qualification PASSI ayant pour but d'accroître la qualité des audits de sécurité en imposant certains critères, qui sont garantis par la réalisation d'une prestation qualifiée conforme au référentiel PASSI. Pour cela, il est nécessaire de prendre en compte les éléments suivants :

– Garantie de compétences des auditeurs en charge de l'audit.
– Garantie de déontologie, de protection et de confidentialité des données, rapports et documents échangés.
– Garantie d'une méthodologie appropriée aux audits de sécurité.
– Recours possible auprès de l'ANSSI si la prestation réalisée s'avère non conforme au référentiel PASSI.

Néanmoins, la certification PASSI ne permet pas d'éviter la signature de mandats d'autorisation à la réalisation des tests entre les parties prenantes.

L'auteur de ce livre ainsi que les Éditions ENI ne pourraient être tenus pour responsables si les techniques décrites au sein de cet ouvrage étaient utilisées de manière non éthique. Soyez entièrement responsable de vos actions.

2. Installation native de Metasploit

Malgré la complexité de l'outil, Rapid7 met à disposition des installeurs pour le Framework Metasploit. Ces installeurs sont actuellement disponibles sur les plateformes GNU/Linux, Mac OS X et Windows.

Ces derniers permettent une installation simple et rapide du Framework grâce à l'inclusion de l'ensemble des dépendances nécessaires (John the Ripper, Nmap, etc.).

Avant de procéder à l'étape d'installation, il est nécessaire de s'assurer que les plateformes répondent à différents prérequis. En effet, dans un souci d'une utilisation optimale, Rapid7 préconise les actions suivantes.

Vérifier le matériel

Afin de disposer d'un outil réactif, il est conseillé de disposer de la configuration suivante :

– un processeur cadencé à 2 GHz+
– 4 Go de mémoire RAM (8 Go recommandés)
– 1 Go d'espace disque (50 Go recommandés)

Les recommandations concernant le matériel pouvant être amenées à évoluer, il est préférable de se référer à la documentation officielle sur le site de Rapid7 : https://www.rapid7.com/products/metasploit/system-requirements

Désactiver votre antivirus

En restant du bon côté de la barrière, Metasploit est un outil permettant de découvrir et d'exploiter des vulnérabilités présentes sur une machine et/ou un réseau. Il est fréquent que Metasploit exploite exactement les mêmes vulnérabilités que des outils malveillants (virus, malware, etc.).

Un antivirus n'étant pas en mesure de séparer le bon grain de l'ivraie, il bloquera certaines fonctionnalités jugées comme dangereuses bien que nécessaires pour les tests d'intrusion. De son point de vue, il a fait son travail.

Afin de ne souffrir d'aucune restriction, Rapid7 recommande de désactiver l'antivirus ou d'exclure le répertoire Metasploit ainsi que les répertoires courants de l'analyse antivirale.

En outre, il est nécessaire d'obtenir Metasploit depuis le site officiel afin de s'assurer qu'aucun programme malveillant n'a été ajouté, pouvant entraîner d'importants dégâts.

Désactiver le pare-feu

Outre l'antivirus, il est préférable de désactiver le firewall (firewall Windows, iptables, Little Snitch, etc.) pour permettre aux payloads de se connecter à Metasploit.

Disposer des droits d'administration lors de l'installation

Au cours de l'installation, il sera nécessaire de disposer des droits d'administration afin d'installer l'ensemble des composants relatifs à Metasploit.

2.1 Installation sous Linux ou OS X

En se rendant sur le GitHub officiel de Metasploit, il est possible d'y trouver des « **nightly installers** » (https://github.com/rapid7/metasploit-framework/wiki/Nightly-Installers). Ces installeurs pour **Windows**, **OS X** et **Linux** sont compilés une fois par jour et mis à disposition par Rapid7.

Ces installeurs permettent ainsi de simplifier au maximum l'installation en incluant l'ensemble des éléments nécessaires :

```
root@ubuntu:/tmp# curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/
master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall

  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  5532  100  5532    0     0   8381      0 --:--:-- --:--:-- --:--:--  8369
```

Le lecteur curieux ou ne souhaitant pas exécuter n'importe quel script sur sa machine pourra s'assurer que l'ensemble des données contenues au sein du fichier **msfinstall** permet d'installer l'ensemble des paquets nécessaires au bon fonctionnement du framework en fonction du système d'exploitation :

```
root@ubuntu:/tmp# tail -n 21 msfinstall
if [ "$ID" -ne 0 ]; then
 if ! hash sudo 2>/dev/null; then
   echo "This script must be executed as the 'root' user or with sudo"
   exit 1
 else
   echo "Switching to root user to update the package"
   sudo -E $0 $@
   exit 0
 fi
fi

case $PKGTYPE in
 deb)
   install_deb
   ;;
 rpm)
```

```
    install_rpm
    ;;
 *)
    install_pkg
esac
```

Il ne reste plus qu'à donner les bonnes permissions sur le fichier et à l'exécuter :

```
root@ubuntu:/tmp# chmod 755 msfinstall
root@ubuntu:/tmp# ./msfinstall
Adding metasploit-framework to your repository list..OK
Updating package cache..OK
Checking for and installing update..
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
 metasploit-framework
0 upgraded, 1 newly installed, 0 to remove and 155 not upgraded.
[...]
Run msfconsole to get started
```

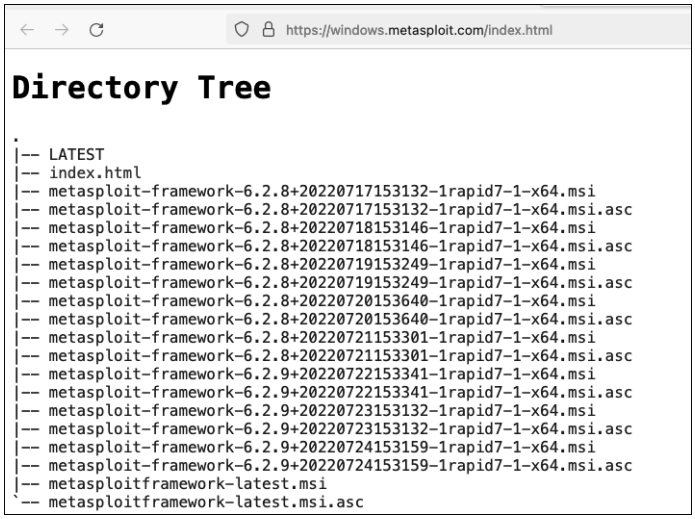
En revenant avec un compte sans privilège, il est maintenant possible d'exécuter **msfconsole** :

```
root@ubuntu:/tmp# exit
rsenet@ubuntu:~$ msfconsole

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`."".
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt

      =[ metasploit v5.0.15-dev-                         ]
+ -- --=[ 1870 exploits - 1059 auxiliary - 327 post       ]
+ -- --=[ 546 payloads - 44 encoders - 10 nops            ]
+ -- --=[ 2 evasion

msf6 >
```

2.2 Installation sous Windows

Qu'importe la date à laquelle vous lisez ce livre, il est possible de télécharger la dernière version du Framework Metasploit sur Windows à l'adresse suivante :
https://windows.metasploit.com/metasploitframework-latest.msi

De plus, les anciennes versions sur Windows sont également disponibles à l'adresse suivante : https://windows.metasploit.com/index.html.



Une fois la dernière version téléchargée, il est possible de l'installer en double cliquant sur le fichier **metasploitframework-latest.msi**.

Remarque

Dans le cas où vous n'auriez pas désinstallé votre protection antivirale, il est nécessaire de préciser à votre antivirus d'ignorer le dossier c:\metasploit (valeur par défaut à adapter en fonction de l'installation).

Néanmoins, il est possible que certaines fonctionnalités soient bloquées par la présence d'un antivirus. Il est donc recommandé de le désactiver entièrement.

L'installation se fait de manière assez classique, seuls certains points sont à prendre en compte. Seul le choix du dossier d'installation est important, car ce dernier doit coïncider avec le dossier qui ne sera pas analysé par un éventuel antivirus.

3. Utilisation alternative

Plutôt que de modifier la configuration de votre ordinateur, il est également possible de passer par des manières alternatives pour utiliser le Framework Metasploit. Pour cela, il est par exemple possible d'utiliser une machine virtuelle de type VirtualBox ou VMware ou encore un système de conteneur de type Docker. Dans les deux cas de figure précédents, il est alors possible de reprendre les installations précédemment abordées ou bien d'utiliser des systèmes clés en main.

3.1 Les systèmes d'exploitation orientés sécurité

Dans le cas où l'installation de Metasploit semble trop fastidieuse, il est possible d'utiliser des systèmes d'exploitation orientés sécurité tels que Parrot Security OS, BlackArch ou encore le très célèbre Kali.

Kali Linux est donc une distribution Linux orientée sécurité, basée sur le système d'exploitation Debian. L'objectif de Kali est de fournir aux professionnels de la sécurité des systèmes d'information, une distribution contenant l'ensemble des outils nécessaires pour mener à bien tout type d'audit.