Utilisation Optimale du

MetaSploit Framework

Groupe NT securite

OSSIR

Jérôme ATHIAS

Présentation

C:\>whoami

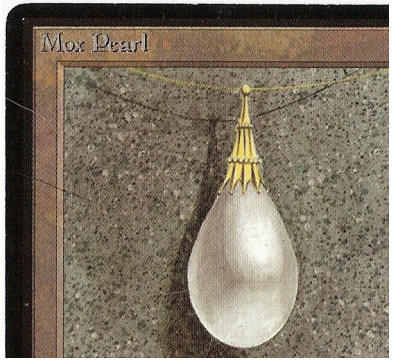
Analyste-programmeur en province
Passionné de sécurité : autodid*hack*te
Présence dans différentes mailinglists / forums
Site: https://www.securinfos.info

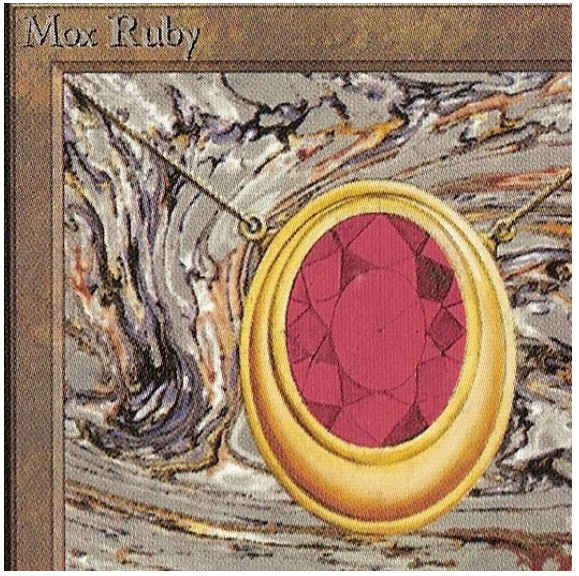
SECURINFOS

Introduction

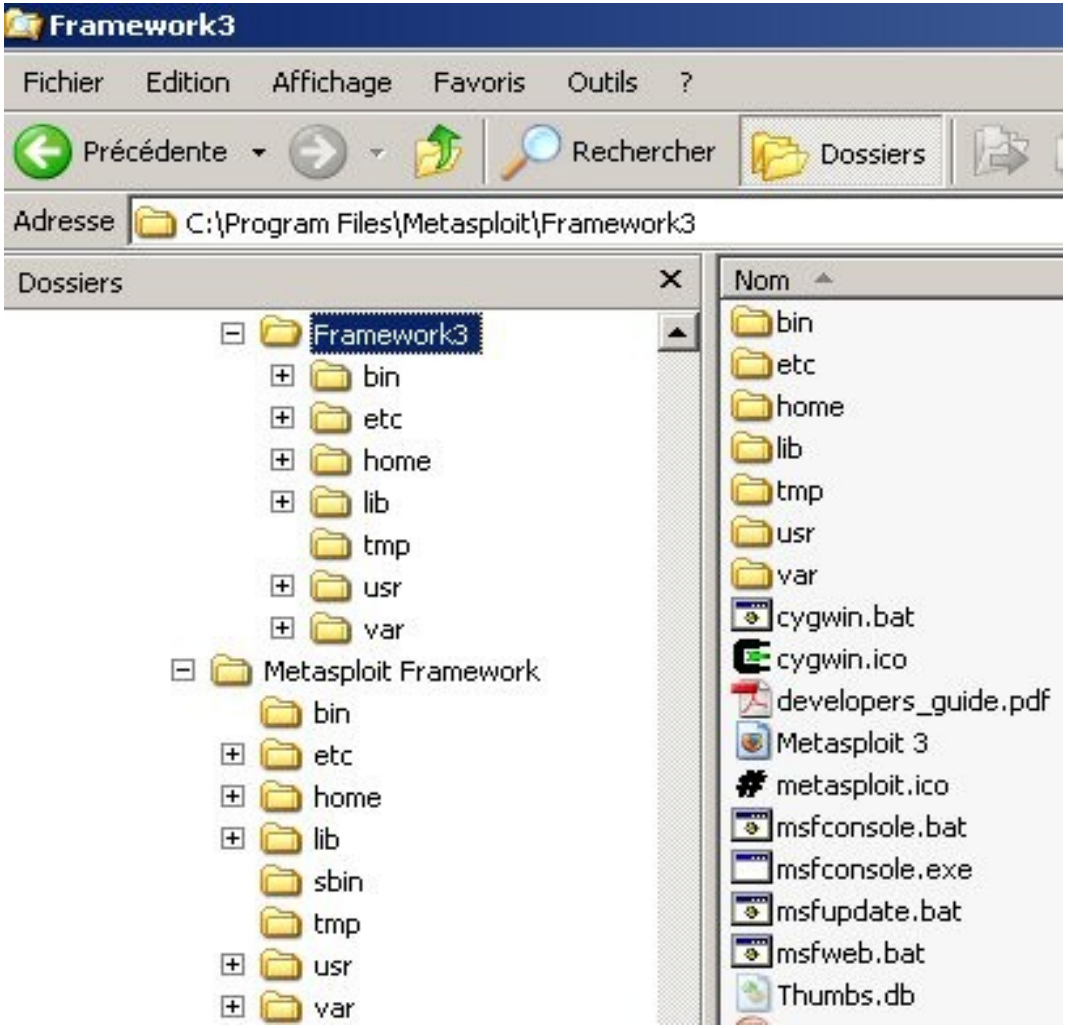
Le METASPLOIT FRAMEWORK, c'est quoi?

Une plateforme de tests d'intrusion
Version 2.x : PERL
Version 3.x : RUBY



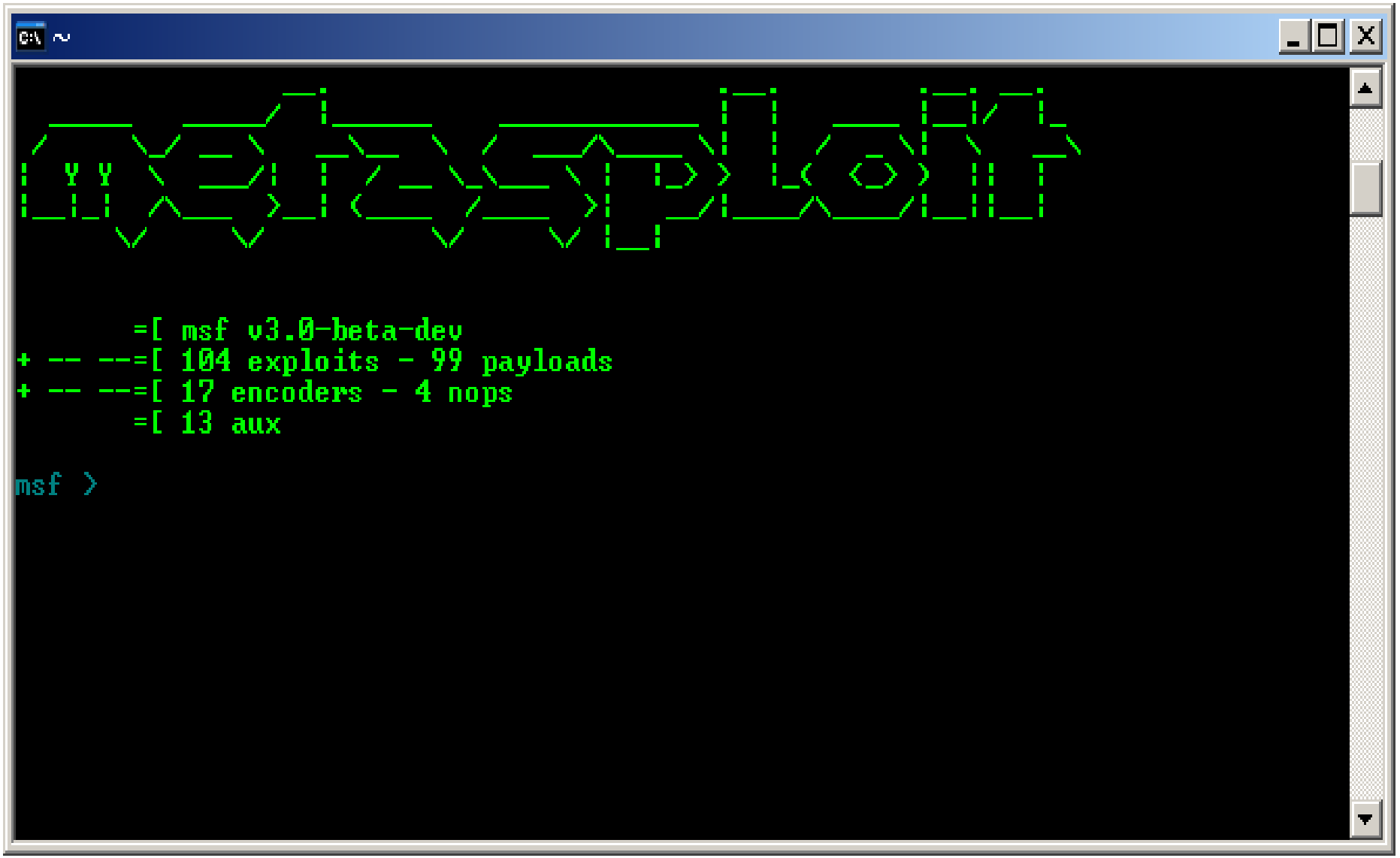


Arborescence



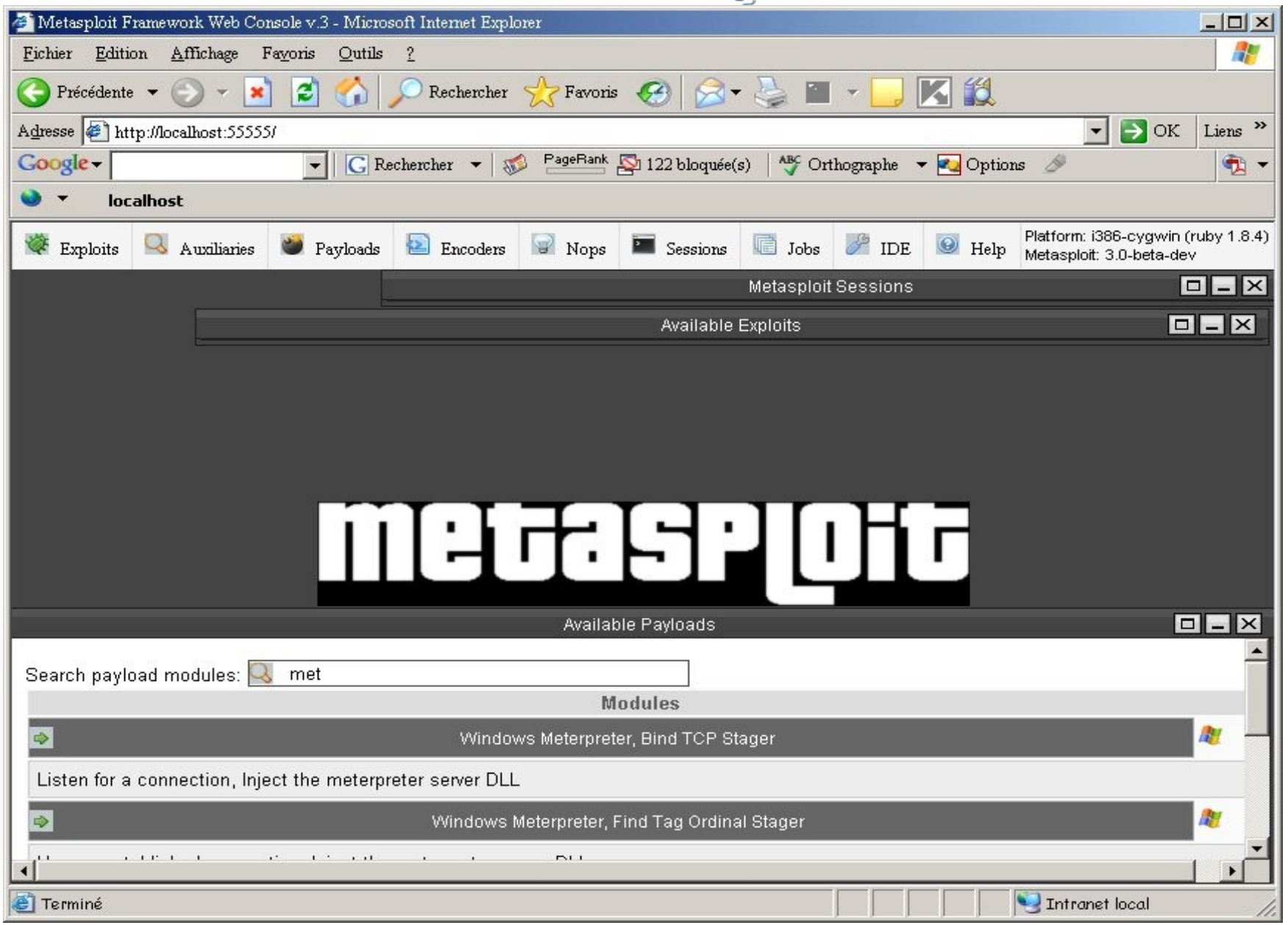
Interfaces

Console



Interfaces

Web

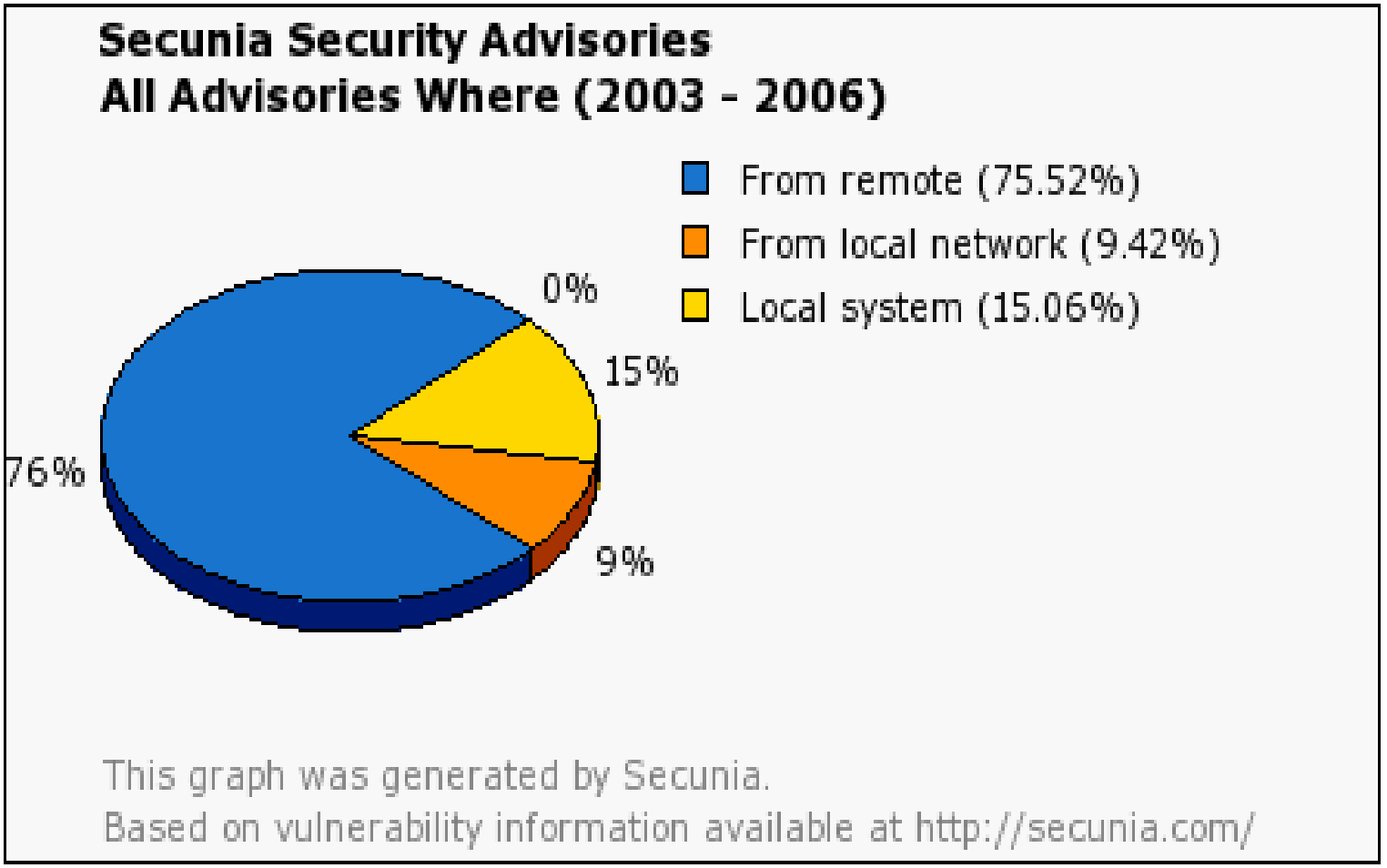


Processus d'Exploitation

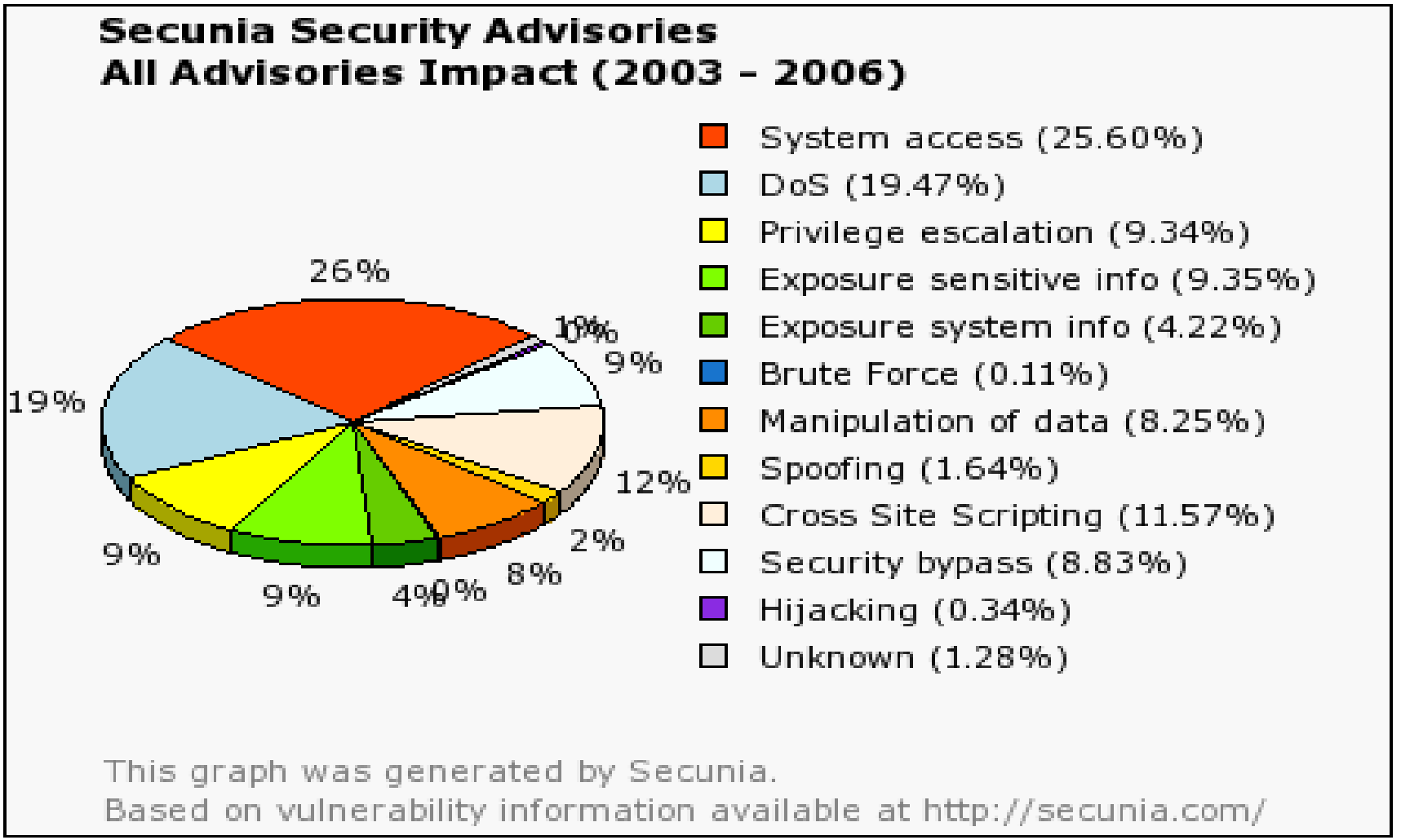
Exploitation globale classique:

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



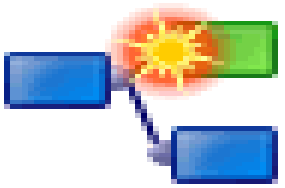
Détection – identification des failles

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

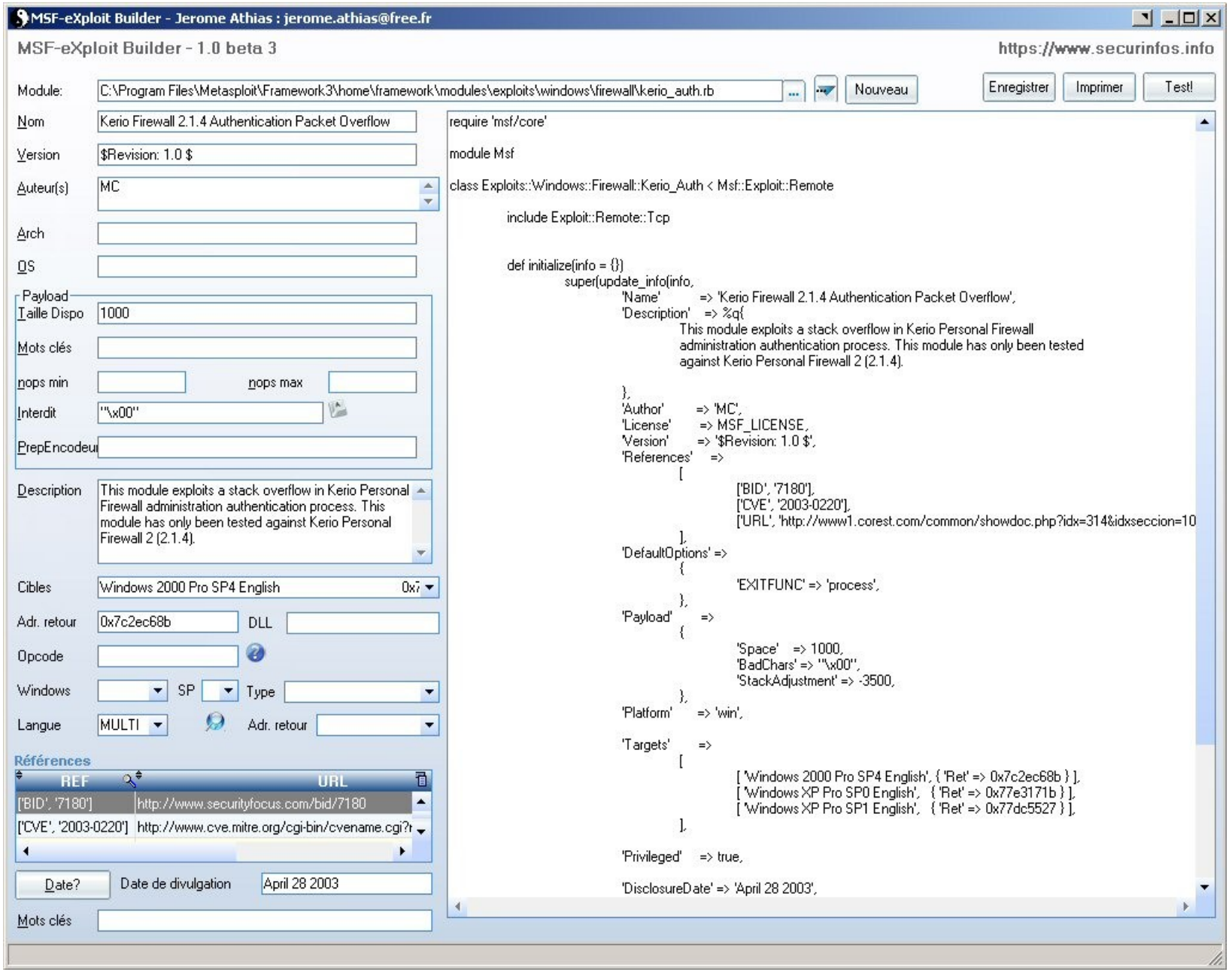
Obligation de modifier l'adresse de retour dans le code d'un module exploit pour une cible non-US, « obligation » de recharger le MSF pour prise en compte de cette modification d'adresse.

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

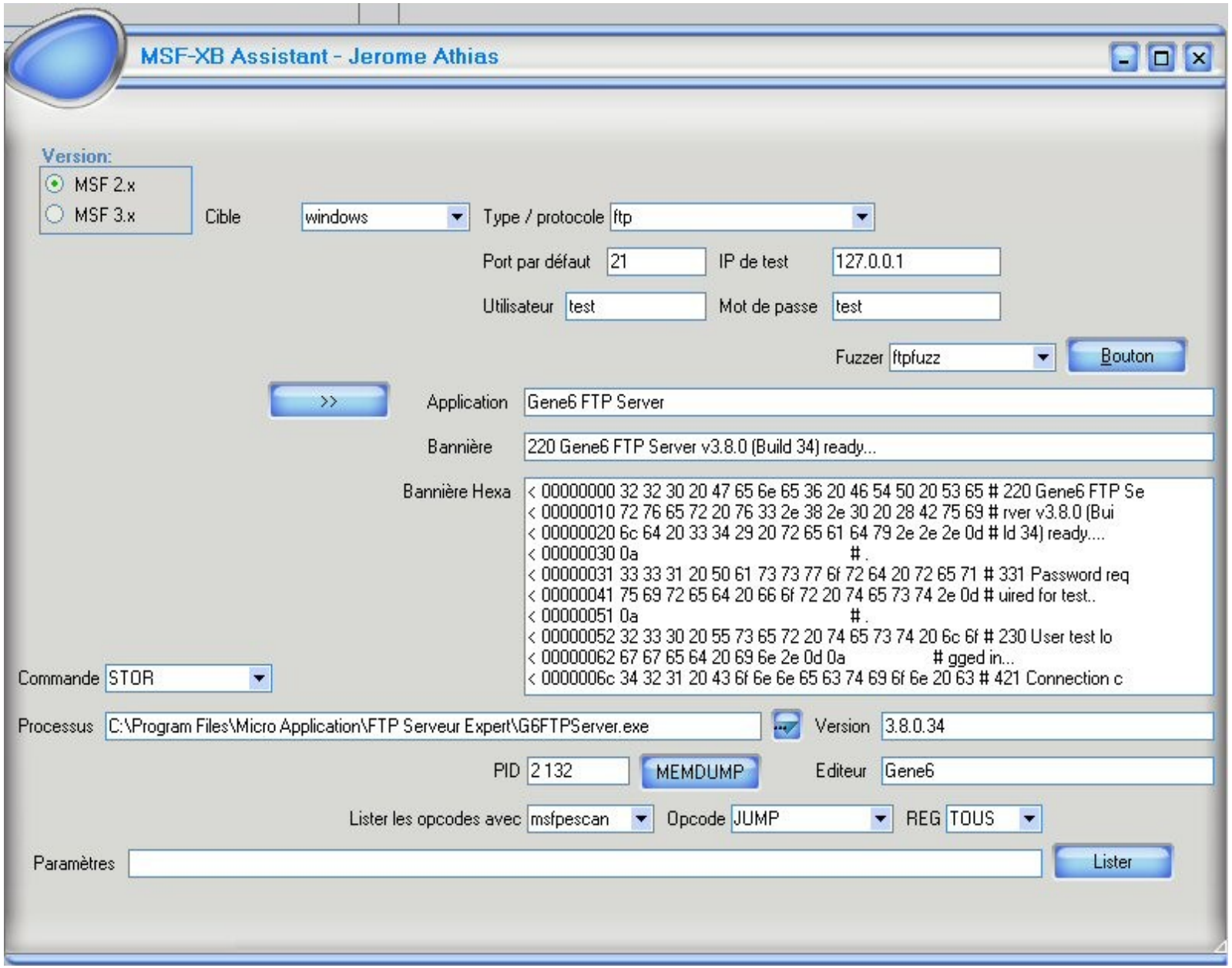
THEXPLOITER

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

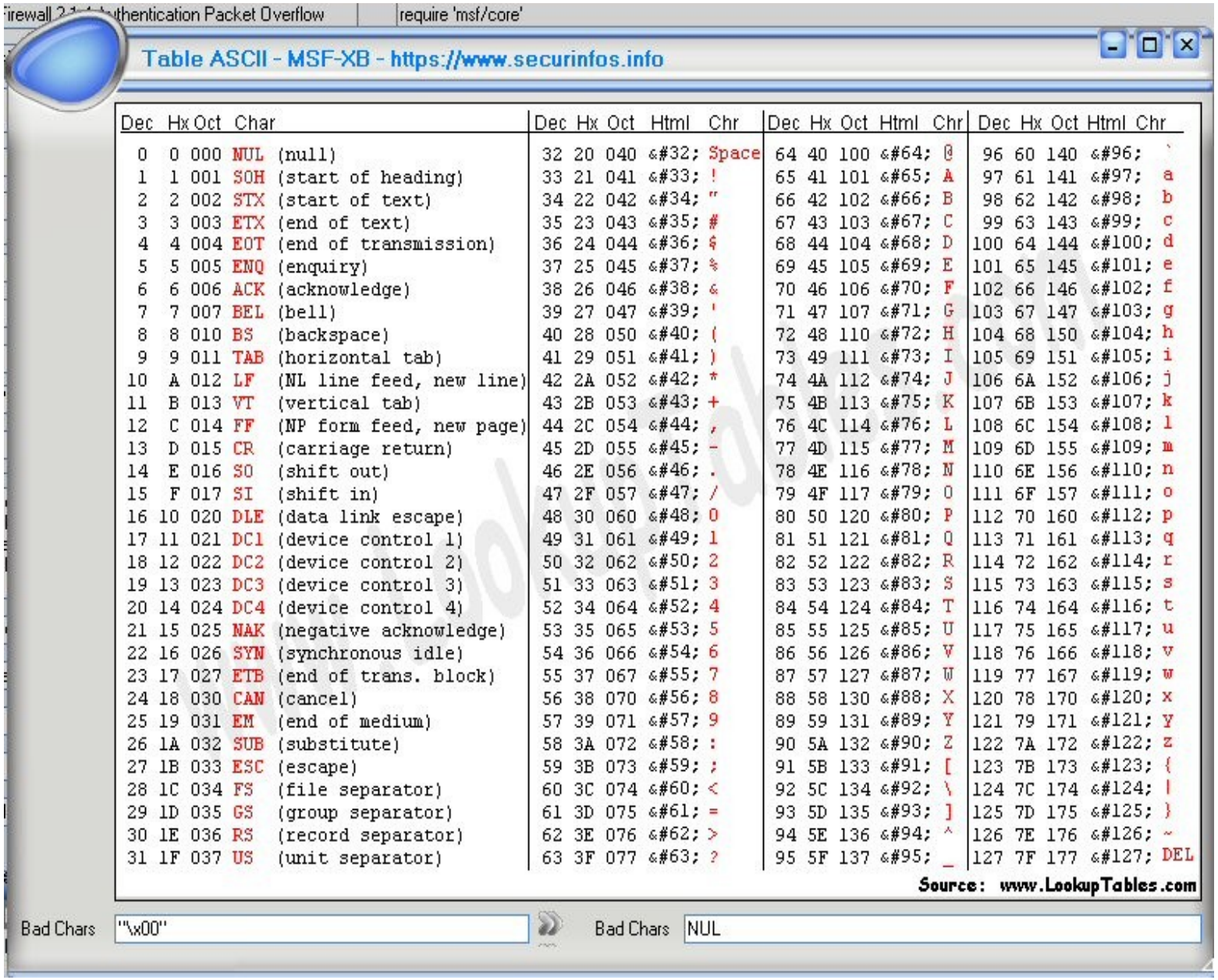
Editeur d'exploit



Assistant

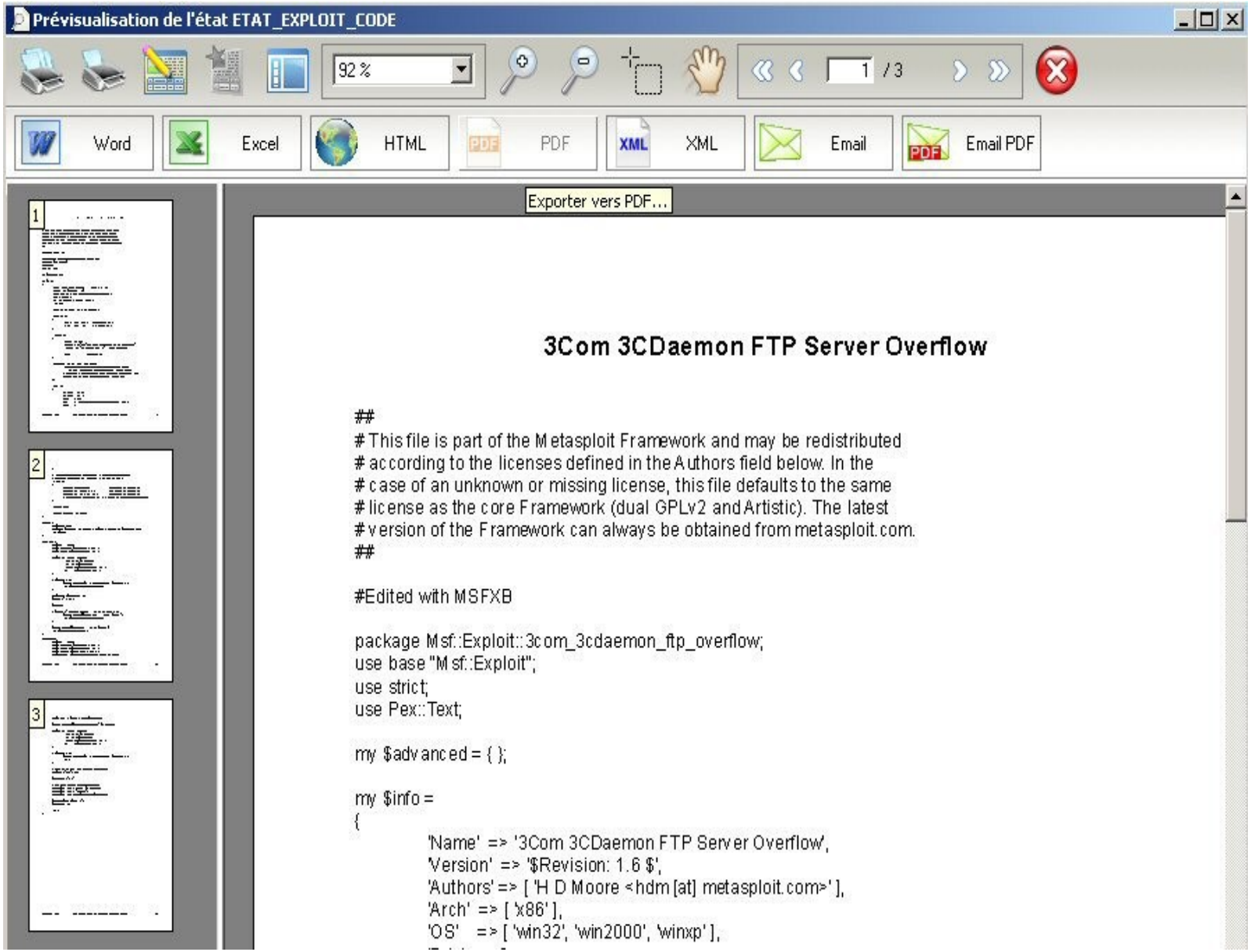

MSF-XB Assistant - Jerome Athias
Version:
MSF 2.x
MSF 3.x
Cible
windows
Type / protocole
ftp
Port par défaut
21
IP de test
127.0.0.1
Utilisateur
test
Mot de passe
test
Fuzzer
ftpfuzz
Bouton
>>
Application
Gene6 FTP Server
Bannière
220 Gene6 FTP Server v3.8.0 (Build 34) ready...
Bannière Hexa
< 00000000 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...

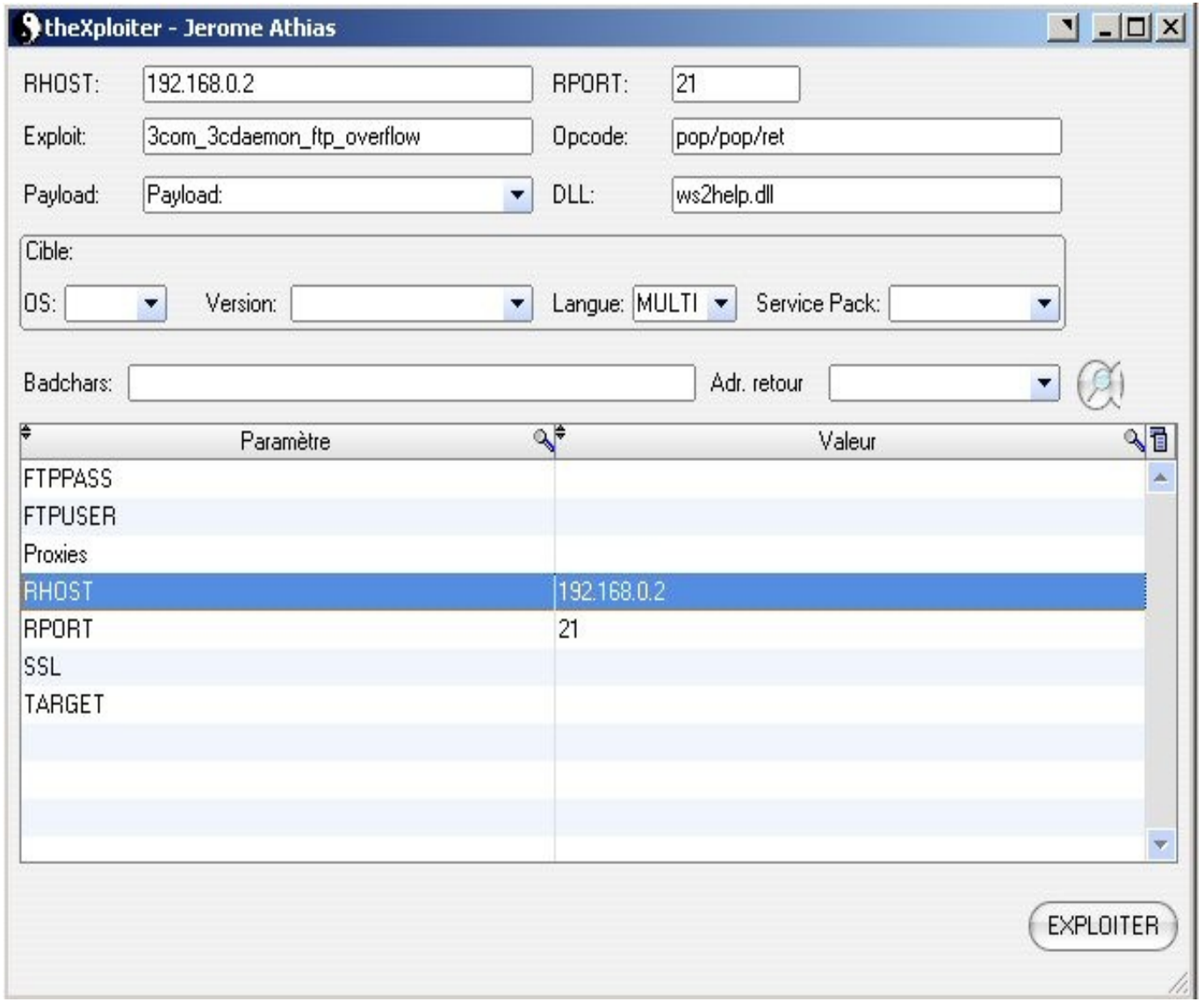


Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of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

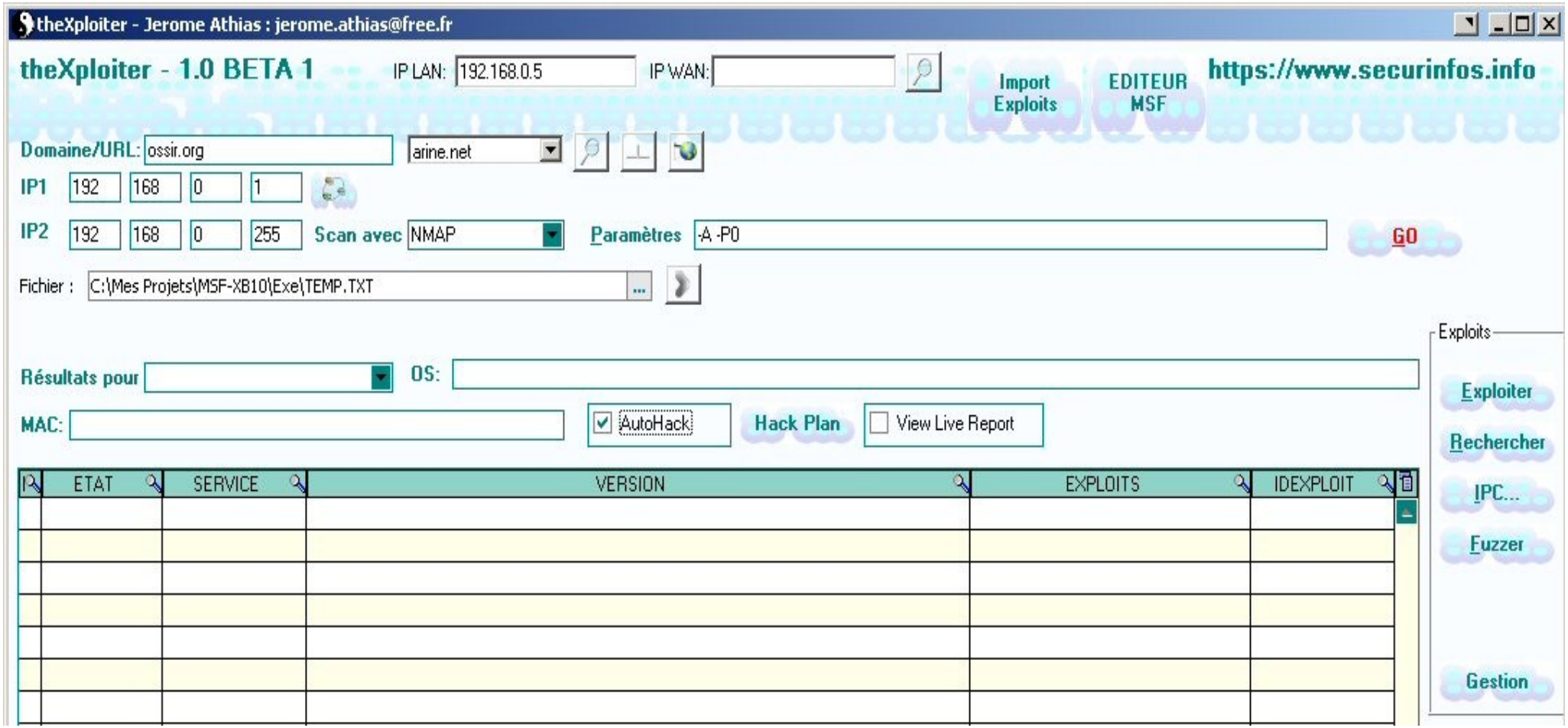
Outils : impression



Outils : testeur d'exploit



THEXPLOITER



Exploit - Entêtes - Jerome Athias : jerome.athias@free.fr

2

<< < > >>

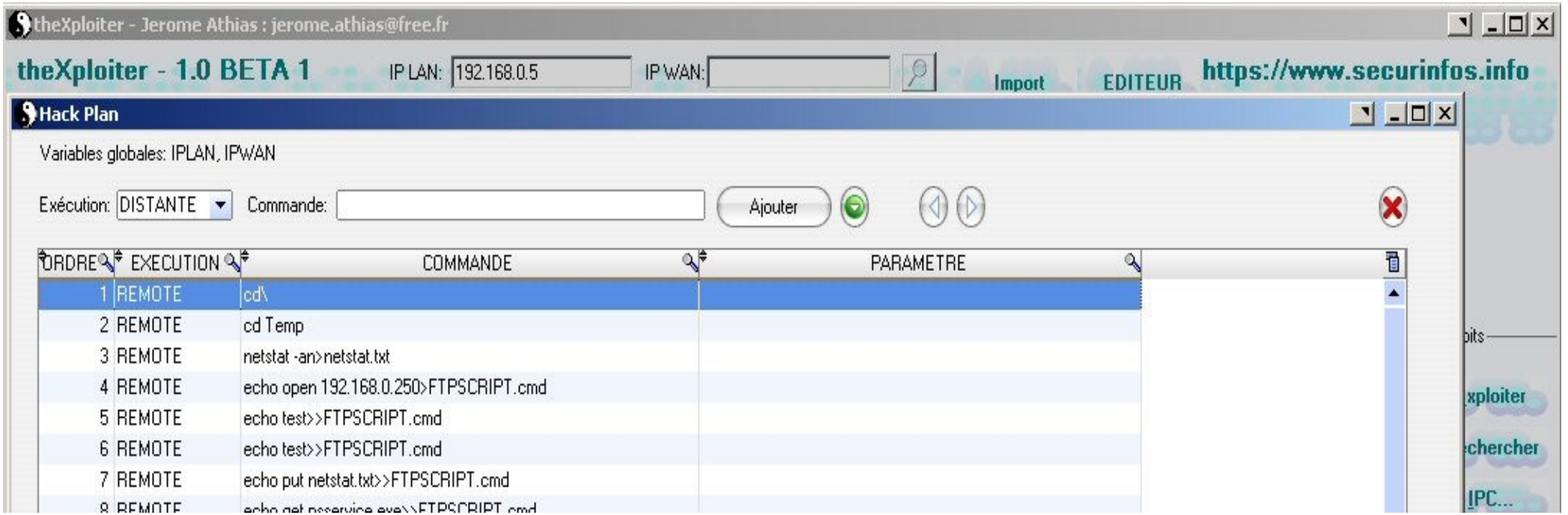
Nom_fichier 3com_3cdaemon_ftp_overflow.pm

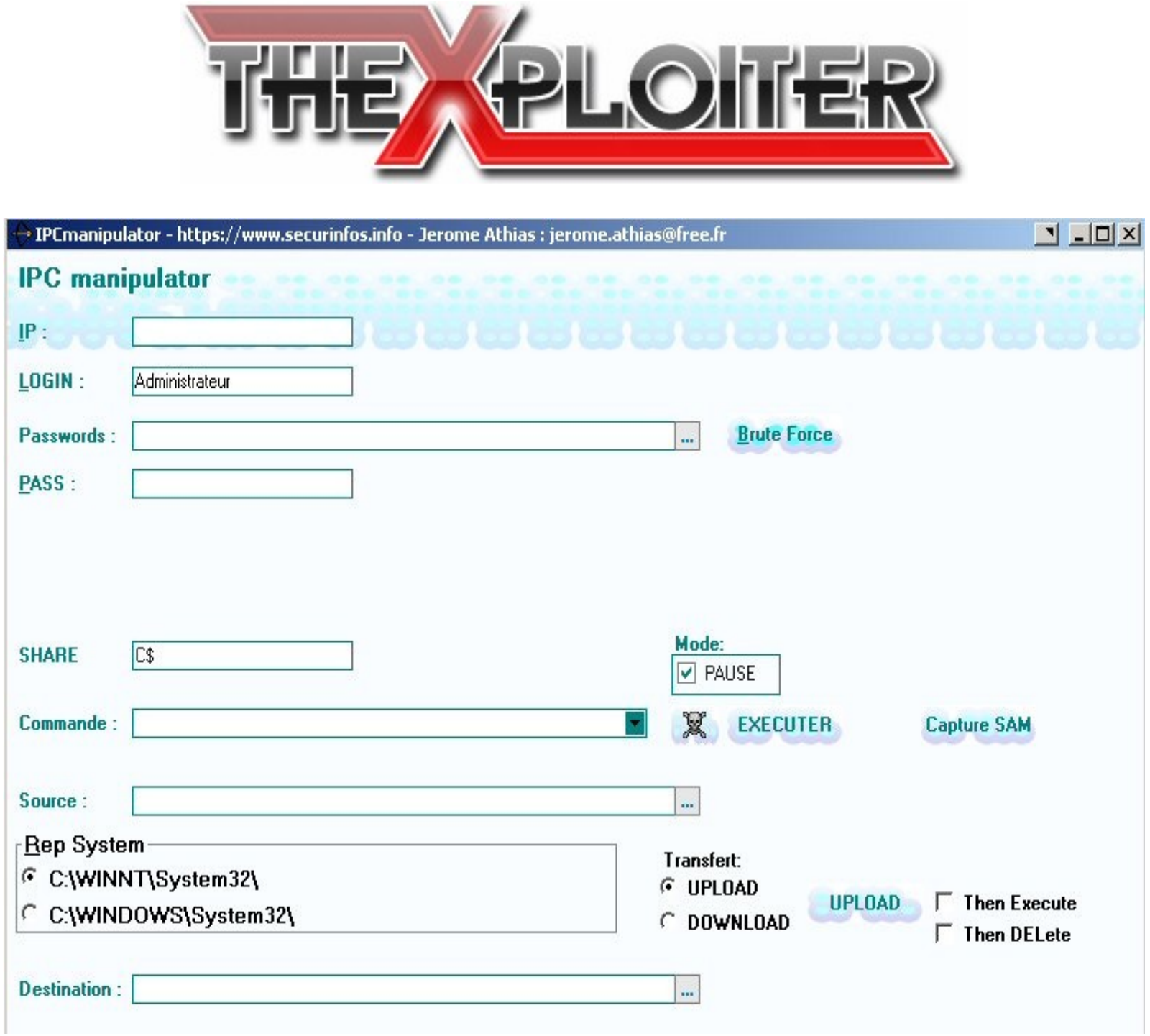
HEADER

Libellé	IDEXPLOIT
3Com 3CDaemon FTP Server Version	2
3Com 3CDaemon ftpd 2.0	2
3Com 3CDaemon	2

Supprimer

THEXPLOITER




IPCmanipulator - https://www.securinfos.info - Jerome Athias : jerome.athias@free.fr
IPC manipulator
IP :
LOGIN :
Administrateur
Passwords :
Brute Force
PASS :
SHARE
C$
Mode:
PAUSE
Commande :
EXECUTER
Capture SAM
Source :
Rep System
C:\WINNT\System32\
C:\WINDOWS\System32\
Transfert:
UPLOAD
DOWNLOAD
UPLOAD
Then Execute
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 dédicacée à mon grand-père Robert qui nous a quittés le 08/10/2006.