



RootMe
-hacking platform-

Extrait du Root Me : plateforme d'apprentissage dédiée au Hacking et à la Sécurité de l'Information

<https://www.root-me.org/fr/Documentation/Applicatif/Buffer-Overflow-et-shellcodes-sous-windows>

Buffer Overflow et shellcodes sous windows

- fr - Documentation - Applicatif -

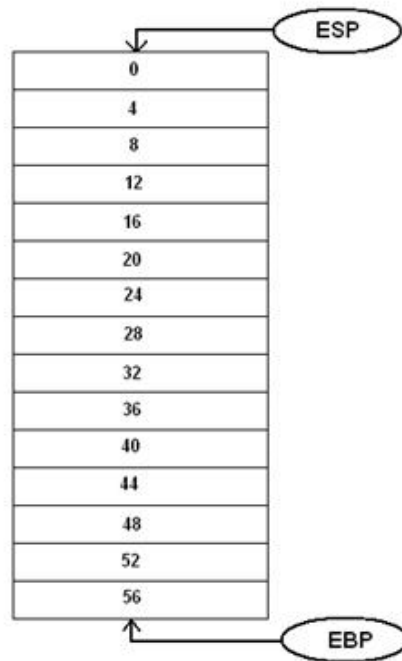


Date de mise en ligne :

Description :

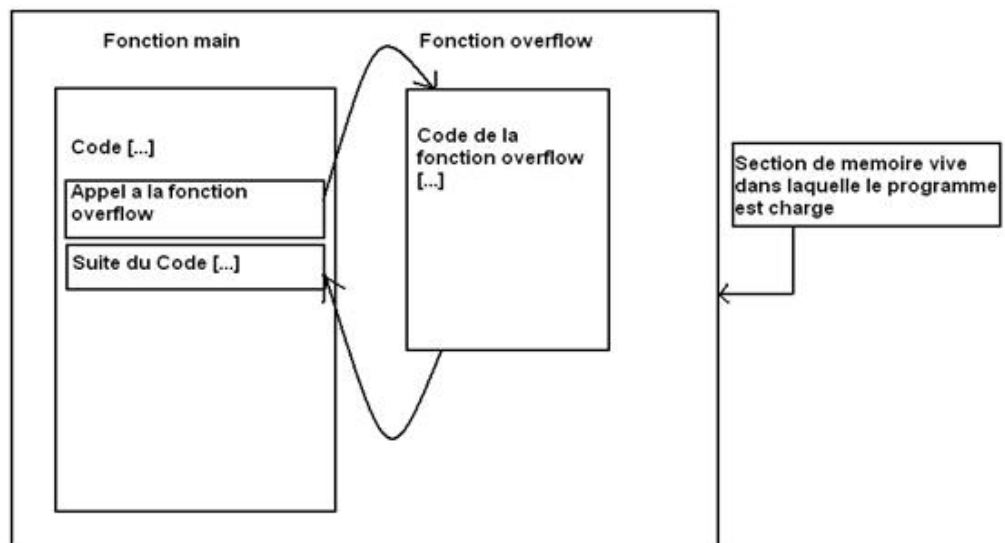
Copyright © Root Me : plateforme d'apprentissage dédiée au Hacking et à la
Sécurité de l'Information - Tous droits réservés

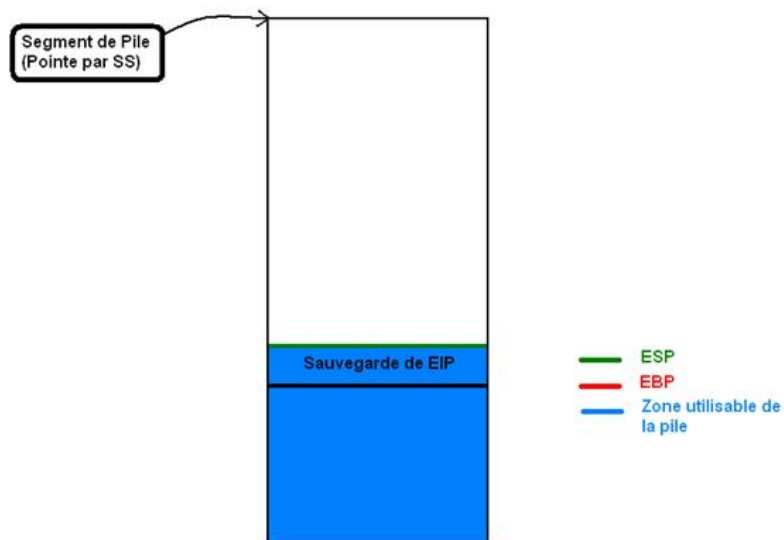
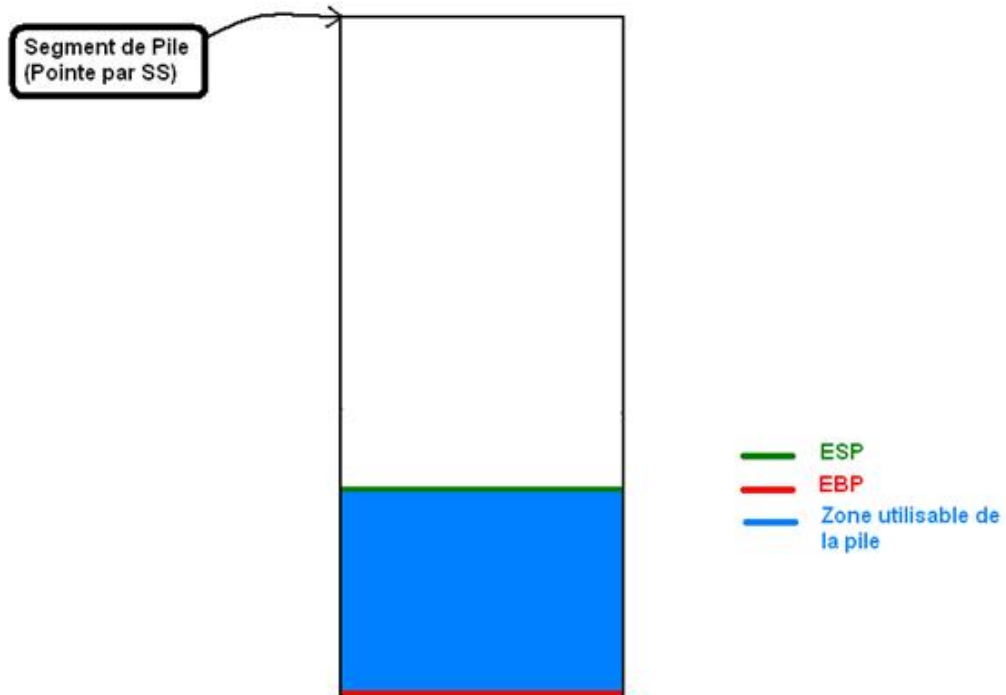
- ▶
- ▶
- ▶
- ▶
- ▶
- ▶
- ▶
- ▶
- ▶
- ▶
- ▶
- ▶
- ▶
- ▶

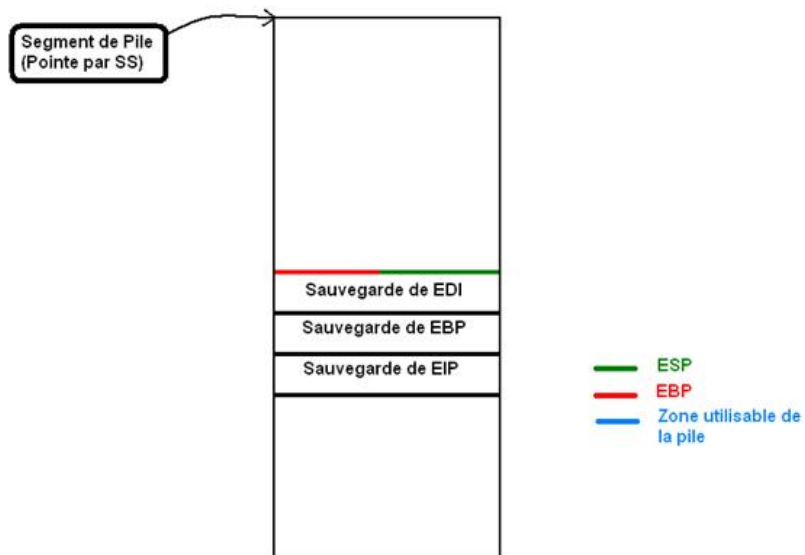
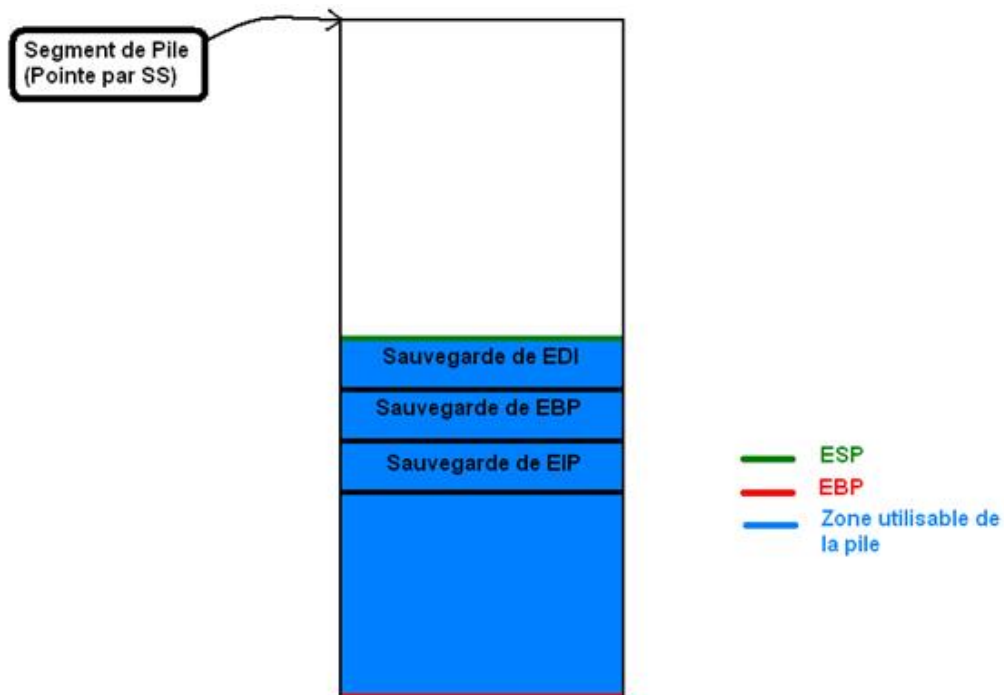


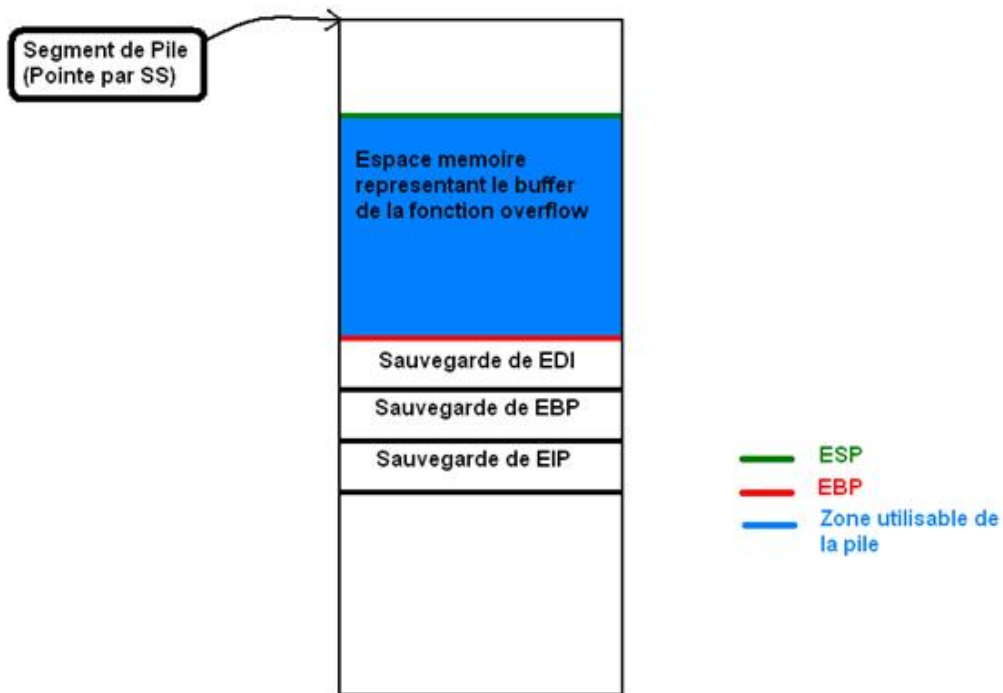
►
►
►
►

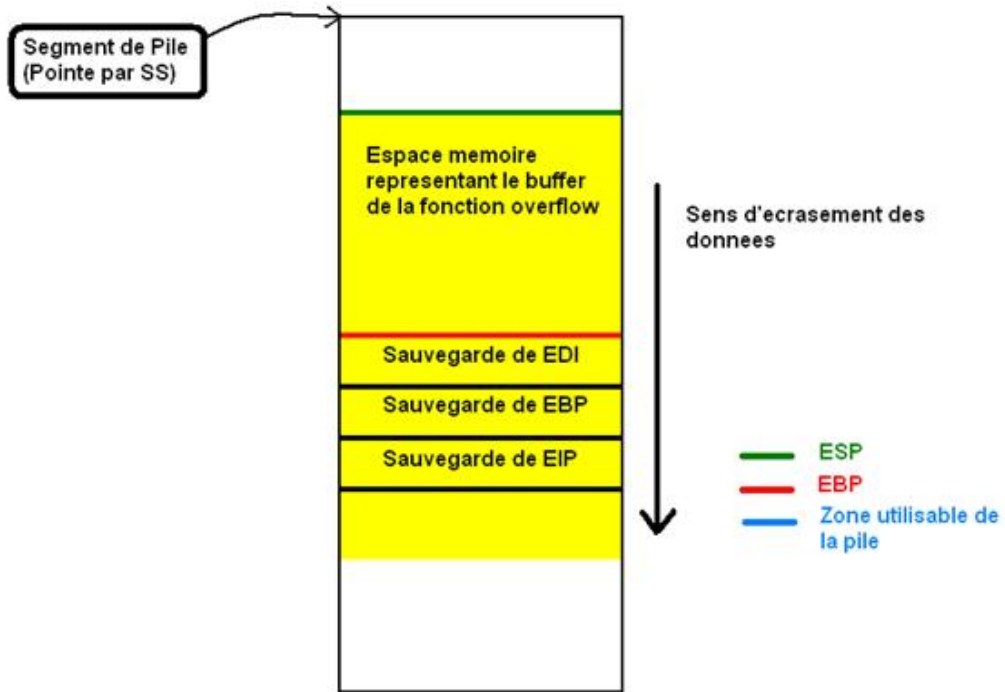
►
►
►
►
►
►
►

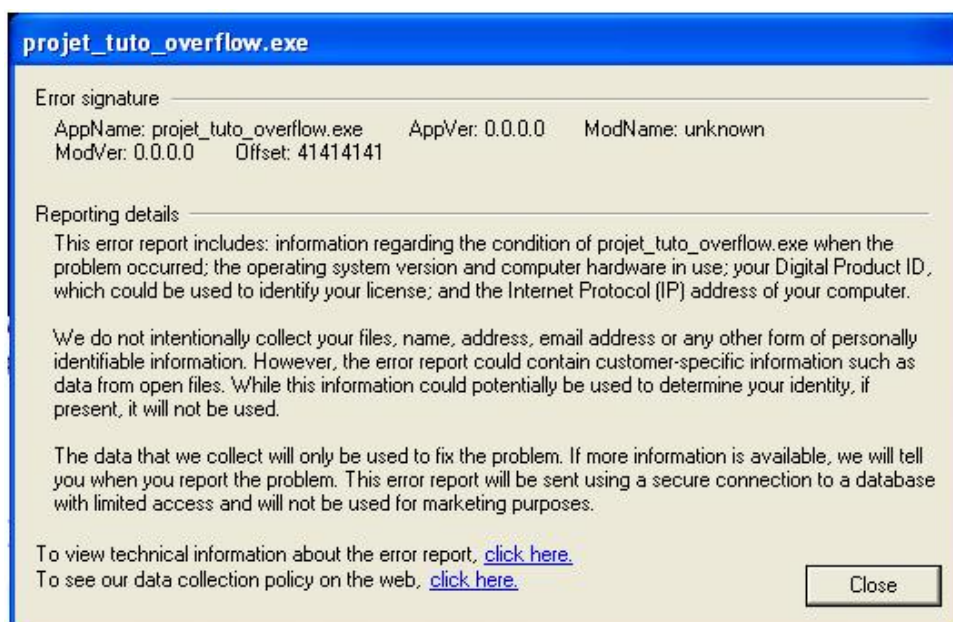


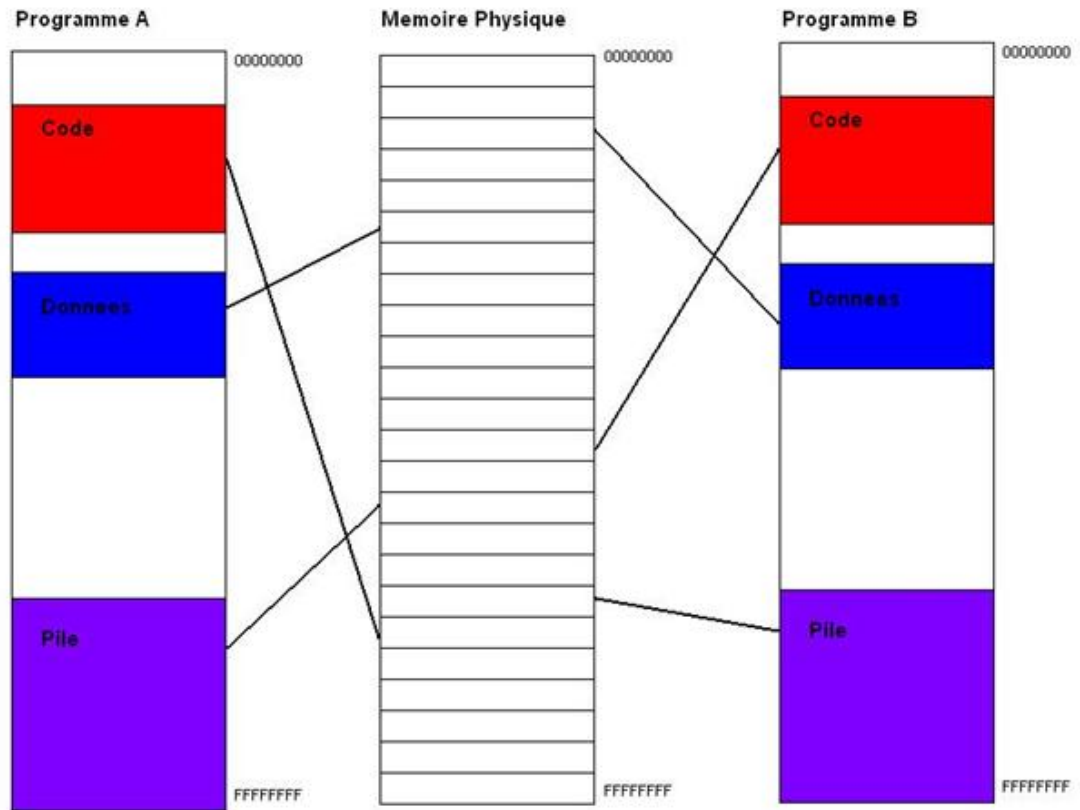


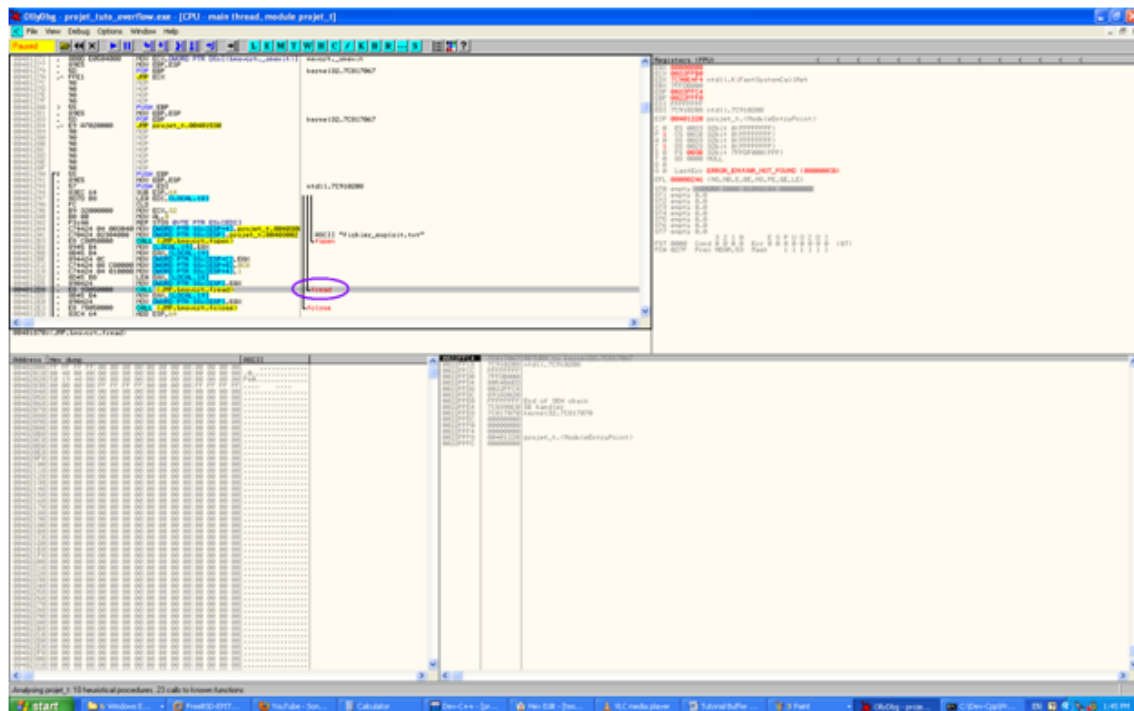










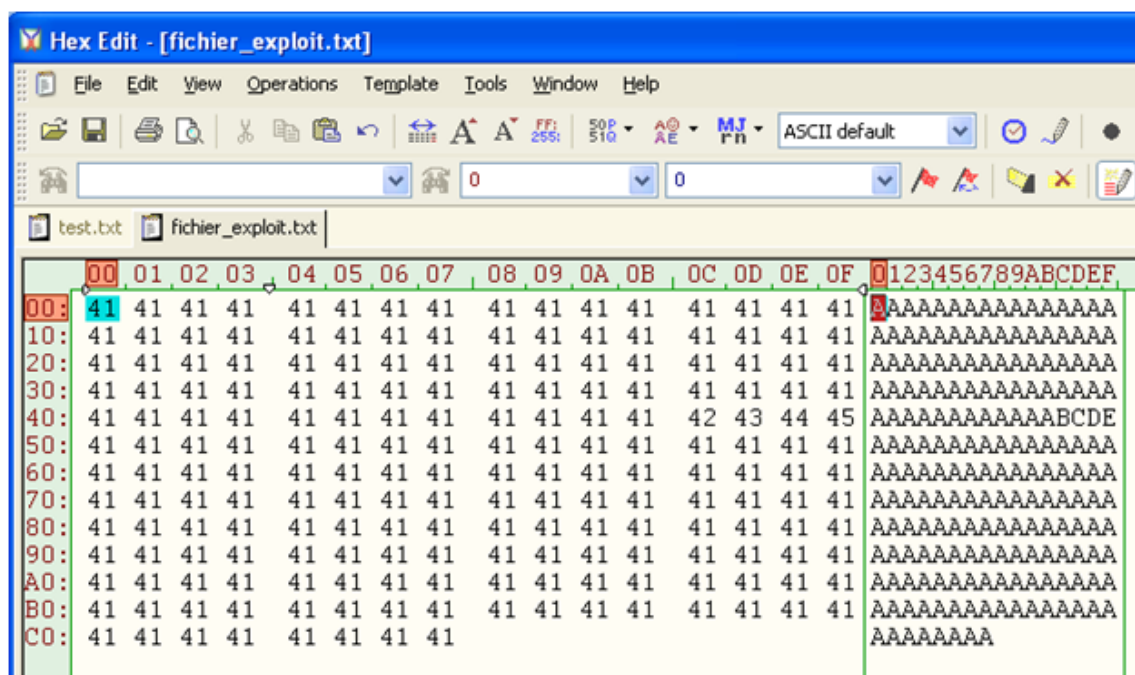
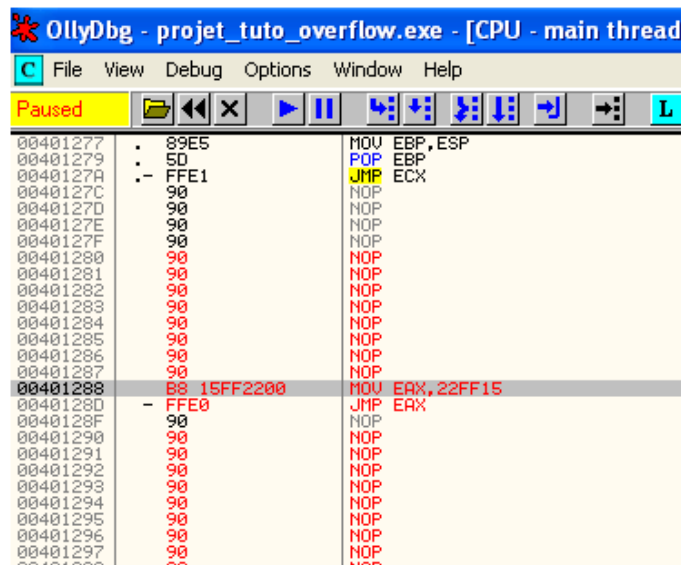


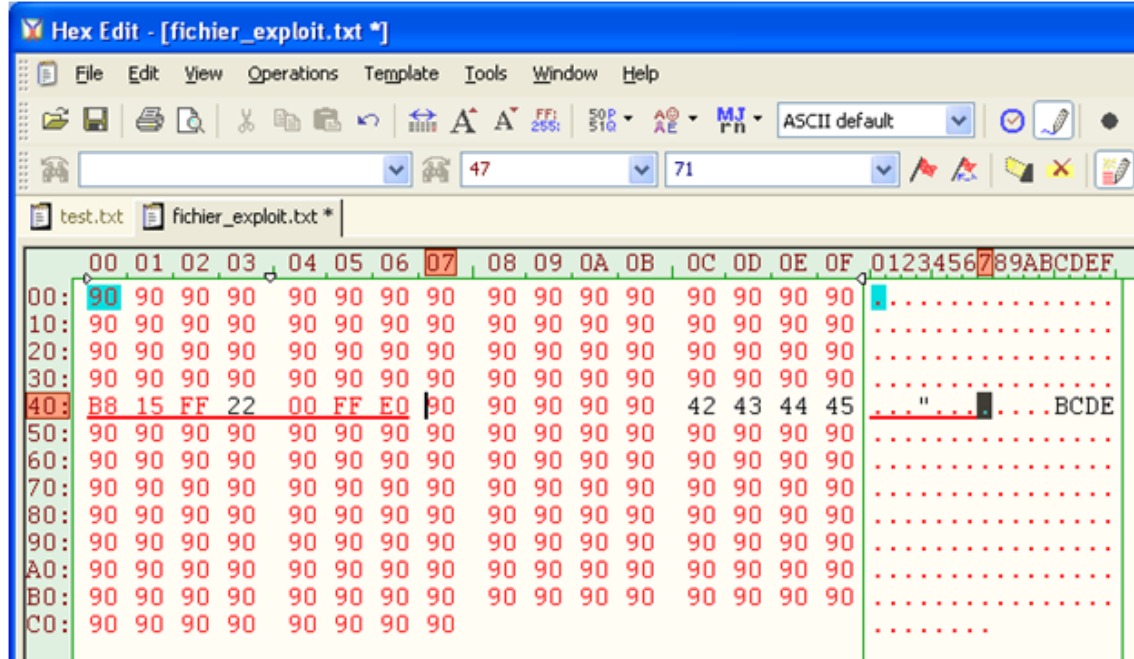
0022FEF0	0022FF10	ptr = 0022FF10
0022FEF4	00000001	size = 1
0022FEF8	000000C8	n = C8 (200.)
0022FEFC	77C5FCE0	stream = msvrt.77C5FCE0
0022FF00	0022FF3C	
0022FF04	77C39D60	msvrt.77C39D60
0022FF08	00000008	
0022FF0C	77C5FCE0	msvrt.77C5FCE0
0022FF10	00000000	
0022FF14	00000000	
0022FF18	00000000	
0022FF1C	00000000	
0022FF20	00000000	
0022FF24	00000000	
0022FF28	00000000	
0022FF2C	00000000	
0022FF30	00000000	
0022FF34	00000000	
0022FF38	00000000	
0022FF3C	00000000	
0022FF40	77C30000	msvrt.77C30000
0022FF44	00401370	projet_t.00401370
0022FF48	0022FF58	
0022FF4C	00401456	projet_t.00401456
0022FF50	00401370	projet_t.00401370
0022FF54	7C910208	ntdll.7C910208
0022FF58	0022FF78	
0022FF5C	0040131D	RETURN to projet_t.0040131D from projet_t.00401290
0022FF60	77C3A000	RETURN to msvrt.77C3A000 from msvrt.77C3B75C
0022FF64	7C910208	ntdll.7C910208
0022FF68	003E2AB0	
0022FF6C	00401313	RETURN to projet_t.00401313 from projet_t.00401770
0022FF70	0000003A	
0022FF74	00000010	
0022FF78	0022FFB0	
0022FF7C	004011E7	RETURN to projet_t.004011E7 from projet_t.004012EE
0022FF80	00000001	
0022FF84	003E24F0	
0022FF88	003E2AB0	
0022FF8C	00404000	ASCII "≡\$>"

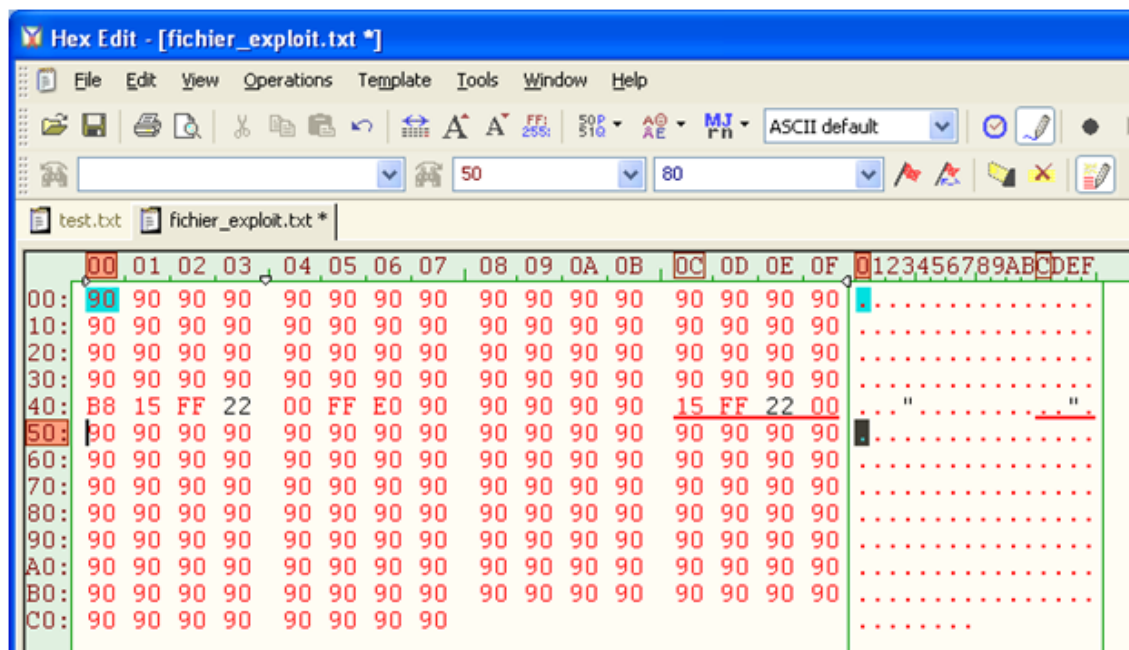
0022FEF0	• 0022FF10	ptr = 0022FF10
0022FEF4	• 00000001	size = 1
0022FEF8	• 000000C8	n = C8 (200.)
0022FEFC	• 77C5FCE0	stream = msvrt.77C5FCE0
0022FF00	• 0022FF3C	msvrt.77C39D60
0022FF04	• 77C39D60	
0022FF08	• 00000008	
0022FF0C	• 77C5FCE0	msvrt.77C5FCE0
0022FF10	• 00000000	
0022FF14	• 00000000	
0022FF18	• 00000000	
0022FF1C	• 00000000	
0022FF20	• 00000000	
0022FF24	• 00000000	
0022FF28	• 00000000	
0022FF2C	• 00000000	
0022FF30	• 00000000	
0022FF34	• 00000000	
0022FF38	• 00000000	
0022FF3C	• 00000000	
0022FF40	• 77C30000	msvrt.77C30000
0022FF44	• 00401370	projet_t.00401370
0022FF48	• 0022FF58	
0022FF4C	• 00401456	projet_t.00401456
0022FF50	• 00401370	projet_t.00401370
0022FF54	• 7C910208	ntdll.7C910208
0022FF58	• 0022FF78	
0022FF5C	• 0040131D	RETURN to projet_t.0040131D from projet_t.00401290
0022FF60	• 77C30000	77C30000
0022FF64	• 7C910208	RETURN to msvrt.77C30000 from msvrt.77C30000
0022FF68	• 003E2AB0	ntdll.7C910208
0022FF6C	• 00401313	RETURN to projet_t.00401313 from projet_t.00401770
0022FF70	• 0000003A	
0022FF74	• 00000010	
0022FF78	• 0022FFB0	
0022FF7C	• 004011E7	RETURN to projet_t.004011E7 from projet_t.004012EE
0022FF80	• 00000001	
0022FF84	• 003E24F0	
0022FF88	• 003E2AB0	
0022FF8C	• 00404000	ASCII "=\$>"

0022FEF0	• 0022FF10	ASCII 41,"AA
0022FEF4	• 00000001	
0022FEF8	• 000000C8	
0022FEFC	• 77C5FCE0	ASCII "":>"
0022FF00	• 0022FF3C	ASCII 41,"AA
0022FF04	• 77C39D60	msvrt.77C39D60
0022FF08	• 00000008	
0022FF0C	• 77C5FCE0	ASCII "":>"
0022FF10	• 41414141	
0022FF14	• 41414141	
0022FF18	• 41414141	
0022FF1C	• 41414141	
0022FF20	• 41414141	
0022FF24	• 41414141	
0022FF28	• 41414141	
0022FF2C	• 41414141	
0022FF30	• 41414141	
0022FF34	• 41414141	
0022FF38	• 41414141	
0022FF3C	• 41414141	
0022FF40	• 41414141	
0022FF44	• 41414141	
0022FF48	• 41414141	
0022FF4C	• 41414141	
0022FF50	• 41414141	
0022FF54	• 41414141	
0022FF58	• 41414141	
0022FF5C	• 41414141	
0022FF60	• 41414141	
0022FF64	• 41414141	
0022FF68	• 41414141	
0022FF6C	• 41414141	
0022FF70	• 41414141	
0022FF74	• 41414141	
0022FF78	• 41414141	
0022FF7C	• 41414141	
0022FF80	• 41414141	
0022FF84	• 41414141	
0022FF88	• 41414141	
0022FF8C	• 41414141	
0022FF90	• 41414141	
0022FF94	• 41414141	
0022FF98	• 41414141	
0022FF9C	• 41414141	
0022FFA0	• 41414141	
0022FFA4	• 41414141	
0022FFA8	• 41414141	
0022FFAC	• 41414141	
0022FFB0	• 41414141	
0022FFB4	• 41414141	
0022FFB8	• 41414141	
0022FFBC	• 41414141	


```
0022FEF0 • 0022FF10 ASCII 41,"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
0022FEF4 • 00000001
0022FEF8 • 000000C8
0022FEFC • 77C5FCE0 msvcrt.77C5FCE0
0022FF00 • 0022FF3C ASCII 41,"AAAAAAAAAAAAAAAAAAAAAAAAAAAAABCDAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
0022FF04 • 77C39D60 msvcrt.77C39D60
0022FF08 • 00000000
0022FF0C • 77C5FCE0 msvcrt.77C5FCE0
0022FF10 • 41414141
0022FF14 • 41414141
0022FF18 • 41414141
0022FF1C • 41414141
0022FF20 • 41414141
0022FF24 • 41414141
0022FF28 • 41414141
0022FF2C • 41414141
0022FF30 • 41414141
0022FF34 • 41414141
0022FF38 • 41414141
0022FF3C • 41414141
0022FF40 • 41414141
0022FF44 • 41414141
0022FF48 • 41414141
0022FF4C • 41414141
0022FF50 • 41414141
0022FF54 • 41414141
0022FF58 • 41414141
0022FF5C • 45444342
0022FF60 • 41414141
0022FF64 • 41414141
0022FF68 • 41414141
0022FF6C • 41414141
0022FF70 • 41414141
0022FF74 • 41414141
0022FF78 • 41414141
0022FF7C • 41414141
0022FF80 • 41414141
0022FF84 • 41414141
0022FF88 • 41414141
0022FF8C • 41414141
0022FF90 • 41414141
```







0022FF5C	0022FF15
0022FF60	90909090
0022FF64	90909090
0022FF68	90909090
0022FF6C	90909090
0022FF70	90909090
0022FF74	90909090
0022FF78	90909090
0022FF7C	90909090
0022FF80	90909090
0022FF84	90909090
0022FF88	90909090
0022FF8C	90909090
0022FF90	90909090
0022FF94	90909090
0022FF98	90909090
0022FF9C	90909090
0022FFA0	90909090
0022FFA4	90909090
0022FFA8	90909090
0022FFAC	90909090
0022FFB0	90909090
0022FFB4	90909090
0022FFB8	90909090
0022FFBC	90909090
0022FFC0	90909090
0022FFC4	90909090
0022FFC8	90909090
0022FFCC	90909090
0022FFD0	90909090
0022FFD4	90909090
0022FFD8	0022FFC8
0022FFDC	831A1728
0022FFE0	FFFFFFFF
0022FFE4	7C839AC0
0022FFE8	7C817070
0022FFEC	00000000
0022FFF0	00000000
0022FFF4	00000000
0022FFF8	00401220
0022FFFC	00000000

End of SEH chain
SE handler:
kernel!32.7C817070

projet_t.<ModuleEntryPoint>

