ENEE457 – Computer Systems Security
Project 1 Rubric

The project has been divided into 2 parts:

(1) ***Buffer Overflow Attack Lab*** – tasks 1 to 5
(2) ***Return-to-libc Attack Lab*** – tasks 1 to 4. The 5th task is optional and bonus points will be assigned.

Task #	Description	Points
Buffer Overflow Attack Lab (55 points)		
1	Invoke the shellcode and provide description of observations when running 32-bit and 64-bit versions	5
2	Understanding the vulnerable program	2
3	Prepare a payload, save it inside *badfile* and provide explanation of the construction (i.e. how the values are decided)	10
	Gain a root shell after correctly implementing the exploit	5
4	Construct one payload that works for any buffer size within the range	10
	Provide description of method used and other evidence	3
5	Successfully launch attack on stack-L3	5
	Provide detailed description of method used and other evidence	15
Return-to-libc Attack Lab (45 points)		
1	Find the addresses of system() and exit()	3
2	Find the address of MYSHELL	1
3	Create a meaningful *badfile* and explain its structure (i.e. describe how you decide the values for X, Y and Z)	15
	Gain a root shell through BOF	10
	Repeat the attack without invoking exit() and explain	2
	Repeat the attack after lengthening the name of retlib and explain	2
4	Defeat shell's countermeasure through BOF	2
	Provide explanation of how you constructed your input	10
5	Exploit the buffer-overflow problem using ROP (BONUS)	+5
	TOTAL POINTS (excluding bonus):	**100**