**Quiz #2**

**Name**:

Q1: Given the buffer size of 5000 bytes, the SEH offset of 3400 bytes, and a shellcode that is 500 bytes in length, how would you construct the buffer overflow payload to overwrite the SEH and execute the shellcode? Consider the payload layout starting from the buffer’s beginning and moving towards the SEH. In your response, detail the content and the order of each component of the exploit payload, including any NOP sleds or other techniques you would use to ensure that the shellcode is executed when the SEH handler is triggered.

Answer:

* SEH offset is 3400, so NSEH offset will be 3400-4= 3396

The exploit will be:   
- CMD + 3396 \* “A” + NSEH + SEH + (5000-3396 -4 -4 )

-CMD + 3396 \* “A” + NSEH + SEH + 1596\* “B”

Now we can place the shellcode either in the pre SEH pad or the post one:   
- CMD + 2896 \* “A” + shellcode + NSEH + SEH + 1596\* “B”

-CMD + 3396 \* “A” + NSEH + SEH + +shellcode +1096\* “B”   
  
SEH= pop pop ret address   
NSEH = address to shellcode (or jump instruction)