****

**system security**

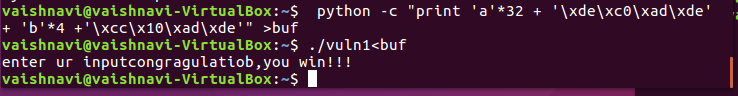
**Second periodical**

****

**VAISHNAVI V RAO**

**AM.EN.P2CSN19009**

1.



The output looks weird since I had to write it in virtual machine.

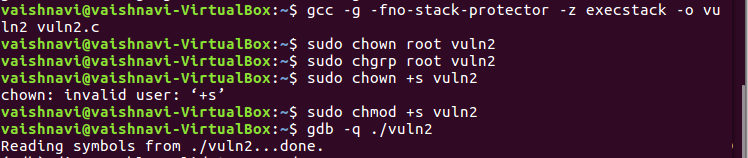
This is similar to assignment 1

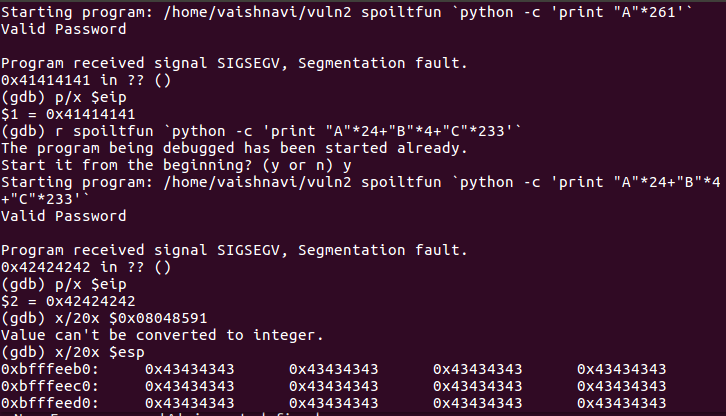
Disable aslr

Run gdb

Addresses are already given run the python script and exploit the program.

2.







We need to compile first all the commands sdisassemble aslr

Now run gdb

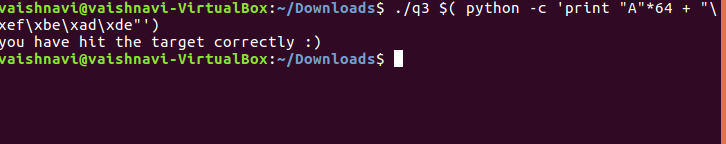
In the program we can see that return type is of strlen() is unsigned int whixh is stored in char data type hence any value greater than 255 causes integer overflow so when password length is 261 261 is wrapped and stored as 5. Hence through this we can bypass the boundary check.

We see in stack layout that return address is 0x18 hence user enters A-24 B4 C-233

We need to find the retun address

Put it in the script and run the program

3.



Here the placeholders accept the key in the form of %d and %n.formatting of one of these placeholders that will expand a single placeholder out into being 64 bytes wide. Whatever comes after this 64-byte placeholder will overwrite the memory above the buffer. we overwrite target with the target value from the if statement, we should get the printf hence give the above command.