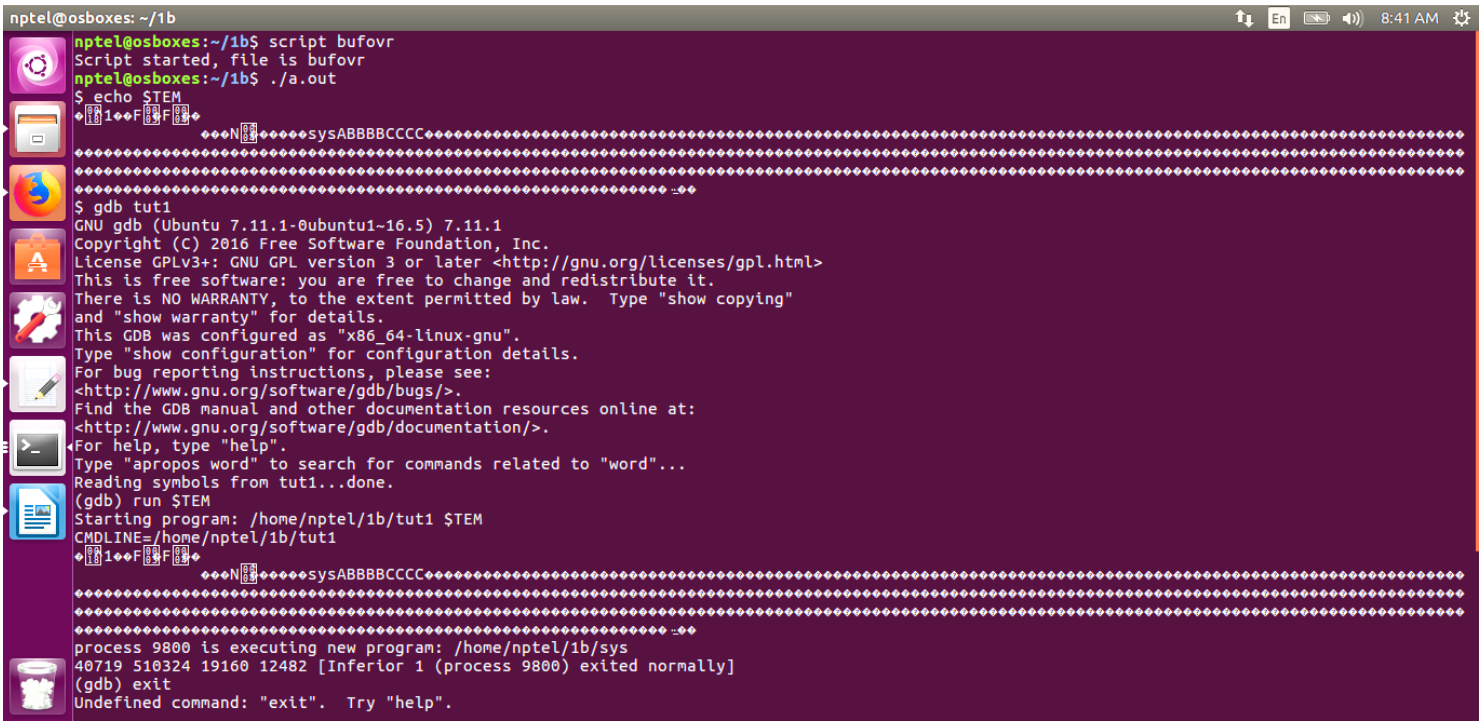
Assignment 1b

Rishabh Thakur, CS16B047 & Nipam Basumatary, CS16B111

The printargv.c program had a vulnerability in its mergecmdline() function. The vulnerability was the fixed sized of buffer declared but no limit on the copying to this buffer. This vulnerability was exploited using a buffer overflow attack.

The attack was designed so as to give a payload using command line argument which will overflow the function stack and replace the return address to the address of the payload which was already on the stack(stack was executable).

To achieve this a assembly level program was written which will call the sysinfo.c executable(sys) and hence print the server information. This program was translated to machine level program where there was no 00 instruction present. After doing this this was set as the payload and the rest of the buffer was copied with NOP instruction until the return address which was set to the address in the stack of this payload.



As seen from the above screenshot, first the program bufov.c is executed(a.out) which will have the desired argument as an environment variable(TEM).
Next, we run gdb and execute tut1(printargv.c) and give the argument as $TEM, which terminates on printing the 4 server states.