Reversing

GDB (debugging)

<http://egloos.zum.com/psyoblade/v/2653919>

<https://forum.tuts4you.com/>

run

list

break [source file name]:[line] // break bof.c:9

info breakpoints

condition 1 i==2

print i

[control] + x + a

next

step

quit

<strcpy function>

<gets function>

(python -c “print(‘\x90’ \* (size) + ‘\xbe\xba\xfa\xca’)” ; cat ) | ./bof

<binary file view>

xxd command