**实 验 报 告**



**Format String Server**

|  |  |
| --- | --- |
| **课程名称** | **软件安全** |
| **学 院** | **计算机科学技术学院** |
| **专 业** | **信息安全** |
| **姓 名** | **冉津豪** |
| **学 号** | **17307130179** |

**开 课 时 间 2019 至 2020 学年第 二 学期**

目录

[Pre-Task Turning Off Countermeasures 2](#_Toc40038355)

[Task 1: Finding out the addresses of libc functions 2](#_Toc40038356)

[Task 2: Putting the shell string in the memory 2](#_Toc40038357)

[Task 3: Exploiting the buffer-overflow vulnerability 3](#_Toc40038358)

[Task 4: Turning on address randomization 4](#_Toc40038359)

[Task 5: Defeat Shell’s countermeasure 4](#_Toc40038360)

# Pre-Task Turning Off Countermeasures

关闭地址空间随机化。

sudo sysctl -w kernel.randomize\_va\_space**=**0

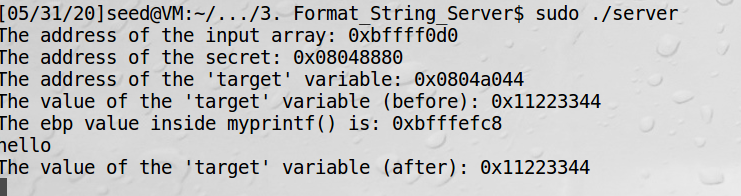
# Task 1: The Vulnerable Program

编译server.c, 定义DUMMY\_SIZE为200，并用ROOT运行。

gcc -DDUMMY\_SIZE**=**200 -z execstack -o server server.c

sudo ./server

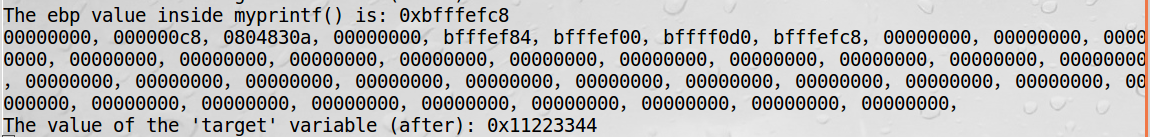
在另一个shell中，向Server发送hello。

**echo** hello **|** nc -u 127.0.0.1 9090

# Task 2: Understanding the Layout of the Stack

生成一个badfile，并发送到server，打印栈上的内容。

python -c 'print("%.8x，"\*40)' **>** badfile

nc -u 127.0.0.1 9090 **<** badfile

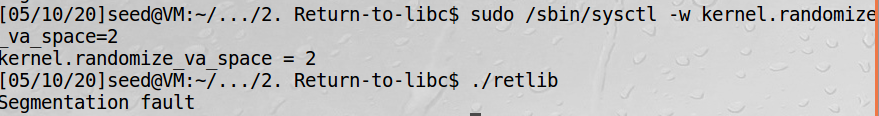
# Task 3: Crash the Program

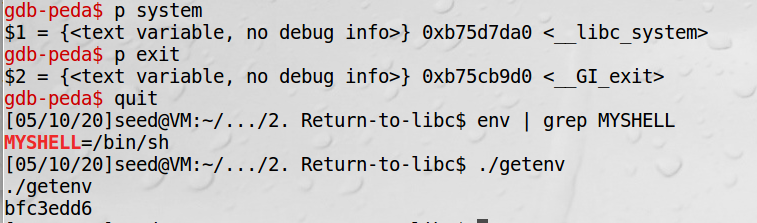
获取到需要的地址后，现在确定exploit中的XYZ。

# Task 4: Print Out the Server Program’s Memory

将地址随机化复原：

sudo /sbin/sysctl -w kernel.randomize\_va\_space**=**2

此时产生segmentation fault。

关闭gdb的禁用地址随机化后，查看所有地址，三者地址均与之前不同，所以攻击失效。

# Task 5: Change the Server Program’s Memory

# Task 6: Inject Malicious Code into the Server Program

# Task 7: Getting a Reverse Shell

# Task 8: Fixing the Problem