

# 实 验 报 告



课程名称 《网络攻击与防御技术》

学 院 计算机科学技术学院

专 业 信息安全

姓 名 黄 力

学 号 15307130275

开 课 时 间 2018 至 2019 学年第 1 学期

实验项目 名 称	Linux 本地栈溢出	成绩	
-------------	-------------	----	--

## 一、实验目的

- (1) 了解 C 语言程序中函数调用时程序栈的变化情况和栈溢出的基本原理
- (2) 通过实验掌握如何使用栈溢出获取带有 root 权限的 shell
- (3) 熟悉一些基本的 linux 命令，了解 linux 下的编程和调试基本工具。

## 二、实验内容

- (1) 在非 root 用户下利用 tryof.c 编译得到的 tryof 程序中的栈溢出漏洞和其具备 suid 标志位的属性获取具有 root 权限的 shell
- (2) 分析实验成功或失败的原因

## 三、实验环境

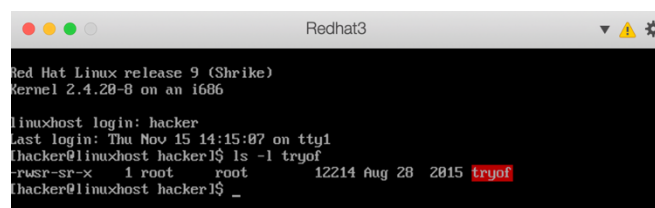
- (1) PC 机操作系统: macOS Mojave 10.14
- (2) 虚拟机操作系统 (Parallels Desktop 13.1.1): 32 位 redhat3

## 四、实验原理

通过阅读 tryof 程序的源代码 tryof.c 可以发现该程序的主要功能是将用户在命令行参数中给出的字符串使用 strcpy 函数拷贝到大小为 300 字节的 buf 中。在本实验中，程序开启了栈上内容可执行并关闭了栈地址随机化，结合 tryof 具备 suid 标志位的属性。为获得具有 root 权限的 shell，可以利用该栈溢出漏洞构造 shellcode 填充到程序栈中，并修改 strcpy 函数执行完后的返回地址至 shellcode 的起始地址使得程序从 strcpy 函数返回后继续执行构造的 shellcode 从而达到攻击。

## 五、实验步骤及结果

- (1) 从云复旦 <http://cloud.fudan.edu.cn/shareFolder/466220002/UHWpvrr> 中下载 redhat3.rar，解压并利用其中的虚拟硬盘在 Parallels Desktop 安装 redhat 操作系统获得实验环境，使用 hacker 作为登入帐号（无密）登入，登入目录为/home/hacker，在此目录中已有编译好的具备 suid 标志位的 tryof 程序。可使用 ls -l tryof 命令查看，结果如下图：



```

Redhat3
Red Hat Linux release 9 (Shrike)
kernel 2.4.29-8 on an i686

linuxhost login: hacker
Last login: Thu Nov 15 14:15:07 on tty1
hacker@linuxhost hacker$ ls -l tryof
-rwsr-sr-x 1 root root 12214 Aug 28 2015 tryof
hacker@linuxhost hacker$ _

```

- (2) 阅读 tryof.c 源码文件发现 buf 的大小为 300 字节，但由于程序中还定义了 ret 等其余变量，所以 buf 的溢出大小比 300 应该要大一点，但不会大太多。这里可以利用两种方法来得到产生 segment fault 的溢出大小值：第一种方法是使用 objdump -d tryof 命令查看 tryof 的汇编代码找到 strcpy 函数调用前给 %eax 寄存器赋值的大小（%eax 的值代表 buf 的地址），如下左图红圈所示，0x14c 也就是十进制的 332 即是溢出大小；第二种方法是使用二分法在尝试不同长度的字符串输入是否产生 segment fault 来判断，如下右图当使用 331 个 a 作为输入时不产生 segment fault，而使用 332 个 a 作为输入时则会产生 segment fault。



令编译得到攻击程序 `tryof_exploit`，然后使用 `./tryof_exploit` 命令运行攻击程序，结果如下图，获得 shell 后可以分别使用 `whoami` 和 `id` 命令验证结果，从下图中红圈部分可得知本次实验已经成功。

```
hacker@linuxhost hacker]$ gcc -o tryof_exploit tryof_exploit.c
tryof_exploit.c: In function 'main':
tryof_exploit.c:16: warning: assignment makes integer from pointer without a cast
hacker@linuxhost hacker]$ ./tryof_exploit
sp=bfffe2b8,buf=bfffe2d0,ret=bfffe40c,i=bfffe2ccsh-2.05b# whoami
root
sh-2.05b# id
uid=0(root) gid=101(hacker) groups=101(hacker)
sh-2.05b#
```

## 六、实验总结

通过本次实验，我理解了栈溢出的原理，并成功编写 `exploit` 程序利用该漏洞获得了具有 `root` 权限的 shell。本次实验的难点主要有两点：一是 shellcode 的编写，解决方法是借用了老师提供的 shellcode。二是 332 这个溢出值的寻找，解决方法是参考使用了参考资料 1 中的方法。

## 七、主要参考资料

- 1、<https://blog.csdn.net/tyskfs2/article/details/42318531>
- 2、<https://github.com/tinyclub/open-c-book/blob/master/zh/chapters/02-chapter5.markdown>
- 3、<https://blog.csdn.net/azloong/article/details/6158401>
- 4、<https://blog.csdn.net/raintungli/article/details/43865041>