**期末报告安装文档**

**王泽鹏 2017301510036**

**2020.6.26**

# 一、文档介绍

**1.实验环境：**

Ubuntu 32bit、服务端和客户端程序处于同一局域网下，其中服务端ip：10.0.2.5，客户端ip：10.0.2.4。

服务端和客户端需安装SSL服务，并进行无密连接的设置，客户端还需搭建一个ftp服务器。

**2.文件说明：**

压缩包解压得到：①server文件夹；②client文件夹；③设计文档；④安装说明文档。

其中，server文件夹存储服务端相关文件，包括server.c（服务端socket通信主程序代码）、server（服务端可执行程序）、rsa\_private\_key.pem（RSA解密使用的私钥）、decrypt\_file（RSA解密文件的py程序）。

client文件夹存储客户端相关文件，包括client.c（客户端socket通信主程序代码）、client（客户端可执行程序）、shellcode.h（头文件，包含客户端进行缓冲区溢出攻击时使用的shellcode）、create\_file.asm（编写创建文件shellcode的汇编代码）、reverse\_shell（编写获取服务端反弹shell的shellcode的汇编代码）、daemon.sh（自动查找包含姓名的文件并传输的shell脚本）、pubkey.pem（RSA加密使用的公钥）、encrypt\_file.py（RSA加密文件的py程序）。

**3.编译运行命令（在设计文档的演示部分都有截图，这里按文本形式列出）：**

**服务端首先要关闭ASLR地址随机化：**

sudo su

echo 0 > /proc/sys/kernel/randomize\_va\_space

**服务端编译server.c文件（栈可执行和关闭栈保护）：**

gcc -z execstack -fno-stack-protector server.c -o server

**客户端编译client.c文件：**

gcc client.c -o client

**客户端编译链接两个汇编代码：**

nasm -felf32 -o create\_file.o create\_file.asm

nasm -felf32 -o reverse\_shell.o reverse\_shell.asm

ld create\_file.o -o create\_file.asm

ld reverse\_shell.o -o reverse\_shell.asm

**获得机器码（shellcode）：**

objdump -d ./create\_file|grep '[0-9a-f]:'|grep -v 'file'|cut -f2 -d:|cut -f1-6 -d' '|tr -s ' '|tr '\t' ' '|sed 's/ $//g'|sed 's/ /\\x/g'|paste -d '' -s |sed 's/^/"/'|sed 's/$/"/g'

objdump -d ./reverse\_shell|grep '[0-9a-f]:'|grep -v 'file'|cut -f2 -d:|cut -f1-6 -d' '|tr -s ' '|tr '\t' ' '|sed 's/ $//g'|sed 's/ /\\x/g'|paste -d '' -s |sed 's/^/"/'|sed 's/$/"/g'

**客户端监听反弹shell命令：**

netcat -lvp 9999

**客户端在服务端反弹shell中运行shell脚本命令：**

sh daemon.sh

**服务端抓包命令：**

sudo su

tcpdump -i any -A |more

**客户端加密文件命令：**

python encrypt\_file.py wangzepeng.txt

**服务端解密文件命令：**

python decrypt\_file.py

**4.其他**

除打包提交的最终代码外，所有实验代码（包括之前的各种尝试的代码）将在6月27日（ddl）后上传到github，可供辅助检查。

附1：全部代码部分截图。



附2：项目github地址：<https://github.com/xiaopeng-whu/socket-buffer_overflow>