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	木马/后门编程	成绩	

一、实验目的

（1）通过本实验初步了解木马后门软件的原理。

二、实验内容

（1）编写一个简单的木马程序，接受客户端指令，并在目标主机上执行，最后将结果返回给客户端

（3）在（1）的基础上通过木马程序在目标主机上建立一个用户 Hacker, 密码设置为 HackerPWD，将 Hacker 添加到管理员组。并将程序设置为开机自动运行

（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）：64 位 Ubuntu18.04 Sever

四、实验原理

本次实验的原理很简单，我使用 Python2.7 作为编程语言，服务端代码为 server.py，客户端代码为 client.py，server.py 中创建套接字绑定 2333 端口等待客户端连接，在收到客户端发来的指令数据后执行该命令并将结果再发回客户端。目标主机使用 ubuntu 系统。

五、实验步骤及结果

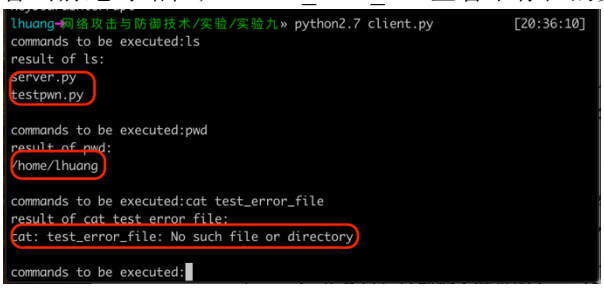
（1）编写服务端代码 server.py 与客户端代码 client.py，其中 server.py 的代码逻辑是：使用 commands 模块执行客户端的指令并将输出返回给客户端，client.py 的代码逻辑是：接受用户输入指令并将指令发给服务端然后输出服务端返回的结果。

（2）在目标主机（虚拟机）上运行服务端，在本机上运行客户端并与服务端交互：

1、在虚拟机中使用 python2 server.py 启动服务端

2、在本机上使用 python2.7 client.py 启动客户端

3、在客户端分别输入常见的 linux 命令发给服务端执行，以下选择了三个命令：ls 查看服务端当前文件夹下的文件；pwd 查看当前绝对路径；cat test_error_file 查看不存在的文件。结果如下图所示：



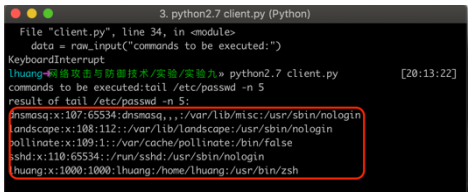
从 3 个红圈可以得知木马程序能够在目标主机上执行 shell 命令并正确返回结果

（3）通过木马程序在目标主机上建立一个新用户 Hacker, 密码设为 HackerPWD，并添加到 root 组。

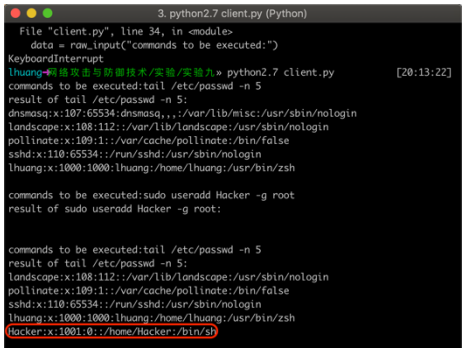
1、在虚拟机中使用 python2 server.py 启动服务端

2、在本机上使用 python2.7 client.py 启动客户端

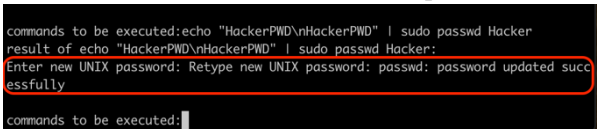
3、在客户端输入 tail /etc/passwd -n 5 查看服务端的/etc/passwd 文件，确认 Hacker 用户不存在，结果如下图：



4、在客户端输入 sudo useradd Hacker -g root 添加一个新用户 Hacker 并设置其组别为 root，然后输入 tail /etc/passwd -n 5 查看服务端的/etc/passwd 文件，Hacker 用户已经成功添加，结果如下图红圈所示：



5、在客户端输入 echo “HackerPWD\nHackerPWD” | sudo passwd Hacker 为 Hacker 用户设置密码为 HackerPWD，此处巧妙使用了管道将 echo 的输出作为 sudo passwd Hacker 的输入，结果如下图：



从红圈可以看出设置密码已经成功。

6、在客户端输入 id Hacker 查看 Hacker 用户的信息，结果如下图：uid 为 1001，gid 为 0，组别为 root

（4）设置 server 程序在目标主机开机自启动：若目标主机为 linux 系统，有两种方法：第一种方法是在 /etc/rc.local 文件中添加一行：python2 /home/lhuang/server.py &，&将 server 作为后台程序运行，不在 shell 中输出结果。第二种方法是编写一个 shell 脚本文件 auto_server.sh，内容为 python2 /home/lhuang/server.py,最后在/etc/profile 中添加 auto_server.sh 的绝对路径，目标主机在开机时会执行 /etc/profile 中的程序从而启动木马服务端。若目标主机为 windows 系统，则需要修改注册表（详见参考资料）。

六、实验总结

通过本次实验，我初步了解了木马后门程序的实现原理，并编写了一个 naïve 的木马程序，成功利用该程序在服务端完成了本次实验要求的添加新用户的任务。本次实验没有难点。比较巧妙的是在设置密码时为解决密码的两次输入问题用到了管道。此外本程序必须由 root 组的用户执行才能添加用户。

七、参考资料

1、https://blog.csdn.net/qq_29113041/article/details/78675396