**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> |