

“网络安全综合实验（I）”实验报告

**题目：Linux网络安全2**

院 系

专业班级

姓 名

学 号

日 期 2020 年 月

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 评分表 | Linux网络安全2（50分） | | | | 完成（50分） | 成绩 | |
| 评分 项目 | 过程 | 分析与小结 | 撰写 | 创新 | 完成任务 | 合计 | 教师 |
| 分值 | 20 | 20 | 5 | 5 | 50 | 100 | 签名 |
| 评分 |  |  |  |  |  |  |  |

报告要求及评分规则

1.请按照模板给出的格式，包括行距、字体、段落格式等，完成报告；

2.报告封面保持一致(如实填写基本信息及完成日期)；

3.实验报告内容应包括：封面、评分规则、实验过程记录、实验问题分析与总结、参考文献及资料列表；

4提交：电子材料应包括本实验电子版（doc）、实验参考文献资料的电子资源文件（pdf）。

5.主要考察能力： 实验动手能力、问题分析与归纳能力、文档规范撰写能力、创新能力；

6.其他要求：可按指导老师要求的时间和提交方式提交；每次课实验报告可以单独提交；如果需要最终纸质报告的，可去掉模板中说明文字（斜体）之后，双面打印；

7.总评分=课程每次实验分数之和/课程实验次数。

其中：

每次实验分=实验完成分（50分）+实验报告分（50分）-扣分+加分；

计算方法：

实验完成分=（完成任务数量/总任务数量）\*50；

实验报告分=以下1-4项合计；

1）过程（要求：实验过程完整、清晰）(满分20)（优秀：18+ 良好：16+ 一般：14+）；

2）问题分析与小结（要求：有条理、细致）（满分20）（优秀：18+ 良好：16+ 一般14+）；

3）撰写（要求：语句通畅、格式规范）（满分5）（优秀：4+ 良好：3+ 一般：2+）；

4）创新（要求：见解独到、有创意）（满分5）（优秀：4+ 良好：3+ 一般：2+）；

扣分=报告迟交天数\*2分（满分10分）  （发现雷同抄袭的内容，该次实验不得分）；

加分=搜集整理与实验相关的学习资料作为附件，资料能帮助同学更好掌握相关知识的；获得同组人互评优秀的；提交最终报告时间为班级前3名。（满分5分）（项数\*1分）；

# 实验九：Linux网络安全攻防2

## 实验环境及要求

本实验不进行分组，独立完成，每个人需要两台主机：

A主机：kali linux的虚拟机

B主机：跟A网络连通、能监听报文

选项1： win7虚拟机（或者物理机，物理机上要求安装wireshark）

选项2： linux虚拟机，可以运行tcpdump监听报文)

**截图要求**：如果能在一个截图中把一个任务的多个步骤都能截到的话，可以就截一个图（尽量精简截图的工作）

## 实验任务（共8个任务关卡）

**实验环境：**

主机 A的 IP（ ）--------------- B的 IP（ ）

### 任务2：构造IP报文

在主机A上使用IP()函数构造一个目的地址为B的IP报文，然后用send()函数将该IP报文发送给B，在B上开启wireshark以验证是否收到该报文。

### 任务3：构造二层报文

在B上开启监听；

1. 用sendp()配合Ether()和ARP()函数来构造一个ARP报文，目的ip为B的ip，源MAC地址为A的mac地址；
2. 在B上验证是否收到该报文；

进阶(选做）：用网关的ip，A的mac地址，发送一个伪造网关的ARP报文（Ether()增加src参数的输入，ARP操作码为response），看B的arp表中网关的mac地址是否变为A的mac地址了。（查看arp表的命令 arp -a)。

### 任务4：接收IP报文

用sr()函数给B发送ICMP报文，显示发送和接收报文的信息；

用sr()函数给一个不存在的ip发送ICMP报文，显示发送和未接收的报文的信息；

### 任务5: 接收二层报文

用srp()配合Ether()和ARP()构造一个arp广播报文，二层目的地址为ff:ff:ff:ff:ff:ff，三层目的地址为A主机所在网络的网络地址, 超时时间设为5秒，显示本网络中回应的主机列表，以及未回应的主机列表。

### 任务6：构造四层报文

实验开始前，首先在B上启用HTTP服务，打开TCP 80端口，并开启tcpdump或wireshark。

（1）在A的scapy上使用IP()和TCP()函数来构造一个目的地IP为B，源端口为30，目的端口为80的TCP SYN报文。 验证从主机A发出的包，以及从B收到的包。

（2）分别使用RandShort(), RandNum()和Fuzz()这几个函数来让scapy帮你自动生成一个随机的端口号，用作sport(源端口号)，验证报文从A发出，以及B收到了。

### 任务7 嗅探

用scapy的sniff()函数嗅探报文，打印嗅探的报文信息

### 任务8 编写python脚本，执行嗅探任务

1. 退出scapy的交互模式，编写python脚本，调用sniff()函数监听IP报文，sniff参数用回调函数来打印监听的ip报文的数据；
2. 调用sniff()函数监听tcp报文信息，回调函数中打印tcp报文的五元组信息（源IP：源端口，目的ip：目的端口，协议）

# 小结：学习心得与体会

学生自己总结本次实验的内容，心得体会，意见和建议。

# 参考文献：

这部分要求学生把查阅的资料整理出来，并附上pdf归档包，作为积累的内容。