

“网络安全综合实践（I）”实验报告

**题目：Scapy发包实验**

院 系 网络空间安全学院

专业班级 网安2002班

姓 名 范启航

学 号 U202012043

日 期 2021 年 12 月

# 网络安全2——Scapy发包实验

## 实验环境

请填写A、B的IP

主机 A的 IP（ 192.168.43.10 ）--------------- B的 IP（ 192.168.43.27 ）

### 任务1：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。

发送报文：

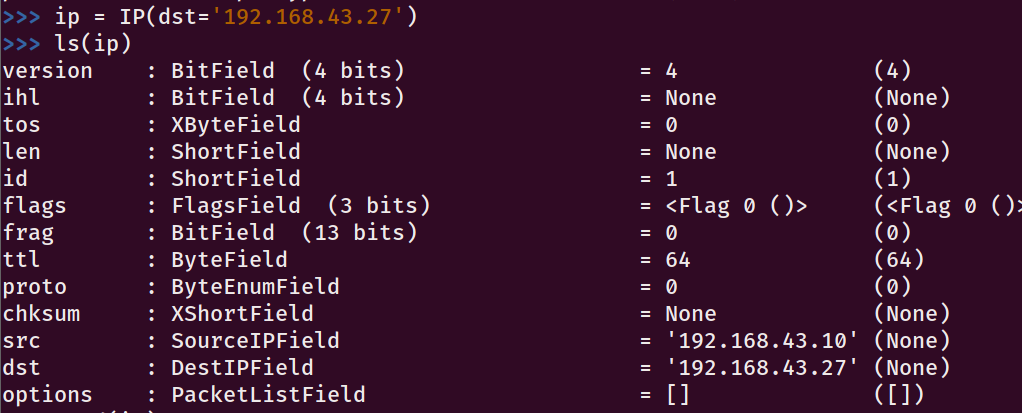
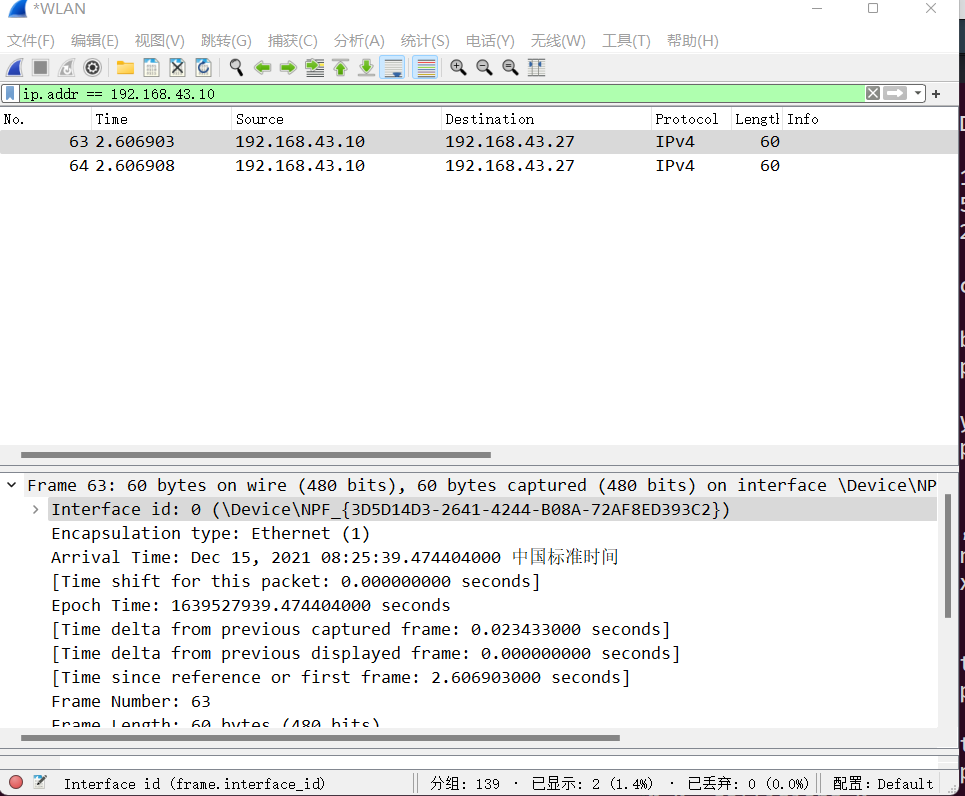
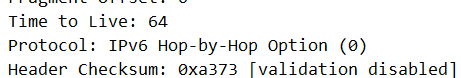




图1-1 发送报文

接收报文：



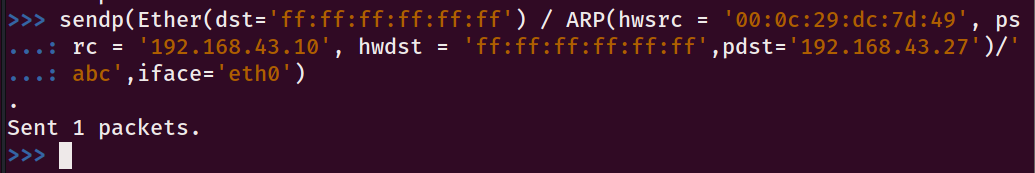


### 任务2：构造二层报文

在B上开启wireshark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；

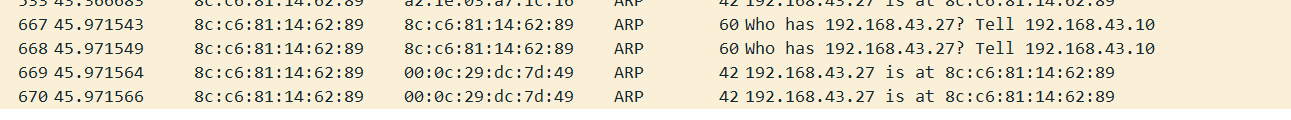
发送报文：



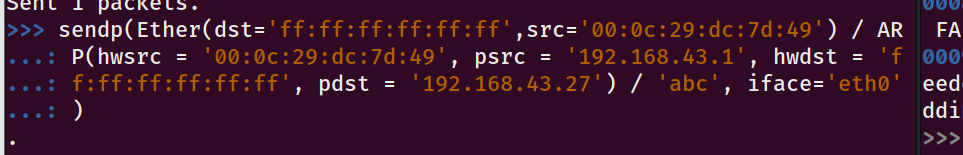


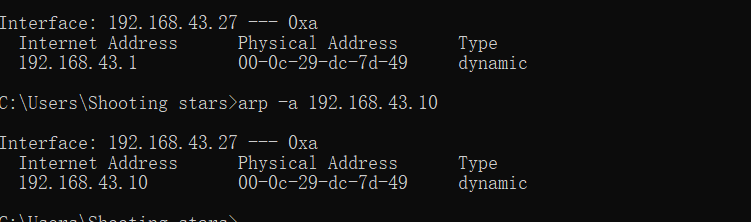


1. 在B上验证是否收到该报文；



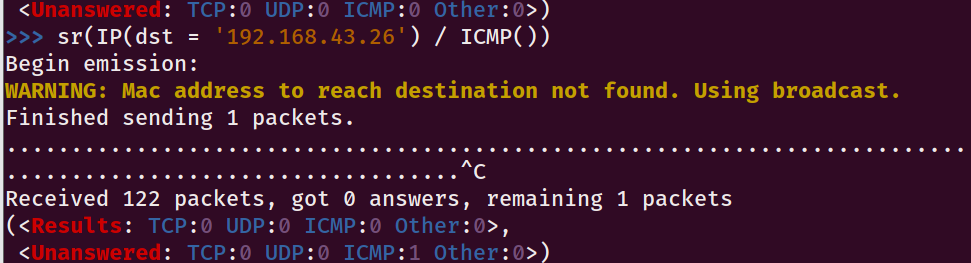
进阶(选做）：用网关的IP，A的MAC地址（或任意的MAC地址），发送一个伪造网关的ARP报文（Ether()增加src参数的输入，ARP操作码为2），看B的arp表中网关的mac地址是否变为A的mac地址了。（查看arp表的命令 arp -a)。

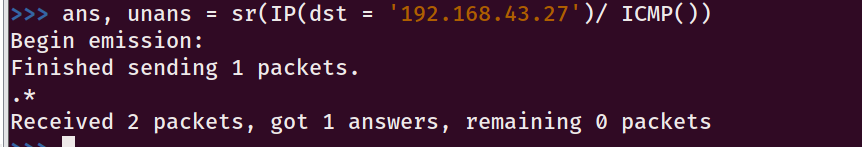


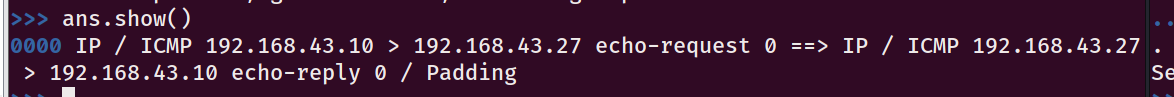


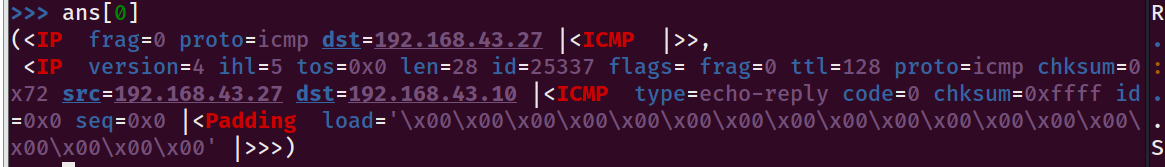
### 任务3：接收IP报文

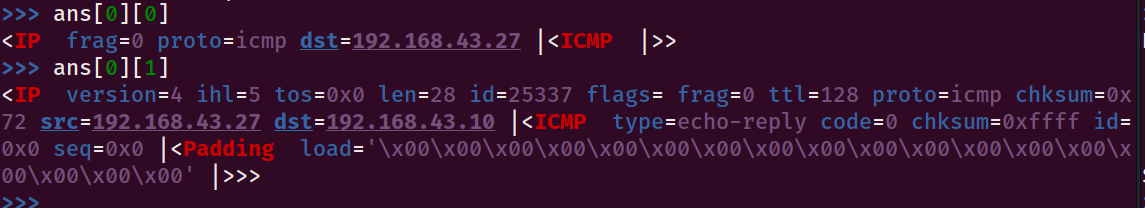
用sr()函数给B发送ICMP报文，显示发送和接收报文的信息；



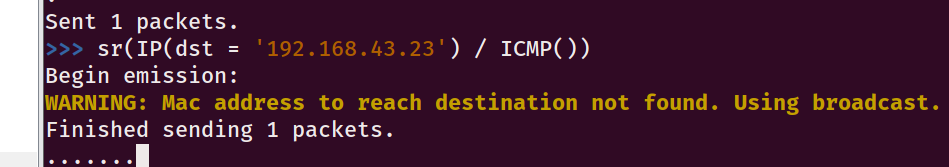


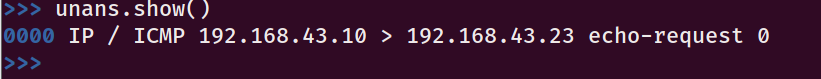






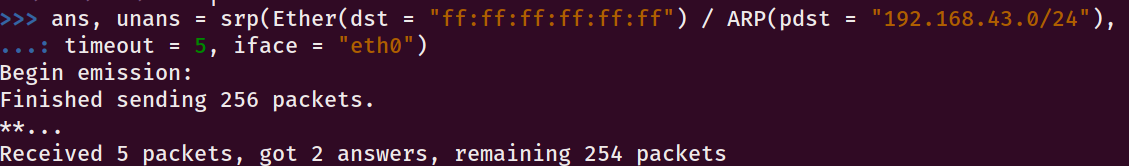
用sr()函数给一个不存在的ip发送ICMP报文，显示发送和未接收的报文的信息；

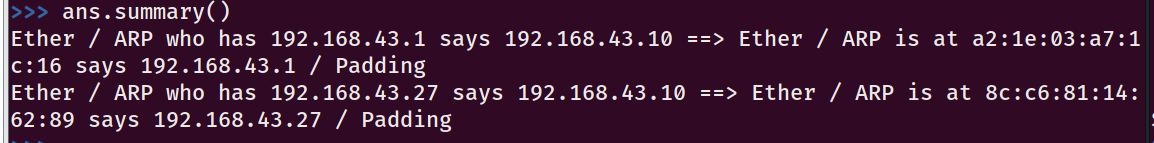


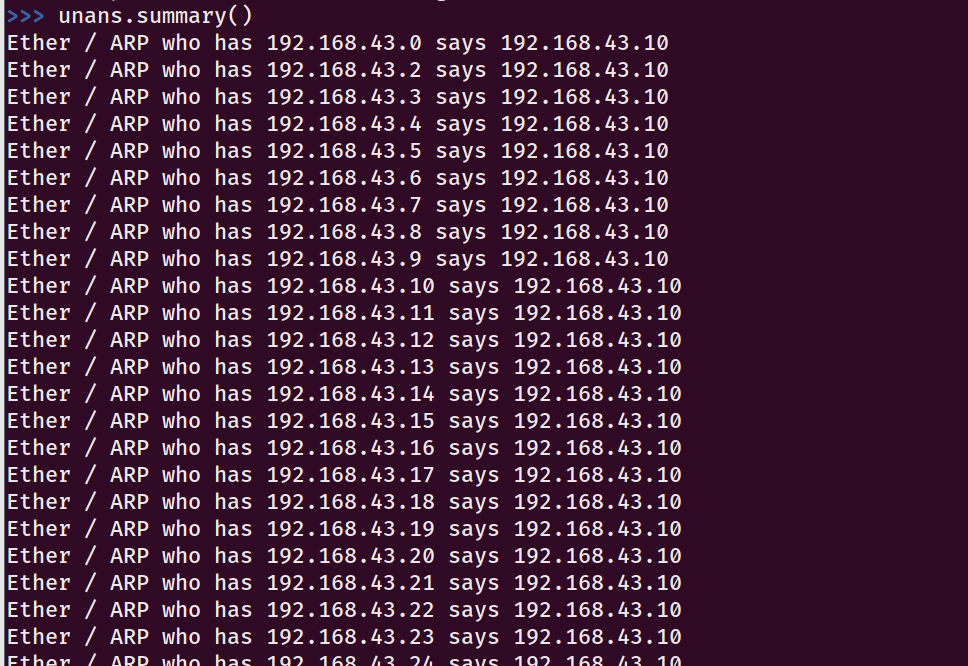


### 任务4: 接收二层报文

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5 嗅探

退出scapy的交互模式，编写python脚本，用scapy的sniff()函数嗅探tcp报文，打印嗅探的报文信息（sniff的过滤器修改为tcp协议，需要打印源IP、目的IP、源端口、目的端口、协议号等信息）

#!usr/bin/python3

from scapy.all import \*

def print\_pkt(pkt):

print("Source IP:", pkt[IP].src)

print("Destination IP",pkt[IP].dst)

print("TCP src Port", pkt[TCP].sport)

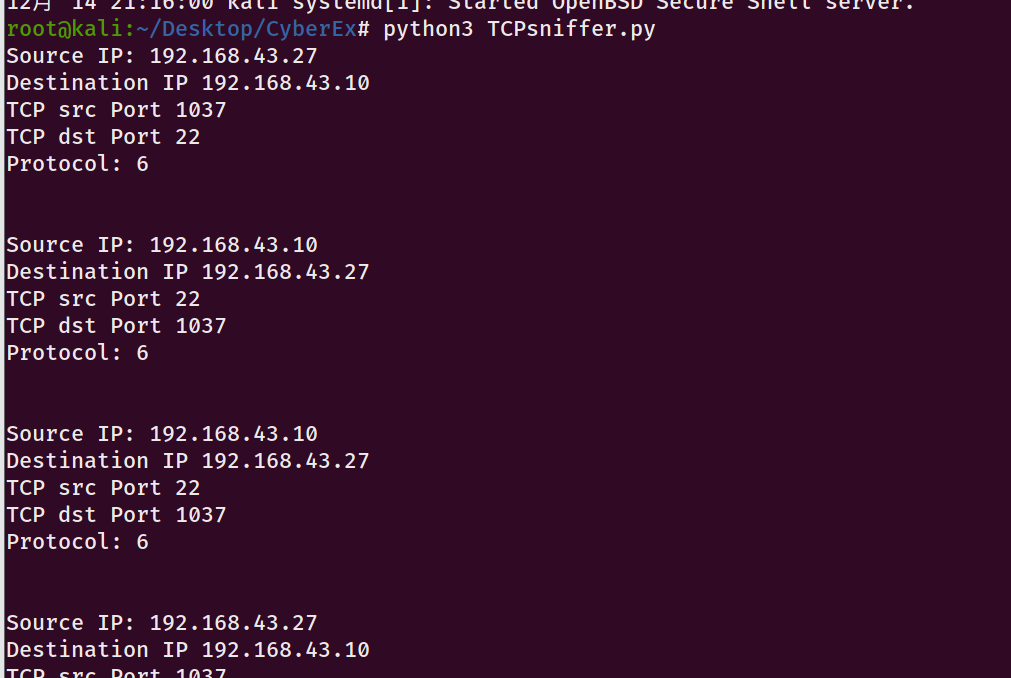
print("TCP dst Port", pkt[TCP].dport)

print("Protocol:", pkt[IP].proto)

print("\n")

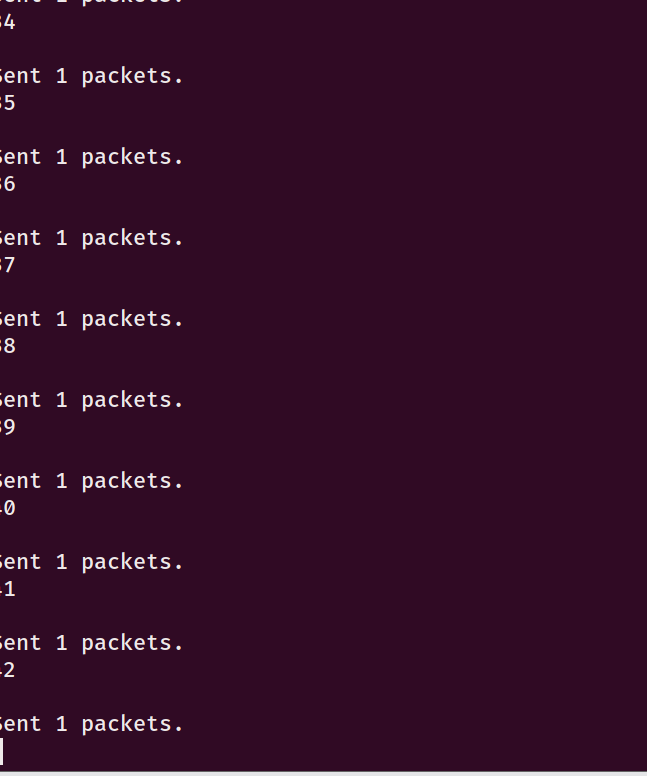
if \_\_name\_\_ == "\_\_main\_\_":

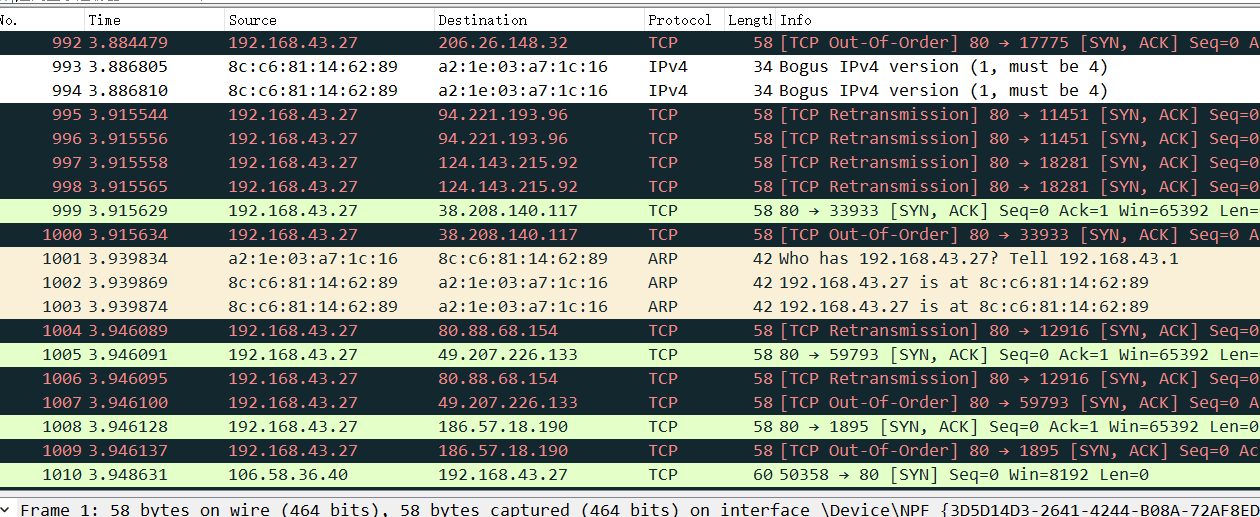
pkt = sniff(filter='tcp',prn=print\_pkt)



### 任务6：TCP SYN-Flood攻击程序

用scapy构造 TCP（第四层）SYN报文，循环发送给靶机，要求源地址、源端口随机化，在靶机上进行验证。（由于scapy发包速度比较慢，拒绝服务效果可能出不来，只要靶机上能用wireshark监听到这些报文，netstat -nat 能查看到相应连接即可）。





# 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。

通过本次实验，我学会了使用scapy工具进行一系列有关网络安全方面的测试与发包手段，能够对网卡通讯的包进行抓取，分析，发送自己虚假的报文，同时能够利用python调用scpay库进行一系列攻击手段的实现，加深了我对于网络安全的理解。