项目二

目录

[一、搭建实验环境： 2](#_Toc114484966)

[1. 网络环境架构 2](#_Toc114484967)

[2. 实验环境与工具: 2](#_Toc114484968)

[3. 搭建两侧的局域网 2](#_Toc114484969)

[4. 搭建路由 4](#_Toc114484970)

[二、MAC泛洪攻击 7](#_Toc114484971)

[1. 实验环境 7](#_Toc114484972)

[2. 实验过程 7](#_Toc114484973)

[3. 实验分析： 9](#_Toc114484974)

[三、ARP DOS攻击 9](#_Toc114484975)

[1. 实验环境 9](#_Toc114484976)

[2. 实验过程 9](#_Toc114484977)

[3. 实验分析： 10](#_Toc114484978)

[四、ARP Middleman 攻击 11](#_Toc114484979)

[1. 实验环境 11](#_Toc114484980)

[2. 实验过程 11](#_Toc114484981)

[3. 实验分析 12](#_Toc114484982)

[五、IP地址欺骗 13](#_Toc114484983)

[1. 实验环境 13](#_Toc114484984)

[2. 实验过程 13](#_Toc114484985)

[3. 实验分析 14](#_Toc114484986)

[六、ICMP DOS 攻击 14](#_Toc114484987)

[1. 实验环境 14](#_Toc114484988)

[2. 实验过程： 14](#_Toc114484989)

[3. 实验分析 15](#_Toc114484990)

# 一、搭建实验环境：

## 1. 网络环境架构

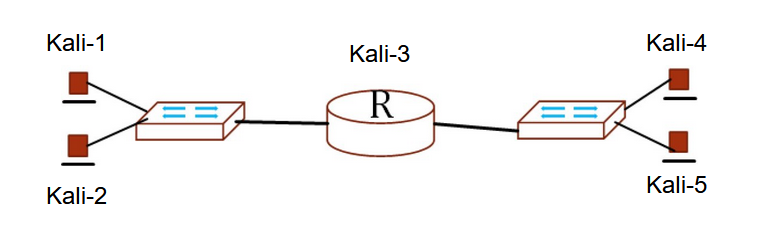


图 1 整体网络架构

## 2. 实验环境与工具:

Kali-Linux-2022.2-vmware-amd64 五台

VMware Workstation Pro 16 一份

## 3. 搭建两侧的局域网

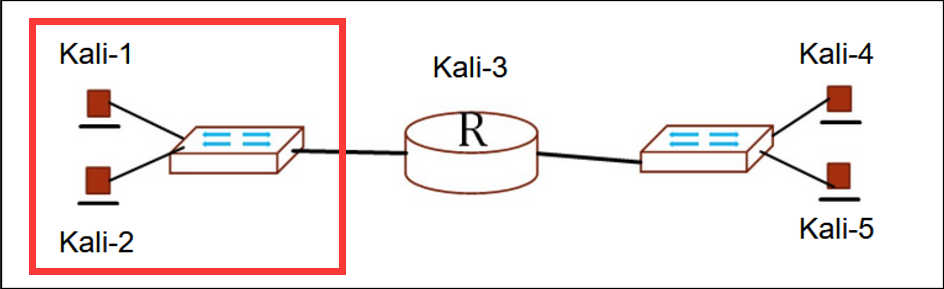


图 2 搭建左侧局域网

1. 首先打开虚拟机，设置一块网卡，操作步骤如下：

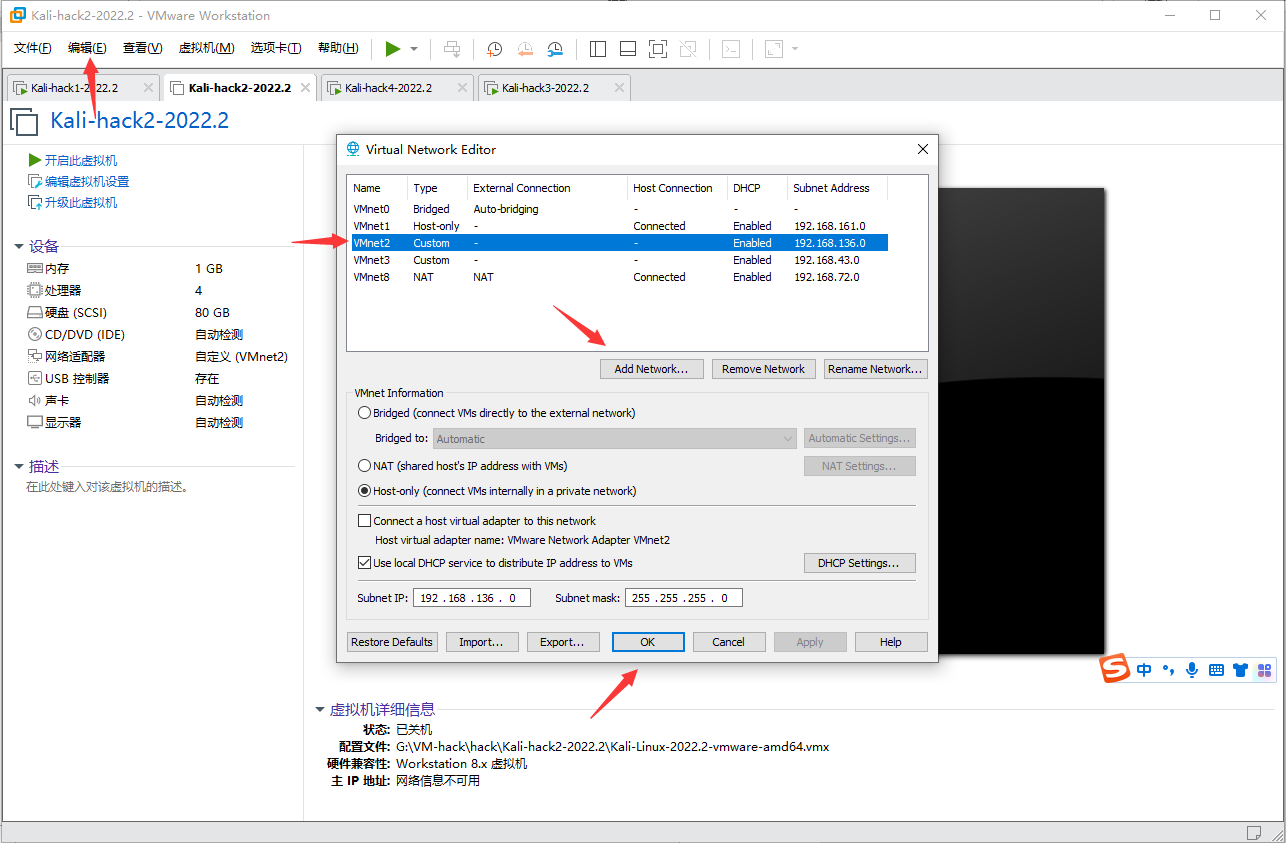


图 3 设置网卡Vmnet2

1. 打开两个虚拟机kali-hack1和kali-hack2。用ifconfig命令查看对应的网卡信息和ip地址, kali-hack1的ip地址为192.168.136.128，kali-hack2的ip地址为192.168.136.129。
2. 使用Ping命令，观测两台虚拟机是否在同一局域网，效果如下：(双方可以ping通)

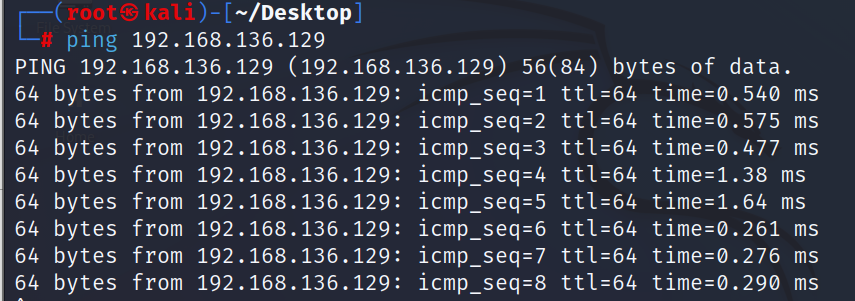


图 4 kali-hack1 ping kali-hack2

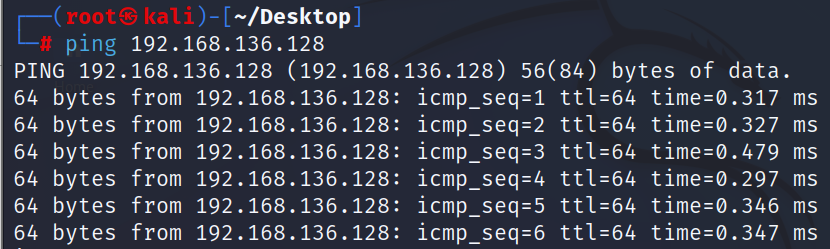


图 5 kali-hack2 ping kali-hack1

1. 双方可以互相ping通，证明VMnet2搭建成功
2. 右侧局域网搭建和上面操作相同，下面显示搭建成果：

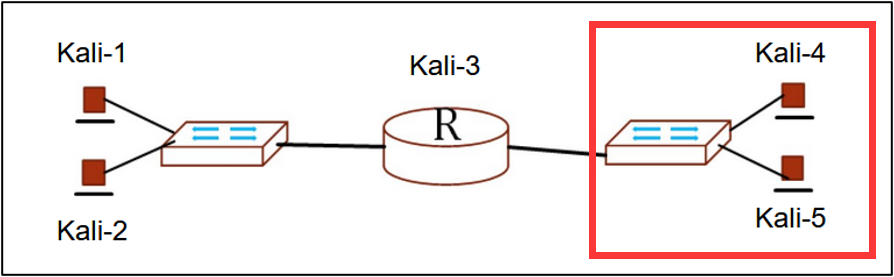


图 6搭建右侧局域网

1. Kali-hack4的ip地址为192.168.43.129，kali-hack5的ip地址为192.168.43.131使用ping命令观测两台虚拟机是否在同一局域网，效果如下：(双方可以ping通)

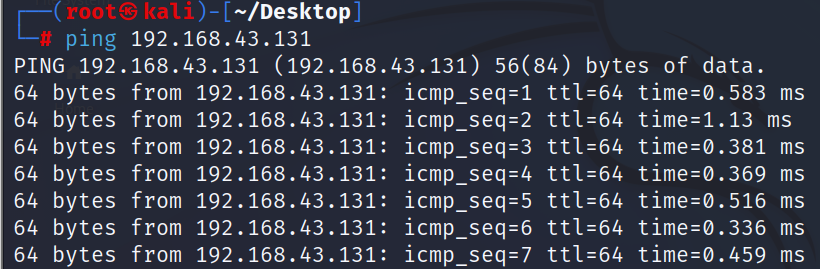


图 7 kali-hack4 ping kali-hack5

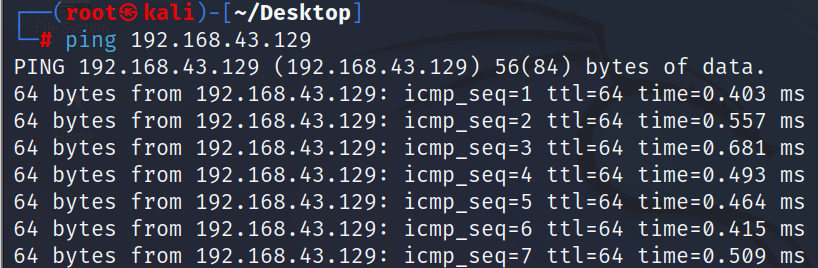


图 8 kali-hack5 ping kali-hack4

1. 双方可以互相ping通，证明Vmnet3搭建成功

## 4. 搭建路由

1. 为Kali-hack3配置两块网卡，分别为Vmnet2、Vmnet3，如下图：

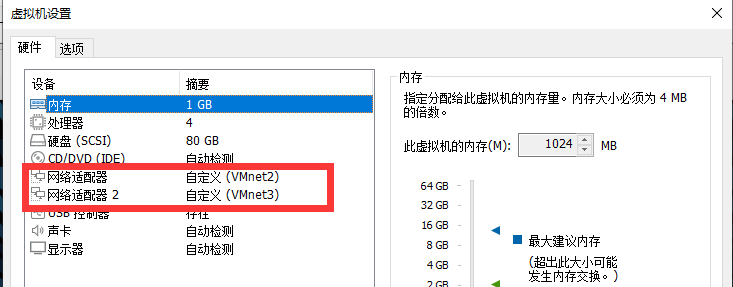


图 9 设置两块网卡

1. 为两块网卡创建对应的ip地址，使用如下命令：

ifconfig eth0 192.168.136.130

ifconfig eth1 192.168.43.130

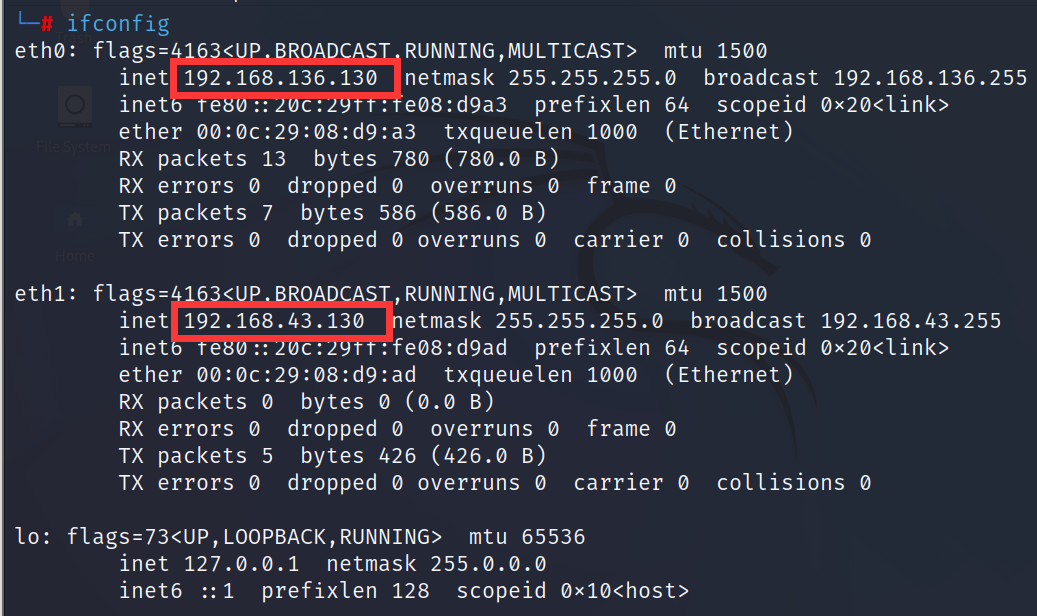


图 10 为网卡设置对应的IP地址

1. 设置网关：

为kali-hack1和kali-hack2设置网关的地址为kali-hack3的地址192.168.136.130，命令为：route add default gw 192.168.136.130

为kali-hack4和kali-hack5设置网关的地址为kali-hack3的地址192.168.43.130，命令为：route add default gw 192.168.43.130

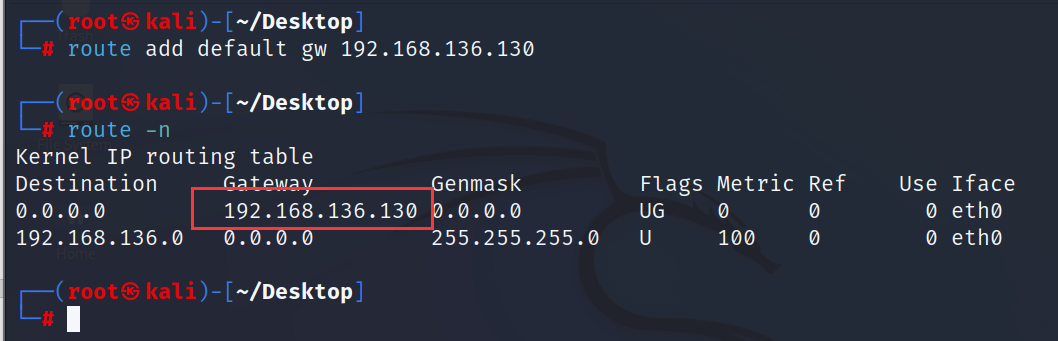


图 11 左侧局域网设置网关

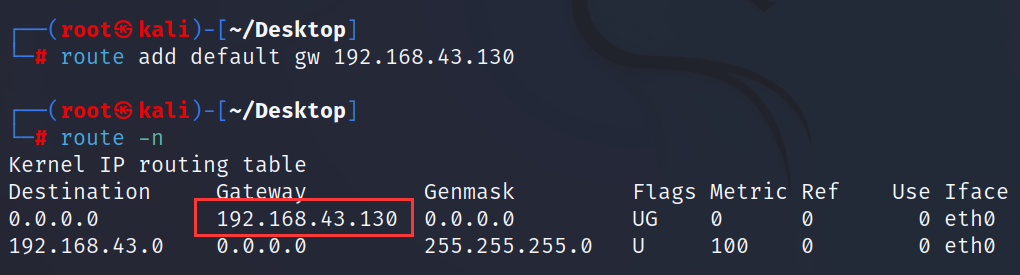
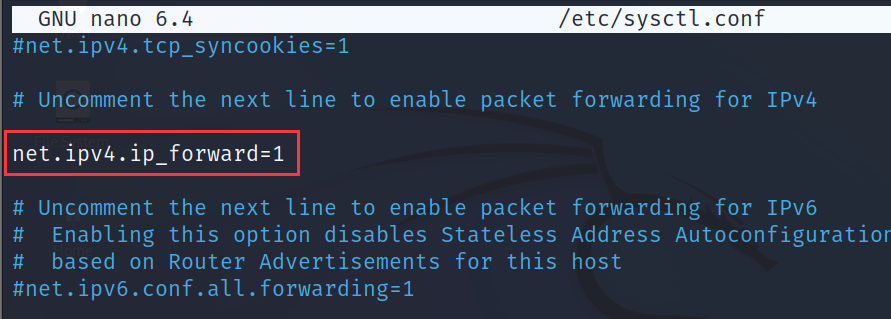


图 12 右侧局域网设置网关

1. 启动ip转发：

在kali-hack3中命令行输入nano /etc/sysctl.conf 将其中的net.ipv4.ip\_forward = 1服务打开，然后sysctl -p 重启服务。



将192.168.136.0:3307 转发到 192.168.43.0:3307，命令如下：

iptables -t nat -A PREROUTING -p tcp --dport 3307 -j DNAT --to-destination 192.168.136.0:3307

iptables -t nat -A POSTROUTING -d 192.168.136.0 -p tcp --dport 3307 -j SNAT --to 192.168.43.0

iptables -t nat -A PREROUTING -p tcp --dport 3307 -j DNAT --to-destination 192.168.43.0:3307

iptables -t nat -A POSTROUTING -d 192.168.43.0 -p tcp --dport 3307 -j SNAT --to 192.168.136.0

最后输入modprobe ip\_tables 启动服务。

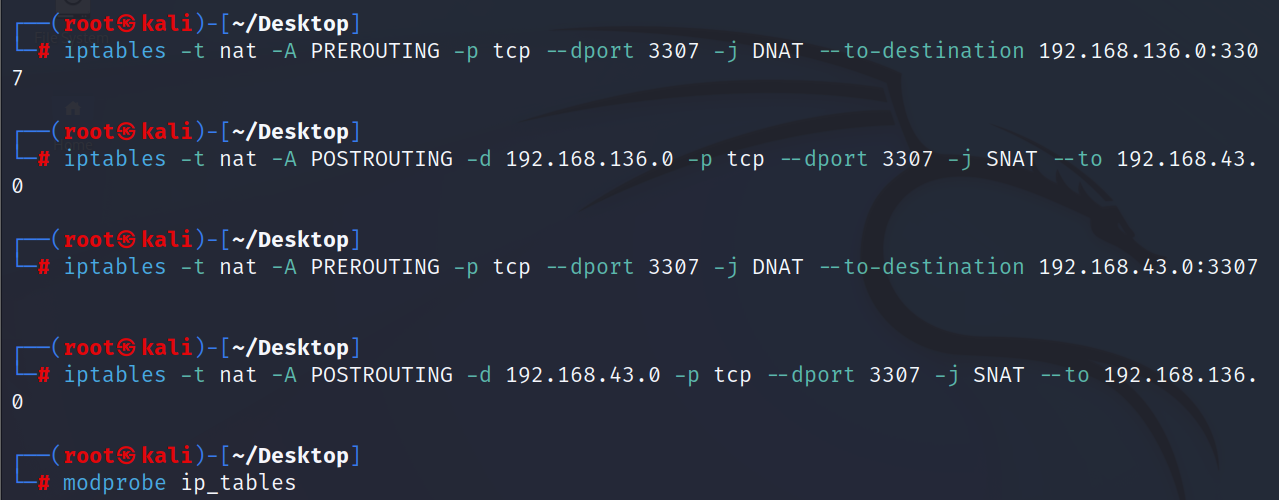


图 13 启动ip转发

1. 测试

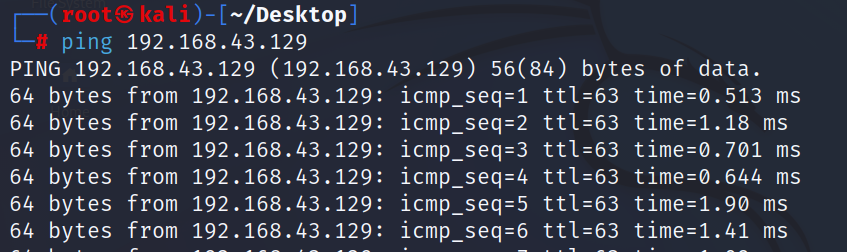


图 14 Kali-hack1 ping kali-hack4：

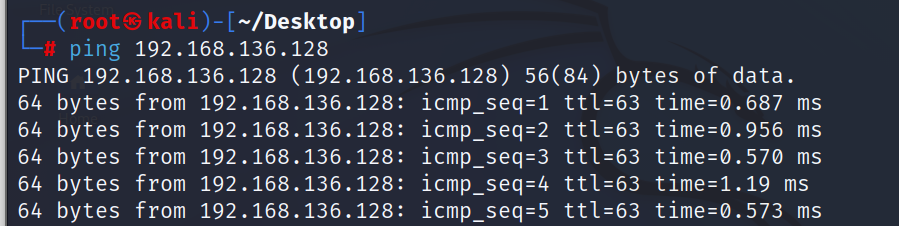


图 15 Kali-hack4 ping kali-hack1：

左侧局域网通过中间路由ping通右侧局域网，至此，已经成功的搭建了网络。

# 二、MAC泛洪攻击

## 1. 实验环境

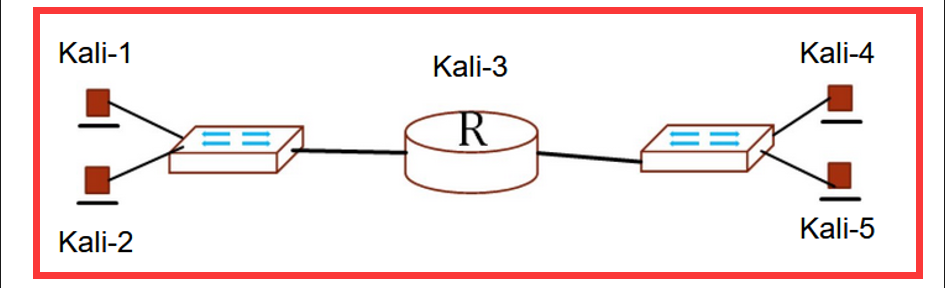


图 16 MAC泛洪攻击实验环境

## 2. 实验过程

1. Kali-hack1 作为监听者；

Kali-hack2 作为ftp服务器；

Kacl-hack4作为用户

1. 在Kali-hack2上部署ftp服务

使用 apt-get install vsftpd 和 systemctl restart vsftpd 来启动ftp服务

然后设置ftp用户 账号为：ftpuser 密码为：ftphack

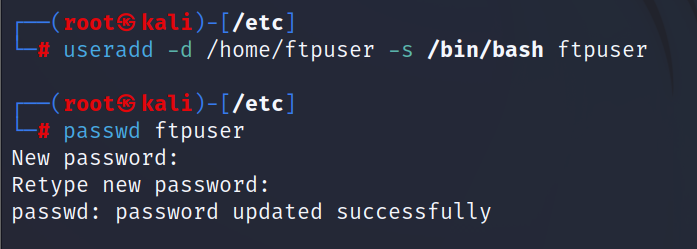


图 17部署ftp服务

1. 在攻击机Kali-hack1中打开WireShark 监听ftp服务，并设置过滤ftp

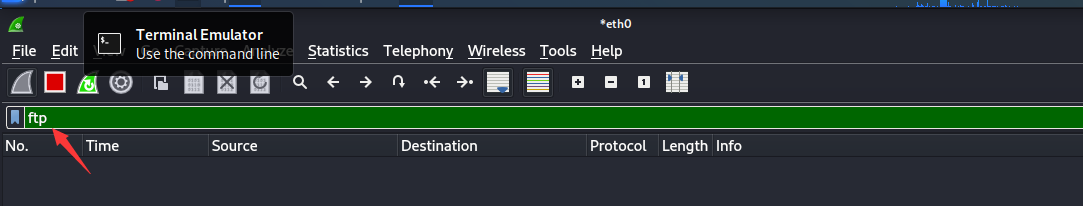


图 18 Wireshark设置过滤ftp

1. 在客户机4上尝试登录服务器2，此时攻击机1并不能窃听到信息。
2. 在攻击机中使用macof命令，发送大量的MAC地址，当表被填满后，新的表项将会替代旧的表项。

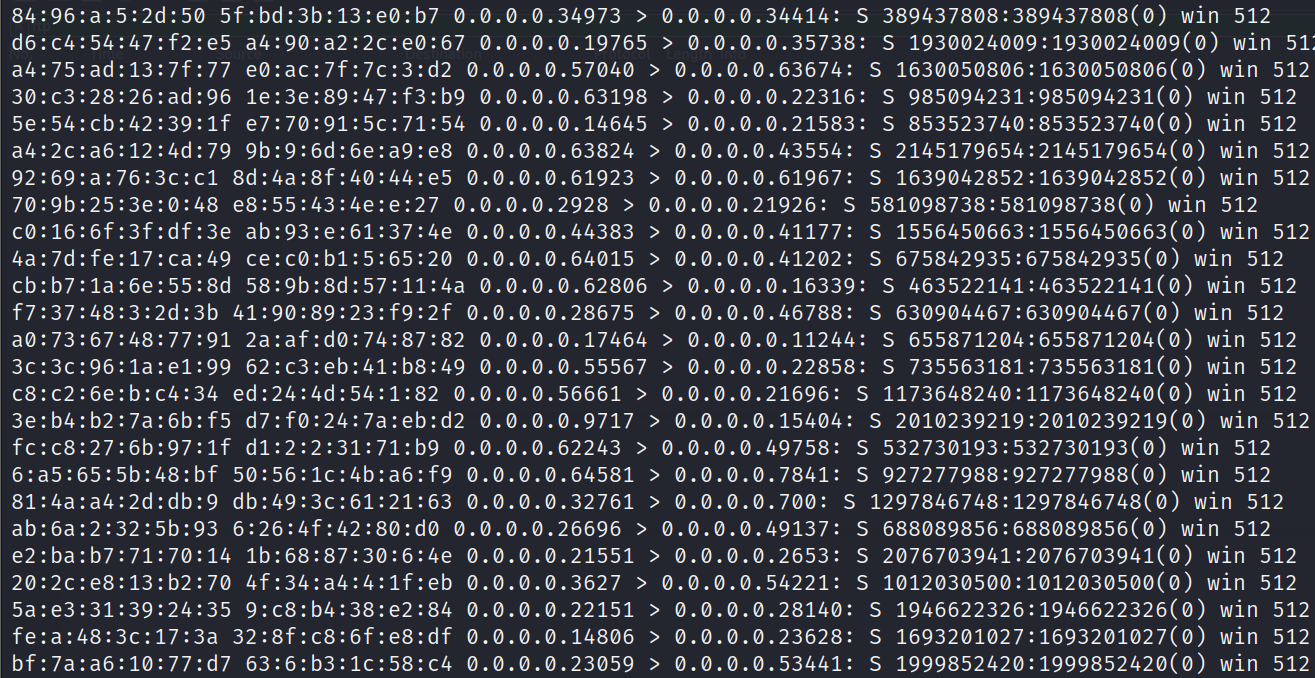


图 19 使用macof填满表项

1. 一段时间后，在客户机4上登录ftp服务器2，此时在攻击机1上，窃听到信息。

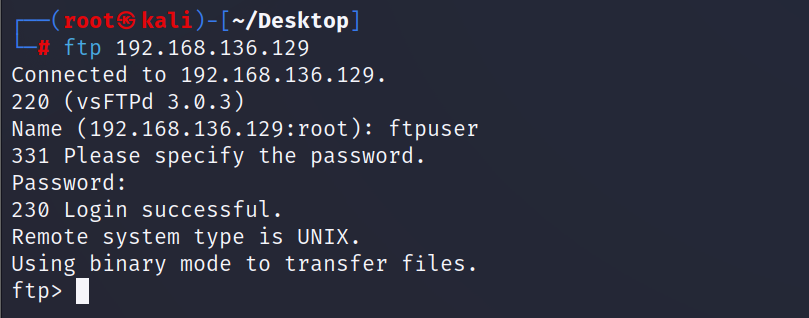


图 20 客户机登录ftp服务

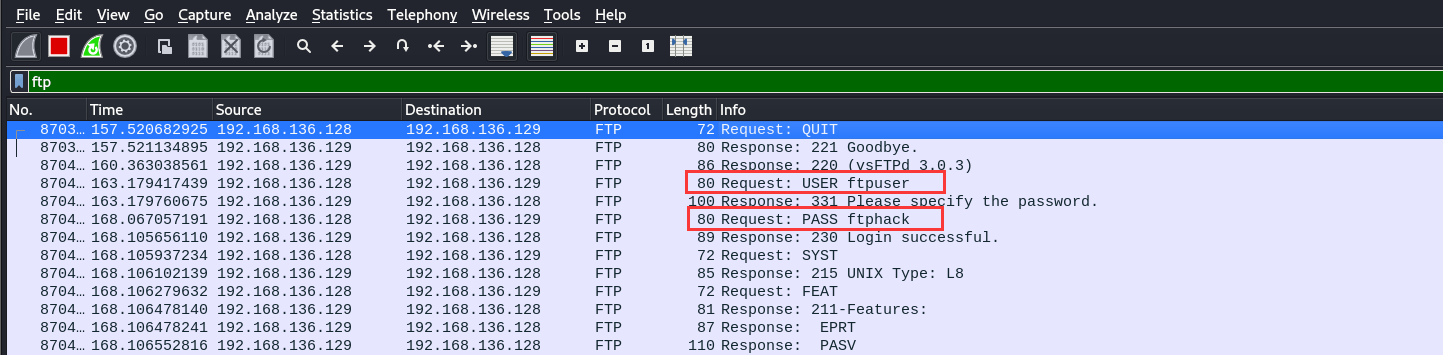


图 21 攻击机抓到ftp数据包

## 3. 实验分析：

由于交换表空间的有限性，新的来源MAC地址不断的填写交换表项，当表被填满后，新的表项将会替代旧的表项。如果攻击者发送大量的具有不同伪造源MAC地址的帧，由于交换机的自学习功能，整个交换表将会被垃圾表项填满。当有正常的数据帧到达时，由于交换表不再有正常的MAC地址表项，交换机完全退化为广播模式，从而使得攻击者又可以用嗅探的方式窃听数据。

# 三、ARP DOS攻击

## 1. 实验环境

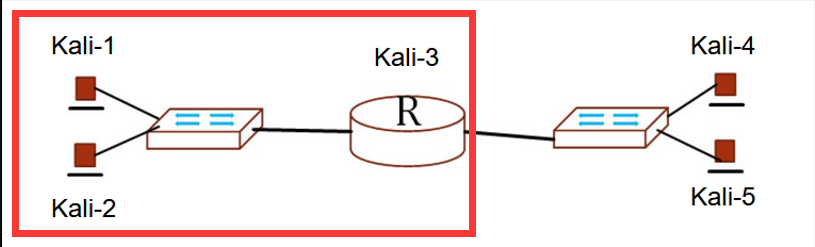


图 22 ARP DOS攻击实验环境

## 2. 实验过程

1. Kali-hack1 为被攻击机

Kali-hack2 为攻击机

Kali-hack3 为网关

1. 首先检测被攻击机Kali-hack1和攻击机2，网关3的连通性：

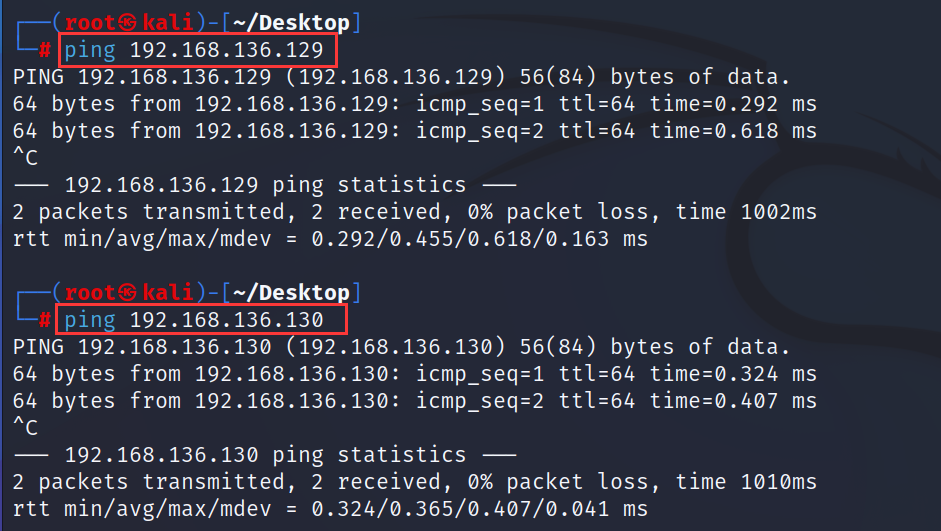


图 23 kali-hack1可以ping通kali-hack2&3

1. 攻击机2向被攻击机发送大量arp响应报文，

命令为arpspoof -i eth0 -t 192.168.136.128 192.168.136.130

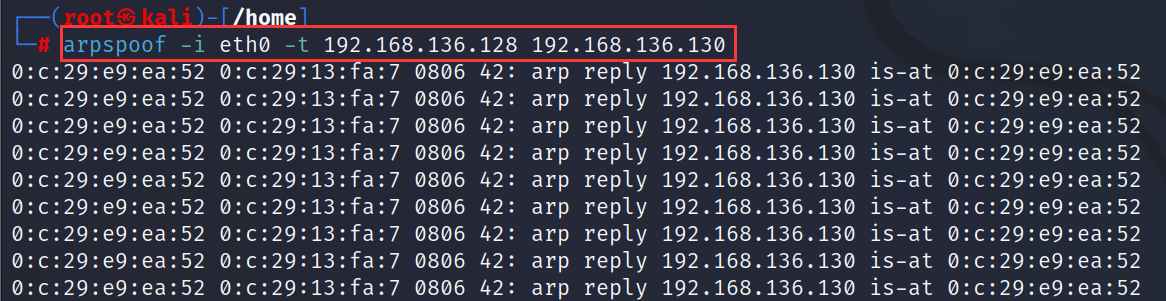


图 24攻击机2向被攻击机发送大量arp响应报文

1. 查看攻击效果：

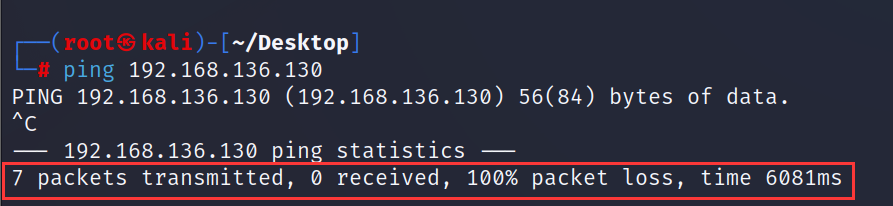


图 25 被攻击机 1访问网关3失败

当攻击机2停止arp-dos攻击时，被攻击机1可以访问网关3，则本次实验攻击成功。

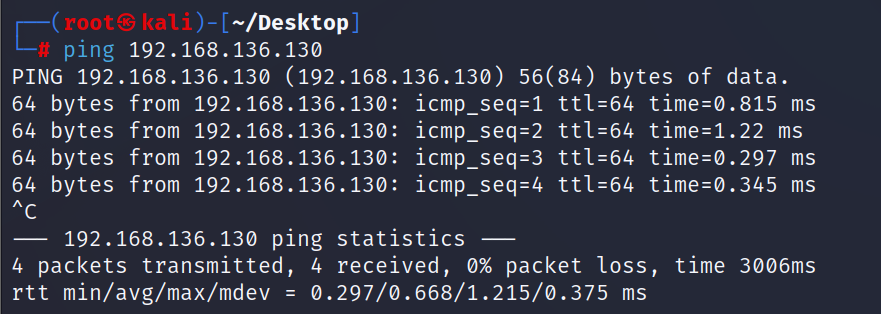


图 26 被攻击机 1访问网关3成功

## 3. 实验分析：

本次实验的攻击思路为：阻止某个主机正常通信，可向其发送ARP回应报文，其中源IP地址为网关（或另一个主机）的IP，源MAC地址为一不存在地址；以广播方式发送ARP回应报文，冒充网关，阻止网络中的主机与真正的网关通信，即报文中的源IP地址为网关IP，源MAC地址为一不存在地址。向网关不断发送伪造IP地址的ARP请求和回应报文，一方面大量消耗网关CPU资源，另一方面致使网关不断更新自己的ARP表，导致网关ARP表溢出，真实主机的IP-MAC项被移除，网关无法与网络内主机通信。

# 四、ARP Middleman 攻击

## 1. 实验环境

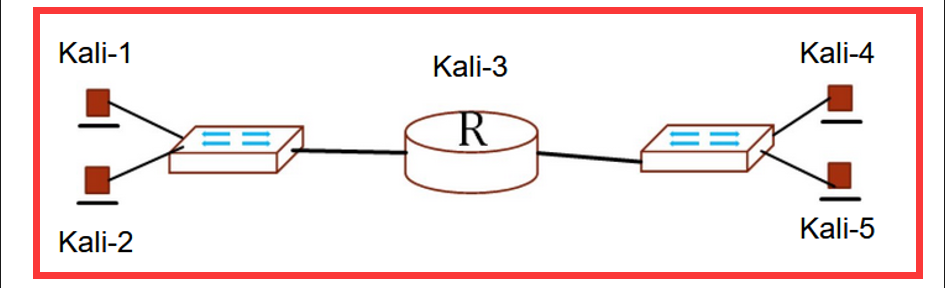


图 27 ARP Middleman 攻击环境

## 2. 实验过程

1. Kali-hack1 为被窃听机

Kali-hack2 为中间人

Kali-hack3 为网关，

Kali-hack4 为ftp服务器

1. 攻击机中间人2使用arpsppof工具进行欺骗：

arpspoof -i eth0 -t 192.168.136.128 192.168.136.130

1. 此时，被窃听机1无法正常访问到网关和ftp服务器

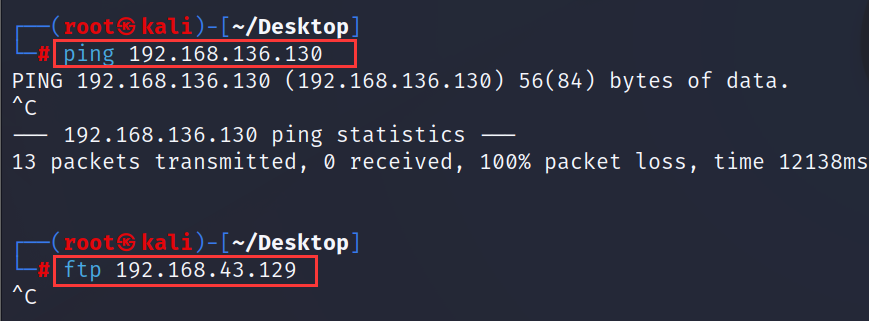


图 28 kali-1访问不到网关kali-3和ftp服务器kali-4

1. 在kali-hack2中命令行输入nano /etc/sysctl.conf 将其中的net.ipv4.ip\_forward = 1服务打开，然后sysctl -p 重启服务。

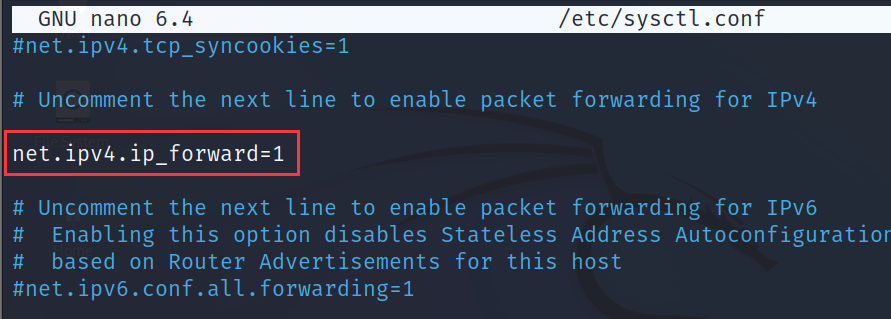


图 29 中间人kali-2打开ip转发

1. 第四步完成后，中间人开启了ip转发，相当于向主机1表明自己是网关，同时截获1的数据包发给真正的网关3，达成窃听的目的。此时，被窃听机可以正常访问到网关。此时，被攻击机1访问ftp服务器4可以被攻击机2窃听到。

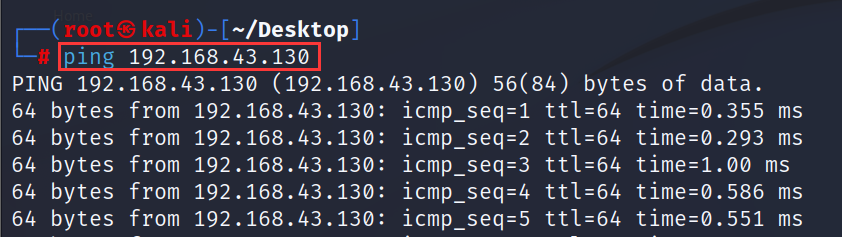


图 30 kali-1可以ping通网关kali-3

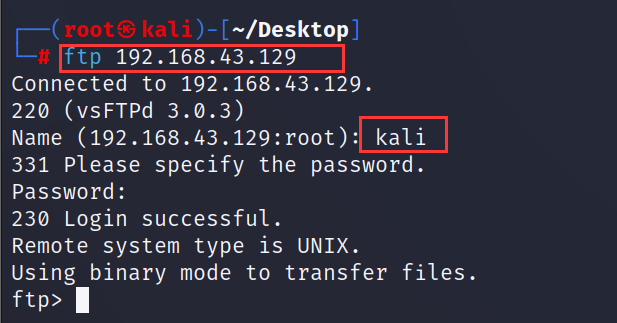


图 31 kali-1远程连接ftp服务器kali-4

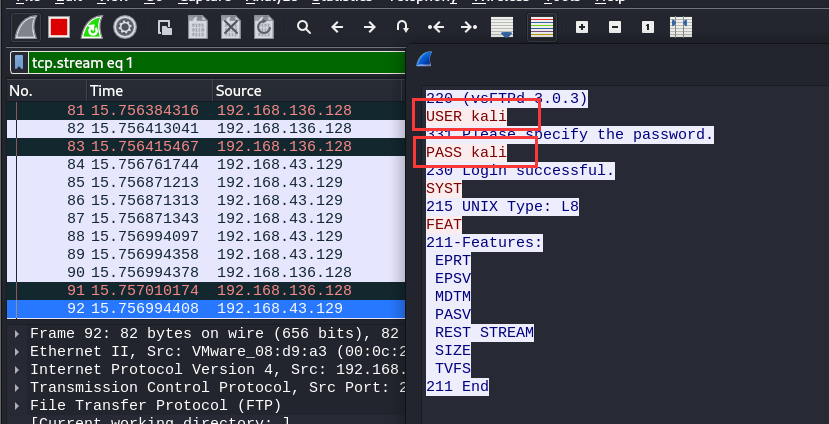


图 32 kali-2捕获到kali-1发往kali-4的数据包

## 3. 实验分析

1、如果主机A和主机B为正常通信的主机，攻击者向主机发送ARP回应报文，宣称自己是主机B，即ARP回应报文中的源IP地址为主机B，源MAC地址为攻击者。同样地，攻击者也向主机B发送类似的ARP报文，宣称自己是主机A，即ARP回应报文中的源IP地址为主机A，源MAC地址为攻击者。

2、主机A和主机B收到相应ARP回应报文后更新各自的ARP表。当主机A有报文向主机B发送时，实际上发送给了攻击者。同样地，主机B发送给主机A的报文也发送给了攻击者。因此，攻击者截获了主机A和主机B之间的通信信息。

3、为了不让主机A和主机B发现通信被窃听，攻击者在截获主机A和主机B的报文后，还会将报文转发，使主机A和主机Ｂ依然能够收到报文。

# 五、IP地址欺骗

## 1. 实验环境

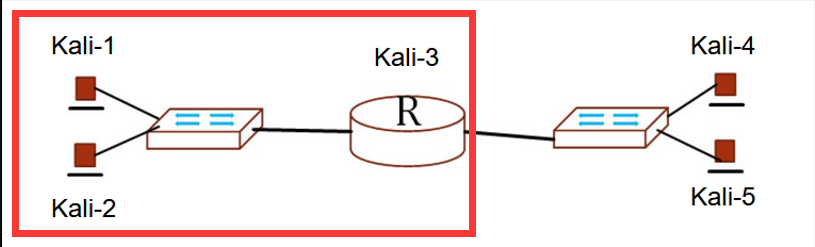


图 33 IP地址欺骗攻击环境

## 2. 实验过程

1. Kali-hack1 为被攻击机，ip地址为192.168.128

Kali-hack2 为攻击机， ip地址为192.168.129

Kali-hack3 为被冒充机，ip地址为192.168.130

1. 攻击机Kali-hack2使用命令hping3 --flood -a 192.168.136.130 192.168.136.128

假装自己是Kali-hack3来给Kali-hack1发送数据包：

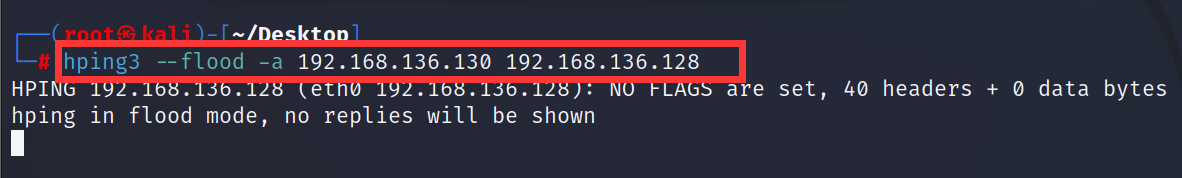


图 34 Kali-hack3伪装ip给Kali-hack1发送数据包

1. 被攻击机Kali-hack1打开Wireshark抓取TCP流量包，可以发现大量的ip地址为被冒充机的数据包

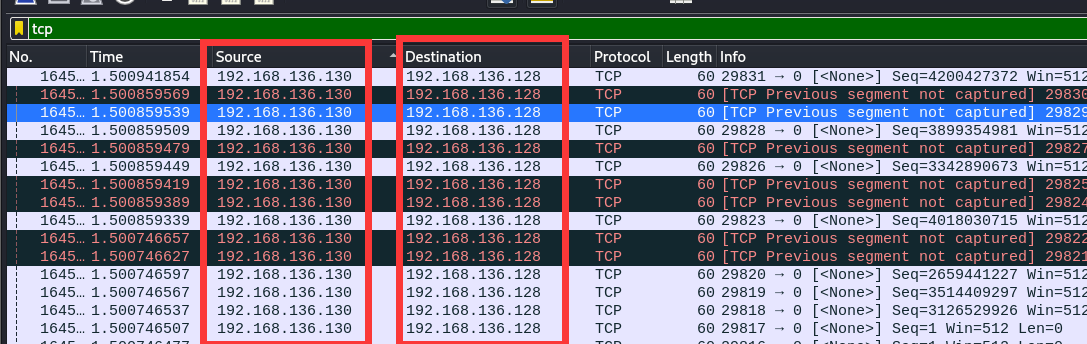


图 35被攻击机抓取的数据包

1. 至此，攻击成功。

## 3. 实验分析

1. 攻击者首先选择一个被攻击主机信任的主机作为被冒充主机。
2. 攻击者通过采用诸如拒绝服务一类的攻击行为使被冒充主机瘫痪。
3. 攻击者向被攻击主机发送源IP地址为被冒充主机IP地址的连接请求报文。这是利用了路由器进行转发时不检查源地址是否合法的漏洞。
4. 攻击者在估算的时间延迟后向攻击主机发送确认报文。因为被攻击主机在收到攻击主机的请求报文后会向被冒充主机发送同步确认报文。攻击成功，即可登陆被攻击主机。

# 六、ICMP DOS 攻击

## 1. 实验环境

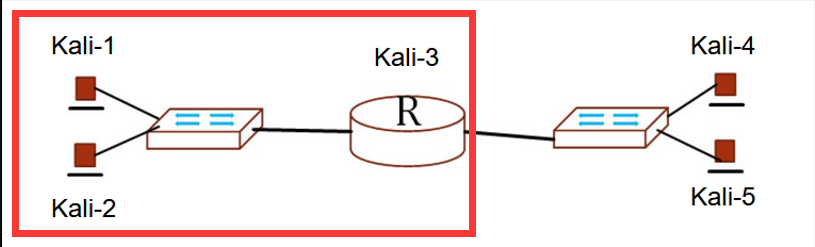


图 36 ICMP DOS攻击

## 2. 实验过程：

1. Kali-hack1 为被攻击机，ip地址为192.168.128

Kali-hack2 为攻击机， ip地址为192.168.129

Kali-hack3 为被冒充机，ip地址为192.168.130

1. 攻击机Kali-hack2使用命令hping3 -1 --flood -a 192.168.136.130 192.168.136.128 (-1 代表 ICMP模式)

假装自己是Kali-hack3来给Kali-hack1发送大量的ping：

1. 被攻击机Kali-hack1打开Wireshark抓取ICMP流量包，可以发现大量的ip地址为被冒充机的数据包

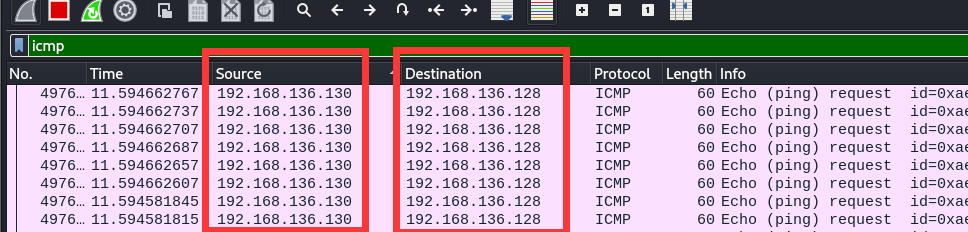
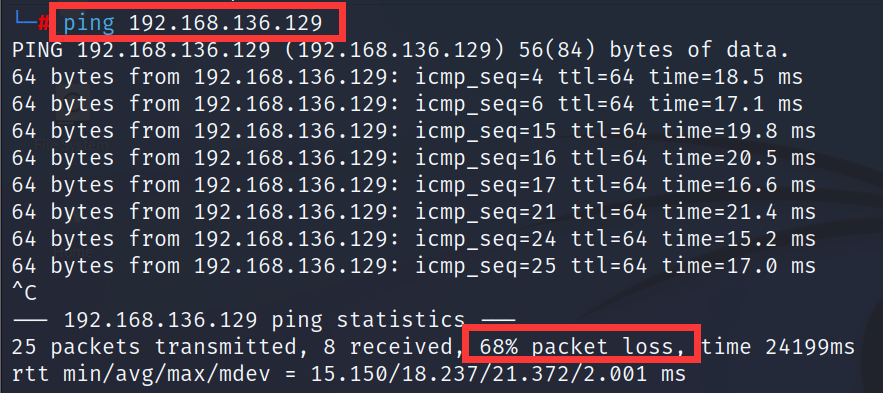


图 37 被攻击机抓取的数据包

1. 此时，被攻击机ping正常内的局域网，会有大量的数据包丢失。本次实验采用的攻击机数量较少，不能全部挤占被攻击机的资源，所以导致会有部分数据包是有效的，所以当攻击机数量足够多时，dos攻击时成功的。



## 3. 实验分析

1、ICMP DOS采用的是一种反弹式攻击，利用了ICMP的请求响应报文进行攻击，并能够很好的隐藏攻击者的行踪。

2、首先，攻击者选择一个有足够多主机的网络，并向这个网络的网关发送一个源地址是目标系统的ICMP请求响应广播报文。

3、其次，被选定的网关在收到广播报文后向其管辖范围内的所有主机系统发送该请求响应报文。

4、最后，所有接收到请求响应报文的主机向报文中的源地址发送响应应答报文。目标主机因为资源耗尽而瘫痪。