

《网络攻击与防御》实验报告

作者：郑红美

2025 年 6 月 20 日

1 实验名称

Wireshark 嗅探和协议分析。

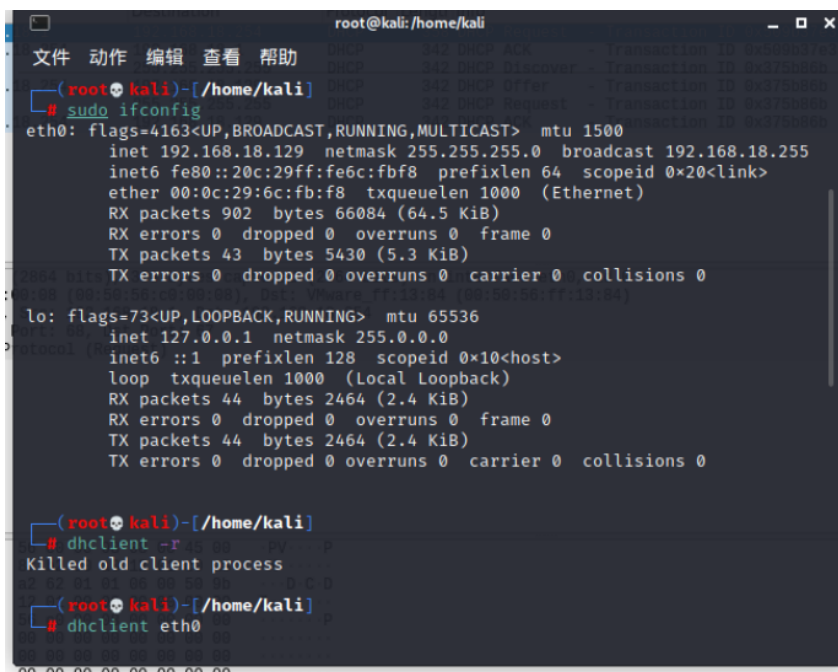
2 实验环境

系统环境：Windows 7/8/10 操作系统、Centos6.8 浏览器：IE10/11 Wireshark：Version 2.2.5 WinPcap 4.1.0.2980 8Uftp 3.8.2.0 Foxmail 7.2

3 实验步骤及结果

1、DHCP 协议抓包实验以 Win10 操作系统为例进入 Win10 系统设置界面，点击页面中的“网络和 Internet”选项，进入 Internet 网络设置界面，点击“WLAN”网络，然后选择页面中的“管理已知网络”选项，把除了做实验需要的 WLAN 之外的其他网络全部选择“忘记”。启动 Wireshark，选中 WLAN 开始抓取数据包。以管理员方式打开 CMD，运行命令 `ipconfig /release`，释放获取到的 IP 地址。运行命令 `ipconfig /renew`，重新获取 IP 地址，稍等片刻，获取成功以后，在 Wireshark 中停止抓取数据包。在 Wireshark 的过滤器中输入 `bootp`，表示只筛选 DHCP 数据包。数据包分析如下：No106：本机 localhost (10.133.81.229) 向 DHCP server (10.133.0.1) 发送了一个 DHCP Release 数据包，终止了 ip 租赁。将本机 IP 地址清空。No267：本机 localhost 向局域网广播一个 DHCP Discover 包，此时本机 localhost 的 IP 地址为 0.0.0.0。广播地址为 255.255.255.255。本地端口为 68，目的端口为 67。No277：Ipv4 地址为 10.133.0.1 的 DHCP 服务器收到该包后，向本机发送一个 DHCP Offer 数据包。进一步分析该回应数据包内容为：该包内包含预分配给本机 localhost 的 ip 地址（截图中高亮行）、dns 服务

器地址、子网掩码、ip 租赁期等基本信息。No278: DHCP Request 包由本机 localhost 广播，表示本机已经收到 DHCP Offer 包，对此事进行通告，通告的内容包括预分配给本机的 IP 地址，本机的 MAC 地址，本机的计算机名等信息。No279: DHCP server (10.133.0.1) 向本机 localhost (10.133.81.229) 发送了一个 DHCP Ack 数据包。确认 IP 地址，路由、DNS、IP 租赁时间、子网掩码等信息。本机 localhost 收到该确认包后，不会立即更新自己的信息。其将会向网络发送 ARP 请求，询问是否已经有人占用该分配 IP，如果没有人回应，本机 localhost 将更新自己的 ipv4 信息，IP 分配过程结束。结果：



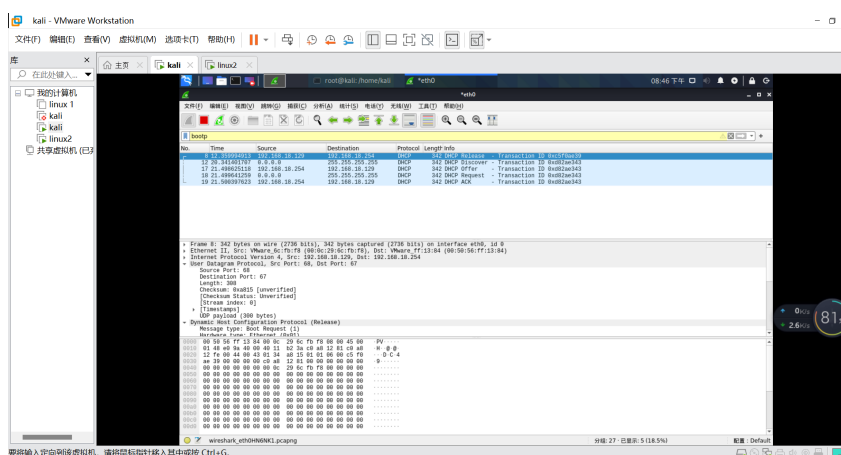
```

root@kali: /home/kali
文件 动作 编辑 查看 帮助
(root@kali)~[/home/kali]
# sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.18.129 netmask 255.255.255.0 broadcast 192.168.18.255
    inet6 fe80::20c:29ff:fe6c:fbf8 prefixlen 64 scopeid 0<20<link>
    ether 00:0c:29:6c:fb:f8 txqueuelen 1000 (Ethernet)
    RX packets 902 bytes 66084 (64.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 43 bytes 5430 (5.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

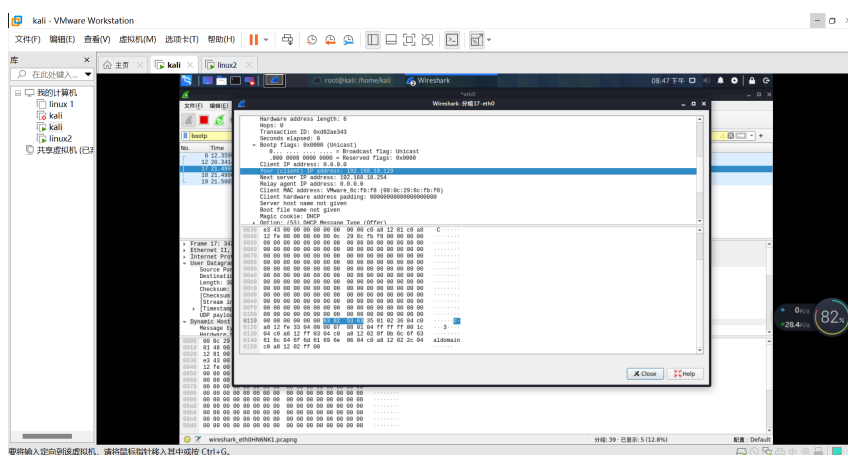
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 44 bytes 2464 (2.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 44 bytes 2464 (2.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@kali)~[/home/kali]
# dhclient -r
Killed old client process

(root@kali)~[/home/kali]
# dhclient eth0
  
```



2、抓取 FTP 密码实验首先，搭建自己的 FTP 服务器，这里以 Centos6.8 为例。运行命令 `rpm -f vsftpd` 看 ftp 服务是否安装，如果没安装的话，依次执行下列命令：`yum -y install vsftpd` # 安装 vsftpd 服务修改 `/etc/vsftpd/vsftpd.conf`，把相关字段改为如下所示：`anonymous——enable=NO` # 不允许匿名用户登录 `chroot——local——user=YES`



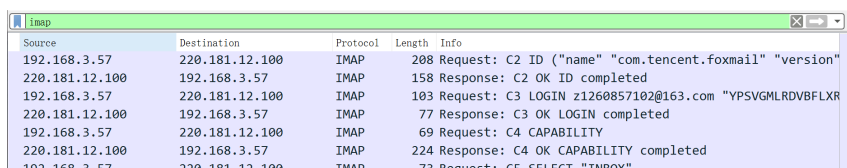
不可以让 ftp 用户跳出自己的家目录 useradd -s /sbin/nologin -d /var/www/html testftp # 添加用户 testftp, 此用户只能连接 ftp, 无法直接登录系统, 默认家目录是在 var/www/html 文件夹 passwd testftp # 为 testftp 用户设置密码 chmod o+w /var/www/html/ # 修改 testftp 用户家目录权限, 允许上传 setenforce 0 # 临时关闭 SELINUX 如果需要长期修改, 可以修改/etc/selinux/config 文件, 把相关字段改为: SELINUX=disabled, 然后重启 CentOS. service iptables stop # 关闭 iptables service vsftpd start # 开启 vsftpd 服务。然后, 使用 8Uftp 客户端上传/下载文件, 测试是否搭建成功。断开 8Uftp 客户端的连接。开启 Wireshark, 选择相应的网卡, 由于 CentOS 是用 VMWare12Pro 搭建在本机上的, 所以要使用的网卡为 VMware Network Adapter VMnet8。使用 8Uftp 客户端连接服务器, 输入地址, 用户名, 密码。在 Wireshark 中设置过滤器为 ftp, 可以看到明文的用户名和密码。如下图所示:



3、抓取 Foxmail 邮箱客户端密码实验首先, 自己在 mail.163.com 上申请一个邮箱, 通过网页登录邮箱后, 选择设置 POP3/SMTP/IMAP, 如下图所示: 勾选使用使用授权

231	15.802475	192.168.67.136	192.168.67.131	FTP	90 Response: 226 Transfer complete.
246	17.086342	192.168.67.131	192.168.67.136	FTP	74 Request: TYPE A
247	17.086557	192.168.67.136	192.168.67.131	FTP	96 Response: 200 Switching to ASCII mode.
248	17.086746	192.168.67.131	192.168.67.136	FTP	72 Request: PASV
249	17.086941	192.168.67.136	192.168.67.131	FTP	118 Response: 227 Entering Passive Mode (192,168,67,136,195,89).
254	17.087415	192.168.67.131	192.168.67.136	FTP	72 Request: LIST

码登录第三方邮件客户端。然后，安装 Foxmail7.2 版本，确认成功登录。退出 Foxmail，开启 Wireshark，选择相应的网卡，打开 Foxmail，登录成功，停止 Wireshark 抓包。可以看到明文的用户名和密码。如下图所示：



The image shows a Wireshark packet capture window titled 'imap'. The packet list on the left shows several IMAP packets between 192.168.3.57 and 220.181.12.100. The packet details pane on the right shows the content of one of these packets, which is an IMAP LOGIN request. The request contains the username 'z1260857102@163.com' and the password 'YPSVGMLRDVBFLXR' in plaintext.

Source	Destination	Protocol	Length	Info
192.168.3.57	220.181.12.100	IMAP	208	Request: C2 ID ("name" "com.tencent.foxmail" "version"
220.181.12.100	192.168.3.57	IMAP	158	Response: C2 OK ID completed
192.168.3.57	220.181.12.100	IMAP	103	Request: C3 LOGIN z1260857102@163.com "YPSVGMLRDVBFLXR"
220.181.12.100	192.168.3.57	IMAP	77	Response: C3 OK LOGIN completed
192.168.3.57	220.181.12.100	IMAP	69	Request: C4 CAPABILITY
220.181.12.100	192.168.3.57	IMAP	224	Response: C4 OK CAPABILITY completed
192.168.3.57	220.181.12.100	IMAP	73	Request: C5 SELECT "INBOX"

4 实验心得

环境配置很重要，任何一个小细节没有处理好，都会使得最后抓包失败，要注重细节