ARP欺骗与防御

1.使用一台Kali Linux攻击一台Windows 10。

2.使用Kali源下载dsniff软件。首先修改Kali源网址的配置，使用以下命令

vim /etc/apt/sources.list

访问源配置文件，修改源网址为可以使用的国内源网址；然后使用以下命令

apt-get update

更新Kali Linux配置。然后通过以下命令

apt-get install dsniff

安装dsniff软件。

3.使用dsniff软件的arpspoof命令对Windows 10主机进行ARP欺骗，命令为

arpspoof -i 网卡名称（eth0） -t 受欺骗主机IP地址 受欺骗网关IP地址

4.使用arp -a命令观察在受欺骗主机的网关的MAC地址在欺骗前后的变化，并使用Wireshark抓取网络中的欺骗攻击流量，并分析该流量具有怎样的形式。观察受欺骗主机能否正常上网。

5.使用以下命令开启Kali Linux的IP转发功能

echo 1 >> /proc/sys/net/ipv4/ip\_forward

，或者直接在文件/proc/sys/net/ipv4/ip\_forward里面修改值为1。观察此时受欺骗主机能否正常上网。

6.在受攻击主机上进行ARP绑定，绑定网关的IP地址与MAC地址为环境中网关的真实地址进行ARP防御，抓取相关的流量，并分析查看ARP攻击是否被防御。

7.在Kali Linux上使用Wireshark抓取网络中流量，观察是否有受欺骗主机的应用层网络流量。以http访问http://www.uooconline.com网站，创建一个账户密码，并使用该账户密码登录该网站。尝试在Wireshark抓取的流量里面找到账户名和密码。

8.使用Kali源下载driftnet软件，使用driftnet命令

driftnet -i eth0

打开driftnet的图片抓取程序，观察能否抓取到受欺骗主机在访问http网站时的图片。