**信息安全实验报告**

**Lab 14 ARP Cache Poisoning Attack Lab**

**孙铁**

**SA20225414**

**Task 1**

Task需要用到三个虚拟机：

- M：IP地址：10.0.2.7；

MAC地址：08:00:27:32:83:13；

- A：IP地址：10.0.2.8；

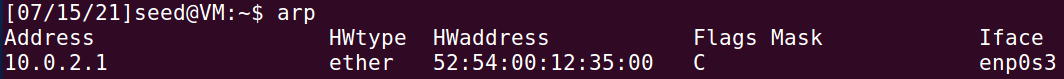
MAC地址：08:00:27:89:23:2d；

- B：IP地址：10.0.2.9；

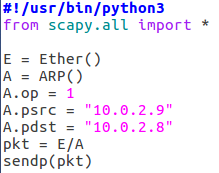
MAC地址：08:00:27:0c:4a:80。

**Task 1A**

查看A（10.0.2.8）的ARP缓存表：

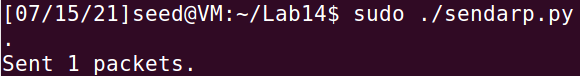


在M（10.0.2.7）上创建文件sendarp.py：

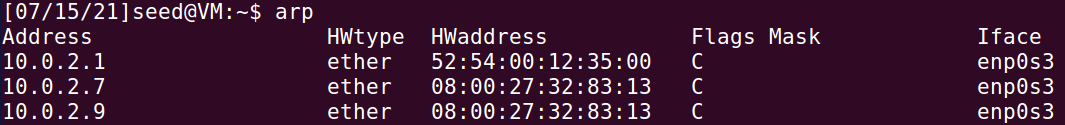


为了通过ARP请求报文实现将B的IP地址与M的MAC地址匹配，从M向A发送ARP请求报文：ARP类型为1，代表ARP请求报文；IP源地址为B；IP目的地址为A。

运行M上的sendarp.py发送报文：



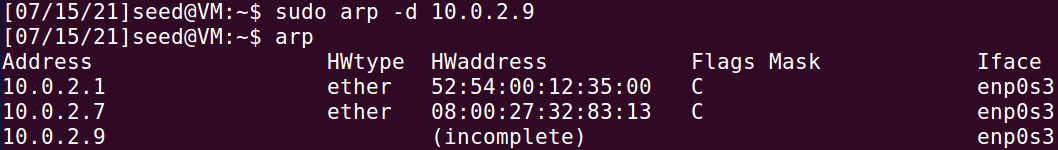
查看A上的ARP缓存表：



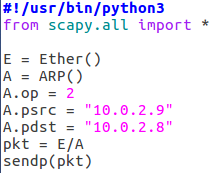
成功将B的IP地址与M的MAC地址匹配。

**Task 1B**

重置A上关于B的ARP缓存：

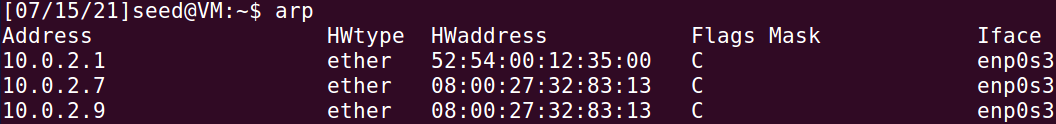


修改M上文件sendarp.py：



为了通过ARP应答报文实现将B的IP地址与M的MAC地址匹配，从M向A发送ARP应答报文：ARP类型为2，代表ARP应答报文；IP源地址为B；IP目的地址为A；

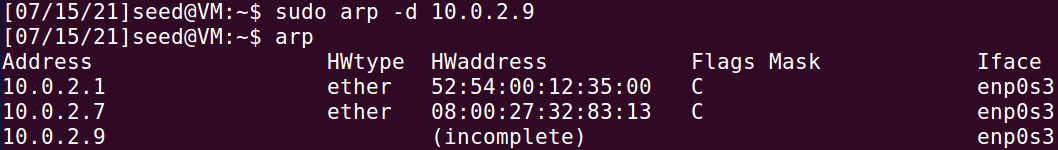
在M上运行sendarp.py发送报文并查看A上的ARP缓存表：



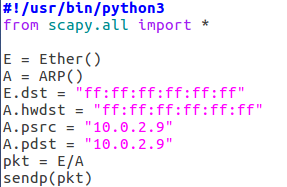
成功将B的IP地址与M的MAC地址匹配。

**Task 1C**

重置A上关于B的ARP缓存：

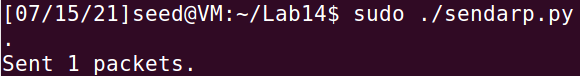


修改M上文件sendarp.py：

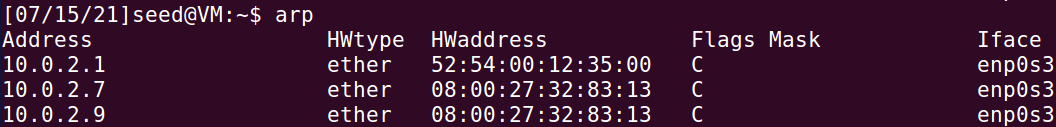


为了通过gratuitous ARP报文实现将B的IP地址与M的MAC地址匹配，从M发送gratuitous ARP报文：IP源地址与IP目的地址皆为B；ARP报文和以太网帧的目的MAC地址皆为“ff:ff:ff:ff:ff:ff”。

运行sendarp.py发送报文：



查看A上的ARP缓存表：



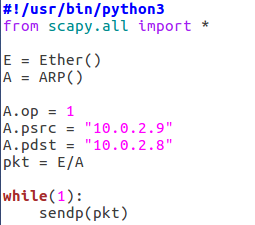
成功将B的IP地址与M的MAC地址匹配。

**Task 2**

**Step 1**

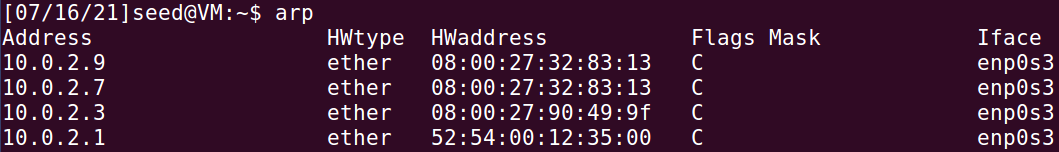
为了让M能够在A与B的通信过程中成为中转，首先需要在A的ARP表上将B的IP地址与M的MAC地址匹配；然后在B的ARP表上将A的IP地址与M的MAC地址匹配。

在M（10.0.2.7）中修改文件sendarp.py：

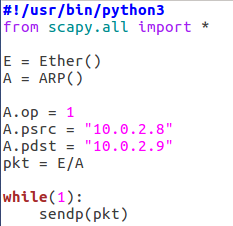


由于实验过程中ARP表会刷新，这里在Task1的基础上进行修改，不断发送ARP包确保ARP表维持中毒状态。

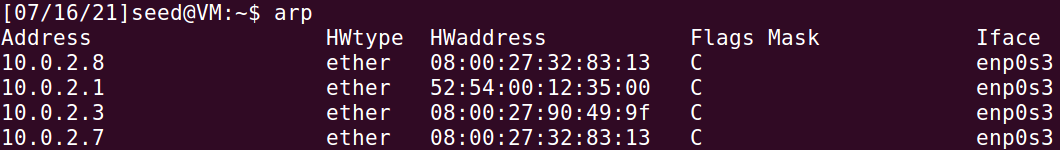
运行sendarp.py，A的ARP表上将B的IP地址与M的MAC地址匹配：



在M（10.0.2.7）中创建文件sendarp2.py：



运行sendarp2.py，B的ARP表上将A的IP地址与M的MAC地址匹配：

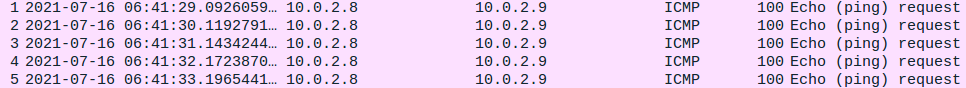


**Step 2**

从A向B使用PING命令：



此时M上的Wireshark成功抓到从A向B发送的ICMP报文：



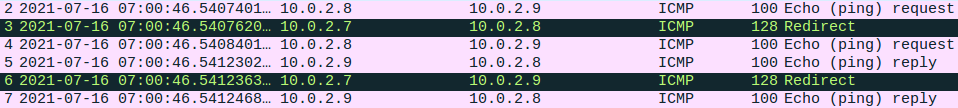
发现此时只能抓到ICMP的request报文。

**Step 3**

在M上打开IP转发：

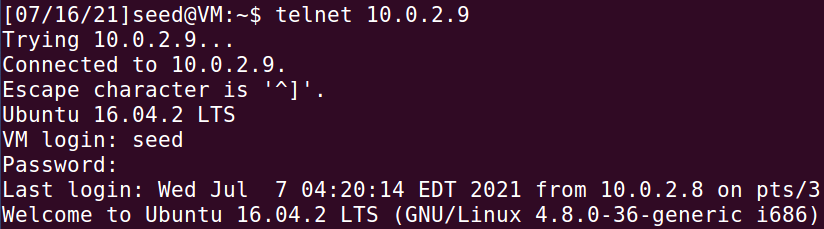


重复**Step 2**，发现在M中用Wireshark可以抓到ICMP的请求和回复报文：



**Step 4**

从A（10.0.2.8）上向B（10.0.2.9）建立telnet链接：



在M上关闭IP转发：



此时在A上输入任意字符：

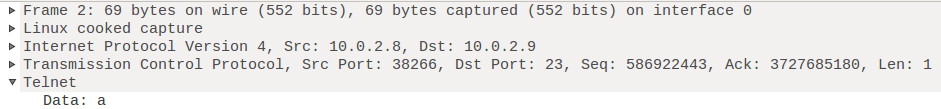


Wireshark会抓到A向B发送的ARP包：

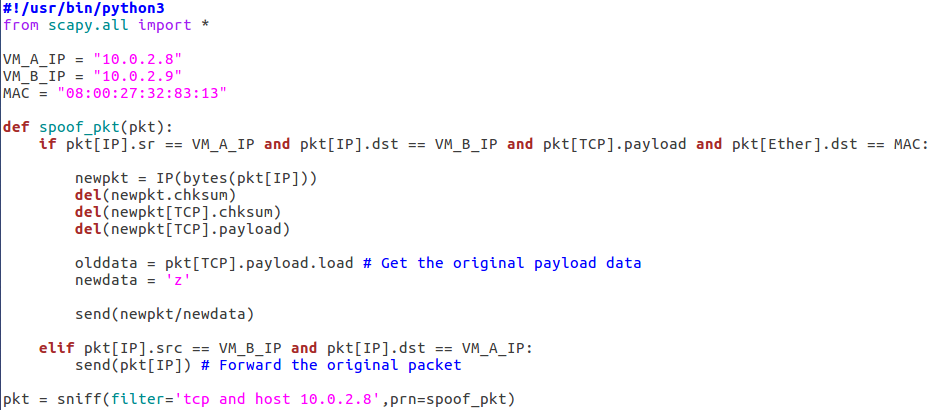


这样一来中毒的ARP会被修复。

抓到的telnet包，data为“a”：



在M上创建文件spoof.py:

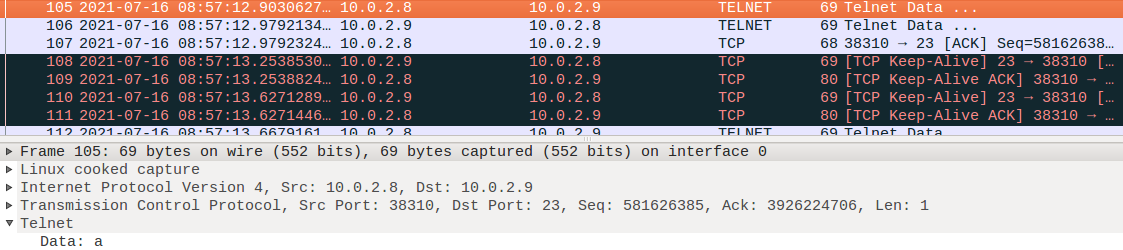


代码作用是将所有M收到的来自A的TCP报文中的数据域修改为字符“z”。

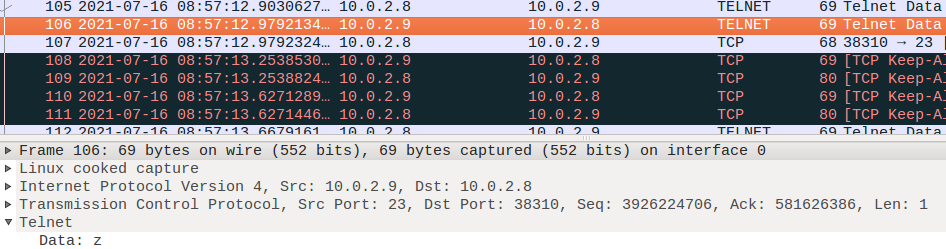
当运行spoof.py之后，A上输入任意字符都会被转换为z：



抓到的telnet包证明从A发出的数据是a：

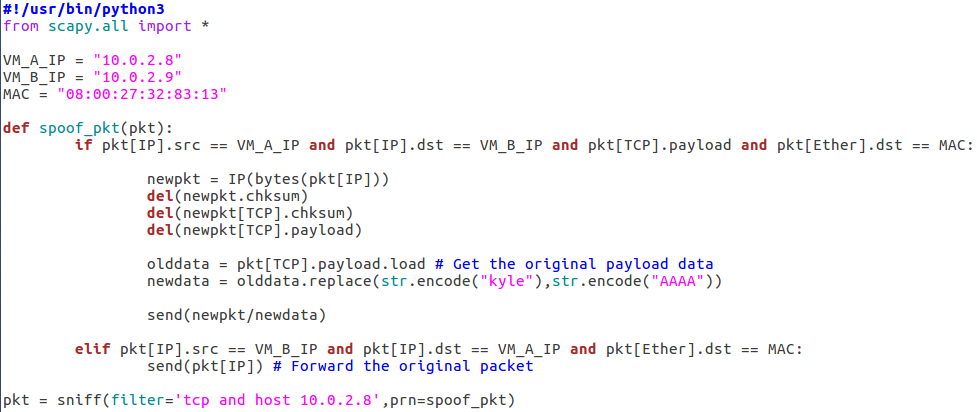


而经过M之后数据被替换为z：



**Task 3**

在M上创建文件spoof2.py:



代码作用是将所有M收到的来自A的TCP报文中数据域出现的所有“kyle”字符串替换为等长字符串“AAAA”。

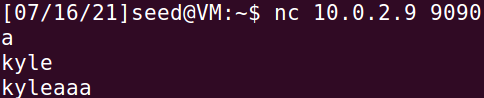
在B（10.0.2.9）上通过9090端口开启netcat：



在A（10.0.2.8）上向B发送netcat请求成功建立链接：



在A上输入任意字符：



每次传输字符之后需要重新进行ARP投毒攻击。

B上接收到的信息中，“kyle”字符被替换为“AAAA”：

