**信息安全技术实验报告**

|  |  |  |
| --- | --- | --- |
| **实验名称** | **局域网安全** | |
| **组长** | **姓名** | **学号** |
| 李骏豪 | 21307359 |
| **组员** | 李骏豪 | 21307359 |
| 梁铭恩 | 21307360 |
| 叶梓聪 | 21307417 |
| **实验分工** | | |
| **姓名** | **任务** | |
| 李骏豪 | 完成了实验1及实验报告 | |
| 叶梓聪 | 完成了实验1及实验报告 | |
| 梁铭恩 | 完成了实验2 | |

表1-1 实验中的节点名称、用户名及密码

|  |  |  |
| --- | --- | --- |
| **节点名称** | **用户名** | **密码** |
| 正常用户 | imool | imool |
| 攻击者 | kali | kali |
| 外网服务器 | root | root |

【**交报告**】使用FTP方式提交，推荐使用Filezilla客户端

地址为ftp://ftp.network-security.asia；账号与密码为：student/5ecur1ty

文件以组号（组长学号）+实验名称命名

# 实验目的

1. - 掌握ARP协议的工作原理及作用
2. - 掌握ARP投毒攻击的基本原理
3. - 深入理解局域网中交换机和路由器的作用和工作原理
4. - 深入理解局域网中的标识
5. - 思考并掌握防范ARP攻击的技术

# 实验任务

## 实验1：ARP缓存投毒攻击

1. **基于ARP Request的缓存投毒攻击**
2. 查看正常用户主机的`ARP`缓存
3. 获取正常用户主机的`MAC`地址，填写表1-2与表1-3‘攻击前’

表1-2 IP地址与MAC地址映射表

|  |  |  |  |
| --- | --- | --- | --- |
|  | 路由器局域网接口 | 正常用户 | 攻击者 |
| IP地址 |  |  |  |
| MAC地址 |  |  |  |

1. 编写攻击脚本
2. 发起攻击，填写表1-3‘ARP Request缓存投毒后’
3. 重要过程和结果截图放在实验报告的相应步骤中

表1-3 正常用户机器中的ARP缓存及说明表

|  |  |  |  |
| --- | --- | --- | --- |
| ARP缓存中的IP与MAC地址的对应关系 | | | |
|  | IP地址 | MAC地址 | 谁假冒了谁 |
| 攻击前 |  |  |  |
| ARP Request缓存投毒后 |  |  |  |
| ARP Reply缓存投毒后 |  |  |  |

1. **基于ARP Reply的缓存投毒攻击**
2. 查看ARP缓存
3. 编写攻击脚本
4. 发起攻击，填写表1-3‘ARP Reply缓存投毒后’
5. 重要过程和结果截图放在实验报告的相应步骤中
6. **思考：**ARP缓存投毒攻击后，如果正常用户再次ping路由器的GE0/2端口，会发现正常用户主机的ARP缓存恢复正常，为什么？

## 实验2：使用wireshark分析Web访问过程流量

1. **查看正常情况下的HTTP 请求**
2. 登录攻击者主机并打开wireshark监听流量；
3. 登陆正常用户主机，使用浏览器访问www.imool.com.cn网站；
4. 在攻击者主机上，编写查看过滤器规则，查看攻击者主机是否能够捕获正常用户访问www.imool.com.cn网站所产生的网络流量。
5. **编写基于ARP缓存投毒的中间人攻击脚本**

可以在`实验1：ARP缓存投毒攻击`中所实现的`ARP Reply`投毒脚本基础上，实现对正常用户主机和网关的arp缓存投毒；也可以重新编写arp投毒脚本。

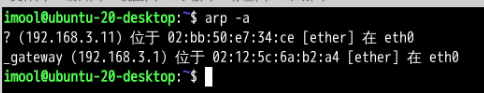
1. **发起攻击并验证攻击效果**
2. 在攻击者主机上，打开IP转发。执行以下命令（需要root权限）打开IP转发：
3. 在攻击者主机上，执行基于ARP缓存投毒的中间人攻击脚本，并监听流量。正确编写攻击脚本后，在攻击者主机上执行脚本实施基于ARP缓存投毒的中间人攻击。执行完毕后，打开`Wireshark`监听流量。
4. 在正常用户主机上，使用浏览器访问www.imool.com.cn网站，尝试使用用户名和密码登录。
5. 在攻击者主机上，验证是否可以捕获到正常用户访问www.imool.com.cn网站的网络流量，比如，是否可以捕获到正常用户输入的用户名和口令等网络流量
6. 将重要过程和结果截图，完成实验报告。
7. **思考：**
8. 为什么在该攻击过程中要打开IP转发？不打开会有什么后果？
9. 在该攻击中，使用`ARP Request`方式同时污染用户主机与网关是不可行的。试分析原因。
10. （选做）在该攻击中，正常用户主机与网关之间的通信流量均会经过攻击者主机，因此理论上攻击者可以随意修改双方通信的内容。尝试使用Scapy提供的函数，篡改www.imool.com.cn网站返回的页面内容（例如，向返回的html代码中插入一个标题：“Hacked by XXX!”）。

# 实验步骤与实验结果记录

## 实验1：ARP缓存投毒攻击

**1.基于ARP Request的缓存投毒攻击**

（1）查看正常用户主机的`ARP`缓存



（2）获取正常用户主机的`MAC`地址，填写表1-2与表1-3‘攻击前’

攻击者执行arp -a获取正常用户主机的MAC地址

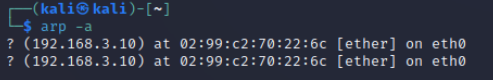


表1-2 IP地址与MAC地址映射表

|  |  |  |  |
| --- | --- | --- | --- |
|  | 路由器局域网接口 | 正常用户 | 攻击者 |
| IP地址 | 192.168.3.1 | 192.168.3.10 | 192.168.3.11 |
| MAC地址 | 02:12:5c:6a:b2:a4 | 02:99:c2:70:22:6c | 02:bb:50:e7:34:ce |

（3）编写攻击脚本



（4）发起攻击，填写表1-3‘ARP Request缓存投毒后’

（5）重要过程和结果截图放在实验报告的相应步骤中

Arp request攻击后正常用户的arp表

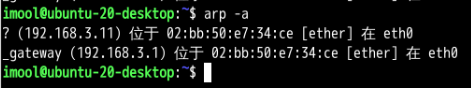


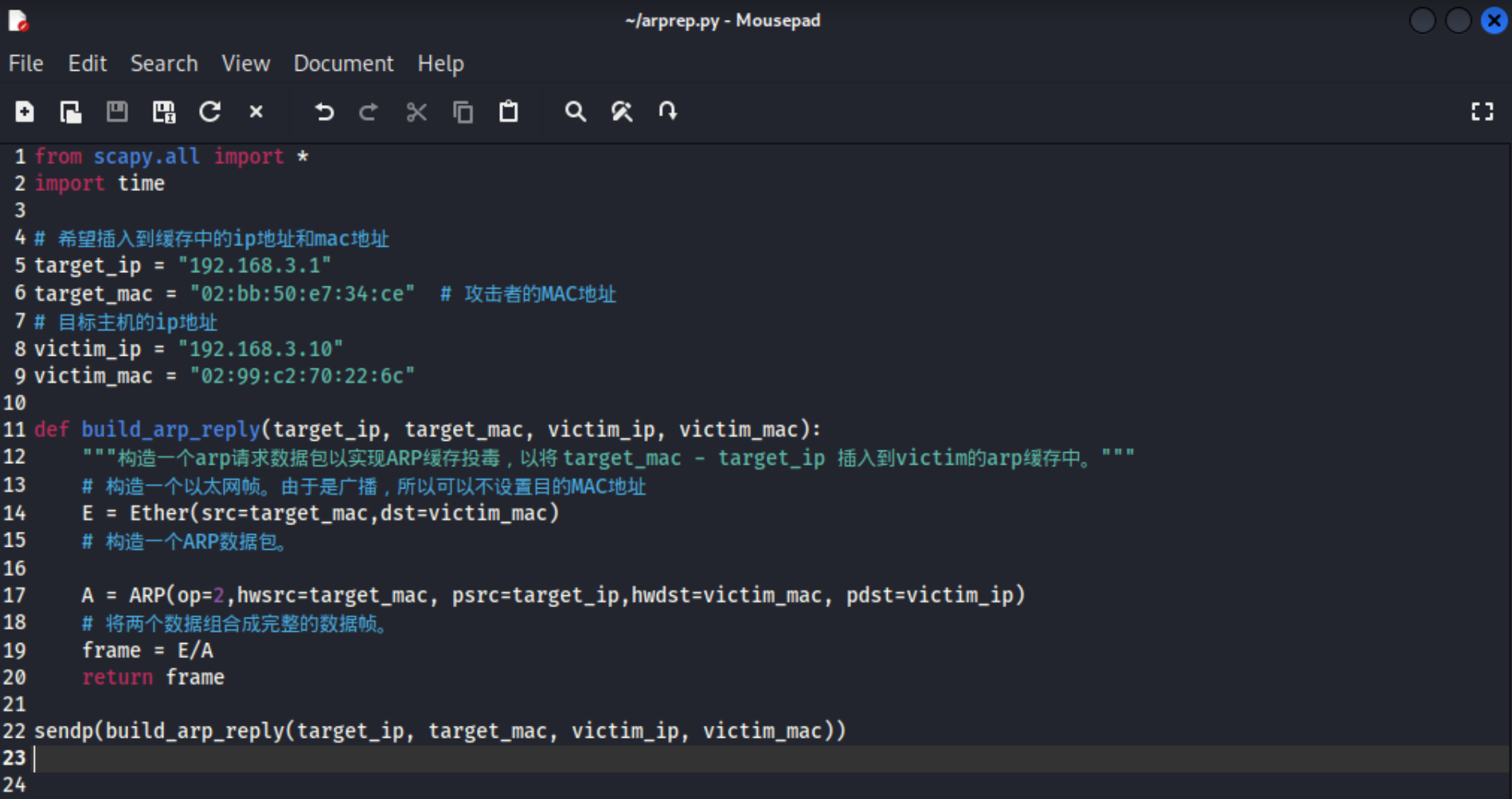
表1-3 正常用户机器中的ARP缓存及说明表

|  |  |  |  |
| --- | --- | --- | --- |
| ARP缓存中的IP与MAC地址的对应关系 | | | |
|  | IP地址 | MAC地址 | 谁假冒了谁 |
| 攻击前 | 192.168.3.1 | 02:12:5c:6a:b2:a4 | 无 |
| ARP Request缓存投毒后 | 192.168.3.1 | 02:bb:50:e7:34:ce | 攻击者假冒了网关 |
| ARP Reply缓存投毒后 | 192.168.3.1 | 02:bb:50:e7:34:ce | 攻击者假冒了网关 |

**2.基于ARP Reply的缓存投毒攻击**

（1）查看ARP缓存

（2）编写攻击脚本



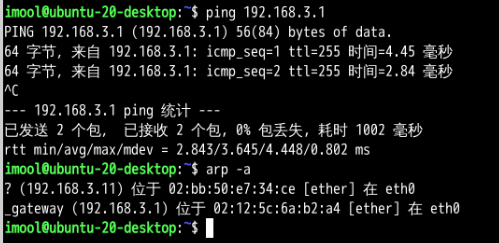
（3）发起攻击，填写表1-3‘ARP Reply缓存投毒后’

（4）重要过程和结果截图放在实验报告的相应步骤中

**3.思考：**ARP缓存投毒攻击后，如果正常用户再次ping路由器的GE0/2端口，会发现正常用户主机的ARP缓存恢复正常，为什么？

答：

会恢复正常



原因：当正常用户再次ping路由器的GE0/2端口时，他们的系统会发送一个ARP请求来查询路由器IP地址对应的MAC地址。路由器或其他正确的主机收到这个请求后，会回复一个真实的ARP回复，将正确的MAC地址告诉正常用户的主机。这样，正常用户主机的ARP缓存就会更新为正确的条目。

## 实验2：使用wireshark分析Web访问过程流量

**1.查看正常情况下的HTTP 请求**

（1）登录攻击者主机并打开wireshark监听流量；

（2）登陆正常用户主机，使用浏览器访问www.imool.com.cn网站；

（3）在攻击者主机上，编写查看过滤器规则，查看攻击者主机是否能够捕获正常用户访问www.imool.com.cn网站所产生的网络流量。

**2.编写基于ARP缓存投毒的中间人攻击脚本**

可以在`实验1：ARP缓存投毒攻击`中所实现的`ARP Reply`投毒脚本基础上，实现对正常用户主机和网关的arp缓存投毒；也可以重新编写arp投毒脚本。

**3.发起攻击并验证攻击效果**

（1）在攻击者主机上，打开IP转发。执行以下命令（需要root权限）打开IP转发：

（2）在攻击者主机上，执行基于ARP缓存投毒的中间人攻击脚本，并监听流量。正确编写攻击脚本后，在攻击者主机上执行脚本实施基于ARP缓存投毒的中间人攻击。执行完毕后，打开`Wireshark`监听流量。

（3）在正常用户主机上，使用浏览器访问www.imool.com.cn网站，尝试使用用户名和密码登录。

（4）在攻击者主机上，验证是否可以捕获到正常用户访问www.imool.com.cn网站的网络流量，比如，是否可以捕获到正常用户输入的用户名和口令等网络流量

（5）将重要过程和结果截图，完成实验报告。

**4.思考：**

（1）为什么在该攻击过程中要打开IP转发？不打开会有什么后果？

（2）在该攻击中，使用`ARP Request`方式同时污染用户主机与网关是不可行的。试分析原因。

（3）（选做）在该攻击中，正常用户主机与网关之间的通信流量均会经过攻击者主机，因此理论上攻击者可以随意修改双方通信的内容。尝试使用Scapy提供的函数，篡改www.imool.com.cn网站返回的页面内容（例如，向返回的html代码中插入一个标题：“Hacked by XXX!”）。