电子科技大学信息与软件工程学院

**实 验 报 告**

学 号 2018091618008

姓 名 袁昊男

(实验) 课程名称 网络安全攻防技术

理论教师 王瑞锦

实验教师 王瑞锦

**电子科技大学教务处制表**

**电 子 科 技 大 学**

**实 验 报 告**

**学生姓名：袁昊男 学号：2018091618008 指导教师：王瑞锦**

**实验地点：信软楼306 实验时间：2020.09.27**

**一、实验室名称：信息与软件工程学院实验中心**

**二、实验名称：ARP欺骗的验证及原理**

**三、实验学时：2学时**

**四、实验原理：**

1. **ARP地址解析协议**

地址解析协议，即ARP（Address Resolution Protocol），是根据IP地址获取物理地址的一个TCP/IP协议。主机发送信息时将包含目标IP地址的ARP请求广播到局域网络上的所有主机，并接收返回消息，以此确定目标的物理地址；收到返回消息后将该IP地址和物理地址存入本机ARP缓存中并保留一定时间，下次请求时直接查询ARP缓存以节约资源。即负责完成逻辑地址向物理地址的动态映射，将32位逻辑地址（IP地址）转化为48位物理地址（MAC地址）。

1. **ARP欺骗**

地址解析协议是建立在网络中各个主机互相信任的基础上的，它的诞生使得网络能够更加高效的运行，但其本身也存在缺陷：ARP地址转换表是依赖于计算机中高速缓冲存储器动态更新的，而高速缓冲存储器的更新是受到更新周期的限制的，只保存最近使用的地址的映射关系表项，这使得攻击者有了可乘之机，可以在高速缓冲存储器更新表项之前修改地址转换表，实现攻击。ARP请求为广播形式发送的，网络上的主机可以自主发送ARP应答消息，并且当其他主机收到应答报文时不会检测该报文的真实性就将其记录在本地的MAC地址转换表，这样攻击者就可以向目标主机发送伪ARP应答报文，从而篡改本地的MAC地址表。ARP欺骗可以导致目标计算机与网关通信失败，更会导致通信重定向，所有的数据都会通过攻击者的机器，因此存在极大的安全隐患。

**五、实验目的：**

1. 使用Kali系统验证ARP欺骗攻击；
2. 深入理解ARP协议与欺骗攻击原理，并提出防范措施。

**六、实验内容：**

1. 使用Kali系统中“arpspoof -i [网卡] -t [目标IP] [网关]”命令实现对虚拟机的ARP欺骗攻击；
2. 分析实验结果，深入理解ARP协议与欺骗攻击原理，并提出防范措施。

**七、实验器材（设备、元器件）：**

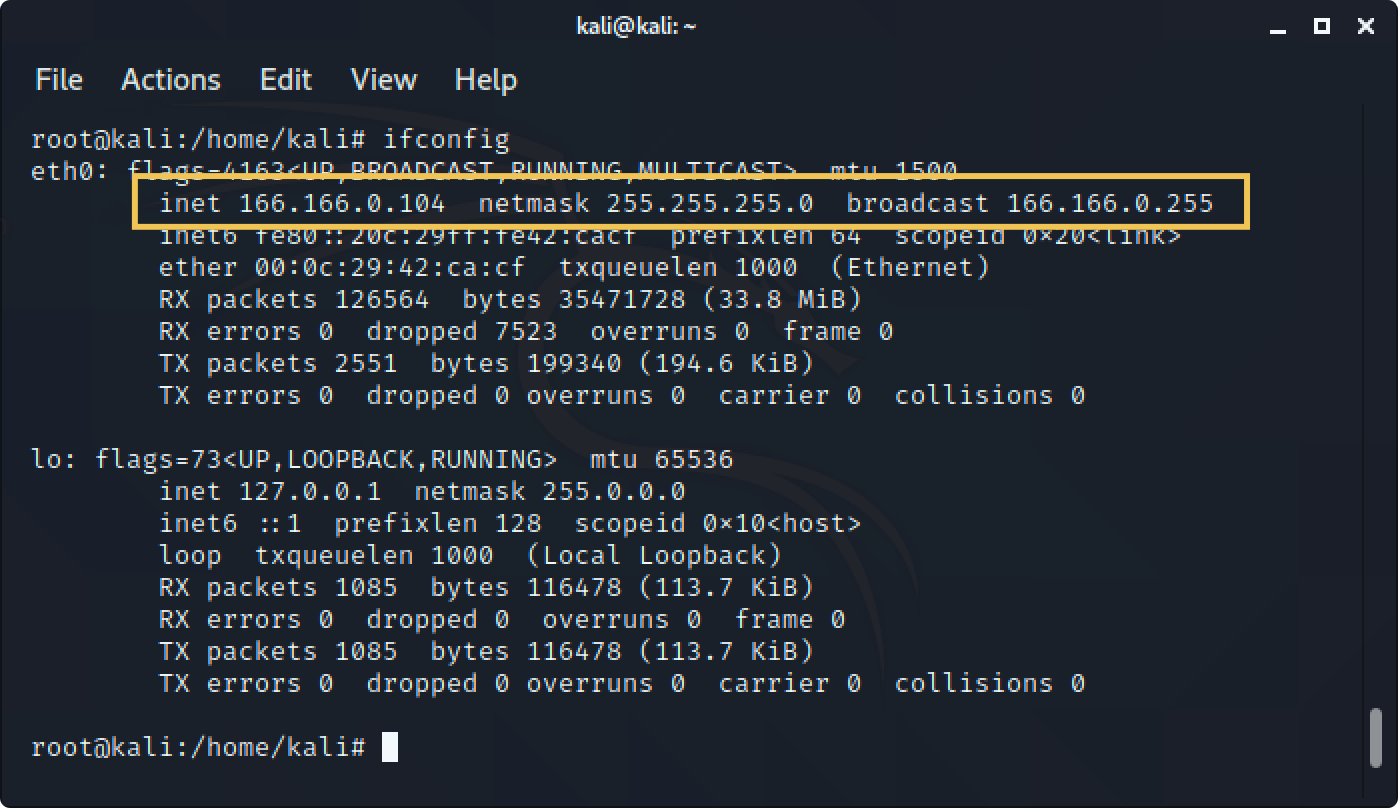
1. 个人PC一台并安装有VMware虚拟机软件和Kali系统；
2. 攻击机与被攻击机处于同一局域网中，其中攻击机安装有Kali系统。

**八、实验步骤：**

1. 检查攻击机与被攻击机是否处于同一局域网内，并使用ping命令或打开网页测试被攻击机能否连接到互联网。
2. 获取局域网的网关地址、被攻击机的局域网IP地址。
3. 在攻击机Kali系统命令行工具中使用“fping -asg [网络号/前缀]”命令扫描局域网内的在线主机。
4. 在攻击机Kali系统命令行工具中使用“arpspoof -i [网卡] -t [目标IP] [网关]”命令发起ARP欺骗攻击。
5. 验证被攻击机在ARP欺骗攻击发起与停止后的联网情况。
6. 分析实验结果，提出ARP欺骗攻击的防范措施，撰写实验报告。

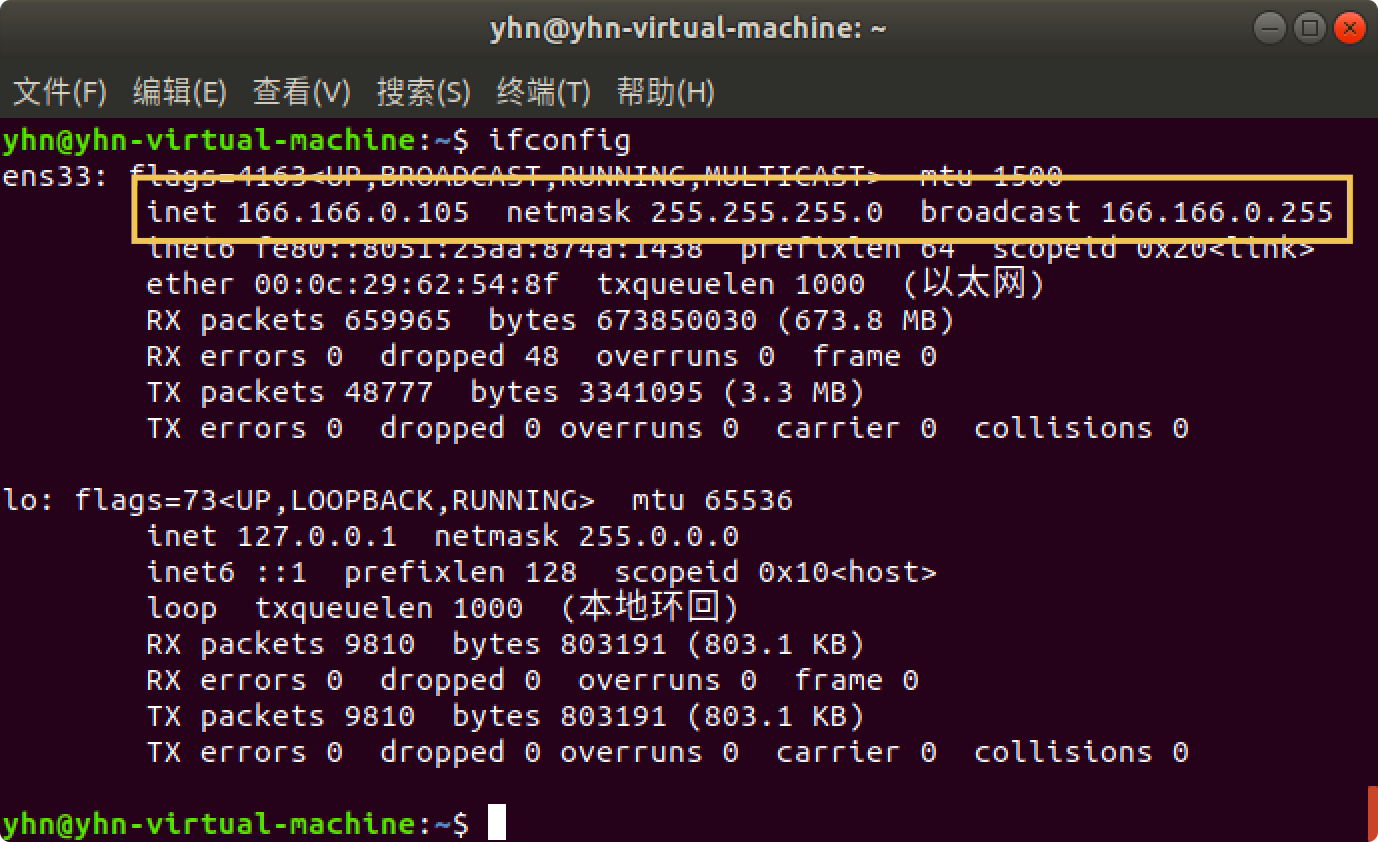
**九、实验数据及结果分析**

1. **查看攻击机网络配置**



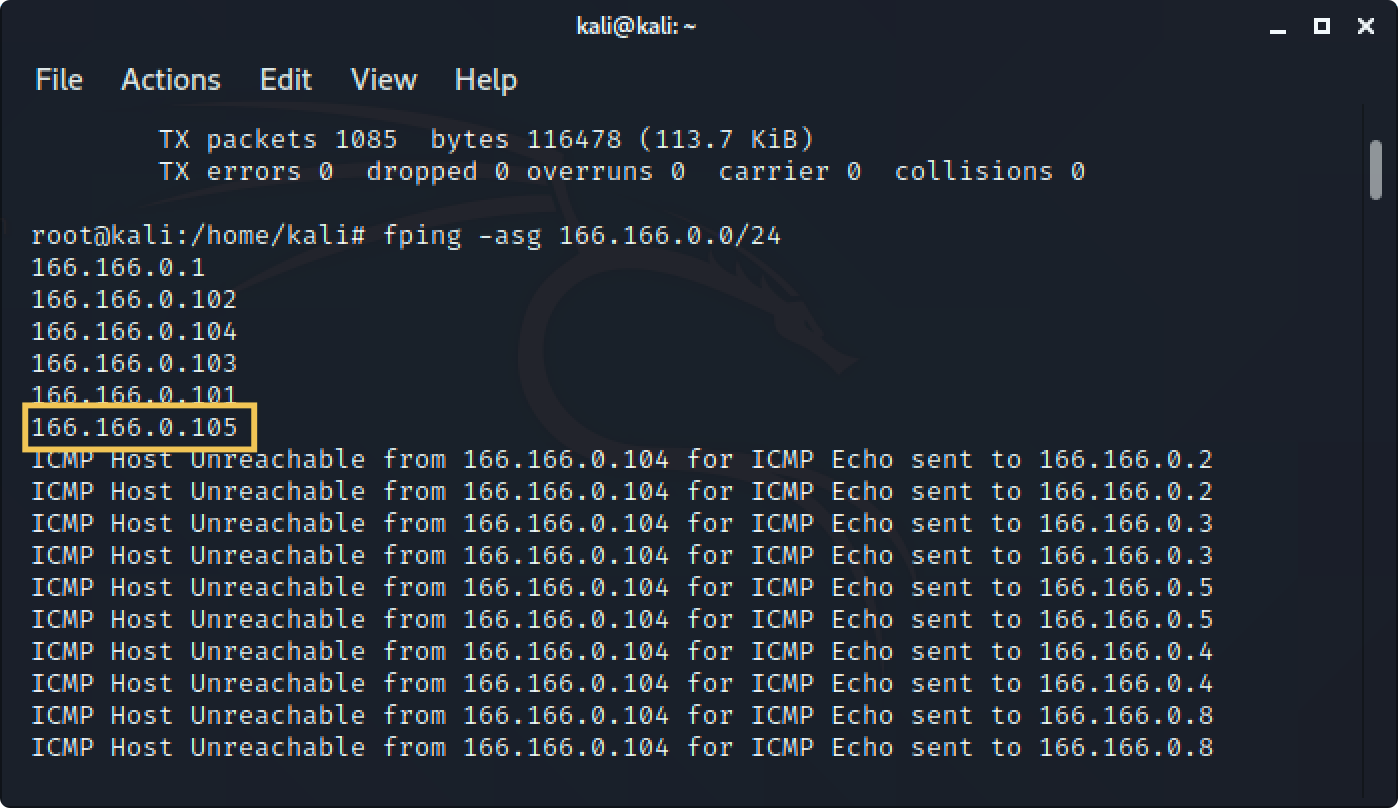
**可以看出：**攻击机网卡为eth0，局域网IP地址为166.166.0.104，局域网网关为166.166.0.1。

1. **查看被攻击机网络配置**



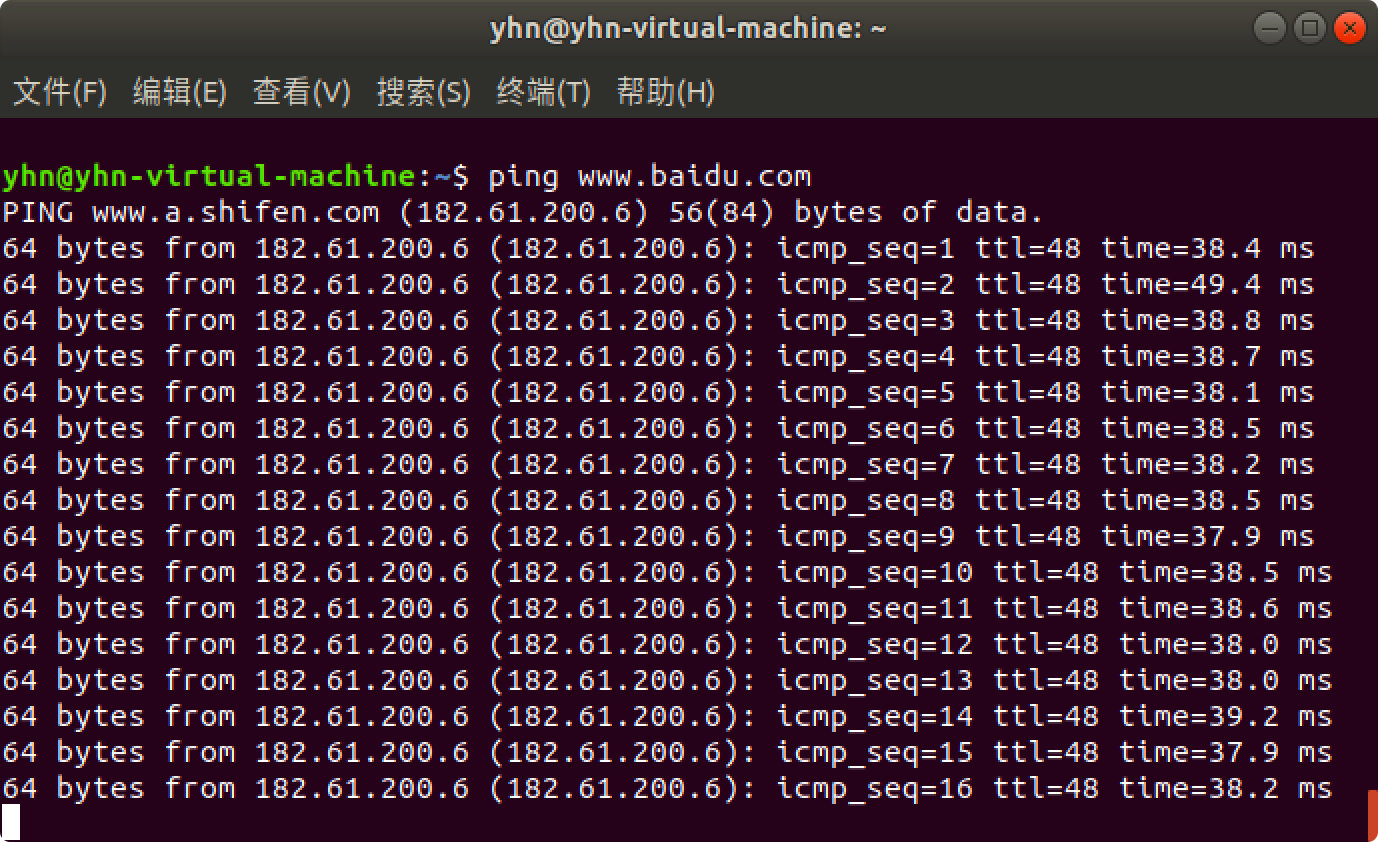
**可以看出：**被攻击机局域网IP地址为166.166.0.105，局域网网关为166.166.0.1。可以验证攻击机与被攻击机处于同一局域网中。

1. **扫描局域网中在线主机**



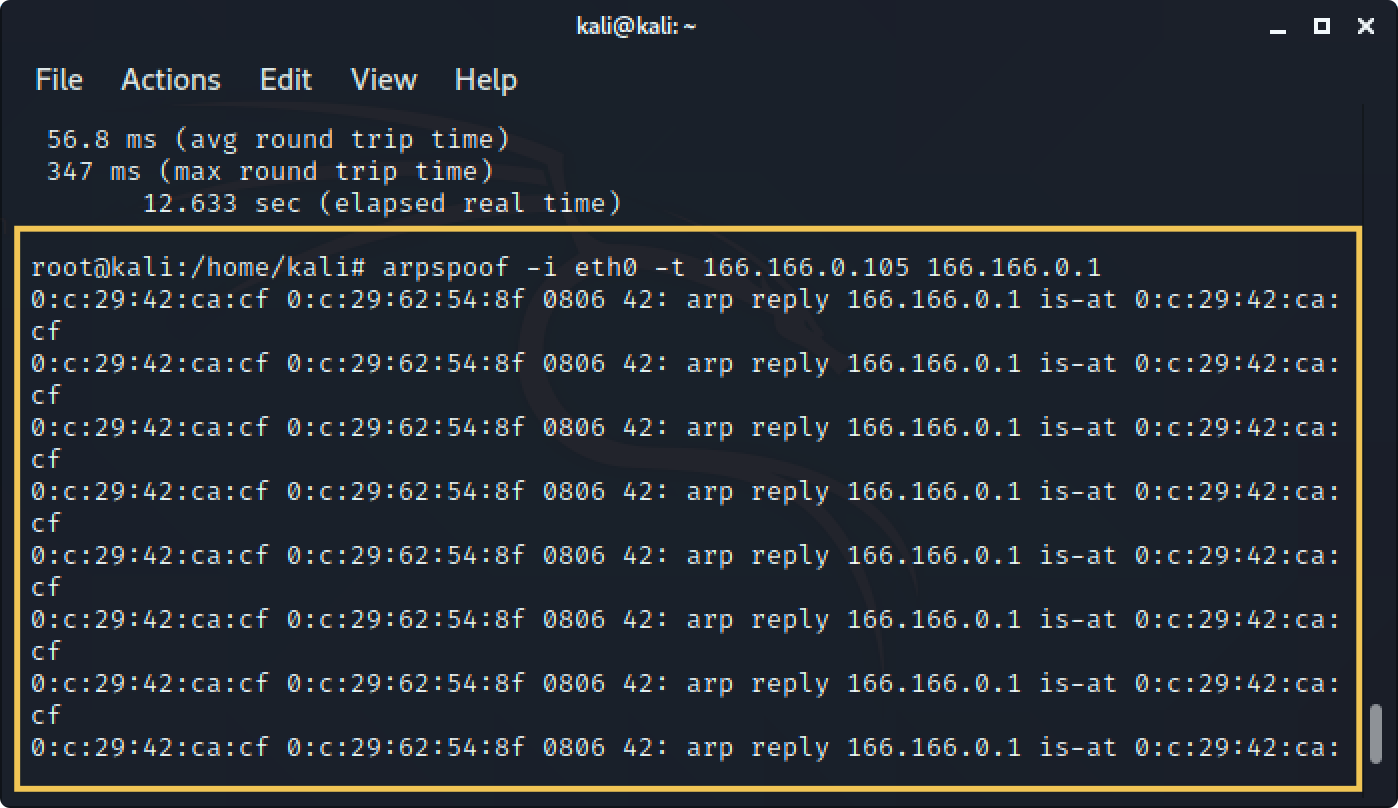
**可以看出：**被攻击机166.166.0.105出现在扫描得到的主机列表中。

1. **检查被攻击机在被攻击前的联网情况**



**可以看出：**使用“ping www.baidu.com”命令连接百度服务器成功，说明此时被攻击机可以正常联网。

1. **发起ARP欺骗攻击**



**可以看出：**使用“arpspoof -i eth0 -t 166.166.0.105 166.166.0.1”命令后，攻击机发起ARP欺骗攻击，成功冒充被攻击机的MAC地址，网关将本应转发至被攻击机的数据转发到攻击机。

1. **检查被攻击机在被攻击后的联网情况**



**可以看出：**被攻击机已经无法成功连接至互联网，说明ARP攻击成功。在攻击机中使用“ctrl+Z”命令即可终止arpspoof命令，被攻击机即可正确连接至互联网（若仍不能上网，则需要清除ARP缓存）。

**十、实验结论**

使用Kali系统中的arpspoof命令可成功对处于同一局域网中的主机发起ARP欺骗攻击。

**十一、总结及心得体会**

ARP欺骗攻击简单易行，同时说明ARP协议有非常高的安全风险，需要采取措施防范：

1. **主机级被动检测：**当系统接收到来自局域网上的ARP请求时，系统检查该请求发送端的IP地址是否与自己的IP地址相同。如果相同，则说明该网络上另有一台机器与自己具有相同的IP地址。
2. **主机级主动监测：**主机定期向所在局域网发送查询自己IP地址的ARP请求报文。如果能够收到另一ARP响应报文，则说明该网络上另有一台机器与自己具有相同的IP地址。
3. **服务器级检测：**当服务器收到ARP响应时，为了证实它的真实性，根据反向地址解析协议（RARP）就用从响应报文中给出的MAC地址再生成一个RARP请求，它询问这样一个问题：“如果你是这个MAC地址的拥有者，请回答你的IP地址”。这样就会查询到这个MAC地址对应的IP地址，比较这两个IP地址，如果不同，则说明对方伪造了ARP响应报文。
4. **网络级检测：**配置主机定期向中心管理主机报告其ARP缓存的内容。这样中心管理主机上的程序就会查找出两台主机报告信息的不一致，以及同一台主机前后报告内容的变化。这些情况反映了潜在的安全问题。或者利用网络嗅探工具连续监测网络内主机硬件地址与IP地址对应关系的变化。

**十二、对本实验过程及方法、手段的改进建议**

本实验设计与教材结合紧密、难度适中，通过对ARP欺骗攻击问题的实现，强化了学生对ARP协议、ARP欺骗攻击原理等知识点的理解与掌握。此外，还使学生熟悉Kali系统的基本环境，了解Kali系统下的攻击操作，对网络安全攻防技术的深入学习打下了坚实的基础。

**报告评分：**

**指导教师签字：**