 网络协议分析

**ARP欺骗和协议数据分析报告**

2019/3/21

1. **ARP欺骗原理**

ARP原理：某机器A要向主机B发送报文，会查询本地的ARP缓存表，找到B的IP地址对应的MAC地址后，就会进行数据传输。如果未找到，则A广播一个ARP请求报文（携带主机A的IP地址Ia——物理地址Pa），请求IP地址为Ib的主机B回答物理地址Pb。网上所有主机包括B都收到ARP请求，但只有主机B识别自己的IP地址，于是向A主机发回一个ARP响应报文。其中就包含有B的MAC地址，A接收到B的应答后，就会更新本地的ARP缓存。接着使用这个MAC地址发送数据（由网卡附加MAC地址）

欺骗原理：ARP是无状态协议，接收到ARP应答包后不会检验是否曾经发出过ARP请求包便会更新ARP状态表。ARP这个缺陷为实现ARP欺骗提供了可能。

1. **ARP欺骗实现的方法**

主机在实现ARP缓存表的机制中存在一个 不完善的地方，当主机收到一个ARP应答 包后，它并不会去验证自己是否发送过这个 ARP请求，而是直接将应答包里的MAC地址与IP对应的关系替换掉原有的ARP缓存表里的相应信息，ARP欺骗正是利用了这一点从而使得之后原先要发到别的mac地址的数据被发到黑客的主机。

1. **ARP欺骗的实现过程**

使用工具：

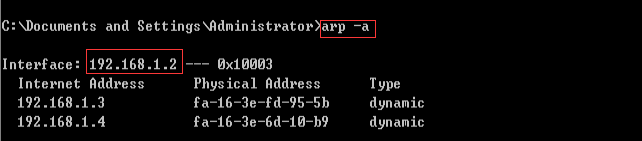
* window7操作系统
* cain

实验过程：使用cain进行arp欺骗

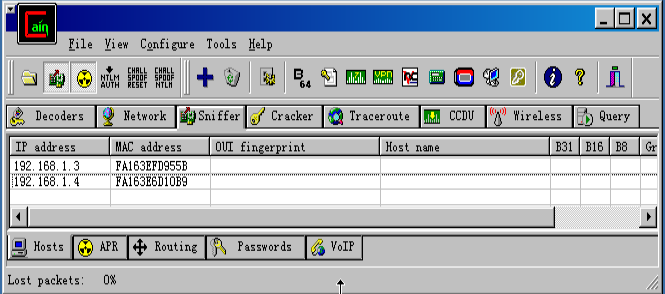
使用同在一个局域网中的攻击机和两台靶机进行实验。三者能ping通



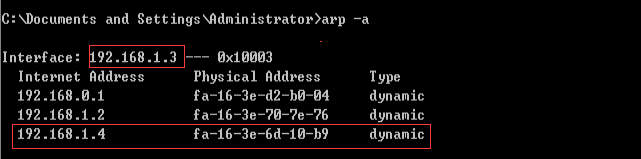
攻击机看arp 缓存 arp –a

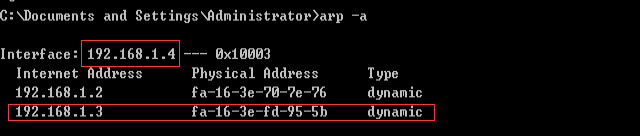


使用cain扫描局域网中所有MAC地址

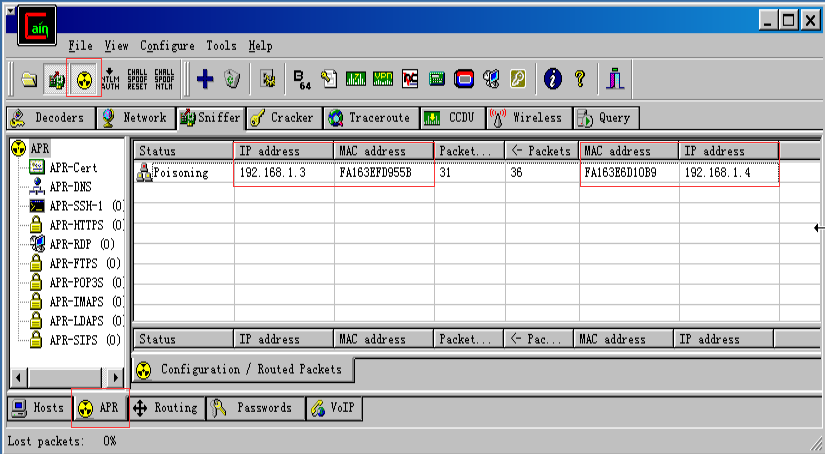


两台靶机分别查看本地arp



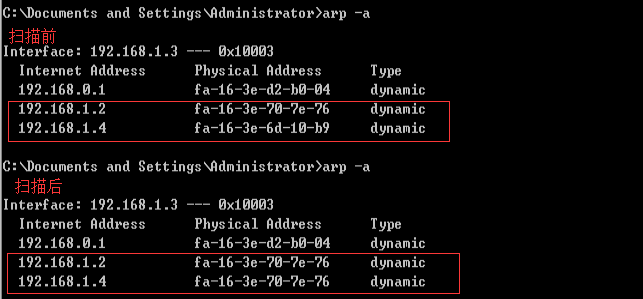


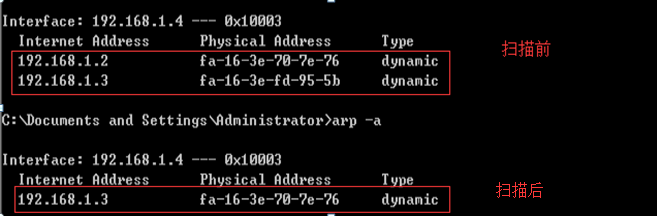
使用cain开启arp欺骗



1. **ARP欺骗的实现结果**

查看当前被欺骗主机的arp 可见两者对对方的mac都被修改为攻击机的mac地址





班级：16272412

学号：16272203

姓名：黄萍萍