《信息安全及实践》课程实验报告

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 学院： | 信息学院 | 专业： | 计算机科学与技术 | 年级： | 2019 |

|  |  |  |  |
| --- | --- | --- | --- |
| 姓名： | 白文强 | 学号： | 20191060064 |
| 姓名： | 赵浩杰 | 学号： | 20191060074 |
| 姓名： | 李泽昊 | 学号： | 20191060065 |

|  |  |
| --- | --- |
| 实验时间： | 2021年10月08日 |

|  |  |
| --- | --- |
| 实验名称： | MAC地址欺骗攻击实验和Smurf攻击实验 |

|  |  |
| --- | --- |
| 实验成绩： |  |

MAC地址欺骗攻击实验

一、实验目的

(1)验证交换机建立MAC表(转发表) 过程。

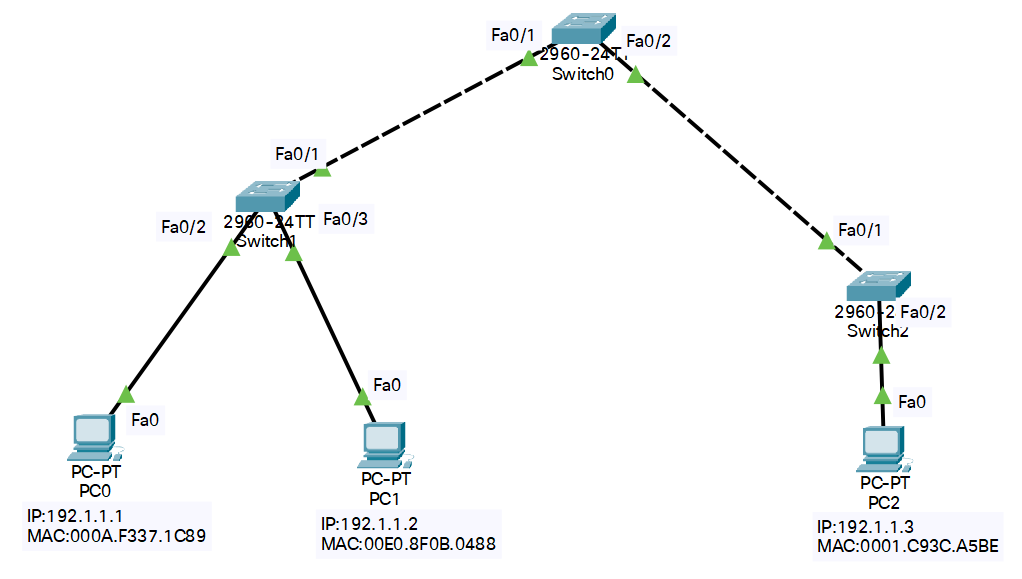
(2)验证交换机转发MAC帧机制。

(3)验证MAC地址欺骗攻击原理。

(4)掌握MAC地址欺骗攻击过程。

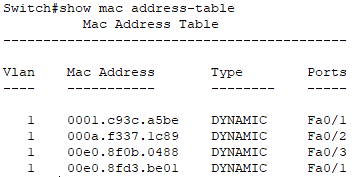
二、实验步骤

(1)设备放置并连接，并配置IP地址及子网掩码，查看MAC地址

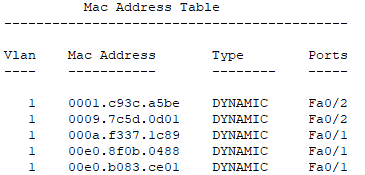


(2) 完成PC0 PC1和PC2两两之间的ICMP报文传输过程，查看MAC地址转发表

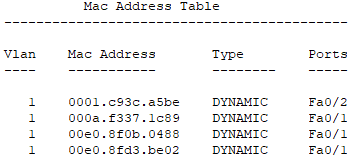
**switch1：**



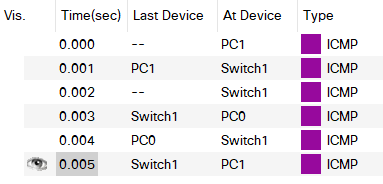
**switch0：**



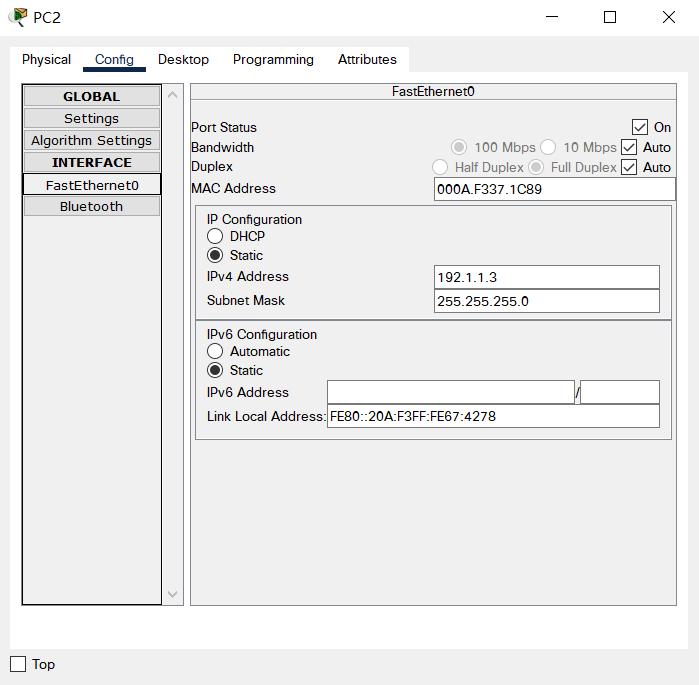
**switch2：**

****

(3)切换到模拟操作模式，进入“EditFilters”配置界面，勾选协议ICMP。通过简单报文工具启动PC1至PC0的ICMP报文传输过程。

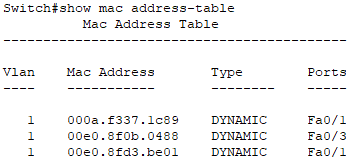


(4)切换到实时操作模式。修改PC2的MAC地址改为PC0的MAC地址000A.F337.1C89。

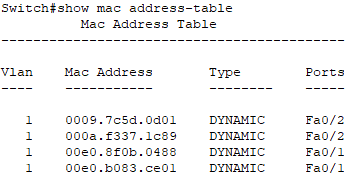


(5)通过简单报文工具启动PC2到PC1的ICMP报文传输过程。查看交换机的MAC地址转发表。

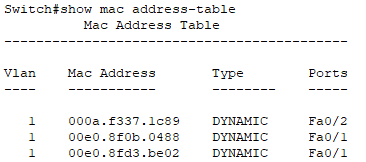
switch1:



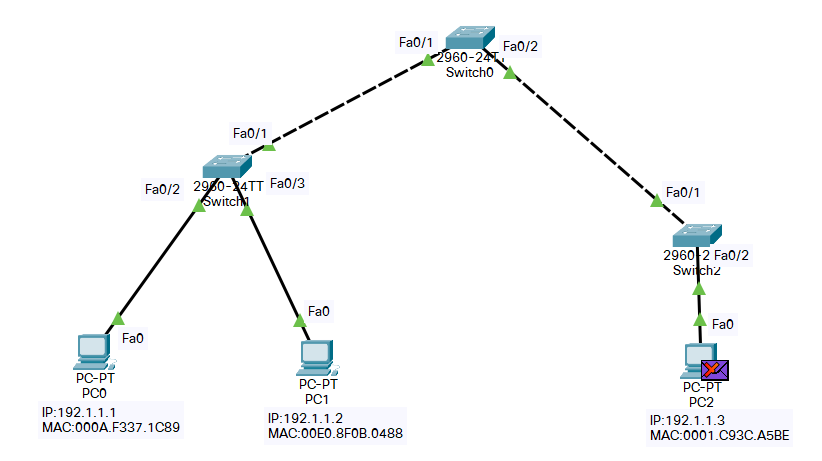
switch0:

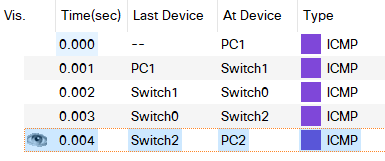


switch2:



(7)切换到模拟操作模式，通过简单报文工具启动PC1至PC0的ICMP报文传输过程。





三、实验结果及分析

连接设备并设置完IP地址后，PC0、PC1、PC2之间可以两两ping通，设备连接及配置没有问题。

随后在模拟操作模式进行PC0和PC1之间的ICMP通信，可以看到，ICMP报文从PC1到switch1再到PC0，再由PC0经switch1到达PC1，报文没有到达switch0、switch2和PC2，证明本次ICMP通信正常。

将PC2的MAC地址改为PC0的MAC地址后，再进行PC2和PC1之间的ICMP报文通信，由于PC2的MAC地址和PC0相同，且PC2与PC1之间进行了一次ICMP报文通信，在交换机中的MAC地址转发表中，到达MAC地址000A.F337.1C89 (即PC0 MAC地址)的报文会被转发到switch0进而转发到PC2。在实验中也可以看到，从PC1发出的ICMP报文，没有到达PC0，而是经过switch0、switch2到达PC2，且PC2没有接收该报文，MAC欺骗攻击成功。

四、实验总结及体会

在实验中并未遇到比较棘手的困难，遇到的最大问题是对软件模拟的不熟悉，一开始没有找到简单报文工具和复杂报文工具，不知道具体的模拟仿真流程，但经过研究探索，对软件的模拟仿真流程有了一些熟悉。随后的实验便比较顺利了。

实验总结：MAC地址欺骗可以利用交换机端口学习的漏洞，通过客户端向交换机发送欺骗报文、攻击交换机的CAM表的方式，使交换机CAM表的记录与真实的主机对应MAC地址不一致，从而使交换机将报文错误转发给攻击者.

Smurf攻击实验

一、实验目的

(1)验证ICMPECHO请求、响应过程。

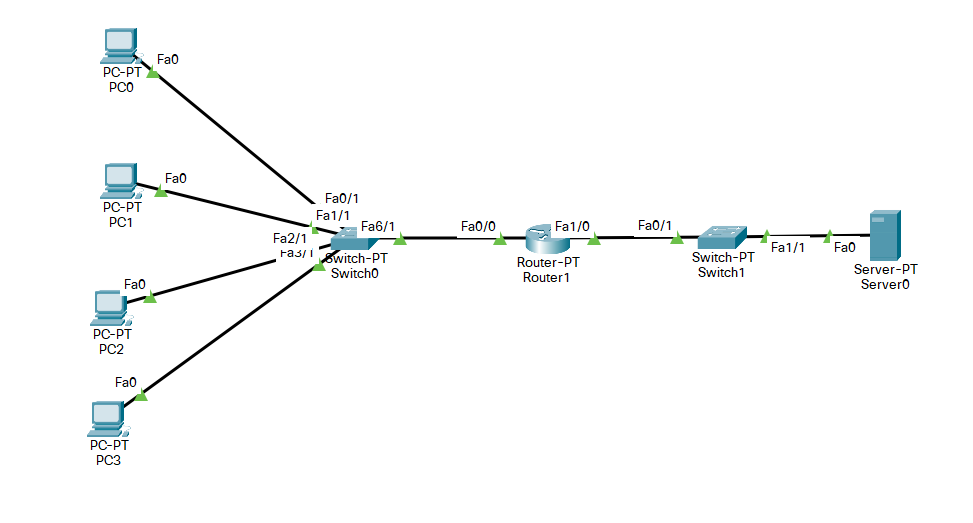
(2)验证网络放大ICMPECHO响应报文的过程。

(3)验证间接攻击原理。

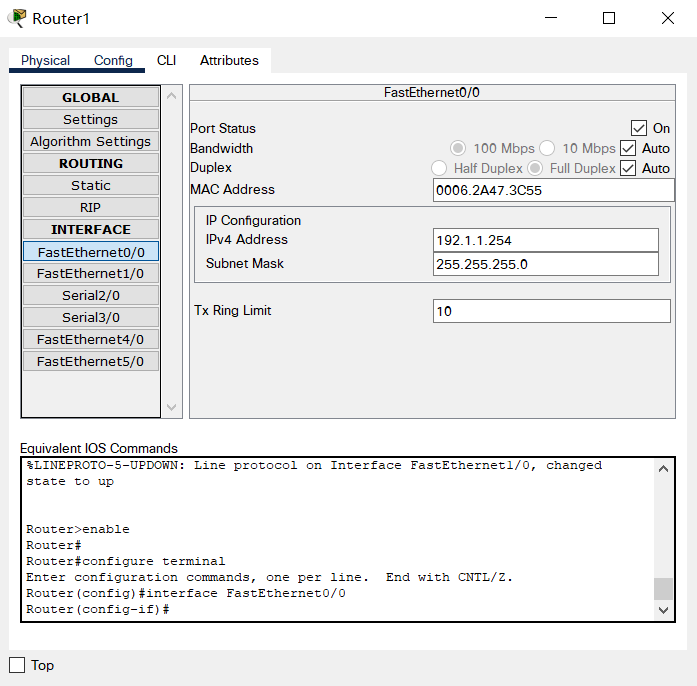
(4)验证Smurf攻击过程。

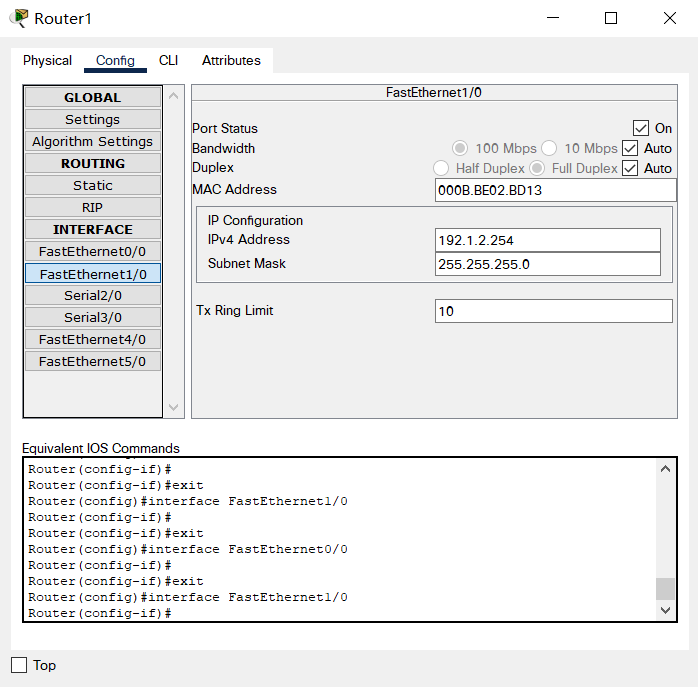
二、实验步骤

(1)启动PacketTracer，放置和连接设备。

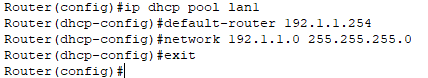


(2)完成路由器接口IP、子网掩码配置

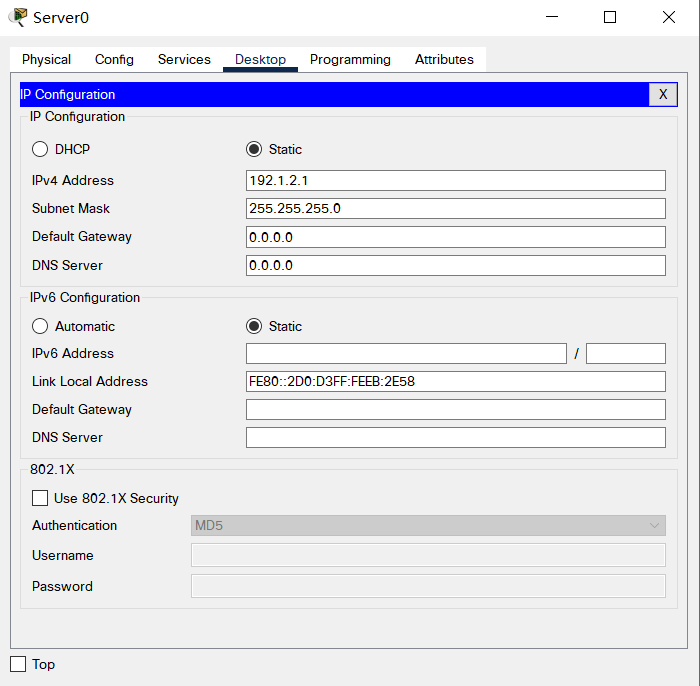




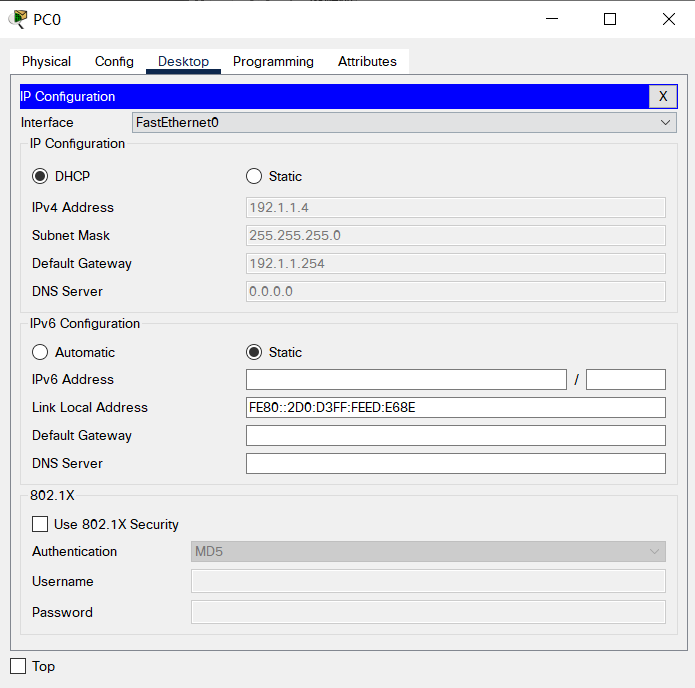
(3)完成路由器Router DHCP服务器配置过程



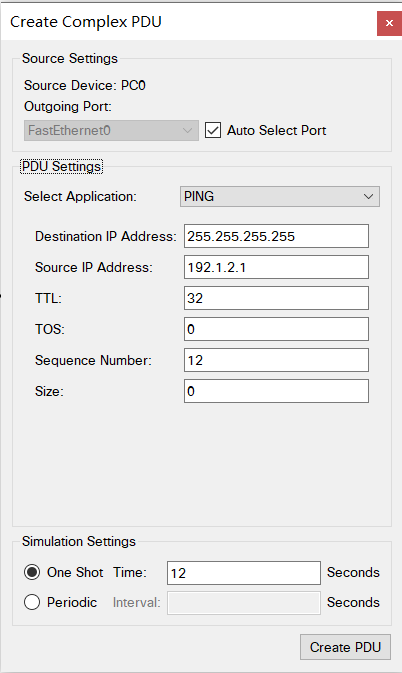
(4)完成Web服务器网络信息配置过程



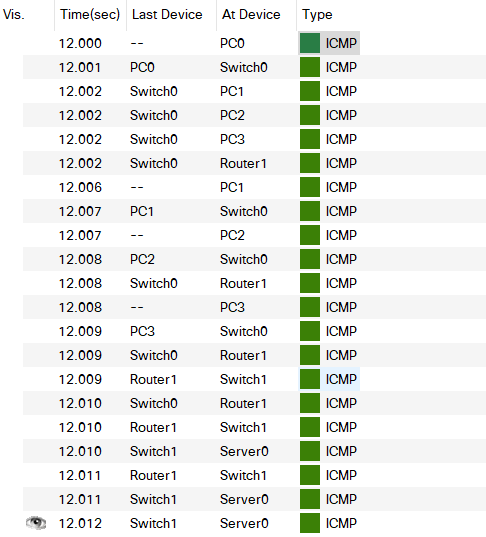
(5)给PC0、PC1、PC2、PC3配置DHCP，使其可以自动获取网络信息



(6)切换到模拟操作模式，通过复杂报文工具在PC0上生成ICMP ECHO请求报文，该ICMP ECHO请求报文封装成源IP地址是Web服务器的IP地址192.1.2.1、目的IP地址是全1的广播地址的IP分组。该IP分组在由Switch1构成的以太网上广播，到达所有其他终端和路由器Router。



(7)进行ICMP通信



三、实验结果及分析

由模拟状态下ICMP通信结果看到，最终Server0收到了ICMP报文。

分析：终端A将ICMPECHO请求报文封装成以Web服务器的IP地址为源IP地址、以全1广播地址为目的IP地址的IP分组，该ICMPECHO请求报文到达LAN1中的所有其他终端和路由器R，接收到该ICMPECHO请求报文的终端均发送ICMPECHO响应报文，由于请求报文中的源IP地址为Web服务器的IP地址，因此，这些ICMPECHO响应报文都被封装成以Web服务器的IP地址为目的IP地址的IP分组，导致ICMPECHO响应报文全部到达Web服务器。

四、实验总结及体会

这种攻击方法结合使用了IP欺骗和ICMP回复方法使大量网络传输充斥目标系统。可以试想，如果一个网络上的拥有足够多的终端，若有人利用Smurf攻击对一台Web服务器进行拒绝服务攻击，通过伪造报文源IP地址为服务器，目的IP地址广播，散步到各个终端，设置周期短、次数高的复杂报文发送，通过各个终端进行回复的报文进行占用服务器的网络信道，造成信道拥塞，使得服务器在短时间内无法与外界进行通信，造成可用性的缺失。