警示：实验报告如有雷同，雷同各方当次实验成绩均以 0 分计；在规定时间内未上交实验报告的，不得以其他方式补交，当次成绩按 0 分计；实验报告文件以 PDF 格式提交。

院系	软件学院	班级	6	学号	13331233	姓名	孙中阳
完成日期： 2016 年 11 月 11 日							

ARP 测试与防御实验

【实验名称】

ARP测试与防御。

【实验目的】

使用交换机的ARP检查功能，防止ARP欺骗攻击。

【实验原理】

ARP（Address Resolution Protocol，地址解析协议）是一个位于 TCP/IP 协议栈中的低层协议，负责将某个 IP 地址解析成对应的 MAC 地址。

(1) 对路由器 ARP 表的欺骗

原理：截获网关数据。它通知路由器一系列错误的内网 MAC 地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在路由器中，结果路由器的所有数据只能发送给错误的 MAC 地址，造成正常 PC 无法收到信息。

(2) 对内网 PC 的网关欺骗

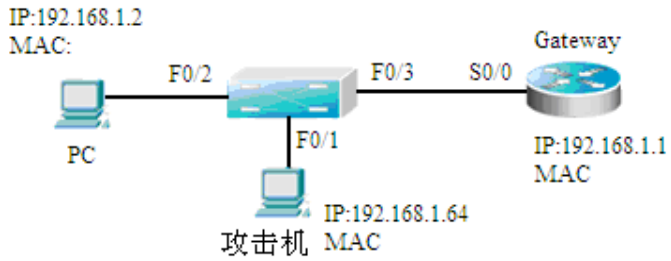
原理：伪造网关。它的原理是建立假网关，让被它欺骗的 PC 向假网关发数据，而不是通过正常的路由器途径上网。在 PC 看来，就是上不了网了，“网络掉线了”。

交换机的 ARP 检查功能，可以检查端口收到的 ARP 报文的合法性，并可以丢弃非法的 ARP 报文，防止 ARP 欺骗攻击。

【需求分析】

ARP欺骗攻击是目前内部网络出现的最频繁的一种攻击。对于这种攻击，需要检查网络中ARP报文的合法性。交换机的ARP检查功能可以满足这个要求，防止ARP欺骗攻击。

【实验拓扑】



ARP 实验拓扑图（例）

【实验设备】

交换机1台；

PC机2台（其中一台需要安装ARP欺骗攻击工具WinArpSpoofer）；

路由器 1 台（作为网关）。

【实验步骤】

说明：本次实验是我与谭潇同学在实验中心B403合作完成。谭潇同学使用IP为192.168.1.64的机器作为攻击机，而我则使用IP为192.168.1.2的机器作为攻击机，相当于进行了两轮实验，在实验中攻防对调

步骤1 配置IP地址，测试网络连通性。

按照拓扑图正确配置PC机、攻击机、路由器的IP地址，使用ping命令验证设备之间的连通性，保证可以互通。查看PC机本地的ARP缓存，ARP表中存有正确的网关的IP与MAC地址绑定，在命令窗口下，arp –a。

```
C:\Users\B403>ping 192.168.1.1

正在 Ping 192.168.1.1 具有 32 字节的数据:
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=64

192.168.1.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 1ms, 平均 = 0ms

C:\Users\B403>ping 192.168.1.2

正在 Ping 192.168.1.2 具有 32 字节的数据:
来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=128

192.168.1.2 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\B403>arp -a

接口: 192.168.1.64 --- 0xb
  Internet 地址         物理地址              类型
  192.168.1.1           00-1a-a9-3d-7f-de     动态
  192.168.1.2           6c-62-6d-86-13-58     动态
  192.168.1.255         ff-ff-ff-ff-ff-ff     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  224.0.1.140           01-00-5e-00-01-8c     静态

接口: 172.16.20.2 --- 0xc
  Internet 地址         物理地址              类型
  172.16.0.1            00-09-4c-e9-fd-b5     动态
  172.16.255.255        ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  224.0.1.140           01-00-5e-00-01-8c     静态

C:\Users\B403>
```

结果如图，被攻击机可以ping通路由器和攻击机。

Arp －a 的结果显示，攻击机的 MAC 地址是 6C62.6D86.1358。

步骤2 在攻击机上运行WinArpSpoofer软件（在网络上下载）后，在界面“Adapter”选项卡中，选择正确的网卡后，WinArpSpoofer会显示网卡的IP地址、掩码、网关、MAC地址以及网关的MAC地址信息。

步骤3 在WinArpSpoofer配置

在WinArpSpoofer界面中选择“Spoofing”标签，打开“Spoofing”选项卡界面；

在“Spoofing”页面中，取消选中“Act as a Router（or Gateway）while spoofing.”选项。如果选中，软件还将进行ARP中间人攻击。点选“->Gateway”，配置完毕后，单击“OK”按钮。

步骤4 使用WinArpSpoofer进行扫描。

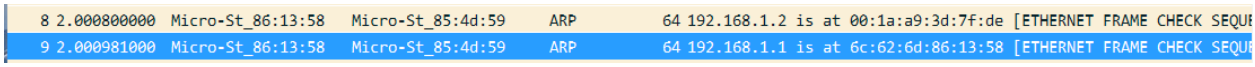
单击工具栏中的“Scan”按钮，软件将扫描网络中的主机，并获取其IP地址、MAC地址等信息。

步骤5 进行ARP欺骗。

单击工具栏中的“Start”按钮，软件将进行ARP欺骗攻击。

步骤6 验证测试。

通过使用Wireshark捕获攻击机发出的报文，可以看出攻击机发送了经过伪造的ARP应答（Reply）报文。



抓包数据显示 ，攻击机 确实 发送了 伪造的 ARP应答。

步骤7 验证测试。

使用PC机ping网关的地址，发现无法ping通。查看PC机的ARP缓存，可以看到PC机收到了伪造的ARP应答报文后，更新了ARP表，表中的条目为错误的绑定，即网关的IP地址与攻击机的MAC地址进行了绑定。这可在命令窗口下用arp –a进行显示。

结果如图，被攻击机已经不能ping通路由器。

Arp －a结果显示，路由器和攻击机的MAC地址对调了，这说明被攻击机被ARP攻击成功。

步骤8 配置ARP检查，防止ARP欺骗攻击。

在交换机连接攻击者PC的端口上启用ARP检查功能，防止ARP欺骗攻击。

Switch(config)#interface fastEthernet 0/1

Switch(config-if)#switchport port-security

Switch(config-if)#switchport port-security mac-address [MAC] ip-address [IP] ！将攻击者的MAC地址与其真实的IP地址绑定（MAC、IP以实际值代入）。

```
20-S5750-1#configure
Enter configuration commands, one per line.  End with CNTL/Z.
20-S5750-1(config)#interface gigabitEthernet 0/2
20-S5750-1(config-if-GigabitEthernet 0/2)#switchport port-security
20-S5750-1(config-if-GigabitEthernet 0/2)#$c-address 6C62.6D86.1358 ip-address$
20-S5750-1(config-if-GigabitEthernet 0/2)#exit
20-S5750-1(config)#
```

步骤9 验证测试。

启用 ARP 检查功能后，当交换机端口收到非法 ARP 报文后，会将其丢弃。这时在 PC 机上查看 ARP 缓存，可以看到 ARP 表中的条目是正确的，且 PC 可以 ping 通网关。（注意：由于 PC 机之前缓存了错误的 ARP 条目，所以需要等到错误条目超时或者使用 arp –d 命令进行手动删除之后，PC 机才能解析出正确的网关 MAC 地址。

```
C:\Users\B403>ping 192.168.1.1

正在 Ping 192.168.1.1 具有 32 字节的数据:
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=64

192.168.1.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\B403>arp -a

接口: 192.168.1.64 --- 0xb
  Internet 地址         物理地址              类型
  192.168.1.1           00-1a-a9-3d-7f-de     动态
  192.168.1.2           6c-62-6d-86-13-58     动态
  192.168.1.255         ff-ff-ff-ff-ff-ff     静态
  224.0.0.252           01-00-5e-00-00-fc     静态

C:\Users\B403>
```

【实验思考】

(1) ARP 欺骗攻击比较常见，讨论有那些普通适用的防御措施。

a) 像实验中所采取的策略一样，将 IP 地址与 MAC 绑定；

b) 采用支持 ARP 过滤的防火墙；

c) 建立 DHCP 服务器；

d) 划分安全区域。

(2) 在 IPv6 协议下，是否有 ARP 欺骗攻击？

IPV4 中的 ARP 攻击在 IPV6 对应于 ND 攻击,因为 ARP 协议对应于 IPV6 的 ND 协议。ND 协议设 计同 ARP 有类似弱点,因此在没有安全扩展的情况下仍然会有 ND 攻击。 然而,据资料显示,在 RFC3971 和 3972 中已经提出了 Secure ND 协议,该协议利用 IPv6 地址空 间长这一特性,在自动生成地址的同时,将实际的签名信息也保存在了生成的 IPv6 地址内部。 通过这种方式使得源地址的拥有权声明是可验证的,从而解决了 ND 攻击问题。

综上,在 Secure ND 没有普及的时候,IPV6 是可能遭到 ND 攻击的,而采用了 Secure ND 协议则 不会遭到攻击。