

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	数据科学与计算机学院	班级	软件工程教务一班	学号	17343094	姓名	彭湃
完成日期： 2019 年 12 月 26 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

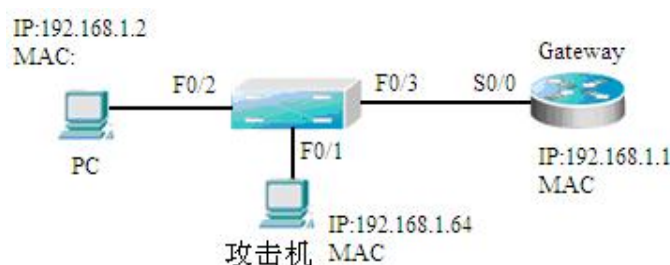
原理：伪造网关。它的原理是建立假网关，让被它欺骗的 PC 向假网关发数据，而不是通过正常的路由器途径上网。在 PC 看来，就是上不了网了，“网络掉线了”。

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；（设备都用的计网实验室设备）

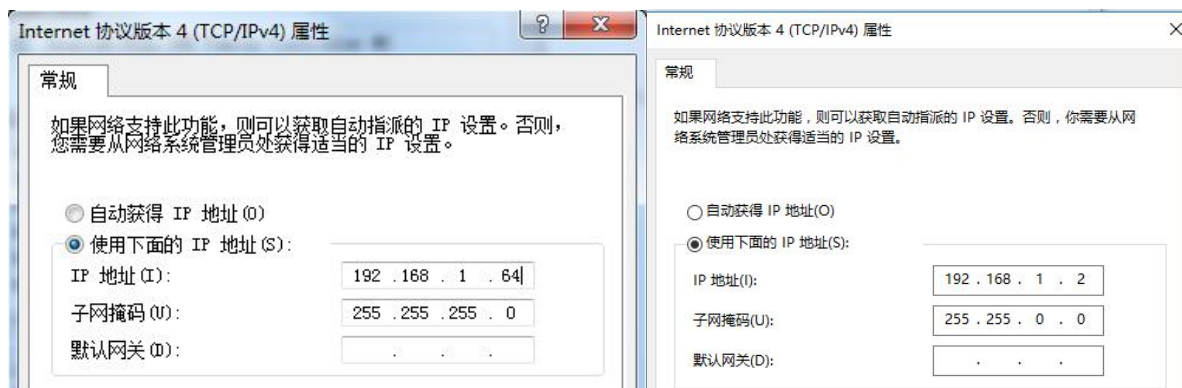
PC机2台，我们选择其中一台安装ARP欺骗攻击工具，因为WinArpSpoofers已经被封禁掉了，所以我们选用WinArpSpoofers的衍生软件，WinArpAttacker，它的功能页面等都和Spoofers类似，这台电脑是Win7系统；另外一台作为被攻击机，这台电脑是Win10系统。

路由器 1 台（作为网关）。

【实验步骤】

步骤1 配置IP地址，测试网络连通性。

①我们首先按照拓扑图正确配置PC机、攻击机、路由器的IP地址。



设置两台PC的ip地址

```
20-RSR20-1(config)#show ip interface brief
Interface                               IP-Address(Pri)    IP-Address(Sec)    Statu
s
Serial 2/0                             no address         no address         up
down
Serial 4/0                             no address         no address         down
down
FastEthernet 0/0                       no address         no address         up
down
FastEthernet 0/1                       no address         no address         down
down
20-RSR20-1(config)#interface fastethernet 0/0
20-RSR20-1(config-if-FastEthernet 0/0)#ip address 192.168.1.1 255.255.255.0
20-RSR20-1(config-if-FastEthernet 0/0)#no shutdown
20-RSR20-1(config-if-FastEthernet 0/0)#exit
```

设置路由器的ip

②用ping命令验证设备之间的连通性，保证可以互通。

```
C:\Users\Administrator>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 = 1ms, 平均 = 0ms
```

```
C:\Users\Administrator>ping 192.168.1.64

正在 Ping 192.168.1.64 具有 32 字节的数据:
来自 192.168.1.64 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.64 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.64 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.64 的回复: 字节=32 时间<1ms TTL=128

192.168.1.64 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
```

③接下来我们分别在两台pc机上使用arp -a指令查看PC机本地的ARP缓存，我们可以看得出ARP表中存有正确的网关的IP与MAC地址绑定。

```
C:\Users\Administrator>arp -a

接口: 169.254.46.27 --- 0xb
Internet 地址      物理地址      类型
169.254.160.231    44-33-4c-0e-be-33 动态
169.254.255.255    ff-ff-ff-ff-ff-ff 静态
224.0.0.5          01-00-5e-00-00-05 静态
224.0.0.22         01-00-5e-00-00-16 静态
224.0.0.251        01-00-5e-00-00-fb 静态
224.0.0.252        01-00-5e-00-00-fc 静态
239.255.255.250    01-00-5e-7f-ff-fa 静态
255.255.255.255    ff-ff-ff-ff-ff-ff 静态

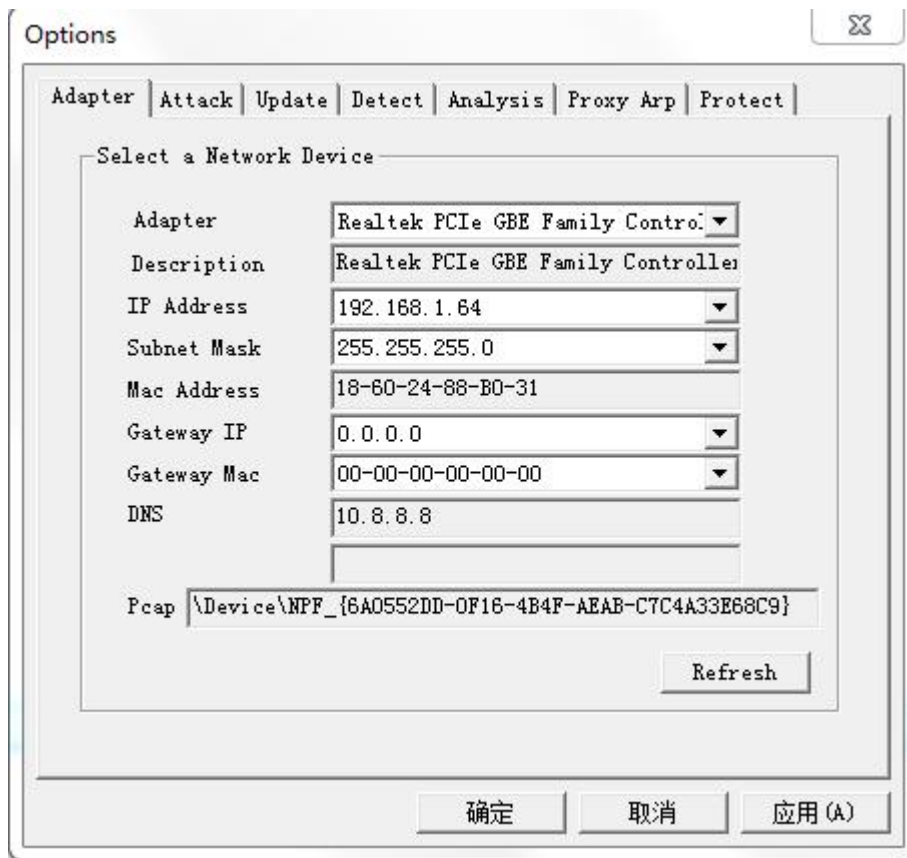
接口: 192.168.1.64 --- 0xd
Internet 地址      物理地址      类型
172.16.15.1        18-60-24-8c-93-10 动态
172.16.20.2        18-60-24-8c-17-07 动态
192.168.1.2        18-60-24-8c-17-07 动态
192.168.1.253      48-d5-39-1b-50-b5 动态
192.168.1.255      ff-ff-ff-ff-ff-ff 静态
224.0.0.5          01-00-5e-00-00-05 静态
224.0.0.22         01-00-5e-00-00-16 静态

C:\Users\Administrator>arp -a

接口: 169.254.38.230 --- 0x2
Internet 地址      物理地址      类型
169.254.255.255    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
239.255.255.250    01-00-5e-7f-ff-fa 静态
255.255.255.255    ff-ff-ff-ff-ff-ff 静态

接口: 192.168.1.2 --- 0x3
Internet 地址      物理地址      类型
172.16.15.1        18-60-24-8c-93-10 动态
172.16.20.3        18-60-24-8c-17-49 动态
172.16.22.1        18-60-24-88-b0-50 动态
172.16.22.3        18-60-24-8c-17-04 动态
192.168.1.64       18-60-24-88-b0-31 动态
192.168.255.255    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
239.255.255.250    01-00-5e-7f-ff-fa 静态
```

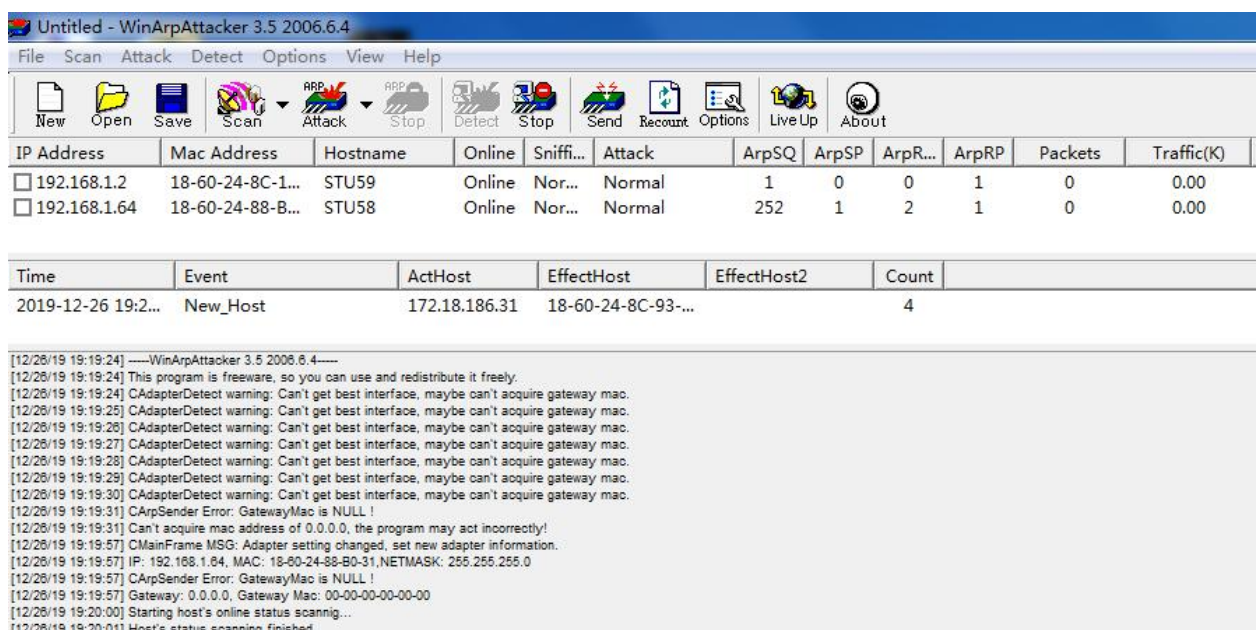
步骤2 我们在攻击机上运行WinArpAttacker软件，在界面“Adapter”选项卡中，选择正确的网卡（我们的是Realtek PCIe GBE Family Control），WinArpAttacker会显示网卡的IP地址、掩码、网关、MAC地址以及网关的MAC地址信息。



步骤3 对软件进行相关配置，因为我们这个Attacker软件选择好网卡后，剩下的部分是自动进行的，所以这一步我们不需要进行过多的配置，因此就不放图啦。

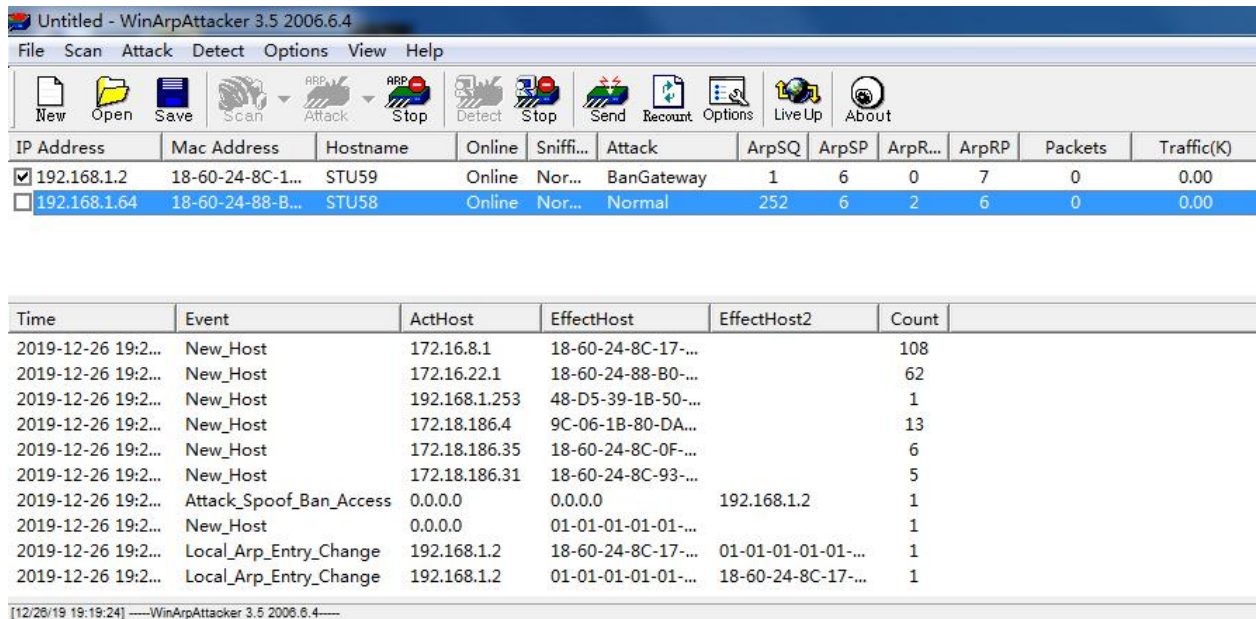
步骤4 使用WinArpSpoofing进行扫描。

我们直接单击软件工具栏中的“Scan”按钮，我们的软件就将自动扫描整个网络中的主机，并获取其IP地址、MAC地址等信息。



步骤5 进行ARP欺骗。

我们单击软件工具栏中的“Attack”按钮，软件将自动进行ARP欺骗攻击。如下图，软件已经开始ARP欺骗，直到我们按下停止键结束。



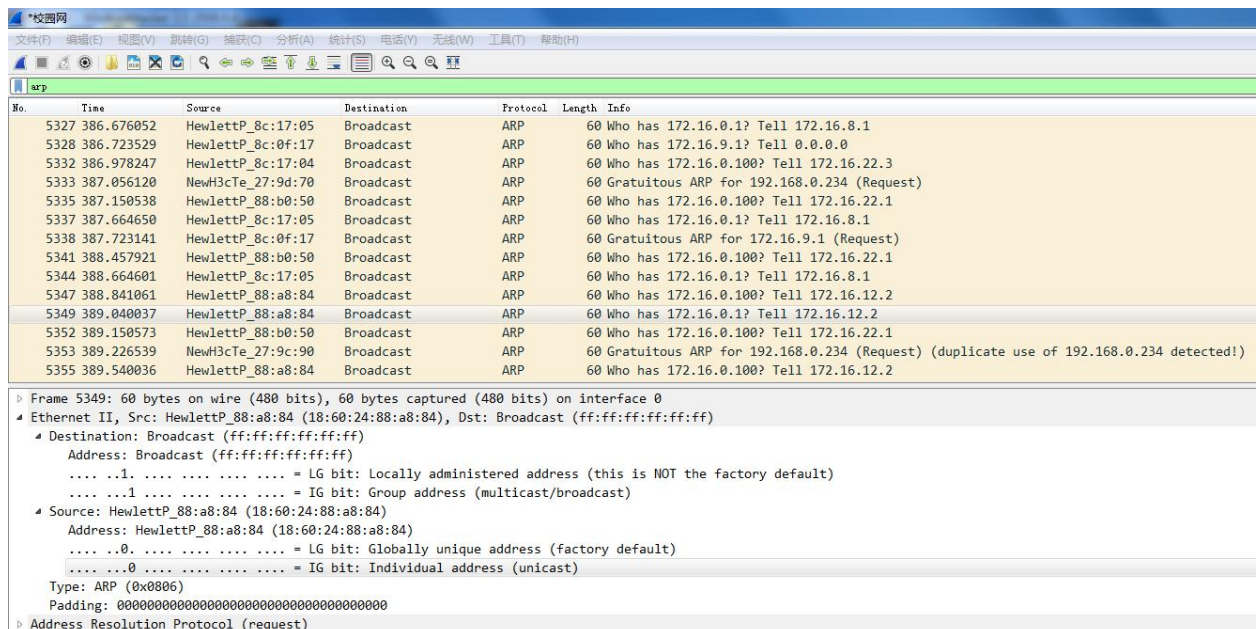
IP Address	Mac Address	Hostname	Online	Sniffi...	Attack	ArpSQ	ArpSP	ArpR...	ArpRP	Packets	Traffic(K)
<input checked="" type="checkbox"/> 192.168.1.2	18-60-24-8C-1...	STU59	Online	Nor...	BanGateway	1	6	0	7	0	0.00
<input type="checkbox"/> 192.168.1.64	18-60-24-88-B...	STU58	Online	Nor...	Normal	252	6	2	6	0	0.00

Time	Event	ActHost	EffectHost	EffectHost2	Count
2019-12-26 19:2...	New_Host	172.16.8.1	18-60-24-8C-17-...		108
2019-12-26 19:2...	New_Host	172.16.22.1	18-60-24-88-B0-...		62
2019-12-26 19:2...	New_Host	192.168.1.253	48-D5-39-1B-50-...		1
2019-12-26 19:2...	New_Host	172.18.186.4	9C-06-1B-80-DA...		13
2019-12-26 19:2...	New_Host	172.18.186.35	18-60-24-8C-0F-...		6
2019-12-26 19:2...	New_Host	172.18.186.31	18-60-24-8C-93-...		5
2019-12-26 19:2...	Attack_Spoof_Ban_Access	0.0.0.0	0.0.0.0	192.168.1.2	1
2019-12-26 19:2...	New_Host	0.0.0.0	01-01-01-01-01-...		1
2019-12-26 19:2...	Local_Arp_Entry_Change	192.168.1.2	18-60-24-8C-17-...	01-01-01-01-01-...	1
2019-12-26 19:2...	Local_Arp_Entry_Change	192.168.1.2	01-01-01-01-01-...	18-60-24-8C-17-...	1

[12/26/19 19:19:24] —WinArpAttacker 3.5 2006.6.4—

步骤6 验证测试。

在开启ARP欺诈的同时，我们可以通过使用Wireshark捕获攻击机发出的报文，从其中可以看出攻击机发送了经过伪造的ARP应答（Reply）报文。



No.	Time	Source	Destination	Protocol	Length	Info
5327	386.676052	HewlettP_8c:17:05	Broadcast	ARP	60	Who has 172.16.0.1? Tell 172.16.8.1
5328	386.723529	HewlettP_8c:0f:17	Broadcast	ARP	60	Who has 172.16.9.1? Tell 0.0.0.0
5332	386.978247	HewlettP_8c:17:04	Broadcast	ARP	60	Who has 172.16.0.100? Tell 172.16.22.3
5333	387.056120	NewH3cTe_27:9d:70	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.234 (Request)
5335	387.150538	HewlettP_88:b0:50	Broadcast	ARP	60	Who has 172.16.0.100? Tell 172.16.22.1
5337	387.664650	HewlettP_8c:17:05	Broadcast	ARP	60	Who has 172.16.0.1? Tell 172.16.8.1
5338	387.723141	HewlettP_8c:0f:17	Broadcast	ARP	60	Gratuitous ARP for 172.16.9.1 (Request)
5341	388.457921	HewlettP_88:b0:50	Broadcast	ARP	60	Who has 172.16.0.100? Tell 172.16.22.1
5344	388.664601	HewlettP_8c:17:05	Broadcast	ARP	60	Who has 172.16.0.1? Tell 172.16.8.1
5347	388.841061	HewlettP_88:a8:84	Broadcast	ARP	60	Who has 172.16.0.100? Tell 172.16.12.2
5349	389.040037	HewlettP_88:a8:84	Broadcast	ARP	60	Who has 172.16.0.1? Tell 172.16.12.2
5352	389.150573	HewlettP_88:b0:50	Broadcast	ARP	60	Who has 172.16.0.100? Tell 172.16.22.1
5353	389.226539	NewH3cTe_27:9c:90	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.234 (Request) (duplicate use of 192.168.0.234 detected!)
5355	389.540036	HewlettP_88:a8:84	Broadcast	ARP	60	Who has 172.16.0.100? Tell 172.16.12.2

Frame 5349: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

Ethernet II, Src: HewlettP_88:a8:84 (18:60:24:88:a8:84), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

- Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 - Address: Broadcast (ff:ff:ff:ff:ff:ff)
 - ...1. = LG bit: Locally administered address (this is NOT the factory default)
 - ...1. = IG bit: Group address (multicast/broadcast)
- Source: HewlettP_88:a8:84 (18:60:24:88:a8:84)
 - Address: HewlettP_88:a8:84 (18:60:24:88:a8:84)
 - ...0. = LG bit: Globally unique address (factory default)
 - ...0. = IG bit: Individual address (unicast)

Type: ARP (0x0806)

Padding: 00000000000000000000000000000000

Address Resolution Protocol (request)

步骤7 验证测试。

除了上面使用的wireshark捕捉流量包进行分析外，我们同时还可以使用ping网关和查看ARP表的方式，来验证我们的ARP欺诈成功。

- ①我们先使用PC机ping网关的地址，发现此时我们已经无法ping通。

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

正在 Ping 192.168.1.1 具有 32 字节的数据:
来自 192.168.1.2 的回复: 无法访问目标主机。
来自 192.168.1.2 的回复: 无法访问目标主机。
来自 192.168.1.2 的回复: 无法访问目标主机。
来自 192.168.1.2 的回复: 无法访问目标主机。

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),

C:\Users\Administrator>
```

②然后我们可以接着使用arp -a指令查看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。

```
C:\Users\Administrator>arp -a

接口: 169.254.38.230 --- 0x2
Internet 地址      物理地址      类型
169.254.255.255    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
239.255.255.250    01-00-5e-7f-ff-fa 静态
255.255.255.255    ff-ff-ff-ff-ff-ff 静态

接口: 192.168.1.2 --- 0x3
Internet 地址      物理地址      类型
172.16.15.1        18-60-24-8c-93-10 动态
172.16.20.3         18-60-24-8c-17-49 动态
172.16.22.1         18-60-24-88-b0-50 动态
172.16.22.3         18-60-24-8c-17-04 动态
192.168.1.64        18-60-24-88-b0-31 动态
192.168.255.255     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
239.255.255.250     01-00-5e-7f-ff-fa 静态
```

步骤8 配置ARP检查, 防止ARP欺骗攻击。

我们直接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。具体的指令是

```
Switch(config)#interface fastEthernet 0/1
```

```
Switch(config-if)#switchport port-security
```

```
Switch(config-if)#switchport port-security mac-address mac地址 ip-address ip地址
```

```
S5750-20-1(config)#interface giga 0/1
S5750-20-1(config-if-GigabitEthernet 0/1)#switchport port-security
S5750-20-1(config-if-GigabitEthernet 0/1)#$p-address [192.168.1.64]
switchport port-security mac-address [18602488b031] ip-address [192.168.1.64]

% Invalid input detected at '^' marker.

S5750-20-1(config-if-GigabitEthernet 0/1)#$31] ip-address [192.168.1.64]
switchport port-security mac-address [18-60-24-88-b0-31] ip-address [192.168.1.64]

% Invalid input detected at '^' marker.

S5750-20-1(config-if-GigabitEthernet 0/1)#$address 192.168.1.64
S5750-20-1(config-if-GigabitEthernet 0/1)#
```

这一步有个坑就是：ip地址和mac地址不要加[]，同时需要注意的是，mac地址之间不需要用“-”进行连接，例如18-60-24-8c-17-04直接写成1860248c1704。

步骤9 验证测试。

当我们启用 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。这个时候之前被 ARP 欺骗影响的功能都恢复了正常。

①这时在我们再 PC 机上查看 ARP 缓存，可以看到 ARP 表中的条目是正确的。当然我们需要先用 arp -d 清除一下之前的 ARP 缓存，这个需要 root 权限，windows 下我们直接在 powershell 下使用就行，然后再查看 ARP 缓存表就能看到正确内容：

```
PS C:\Windows\system32> arp -d
C:\Windows\system32\cmd.exe
C:\Users\Administrator>arp -a

接口: 169.254.38.230 --- 0x2
Internet 地址      物理地址          类型
224.0.0.22         01-00-5e-00-00-16 静态
239.255.255.250    01-00-5e-7f-ff-fa 静态
255.255.255.255    ff-ff-ff-ff-ff-ff 静态

接口: 192.168.1.2 --- 0x3
Internet 地址      物理地址          类型
192.168.1.64       18-60-24-88-b0-31 动态
192.168.1.255      ff-ff-ff-ff-ff-ff 静态
```

②然后此时我们再用 PC 机去 ping 网关，此时我们发现可以 ping 通了。

```
C:\Users\Administrator>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=128
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=128

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
```

【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。

Answer:

防御 ARP 欺骗攻击的方法还是挺多的，把我想到的几种列举在下面：

- 使用 arp 欺骗防护软件，现在像 360、腾讯电脑管家等都自带了相应的 ARP 欺骗防护功能。
- 直接像我们这次一样，在交换机上设置访问控制。
- 使用静态的 ARP 缓存表，静态的 ARP 绑定正确的 MAC 可以避免 ARP 攻击。

(2) 在 IPv6 协议下，是否有 ARP 欺骗攻击？

Answer:

查找了下资料，在 IPV6 中，已经使用 NDP(邻居发现协议)替代了 ARP，所以我觉得应该在 ipv6 中是不存在有 ARP 欺骗攻击这种说法的，但是针对 NDP，是否有新的欺骗或者攻击，我觉得是肯定

的，因为互联网每种新事物的诞生，肯定都会伴随着破解和攻击。