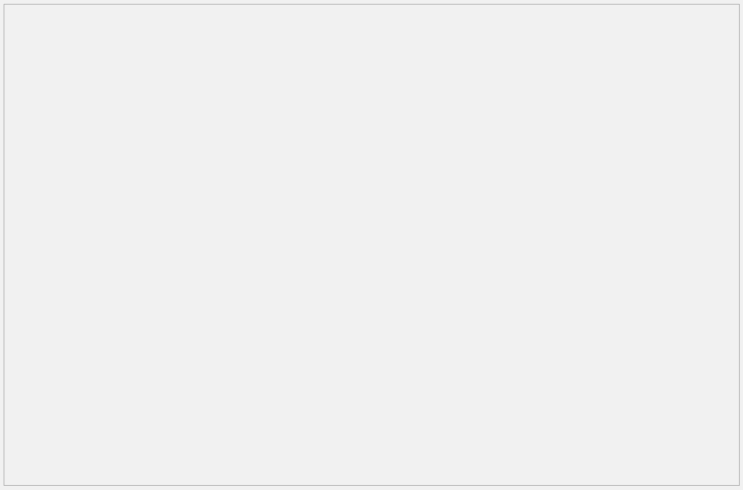
动态ARP检测测试经验案例

凌勇 2008-03-31 发表

动态ARP检测测试经验案例

一、组网及说明：



低端交换机的动态ARP检测和IP CHECK特性已经出来有一段时间了，而针对该特性的指导手册却不多，此次有一个测试项目中进行了该特性的测试，整理了这篇测试文档，希望对大家有所借鉴。

如组网是一个非常常见的组网结构，DHCP server在核心交换机7506E上（也可以用其他的服务器），3600-EI与7506E为TRUNK相连，网关在7506E上，PC1、PC2同属一个VLAN。

测试中要模拟非法ARP攻击，因此需要ARP发包工具，在网上比较容易找到的是网络执法官，建议下载V2.96.12试用版，其他一些破解版本如V2.88等都附有病毒。

本次测试使用的交换机是3600-EI，软件版本为3.10-R1602P02。

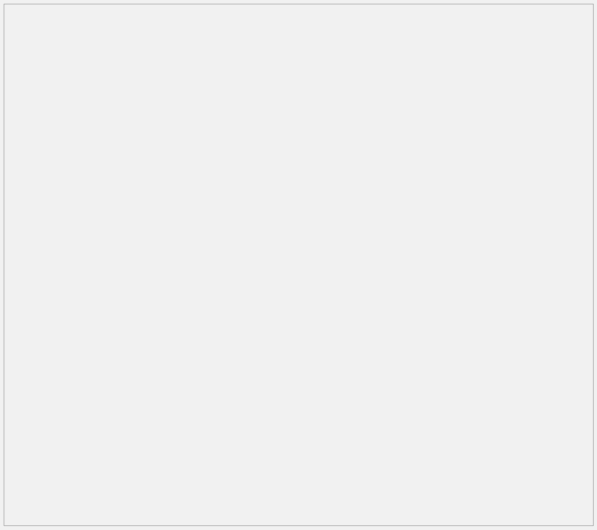
二、测试过程：

首先需要测试在未启用动态ARP检测特性时的现象，

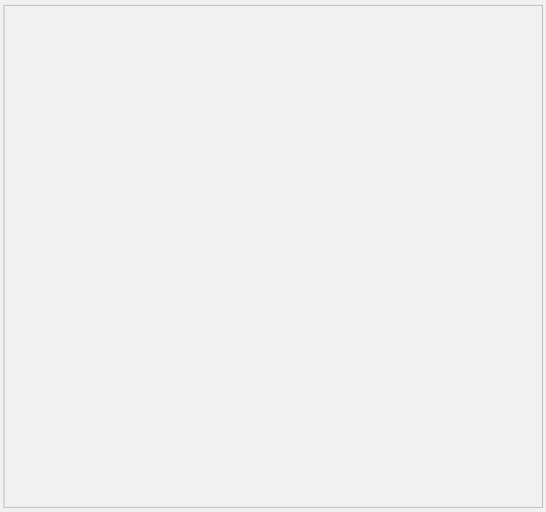
3600-EI除启用dhcp-snooping不做任何特殊配置，PC1和PC2都通过DHCP获取地址，分别为172.17.2.1/24和172.17.2.21/24。测试前保证PC1、PC2与网关互通。

在PC1上打开一个DOS窗口，可以看到172.17.2.254的MAC地址是：000f-e27b-f74e，常PING 172.17.2.254，可以看到是通的。

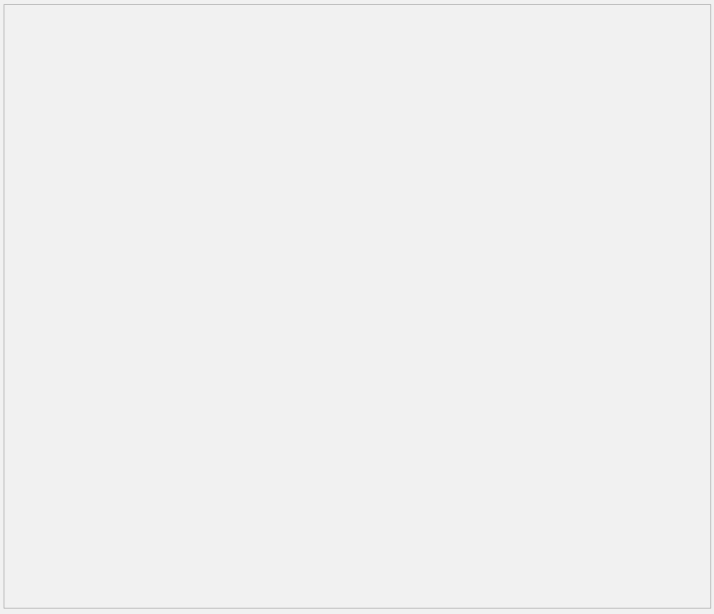
在PC2上打开网络执法官，做如下配置：



选择当前使用的网卡，并添加监控网段。

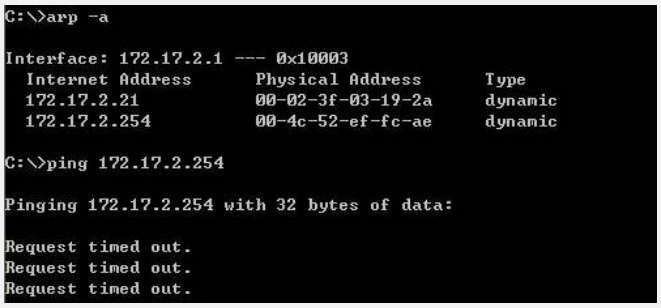


选择“设置”/“关键主机”，将网关的IP增加到关键主机列表中。
此时还需要在PC2同时打开ethereal抓包工具收集证据，开始抓包。做好准备工作后就可以发动攻击了。



在主页面中右击PC1对应的条目，选择“设定权限”，如上图进行设置。
此时切换到ethereal，查看刚刚抓的包：

可以看到PC2伪造了2个ARP回应包，分别是172.17.2.1->172.17.2.254 / 172.17.2.254->172.17.2.1，源MAC都做了修改。
切换到常PING 172.17.2.254的DOS窗口，可以发现已经不通了，网关ARP已被更改。



在3600-EI上查看ARP表，PC1的MAC地址同样被更改：

<S7506E>disp arp vlan 2
Type: S-Static D-Dynamic

IP Address	MAC Address	VLAN ID	Interface	Aging	Type
172.17.2.1	00c0-9fa2-53fa	2	GE2/0/3	17	D
172.17.2.21	0002-3f03-192a	2	GE2/0/3	20	D

以上可以很明显地看到ARP攻击的表现。
接下来就展现3600-EI如何有效地防范了。在3600-EI上增加如下配置：

```
vlan 2
arp detection enable
#
interface Ethernet1/0/4
 port access vlan 2
 ip check source ip-address mac-address
#
interface Ethernet1/0/5
#
interface Ethernet1/0/6
 port access vlan 2
 ip check source ip-address mac-address
#
interface GigabitEthernet1/1/4
 port link-type trunk
 port trunk permit vlan 1 to 3 10
 dhcp-snooping trust
 ip source static binding ip-address 172.17.2.254 mac-address 000f-e27b-f74e
#
dhcp-snooping
#
```

此时再按上述步骤依次演示，注意同样要保证测试开始前PC1、PC2与网关互通，可以看到最后PC2发动攻击后PC1还是可以正常PING通网关，查看PC2上ethereal所抓的包，发现依然还是有伪造包发出，但3600-EI和PC1的ARP表都没有被更改。

三、经验总结：

此案例同样适用于开局时向客户演示我们的功能特点，对于客户网络中已部署了DHCP服务器的很容易实施，但在没有部署DHCP服务器的环境下，我们同样可以实现，需

要在用户接口上增加IP静态绑定表，如上例中需要在连接PC1、PC2的端口上手工配置IP静态绑定表：

```
interface Ethernet1/0/4
ip source static binding ip-address 172.17.2.21 mac-address 0002-3f03-192a
#
interface Ethernet1/0/6
ip source static binding ip-address 172.17.2.1 mac-address 00c0-9f9b-2b98
```

四、注意事项：

测试前需要确定待测低端交换机是否支持该特性，且需要升级到相应版本，请与全球技术服务部技术支持中心确认。