SecPath防火墙ip-sweep和port-scan攻击防范动态加入黑名单的典型配置

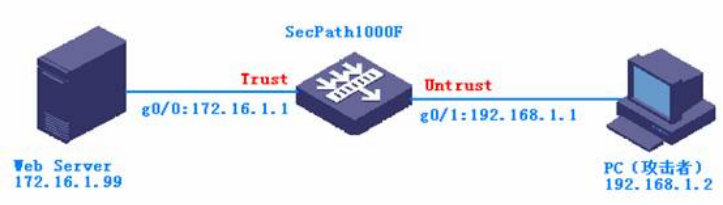
赵彪 2006-10-11 发表

SecPath防火墙ip-sweep和port-scan攻击防范
动态加入黑名单的典型配置

一、 组网需求：

测试SecPath防火墙ip-sweep和port-scan防范功能，对扫描类的攻击动态加入到黑名单。

二、 组网图



SecPath1000F：版本为Version 3.40, ESS 1604P01；
Web Server：Windows 2003操作系统；
PC：Windows XP操作系统，安装EasyToolKit攻击工具。

三、 配置步骤

1. SecPath1000F的主要配置

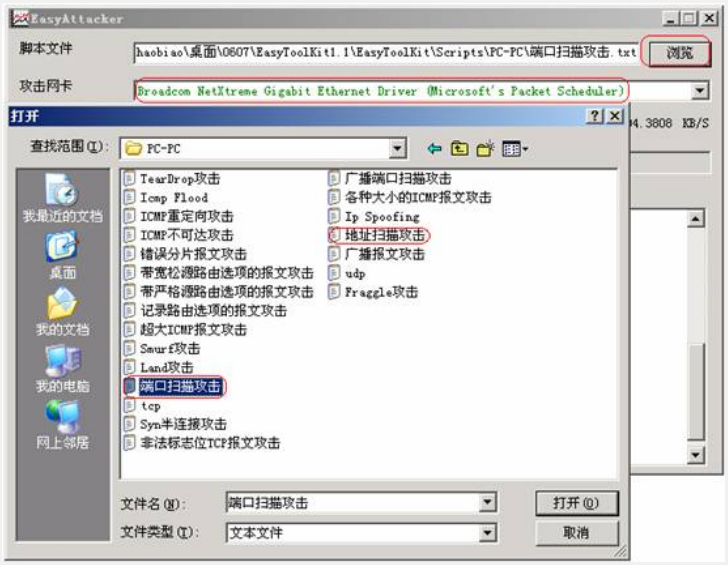
```
#
 sysname Quidway
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
 firewall statistic system enable                //全局模式启用统计功能
#
 firewall blacklist enable                       //启用黑名单功能
 firewall blacklist 202.38.1.99                  //手工添加到黑名单条目
#
interface GigabitEthernet0/0
 ip address 172.16.1.1 255.255.255.0
#
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
#
firewall zone trust
 add interface GigabitEthernet0/0
 set priority 85
#
firewall zone untrust
 add interface GigabitEthernet0/1
 set priority 5
 statistic enable ip outzone                     //连接发起域出方向启用IP统计功能
#
 firewall defend ip-sweep max-rate 300 blacklist-timeout 15   //配置ip-sweep防范属性
 firewall defend port-scan max-rate 300 blacklist-timeout 10   //配置port-scan防范属性
#
[Quidway]dis firewall blacklist item             //显示黑名单表项
 Firewall blacklist item :
 Current manual insert items : 1
 Current automatic insert items : 2
 Need aging items : 2

 IP Address      Insert reason   Insert time          Age time(minutes)
```

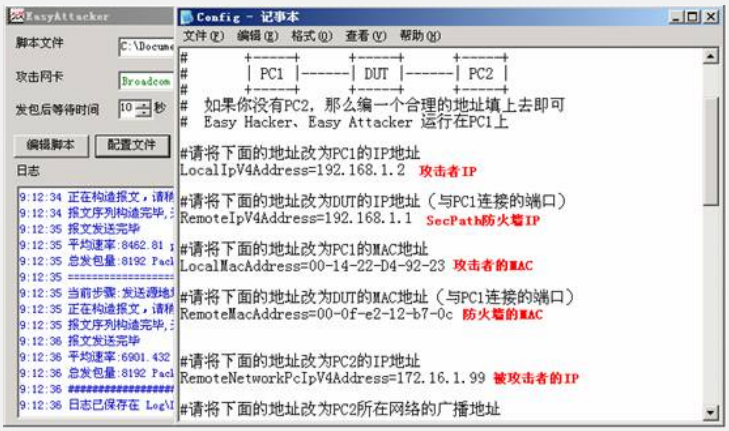
```
------------------------------------------------------------------------------
202.38.1.99     Manual          2006/10/11 08:30:22     Permanent
192.168.1.2     Port Scan       2006/10/11 08:59:53     10
192.168.1.2     IP Sweep        2006/10/11 09:55:13     15
[Quidway]dis firewall statistic system defend      //显示攻击防范统计
  Display firewall defend statistic:
                IP-sweep,             2 time(s)
          TCP port-scan,              2 time(s)
          UDP port-scan,              0 time(s)
                total,                4 time(s)
```

2. PC攻击工具配置

打开“EasyAttacker”程序，选择攻击网卡，浏览选择攻击类型：

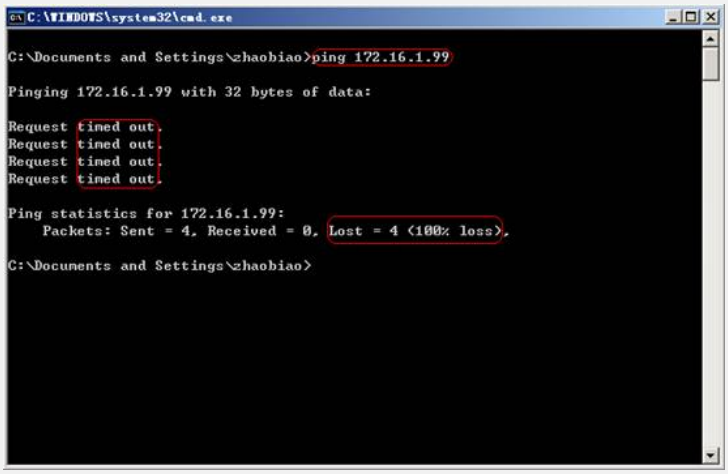


编辑配置文件：



运行脚本，构造攻击报文：

验证结果：



四、 配置关键点

1. 连接发起域出方向启用IP统计功能；
2. 使用“EasyToolKit”前，必须安装“dotnetfx.exe”和“WinPcap”；
3. 全局下必须开启统计功能；
4. max-rate默认值为4000；
5. 默认不加入黑名单。