赵彪 2006-10-10 发表

#

```
SecPath防火墙SYN Flood攻击防范的典型配置
一、 组网需求:
模拟Utrust区域用户攻击DMZ区域的服务器,通过在SecPath1000F防火墙配置攻击防
范阻断攻击。
二、组网图
 SecPath1000F:版本为Version 3.40, ESS 1604P01;
 Web Server: Windows 2003操作系统;
 PC1: 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
#
                          //全局启用统计功能,必须启用
firewall statistic system enable
#
interface GigabitEthernet0/0
ip address 172.16.1.1 255.255.255.0
#
interface GigabitEthernet0/1
ip address 202.38.1.1 255.255.255.0
#
interface GigabitEthernet1/0
ip address 192.168.1.1 255.255.255.0
#
firewall zone trust
add interface GigabitEthernet1/0
set priority 85
#
firewall zone untrust
add interface GigabitEthernet0/1
set priority 5
#
firewall zone DMZ
add interface GigabitEthernet0/0
set priority 50
statistic enable ip inzone //在DMZ区域对进来的IP进行统计
#
firewall defend syn-flood enable
                                    //启用syn-flood攻击防范功能
firewall defend syn-flood zone DMZ max-rate 200 tcp-proxy //对DMZ区进行syn-
flood攻击保护,每秒新建连接数超过200启用tcp-proxy阻断后续连接
```

```
没有配置攻击防范时,防火墙产生大量Session:
<Quidway>dis firewall session table //查看防火墙会话
Total session number: 3085 //syn-flood攻击产生3085个会话
tcp:172.16.1.99:2230<--202.38.1.2:4277
tcp:172.16.1.99:2229<--202.38.1.2:4276
tcp:172.16.1.99:2231<--202.38.1.2:4278
tcp:172.16.1.99:2233 <-- 202.38.1.2:4280
tcp:172.16.1.99:2232<--202.38.1.2:4279
tcp:172.16.1.99:2235<--202.38.1.2:4282
tcp:172.16.1.99:2234<--202.38.1.2:4281
tcp:172.16.1.99:2236<--202.38.1.2:4283
tcp:172.16.1.99:2238<--202.38.1.2:4285
<Quidway>dis firewall statistic system defend //查看攻击防范统计
Display firewall defend statistic:
            SYN-flood, 0 time(s)
                         0 time(s)
              total,
配置攻击防范后,防火墙产生少量Session:
<Quidway>dis firewall session table
Total session number: 2
NBT datagram:202.38.1.255:138<--202.38.1.2:138
NBT name:202.38.1.255:137<--202.38.1.2:137
<Quidway>dis firewall statistic system defend //查看攻击防范统计
 Display firewall defend statistic:
            SYN-flood, 4 time(s)
              total, 4 time(s)
2. PC1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:

EasyAttacke		👺 Config - 记事本	_ 🗆 ×
脚本文件	C:\Docume	文件(2)编辑(2)格式(2)查看(2)帮助(2)	22
攻击网卡	Broadcon	# PC1 DUT PC2	-
发包后等待时间	10 - 10	# ++ # 如果你没有PC2,那么编一个合理的地址填上去即可 # Easy Hacker、Easy Attacker 运行在PC1上	
<u> 編編期本</u> [日志	配置文件	#请将下面的地址改为PC1的IP地址 LocalIpV4Address=202.38.1.2) 攻击者IP	
19:36:44	已经加载起	。 情情将下面的地址改为DIII的IP地址(与PC1连转的端口) RemoteIpV4Address= <u>202.38.1.1</u> 防火着外网口IP	-
		#请将下面的地址改为PC1的MAC地址 LocalMacAddress= (0-14-22-D4-92-23) 攻击者的MAC	
		#请将下面的地址改为 <u>DUT的MAC地址(</u> 与PC1连接的端口) RemoteMacAddress=00-0f-e2-12-b7-0c) <mark>防火塩外間口的MAC</mark>	
		#请将下面的地址改为PC2的IP地址 RemoteNetworkPcIpV4Address=172.16.1.99	
		#请将下面的地址改为PC2所在网络的广播地址	

运行脚本,构造攻击报文:

3. Web Server的抓包结果

没有配置攻击防范时的抓包,收到大量数据包:

启用syn-flood攻击防范后,收到很少的数据包:



四、配置关键点

- 1、使用"EasyToolKit"前,必须安装"dotnetfx.exe"和"WinPcap";
- 2、全局下必须开启统计功能;
- 3、Syn-flood开启后, 默认max-rate值为10000。