## 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 Trust Untrust g0/0:172.16.1.1 g0/1:192.168.1.1 Veb Server 172.16.1.99 PC(攻击者) 192.168.1. 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 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:

XX EasyAttacker	📴 Config - 记事本	- O ×
脚本文件 C:\Docum	文件(12)编辑(12)格式(12)查看(12)帮助(13)	
攻击网卡 Broadcom	# ++ ++ #   PC1    DUT    PC2   ++	-
发包后等待时间 10 🛨 秒	# 如果你没有PC2, 那么编一个合理的地址填上去即可 # Basy Hacker、Easy Attacker 运行在PC1上	
	#请将下面的地址改为PC1的IP地址 LocalIpV4Address=192.168.1.2 <mark>攻击者IP</mark>	
9:12:34 正在构造报文,请称 9:12:34 报文序列构造完毕, 9:12:35 报文发送完毕	#请将下面的地址改为DUT的IP地址(与PC1连接的端口) RemoteIpV4Address=192.168.1.1 SecPath防火着IP #请将下面的地址改为PC1的MAC地址 LocalMacAddress=00-14-22-D4-92-23 攻击者的MAC #请将下面的地址改为DUT的MAC地址(与PC1连接的端口) RemoteMacAddress=00-0f-e2-12-b7-0c 防火着的MAC	
9:12:35 平均速率:8462.81 9:12:35 总发包量:8192 Pac 9:12:35 ====================================		
9:12:35 当前步囊:发送源地 9:12:35 正在构造报文,请和 9:12:35 报文序列构造完毕, 9:12:36 报文发送完毕		
9:12:36 平均速率:6901.432 9:12:36 总发包量:8192 Pac 9:12:36	#请将下面的地址改为FC2的IP地址 RemoteNetworkPcIpV4Address=172.16.1.99 <b>被攻击者的IP</b>	
9:12:36 日志已保存在 Log	I#请将下面的地址改为PC2所在网络的广播地址	-1

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。