SecPath地址扫描和端口扫描攻击防范典型配置

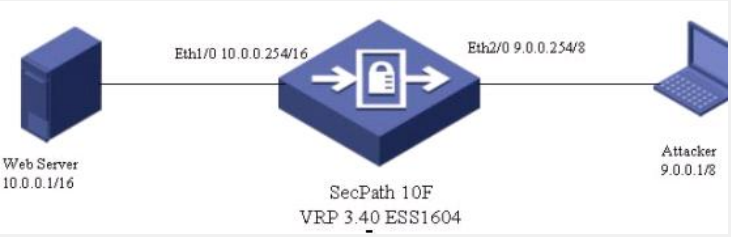
巫继雨 2006-09-25 发表

SecPath地址扫描和端口扫描攻击防范典型配置

一、组网需求

部署SecPath防火墙，对地址扫描(ip-sweep)和端口扫描(port-scan)攻击进行防范，并利用黑名单功能将攻击者进行隔离。

二、组网图



三、配置步骤

```
[SecPath10F]dis cur
#
 sysname SecPath10F
#
 firewall packet-filter enable                    //开启全局报文统计功能
 firewall packet-filter default permit
#
 undo connection-limit enable
 connection-limit default deny
 connection-limit default amount upper-limit 50 lower-limit 20
#
 firewall statistic system enable
#
 firewall blacklist enable                        //启用黑名单功能
#
radius scheme system
#
domain system
#
local-user admin
 password cipher .]@USE=B,53Q=^Q`MAF4<1!!
 service-type telnet terminal
 level 3
 service-type ftp
#
interface Ethernet1/0
 ip address 10.0.0.254 255.255.0.0
#
interface Ethernet2/0
 speed 10
 duplex half
 ip address 9.0.0.254 255.0.0.0
#
interface NULL0
#
firewall zone local
 set priority 100
#
firewall zone trust
 add interface Ethernet1/0
 set priority 85
#
firewall zone untrust
 add interface Ethernet2/0
```

```
 set priority 5
 statistic enable ip outzone                    //对非信任域出方向的报文进行统
计
#
firewall zone DMZ
 set priority 50
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local DMZ
#
firewall interzone trust untrust
#
firewall interzone trust DMZ
#
firewall interzone DMZ untrust
#
 FTP server enable
#
 //设置地址扫描的阈值为每秒50次，将攻击者加入到黑名单并阻断10分钟

 firewall defend ip-sweep max-rate 50 blacklist-timeout 10
//设置端口扫描的阈值为每秒100次，将攻击者加入到黑名单并阻断10分钟
firewall defend port-scan max-rate 100 blacklist-timeout 10
#
user-interface con 0
user-interface vty 0 4
 authentication-mode scheme
#
return
```

四、配置关键点

1．对域进入或送出的报文进行统计；

2．开启黑名单功能；

3．设置地址/端口扫描的阈值和攻击者被阻断的时间。

五、验证结果

1， 在攻击机上ping 10.0.0.1，可以ping通。然后在攻击机9.0.0.1上使用nmap对10.0.0.1进行地址扫描：nmap -v --min-hostgroup 100 -sS 10.0.0.0/16

```
//防火墙弹出地址扫描告警
[SecPath10F]
%Jan  1 00:15:54:165 2000 SecPath10F
SEC/5/BLS:blsOptMode(1026)=add;srcIPAddr(10
17)=9.0.0.1;blsOptReason(1027)= IP Sweep ;blsHoldTime(1028)=10
%Jan  1 00:16:08:915 2000 SecPath10F SEC/5/ATCKDF:atckType(1016)=(16)IP-sw
eep;rc
vIfName(1023)=Ethernet2/0;srcIPAddr(1017)=9.0.0.1;srcMacAddr(1021)=;destIPAddr(
1
019)=10.0.0.51;destMacAddr(1022)=;atckSpeed(1047)=50;atckTime_cn(1048)=20000
1010
01554
//攻击者地址已经加入到黑名单中，并且阻断时间为10分钟

[SecPath10F]dis firewall blacklist item
 Firewall blacklist item :
 Current manual insert items : 0
 Current automatic insert items : 1
 Need aging items : 1

 IP Address      Insert reason    Insert time            Age time(minutes)
 ------------------------------------------------------------------------------------------------
 9.0.0.1         IP Sweep         2000/01/01 00:15:53    10
```

此时在攻击机上ping 10.0.0.1，发现无法ping通。

2， 10分钟阻断时间过后，在攻击机9.0.0.1上ping 10.0.0.1，可以ping通。然后，使用nmap对10.0.0.1进行端口扫描：nmap -v -p 1-65535 10.0.0.1

//防火墙弹出端口扫描告警

[SecPath10F]

%Jan 1 00:03:55:514 2000 SecPath10F SEC/5/BLS:blsOptMode(1026)=add;srcIPAddr(1017)=9.0.0.1;blsOptReason(1027)= Port Scan ;blsHoldTime(1028)=10

%Jan 1 00:04:08:915 2000 SecPath10F SEC/5/ATCKDF:atckType(1016)=(25)TCP port-scan;rcvIfName(1023)=Ethernet2/0;srcIPAddr(1017)=9.0.0.1;srcMacAddr(1021)=;destIPAddr(1019)=10.0.0.1;destMacAddr(1022)=;atckSpeed(1047)=100;atckTime_cn(1048)=2000

0101000355

//攻击者地址已经加入到黑名单中，并且阻断时间为10分钟

[SecPath10F]dis firewall blacklist item

Firewall blacklist item :

Current manual insert items : 0

Current automatic insert items : 1

Need aging items : 1

IP Address	Insert reason	Insert time	Age time(minutes)
9.0.0.1	Port Scan	2000/01/01 00:03:54	10

此时在攻击机上ping 10.0.0.1，发现无法ping通。