配置IDS TCP复位使用VM IDS MC

目录

简介

本文通过VPN/安全管理解决方案(VM)提供Cisco入侵检测系统(IDS)的配置示例， IDS管理控制台(IDS MC)。在这种情况下，从IDS传感器的TCP重置到Cisco路由器配置。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 传感器为感觉必要的流量安装并且配置。
- 探测接口被跨过对路由器外部接口。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 与IDS MC和安全监视器1.2.3的VM 2.2

- Cisco IDS传感器4.1.3S(63)
- 运行Cisco IOS软件版本12.3.5的Cisco路由器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

配置

本文档使用以下配置。

- 路由器灯
- 路由器 House

路由器灯

```
Current configuration : 906 bytes
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname light ! enable password cisco ! username cisco
password 0 cisco ip subnet-zero ! ! ! ip ssh time-out
120 ip ssh authentication-retries 3 ! call rsvp-sync ! !
! fax interface-type modem mta receive maximum-
recipients 0 ! controller E1 2/0 ! ! ! interface
FastEthernet0/0 ip address 100.100.100.2 255.255.255.0
duplex auto speed auto ! interface FastEthernet0/1 ip
address 1.1.1.1 255.255.255.0 duplex auto speed auto !
interface BRI4/0 no ip address shutdown ! interface
BRI4/1 no ip address shutdown ! interface BRI4/2 no ip
address shutdown ! interface BRI4/3 no ip address
shutdown ! ip classless ip route 0.0.0.0 0.0.0.0
100.100.100.1 ip http server ip pim bidir-enable ! !
dial-peer cor custom ! ! line con 0 line 97 108 line aux
0 line vty 0 4 login ! end
```

路由器 House

```
Building configuration...

Current configuration : 797 bytes
```

```
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname House ! logging queue-limit 100 enable password
cisco ! ip subnet-zero no ip domain lookup ! ! interface
Ethernet0 ip address 10.66.79.210 255.255.255.224 hold-
queue 100 out ! interface Ethernet1 ip address
100.100.100.1 255.255.255.0 ip classless ip route
0.0.0.0 0.0.0.0 10.66.79.193 ip route 1.1.1.0
255.255.255.0 100.100.100.2 ip http server no ip http
secure-server ! ! ! line con 0 stopbits 1 line vty 0 4
password cisco login ! scheduler max-task-time 5000 end
```

最初的传感器配置

注意： 如果已经执行您的传感器初始设置，请继续到导入传感器到IDS MC部分里。

1. 控制到传感器。系统会提示您输入用户名和密码。如果这是您第一次控制传感器，您必须使用用户名cisco和密码cisco进行登录。
2. 提示您更改密码，并重新输入新密码，以确认。
3. 键入**设置**并且进入相应的信息在每及时根据此示例设置您的传感器的基本参数，

   ：sensor5#**setup** --- System Configuration Dialog --- At any point you may enter a question mark '?' for help. User ctrl-c to abort configuration dialog at any prompt. Default settings are in square brackets '[]'. Current Configuration: networkParams ipAddress **10.66.79.195** netmask **255.255.255.224** defaultGateway **10.66.79.193** hostname **sensor5** telnetOption **enabled accessList ipAddress 10.66.79.0 netmask 255.255.255.0** exit timeParams summerTimeParams active-selection none exit exit service webServer general ports 443 exit exit 5 Save the config: (It might take a few minutes for the sensor saving the configuration) [0] Go to the command prompt without saving this config. [1] Return back to the setup without saving this config. [2] Save this configuration and exit setup. Enter your selection[2]: **2**

导入传感器到IDS MC

完成这些步骤为了导入传感器到IDS MC。

1. 浏览对您的传感器。在这种情况下， **http://10.66.79.250:1741**或**https://10.66.79.250:1742**。
2. 有适当的用户名和密码的洛金。在本例中，用户名是**admin**，并且密码是**cisco**。
3. 选择**VPN/Security Management Solution > Management Center**并且点击**IDS传感器**。
4. 点击Devices选项并且选择**传感器组**。
5. 突出显示**全局**并且单击**创建小群**。
6. 输入组名并且保证**默认**选择，然后点击OK键为了添加小群到IDS MC。
7. 选择**设备>传感器**，突出显示在上一步创建的小群(在这种情况下，**测验**)，并且单击**添加**。
8. 突出显示小群并且**其次**单击。
9. 根据此示例输入详细信息并且**其次**单击为了继续。
10. 当您提交与陈述消息时，请点击**芬通社**为了继续。
11. 您的传感器导入到IDS MC。在这种情况下，传感器5导入。

导入传感器到安全监视器

完成这些步骤为了导入传感器到安全监视器。

1. 在VMS Server菜单，请选择**VPN/安全管理解决方案>监听集中>** Security**箴言报**。
2. 选择Devices选项，然后点击**导入**并且根据此示例输入IDS MC服务器信息。
3. 选择您的传感器(在这种情况下，**传感器5**)并且**其次**单击为了继续。
4. 若需要，请更新您的传感器的NAT地址，然后点击**芬通社**为了继续。
5. 点击OK键为了完成导入从IDS MC的传感器到安全监视器。
6. 您能当前看到您的传感器顺利地导入

请使用IDS MC签名更新

此步骤解释如何使用IDS MC签名更新。

1. 下载网络ID签名更新(仅限注册用户)并且救他们在您的VMS服务器的**C:\PROGRA~1\CSCOpx\MDC\etc\ids\updates**目录。
2. 在VMS服务器控制台，请选择**VPN/Security Management Solution > Management Center > IDS Sensors**。
3. 选择Configuration选项并且点击**更新**。
4. 点击**更新网络ID签名**。
5. 选择您要从下拉菜单升级的签名并且单击**应用**为了继续。
6. 选择传感器更新并且**其次**单击为了继续。
7. 在提示您应用更新到管理中心，以及传感器后，请点击**芬通社**为了继续。
8. 远程登录或控制到传感器命令行界面。您看到信息类似于此：
```
sensor5#
Broadcast message from root (Mon Dec 15 11:42:05 2003):
Applying update IDS-sig-4.1-3-S63. This may take several minutes. Please do not reboot the
sensor during this update. Broadcast message from root (Mon Dec 15 11:42:34 2003): Update
complete. sensorApp is restarting This may take several minutes.
```
9. 等待几分钟允许升级完成，然后输入**show version**为了验证。
```
sensor5#show version
Application Partition: Cisco Systems Intrusion Detection Sensor, Version 4.1(3)S63 Upgrade
History: * IDS-sig-4.1-3-S62 07:03:04 UTC Thu Dec 04 2003 IDS-sig-4.1-3-S63.rpm.pkg
11:42:01 UTC Mon Dec 15 2003
```

配置IOS路由器的TCP重置

完成这些步骤为了配置IOS路由器的TCP重置。

1. 选择**VPN/Security Management Solution > Management Center > IDS Sensors**。
2. 选择Configuration选项，选择您的从对象选择器的传感器，然后点击**设置**。
3. 选择**签名**，点击**自定义**，并且单击**添加**为了添加一个新的签名。
4. 输入新的签名名称，然后选择引擎(在这种情况下， **STRING.TCP**)。
5. 检查appropriate单选按钮为了定制可用的参数然后单击请**编辑**。在本示例中，ServicePorts参数值被编辑更改为23(端口23)。RegexString参数是也编辑的添加值**testattack**。当这完成时，请点击OK键继续。
6. 点击签名的名称为了编辑签名严重性和操作或者启用/禁用签名。
7. 在这种情况下，将严重性更改为“高”，同时选择“操作日志&重置”。单击 **OK** 以继续。
8. 完整签名看起来类似于此：
9. 选择**待定的Configuration>**，检查待定配置保证它正确，并且点击**“Save”**。
10. 选择**部署>生成**，然后单击**应用**为了推送对传感器的配置更改。
11. 选择**Deployment > Deploy**并且单击**提交**。
12. 在您的传感器旁边检查复选框并且单击**部署**。

13. 检查复选框在队列的工作并且**其次**单击为了继续。
14. 输入任务名称并且安排工作如**立即**，然后点击**芬通社**。
15. 选择**待定的Deployment > Deploy >**。请等待几分钟，直到所有待定工作完成。队列应该然后是空的。
16. 选择**Configuration>历史记录**为了确认部署。保证配置的状况显示如**部署**。这意味着传感器配置顺利地更新。

验证

使用本部分可确认配置能否正常运行。

发起攻击和 TCP 复位

发起测验攻击并且检查结果为了验证阻塞流程正确地运作。

1. 在攻击启动前，请选择**VPN/安全管理解决方案>监听集中>** Security**箴言报**。
2. 从主菜单选择**箴言报**并且点击**事件**。
3. 点击**启动事件查看器**。
4. 从一个路由器远程登录到其他并且键入**testattack**为了发起攻击。在这种情况下，我们从路由器Light远程登录到路由器House。当您按**<space>**或**<enter>**，在您键入**testattack后**，您的远程登录会话应该重置。`light#telnet 100.100.100.1 Trying 100.100.100.1 ... Open User Access Verification Password: house>en Password: house#testattack !--- The Telnet session is reset due to the !--- signature "testattack" being triggered. [Connection to 100.100.100.1 lost]`
5. 从事件查看器，当前请单击新的事件的**查询数据库**。您为以前启动的攻击看到警报
6. 在事件浏览器中，突出显示告警，右击鼠标并选择视图上下文缓冲区或查看NSDB，查看更多关于告警的详细信息。

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除步骤

完成这些步骤为了排除故障。

1. 在IDS MC中，请选择**报告>生成**。根据问题类型，在七个可用报告中的一个报告中应该能找到更详细的信息。
2. 当阻塞使用命令和控制端口配置路由器access-lists时，从传感器的探测接口发送TCP重置。使用**set span命令**在交换机，保证您跨过了正确端口，类似于此：
   `set span <src_mod/src_port><dest_mod/dest_port> both inpkts enable banana (enable) set span 2/12 3/6 both inpkts enable Overwrote Port 3/6 to monitor transmit/receive traffic of Port 2/12 Incoming Packets enabled. Learning enabled. Multicast enabled. banana (enable) banana (enable) banana (enable) show span Destination : Port 3/6 !--- Connect to sniffing interface of the Sensor. Admin Source : Port 2/12 !--- In this case, connect to Ethernet1 of Router House. Oper Source : Port 2/12 Direction : transmit/receive Incoming Packets: enabled Learning : enabled Multicast : enabled`
3. 如果TCP重置不工作，请登陆对传感器并且输入**show event命令**。启动攻击，并查看是否触发了告警。如果触发告警，检查并确保它为动作类型TCP重置设置。

相关信息

- Cisco安全入侵检测支持页
- Cisco安全入侵监测系统的文档
- CiscoWorks VPN/Security Management Solution支持页面
- 技术支持和文档 - Cisco Systems