Configurando IDS TCP Reset usando os ID de VMS MC

Índice

Introdução

O documento fornece uma configuração de exemplo do Sistema de Detecção de Intrusão da Cisco (IDS) através do VPN/Security Management Solution (VMS), o console de gerenciamento IDS (IDS MC). Neste caso, o TCP Reset do sensor de IDS a um roteador Cisco é configurado.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- O sensor é instalado e configurado detectando o tráfego necessário.
- O farejando interface é medido à interface externa do roteador.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- VMS 2.2 com IDS MC e monitor 1.2.3 da Segurança
- Sensor do Cisco IDS 4.1.3S(63)
- Roteador Cisco que executa o Software Release 12.3.5 de Cisco IOS®

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Configurações

Este documento utiliza estas configurações.

- Luz do Roteador
- Companhia do Roteador

Luz do Roteador

```
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
```

Companhia do Roteador

```
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
```

Configuração de sensor inicial

Nota: Se você tem executado já a instalação inicial de seu sensor, continua à importação o sensor na seção IDS MC.

1. Console no sensor.Você é alertado para um nome de usuário e senha. Se isto é a primeira vez você está consolando no sensor, você deve entrar com o username **Cisco** e senha **Cisco**.
2. Você é alertado mudar a senha e datilografar a senha nova para confirmar.
3. Datilografe a **instalação** e incorpore a informação apropriada em cada alerta para estabelecer parâmetros básicos para seu sensor, conforme este exemplo:
```
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
```

Importe o sensor em IDS MC

Termine estas etapas a fim importar o sensor no IDS MC.

1. Consulte a seu sensor. Neste caso, **http://10.66.79.250:1741** ou **https://10.66.79.250:1742**.
2. Início de uma sessão com o nome de usuário e senha apropriado.Neste exemplo, o username é **admin** e a senha é **Cisco**.
3. Escolha o **Solução de Gerenciamento de VPN/de Segurança > Centro de Gerenciamento** e clique **sensors de IDS**.

4. Clique a aba dos dispositivos e escolha o **grupo do sensor**.
5. Destaque **global** e o clique **cria o subgrupo**.
6. Dê entrada com o nome do grupo e assegure-se de que o **padrão** esteja escolhido, a seguir clicam a **APROVAÇÃO** a fim adicionar o subgrupo no IDS MC.
7. Escolha **dispositivos > sensor**, destaque o subgrupo criado na etapa precedente (neste caso, **teste**), e o clique **adiciona**.
8. Destaque o subgrupo e clique-o **em seguida**.
9. Incorpore os detalhes conforme este exemplo e clique-os **em seguida** a fim continuar.
10. Quando você é presentado com uma mensagem que os estados `importem com sucesso a configuração de sensor`, clique o **revestimento** a fim continuar.
11. Seu sensor é importado no IDS MC. Neste caso, Sensor5 é importado.

Importe o sensor no monitor da Segurança

Termine estas etapas a fim importar o sensor no monitor da Segurança.

1. No menu de servidor VMS, escolha **monitor Center do >** segurança do **VPN/Security Management Solution >** da **monitoração**.
2. Selecione a aba dos dispositivos, a seguir clique a **importação** e incorpore a informação do servidor IDS MC, conforme este exemplo.
3. Selecione seu sensor (neste caso, **sensor5**) e clique-o **em seguida** a fim continuar.
4. Se necessário, atualize o endereço NAT para seu sensor, a seguir clique o **revestimento** a fim continuar.
5. Clique a **APROVAÇÃO** a fim terminar importar o sensor de IDS MC no monitor da Segurança.
6. Você pode agora ver que seu sensor está importado com sucesso

Use IDS MC para atualizações de assinatura

Este procedimento explica como usar IDS MC para atualizações de assinatura.

1. Transfira as atualizações de assinatura dos ID de rede (clientes registrados somente) e salvar as no diretório **C:\PROGRA~1\CSCOpx\MDC\etc\ids\updates\ em** seu servidor VMS.
2. No console do servidor VMS, escolha o **Solução de Gerenciamento de VPN/Segurança > Centro de Gerenciamento > Sensores de IDS**.
3. Selecione o guia de configuração e clique **atualizações**.
4. Clique **assinaturas dos ID de rede da atualização**.
5. Selecione a assinatura que você quer promover do menu suspenso e o clique **aplica-se** a fim continuar.
6. Selecione os sensores para atualizar **em seguida** e clicar a fim continuar.
7. Depois que você é alertado aplicar a atualização ao centro de gerenciamento, assim como o sensor, **revestimento do** clique a fim continuar.
8. Telnet ou console na interface da linha de comando do sensor. Você vê a informação similar a esta:
```
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. Espere por alguns minutos para permitir que a elevação termine, a seguir incorpore a **versão**

da mostra a fim verificar.`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`

Configurar o TCP Reset para o IOS Router

Termine estas etapas a fim configurar o TCP Reset para o IOS Router.

1. Escolha o **Solução de Gerenciamento de VPN/Segurança > Centro de Gerenciamento > Sensores de IDS**.
2. Selecione o guia de configuração, selecione seu sensor do seletor do objeto, a seguir clique **ajustes**.
3. Selecione **assinaturas**, clique o **costume**, e o clique **adiciona** a fim adicionar uma assinatura nova.
4. Dê entrada com o nome novo da assinatura, a seguir selecione o motor (neste caso, **STRING.TCP**).
5. Verifique o botão Appropriate Radio Button a fim personalizar os parâmetros disponíveis e para clicar então **edite**.Neste exemplo, o parâmetro de ServicePorts é editado para mudar seu valor a **23** (para a porta 23). O parâmetro RegexString é editado igualmente para adicionar o **ataque de teste do** valor. Quando isto está completo, clique a **APROVAÇÃO** para continuar.
6. Clique o nome da assinatura a fim editar a gravidade da assinatura e as ações ou permiti-los/desabilitação a assinatura.
7. Neste caso, a severidade é mudada à **elevação** e o **log & a restauração da** ação são escolhidos. **APROVAÇÃO do** clique a fim continuar.
8. A assinatura completa olha similar a esta:
9. Escolha a **configuração > pendente**, verifique a configuração pendente para assegurar-se de que esteja correta, e clique a **salvaguarda**.
10. Escolha o **desenvolvimento > gerenciem**, e clicam então **aplicam-se** a fim empurrar as alterações de configuração para o sensor.
11. Escolha o **distribuição > distribuir** e o clique **submete-se**.
12. Verifique a caixa de seleção ao lado de seu sensor e o clique **distribui**.
13. Verifique a caixa de seleção para ver se há o trabalho na fila e clique-a **em seguida** a fim continuar.
14. Dê entrada com o nome do trabalho e programe o trabalho como **imediato**, a seguir clique o **revestimento**.
15. Escolha o **distribuição > distribuir > pendente**.Espere alguns minutos até que todos os trabalhos pendentes estejam terminados. A fila deve então estar vazia.
16. Escolha a **configuração** > a **história** a fim confirmar o desenvolvimento.Assegure-se de que o estado da configuração esteja indicado como **distribuído**. Isto significa que a configuração de sensor está atualizada com sucesso.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Inicie o ataque e a redefinição TCP

Lance um ataque do teste e verifique os resultados a fim verificar que os trabalhos de processo de bloqueio corretamente.

1. Antes que o ataque esteja lançado, escolha **monitor Center do >** segurança do **VPN/Security Management Solution >** da **monitoração**.
2. Escolha o **monitor do** menu principal e clique **eventos**.
3. Clique o **visualizador de eventos do lançamento**.
4. Telnet de um roteador ao outro e ao tipo **ataque de teste** a fim lançar o ataque.Neste caso, nós em telnet da luz de roteador à casa do roteador. Assim que você pressionar o **<space>** ou o **<enter>**, depois que você datilografa o **ataque de teste**, sua sessão de Telnet deve ser restaurada.`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. Do visualizador de eventos, **base de dados da pergunta do** clique para eventos novos agora.Você vê o alerta para o ataque previamente lançado
6. No visualizador de eventos, destaque o alarme, clicar-lo com o botão direito e selecione-o um ou outro **buffer do contexto da vista** ou **veja-o o NSDB** para ver mais informação detalhada sobre o alarme.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Procedimento de Troubleshooting

Termine estas etapas a fim pesquisar defeitos.

1. No IDS MC, escolha **relatórios > gerenciem**.Segundo o tipo de problema, uns detalhes mais adicionais devem ser encontrados em um dos sete relatórios disponíveis.
2. Quando obstruir utilizar o comando e a porta de controle configurar as listas de acessos do roteador, as restaurações TCP estão enviadas do farejando interface do sensor. Assegure-se de que você meça a porta correta, usando o **comando set span no** interruptor, similar a este:
   `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. Se o TCP Reset não está trabalhando, entre ao sensor e inscreva o **comando show event**.Lance o ataque, e a verificação para ver mesmo se o alarme está provocado. Se o alarme é provocado, a verificação para assegurá-lo está ajustada para o tipo **TCP Reset da** ação.

Informações Relacionadas

- Página de suporte do Cisco Secure Intrusion Detection

- Documentação para Cisco Secure Intrusion Detection System
- Página de suporte da Solução de gerenciamento de VPN/segurança CiscoWorks
- Suporte Técnico e Documentação - Cisco Systems