Configurando IPS TCP Reset usando IME

Índice

Introdução

Este documento discute a configuração do Intrusion Prevention System (IPS) TCP Reset usando o gerente IPS expresso (IME). Os sensores IME e IPS são usados para controlar um roteador Cisco para o TCP Reset. Quando você revê esta configuração, recorde estes artigos:

- Instale o sensor e certifique-se dos trabalhos do sensor corretamente.
- Faça com que a interface de monitoramento se estenda até o roteador fora da interface.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- O gerente do ips Cisco expressa 7.0
- Sensor 7.0(0.88)E3 do ips Cisco

- Roteador de Cisco IOS® com Cisco IOS Software Release 12.4

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

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Configurar

Diagrama de Rede

Este documento utiliza a configuração de rede mostrada neste diagrama.

Configurações

Este documento utiliza as configurações mostradas aqui.

- Luz do Roteador
- Companhia do Roteador

Luz do Roteador

```
Current configuration : 906 bytes
!
version 12.4
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 10.100.100.2 255.255.255.0
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
10.100.100.1 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

```
Current configuration : 939 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

```
!
hostname house ! logging queue-limit 100 enable password
cisco ! ip subnet-zero ! ! no ip cef no ip domain lookup
! ip audit notify log ip audit po max-events 100 ! ! no
voice hpi capture buffer no voice hpi capture
destination ! ! ! ! interface FastEthernet0/0 ip address
10.66.79.210 255.255.255.224 duplex auto speed auto !
interface FastEthernet0/1 ip address 10.100.100.1
255.255.255.0 duplex auto speed auto ! interface ATM1/0
no ip address shutdown no atm ilmi-keepalive ! 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 10.100.100.2 no ip http server no
ip http secure-server ! ! ! ! call rsvp-sync ! ! mgcp
profile default ! ! line con 0 exec-timeout 0 0 line aux
0 line vty 0 4 exec-timeout 0 0 password cisco login
line vty 5 15 login ! ! end
```

Comece a configuração de sensor

Termine estas etapas para começar a configuração do sensor.

1. Se esta é sua primeira vez registrar no sensor, você deve entrar em **Cisco** como o nome de usuário e em **Cisco** como a senha.
2. Quando o sistema solicitar, altere a senha.**Nota:** O cisco123 é uma palavra do dicionário e não é permitido no sistema.
3. Datilografe a **instalação** e termine a alerta do sistema a fim estabelecer os parâmetros básicos para os sensores.
4. Insira esta informação:
```
sensor5#setup --- System Configuration Dialog --- !--- At any point
you may enter a question mark '?' for help. !--- Use ctrl-c to abort the 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 Corp-IPS telnetOption enabled !--- Permit the IP address of
workstation or network with IME 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. Salve a configuração.Pode tomar alguns minutos para que o sensor salvar a configuração.
```
[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
```

Adicionar o sensor no IME

Termine estas etapas a fim adicionar o sensor no IME:

1. Vá ao PC Windows, que instalaram o gerente IPS expresso, e abra o gerente IPS expresso.
2. Escolha o **> Add home**.
3. Datilografe dentro esta informação e clique a **APROVAÇÃO** a fim terminar a configuração.
4. Escolha **dispositivos > Corp-IPS** a fim verificar o Status do sensor e clicar com o botão direito então a fim escolher o **status de dispositivo**.Certifique-se de que você pode ver a assinatura aberta com sucesso.

Configurar o TCP Reset para o roteador do Cisco IOS

Termine estas etapas a fim configurar o TCP Reset para o roteador do Cisco IOS:

1. Do IME PC, abra seu navegador da Web e vá a **https://10.66.79.195**.
2. Clique a **APROVAÇÃO** a fim aceitar o certificado HTTPS transferido do sensor.
3. No indicador do início de uma sessão, incorpore **Cisco** para o nome de usuário e **123cisco123** para a senha.Esta interface de gerenciamento IME aparece:
4. Do guia de configuração, clique **assinaturas ativas**.
5. Clique então o **Wizard de Assinatura.**
6. No assistente, escolha **sim** e escolha a **corda TCP** como o Engine de assinatura. Clique em Next.
7. Você pode deixar esta informação como o efdault ou incorporar seus próprios ID de assinatura, nome da assinatura e notas do usuário. Clique em Next.
8. Escolha a **ação do evento**, e escolha o **alerta do produto** e **restaure a conexão de TCP**. Clique a **APROVAÇÃO** e a fim continuar então **em seguida**.
9. Incorpore uma expressão regular, e o `ataque de teste` é usado neste exemplo. Incorpore **23** para portas do serviço, escolha-os **prestar serviços de manutenção em seguida** para o sentido, e o clique a fim continuar.
10. Você pode deixar esta informação como o padrão. Clique em Next.
11. **Revestimento do** clique a fim terminar o assistente.
12. Escolha a **configuração > o sig0 > assinaturas ativas** a fim encontrar a assinatura recém-criado pelos **Sig ID** ou pelo **nome dos Sig**. O clique **edita** a fim ver a assinatura.
13. Clique a **APROVAÇÃO** depois que você confirma e clica o **botão Apply Button** a fim aplicar a assinatura ao sensor.

Verificar

Lance o ataque e o TCP Reset

Termine estas etapas a fim lançar o ataque e o TCP Reset:

1. Antes que você lance o ataque, vai ao **IME**, escolhe o **monitoramento de evento > a opinião deixada cair dos ataques** e escolhe o sensor à direita.
2. Do Router Light, Telnet para o Router House e inserir um teste de ataque.Bata o **<space>** ou o **<enter>** a fim restaurar sua sessão de Telnet.
```
light#telnet 10.100.100.1 Trying 10.100.100.1 ... Open User Access Verification Password: house>en Password: house#testattack [Connection to 10.100.100.1 closed by foreign host] !--- Telnet session has been reset due to the !--- signature "String.tcp" triggered.
```
3. Do painel do visualizador de eventos IPS, o alarme vermelho aparece uma vez que o ataque é lançado.

Troubleshooting

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

Dicas

Use estes dicas de Troubleshooting:

- Evitar dá certo do comando e da porta de controle reprogram o Access Control Lists (ACLs) do roteador. As restaurações TCP são enviadas do **farejando interface do** sensor. Quando você **ajusta o período no** interruptor, use o **comando set span <src_mod/src_port><dest_mod/dest_port>** com ambos os pacotes recebidos permitidos como mostrado aqui.`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 !--- connect to FastEthernet0/0 of Router House Oper Source : Port 2/12 Direction : transmit/receive Incoming Packets: enabled Multicast : enabled`
- Se as restaurações TCP estão trabalhando, verifique se o alarme é provocado para o tipo TCP Reset da ação. Se o alarme aparece, certifique-se do tipo da assinatura esteja ajustado ao TCP Reset.Entre usando a conta de serviço SU para enraizar e emitir este comando. Este comando supõe que a relação de detecção está ajustada ao eth0.`[root@sensor1 root]#`**`tcpdump -i eth0 -n`** **Nota:** Cem restaurações tcp obtêm enviadas à vítima/alvo então cem obtêm enviadas ao atacante/cliente.Esta é uma saída de exemplo:

```
03:06:00.598777
64.104.209.205.1409 >
 10.66.79.38.telnet: R 107:107(0) ack 72 win 0
03:06:00.598794 64.104.209.205.1409 >
 10.66.79.38.telnet: R 108:108(0) ack 72 win 0

03:06:00.599360 10.66.79.38.telnet >
 64.104.209.205.1409: R 72:72(0) ack 46 win 0
03:06:00.599377 10.66.79.38.telnet >
 64.104.209.205.1409: R 73:73(0) ack 46 win 0
```

Informações Relacionadas

- Página de suporte segura da prevenção de intrusão de Cisco
- Documentação para o sistema seguro da prevenção de intrusão de Cisco
- Suporte Técnico e Documentação - Cisco Systems