ESA FAQ: Como você analisa edições intermitentes da entrega de correio no ESA?

Índice

Introdução

Este documento descreve como analisar edições intermitentes da entrega de correio na ferramenta de segurança do email de Cisco (ESA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco ESA
- AsyncOS

Componentes Utilizados

A informação neste documento é baseada em todas as versões de AsyncOS.

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.

Como você analisa edições intermitentes da entrega de correio

no ESA?

Você pode usar a injeção debuga entra a ordem para seguir a conversação inteira do Simple Mail Transfer Protocol (SMTP) entre o ESA e a conexão de servidor de entrada. Cada linha dentro da injeção debuga logs esboça os dados que são enviados e recebidos durante a conversação SMTP.

Termine estas etapas a fim permitir a injeção debugam logs com o GUI:

1. Navegue às **assinaturas da administração do sistema > do log no** GUI.
2. Escolha **adicionam a assinatura do log….**
3. No log datilografe o campo, a **injeção** seleta **debuga logs** e entra os dados apropriados.

Estão aqui algumas considerações importantes quando você entra a injeção debuga o data&colon dos logs;

- Os endereços CIDR, tais como **10.1.1.0/24**, são permitidos.
- Os intervalos de endereço IP, tais como **10.1.1.10-20**, são permitidos.
- O sub-redes IP, tal como **10.2.3**, é permitido.
- Os nomes de host e os convites, tais como **crm.example.com**, são permitidos (mas não **example.com**).
- Os convites devem ser expressados como **.example.com** (sem um asterisco).
- Quando você segue um email de entrada, o nome de host deve combinar o host do remetente.
- Quando você segue um email de partida, o nome de host deve combinar os nomes de host interno.
- O número de sessões de SMTP deve estar entre uma e 25.

Termine estas etapas a fim permitir a injeção debugam logs com o CLI:

1. Inscreva o **logconfig > o comando new no** CLI.
2. Escolha a **injeção debugam logs**.
3. Dê entrada com um nome para o log, tal como o **debugging_example**.
4. Entre no hostname, endereço IP de Um ou Mais Servidores Cisco ICM NT, ou o bloco de endereços IP de Um ou Mais Servidores Cisco ICM NT para que você quer gravar a injeção debuga a informação, tal como **mail1.example.com**.

5. Incorpore o número de sessões de SMTP que você quer gravar para este domínio. Assegure-se de que o valor esteja entre um e 25.

6. Incorpore o método que você quer usar a fim recuperar os logs, tais como a **votação FTP**.

7. Incorpore o nome de arquivo. Você pode usar o nome de arquivo do padrão se você deseja.

8. Selecione os padrões que permanecem.

Este exemplo mostra que a injeção debuga logs quando o ESA aceita o correio de um server.

> Nota: A injeção debuga logs e o domínio debuga logs é similar aos mail_logs, assim que você pode usar o **grep** e os **comandos tail**.

```
Sent to '10.251.21.203': '220 ironportappliance ESMTP\r\n'
Rcvd from '10.251.21.203': 'EHLO outgoing.example.com\r\n'
Sent to '10.251.21.203': '250-nibbles.run\r\n250-8BITMIME\r\n250
 SIZE 104857600\r\n'
Rcvd from '10.251.21.203': 'MAIL FROM:<jsmith@example.com>\r\n'
Sent to '10.251.21.203': '250 sender <jsmith@example.com> ok\r\n'
Rcvd from '10.251.21.203': 'RCPT TO:<test@example.org>\r\n'
Sent to '10.251.21.203': '250 recipient <test@example.org>ok\r\n'
Rcvd from '10.251.21.203': 'DATA\r\n'
Sent to '10.251.21.203': '354 go ahead\r\n'
Rcvd from '10.251.21.203': 'To: "test@example.org" <test@example.org>
 \r\nSubject: 12:14pm - test\r\nFrom: Hotel_Users <jsmith@example.com>
 \r\nContent-Type: text/plain; format=flowed; delsp=yes;
 charset=iso-8859-15\r\nMIME-Version: 1.0\r\nContent-Transfer-Encoding:
 7bit\r\nDate: Tue, 09 Jan 2007 12:14:35 -0800\r\nMessage-ID:
 <op.tlwk6lvgwomlp4@outgoing.example.com>\r\nUser-Agent: Opera Mail/9.10
 (Win32)\r\n\r\ntest\r\n'
Rcvd from '10.251.21.203': '\r\n.\r\n'
Sent to '10.251.21.203': '250 ok: Message 270 accepted\r\n'
Rcvd from '10.251.21.203': 'QUIT\r\n'
Sent to '10.251.21.203': '221 nibbles.run\r\n'
```