Dados do pacote da transferência (arquivo PCAP) que usam a relação de usuário de web

Índice

Introdução

Usando a relação de usuário de web, você pode transferir os pacotes que provocaram a regra do Snort. O artigo fornece as etapas para transferir os dados da captura de pacote de informação (arquivo PCAP) que usam a relação de usuário de web de um sistema de administração de Sourcefire FireSIGHT.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento no dispositivo de Sourcefire FirePOWER e nos modelos do dispositivo virtual.

Componentes Utilizados

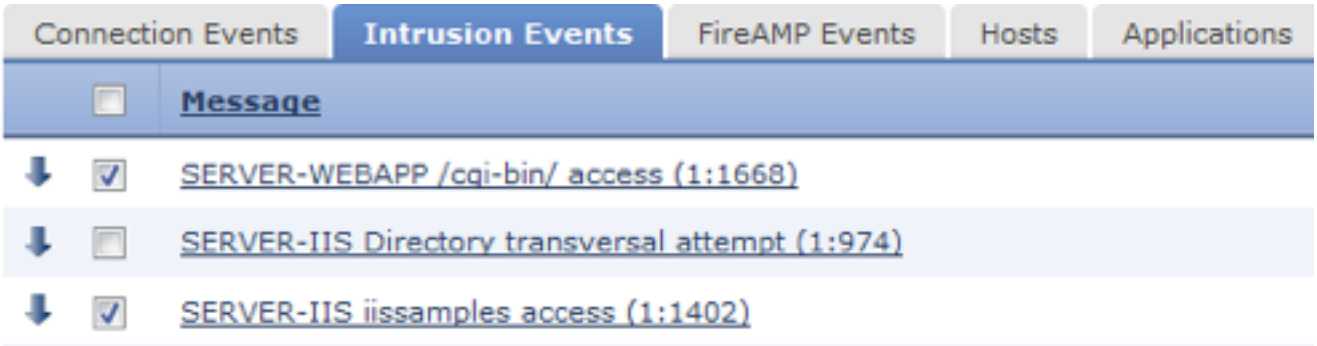
A informação neste documento é baseada no centro de gerenciamento de Sourcefire FireSIGHT, igualmente conhecido como o centro da defesa, a versão de software running 5.2 ou maior.

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.

Etapas para transferir o arquivo PCAP

Passo 1: O início de uma sessão a um centro ou a um centro de gerenciamento da defesa de Sourcefire, e navega à página dos eventos da intrusão como abaixo:

Passo 2: Usando a caixa de verificação, selecione os eventos de que você gostaria de transferir dados da captura de pacote de informação (arquivo PCAP).



Passo 3: Rolo à parte inferior da página e de qualquer uma:

- Pacote da transferência do clique para transferir os pacotes que provocaram os eventos selecionados da intrusão
- A transferência do clique todos os pacotes para transferir todos os pacotes que provocaram os eventos da intrusão na corrente forçou a vista

Note: Os pacotes transferidos salvar como um PCAP. Se você quer analisar a captura de pacote de informação, você precisará de transferir e instalar o software que é capaz de ler um arquivo PCAP.

Passo 4: Quando alertado, salvar o arquivo PCAP a seu disco rígido.