Scarica dati pacchetto (file PCAP) tramite interfaccia utente Web

Sommario

Introduzione

Tramite l'interfaccia utente Web è possibile scaricare i pacchetti che hanno attivato la regola Snort.In questo documento viene descritto come scaricare i dati di acquisizione dei pacchetti (file PCAP) utilizzando l'interfaccia utente Web di un sistema di gestione Sourcefire FireSIGHT.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei dispositivi Sourcefire FirePOWER e dei modelli di dispositivi virtuali.

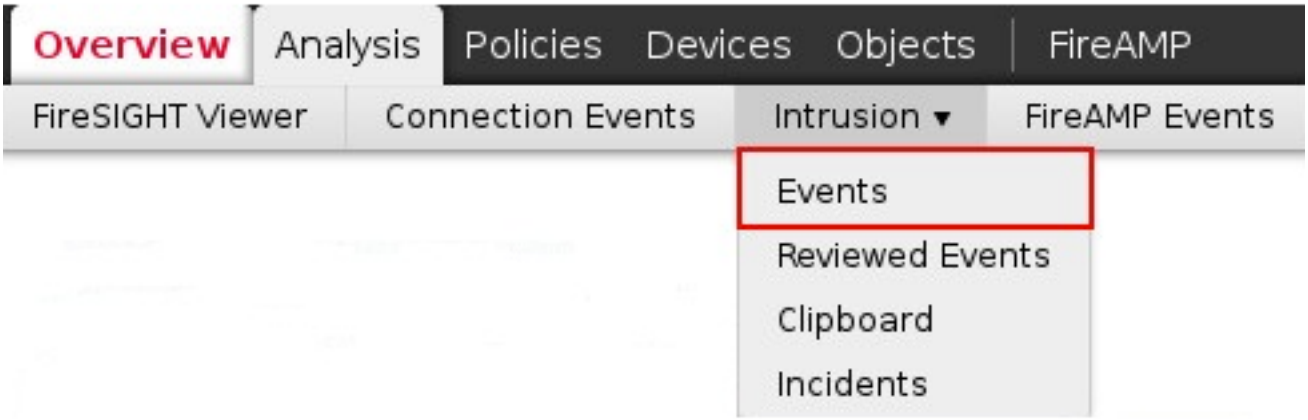
Componenti usati

Le informazioni contenute in questo documento si basano sul Sourcefire FireSIGHT Management Center, noto anche come Defense Center, che esegue software versione 5.2 o successive.

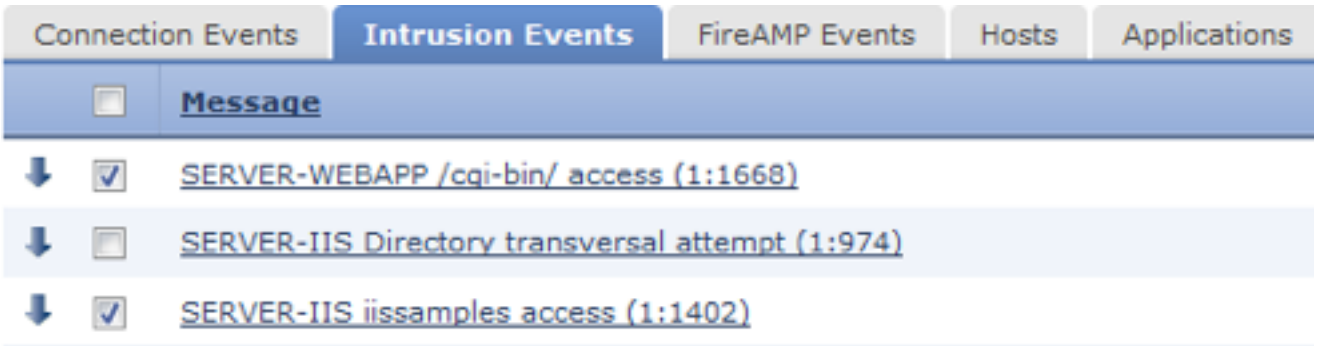
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Procedura per il download del file PCAP

Passaggio 1: Accedere a un centro di difesa o di gestione Sourcefire e passare alla pagina Eventi intrusione come indicato di seguito:



Passaggio 2: Utilizzando la casella di controllo, selezionare gli eventi che si desidera scaricare i dati di acquisizione dei pacchetti (file PCAP).



Passaggio 3: Scorrere fino alla fine della pagina e:

- Fare clic su Scarica pacchetto per scaricare i pacchetti che hanno attivato gli eventi di intrusione selezionati
- Fare clic su Scarica tutti i pacchetti per scaricare tutti i pacchetti che hanno attivato gli eventi di intrusione nella visualizzazione vincolata corrente

Nota: I pacchetti scaricati verranno salvati come PCAP. Per analizzare l'acquisizione dei pacchetti, è necessario scaricare e installare un software in grado di leggere un file PCAP.

Passaggio 4: Quando richiesto, salvare il file PCAP sul disco rigido.