Web ユーザ インターフェイスを使ったパケット データ(PCAP ファイル)のダウンロード

内容

<u>概要</u> <u>前提条件</u> <u>要件</u> <u>使用するコンポーネント</u> <u>PCAP ファイルのダウンロード手順</u>

概要

この記事では、Sourcefire FireSIGHT Management SystemのWebユーザインターフェイスを使用 してパケットキャプチャデータ(PCAPファイル)をダウンロードする手順について説明します 。

前提条件

要件

Sourcefire FirePOWER デバイスとバーチャル デバイスのモデルに関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、ソフトウェア バージョン 5.2 以降が稼働する Sourcefire FireSIGHT Management Center (Defense Center とも呼ばれる) に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

PCAP ファイルのダウンロード手順

ステップ 1: Sourcefire Defense Center または Management Center にログインし、次に示すように [Intrusion Events] ページに移動します。

Overview	Analysis	Policies	Devic	es	Objects	Fir	eAMP
FireSIGHT Viewer Connection Events				Intrusion 🔻 FireA		AMP Events	
				Ev	ents		
					Reviewed Events		
				Cli	pboard		
				Ind	cidents		

ステップ 2: チェックボックスを使用して、パケット キャプチャ データ(PCAP ファイル)をダ ウンロードするイベントを選択します。

Connection Events		on Events	Intrusion Events FireAMP Events		Hosts	Applications		
		<u>Message</u>						
4	V	SERVER-WEBAPP /cgi-bin/ access (1:1668)						
۰Ļ		SERVER-IIS Directory transversal attempt (1:974)						
4	1	SERVER-IIS iissamples access (1:1402)						

ステップ3:ページの下部までスクロールし、次のいずれかを実行します。

- [Download Packet] をクリックし、選択されている侵入イベントをトリガーしたパケットをダウンロードします。
- [Download All Packets] をクリックし、現在の制限ビューに示されている侵入イベントをトリ ガーしたすべてのパケットをダウンロードします。

注:ダウンロードしたパケットは PCAP として保存されます。 パケット キャプチャを分 析するには、PCAP ファイルを読み取ることができるソフトウェアをダウンロードしてイン ストールする必要があります。

ステップ 4: プロンプトが表示されたら、ハード ドライブに PCAP ファイルを保存します。