Download Packet Data (PCAP File) Using Web User Interface

Document ID: 117892

Contributed by Nazmul Rajib, Cisco TAC Engineer.
Jul 09, 2014

Contents

Introduction

Using the Web User Interface, you can download the packet(s) that triggered Snort rule.The article provides the steps to download packet capture data (PCAP file) using the Web User Interface of a Sourcefire FireSIGHT Management System.

Prerequisites

Requirements

Cisco recommends that you have knowledge on Sourcefire FirePOWER device and the virtual device models.

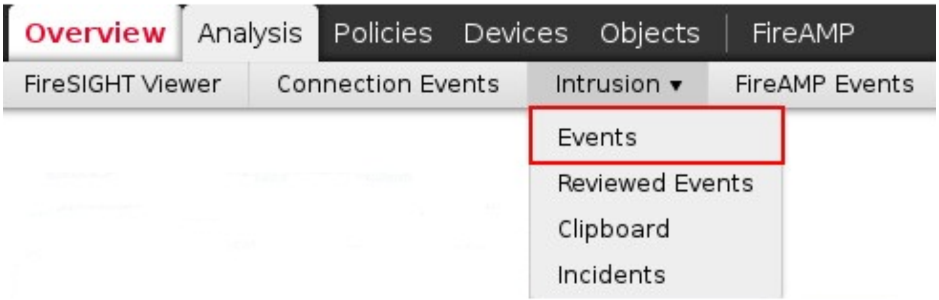
Components Used

The information on this document is based on Sourcefire FireSIGHT Management Center, also known as Defense Center, running software version 5.2 or greater.

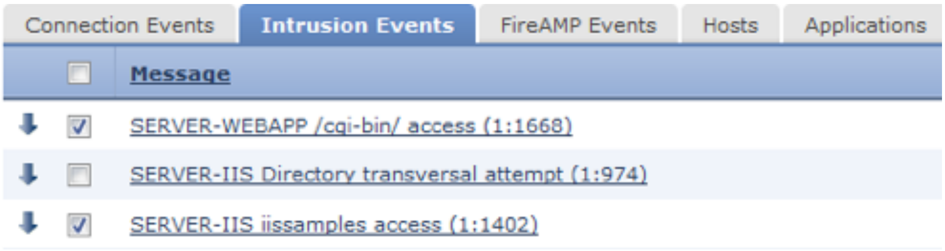
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Steps to Download PCAP File

Step 1: Login to a Sourcefire Defense Center or Management Center, and navigate to the Intrusion Events page as below:



Step 2: Using the check box, select the event(s) that you would like to download packet capture data (PCAP file).



	□	Message
⬇	☑	SERVER-WEBAPP /cgi-bin/ access (1:1668)
⬇	□	SERVER-IIS Directory transversal attempt (1:974)
⬇	☑	SERVER-IIS iissamples access (1:1402)

Step 3: Scroll to the bottom of the page and either:

- Click Download Packet to download the packets that triggered the selected intrusion event(s)
- Click Download All Packets to download all packets that triggered the intrusion events in the current constrained view

Note: The downloaded packets will be saved as a PCAP. If you want to analyze the packet capture, you will need to download and install software that is capable of reading a PCAP file.

Step 4: When prompted, save the PCAP file to your hard drive.

Updated: Jul 09, 2014 Document ID: 117892