Télécharger les données de paquets (fichier PCAP) à l'aide de l'interface utilisateur Web

Contenu

Introduction

Àl'aide de l'interface utilisateur Web, vous pouvez télécharger le ou les paquets qui ont déclenché la règle Snort.L'article décrit les étapes à suivre pour télécharger les données de capture de paquets (fichier PCAP) à l'aide de l'interface utilisateur Web d'un système de gestion FireSIGHT Sourcefire.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître le périphérique FirePOWER Sourcefire et les modèles de périphériques virtuels.

Components Used

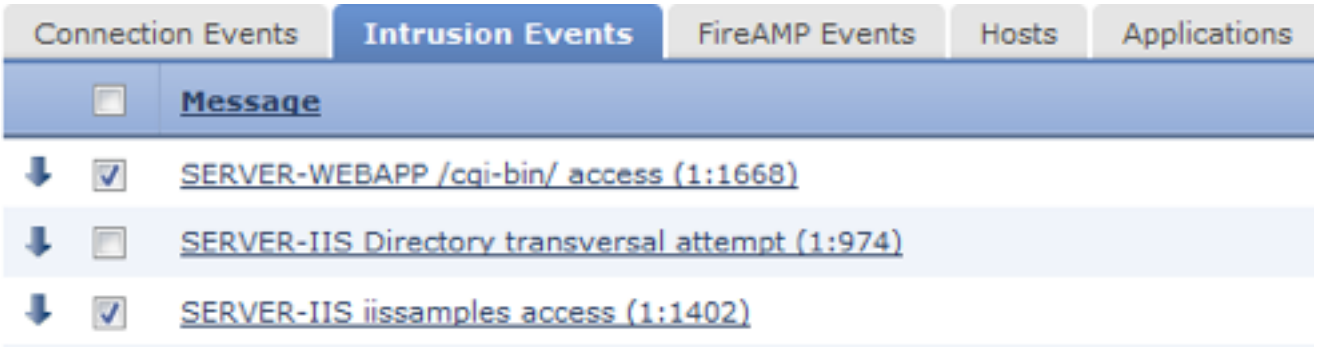
Les informations contenues dans ce document sont basées sur Sourcefire FireSIGHT Management Center, également appelé Defense Center, exécutant le logiciel version 5.2 ou ultérieure.

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.

Étapes de téléchargement du fichier PCAP

Étape 1 : Connectez-vous à un centre de défense Sourcefire ou à un centre de gestion et accédez à la page Intrusion Events comme suit :

Étape 2 : À l'aide de cette case à cocher, sélectionnez le ou les événements que vous souhaitez télécharger des données de capture de paquets (fichier PCAP).



Étape 3 : Faites défiler la page jusqu'en bas et effectuez les opérations suivantes :

- Cliquez sur Download Packet (Télécharger le paquet) pour télécharger les paquets qui ont déclenché les événements d'intrusion sélectionnés.
- Cliquez sur Download All Packets (Télécharger tous les paquets) pour télécharger tous les paquets qui ont déclenché les événements d'intrusion dans la vue contrainte actuelle.

  Note: Les paquets téléchargés seront enregistrés en tant que PCAP. Si vous voulez analyser la capture de paquets, vous devez télécharger et installer un logiciel capable de lire un fichier PCAP.

Étape 4 : Lorsque vous y êtes invité, enregistrez le fichier PCAP sur votre disque dur.