Données de paquets de téléchargement (fichier PCAP) utilisant l'interface utilisateur d'utilisateur web

Contenu

Introduction

Utilisant l'interface utilisateur d'utilisateur web, vous pouvez télécharger les paquets qui ont déclenché reniflent la règle. L'article prévoit les étapes pour télécharger des données de capture de paquet (fichier PCAP) utilisant l'interface utilisateur d'utilisateur web d'un système de gestion de Sourcefire FireSIGHT.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance sur le périphérique de puissance de feu de Sourcefire et les modèles de périphérique virtuel.

Composants utilisés

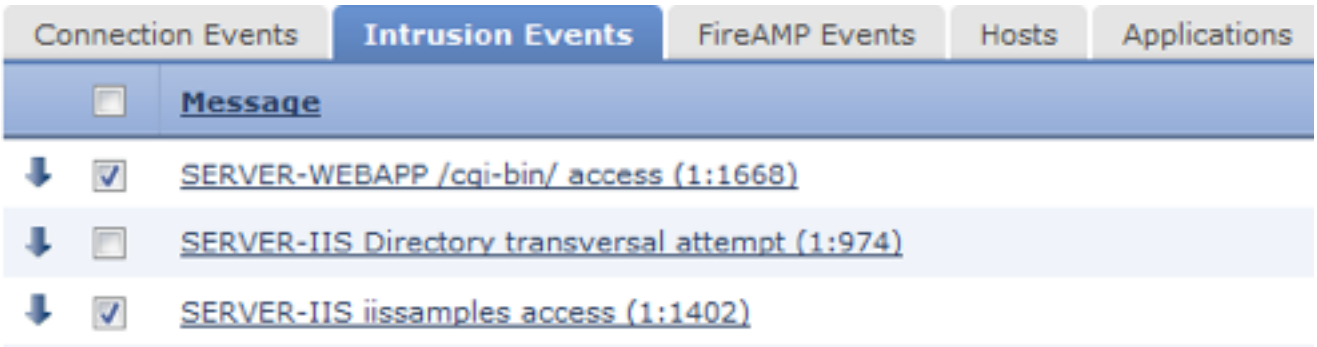
Les informations sur ce document sont basées sur le centre de Gestion de Sourcefire FireSIGHT, également connu sous le nom de centre de la défense, version de logiciel courante 5.2 ou plus grand.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Étapes pour télécharger le fichier PCAP

Étape 1 : La procédure de connexion à un centre de la défense de Sourcefire ou au centre de Gestion, et naviguent vers la page d'événements d'intrusion en tant que ci-dessous :

Étape 2 : Utilisant la case, sélectionnez les événements qui vous voudriez que téléchargent des données de capture de paquet (fichier PCAP).



Étape 3 : Défilement au bas de page et à l'un ou l'autre :

- Cliquez sur Download le paquet pour télécharger les paquets qui ont déclenché les événements sélectionnés d'intrusion
- Cliquez sur Download tous les paquets pour télécharger tous les paquets qui ont déclenché les événements d'intrusion dans la vue contrainte par courant

  Remarque: Les paquets téléchargés seront enregistrés comme PCAP. Si vous voulez analyser la capture de paquet, vous devrez télécharger et installer le logiciel qui est capable de lire un fichier PCAP.

Étape 4 : Une fois incité, sauvegardez le fichier PCAP à votre disque dur.