Initiez des captures de paquets de précision pour analyser les conditions de fenêtre zéro

Publié: 2024-09-26

Dans les métriques TCP, la taille de la fenêtre indique la quantité de données qu'un équipement peut recevoir et traiter au cours d'un flux. Lorsque la taille de la fenêtre est nulle, les transmissions sont interrompues jusqu'à ce que l'équipement indique qu'il dispose de l'espace nécessaire pour recevoir à nouveau des données.

Il n'est pas rare que les fenêtres ne durent qu'une ou deux secondes, surtout en période de fort trafic. Cependant, des conditions de fenêtre zéro qui durent plus longtemps peuvent indiquer un problème plus grave et entraîner des problèmes de performances.

Vous pouvez créer un tableau de bord ou configurer des notifications d'alerte pour ne suivre aucune occurrence de fenêtre, mais la cause peut être difficile à déterminer. Par exemple, l'utilisation du processeur, de la mémoire et de la carte réseau peut être normale et vous ne savez pas si le problème provient du réseau, des serveurs ou de l'application. Mais vous pouvez toujours trouver la vérité dans le paquet !

Dans cette procédure pas à pas, vous allez créer un déclencheur qui capture les paquets sans conditions de fenêtre sur les transactions HTTP. Vous téléchargerez ensuite les captures afin de pouvoir télécharger les données vers un analyseur de paquets afin de vous aider à déterminer l'état du client et du serveur sur un flux lorsque des conditions de fenêtre zéro se sont produites.

Prérequis

- Vous devez disposer de privilèges d'administration du système et des droits d'accès ou de privilèges d'écriture complets avec l'accès aux paquets activé.
- Vous devez activer la capture de paquets via la page d'administration.
- Vous devez disposer d'un analyseur de paquets, tel que WireShark ou Microsoft Network Monitor.
- Familiarisez-vous avec DÉCLENCHEURS les concepts et les procédures dans Créez un déclencheur.

Écrire le déclencheur de capture de précision

Dans les étapes suivantes, vous allez écrire un déclencheur qui lance une capture de paquet précise chaque fois qu'une condition de fenêtre nulle se produit sur une transaction HTTP.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **éléments déclencheurs**.
3. Cliquez **Créez**.
4. Spécifiez les paramètres de configuration du déclencheur suivants :
   a) Tapez `PCAP à taille de fenêtre à zéro` dans le **Nom** champ.
   b) Dans la liste des événements, sélectionnez **FLOW_TICK**.
   c) Dans le champ Devoirs, tapez `HTTP Servers`, puis sélectionnez **Serveurs HTTP**.
   d) Sélectionnez le **Activer le journal de débogage** case à cocher.
   e) Cliquez **Afficher les options avancées** et tapez `128` dans le champ Octets par paquet à capturer.

   Conseil La valeur par défaut est 0. Conservez cette valeur pour capturer tous les octets de chaque paquet.

5. Dans le volet droit, tapez le code suivant pour lancer la capture de paquets lorsqu'une condition de fenêtre nulle se produit :

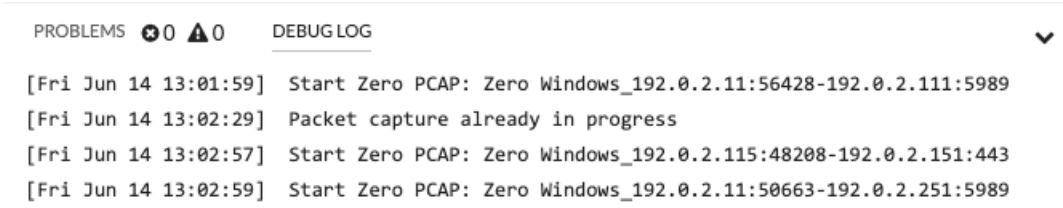
```
// Check to make sure that this is an HTTP transaction
if ( Flow.l7proto !== 'HTTP' ){
    return;
}

//The packet capture name, which includes the client and server
//IP addresses and port numbers
var pcapName = 'Zero Windows_'
    + Flow.client.ipaddr + ':' + Flow.client.port
    + '-'
    + Flow.server.ipaddr + ':' + Flow.server.port;

//Initiate packet capture each time a zero window occurs on
//the client or the server
if ( Flow.zeroWnd1 > 0 || Flow.zeroWnd2 > 0 ) {
    var opts = {
        maxPackets: 30,        // Capture up to 30 packets
        maxPacketsLookback: 15 // Capture up to 15 lookback packets
    };
    Flow.captureStart(pcapName, opts);
    //Show capture activity in debug log
    debug('Start Zero PCAP: ' + pcapName);
}
```

6. Cliquez **Enregistrer**.

Afficher la sortie de débogage dans le journal de débogage

Au cours des étapes suivantes, vous allez consulter la sortie de débogage du déclencheur pour confirmer que le déclencheur est en cours d'exécution et qu'il capture des paquets. Une fois que vous avez attribué le déclencheur à vos sources de données , le système exécute le déclencheur lorsque le trafic HTTP se produit, et si une transaction contient une fenêtre zéro, le système envoie les résultats du débogage au journal de débogage.

1. Cliquez sur l'icône des paramètres système, puis cliquez sur **DÉCLENCHEURS**.
2. Cliquez sur **PCAP de taille de fenêtre à zéro** déclencheur que vous venez de créer.
3. Cliquez **Modifier le script de déclenchement**.
4. Cliquez sur le **Journal de débogage** onglet.
   Le journal de débogage affiche des résultats similaires à ceux de la figure suivante :



Télécharger et afficher les captures de paquets

Au cours des étapes suivantes, vous allez télécharger des captures de paquets.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Dans le menu supérieur, cliquez sur **Disques**.
3. Cliquez **Afficher les enregistrements**.

4. Dans la liste déroulante Type d'enregistrement, sélectionnez **Capture de paquets**.
5. Une fois que les enregistrements associés à votre capture de paquets apparaissent, cliquez sur l'icône Paquets, puis cliquez sur **Télécharger PCAP**.