Hop supplémentaire

Créez un déclencheur pour surveiller les réponses aux requêtes NTP monlist

Publié: 2024-07-03

Les machines de votre environnement synchronisent les horloges via le protocole NTP (Network Time Protocol), mais celui-ci présente certaines failles de sécurité, telles que les attaques par amplification qui entraînent un déni de service.

Par exemple, un attaquant peut usurper l'adresse IP de votre serveur NTP, puis envoyer à plusieurs reprises une commande monlist via cette adresse usurpée. La commande monlist demande une liste des 600 derniers hôtes connectés au serveur NTP, mais comme l'adresse IP demandée est usurpée, le serveur envoie la liste à l'adresse usurpée. La réponse est considérablement plus importante que la demande, et le client falsifié est surchargé, ce qui peut entraîner le refus de demandes légitimes.

Dans cette procédure pas à pas, vous allez écrire un déclencheur qui vérifie le trafic UDP sur votre serveur NTP pour détecter les réponses aux commandes monlist. Le déclencheur envoie également un message d'alerte à un serveur Syslog distant lorsqu'une réponse monlist se produit.

Prérequis

- Vous devez avoir accès à un système ExtraHop avec un compte utilisateur doté de privilèges d'administration du système et des accès.
- Vous devez avoir au moins un serveur NTP à surveiller.
- Vous devez disposer d'un serveur Syslog distant capable de recevoir des données du système ExtraHop.
- Vous devez être familiarisé avec JavaScript.
- Familiarisez-vous avec les concepts présentés dans cette procédure pas à pas en lisant le Flux de données ouverts section du Guide de l'interface utilisateur d'ExtraHop et le Commencez avec les déclencheurs section du Guide de l'utilisateur du système ExtraHop .
- Familiarisez-vous avec les processus de création de déclencheurs et de configuration de flux de données ouverts en remplissant le Procédure pas à pas du déclencheur et le Procédure pas à pas de l'ODS.

Configuration d'un flux de données ouvert vers une cible Syslog

Dans les étapes suivantes, vous allez configurer l'hôte, le port et le protocole pour la cible du flux de données ouvert.

1. Connectez-vous au système ExtraHop à partir duquel vous souhaitez envoyer des données avec un compte doté de privilèges d'administration du système et des accès.
2. Cliquez sur l'icône des paramètres système, puis cliquez sur **Toute l'administration**.
3. Dans la section Configuration du système, cliquez sur **Flux de données ouverts**.
4. Cliquez **Ajouter une cible**.
5. Sélectionnez **Syslog** à partir du Type de cible liste déroulante.
6. Dans le Nom champ, type `Syslog NTP` sauf s'il s'agit de la première cible Syslog que vous avez créée. Dans ce cas, la cible est automatiquement nommée « par défaut » et ne peut pas être renommée.
7. Dans le Hôte dans ce champ, saisissez l'adresse IP ou le nom d'hôte du serveur Syslog auquel vous souhaitez envoyer des données.

8. Dans le Port dans ce champ, saisissez le numéro de port auquel vous souhaitez envoyer des données.
9. Dans la liste des protocoles, sélectionnez **UDP**.

   Conseil Cliquez **Tester** pour établir une connexion et envoyer un message de test du système ExtraHop au serveur Syslog distant.
10. Sélectionnez **Local** si vous souhaitez envoyer des informations Syslog avec des horodatages dans le fuseau horaire local du système ExtraHop. Dans le cas contraire, les horodatages sont envoyés en GMT.
11. Cliquez **Enregistrer**.
    La cible est ajoutée à la table Syslog sur la page Open Data Stream .

Écrire un déclencheur pour analyser les charges utiles NTP

Dans les étapes suivantes, vous allez écrire un déclencheur qui indique les données à examiner à partir des réponses du serveur NTP et s'il convient de les envoyer à un serveur Syslog distant.

1. Cliquez sur le logo ExtraHop dans le coin supérieur gauche pour revenir au système ExtraHop .
2. Cliquez sur l'icône des paramètres système , puis cliquez sur **DÉCLENCHEURS**.
3. Cliquez **Créez**.
4. Dans le Nom champ, type `Analyse la charge utile UDP pour les réponses NTP .`
5. Cliquez **Activer le journal de débogage** pour activer le journal de débogage et les mesures de performance du déclencheur.
6. Dans le Évènements champ, sélectionnez **UDP_PAYLOAD**.
7. Cliquez **Afficher les options avancées** et spécifiez les paramètres de charge utile suivants pour rechercher le trafic NTP uniquement sur le port UDP 123 :
   a) Sélectionnez **Exécuter le déclencheur sur tous les paquets UDP**.
   b) Dans le Plage de ports de serveur Champ minimum, type `123`.
   c) Dans le Plage de ports de serveur Champ maximal, type `123`.
8. Dans le volet droit, ajoutez le code déclencheur suivant pour permettre l'accès à la charge utile de réponse du serveur NTP :

```
//Capture the NTP server response
let buf = Flow.server.payload;
//Exit the trigger if the NTP server response cannot be captured
if (buf === null) {
    return;
}
```

9. Ajoutez le code de déclencheur suivant au script existant pour spécifier les champs que le déclencheur doit extraire de l'en-tête de la charge utile et les champs à ignorer :

```
//Define the format of the NTP response
let fmt = ('B' + // Flags (LI, Version, Mode)
           'x' + // Auth + Seq (ignore)
           'x' + // Implementations (ignore)
           'B' + // Request code
           'B'); // Error
```

10. Ajoutez le code déclencheur suivant au script existant pour extraire les champs de la charge utile :

```
//Analyze the NTP response based on the defined format
let values = buf.unpack(fmt);
let mode = values[0] & 0x7;
```

11. Ajoutez le code déclencheur suivant au script existant pour vérifier les valeurs des champs d'en-tête suivants :

```
// Exit the trigger if the mode value is not 7.
if (mode !== 7) {
    return;
}
let reqCode = values[1];

//Save the last four bits of the error code as a variable
let errorCode = values[2] >> 4;
```

Le mode, situé dans les trois derniers bits du champ, indique le mode de fonctionnement NTP. La valeur 7 indique que le serveur NTP répond à une commande en mode privé, qui inclut la commande monlist.

Le champ du code de demande indique le type de demande. Une valeur de 20 ou 42 indique une demande monlist.

Le champ du code d'erreur, situé dans les quatre derniers bits, indique le type d'erreur. La valeur 0 indique que la réponse n'est pas une erreur.

12. Ajoutez le code déclencheur suivant au script existant pour envoyer un message de niveau alerte au serveur Syslog distant si le serveur NTP répond à une commande monlist et si la réponse n'est pas une erreur.

```
//Check that there is no error and that the monlist command has been run
if ((errorCode === 0) && ((reqCode === 20) || (reqCode === 42))) {
    //If the monlist command has been run, send an alert level message
 with
    //the NTP server IP address to the Syslog server
    Remote.Syslog('NTP Syslog').alert('monlist enabled on ' +
 Flow.server.ipaddr);
}
```

Le déclencheur envoie des messages contenant l'adresse IP du serveur NTP au serveur Syslog distant que vous avez configuré précédemment. Si la cible que vous avez configurée a été automatiquement nommée, remplacez `'NTP Syslog'` avec `'default'` dans le code.

13. Ajoutez le code déclencheur suivant au script existant pour vérifier si le débogage est activé et envoyez la sortie spécifiée au journal de débogage.

```
//Print the IP address, request code, and error code in the debug log
debug('NTP Server ' + Flow.server.ipaddr +
      ' responded to mode 7 command ' + reqCode +
      ' with error code '  + errorCode + '.');
```

14. Cliquez **Enregistrer**.

Attribuer le déclencheur UPA à un équipement

Avant que le déclencheur puisse examiner les charges utiles des réponses UDP, vous devez attribuer le déclencheur à au moins un équipement. Pour cette procédure pas à pas, vous allez attribuer le déclencheur aux serveurs NTP de votre réseau.

> **Important:** Attribuez des déclencheurs uniquement aux appareils spécifiques à partir desquels vous devez collecter des métriques afin de minimiser l'impact de vos déclencheurs sur les performances du système ExtraHop.

1. Cliquez **Actifs** depuis le menu supérieur.
2. Dans le volet de gauche, cliquez sur **Appareils**.

3. Dans le Nom colonne, recherchez au moins un serveur NTP et cochez la case.
4. Cliquez **Assigner un déclencheur** en haut de page.
5. Cliquez sur la case à cocher à côté du **Analyse la charge utile UDP pour les réponses NTP** déclencheur, puis cliquez sur **Assigner des déclencheurs**.

Une fois le déclencheur attribué, il fonctionne en continu jusqu'à ce qu'il soit désactivé.

Consultez votre serveur Syslog et le journal de débogage pour connaître les résultats du déclencheur

Lorsqu'une réponse à une commande monlist est envoyée par le serveur NTP, le déclencheur envoie un message de niveau alerte à votre serveur Syslog distant. Le message contient l'adresse IP du serveur NTP qui a envoyé la réponse, similaire au message suivant :

```
1 2017-01-11T22:14:15.003Z mymachine.example.com monlist enabled on
    198.51.100.0
```

En outre, le déclencheur envoie une sortie au journal de débogage si le débogage est activé. Pour afficher les résultats de l'instruction de débogage, retournez au Modifier le déclencheur volet, cliquez **Modifier le script de déclenchement**, puis cliquez **Journal de débogage**. La sortie inclut l'adresse IP du serveur NTP, le code de requête monlist et le code d'erreur, comme dans le résultat suivant :

```
NTP Server 198.51.100.0 responded to mode 7 command 42 with error code 0.
```

Si les résultats du déclencheur indiquent que votre serveur NTP a répondu à une commande monlist, vous pouvez effectuer l'une des actions suivantes :

- Mettez à niveau votre serveur NTP vers la version 4.2.7 ou ultérieure, qui interdit les commandes monlist par défaut. Les téléchargements sont disponibles sur le Téléchargements de logiciels NTP page sur www.ntp.org.
- Modifiez le `ntp.conf` fichier sur le serveur NTP pour désactiver la fonction de surveillance qui autorise les commandes monlist. Les instructions sont disponibles sur le Restrictions d'accès page sur www.ntp.org.
- Si votre flux de travail de sécurité et de surveillance nécessite que votre serveur NTP réponde aux commandes monlist, vous pouvez utiliser ce déclencheur pour renforcer les contrôles relatifs aux réponses NTP. Par exemple, vous pouvez créer des métriques personnalisées basées sur les informations extraites à l'aide du déclencheur. Grâce à ces indicateurs personnalisés, vous pouvez créer un tableau de bord pour suivre l' activité du serveur NTP ou configurer un alerte qui vous informe des réponses aux commandes monlist.

Si votre serveur NTP est déjà configuré pour interdire les commandes monlist, vous ne recevrez aucun message syslog ni aucun résultat dans le journal de débogage. Vous pouvez toujours vérifier que le déclencheur exécute l'une des actions suivantes :

- Retournez au Modifier le déclencheur volet et visualisez le Capturer la charge du déclencheur graphique. Le graphique montre l'activité tant qu'il y a du trafic UDP sur le serveur NTP.
- Consultez le Le déclencheur s'exécute et s'arrête graphique sur le tableau de bord de l'état du système. Le graphique montre l'activité indiquant que le déclencheur est en cours d'exécution.
- Testez les commandes monlist du côté client. Modifiez le déclencheur en réglant le `buf` variable à `Flow.client.payload`, puis envoyez une commande monlist via un programme tel que `ntpdc` au serveur NTP. Ce changement de code associé à la commande monlist extrait la charge utile de la demande et le déclencheur envoie un message à Syslog et affiche les résultats dans le journal de sortie.

En exécutant ce déclencheur, vous découvrez si vos serveurs NTP sont vulnérables aux attaques par amplification et ce que vous pouvez faire pour surveiller les attaques ou désactiver les commandes NTP qui ouvrent la porte aux attaques.