ExtraHop

Erstellen Sie einen Auslöser, um Antworten auf NTP-Monlist-Anfragen zu überwachen

Veröffentlicht: 2024-09-26

Maschinen in Ihrer Umgebung synchronisieren Uhren über das Network Time Protocol (NTP), aber NTP weist einige Sicherheitslücken auf, z. B. Amplification-Angriffe, die zu Denial-of-Service führen.

Ein Angreifer kann beispielsweise die IP-Adresse Ihres NTP-Servers fälschen und dann wiederholt einen monlist-Befehl über die gefälschte Adresse senden. Der Befehl monlist fordert eine Liste der letzten 600 Hosts an, die eine Verbindung zum NTP-Server hergestellt haben. Da die anfordernde IP-Adresse jedoch gefälscht ist, sendet der Server die Liste tatsächlich an die gefälschte Adresse. Die Antwort ist erheblich größer als die Anfrage, und der gefälschte Client wird überlastet, was dazu führen kann, dass legitime Anfragen abgelehnt werden.

In dieser exemplarischen Vorgehensweise schreiben Sie einen Auslöser, der den UDP-Verkehr auf Ihrem NTP-Server auf Antworten auf Monlist-Befehle überprüft. Der Auslöser sendet auch eine Meldung auf Warnstufe an einen Remote-Syslog-Server, wenn eine Monlist-Antwort auftritt.

Voraussetzungen

- Sie benötigen Zugriff auf ein ExtraHop-System mit einem Benutzerkonto, das über System- und Zugriffsadministrationsrechte verfügt.
- Sie müssen mindestens einen NTP-Server haben, den Sie überwachen möchten.
- Sie benötigen einen Remote-Syslog-Server, der Daten vom ExtraHop-System empfangen kann.
- Sie müssen vertraut sein mit Javascript.
- Machen Sie sich mit den Konzepten in dieser Komplettlösung vertraut, indem Sie die Offene Datenströme Abschnitt in der ExtraHop Admin-UI-Leitfaden und der Erste Schritte mit Triggern Abschnitt in der ExtraHop System-Benutzerhandbuch.
- Machen Sie sich mit den Prozessen der Erstellung von Triggern und der Konfiguration offener Datenströme vertraut, indem Sie die Komplettlösung für Trigger und der ODS-Komplettlösung.

Einen offenen Datenstrom für ein Syslog-Ziel konfigurieren

In den folgenden Schritten konfigurieren Sie den Host, den Port und das Protokoll für das offene Datenstromziel.

1. Melden Sie sich bei dem ExtraHop-System, von dem Sie Daten senden möchten, mit einem Konto an , das über System- und Zugriffsadministrationsrechte verfügt.
2. Klicken Sie auf das Symbol Systemeinstellungen, und klicken Sie dann auf **Die gesamte Verwaltung**.
3. Klicken Sie im Abschnitt Systemkonfiguration auf **Offene Datenströme**.
4. klicken **Ziel hinzufügen**.
5. Wählen **Syslog** aus dem Typ des Ziels Drop-down-Liste.
6. In der Name Feld, Typ `NTP-Syslog` es sei denn, dies ist das erste Syslog-Ziel, das Sie erstellt haben. In diesem Fall erhält das Ziel automatisch den Namen „Standard“ und kann nicht umbenannt werden.
7. In der Gastgeber Feld, geben Sie die IP-Adresse oder den Hostnamen des Syslog-Servers ein, an den Sie Daten senden möchten.
8. In der Hafen Feld, geben Sie die Portnummer ein, an die Sie Daten senden möchten.
9. Wählen Sie aus der Protokollliste **UDP**.

Hinweis: klicken **Testen** um eine Verbindung herzustellen und eine Testnachricht vom ExtraHop-System an den Remote-Syslog-Server zu senden.

10. Wählen **Lokal** wenn Sie Syslog-Informationen mit Zeitstempeln in der lokalen Zeitzone des ExtraHop-Systems senden möchten. Andernfalls werden Zeitstempel in GMT gesendet.
11. klicken **Speichern**.
    Das Ziel wird der Syslog-Tabelle auf der Seite Open Data Stream hinzugefügt.

Schreiben Sie einen Auslöser zum Analysieren von NTP-Payloads

In den folgenden Schritten schreiben Sie einen Auslöser, der angibt, welche Daten aus NTP-Serverantworten untersucht werden sollen und ob die Daten an einen Remote-Syslog-Server gesendet werden sollen.

1. Klicken Sie auf das ExtraHop-Logo in der oberen linken Ecke, um zum ExtraHop-System zurückzukehren.
2. Klicken Sie auf das Symbol Systemeinstellungen, und klicken Sie dann **Auslöser**.
3. klicken **Erstellen**.
4. In der Name Feld, Typ `UDP-Nutzlast für NTP-Antworten analysieren`.
5. klicken **Debug-Log aktivieren** um das Debug-Log zu aktivieren und Leistungsmetriken Auslöser.
6. In der Ereignisse Feld, wählen **UDP_PAYLOAD**.
7. klicken **Erweiterte Optionen anzeigen** und geben Sie die folgenden Payload-Einstellungen an, um nur auf UDP-Port 123 nach NTP-Verkehr zu suchen:
   a) Wählen **Auslöser für alle UDP-Pakete ausführen**.
   b) In der Server-Portbereich Hauptfeld, Typ `123`.
   c) In der Server-Portbereich Maximales Feld, Typ `123`.
8. Fügen Sie im rechten Bereich den folgenden Triggercode hinzu, um den Zugriff auf die NTP-Serverantwortpayload zu ermöglichen:

```
//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. Fügen Sie dem vorhandenen Skript den folgenden Triggercode hinzu, um anzugeben, welche Felder der Auslöser aus dem Header der Payload extrahiert und welche Felder ignoriert werden sollen:

```
//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. Fügen Sie dem vorhandenen Skript den folgenden Triggercode hinzu, um die Felder aus der Payload zu extrahieren:

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

11. Fügen Sie dem vorhandenen Skript den folgenden Triggercode hinzu, um die Werte der folgenden Header-Felder zu überprüfen:

```
// 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;
```

Der Modus, der sich in den letzten drei Bits des Feldes befindet, gibt den NTP-Betriebsmodus an. Ein Wert von 7 gibt an, dass der NTP-Server auf einen Befehl im privaten Modus reagiert, zu dem auch der Befehl monlist gehört.

Das Feld Anforderungscode gibt den Anforderungstyp an. Ein Wert von 20 oder 42 gibt eine Monlist-Anfrage an.

Das Fehlercodefeld, das sich in den letzten vier Bits befindet, gibt den Fehlertyp an. Ein Wert von 0 gibt an, dass die Antwort kein Fehler ist.

12. Fügen Sie dem vorhandenen Skript den folgenden Triggercode hinzu, um eine Meldung auf Warnstufe an den Remote-Syslog-Server zu senden, wenn der NTP-Server auf einen monlist-Befehl reagiert und die Antwort kein Fehler ist.

```
//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);
}
```

Der Auslöser sendet Nachrichten, die die IP-Adresse des NTP-Servers enthalten, an den Remote-Syslog-Server, den Sie zuvor konfiguriert haben. Wenn das von Ihnen konfigurierte Ziel automatisch benannt wurde, ersetzen Sie `'NTP Syslog'` mit `'default'` im Code.

13. Fügen Sie dem vorhandenen Skript den folgenden Triggercode hinzu, um zu überprüfen, ob das Debuggen aktiviert ist, und senden Sie die angegebene Ausgabe an das Debug-Log.

```
//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. klicken **Speichern**.

Weisen Sie den UPA-Trigger einem Gerät zu

Bevor der Auslöser UDP-Antwortnutzlasten untersuchen kann, müssen Sie den Auslöser mindestens einem Gerät zuweisen. In dieser exemplarischen Vorgehensweise weisen Sie den Auslöser NTP-Servern in Ihrem Netzwerk zu.

Wichtig: Weisen Sie Trigger nur den spezifischen Geräten zu, von denen Sie Messwerte sammeln müssen, um die Auswirkungen Ihrer Trigger auf die Leistung des ExtraHop-Systems zu minimieren.

1. klicken **Vermögenswerte** aus dem oberen Menü.
2. Klicken Sie im linken Bereich auf **Geräte**.

3. In der Name Spalte, suchen Sie mindestens einen NTP-Server und aktivieren Sie das Kontrollkästchen.
4. klicken **Trigger zuweisen** oben auf der Seite.
5. Klicken Sie auf das Kästchen neben dem **UDP-Nutzlast für NTP-Antworten analysieren** Auslöser und dann klicken **Trigger zuweisen**.

Nachdem der Auslöser zugewiesen wurde, wird er kontinuierlich ausgeführt, bis er deaktiviert wird.

Überprüfen Sie Ihren Syslog-Server und das Debug-Log auf Triggerergebnisse

Wenn der NTP-Server eine Antwort auf einen monlist-Befehl sendet, sendet der Auslöser eine Warnmeldung an Ihren Remote-Syslog-Server. Die Nachricht enthält die IP-Adresse des NTP-Servers, der die Antwort gesendet hat, ähnlich der folgenden Nachricht:

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

Darüber hinaus sendet der Auslöser eine Ausgabe an das Debug-Log, wenn das Debuggen aktiviert ist. Um die Ergebnisse der Debug-Anweisung zu sehen, kehren Sie zurück zu Trigger bearbeiten Fenster, klicken **Trigger-Skript bearbeiten**, und klicken Sie **Debug-Protokoll**. Die Ausgabe enthält die IP-Adresse des NTP-Servers, den Monlist-Anforderungscode und den Fehlercode, ähnlich der folgenden Ausgabe:

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

Wenn die Triggerergebnisse darauf hindeuten, dass Ihr NTP-Server auf einen monlist-Befehl reagiert hat, können Sie eine der folgenden Aktionen ausführen:

- Aktualisieren Sie Ihren NTP-Server auf Version 4.2.7 oder höher, die monlist-Befehle standardmäßig nicht zulässt. Downloads sind erhältlich von NTP-Softwaredownloads Seite bei www.ntp.org.
- Ändern Sie die `ntp.conf` Datei auf dem NTP-Server, um die Überwachungsfunktion zu deaktivieren, die Monlist-Befehle zulässt. Anweisungen finden Sie auf der Zugangsbeschränkungen Seite bei www.ntp.org.
- Wenn Ihr Sicherheits- und Überwachungsworkflow erfordert, dass Ihr NTP-Server auf Monlist-Befehle reagiert, können Sie diesen Auslöser nutzen, um die Kontrollen rund um NTP-Antworten zu verschärfen. Sie können beispielsweise benutzerdefinierte Metriken auf der Grundlage von Informationen erstellen, die mit dem Auslöser extrahiert wurden. Mit diesen benutzerdefinierten Metriken können Sie ein Dashboard erstellen um die NTP-Serveraktivität zu verfolgen oder eine zu konfigurieren Alarm das benachrichtigt Sie über Antworten auf Monlist-Befehle.

Wenn Ihr NTP-Server bereits so konfiguriert ist, dass er Monlist-Befehle nicht zulässt, erhalten Sie keine Syslog-Meldungen und sehen auch keine Ausgabe im Debug-Log. Sie können immer noch überprüfen, ob der Auslöser eine der folgenden Aktionen ausführt:

- Kehren Sie zurück zum Trigger bearbeiten Fenster und Ansicht der Triggerlast erfassen Diagramm. Das Diagramm zeigt die Aktivität, solange UDP-Verkehr auf dem NTP-Server besteht.
- Sehen Sie sich das an Trigger wird ausgeführt und gelöscht Diagramm auf dem Systemintegritäts-Dashboard. Das Diagramm zeigt Aktivitäten, die darauf hinweisen, dass der Auslöser ausgeführt wird.
- Testen Sie auf der Client-Seite auf Monlist-Befehle. Ändern Sie den Auslöser, indem Sie den `buf` variabel zu `Flow.client.payload`, und senden Sie dann einen monlist-Befehl über ein Programm wie `ntpdc` zum NTP-Server. Diese Codeänderung in Verbindung mit dem Befehl monlist extrahiert die Nutzdaten der Anfrage und der Auslöser sendet eine Nachricht an Syslog und zeigt die Ergebnisse im Ausgabelog an.

Wenn Sie diesen Auslöser ausführen, erfahren Sie, ob Ihre NTP-Server anfällig für Amplification-Angriffe sind und was Sie tun können, um entweder Angriffe zu überwachen oder die NTP-Befehle zu deaktivieren, die Angriffen Tür und Tor öffnen .