Identify Kerberos brute force attacks with the Active Directory bundle

Published: 2018-04-18

In a brute force attack, an attacker gains access to your system simply by repeatedly logging in with a variety of passwords until they guess the correct one. The ExtraHop Active Directory bundle can help you discover when these attacks are happening and where they are coming from.

In this walkthrough, you will learn how to download, install, and configure the Active Directory bundle, and then identify potential Kerberos brute force attacks with the Active Directory dashboard.

Prerequisites

- Familiarize yourself with the concepts in this walkthrough by reading the Bundles concepts topic.
- You must have access to an ExtraHop Discover appliance with a user account that has full write privileges.
- You must be familiar with modifying triggers. For more information, see the Triggers concepts topic.

Download the ExtraHop Active Directory Bundle

Before you can upload the Active Directory Bundle to your appliance, you must download the bundle from the ExtraHop website.

1. Download the Active Directory bundle.

   Note: This walkthrough is based on the Active Directory v4 bundle.

2. If you have not already logged into the ExtraHop website, click **Login** in the right pane and then specify a valid username and password.
3. Click **Download Now**.
4. Save the .json file to a location on your local machine.

Upload and apply the Active Directory Bundle to your ExtraHop appliance

After you have downloaded the Active Directory Bundle, you can upload and install the bundle on your appliance.

1. Log into the Web UI of a Discover appliance.
2. Click the System Settings icon in the upper right corner.
3. Click **Bundles**.
4. On the Bundles page, click **Upload**.
5. In the Load Bundle dialog box, click the Choose File button, and then select the Active Directory Bundle file you downloaded from the ExtraHop Solution Bundle Gallery.
6. Click **Upload**.
7. Select the **Apply 9 included assignments** checkbox.
8. From the Existing objects drop-down menu, select **Overwrite**.

   Selecting this option will overwrite any objects that have the same name as objects in the bundle.
9. Click **Apply**.
10. In the Bundle Import Status dialog box, click **OK**.

11. In the View Bundle window, click **OK**.

Configure the Active Directory triggers

In the following steps, you will enable and configure a trigger to mirror the lockout and privileged account settings in your Active Directory environment.

1. Click the System Settings icon .
2. Click **Triggers**.
3. Enable each trigger in the Active Directory v4 bundle by completing the following steps.
   a) In the table, click a trigger name beginning with **AD**.
   b) Clear the **Disable Trigger** checkbox to enable the trigger.
   c) Click **Save and Close**.
4. Modify specific fields in the Kerberos trigger to match your Active Directory accounts by completing the following steps.
   a) In the table, click **AD: Kerberos** and then click the **Editor** tab.
   b) Set the `failedLoginDisableInterval` constant to the match the value of the `Reset account lockout counter after` policy setting in your Active Directory environment.
   c) Set the `accountLockoutDuration` constant to the value of the `Account lockout duration` policy setting in your Active Directory environment.
   d) Add the complete names of any privileged accounts in your environment to the `priv_names` list and any partial matches to the `priv_regex` list.

      The following example shows some common privileged accounts.

      ```
      var priv_names = {‘admin’, ‘administrator’, ‘root’, ‘ss’, ‘sys’,
              ‘sysadmin, ‘informix’}
      ```

   e) Click **Save and Close**.

Configure Active Directory alerts

The Active Directory Bundle includes alerts that you can configure to email you when high processing and response times are detected. You can also be alerted when a privileged account accesses resources for the first time, or if someone attempts to log into a privileged account too many times with an invalid password.

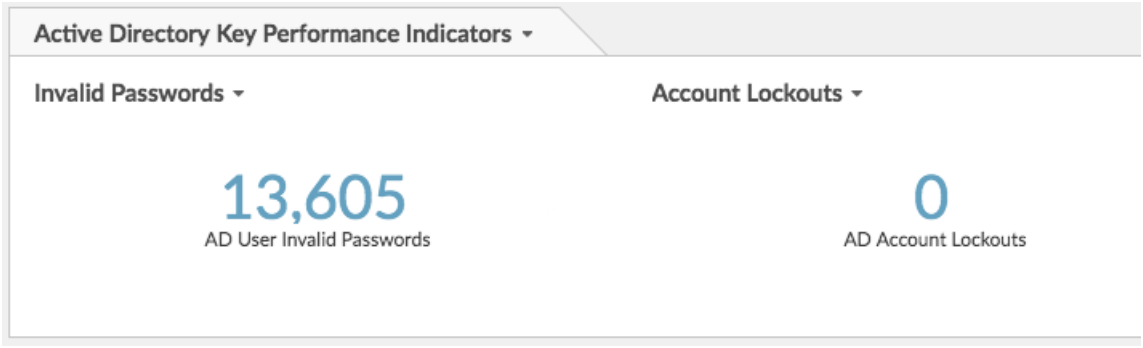
1. Click the System Settings icon .
2. Click **Alerts**.
3. Enable each alert and configure the alert to send notifications to your email address.

   Repeat these steps for each of the five ransomware alerts.
   a) Click **Active Directory <alert>**.
   b) Deselect the **Disable Alert** checkbox.
   c) Click **Notifications**.
   d) In the Additional email addresses field, type your email address.
   e) Click **OK**.

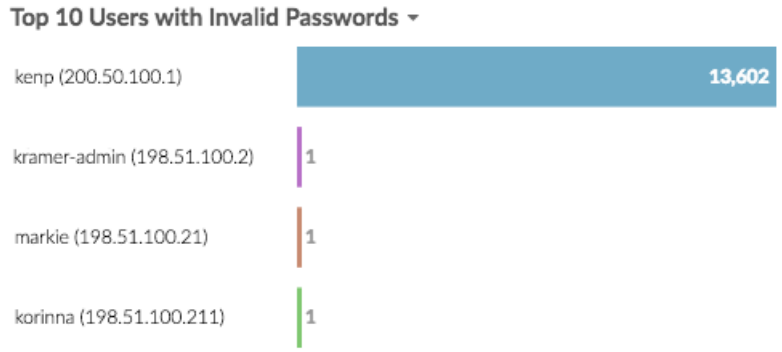
Identify Kerberos brute force attack

This example shows how you can detect Kerberos brute force attacks with the Active Directory bundle.

The Active Directory dashboard shows you how many times a user has attempted to log into a Kerberos system with an invalid password. In the example below, the bundle detected 13,605 unsuccessful log in attempts.

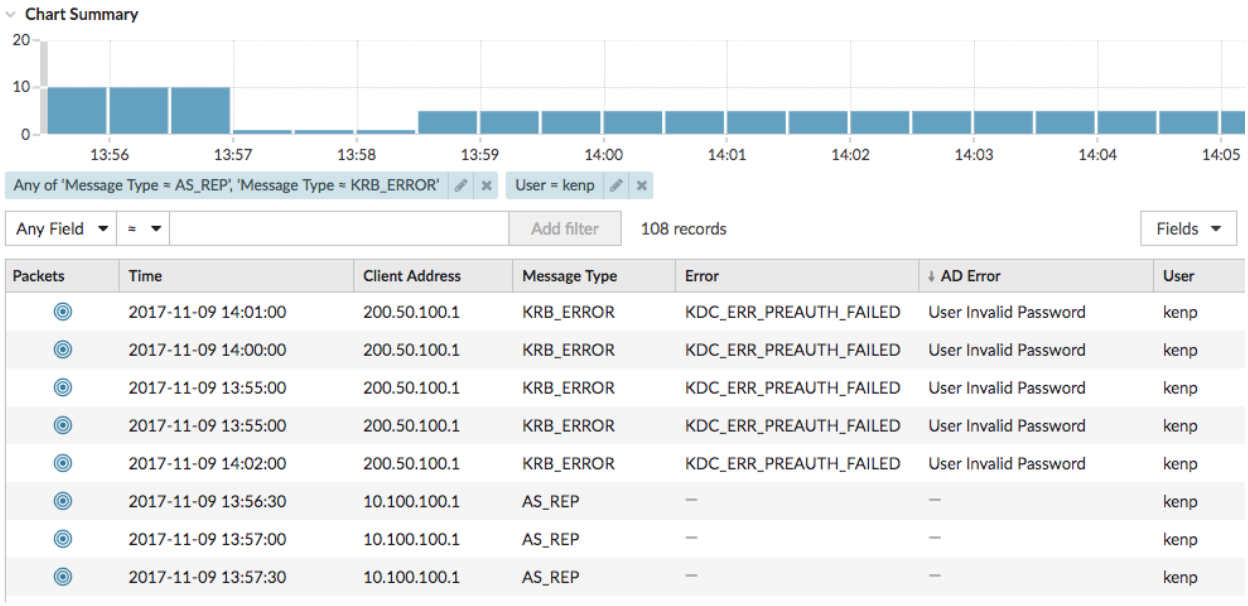


The Top 10 Users with Invalid Passwords chart then shows you which user accounts people are attempting to log into. User names are listed next to the IP address of the machine they attempted to log in from. In the following example, a machine with an IP address of 200.50.100.1 attempted to log into the kenp account 13,602 times:



It is highly unlikely that the legitimate owner of the kenp account attempted to log in thirteen thousand times without contacting an administrator. High levels of invalid logins like this are usually the result of a brute-force attack. The attacker is trying every possible password in an attempt to discover the correct one. With an ExtraHop Explore appliance, we can gain even more insight into the attack. To do this, we type the IP address of the machine into the top search bar, and then click **Search Records for 200.50.100.1**.

The records table shows all transactions related to the specified IP address. Clicking **Kerberos Response AD** in the left pane limits the results to Kerberos transactions only. Sorting the table by AD Error shows us all invalid password requests, including which machines specified those invalid passwords. The table shows that although the invalid password attempts all came from 200.50.100.1, there are a number of successful requests coming from 10.100.100.1:



These results suggest that 10.100.100.1 belongs to the actual user, and 200.50.100.1 belongs to the attacker. We can now block logins from 200.50.100.1 and contact the owners of both machines to confirm.

Next steps

Now that the Active Directory bundle is up and running, you can check out the other charts in the Active Directory dashboard to monitor potential access and authentication issues.