Identify Kerberos brute force attacks with the Active Directory dashboard

Published: 2024-08-07

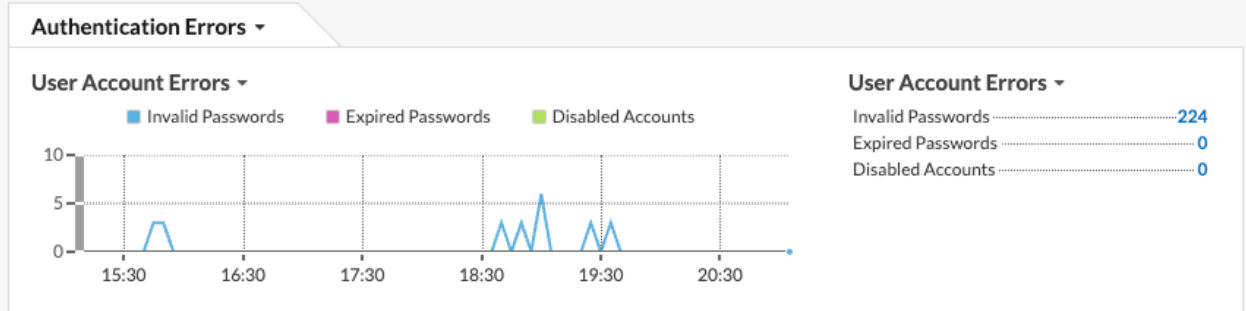
In a brute force attack, an attacker gains access to your system simply by repeatedly logging in with a variety of passwords until they guess the correct one. The ExtraHop Active Directory dashboard can help you discover when these attacks are happening and where they are coming from.

In this walkthrough, you will learn how to identify potential Kerberos brute force attacks with the Active Directory dashboard.

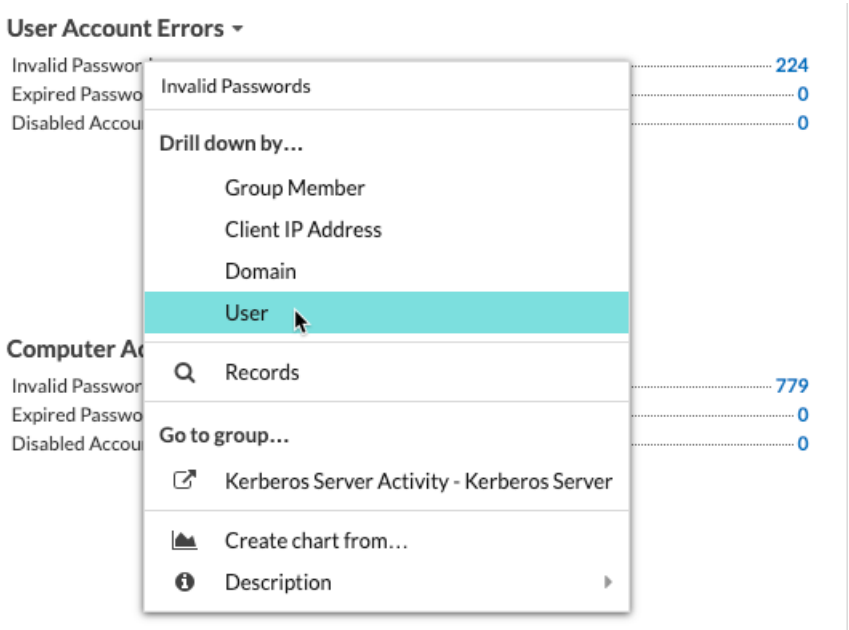
Identify Kerberos brute force attack

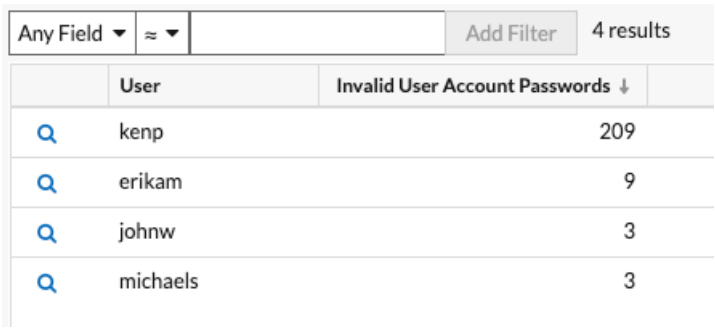
This example shows how you can detect Kerberos brute force attacks with the Active Directory dashboard.

The Active Directory dashboard shows you how many times a user has attempted to log in to a Kerberos system with an invalid password. In the example below, the dashboard shows 224 unsuccessful log in attempts.



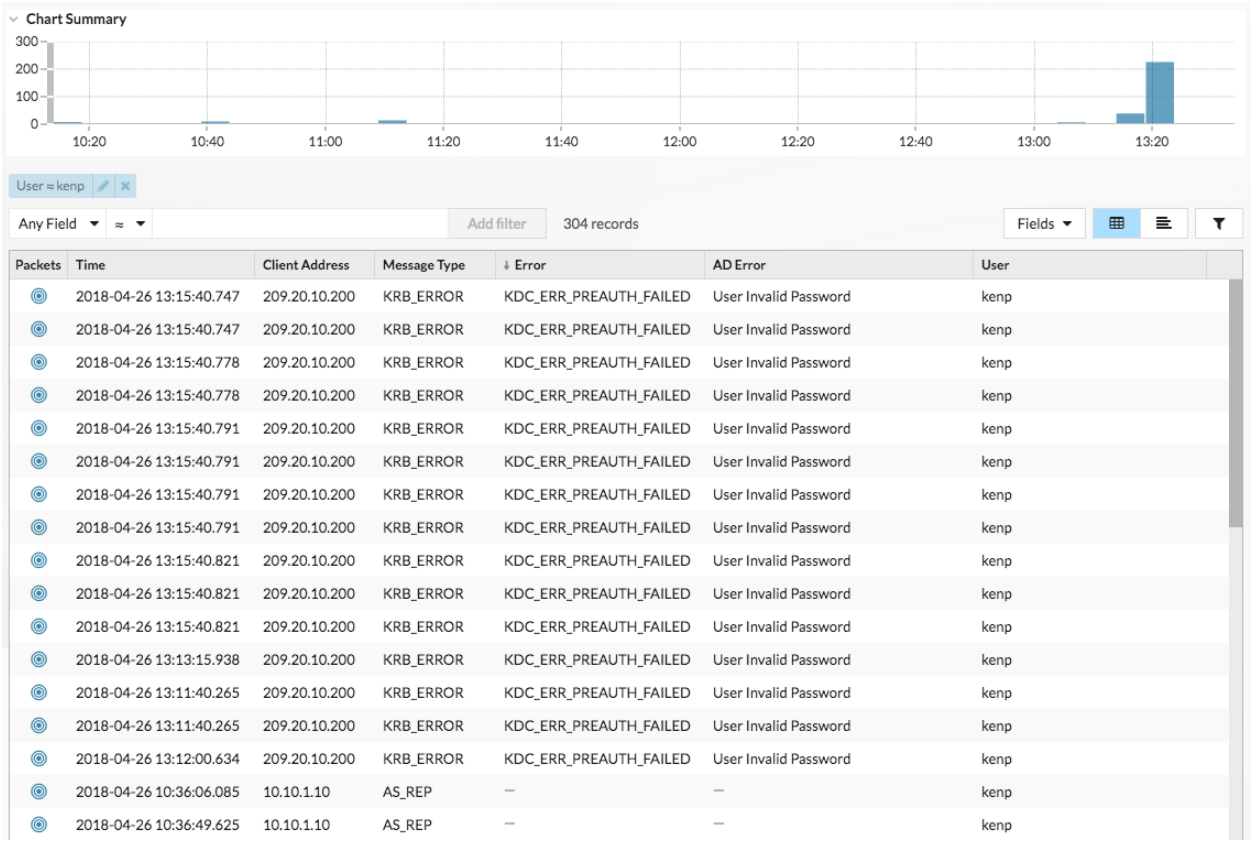
Drilling down on the Invalid Passwords metric by user then shows you which user accounts people are attempting to log in to.





In the example above, someone attempted to log in with the kenp account 209 times. It is highly unlikely that the legitimate owner of the kenp account attempted to log in over 200 times without contacting an administrator. High levels of invalid logins such as these are usually the result of a brute-force attack. The attacker is trying every possible password in an attempt to discover the correct one.

If your ExtraHop system has a recordstore, you can gain even more insight into the attack. From the top navigation, click **Records**. Clicking **Kerberos Response AD** in the left pane limits the results to Kerberos transactions only, and filtering the search by `User = kenp` limits the results to interactions with the kenp user.



The table shows that although the invalid password attempts all came from 209.20.10.200, there are a number of successful requests coming from 10.10.1.10. These results suggest that 10.10.1.10 belongs to the actual user, and 209.20.10.200 belongs to the attacker. We can now block logins from 209.20.10.200 and contact the owners of both machines to confirm.

Next steps

You can check out the other charts in the Active Directory dashboard and to monitor potential access and authentication issues.