Identifizieren Sie Kerberos-Brute-Force-Angriffe mit dem Active Directory Directory-Dashboard

Veröffentlicht: 2024-02-16

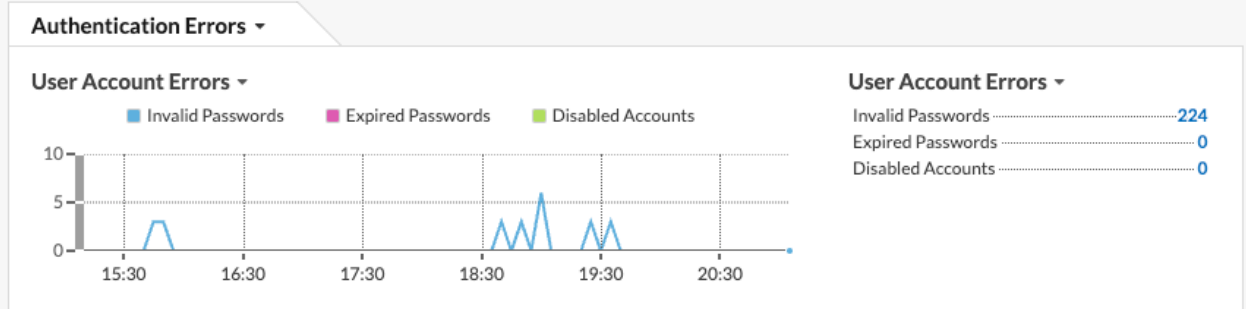
Bei einem Brute-Force-Angriff verschafft sich ein Angreifer Zugriff auf Ihr System, indem er sich einfach wiederholt mit einer Vielzahl von Passwörtern anmeldet, bis er das richtige errät. Mithilfe des Active Directory-Dashboards von ExtraHop können Sie herausfinden, wann diese Angriffe stattfinden und woher sie kommen.

In dieser exemplarischen Vorgehensweise erfahren Sie, wie Sie potenzielle Kerberos-Brute-Force-Angriffe mit dem Active Directory Directory-Dashboard identifizieren können.

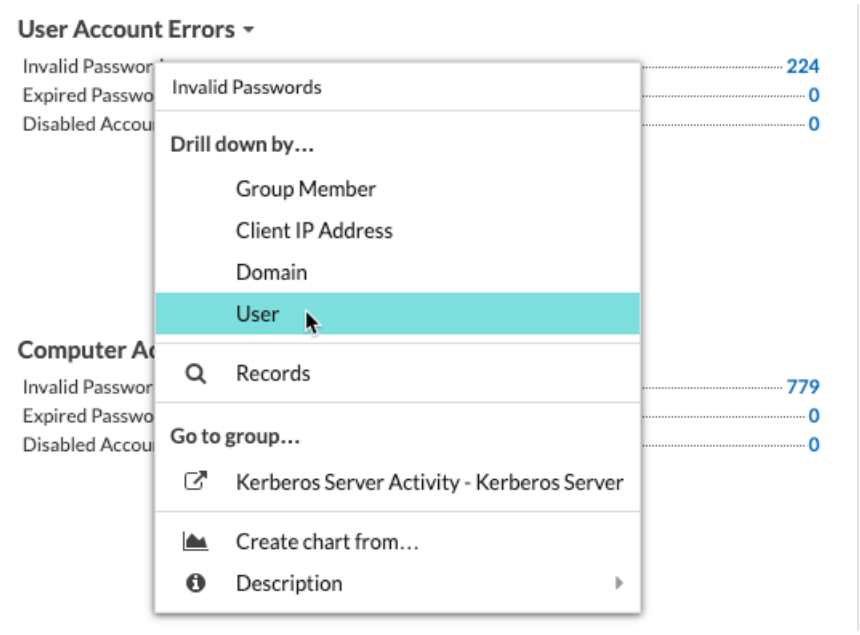
Identifizieren Sie einen Kerberos-Brute-Force-Angriff

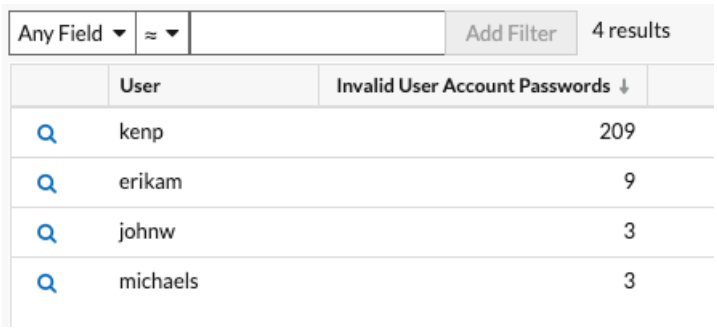
Dieses Beispiel zeigt, wie Sie Kerberos-Brute-Force-Angriffe mit dem Active Directory-Dashboard erkennen können.

Das Active Directory Directory-Dashboard zeigt Ihnen, wie oft ein Benutzer versucht hat, sich mit einem ungültigen Passwort bei einem Kerberos-System anzumelden. Im Beispiel unten zeigt das Dashboard 224 erfolglose Anmeldeversuche.



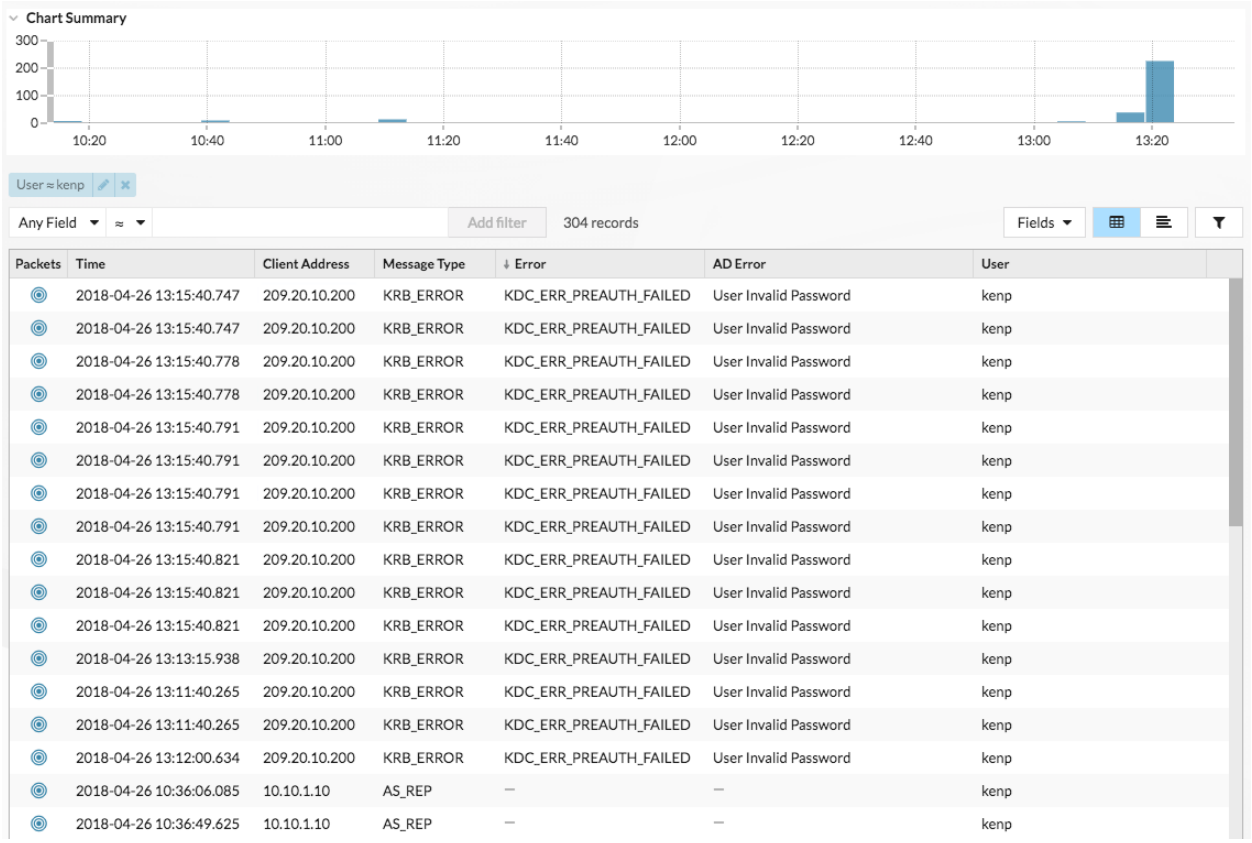
Wenn Sie die Metrik Ungültige Passwörter nach Benutzern aufschlüsseln, wird Ihnen dann angezeigt, mit welchen Benutzerkonten die Benutzer versuchen, sich anzumelden.





Im obigen Beispiel hat jemand 209 Mal versucht, sich mit dem kenp-Konto anzumelden. Es ist sehr unwahrscheinlich, dass der rechtmäßige Besitzer des kenp-Kontos über 200 Mal versucht hat, sich anzumelden, ohne einen Administrator zu kontaktieren. Eine hohe Anzahl ungültiger Logins wie diese ist normalerweise das Ergebnis eines Brute-Force-Angriffs. Der Angreifer versucht jedes mögliche Passwort, um das richtige zu finden.

Wenn Ihr ExtraHop-System über einen Recordstore verfügt, können Sie noch mehr Einblick in den Angriff gewinnen. Klicken Sie in der oberen Navigationsleiste auf **Rekorde**. Klicken **Kerberos-Antwort AD** im linken Bereich beschränkt die Ergebnisse nur auf Kerberos-Transaktionen und filtert die Suche nach `User = kenp` beschränkt die Ergebnisse auf Interaktionen mit dem Kenp-Benutzer.



Packets	Time	Client Address	Message Type	↓ Error	AD Error	User
	2018-04-26 13:15:40.747	209.20.10.200	KRB_ERROR	KDC_ERR_PREAUTH_FAILED	User Invalid Password	kenp
	2018-04-26 13:15:40.747	209.20.10.200	KRB_ERROR	KDC_ERR_PREAUTH_FAILED	User Invalid Password	kenp
	2018-04-26 13:15:40.778	209.20.10.200	KRB_ERROR	KDC_ERR_PREAUTH_FAILED	User Invalid Password	kenp
	2018-04-26 13:15:40.778	209.20.10.200	KRB_ERROR	KDC_ERR_PREAUTH_FAILED	User Invalid Password	kenp
	2018-04-26 13:15:40.791	209.20.10.200	KRB_ERROR	KDC_ERR_PREAUTH_FAILED	User Invalid Password	kenp
	2018-04-26 13:15:40.791	209.20.10.200	KRB_ERROR	KDC_ERR_PREAUTH_FAILED	User Invalid Password	kenp
	2018-04-26 13:15:40.791	209.20.10.200	KRB_ERROR	KDC_ERR_PREAUTH_FAILED	User Invalid Password	kenp
	2018-04-26 13:15:40.791	209.20.10.200	KRB_ERROR	KDC_ERR_PREAUTH_FAILED	User Invalid Password	kenp
	2018-04-26 13:15:40.821	209.20.10.200	KRB_ERROR	KDC_ERR_PREAUTH_FAILED	User Invalid Password	kenp
	2018-04-26 13:15:40.821	209.20.10.200	KRB_ERROR	KDC_ERR_PREAUTH_FAILED	User Invalid Password	kenp
	2018-04-26 13:15:40.821	209.20.10.200	KRB_ERROR	KDC_ERR_PREAUTH_FAILED	User Invalid Password	kenp
	2018-04-26 13:13:15.938	209.20.10.200	KRB_ERROR	KDC_ERR_PREAUTH_FAILED	User Invalid Password	kenp
	2018-04-26 13:11:40.265	209.20.10.200	KRB_ERROR	KDC_ERR_PREAUTH_FAILED	User Invalid Password	kenp
	2018-04-26 13:11:40.265	209.20.10.200	KRB_ERROR	KDC_ERR_PREAUTH_FAILED	User Invalid Password	kenp
	2018-04-26 13:12:00.634	209.20.10.200	KRB_ERROR	KDC_ERR_PREAUTH_FAILED	User Invalid Password	kenp
	2018-04-26 10:36:06.085	10.10.1.10	AS_REP	–	–	kenp
	2018-04-26 10:36:49.625	10.10.1.10	AS_REP	–	–	kenp

Die Tabelle zeigt, dass die ungültigen Kennwortversuche zwar alle von 209.20.10.200 stammen, es jedoch eine Reihe erfolgreicher Anfragen von 10.10.1.10 gibt. Diese Ergebnisse deuten darauf hin , dass 10.10.1.10 dem tatsächlichen Benutzer und 209.20.10.200 dem Angreifer gehört. Wir können jetzt Anmeldungen ab 209.20.10.200 blockieren und die Besitzer beider Maschinen kontaktieren, um dies zu bestätigen.

Nächste Schritte

Sie können sich die anderen Diagramme im Active Directory Directory-Dashboard ansehen und potenzielle Zugriffs- und Authentifizierungsprobleme überwachen.