Identifiez les attaques par force brute de Kerberos à l'aide du tableau de bord Active Directory

Publié: 2024-02-16

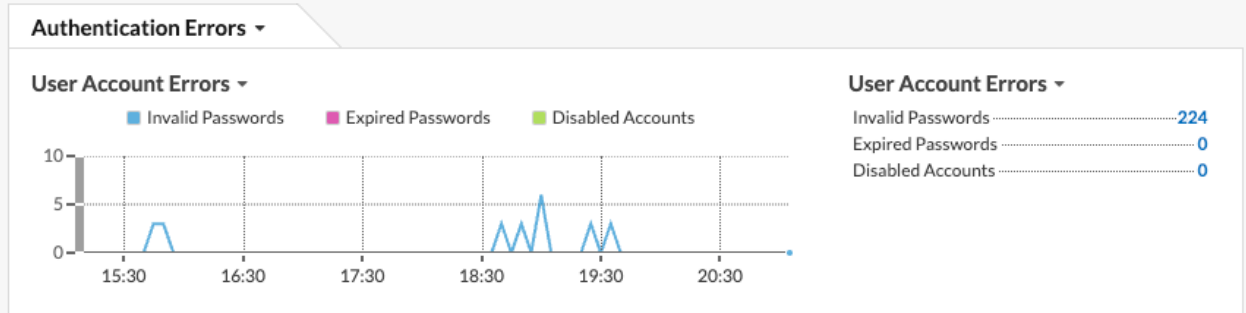
Lors d'une attaque par force brute, un attaquant accède à votre système simplement en se connectant à plusieurs reprises avec différents mots de passe jusqu'à ce qu'il devine le bon. Le tableau de bord ExtraHop Active Directory peut vous aider à découvrir quand ces attaques se produisent et d'où elles viennent.

Dans cette présentation, vous allez apprendre à identifier les attaques potentielles par force brute de Kerberos à l'aide du tableau de bord Active Directory.

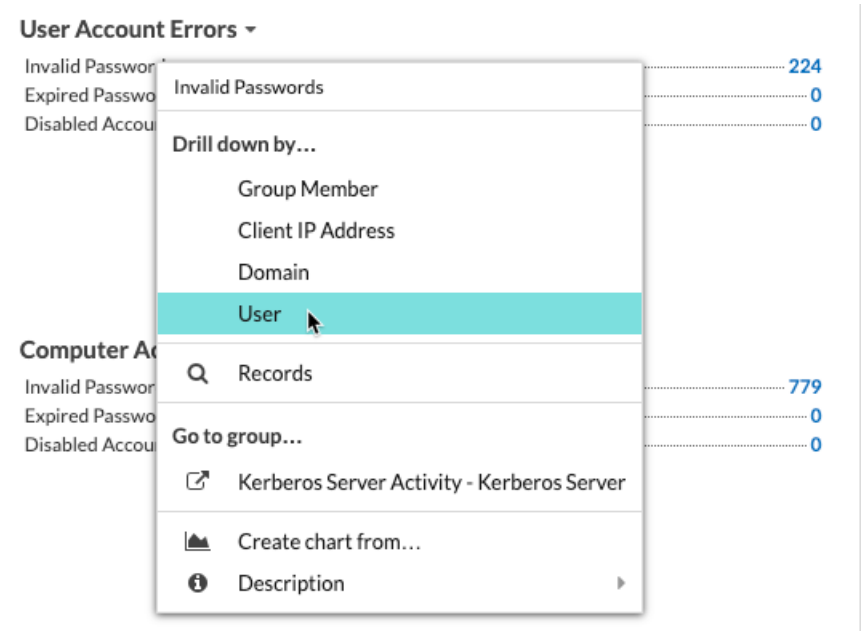
Identifiez l'attaque par force brute de Kerberos

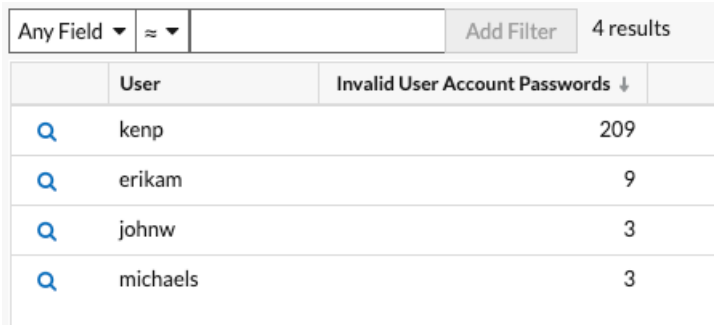
Cet exemple montre comment détecter les attaques par force brute de Kerberos à l'aide du tableau de bord Active Directory.

Le tableau de bord Active Directory indique combien de fois un utilisateur a tenté de se connecter à un système Kerberos avec un mot de passe non valide. Dans l'exemple ci-dessous, le tableau de bord indique 224 tentatives de connexion infructueuses.



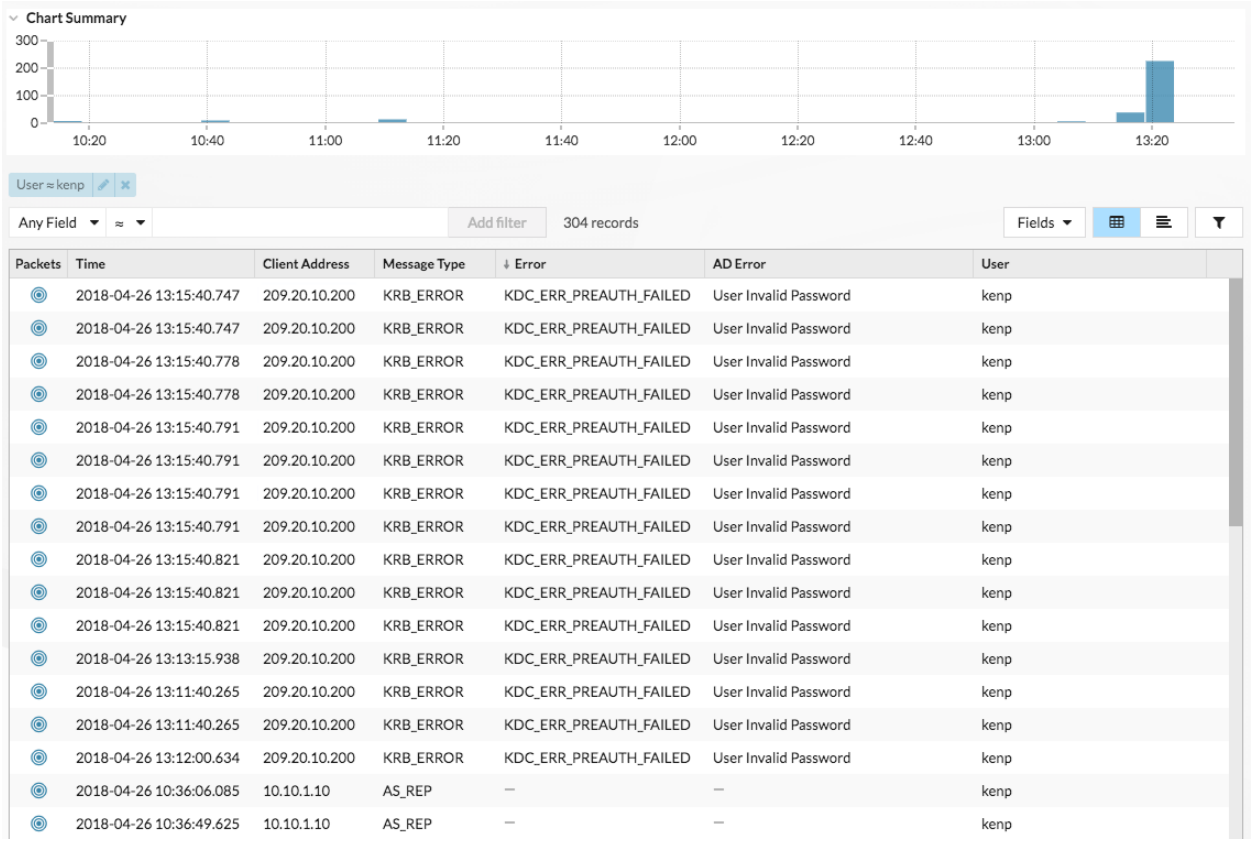
En analysant la métrique des mots de passe invalides par utilisateur, vous verrez ensuite à quels comptes utilisateurs les utilisateurs tentent de se connecter.





Dans l'exemple ci-dessus, quelqu'un a tenté de se connecter au compte kenp 209 fois. Il est très peu probable que le propriétaire légitime du compte kenp ait tenté de se connecter plus de 200 fois sans contacter un administrateur. Les niveaux élevés de connexions non valides de ce type sont généralement le résultat d'une attaque par force brute. L'attaquant essaie de trouver le bon mot de passe par tous les mots de passe possibles.

Si votre système ExtraHop possède un espace de stockage des enregistrements, vous pouvez mieux comprendre l'attaque. Dans le menu de navigation supérieur, cliquez sur **Enregistrements**. En cliquant **Kerberos Response AD** dans le volet de gauche limite les résultats aux transactions Kerberos uniquement et filtre la recherche par `User = kenp` limite les résultats aux interactions avec l'utilisateur kenp.



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

Le tableau montre que même si les tentatives de mot de passe non valides ont toutes été effectuées à partir du 209.20.10.200, un certain nombre de demandes ont été acceptées en provenance du 10.10.1.10. Ces résultats suggèrent que 10.10.1.10 appartient à l'utilisateur réel et que 209.20.10.200 appartient à l'attaquant. Nous pouvons désormais bloquer les connexions à partir du 209.20.10.200 et contacter les propriétaires des deux machines pour confirmer.

Prochaines étapes

Vous pouvez consulter les autres graphiques du tableau de bord Active Directory afin de surveiller les problèmes d'accès et d'authentification potentiels.