Comment employez-vous des expressions régulières (expression régulière) avec le grep pour rechercher des logs ?

Contenu

Question

Comment employez-vous des expressions régulières (expression régulière) avec le grep pour rechercher des logs ?

Environnement

Appliance de sécurité Web de Cisco
Appliance de sécurité du courrier électronique de Cisco
Appliance de Gestion de sécurité Cisco

Solution

Les expressions régulières (expression régulière) peuvent être un outil puissant une fois utilisées avec la commande de « grep » de rechercher par des logs disponibles sur l'appliance, telle qu'Access se connecte, des logs de proxy, et d'autres. Nous pouvons rechercher les logs basés sur le site Web, ou n'importe quelle partie de l'URL, ou de noms d'utilisateur, pour nommer quelques uns, en utilisant la commande « grep » CLI.

Sont ci-dessous quelques scénarios communs où vous pouvez employer l'expression régulière avec le grep pour assister le dépannage.

Scénario 1 : Trouver un site Web particulier dans les logs d'Access

Le scénario le plus commun tente de trouver des demandes étant faites à un site Web dans les logs d'accès de l'appliance de sécurité Web de Cisco (WSA).

Exemple :
Connectez à l'appliance par l'intermédiaire du SSH. Une fois que vous avez la demande, nous pouvons introduire la commande de « grep » de répertorier les logs disponibles.

Grep **CLI>**
Introduisez le nombre du log que vous souhaitez au « grep ». [] > 1 (choisissez # pour des logs d'accès ici)
Écrivez l'expression régulière au « grep ». [] > **site Web \ .com**

Scénario 2 : Tenter pour trouver une extension de fichier ou un domaine de haut niveau particulière

Nous pouvons utiliser la commande de « grep » de trouver une extension de fichier particulière (.doc, .pptx) dans un URL ou un domaine de haut niveau (.com, .org).

Exemple :
Pour trouver tout l'URLs qui nous finissent avec .crl pourrait utiliser l'expression régulière suivante : **\ .crl$**

Pour trouver tout l'URLs qui contiennent l'extension de fichier .pptx, nous pourrions utiliser l'expression régulière suivante : **\ .pptx**

Scénario 3 : Tenter pour trouver un bloc particulier pour un site Web

En recherchant un site Web particulier, nous pourrions également rechercher une réponse de HTTP particulière.

Exemple :
Si nous voulions rechercher tous les messages TCP_DENIED/403 pour domain.com, nous pourrions utiliser l'expression régulière suivante : **tcp_denied/403.*domain\.com**

Scénario 4 : Trouver un nom d'ordinateur dans les logs d'Access

En utilisant le modèle d'authentification NTLMSSP, nous pouvons trouver un exemple par hasard où un agent d'utilisateur (Microsoft NCSI est le plus commun) enverra inexactement des qualifications d'ordinateur au lieu des identifiants utilisateurs quand authentifiant. Pour dépister l'agent URL/User qui entraîne ceci, nous pouvons employer l'expression régulière avec le « grep » pour isoler le requête effectuée quand l'authentification s'est produite.

Si nous n'avons pas le nom d'ordinateur qui a été utilisé, nous pouvons utiliser le « grep » et trouver tous les noms d'ordinateur qui ont été utilisés comme noms d'utilisateur en authentifiant

utilisant l'expression régulière suivante : **\ $@**

Une fois que nous avons la ligne où ceci se produit, nous pouvons « grep » pour le nom d'ordinateur spécifique qui a été utilisé à l'aide de l'expression régulière suivante : **machinename \ $**

La première entrée qui est soulevée devrait être la demande qui a été faite quand l'utilisateur authentifié avec le nom d'ordinateur au lieu du nom d'utilisateur.

Scénario 5 : Trouver une période spécifique dans les logs d'Access

Par défaut, les abonnements de log d'accès n'incluront pas le champ qui affiche le date/heure lisible pour l'homme. Si nous voulons vérifier l'accès se connecte pendant un délai prévu particulier, nous peut suivre les étapes ci-dessous :

Consultation l'horodateur UNIX d'un site tel que http://www.onlineconversion.com/unix_time.htm. Une fois que vous avez l'horodateur, vous pouvez rechercher une heure précise dans les logs d'Access.

Exemple :
Un horodateur d'Unix de 1325419200 est équivalent à 01/01/2012 12:00:00.

Nous pouvons employer l'entrée suivante d'expression régulière pour rechercher les logs d'accès autour de la période de 12:00 le 1er janvier, 2012 : 13254192

Scénario 6 : Rechercher les messages essentiels ou d'avertissement

Nous pouvons rechercher les messages essentiels ou d'avertissement dans tous les logs disponibles, tels que des logs de proxy ou des logs système, utilisant des expressions régulières.

Exemple :
Pour rechercher les messages d'avertissement dans les logs de proxy, nous pouvons entrer dans l'expression régulière suivante :

1. Grep **CLI>**
2. Introduisez le nombre du log que vous souhaitez au « grep ».
   [] > 17 (choisissez # pour des logs de proxy ici)
3. Écrivez l'expression régulière au « grep ».
   [] > **avertissant**

D'autres liens utiles :

Expressions régulières - Guide utilisateur