Comment utilisez-vous les expressions régulières (regex) avec grep pour rechercher des journaux ?

Contenu

Question

Comment utilisez-vous les expressions régulières (regex) avec grep pour rechercher des journaux ?

Environnement

Appareil de sécurité Web Cisco
Appareil de sécurité de la messagerie Cisco
Appareil de gestion de la sécurité Cisco

Solution

Les expressions régulières (regex) peuvent être un outil puissant lorsqu'elles sont utilisées avec la commande « grep » pour effectuer une recherche dans les journaux disponibles sur l'appliance, tels que les journaux d'accès, les journaux de proxy et d'autres. Nous pouvons effectuer des recherches dans les journaux en fonction du site Web, ou de n'importe quelle partie de l'URL, ou des noms d'utilisateur, pour en nommer quelques-uns, en utilisant la commande CLI « grep ».

Vous trouverez ci-dessous quelques scénarios courants dans lesquels vous pouvez utiliser regex avec grep pour faciliter le dépannage.

Scénario 1 : Recherche d'un site Web particulier dans les journaux d'accès

Le scénario le plus courant consiste à tenter de trouver des demandes adressées à un site Web dans les journaux d'accès de l'appareil de sécurité Web Cisco (WSA).

Exemple :
Connectez-vous à l'appliance via SSH. Une fois que vous avez l'invite, nous pouvons taper la commande « grep » pour répertorier les journaux disponibles.

CLI> grep
Entrez le numéro du journal que vous souhaitez « grep ». []> 1 (Choisissez le nombre de journaux d'accès ici)
Entrez l'expression régulière « grep ». []> **site Web\.com**

Scénario 2 : Tentative de recherche d'une extension de fichier particulière ou d'un domaine de premier niveau

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

Exemple :
Pour trouver toutes les URL qui se terminent par .crl, nous pouvons utiliser le regex suivant : **\.crl$**

Pour rechercher toutes les URL qui contiennent l'extension de fichier .pptx, nous pouvons utiliser la commande regex suivante : **\.pptx**

Scénario 3 : Tentative de recherche d'un bloc particulier pour un site Web

Lors de la recherche d'un site Web particulier, nous pouvons également rechercher une réponse HTTP particulière.

Exemple :
Si nous voulions rechercher tous les messages TCP_DENIED/403 pour domain.com, nous pourrions utiliser le regex suivant : **tcp_deny/403.*domain\.com**

Scénario 4 : Recherche d'un nom d'ordinateur dans les journaux d'accès

Lors de l'utilisation du schéma d'authentification NTLMSSP, il se peut qu'un agent utilisateur (Microsoft NCSI est le plus courant) envoie des informations d'identification de machine incorrectement au lieu des informations d'identification d'utilisateur lors de l'authentification. Pour retrouver l'URL/l'agent utilisateur qui cause ceci, nous pouvons utiliser regex avec « grep » pour isoler la demande faite lors de l'authentification.

Si nous n'avons pas le nom de machine utilisé, nous pouvons utiliser « grep » et rechercher tous les noms de machine utilisés comme noms d'utilisateur lors de l'authentification à l'aide de la règle suivante : **\$@**

Une fois que nous avons la ligne où cela se produit, nous pouvons « grep » pour le nom de machine spécifique qui a été utilisé en utilisant le regex suivant : **nommachine\$**

La première entrée qui apparaît doit être la demande qui a été faite lorsque l'utilisateur s'est authentifié avec le nom de la machine au lieu du nom de l'utilisateur.

Scénario 5 : Recherche d'une période spécifique dans les journaux d'accès

Par défaut, les abonnements au journal d'accès n'incluent pas le champ qui indique la date/heure lisible par l'utilisateur. Si nous voulons vérifier les journaux d'accès pour une période donnée, nous pouvons suivre les étapes suivantes :

Recherchez l'horodatage UNIX à partir d'un site tel que http://www.onlineconversion.com/unix_time.htm. Une fois que vous avez l'horodatage, vous pouvez rechercher une heure spécifique dans les journaux d'accès.

Exemple :
Un horodatage Unix de 1325419200 équivaut à 01/01/2012 à 12:00:00.

Nous pouvons utiliser l'entrée regex suivante pour rechercher les journaux d'accès vers 12h00 le 1er janvier ^{2012} : 13254192

Scénario 6 : Recherche de messages critiques ou d'avertissement

Nous pouvons rechercher des messages critiques ou d'avertissement dans tous les journaux disponibles, tels que les journaux proxy ou les journaux système, à l'aide d'expressions régulières.

Exemple :
Pour rechercher des messages d'avertissement dans les journaux de proxy, nous pouvons entrer le regex suivant :

1. **CLI>** grep
2. Entrez le numéro du journal que vous souhaitez « grep ».
   []> 17 (Choisissez le # pour les journaux de proxy ici)
3. Entrez l'expression régulière « grep ».
   []> **avertissement**

Autres liens utiles :

Expressions régulières - Guide de l'utilisateur