¿Cómo se utilizan expresiones regulares (regex) con grep para buscar registros?

Contenido

[Pregunta](#)
[Entorno](#)
[Solución](#)
[Escenario 1: Búsqueda de un sitio web concreto en los registros de acceso](#)
[Escenario 2: Intento de encontrar una extensión de archivo determinada o un dominio de nivel superior](#)
[Escenario 3: Intento de encontrar un bloque determinado para un sitio web](#)
[Escenario 4: Búsqueda de un nombre de equipo en los registros de acceso](#)
[Escenario 5: Búsqueda de un Período de Tiempo Específico en los Registros de Acceso](#)
[Escenario 6: Búsqueda de mensajes críticos o de advertencia](#)

Pregunta

¿Cómo se utilizan expresiones regulares (regex) con grep para buscar registros?

Entorno

Dispositivo de seguridad web de Cisco
Dispositivo de seguridad Cisco Email Security
Dispositivo de administración de seguridad de Cisco

Solución

Las expresiones regulares (regex) pueden ser una potente herramienta cuando se utiliza con el comando "grep" para buscar en los registros disponibles en el dispositivo, como registros de acceso, registros de proxy y otros. Podemos buscar los registros en función del sitio web, o de cualquier parte de la URL, o nombres de usuario, por nombrar algunos, cuando se utiliza el comando CLI "grep".

A continuación se muestran algunos escenarios comunes en los que puede utilizar regex con grep para ayudar con la resolución de problemas.

Escenario 1: Búsqueda de un sitio web concreto en los registros de acceso

El escenario más común es intentar encontrar solicitudes que se realizan a un sitio web en los registros de acceso de Cisco Web Security Appliance (WSA).

Por ejemplo:
Conéctese al dispositivo mediante SSH. Una vez que tenga el mensaje, podemos escribir el comando "grep" para enumerar los registros disponibles.

CLI> grep
Introduzca el número del registro que desea "grep". []> 1 (Elija el nº para los registros de acceso aquí)
Introduzca la expresión regular en "grep". []> **sitio web\.com**

Escenario 2: Intento de encontrar una extensión de archivo determinada o un dominio de nivel superior

Podemos utilizar el comando "grep" para encontrar una extensión de archivo determinada (.doc, .pptx) en una dirección URL o un dominio de nivel superior (.com, .org).

Por ejemplo:
Para encontrar todas las URL que terminan con .crl, podríamos utilizar el siguiente regex: **\.crl$**

Para buscar todas las URL que contienen la extensión de archivo .pptx, podríamos utilizar el siguiente regex: **\.pptx**

Escenario 3: Intento de encontrar un bloque determinado para un sitio web

Cuando buscamos un sitio web determinado, es posible que también estemos buscando una respuesta HTTP determinada.

Por ejemplo:
Si queríamos buscar todos los mensajes TCP_DENIED/403 para domain.com, podríamos utilizar el siguiente regex: **tcp_denied/403.*domain\.com**

Escenario 4: Búsqueda de un nombre de equipo en los registros de acceso

Al utilizar el esquema de autenticación NTLMSSP, es posible que se encuentre una instancia en la que un agente de usuario (Microsoft NCSI es el más común) enviará incorrectamente las credenciales del equipo en lugar de las credenciales del usuario al autenticarse. Para rastrear la URL/User Agent que lo causa, podemos usar regex con "grep" para aislar la solicitud realizada cuando se produjo la autenticación.

Si no tenemos el nombre de la máquina que se utilizó, podemos usar "grep" y buscar todos los nombres de máquinas que se usaron como nombres de usuario al autenticar usando el siguiente regex: **\$@**

Una vez que tenemos la línea donde ocurre esto, podemos "grep" para el nombre específico de la máquina que se usó usando el siguiente regex: **nombre de máquina\$**

La primera entrada que aparece debe ser la solicitud que se realizó cuando el usuario se autenticó con el nombre del equipo en lugar del nombre de usuario.

Escenario 5: Búsqueda de un Período de Tiempo Específico en los Registros de Acceso

De forma predeterminada, las suscripciones a registros de acceso no incluirán el campo que muestra la fecha/hora legible por personas. Si queremos verificar los registros de acceso durante un período de tiempo determinado, podemos seguir los pasos siguientes:

Busque la marca de tiempo UNIX desde un sitio como http://www.onlineconversion.com/unix_time.htm. Una vez que tenga la marca de tiempo, puede buscar una hora específica en los registros de acceso.

Por ejemplo:
Una marca de tiempo Unix de 1325419200 es equivalente a 01/01/2012 12:00:00.

Podemos usar la siguiente entrada regex para buscar los registros de acceso alrededor de las 12:00 del 1 de enero ^{10} de 2012: 13254192

Escenario 6: Búsqueda de mensajes críticos o de advertencia

Podemos buscar mensajes críticos o de advertencia en cualquier registro disponible, como registros de proxy o registros del sistema, mediante expresiones regulares.

Por ejemplo:
Para buscar mensajes de advertencia en los registros de proxy, podemos introducir el siguiente regex:

1. **CLI>** grep
2. Introduzca el número del registro que desea "grep".
   []> 17 (Elija el nº para los registros de proxy aquí)
3. Introduzca la expresión regular en "grep".
   []> **advertencia**

Otros enlaces útiles:

Expresiones regulares - Guía del usuario