Contenido

Pregunta

¿Cómo usted utiliza las expresiones normales (regex) con el grep para buscar los registros?

Entorno

Dispositivo de seguridad de la red de Cisco
Dispositivo de seguridad del correo electrónico de Cisco
Dispositivo de la Administración del Cisco Security

Solución

Las expresiones normales (regex) pueden ser una herramienta potente cuando están utilizadas con el comando del “grep” de buscar a través de los registros disponibles en el dispositivo, tal como registros del acceso, registros del proxy, y otros. Podemos buscar los registros basados en el sitio web, o a cualquier parte del URL, o los Nombres de usuario, para nombrar algunos, al usar el comando CLI “grep”.

Abajo están algunos escenarios frecuentes donde usted puede utilizar el regex con el grep para ayudar con el troubleshooting.

Escenario 1: Encontrar un sitio web determinado en los registros del acceso

La mayoría del escenario frecuente está intentando encontrar las peticiones que son hechas a un sitio web en los registros del acceso del dispositivo de seguridad de la red de Cisco (WSA).

por ejemplo:
Conecte con el dispositivo vía SSH. Una vez que usted tiene el prompt, podemos teclear el comando del “grep” de enumerar los registros disponibles.

Grep **CLI>**
Ingrese el número del registro que usted desea al “grep”. []> 1 (elija # para los registros del acceso aquí)
Ingrese la expresión normal al “grep”. []> **sitio web \ .com**

Escenario 2: El intentar encontrar una extensión de archivo o un dominio del nivel superior determinada

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

por ejemplo:
Para encontrar todos los URL que nos terminan con .crl podría utilizar el regex siguiente: **\ .crl$**

Para encontrar todos los URL que contienen la extensión de archivo .pptx, podríamos utilizar el regex siguiente: **\ .pptx**

Escenario 3: El intentar encontrar un bloque determinado para un sitio web

Al buscar para un sitio web determinado, puede ser que también busquemos para un HTTP de respuesta determinado.

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

Escenario 4: Encontrar un nombre de la máquina en los registros del acceso

Al usar NTLMSSP el esquema de autenticación, podemos parecer un caso donde un agente de usuario (Microsoft NCSI es el más común) enviará incorrectamente las credenciales de la máquina en vez de los credenciales de usuario al autenticar. Para rastrear el agente URL/User que causa esto, podemos utilizar el regex con el “grep” para aislar la petición hecha cuando ocurrió la autenticación.

Si no tenemos el nombre de la máquina que fue utilizado, podemos utilizar el “grep” y encontrar todos los nombres de la máquina que fueron utilizados como Nombres de usuario al autenticar usando el regex siguiente: **\ $@**

Una vez que tenemos la línea donde ocurre ésta, podemos “grep” para el nombre de la máquina específico que fue utilizado usando el regex siguiente: **machinename \ $**

La primera entrada que sube debe ser la petición que fue hecha cuando el usuario autenticado con el nombre de la máquina en vez del Nombre de usuario.

Escenario 5: Encontrar un período específico en los registros del acceso

Por abandono, las suscripciones del registro del acceso no incluirán el campo que muestra la fecha/la hora legibles. Si queremos marcar los registros del acceso por un período de tiempo determinado, podemos seguir los pasos abajo:

Mire para arriba el grupo fecha/hora de UNIX de un sitio tal como http://www.onlineconversion.com/unix_time.htm. Una vez que usted tiene el grupo fecha/hora, usted puede buscar por un tiempo específico dentro de los registros del acceso.

por ejemplo:
Un grupo fecha/hora de Unix de 1325419200 es equivalente a 01/01/2012 12:00:00.

Podemos utilizar la entrada siguiente del regex para buscar los registros del acceso alrededor de la época de 12:00 el 1 de enero, 2012: 13254192

Escenario 6: Búsqueda para crítico o los mensajes de advertencia

Podemos buscar para crítico o los mensajes de advertencia en cualquier registro disponible, tal como registros del proxy o registros del sistema, usando las expresiones normales.

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

1. Grep **CLI>**
2. Ingrese el número del registro que usted desea al “grep”.
   []> 17 (elija # para los registros del proxy aquí)
3. Ingrese la expresión normal al “grep”.
   []> **advirtiendo**

Otros links útiles:

Expresiones normales - Guía del usuario