Grep ESA, S A, y WSA con Regex para buscar los registros

Contenido

Introducción

Este documento describe cómo utilizar las expresiones normales (regex) con el **comando grep** para buscar los registros.

Prerequisites

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dispositivo de seguridad de la red de Cisco (WSA)
- Dispositivo de seguridad del correo electrónico de Cisco (ESA)
- Dispositivo de la Administración del Cisco Security (S A)

Grep con Regex

Regex puede ser una herramienta potente cuando está utilizado con el **comando grep** de buscar a través de los registros disponibles en el dispositivo, tal como registros del acceso, registros del proxy, y otros. Usted puede buscar los registros basados en el sitio web, o a cualquier parte del URL, y los Nombres de usuario con el comando CLI del **grep**.

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

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

La mayoría del escenario frecuente es cuando usted intenta encontrar las peticiones que se hacen a un sitio web en los registros del acceso del WSA.

Aquí tiene un ejemplo:

Conecte con el dispositivo vía el Secure Shell (SSH). Una vez que usted tiene el prompt, ingrese el **comando grep** para enumerar los registros disponibles.

```
CLI> grep
```

Ingrese el número del registro que usted desea al **grep**.

```
[]> 1 (Choose the # for access logs here)
```

Ingrese la expresión normal al **grep**.

```
[]> website\.com
```

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

Usted puede utilizar el **comando grep** para encontrar una extensión de archivo determinada (.doc, .pptx) en un URL o un dominio del nivel superior (.com, .org).

Aquí tiene un ejemplo:

Para encontrar todos los URL que terminen con .crl, utilice este regex:

```
\.crl$
```

Para encontrar todos los URL que contengan la extensión de archivo .pptx, utilice este regex:

```
\.pptx
```

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

Cuando usted busca para un sitio web determinado, usted puede ser que también busque para un HTTP de respuesta determinado.

Aquí tiene un ejemplo:

Si usted quiere buscar para todos los mensajes TCP_DENIED/403 para domain.com, utilice este regex:

```
tcp_denied/403.*domain\.com
```

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

Cuando usted utiliza NTLMSSP el esquema de autenticación, usted puede ser que encuentre un caso donde un agente de usuario (Microsoft NCSI es el más común) envía incorrectamente las credenciales de la máquina en vez de los credenciales de usuario cuando autentica. Para rastrear el agente URL/User que causa este problema, utilice el regex con el **grep** para aislar la petición hecha cuando ocurrió la autenticación.

Si usted no tiene el nombre de la máquina que fue utilizado, utilice el **grep** y encuentre todos los nombres de la máquina que fueron utilizados como Nombres de usuario al autenticar con este regex:

```
\$@
```

Una vez que usted tiene la línea donde ocurre ésta, grep para el nombre de la máquina específico que fue utilizado con este regex:

```
machinename\$
```

La primera entrada que aparece 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: Encuentre un período específico en los registros del acceso

Por abandono, las suscripciones del registro del acceso no incluyen el campo que muestra la fecha/la hora legibles. Si usted quiere marcar los registros del acceso por un período de tiempo determinado, complete estos pasos:

1. Mire para arriba el grupo fecha/hora de UNIX de un sitio tal como conversión en línea.
2. Una vez que usted tiene el grupo fecha/hora, busque por un tiempo específico dentro de los registros del acceso.

Aquí tiene un ejemplo:

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

Usted puede utilizar esta entrada del regex para buscar los registros del acceso cerca de 12:00 el 1 de enero, 2012:

13254192

Escenario 6: Búsqueda para crítico o los mensajes de advertencia

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

Aquí tiene un ejemplo:

Para buscar para los mensajes de advertencia en los registros del proxy, ingrese este regex:

```
CLI> grep
```

Ingrese el número del registro que usted desea al **grep**.

```
[]> 17 (Choose the # for proxy logs here)
```

Ingrese la expresión normal al **grep**.

```
[]> warning
```