Packet Tracer: Generar archivos de registro desde varias fuentes

Objetivos

Parte 1: Utilizar syslog para capturar archivos de registro de varios dispositivos de red.

Parte 2: Observar los registros de acceso de usuarios AAA.

Parte 3: Observar información de NetFlow.

Aspectos Básicos / Situación

En esta actividad, utilizará Packet Tracer para ver datos de red generados por syslog, AAA y NetFlow.

Instrucciones

Parte 1: Ver entradas de registro con Syslog

Paso 1: Servidor Syslog

Syslog es un sistema de mensajería diseñado para admitir el registro remoto. Los clientes syslog envían entradas de registro a un servidor syslog. El servidor syslog concentra y almacena las entradas de registro. Packet Tracer admite operaciones básicas de syslog y se puede utilizar con fines de demostración. La red incluye un servidor syslog y clientes syslog. R1, R2, el Switch de núcleo y el Firewall son clientes syslog. Estos dispositivos están configurados para enviar sus entradas de registro al servidor syslog. El servidor syslog recoge las entradas de registro y permite que se las lea.

Las entradas de registro se categorizan en siete niveles de gravedad. Los niveles más bajos representan los eventos más graves. Los niveles son los siguientes: emergencias (0), alertas (1), crítico (2) errores (3), advertencias (4), notificaciones (5), informativo (6) y depuración (7). Los clientes syslog se pueden configurar para enviar entradas de registro a servidores syslog en función del nivel de gravedad.

a. Haga clic en el **Servidor Syslog** para abrir su ventana.

b. Seleccione la pestaña **Servicios** y, luego, **SYSLOG** en la lista de servicios que aparece a la izquierda.

c. Haga clic en **Activar** para activar el servicio de Syslog.

d. Las entradas de Syslog provenientes de clientes syslog aparecerán en la ventana de la derecha. En este momento no hay ninguna entrada.

e. Mantenga esta ventana abierta y visible y siga con el **Paso 2**.

Paso 2: Habilitar Syslog.

Los dispositivos ya están configurados para enviar mensajes de registro al servidor syslog, pero Packet Tracer solo admite el registro para el nivel de gravedad de depuración con syslog. Por eso debemos generar mensajes del nivel de depuración (nivel 7) para que se puedan enviar al servidor syslog.

a. Haga clic en **R1 > ficha CLI**.

b. Presione Intro para que aparezca un símbolo del sistema y escriba el comando **enable**.

c. Introduzca el comando **debug eigrp packets** para habilitar la depuración EIGRP. La consola de la línea de comandos se llenará inmediatamente con mensajes de depuración.

d. Regrese a la ventana del **Servidor Syslog**. Verifique que las entradas de registro aparezcan en el servidor syslog.

e. Después de que se hayan registrado algunos mensajes, haga clic en el botón de opciones para **Desactivar** el servicio de syslog.

Indique parte de la información que se incluye en los mensajes de syslog que está mostrando el Servidor Syslog.

f. Cierre la ventana del dispositivo R1.

Parte 2: Registrar el acceso de los usuarios

Otro tipo importante de registro está relacionado con el acceso de los usuarios. Tener registros de los inicios de sesión de los usuarios es crucial para la solución de problemas y el análisis de tráfico. Cisco IOS admite Autenticación, Autorización y Auditoría (AAA). Con AAA, es posible no solo delegar la tarea de validación de usuarios a un servidor externo, sino también a actividades de registro.

TACACS+ es un protocolo diseñado para permitir la autenticación remota a través de un servidor centralizado.

Packet Tracer ofrece compatibilidad básica con AAA y TACACS+. R2 también está configurado como servidor TACACS+. R2 le preguntará al servidor si ese usuario es válido; para ello se verificará el nombre de usuario y la contraseña y se concederá o negará el acceso en función de la respuesta. El servidor almacena las credenciales del usuario y también es capaz de registrar transacciones de inicio de sesión del usuario. Sigan los pasos que se indican a continuación para iniciar sesión en R2 y mostrar las entradas de registro relacionadas con ese inicio de sesión:

a. Haga clic en el **Servidor Syslog** para abrir su ventana.

b. Seleccione la ficha **Escritorio** y, luego **Auditoría AAA**. Deje esta ventana abierta.

c. Haga clic en **R2 > CLI**.

d. Presione Intro para que aparezca un símbolo del sistema. **R2** le pedirá su nombre de usuario y contraseña antes de otorgarle acceso a su CLI. Introduzca las siguientes credenciales de usuario: **analyst** y **cyberops** como nombre de usuario y contraseña, respectivamente.

e. Regrese a la ventana Registros de Auditoría AAA del servidor Syslog.

¿Qué información se incluye en la entrada de registro?

En R2, introduzca el comando **logout**.

¿Qué sucedió en la ventana Auditoría AAA?

Parte 3: NetFlow y la visualización

En la topología, el servidor Syslog también es un colector de NetFlow. El firewall está configurado como exportador de NetFlow.

a. Haga clic en el **Servidor Syslog** para abrir su ventana. Cierre la ventana Registros de Auditoría AAA.

b. En la ficha **Escritorio**, seleccione **Colector de Netflow**. Se deben activar los servicios del Colector del NetFlow.

c. Desde cualquier PC, haga un ping al Servidor web corporativo en 209.165.200.194. Después de una breve demora, el gráfico circular se actualizará para mostrar el nuevo flujo de tráfico.

Nota: Los gráficos circulares que se muestren variarán en función del tráfico que haya en la red. Otros flujos de paquetes, como el tráfico relacionado con EIGRP, se están enviando entre los dispositivos. NetFlow está capturando esos paquetes y exportando estadísticas al Colector de NetFlow. Cuanto más tiempo se permita ejecutar NetFlow en una red se capturarán más estadísticas sobre el tráfico.

Reflexión

Si bien las herramientas presentadas en esta actividad son útiles, cada una tiene su propio servicio y es posible que tenga que ser ejecutada en dispositivos totalmente diferentes. Una mejor manera (que se analiza más adelante en el curso) es concentrar toda la información de registro en una sola herramienta, lo que permite facilitar la referencia cruzada y hace posibles potentes funcionalidades de búsqueda. Las plataformas de Administración de información y eventos de seguridad (Security Information and Event Management, SIEM) puede recopilar archivos de registro y otros datos de diversas fuentes e integrar la información correspondiente al acceso por medio de una sola herramienta.