Práctica de laboratorio: Aislar hosts afectados con el método de cinco tuplas

Objetivos

En esta práctica de laboratorio revisará archivos de registro durante el ataque a una vulnerabilidad documentada para determinar los hosts y el archivo comprometidos.

Parte 1: Revisar alertas en Sguil

Parte 2: Pivotar a Wireshark

Parte 3: Pivotar a Kibana

Antecedentes / Escenario

Los administradores de TI utilizan el método de 5 tuplas cuando necesitan identificar los requisitos necesarios para crear un entorno de red operativo y seguro. Los componentes de 5-Tuple son los siguientes: la dirección IP y el número de puerto de origen, la dirección IP y el número de puerto de destino y el protocolo en uso. Este es el campo de protocolo del encabezado del paquete IP.

En esta práctica de laboratorio también revisará los archivos de registros para identificar los hosts comprometidos y el contenido del archivo afectado.

Recursos necesarios

- Máquina virtual Security Onion

Instrucciones

Después del ataque, los usuarios ya no pueden acceder al archivo de nombre **confidential.txt**. Ahora revisarán los archivos de registro para determinar de qué manera se vio afectado el archivo.

Nota: Si esta red fuese de producción, se recomienda que los usuarios **analyst** y **root** cambien sus contraseñas y cumplan con la política de seguridad vigente.

Parte 1: Revisar alertas en Sguil

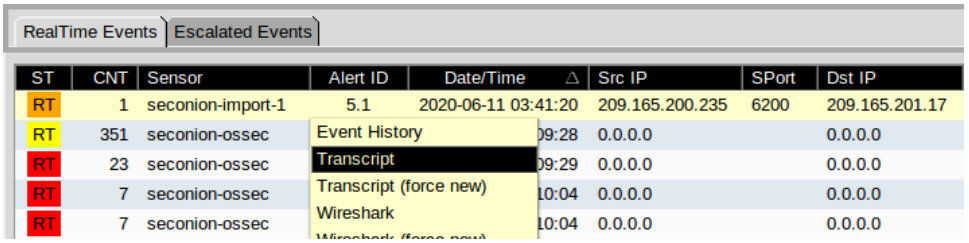
a. Inicie sesión en la máquina virtual Security Onion con el nombre de usuario **analyst** y contraseña **cyberops**

b. Abra **Sguil** e inicie sesión. Haga clic en **Select All** (Seleccionar todo) y, luego, en **Start SGUIL**. (Iniciar SGUIL)

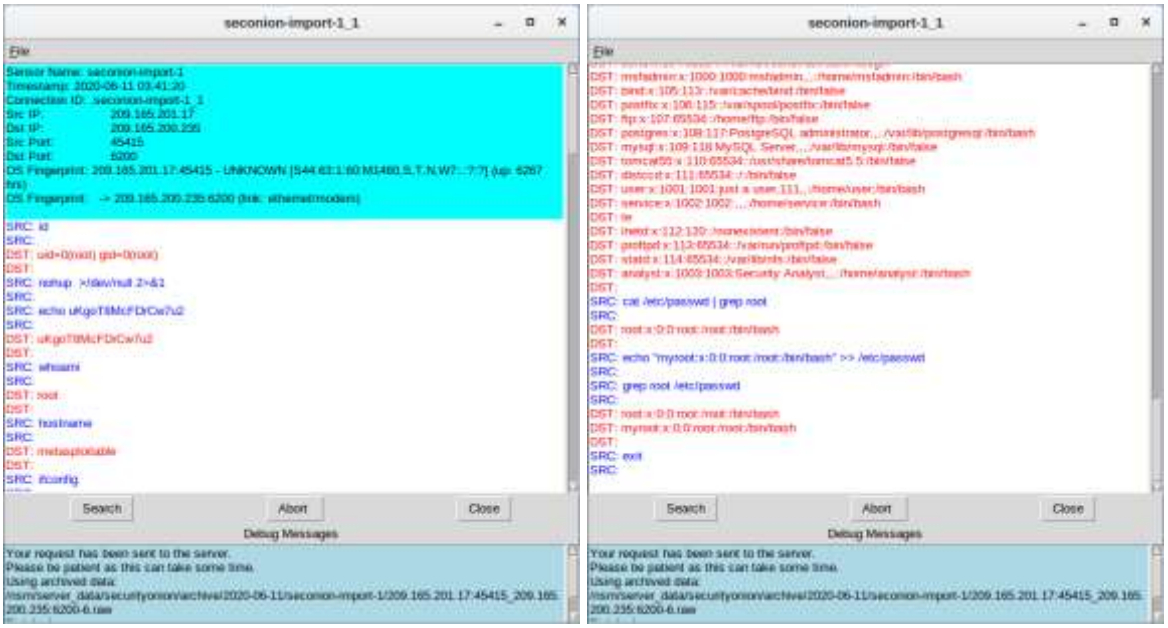
c. Revise los eventos que aparecen en la lista de la columna Event Message (Mensaje de eventos). Uno de los mensajes son **GPL ATTACK_RESPONSE id check returned root.** Este mensaje indica que es posible que se haya obtenido acceso raíz durante un ataque. El host de 209.165.200.235 devolvió el acceso raíz a 209.165.201.17. En este ejemplo se utiliza el ID de alerta **5.1**

d. Seleccione las casillas de verificación **Show Packet Data** (Mostrar datos del paquete) y **Show Rule** (Mostrar regla) para ver cada alerta más detalladamente.

e. Haga clic derecho sobre el ID 5.1 de la alerta y seleccione **Transcript**



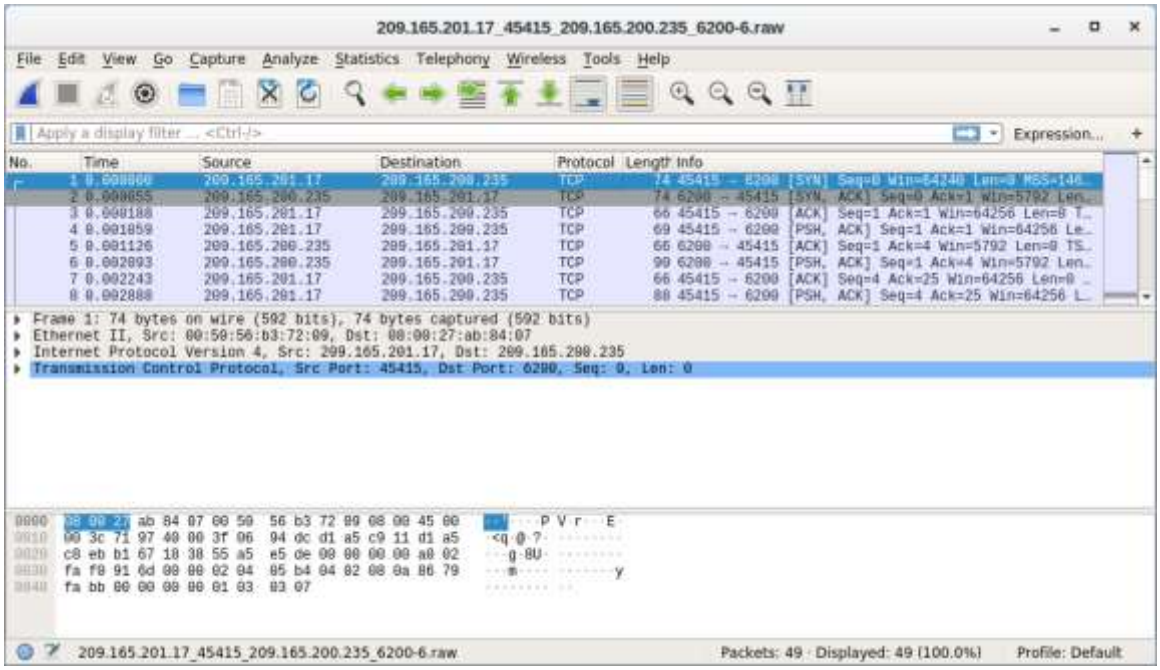
f. Revise las transcripciones correspondientes a todas las alertas. La transcripción muestra las transacciones entre el origen del agente de amenaza (SRC) y el objetivo (DST) durante el ataque. El actor de amenazas está ejecutando comandos Linux en el destino.



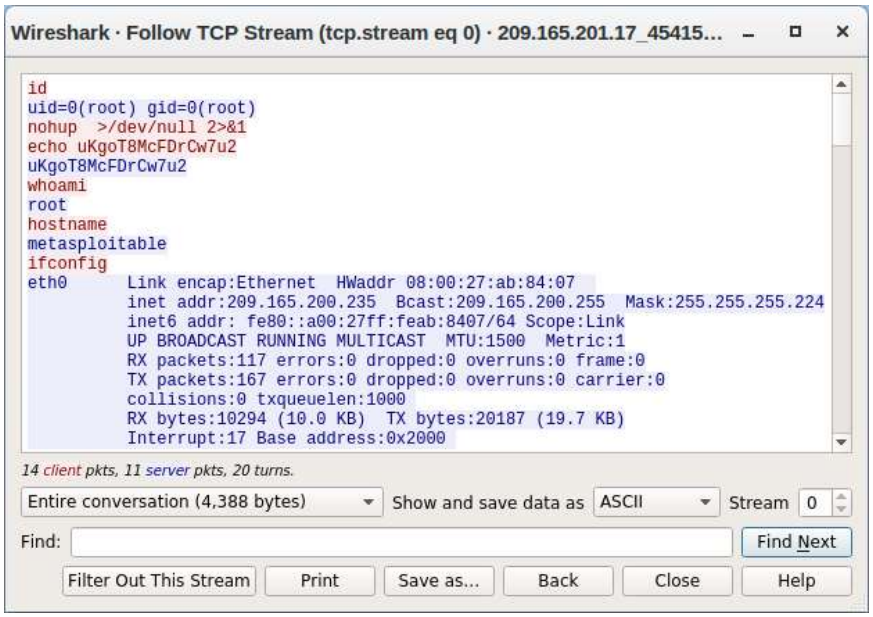
¿Qué tipo de transacciones ocurrieron entre el cliente y el servidor en este ataque?

Parte 2: Pasar a Wireshark

a. Seleccione la alarma que les proporcionó la transcripción en el paso anterior. Haga clic derecho sobre el ID 5.1 de la alerta y seleccione **Wireshark**. En la ventana principal de Wireshark se muestran 3 vistas de un paquete.



b. Para ver todos los paquetes ensamblados en una conversación de TCP, haga clic derecho sobre cualquier paquete y seleccione **Follow** > **TCP Stream** (Seguir flujo de TCP).



¿Qué observó? ¿Qué indican los colores de texto rojo y azul?

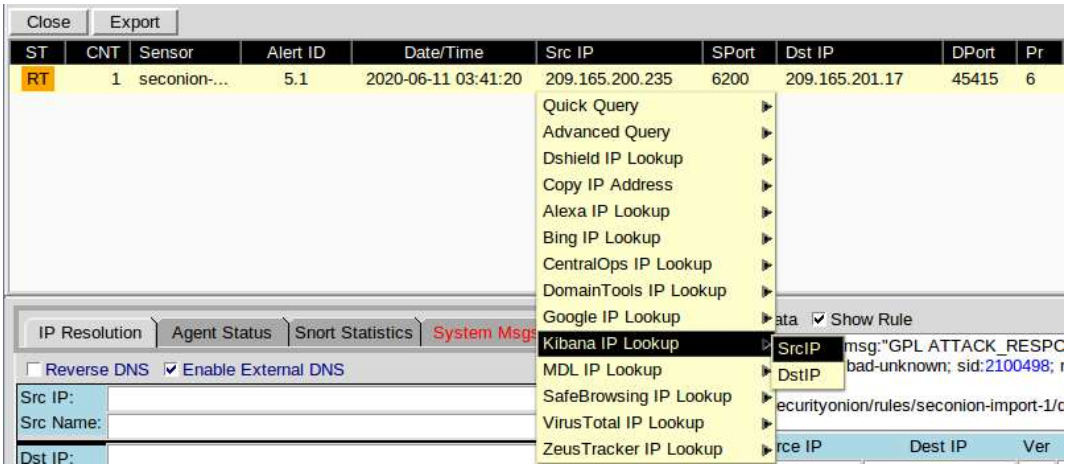
El atacante emite el comando **whoami** en el objetivo. ¿Qué muestra esto sobre el rol de atacante en el equipo de destino?

Desplácese por el flujo TCP. ¿Qué tipo de datos ha estado leyendo el agente de amenaza?

c. Salga de la ventana del flujo de TCP. Cierre **Wireshark** cuando hayan terminado de revisar la información provista por Wireshark.

Parte 3: Pivotar a Kibana

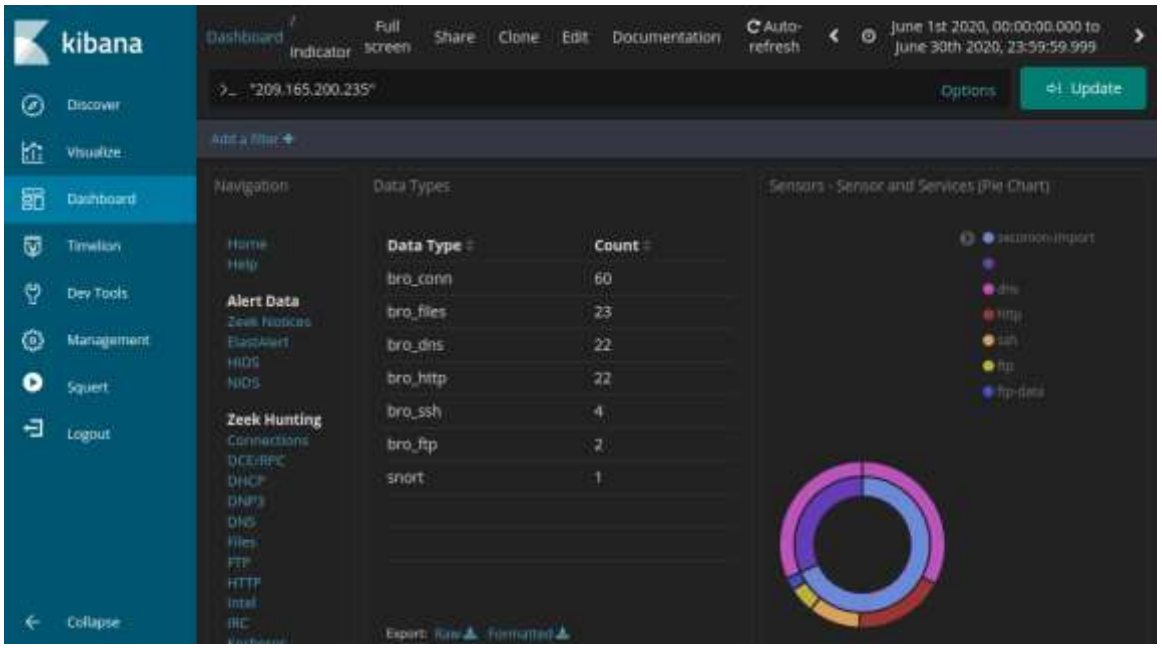
a. Regrese a Sguil. Haga clic con el botón derecho en la IP de origen o destino para el ID de alerta 5.1 y seleccione **Búsqueda IP de Kibana** > **SRCIp**. Introduzca **analyst** como nombre de usuario y **cyberops** como contraseña cuando ELSA se los solicite.



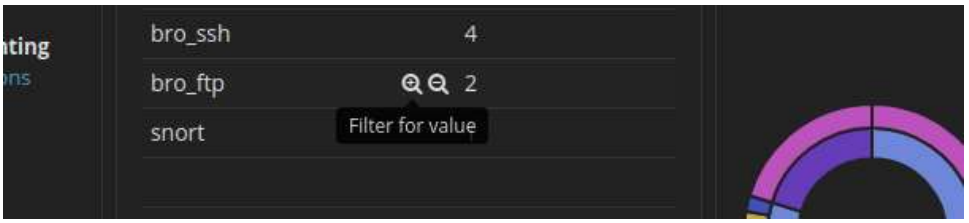
Nota: Si ve el mensaje "Su conexión no es privada", haga clic en **AVANZADAS > Proseguir al host local (inseguro)** para continuar.

b. Si el intervalo de tiempo es de las últimas 24 horas, cámbielo a junio de 2020 para que el 11 de junio esté incluido en el intervalo de tiempo. Utilice la ficha **Absoluto** para cambiar el intervalo de tiempo.

c. En los resultados mostrados, hay una lista de diferentes tipos de datos. Le dijeron que el archivo **confidential.txt** ya no es accesible. En los sensores - sensores y servicios (gráfico circular), ftp y ftp-data están presentes en la lista, como se muestra en la figura. Determinará si se utilizó FTP para robar el archivo.



d. Vamos a filtrar para **bro_ftp**. Pase el cursor sobre el espacio vacío junto al recuento de tipos de datos bro_ftp. Seleccione **+** para filtrar sólo el tráfico relacionado con FTP como se muestra en la figura.



e. Desplácese hasta la sección **All Logs** . Existen dos entradas enumeradas

¿Cuáles son las direcciones IP y los números de puerto de origen y de destino para el tráfico FTP?

f. Expanda y revise ambas entradas de registro. En una de estas entradas, el argumento ftp_tiene una entrada de ftp://209.165.200.235/./confidencial.txt. Revise también el mensaje en la entrada de registro para obtener más información sobre este evento.

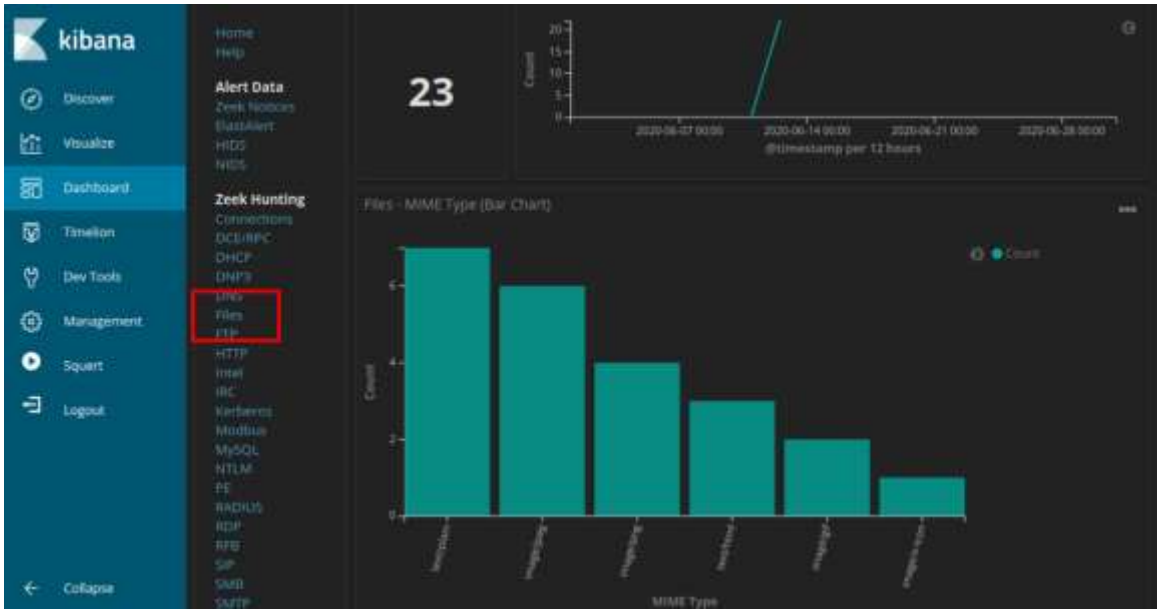
g. Dentro de la misma entrada de registro, desplácese hacia arriba hasta el campo alert _**id** y haga clic en el vínculo.

h. Revise la transcripción de las transacciones entre el atacante y el destino. Si lo desea, puede descargar el pcap y revisar el tráfico usando Wireshark.

¿Cuáles son las credenciales de usuario para acceder al sitio FTP?

i. Ahora que ha verificado que el atacante ha utilizado FTP para copiar el contenido del archivo confidential.txt y luego lo ha eliminado del destino. Entonces, ¿cuál es el contenido del archivo? Recuerde que uno de los servicios enumerados en el gráfico circular es ftp_data.

j. Navegue hasta la parte superior del panel. Seleccione **Archivos** bajo el encabezado Zeek Hunting en el panel izquierdo, como se muestra en la figura. Esto le permitirá revisar los tipos de archivos que se registraron.



¿Cuáles son los diferentes tipos de archivos? Mire la sección Tipo MIME de la pantalla.

Desplácese hasta el encabezado **Archivos - Origen**. ¿Cuáles son los orígenes de archivos enumerados?

k. Para filtrar **FTP_DATA**, pase el cursor sobre el espacio vacío situado junto al Count for FTP_DATA y haga clic en **+**.

l. Desplácese hacia abajo para ver los resultados de la búsqueda.

¿Cuál es el tipo MIME, la dirección IP de origen y destino asociado con la transferencia de los datos FTP? ¿Cuándo ocurrió esta transferencia?

m. En los registros de archivos, expanda la entrada asociada a los datos FTP. Haga clic en el vínculo asociado con alert _**id**.

¿Cuál es el contenido de texto del archivo que se transfirió mediante FTP?

Con toda la información recopilada hasta ahora, ¿cuál es su recomendación para detener nuevos accesos no autorizados?