

## 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: Pivотar a Wireshark

#### Parte 3: Pivотar 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

- Inicie sesión en la máquina virtual Security Onion con el nombre de usuario **analyst** y contraseña **cyberops**
- Abra **Sguil** e inicie sesión. Haga clic en **Select All** (Seleccionar todo) y, luego, en **Start SGUIL**. (Iniciar SGUIL)
- 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**

RealTime Events											
Escalated Events											
ST	CNT	Sensor	Alert ID	Date/Time	△	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	seconion-import-1	5.1	2020-06-11 03:41:20		209.165.200.235	6200	209.165.201.17	45415	6	GPL ATTACK_RESPONSE id check returned root
RT	351	seconion-ossec	1.1	2020-06-19 18:09:28		0.0.0.0	0.0.0.0	0.0.0.0	0		[OSSEC] File added to the system.
RT	23	seconion-ossec	1.2	2020-06-19 18:09:29		0.0.0.0	0.0.0.0	0.0.0.0	0		[OSSEC] Integrity checksum changed.

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

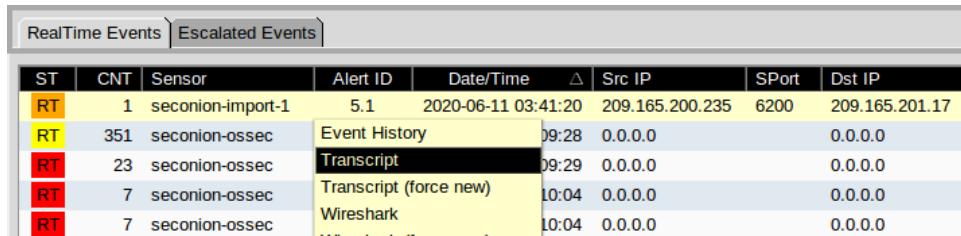
- d. Seleccione las casillas de verificación **Show Packet Data** (Mostrar datos del paquete) y **Show Rule** (Mostrar regla) para ver cada alerta más detalladamente.



The screenshot shows a terminal window with two checked options at the top: "Show Packet Data" and "Show Rule". Below this, the terminal displays a single line of text representing a network rule:

```
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root"; content:"uid=0[28]root[29]"; fast_pattern:only; classtype:bad-unknown; sid:2100498; rev:8; metadata:created_at 2010_09_23, updated_at 2010_09_23); /nsm/server_data/securityonion/rules/seconion-import-1/downloaded.rules: Line 700
```

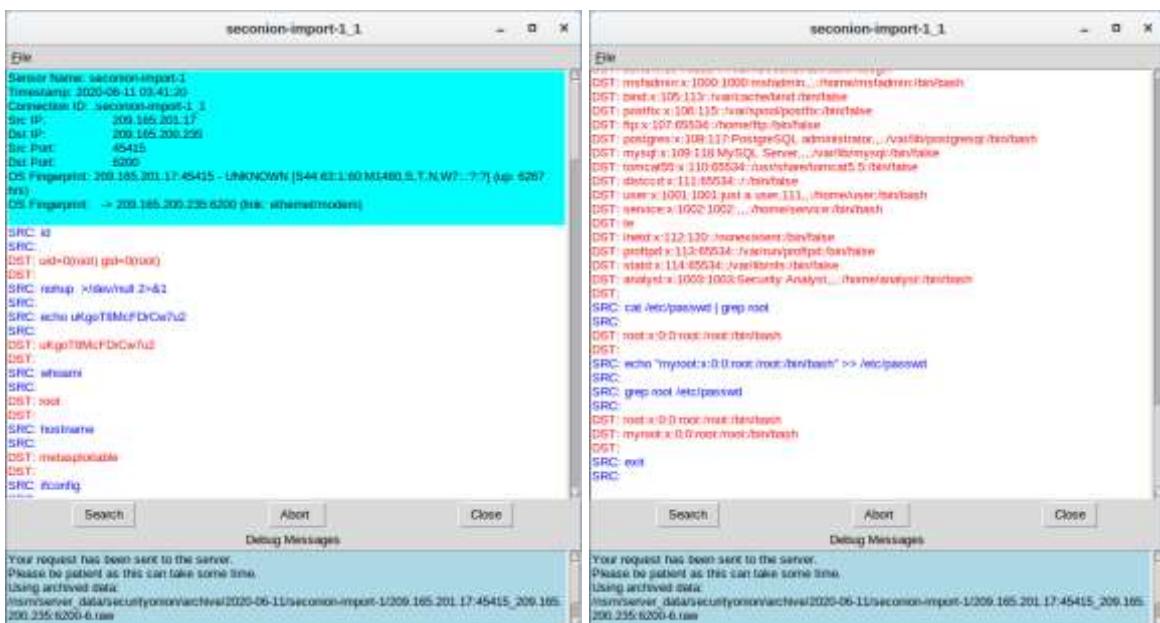
- e. Haga clic derecho sobre el ID 5.1 de la alerta y seleccione **Transcript**



The screenshot shows a table of network alerts. The second row, which has an "RT" status and an ID of 5.1, is highlighted. A context menu is open over this row, with the option "Transcript" highlighted. The table columns are: ST, CNT, Sensor, Alert ID, Date/Time, △, Src IP, SPort, Dst IP.

ST	CNT	Sensor	Alert ID	Date/Time	△	Src IP	SPort	Dst IP
RT	1	seconion-import-1	5.1	2020-06-11 03:41:20		209.165.200.235	6200	209.165.201.17
RT	351	seconion-ossec		Event History	09:28	0.0.0.0		0.0.0.0
RT	23	seconion-ossec		Transcript	09:29	0.0.0.0		0.0.0.0
RT	7	seconion-ossec		Transcript (force new)	10:04	0.0.0.0		0.0.0.0
RT	7	seconion-ossec		Wireshark	10:04	0.0.0.0		0.0.0.0
Wireshark forced now								

- 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.

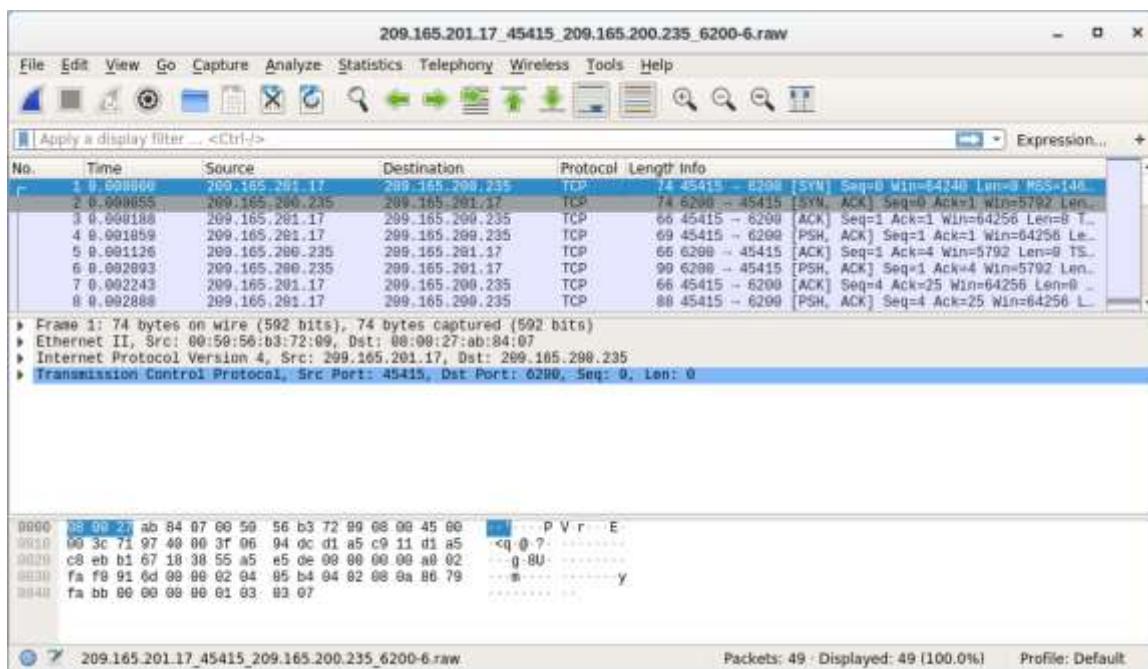


The screenshot shows two terminal windows side-by-side. Both windows have the title "seconion-import-1\_1" and are displaying the transcript of an alert. The transcript shows a series of commands and responses between a source host (SRC) and a destination host (DST). The SRC host is executing various Linux commands like "grep", "cat", and "rm" on the DST host's files. The DST host is responding with error messages and file contents. The transcript is very long and contains many lines of command-line output.

¿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.



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

- 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).



The screenshot shows the Wireshark interface with the title "Wireshark · Follow TCP Stream (tcp.stream eq 0) · 209.165.201.17\_45415...". The main pane displays a series of network packets, with the first few lines of the ASCII dump highlighted in red:  
id  
uid=0(root) gid=0(root)  
nohup >/dev/null 2>&1  
echo uKgoT8McFDrcw7u2  
uKgoT8McFDrcw7u2  
whoami  
root  
hostname  
metasploitable  
ifconfig  
eth0 Link encap:Ethernet Hwaddr 08:00:27:ab:84:07  
inet addr:209.165.200.235 Bcast:209.165.200.255 Mask:255.255.255.224  
inet6 addr: fe80::a00:27ff:feab:8407/64 Scope:Link  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:117 errors:0 dropped:0 overruns:0 frame:0  
TX packets:167 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:10294 (10.0 KB) TX bytes:20187 (19.7 KB)  
Interrupt:17 Base address:0x2000

Below the main pane, there are several controls:  
- A status bar at the bottom left says "14 client pkts, 11 server pkts, 20 turns."  
- A dropdown menu "Show and save data as" with options "ASCII", "Hex", and "Stream".  
- A "Stream" button with a dropdown menu set to "0".  
- A "Find" input field and a "Find Next" button.  
- Buttons for "Filter Out This Stream", "Print", "Save as...", "Back", "Close", and "Help".

¿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: Pivatar a Kibana

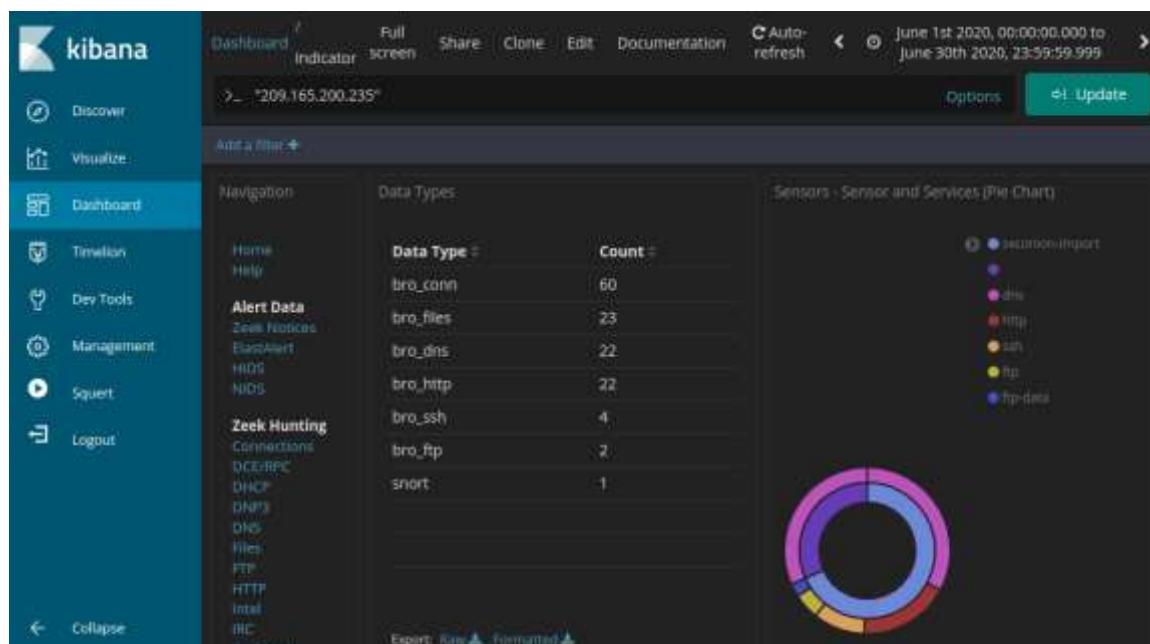
- Regrese a Sguil. Haga clic con el botón derecho en la IP de origen o destino para el ID de alerta 5.1 y seleccione **Búsqueda IP de Kibana > SRCIp**. Introduzca **analyst** como nombre de usuario y **cyberops** como contraseña cuando ELSA se los solicite.

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr
RT	1	seconion...	5.1	2020-06-11 03:41:20	209.165.200.235	6200	209.165.201.17	45415	6

IP Resolution Agent Status Snort Statistics System Msgs  
 Reverse DNS  Enable External DNS  
Src IP:   
Src Name:   
Dst IP:

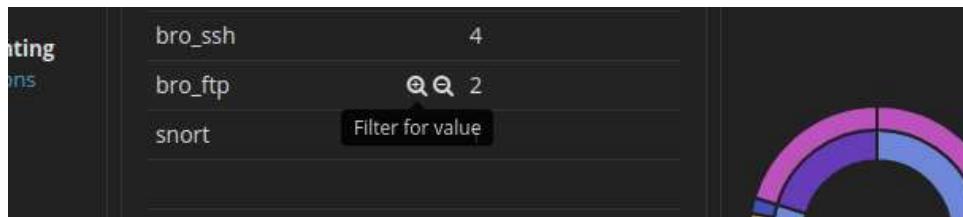
**Nota:** Si ve el mensaje "Su conexión no es privada", haga clic en **AVANZADAS > Proseguir al host local (inseguro)** para continuar.

- 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.
- 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.



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

- 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.

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

- 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 **+**.

Syslog Tunnels Weird X.509	Source	Count	Bytes Seen
	HTTP	22	99.685KB
<b>Host Hunting</b> Autoruns Beats OSSEC	FTP_DATA	1	70.19KB
		Filter for value	
			55.912KB
			50.438KB

- 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?

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

---

- 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?