Práctica de laboratorio: Interpretar datos HTTP y DNS para aislar al actor de la amenaza
Objetivos

En esta práctica de laboratorio, analizará registros durante un explotamiento malicioso de vulnerabilidades HTTP y DNS documentadas.

Parte 1: Investigar un ataque de Inyección SQL

Parte 2: Investigar la exfiltración de datos DNS

Antecedentes / Escenario

MySQL es una base de datos popular que utilizan numerosas aplicaciones web. Desafortunadamente, la Inyección SQL es una técnica de hacking web común. Es una técnica de inyección de código en la que un atacante ejecuta comandos SQL maliciosos para controlar el servidor de bases de datos de una aplicación web.

Los servidores de nombres de dominio (Domain Name Servers, DNS) son directorios de nombres de dominio y traducen los nombres de dominio a direcciones IP. Este servicio puede utilizarse para exfiltrar datos.

El personal de ciberseguridad ha determinado que una vulnerabilidad ha ocurrido, y los datos que contienen PII pueden haber estado expuestos a agentes de amenazas En este laboratorio, utilizará Kibana para investigar las vulnerabilidades para determinar los datos que se exfiltraron utilizando HTTP y DNS durante los ataques.

Recursos necesarios

- Máquina virtual de Security Onion

Instrucciones

Parte 1: Investigar un ataque de Inyección SQL

En esta parte, investigará una vulnerabilidad en el que se realizó acceso no autorizado a la información confidencial que se almacena en un servidor web. Utilizará Kibana para determinar el origen del ataque y la información a la que accede el atacante.

Paso 1: Cambiar el plazo

Se ha determinado que la vulnerabilidad ocurrió en algún momento durante el mes de junio de 2020. Kibana muestra los datos de forma predeterminada durante las últimas 24 horas. Tendrá que cambiar la configuración de la hora para ver los datos del mes de junio de 2020.

a. Inicie sesión en Security Onion con el nombre de usuario **“analyst”**, y la contraseña **“CyberOPS”**.

b. Introduzca el comando **sudo so-status** para comprobar el estado de los servicios. El estado de todos los servicios debe estar **OK** antes de iniciar el análisis. Esto podría demorar unos minutos.

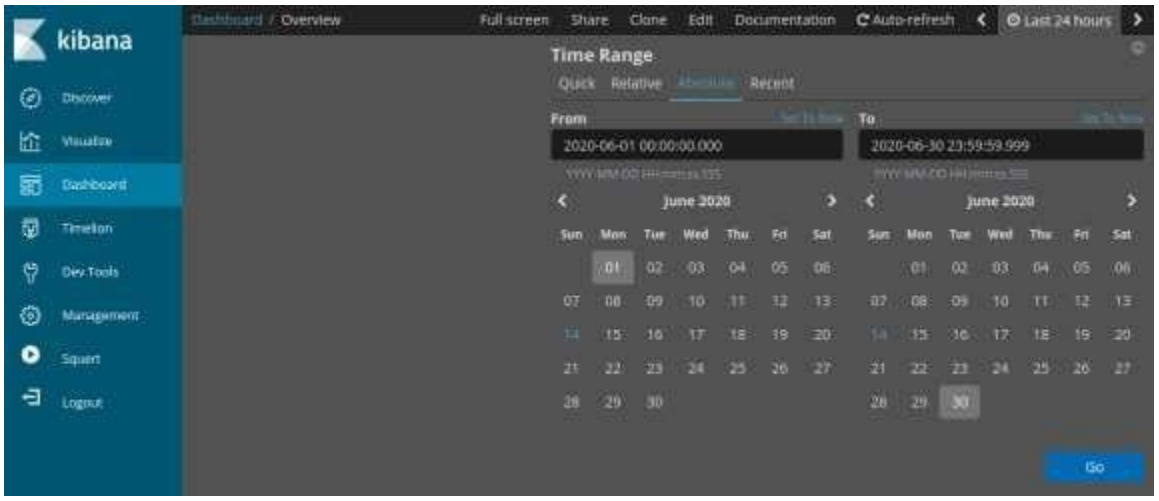
```
analyst@SecOnion:~$ sudo so-status
Status: securityonion
  * sguil server [ OK ]
Status: seconion-import
  * pcap_agent (sguil) [ OK ]
  * snort_agent-1 (sguil) [ OK ]
```

```
  * barnyard2-1 (spooler, unified2 format) [ OK ]
Status: Elastic stack
  * so-elasticsearch [ OK ]
  * so-logstash [ OK ]
  * so-kibana [ OK ]
  * so-freqserver [ OK ]
```

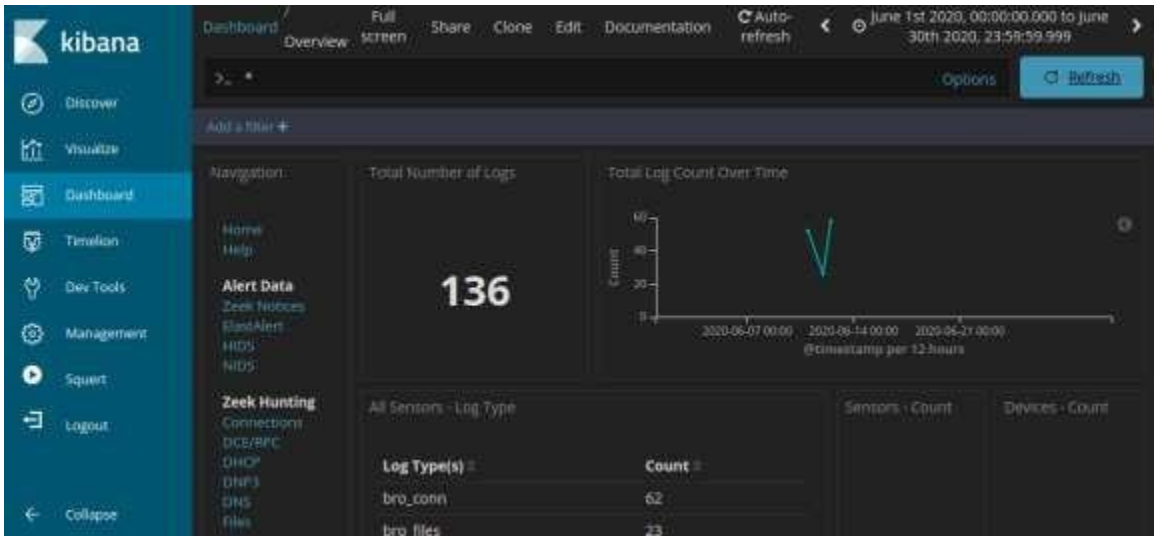
c. Después de iniciar sesión, abra Kibana usando el acceso directo en el escritorio. Inicie sesión con el nombre de usuario **analyst** y la contraseña **cyberops**.

   En Security Onion, Kibana tiene muchos tableros y visualizaciones precompilados para monitoreo y análisis. También puede crear sus propios paneles y visualizaciones personalizados que se adapten a la supervisión de su entorno de red en particular. **Nota**: Es posible que el panel de control no tenga ningún resultado en las últimas 24 horas.

d. En la esquina superior derecha de la ventana, haga clic en **Last 24 hours** en para cambiar el tamaño del intervalo de tiempo de la muestra. Expanda el intervalo de tiempo para incluir las alertas interesantes. Un ataque de inyección SQL tuvo lugar en junio de 2020, por lo que es lo que necesita revisar. Seleccione **Absolute** en Intervalo de tiempo y edite las horas **Desde** y **Hasta** para incluir todo el mes de junio de 2020. Haga clic en **Go** para continuar.



e. Observe el número total de registros para todo el mes de junio de 2020. El panel debe ser similar al que se muestra en la figura. Tómese un momento para explorar la información proporcionada por la interfaz de Kibana.



Paso 2: Filtrar para el tráfico HTTP.

a. Dado que el atacante evaluó los datos almacenados en un servidor web, el filtro HTTP se utiliza para seleccionar los registros asociados con el tráfico HTTP. Seleccione HTTP bajo el encabezado Zeek Hunting, como se muestra en la figura.

Revise los resultados y responda las siguientes preguntas:

¿Cuál es la dirección IP de origen?

¿Cuál es la dirección IP de destino?

¿Cuál es el número de puerto de destino?

b. Desplácese hasta la sección HTTP. El resultado muestra los 10 primeros resultados.

c. Expanda los detalles del primer resultado haciendo clic en la flecha que se encuentra junto a la marca de tiempo de entrada de registro. Tenga en cuenta la información disponible.

¿Cuál es la marca de tiempo del primer resultado?

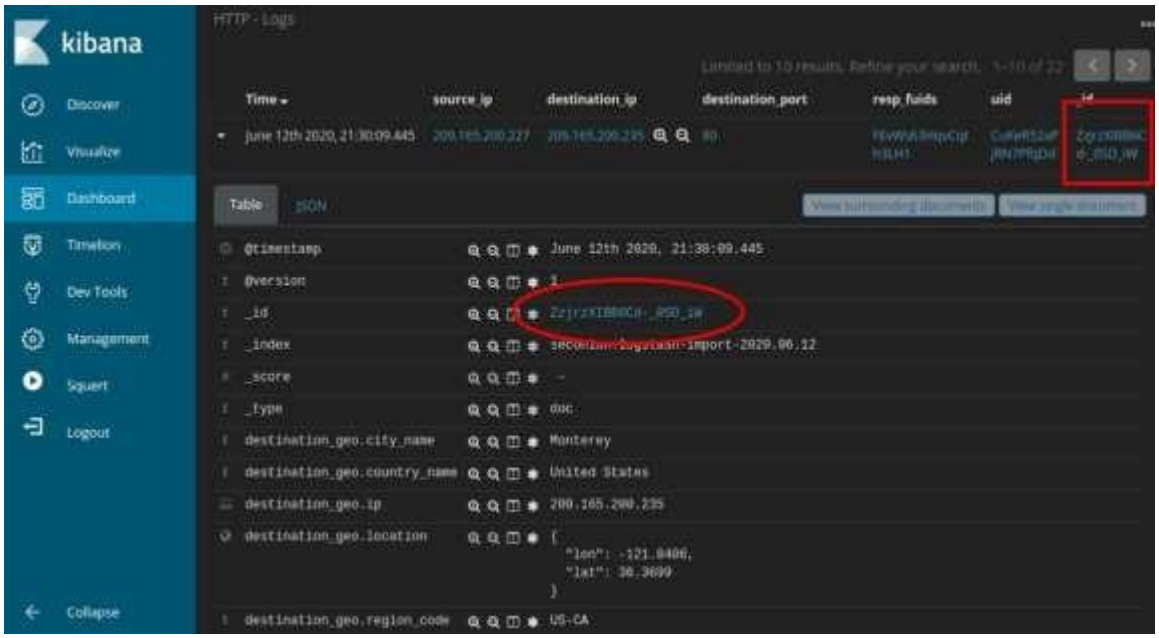
¿Cuál es el tipo de evento?

¿Qué se incluye en el campo de mensaje? Estos son detalles sobre la solicitud HTTP GET que realizó el cliente al servidor. Enfocado especialmente en el **uri** field en el mensaje de texto.

¿Qué es importante sobre esta información?

Paso 3: Revise los resultados

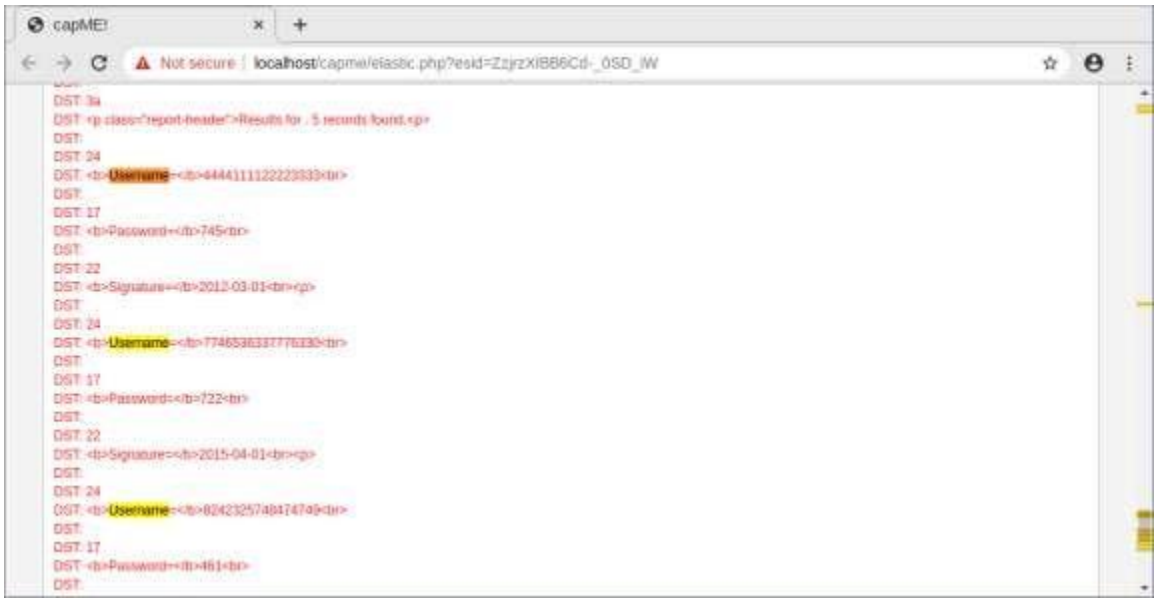
a. Parte de la información de las entradas de registro se enlaza a otras herramientas. Haga clic en el valor del campo de **_id** de alertas de la entrada de registro para obtener una vista diferente del evento.



b. El resultado se abre en una nueva pestaña del navegador web con información de capME!. La pestaña capME! es una interfaz web que le permite ver una transcripción pcap. El texto azul contiene solicitudes HTTP que se envían desde el origen (SRC). El texto rojo son respuestas del servidor web de destino (DST).

c. En la sección entrada de registro, que está al principio de la transcripción, observe la parte **username='+union+select+ccid,ccnumber,ccv,expiration,null+from+credit_cards+--+&password=** indica que alguien puede haber intentado atacar el explorador web mediante la inyección SQL para omitir la autenticación. Las palabras claves, **union** and **select**, son comandos que se utilizan en la búsqueda de información en una base de datos SQL. Si los cuadros de entrada de una página web no está n protegidos correctamente contra la entrada ilegal, los atacantes pueden insertar cadenas de búsqueda SQL u otro código que pueda tener acceso a los datos contenidos en las bases de datos vinculadas a la página web.

d. Busque el nombre de **username** de la palabra clave en la transcripción. Utilice **Ctrl-F** para abrir un cuadro de búsqueda. Utilice el botón de flecha hacia abajo en el cuadro de búsqueda para desplazarse por las apariciones que se encontraron.



Puede ver dónde se utilizó el término nombre de usuario en la interfaz web que se muestra al usuario. Sin embargo, si miramos más abajo, se puede encontrar algo inusual.

¿Qué puede ver más adelante en la transcripción en cuanto a nombres de usuario?

Dé algunos ejemplos de un nombre de usuario, contraseña y firma que se exfiltró.

e. Cierre la pestaña decapME! y vuelva a Kibana

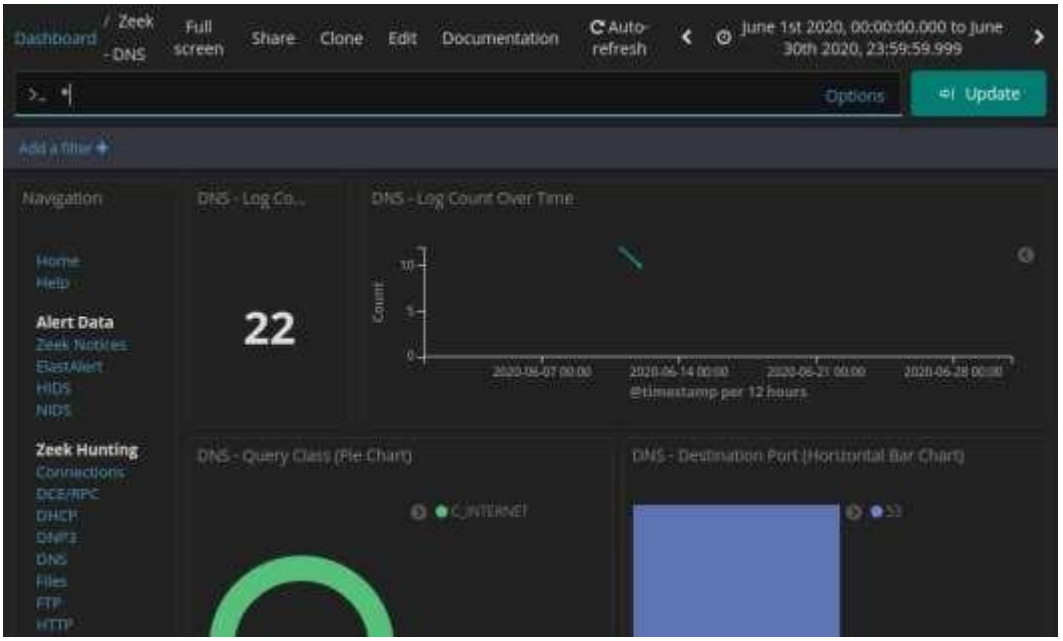
Parte 2: Analice la exfiltración de DNS.

Un administrador de red ha notado consultas DNS anormalmente largas con subdominios de aspecto extraño. Su trabajo es investigar la anormalidad.

Paso 1: Filtro para tráfico DNS

a. En la parte superior del panel de Kibana, borre los filtros y los términos de búsqueda y haga clic en **Home** en la sección Navegación del panel. El periodo de tiempo todavía debe incluir junio 2020.

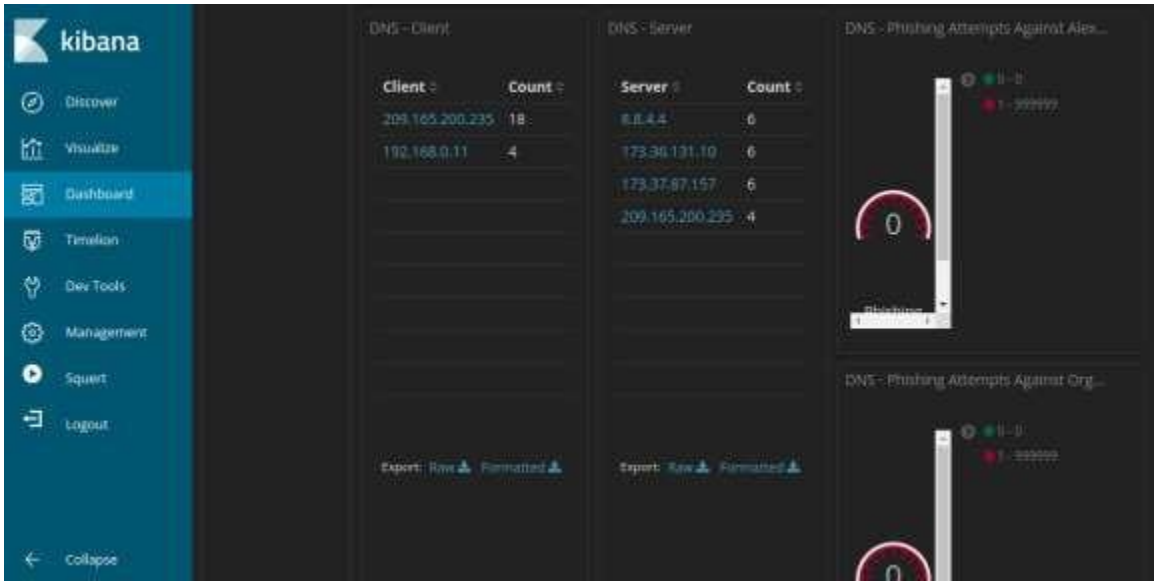
b. En la misma área del panel, haga clic en **DNS** en la sección Zeek Hunting. Observe las métricas de recuento de registros DNS y el gráfico de barras horizontales de puerto de destino.



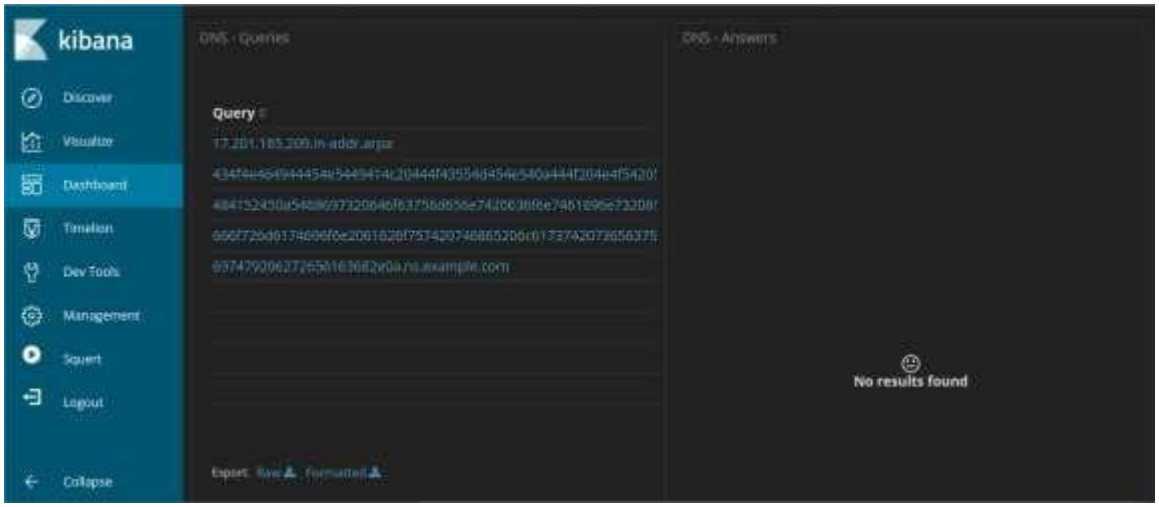
Paso 2: Revise las entradas relacionadas con DNS.

a. Despliegue la ventana. Puede ver los principales tipos de consultas DNS. Es posible que vea registros de direcciones (un registro), registros Quad A de direcciones IPv6 (AAAA), registros NetBIOS (NB) y registros de puntero para resolver los nombres de host (PTR). También puede ver los códigos de respuesta DNS.

b. Al desplazarse más hacia abajo, puede ver una lista de los principales clientes DNS y servidores DNS en función de sus recuentos de solicitudes y respuestas. También hay una métrica para el número de intentos de phishing DNS, que también se conocen como DNS pharming, suplantación de identidad o envenenamiento.



c. Desplazando más abajo por la ventana se puede ver una lista de las principales consultas DNS por nombre de dominio. Observe cómo algunas de las consultas tienen subdominios inusualmente largos asociados a ns.example.com. El example.com de dominio debe investigarse más a fondo



d. Desplácese hacia atrás hasta la parte superior de la ventana e introduzca **example.com** en la barra de búsqueda para filtrar example.com y haga clic en **Update.** Tenga en cuenta que el número de entradas en el recuento de registros es menor porque la visualización ahora está limitada a las solicitudes al servidor example.com

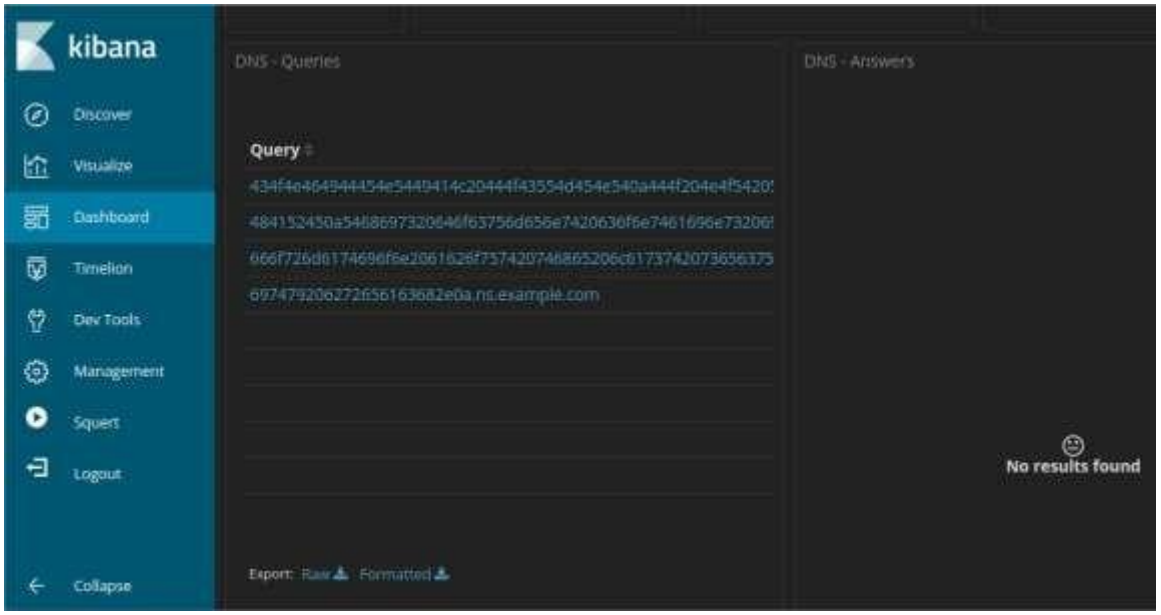
e. Busque información sobre el DNS - Cliente y DNS - Servidor.

Registre las direcciones IP del cliente y servidor DNS

Paso 3: Determine los datos exfiltrados.

a. Continúe desplazándose más hacia abajo para ver cuatro entradas de registro únicas para las consultas DNS a example.com. Observe cómo algunas de las consultas tienen subdominios inusualmente largos asociados a ns.example.com. Las cadenas largas de números y letras en los subdominios parecen texto codificado en hexadecimal (0-9, a-f) en lugar de nombres de subdominios legítimos. Haga clic en el

enlace de descarga **Export: Raw** para descargar las consultas en un archivo externo. Un archivo CSV es descargado a la carpeta /home/analyst/Downloads



b. Navegue a la carpeta **/home/analyst/Downloads**. Abra el archivo con un editor de texto como Notepad. Edite el archivo eliminando el texto que rodea la parte hexadecimal de los subdominios, dejando solo los caracteres hexadecimales. Asegúrese de eliminar las comillas también. El contenido de su archivo debe de verse como la información que se muestra abajo. Guarde el archivo de texto editado con el nombre de archivo original.

```
434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053
484152450a5468697320646f63756d656e7420636f6e7461696e7320696e
666f726d6174696f6e2061626f757420746865206c617374207365637572
697479206272656163682e0a
```

c. En la terminal, use el comando **xxd** para decodificar en el archivo CSV y guardelo como un archivo llamado secret.txt. Utilice **cat** para enviar el contenido de secret.txt a la consola.

```
analyst@SecOnion:~/Downloads$ xxd -r -p "DNS - Queries.csv" > secret.txt
analyst@SecOnion:~/$ cat secret.txt
```

¿Fueron los subdominios de los subdominios de consulta DNS? Si no, ¿Cuál es el texto?

¿Qué implica este resultado sobre esta respuesta DNS en particular? ¿Cuál es el mayor significado?

¿Qué puede haber creado estas consultas DNS codificadas y por qué se seleccionó DNS como los medios para exfiltrar datos?