

Práctica de laboratorio: Leer archivos de registro de un servidor

Objetivos

Parte 1: Leer archivos de registro (log files) con Cat, More, Less, y Tail

Parte 2: Archivos de registro y Syslog

Parte 3: Archivos de registro y Journalctl

NOTA: RESPONDER CADA PREGUNTA CON CAPTURAS DE PANTALLA COMPLETAS DONDE SE VEAN LAS SIGLAS DE SU NOMBRE AL LADO DEL RELOJ. EN LUGAR DE COLOCAR UN TEXTO DEBE DE SELECCIONAR EL TEXTO INVESTIGADO EN UNA PÁGINA WEB Y HACERLE CAPTURA DE PANTALLA COMPLETA, PARA LUEGO COLOCARLA AQUÍ. SI SON VARIAS PREGUNTAS, DEBE COLOCAR VARIAS CAPTURAS DE PANTALLAS COMPLETAS. NO COLOCAR INFORMACIÓN ENCONTRADA EN NETACAD, COLOCAR INFORMACIÓN INVESTIGADA EN OTRAS PÁGINAS WEB O LO REALIZADO POR USTED.

Antecedentes / Escenario

Los archivos de registro son una herramienta importante para la solución de problemas y el monitoreo. Cada aplicación genera archivos de registro diferentes, y cada uno contiene su propio conjunto de campos e información. Si bien la estructura de los campos puede variar de un archivo de registro a otro, las herramientas que se utilizan para leerlos son mayormente las mismas. En esta práctica de laboratorio practicarán para aprender a utilizar herramientas comunes que se emplean para leer archivos de registro.

Recursos necesarios

- Máquina virtual Security Workstation

Instrucciones

Parte 1: Leer archivos de registro con Cat, More, Less y Tail

Los archivos de registro son archivos que se utilizan para registrar eventos específicos iniciados por aplicaciones, servicios o el mismo sistema operativo. Suelen almacenarse como texto plano, y son un recurso indispensable para la solución de problemas.

Paso 1: Abrir archivos de registro

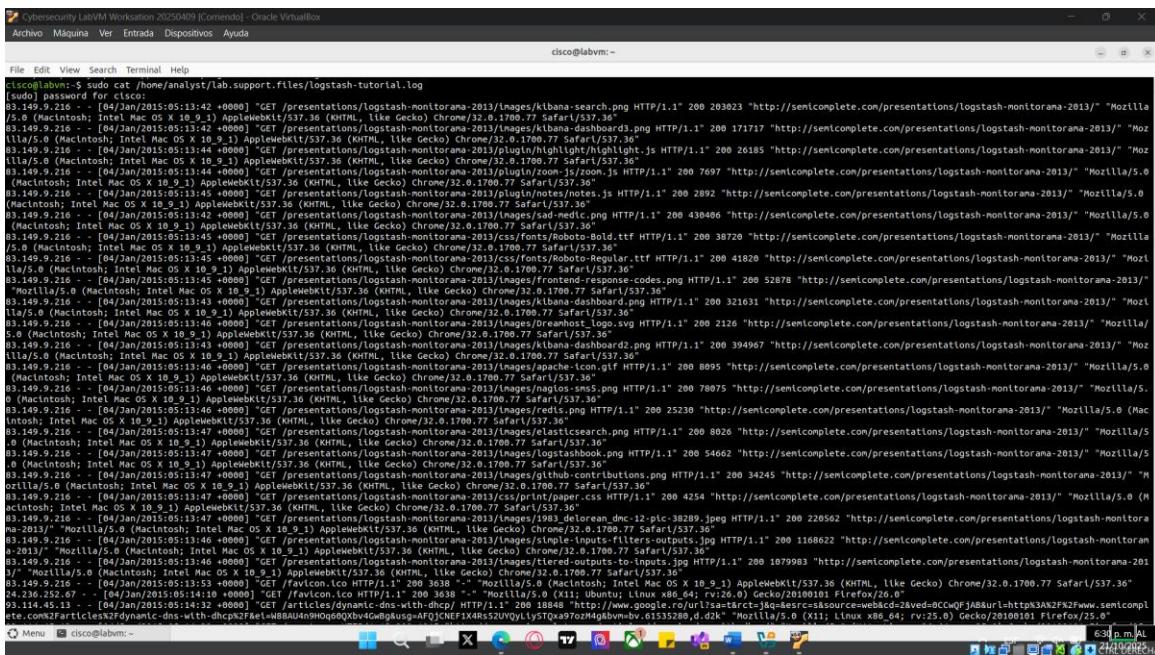
Comúnmente, los archivos de registro contienen información en texto plano que puede ser vista con prácticamente cualquier programa capaz de manejar texto (un editor de texto, por ejemplo). Sin embargo, por motivos de conveniencia, practicidad de uso y velocidad, algunas herramientas se utilizan más que otras. Esta sección se enfoca en cuatro programas basados en la línea de comandos: **cat**, **more**, **less** y **tail**.

Cat, derivado de la palabra ‘concatenar’, es una herramienta de UNIX basada en la línea de comandos que se utiliza para leer y mostrar el contenido de un archivo en la pantalla. Por su simplicidad y capacidad para abrir un archivo de texto y mostrarlo en un terminal de solo texto, **cat** sigue siendo muy utilizado en la actualidad.

- a. Abra el Security Workstation VM y, luego, una ventana del terminal.
 - b. En la ventana del terminal, emiten el siguiente comando para mostrar el contenido del archivo **logstash-tutorial.log**, que está ubicado en la carpeta **/home/analyst/lab.support.files/**:

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

El contenido del archivo debería desplazarse por la ventana del terminal hasta haber mostrado todo el contenido.



Indicar una desventaja de utilizar **cat** con archivos de texto grandes.

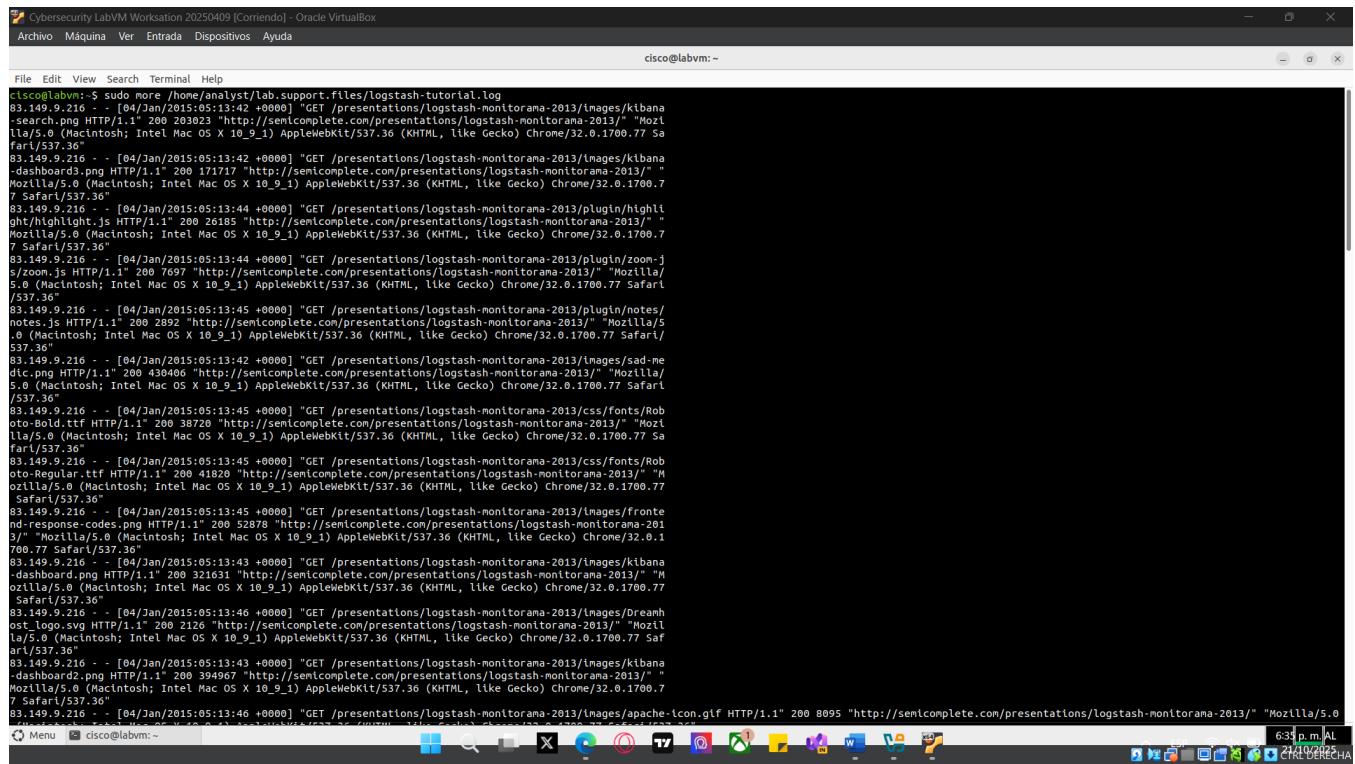
cat vuela todo el contenido al terminal sin paginación; con archivos muy grandes inunda la pantalla, es difícil navegar/leer, puede causar que se pierda la salida anterior y consume tiempo/memoria si se redirige. No permite retroceder o buscar fácilmente.

Otra herramienta popular para visualizar archivos de registro es **more**. Al igual que **cat**, **more** también es una herramienta de UNIX basada en la línea de comandos que puede abrir un archivo de texto y mostrar su contenido en la pantalla. La principal diferencia entre **cat** y **more** es que **more** admite saltos de páginas y eso permite que el usuario vea el contenido de un archivo una página por vez. Esto se puede hacer utilizando la barra espaciadora para mostrar la página siguiente.

- c. En la misma ventana del terminal, utilicen 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. Presionen la barra espaciadora para avanzar a la página siguiente. Presionen Intro para mostrar la siguiente línea de texto?



The screenshot shows a terminal window titled "Cybersecurity LabVM Workstation 20250409 [Corriendo] - Oracle VirtualBox". The command "sudo more /home/analyst/lab.support.files/logstash-tutorial.log" was run. The terminal displays a large amount of log data from January 2015, including various GET requests for logstash-monitorama-2013 images and files. The text is scrollable, with the bottom of the window showing scroll bars and a status bar indicating "633 n.m AL" and "21/07/2025 CIRE DERECHA".

```
cisco@labvm:~$ sudo more /home/analyst/lab.support.files/logstash-tutorial.log
cisco@labvm:~$ [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-search-dashboards.png HTTP/1.1" 200 293023 "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/32.0.1700.75 Safari/537.36"
cisco@labvm:~$ [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-dashboards3.png HTTP/1.1" 200 171717 "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"
cisco@labvm:~$ [04/Jan/2015:05:13:44 +0000] "GET /presentations/logstash-monitorama-2013/plugin/highlight/highlight.js HTTP/1.1" 200 26185 "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"
cisco@labvm:~$ [04/Jan/2015:05:13:44 +0000] "GET /presentations/logstash-monitorama-2013/plugin/zoom_j/zoom.js HTTP/1.1" 200 7697 "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"
cisco@labvm:~$ [04/Jan/2015:05:13:44 +0000] "GET /presentations/logstash-monitorama-2013/plugin/notes/notes.js HTTP/1.1" 200 2892 "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"
cisco@labvm:~$ [04/Jan/2015:05:13:45 +0000] "GET /presentations/logstash-monitorama-2013/images/sad_mehanismo.png HTTP/1.1" 200 43406 "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"
cisco@labvm:~$ [04/Jan/2015:05:13:45 +0000] "GET /presentations/logstash-monitorama-2013/css/fonts/Roboto-Bold.ttf HTTP/1.1" 200 38720 "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"
cisco@labvm:~$ [04/Jan/2015:05:13:45 +0000] "GET /presentations/logstash-monitorama-2013/css/fonts/Roboto-Regular.ttf HTTP/1.1" 200 41820 "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"
cisco@labvm:~$ [04/Jan/2015:05:13:45 +0000] "GET /presentations/logstash-monitorama-2013/images/frontend-response-codes.png HTTP/1.1" 200 52878 "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"
cisco@labvm:~$ [04/Jan/2015:05:13:43 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-dashboard.png HTTP/1.1" 200 321631 "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"
cisco@labvm:~$ [04/Jan/2015:05:13:43 +0000] "GET /presentations/logstash-monitorama-2013/images/dreamhost-logo.svg HTTP/1.1" 200 2126 "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"
cisco@labvm:~$ [04/Jan/2015:05:13:43 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-dashboards2.png HTTP/1.1" 200 394967 "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"
cisco@labvm:~$ [04/Jan/2015:05:13:46 +0000] "GET /presentations/logstash-monitorama-2013/images/apache-icon.gif HTTP/1.1" 200 8095 "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"
```

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

Que permite avanzar por pagina pero no permite retroceder

Sobre la base de la funcionalidad de **cat** y **more**, la herramienta **less** permite mostrar el contenido de un archivo página por página y, a la vez, permitir que el usuario opte por visualizar páginas ya mostradas en pantalla.

- d. En la misma ventana del terminal, utilicen **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. Presionen la barra espaciadora para avanzar a la página siguiente. Presionen Intro para mostrar la siguiente línea de texto? Utilicen las teclas de las flechas hacia arriba y hacia abajo para avanzar y retroceder por el archivo de texto.

Práctica de laboratorio: Leer archivos de registro de un servidor

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

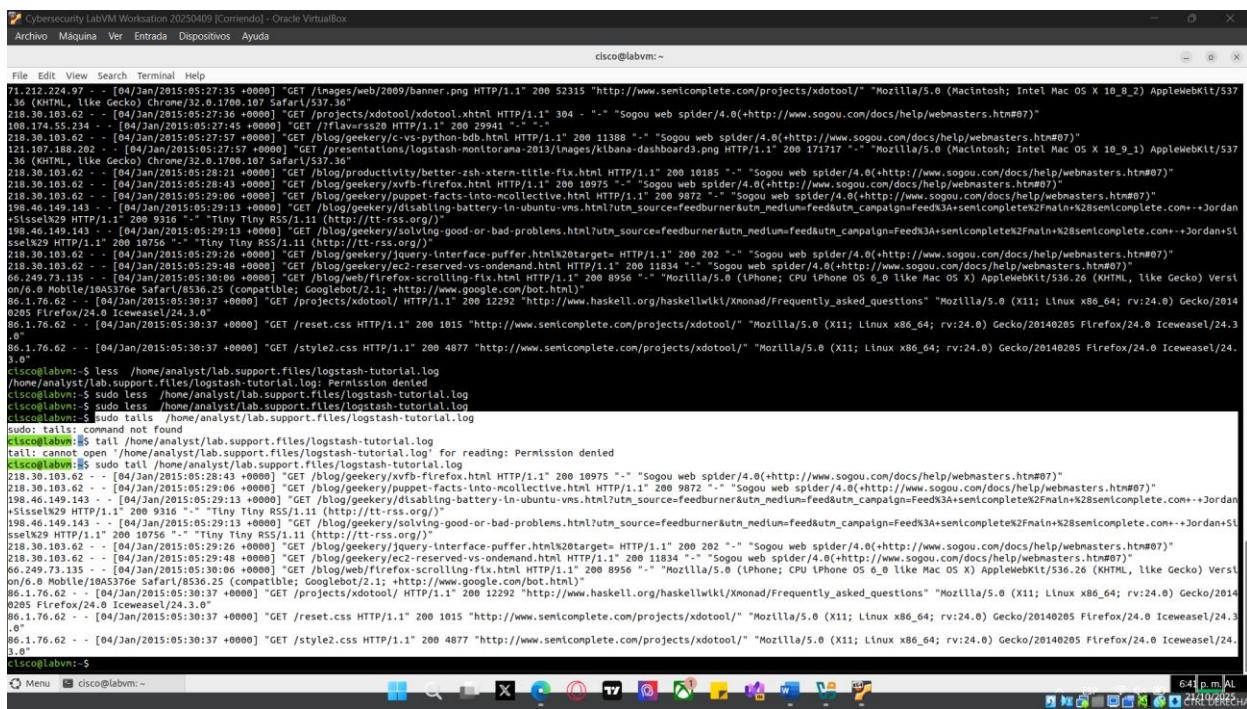
- e. El comando **tail** muestra el final de un archivo de texto. De manera predeterminada, **tail** muestra las últimas diez líneas del archivo.

Utilicen 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
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.com/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(+http://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_campaign=Feed%3A+semicomplete%2Fmai
n+%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_campaign=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/2015:05:29:26 +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)"
66.249.73.135 - - [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)"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /projects/xdotool/ HTTP/1.1" 200
12292 "http://www.haskell.org/haskellwiki/Xmonad/Frequently_asked_questions"
```

Práctica de laboratorio: Leer archivos de registro de un servidor

```
"Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0
Iceweasel/24.3.0"
86.1.76.62 - - [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; Linux x86_64;
rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
86.1.76.62 - - [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; Linux x86_64;
rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
```



```
71.212.224.91 - - [04/Jan/2015:05:27:35 +0000] "GET /images/web/2009/banner.png HTTP/1.1" 200 52315 "http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1790.107 Safari/537.36"
218.30.103.62 - - [04/Jan/2015:05:27:35 +0000] "GET /projects/xdotool/xdotool/xdotool/xhtml HTTP/1.1" 304 - "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
108.174.55.234 - - [04/Jan/2015:05:27:45 +0000] "GET /flavours2m HTTP/1.1" 200 29941 "-" "-"
218.30.103.62 - - [04/Jan/2015:05:27:57 +0000] "GET /blog/geekery/c-vs-python-bdb.html HTTP/1.1" 200 173717 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1790.107 Safari/537.36"
218.30.103.62 - - [04/Jan/2015:05:28:04 +0000] "GET /blog/geekery/puppet-facts-into-mcollective.html HTTP/1.1" 200 10975 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:06 +0000] "GET /blog/geekery/disabling-battery-in-ubuntu-vms.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3a+semicomplete%2fmail%28semicomplete.com%2bJordan+51+Iceweasel%29 HTTP/1.1" 200 9316 "-" "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_campaign=Feed%3a+semicomplete.com%2bJordan+51+Iceweasel%29 HTTP/1.1" 200 2015 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
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_campaign=Feed%3a+semicomplete.com%2bJordan+51+Iceweasel%29 HTTP/1.1" 200 4877 "http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/jQuery-interface-puffer.html?utm_target=HTTP/1.1" 200 10975 "-" "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-on-demand.html HTTP/1.1" 200 11834 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
66.249.73.135 - - [04/Jan/2015:05:29:57 +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/10A537e Safari/8536.20 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
86.1.76.62 - - [04/Jan/2015:05:30:06 +0000] "GET /projects/xdotool/xdotool/xhtml HTTP/1.1" 200 12292 "http://www.haskell.org/haskellwiki/Xmonad/Frequently_asked_questions" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
86.1.76.62 - - [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; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
86.1.76.62 - - [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; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
86.1.76.62 - - [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; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
cisco@labvm:~$ less /home/analyst/lab.support.files/logstash-tutorial.log
/home/analyst/lab.support.files/logstash-tutorial.log: Permission denied
cisco@labvm:~$ sudo less /home/analyst/lab.support.files/logstash-tutorial.log
cisco@labvm:~$ sudo less /home/analyst/lab.support.files/logstash-tutorial.log
cisco@labvm:~$ sudo tails /home/analyst/lab.support.files/logstash-tutorial.log
tail: tails: command not found
cisco@labvm:~$ tails /home/analyst/lab.support.files/logstash-tutorial.log
tail: cannot open /home/analyst/lab.support.files/logstash-tutorial.log: Permission denied
cisco@labvm:~$ sudo tails /home/analyst/lab.support.files/logstash-tutorial.log
cisco@labvm:~$ sudo tails /home/analyst/lab.support.files/logstash-tutorial.log: for reading: Permission denied
cisco@labvm:~$ sudo tails /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?utm_target=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/2015:05:29:06 +0000] "GET /blog/geekery/puppet-facts-into-mcollective.html HTTP/1.1" 200 9872 "-" "Sogou web spider/4.0(+http://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_campaign=Feed%3a+semicomplete.com%2bJordan+51+Iceweasel%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?utm_target=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-on-demand.html HTTP/1.1" 200 11834 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
66.249.73.135 - - [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/10A537e Safari/8536.20 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /projects/xdotool/xdotool/xhtml HTTP/1.1" 200 12292 "http://www.haskell.org/haskellwiki/Xmonad/Frequently_asked_questions" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
86.1.76.62 - - [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; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
86.1.76.62 - - [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; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
cisco@labvm:~$
```

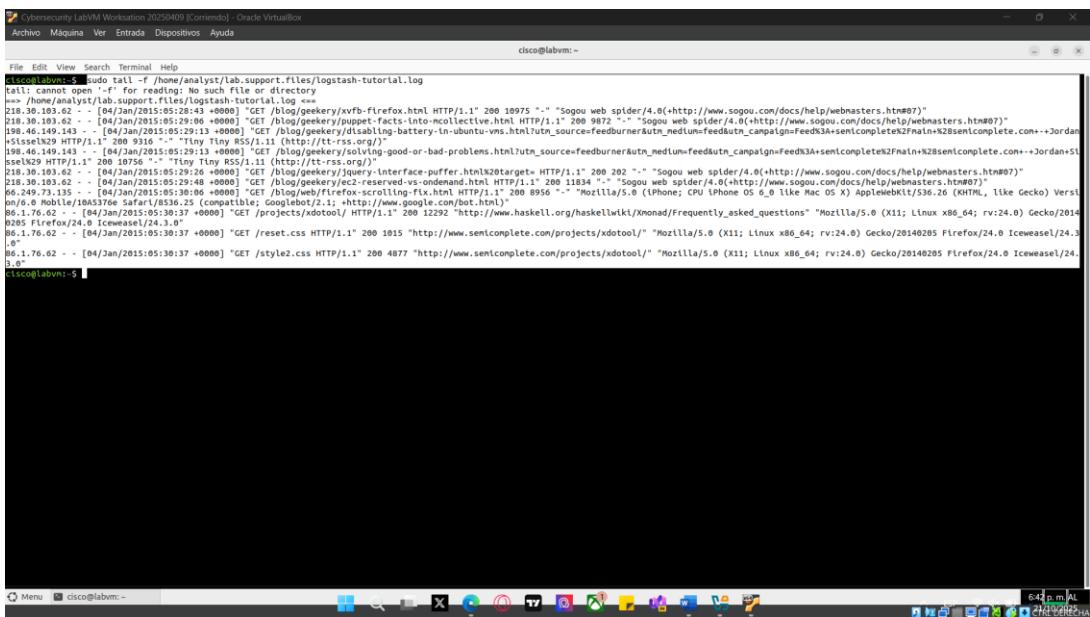
Paso 2: Seguir archivos de registro en forma activa

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.

- Utilicen tail -f para monitorear en forma activa el contenido del archivo **/var/log/syslog**:

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

Práctica de laboratorio: Leer archivos de registro de un servidor



The screenshot shows a terminal window titled "cisco@labvm: ~" running on Oracle VirtualBox. The command "tail -f /home/analyst/lab.support.files/logstash-tutorial.log" is being run. The output displays several log entries from a log file. The log entries include timestamps, IP addresses, user agents, and URLs. Some entries are from search engines like Google and Sogou. The log file also contains entries from a feedburner campaign and various browser versions. The terminal window has a black background with white text and a standard Linux-style menu bar at the top.

```
cisco@labvm: ~
tail -f /home/analyst/lab.support.files/logstash-tutorial.log
tail: cannot open '/home/analyst/lab.support.files/logstash-tutorial.log': No such file or directory
[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.com/docs/help/webmasters.htm#07)"
[218.39.103.02 - - [04/Jan/2015:05:29:06 +0000] "GET /blog/geekery/your-facts-into-mecollective.html HTTP/1.1" 200 9872 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
[198.46.149.143 - - [04/Jan/2015:05:29:08 +0000] "GET /blog/geekery/disabling-battery-in-ubuntu-vms.html?utm_source=feedburner&utm_medium=feedburner&utm_campaign=Feed%3A+sentcomplete2%2Fmain%2Bsentcomplete.com+-+Jordan+St+Jesse%29 HTTP/1.1" 200 9316 "-" "Tiny Tiny RSS/1.11 (http://tt-rss.org/)"
[198.46.149.143 - - [04/Jan/2015:05:29:11 +0000] "GET /blog/geekery/solving-good-or-bad-problems.html?utm_source=feedburner&utm_medium=feedburner&utm_campaign=Feed%3A+sentcomplete2%2Fmain%2Bsentcomplete.com+-+Jordan+St+Jesse%29 HTTP/1.1" 200 10756 "-" "Tiny Tiny RSS/1.11 (http://tt-rss.org/)"
[218.39.103.02 - - [04/Jan/2015:05:29:24 +0000] "GET /blog/geekery/interface-puffer.html?utm_target= HTTP/1.1" 200 202 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
[218.39.103.02 - - [04/Jan/2015:05:29:48 +0000] "GET /blog/geekery/ec2-reserved-vs-on-demand.html HTTP/1.1" 200 11834 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
[66.249.73.135 - - [04/Jan/2015:05:30:06 +0000] "GET /blog/web/firefox-scrolling-fx.html HTTP/1.1" 200 8956 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6.0 like Mac OS X) AppleWebKit/604.1.38 (KHTML, like Gecko) Version/6.0 Mobile Safari/10237.1"
[66.1.76.62 - - [04/Jan/2015:05:30:25 +0000] "(compatible; Googlebot/2.1; http://www.google.com/bot.html)"
[66.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /projects/xdotool/ HTTP/1.1" 200 1225 "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20100101 Firefox/24.0 Iceweasel/24.0 Firefox/24.0 Iceweasel/24.0"
[66.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /reset.css HTTP/1.1" 200 1015 "http://www.sentcomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20100101 Firefox/24.0 Iceweasel/24.0 Firefox/24.0 Iceweasel/24.0"
[66.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /style2.css HTTP/1.1" 200 4877 "http://www.sentcomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20100101 Firefox/24.0 Iceweasel/24.0 Firefox/24.0 Iceweasel/24.0"
```

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

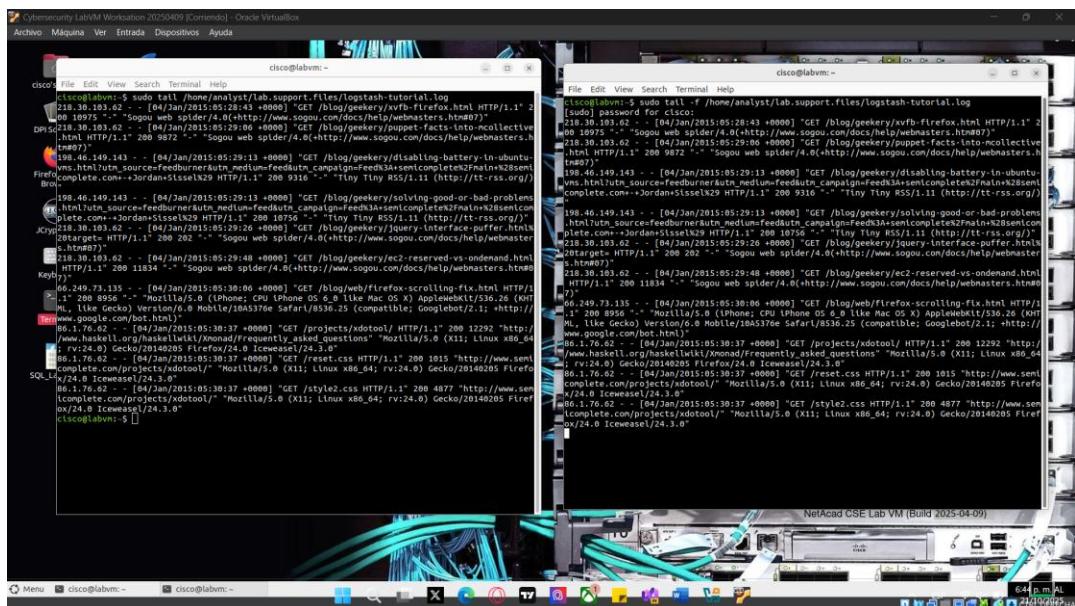
tail muestra las últimas N líneas (por defecto 10) y finaliza. tail -f muestra las últimas líneas y además permanece en ejecución, mostrando en tiempo real cualquier nueva línea que se agregue al archivo hasta que lo detengas (Ctrl+C).

- b. Abran una segunda ventana del terminal para ver tail -f en acción. Organicen la pantalla de modo que puedan ver ambas ventanas del terminal. Cambien el tamaño de las ventanas para poder verlas a la vez, tal como se muestra en la siguiente imagen:

En la ventana del terminal de arriba se está ejecutando **tail -f** para monitorear el archivo **/home/analyst/lab.support.files/logstash-tutorial.log**. Utilicen la ventana del terminal de abajo para agregar información al archivo monitoreado.

Para simplificar la visualización, seleccionen la ventana del terminal de arriba (donde se está ejecutando **tail -f**) y presionen Intro un par de veces. Con esto se agregarán algunas líneas entre el contenido actual del archivo y la información nueva que se debe sumar.

Práctica de laboratorio: Leer archivos de registro de un servidor

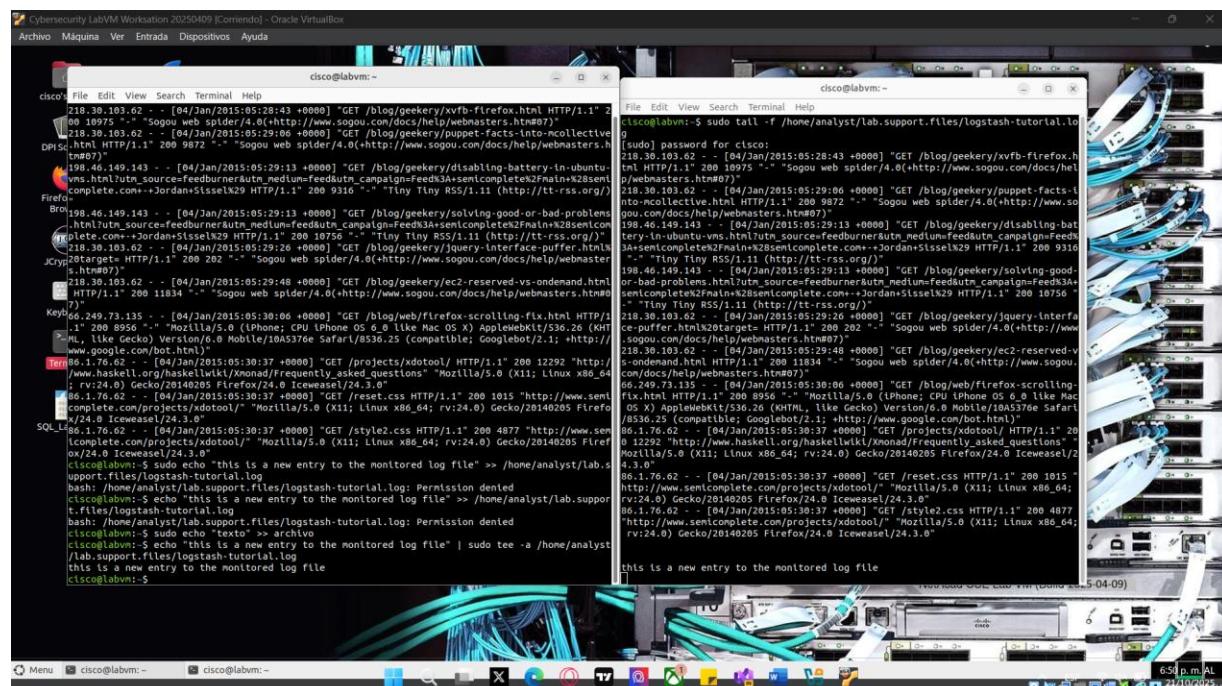


- c. Seleccionen la ventana del terminal de abajo e introduzcan el siguiente comando:

```
[analyst@secOps ~]$ echo "this is a new entry to the monitored log file" >> lab.support.files/logstash-tutorial.log
```

El comando anterior anexa el mensaje "this is a new entry to the monitored log file" ("esta es una entrada nueva que se agrega al archivo de registro monitoreado") al archivo **/home/analyst/lab.support.files/logstash-tutorial.log**. Como tail -f está monitoreando el archivo en ese momento, se agregar una línea al archivo. En la ventana de arriba debería aparecer la línea nueva en tiempo real.

- d. Presionen CTRL + C para detener la ejecución de **tail -f** y regresar al cursor del shell.
e. Cierren una de las dos ventanas del terminal.



Parte 2: Archivos de registro y Syslog

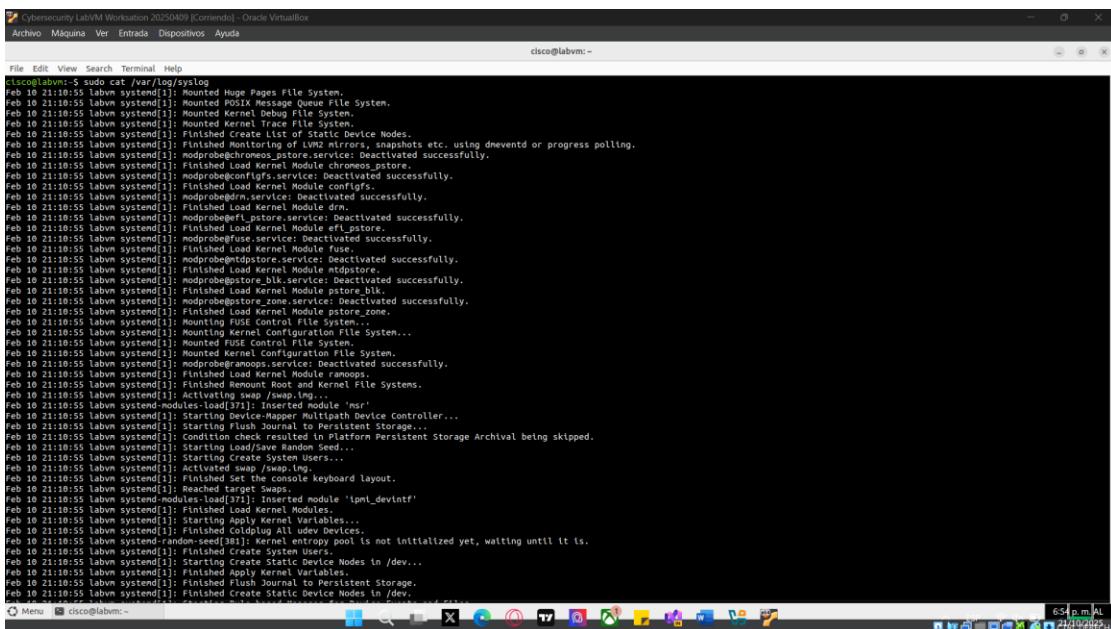
Debido a su importancia, es común concentrar archivos de registro en una computadora de monitoreo. **Syslog** es un sistema diseñado para permitir que los dispositivos envíen sus archivos de registro a un servidor centralizado, que se conoce como servidor **syslog**. Los clientes se comunican con un servidor syslog por medio del protocolo **syslog**. La implementación de **Syslog** es generalizada y admite prácticamente todas las plataformas informáticas.

La VM Security Worstation genera archivos de registro al nivel del sistema operativo y se los entrega a **syslog**.

- a. Utilice el comando **cat** como usuario **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**.

```
analyst@secOps ~$ sudo cat /var/log/syslog.1
[sudo] contraseña para analyst:
Feb 7 13:23:15 secOps kernel: [ 5.458959] psmouse serio1: hgpk: ID: 10 00 64
Feb 7 13:23:15 secOps kernel: [ 5.467285] input: ImExPS/2 BYD TouchPad as
/devices/platform/i8042/serio1/input/input6
Feb 7 13:23:15 secOps kernel: [ 5.502469] RAPL PMU: API unit is 2^-32 Joules, 4 fixed
counters, 10737418240 ms ovfl timer
Feb 7 13:23:15 secOps kernel: [ 5.502476] RAPL PMU: hw unit of domain pp0-core 2^-0
Joules
Feb 7 13:23:15 secOps kernel: [ 5.502478] RAPL PMU: hw unit of domain package 2^-0
Joules
Feb 7 13:23:15 secOps kernel: [ 5.502479] RAPL PMU: hw unit of domain dram 2^-0 Joules
Feb 7 13:23:15 secOps kernel: [ 5.502480] RAPL PMU: hw unit of domain pp1-gpu 2^-0
Joules
Feb 7 13:23:15 secOps kernel: [ 5.672547] ppdev: user-space parallel port driver
Feb 7 13:23:15 secOps kernel: [ 5.709000] pcnet32 0000:00:03.0 enp0s3: renamed from
eth0
Feb 7 13:23:16 secOps kernel: [ 6.166738] pcnet32 0000:00:03.0 enp0s3: link up,
100Mbps, full-duplex
Feb 7 13:23:16 secOps kernel: [ 6.706058] random: crng init done
Feb 7 13:23:18 secOps kernel: [ 8.318984] floppy0: no floppy controllers found
Feb 7 13:23:18 secOps kernel: [ 8.319028] work still pending
Feb 7 14:26:35 secOps kernel: [ 3806.118242] hrtimer: interrupt took 4085149 ns
Feb 7 15:02:13 secOps kernel: [ 5943.582952] pcnet32 0000:00:03.0 enp0s3: link down
Feb 7 15:02:19 secOps kernel: [ 5949.556153] pcnet32 0000:00:03.0 enp0s3: link up,
100Mbps, full-duplex
```

Práctica de laboratorio: Leer archivos de registro de un servidor



```
cisco@labvm:~$ sudo cat /var/log/syslog
Feb 10 21:10:55 labvm systemd[1]: Mounted huge Pages File System.
Feb 10 21:10:55 labvm systemd[1]: Mounted /etc/pxe/pxelinux.0 File System.
Feb 10 21:10:55 labvm systemd[1]: Mounted Kernel Debug File System.
Feb 10 21:10:55 labvm systemd[1]: Mounted Kernel Trace File System.
Feb 10 21:10:55 labvm systemd[1]: Finished Create List of Static Device Nodes.
Feb 10 21:10:55 labvm systemd[1]: Starting Load Kernel Modules etc. using dmeventd or progress polling.
Feb 10 21:10:55 labvm systemd[1]: modprobechromess_pstore.service: Deactivated successfully.
Feb 10 21:10:55 labvm systemd[1]: Finished Load Kernel Module chromes_pstore.
Feb 10 21:10:55 labvm systemd[1]: modprobeconfigfs.service: Deactivated successfully.
Feb 10 21:10:55 labvm systemd[1]: modprobeconfigfs.service: Deactivated successfully.
Feb 10 21:10:55 labvm systemd[1]: modprobedrm.service: Deactivated successfully.
Feb 10 21:10:55 labvm systemd[1]: Finished Load Kernel Module drm.
Feb 10 21:10:55 labvm systemd[1]: modprobeefi_pstore.service: Deactivated successfully.
Feb 10 21:10:55 labvm systemd[1]: modprobeefi_pstore.service: Deactivated successfully.
Feb 10 21:10:55 labvm systemd[1]: modprobefuse.service: Deactivated successfully.
Feb 10 21:10:55 labvm systemd[1]: Finished Load Kernel Module fuse.
Feb 10 21:10:55 labvm systemd[1]: modprobegptstore.service: Deactivated successfully.
Feb 10 21:10:55 labvm systemd[1]: Finished Load Kernel Module gptstore.
Feb 10 21:10:55 labvm systemd[1]: modprobepstore blk.service: Deactivated successfully.
Feb 10 21:10:55 labvm systemd[1]: Finished Load Kernel Module pstore_blk.
Feb 10 21:10:55 labvm systemd[1]: modprobepstore _zone.service: Deactivated successfully.
Feb 10 21:10:55 labvm systemd[1]: Finished Load Kernel Module pstore_Zone.
Feb 10 21:10:55 labvm systemd[1]: Mounting Kernel Configuration File System...
Feb 10 21:10:55 labvm systemd[1]: Mounting Kernel Configuration File System...
Feb 10 21:10:55 labvm systemd[1]: mounted Kernel Configuration File System.
Feb 10 21:10:55 labvm systemd[1]: modproberamoops.service: Deactivated successfully.
Feb 10 21:10:55 labvm systemd[1]: Finished Load Kernel Module ramoops.
Feb 10 21:10:55 labvm systemd[1]: Activating swap /var/swap...
Feb 10 21:10:55 labvm systemd-modules-load[371]: Inserted module 'msr'
Feb 10 21:10:55 labvm systemd[1]: Starting Device-Mapper Multipath Device Controller...
Feb 10 21:10:55 labvm systemd[1]: Condition check resulted in Platform Persistent Storage being skipped.
Feb 10 21:10:55 labvm systemd[1]: Starting Load/Save Random Seed...
Feb 10 21:10:55 labvm systemd[1]: Starting Create System Users...
Feb 10 21:10:55 labvm systemd[1]: /etc/init.d/kmod start...
Feb 10 21:10:55 labvm systemd[1]: Finished Set the console keyboard layout.
Feb 10 21:10:55 labvm systemd[1]: Reached target Swap.
Feb 10 21:10:55 labvm systemd-modules-load[371]: Inserted module 'ipmi_devintf'
Feb 10 21:10:55 labvm systemd[1]: Starting Apply Kernel Variables...
Feb 10 21:10:55 labvm systemd[1]: Finished Coldplug All udev Devices.
Feb 10 21:10:55 labvm systemd-random-seed[981]: Kernel entropy pool is not initialized yet, waiting until it is.
Feb 10 21:10:55 labvm systemd[1]: Starting Create Static Device Nodes in /dev...
Feb 10 21:10:55 labvm systemd[1]: Finished Apply Kernel Variables.
Feb 10 21:10:55 labvm systemd[1]: Finished Flush Journal to Persistent Storage.
Feb 10 21:10:55 labvm systemd[1]: Finished Create Static Device Nodes in /dev...
```

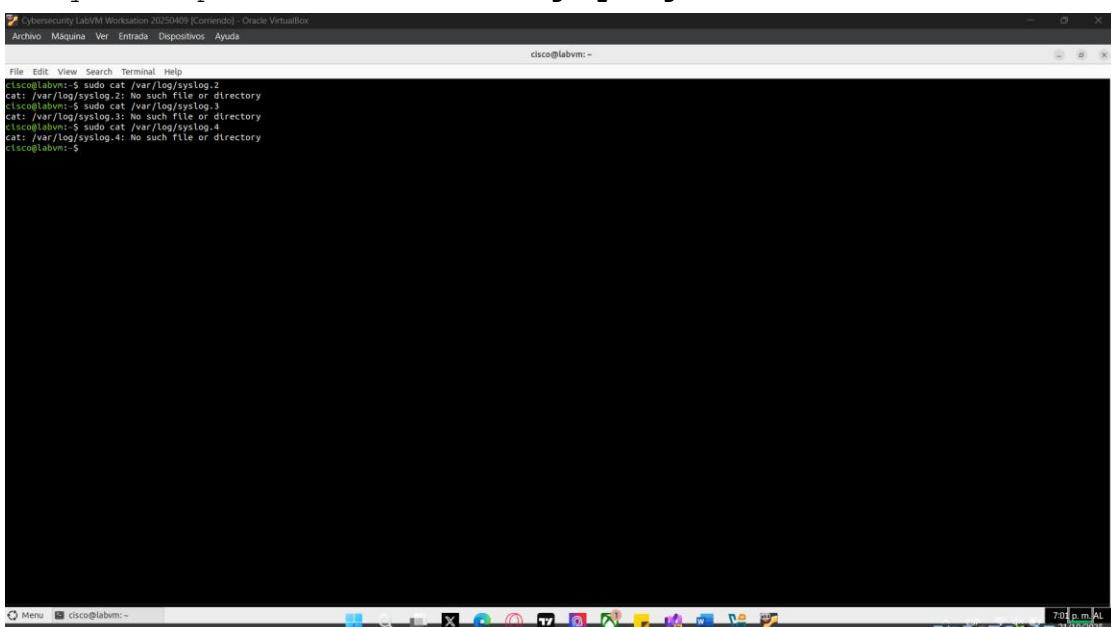
¿Por qué se tuvo que ejecutar el comando **cat** como usuario **root**?

Se tuvo que ejecutar el comando **cat** como usuario **root** porque muchos archivos de registro del sistema, como los que están en **/var/log/**, tienen permisos restringidos por razones de seguridad.

- b. Observen que el archivo **/var/log/syslog** solo almacena las entradas de registro más recientes. Para que el archivo de syslog no se extienda demasiado, el sistema operativo rota periódicamente los archivos de registro y les cambia el nombre a los más antiguos por **syslog.1**, **syslog.2**, y así sucesivamente.

Utilicen el comando **cat** para generar una lista de archivos de **syslog** más antiguos:

```
analyst@secOps ~$ sudo cat /var/log/syslog.2
analyst@secOps ~$ sudo cat /var/log/syslog.3
analyst@secOps ~$ sudo cat /var/log/syslog.4
```



```
cisco@labvm:~$ sudo cat /var/log/syslog.2
cat: /var/log/syslog.2: No such file or directory
cisco@labvm:~$ sudo cat /var/log/syslog.3
cat: /var/log/syslog.3: No such file or directory
cisco@labvm:~$ sudo cat /var/log/syslog.4
cat: /var/log/syslog.4: No such file or directory
cisco@labvm:~$
```

¿Puede pensar en algún motivo por el cual es importante mantener sincronizadas la fecha y la hora de las computadoras?

una hora precisa y sincronizada garantiza que los registros sean confiables y coherentes en toda la red.

Parte 3: Archivos de registro y Journalctl

Otro sistema de administración de registros muy utilizado se conoce como **journal**. Administrador por el daemon **journald**, el sistema está diseñado para centralizar la administración de archivos de registro independientemente de dónde se estén originando los mensajes. En el contexto de esta práctica de laboratorio, la característica más evidente del daemon del sistema **journal** es el uso de archivos binarios "append-only" (solo anexar) que actúan como sus **archivos de registro**.

Paso 1: Ejecutar journalctl sin opciones.

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

```
analyst@secOps ~$ journalctl
-- Logs begin at Fri 2014-09-26 14:13:12 EDT, end at Tue 2017-02-07 13:23:29 ES
Sep 26 14:13:12 dataAnalyzer systemd[1087]: Starting Paths.
Sep 26 14:13:12 dataAnalyzer systemd[1087]: Reached target Paths.
Sep 26 14:13:12 dataAnalyzer systemd[1087]: Starting Timers.
Sep 26 14:13:12 dataAnalyzer systemd[1087]: Reached target Timers.
Sep 26 14:13:12 dataAnalyzer systemd[1087]: Starting Sockets.
Sep 26 14:13:12 dataAnalyzer systemd[1087]: Reached target Sockets.
Sep 26 14:13:12 dataAnalyzer systemd[1087]: Starting Basic System.
Sep 26 14:13:12 dataAnalyzer systemd[1087]: Reached target Basic System.
Sep 26 14:13:12 dataAnalyzer systemd[1087]: Starting Default.
Sep 26 14:13:12 dataAnalyzer systemd[1087]: Reached target Default.
Sep 26 14:13:12 dataAnalyzer systemd[1087]: Startup finished in 18ms.
Sep 26 14:14:24 dataAnalyzer systemd[1087]: Stopping Default.
Sep 26 14:14:24 dataAnalyzer systemd[1087]: Stopped target Default.
Sep 26 14:14:24 dataAnalyzer systemd[1087]: Stopping Basic System.
Sep 26 14:14:24 dataAnalyzer systemd[1087]: Stopped target Basic System.
Sep 26 14:14:24 dataAnalyzer systemd[1087]: Stopping Paths.
Sep 26 14:14:24 dataAnalyzer systemd[1087]: Stopped target Paths.
Sep 26 14:14:24 dataAnalyzer systemd[1087]: Stopping Timers.
Sep 26 14:14:24 dataAnalyzer systemd[1087]: Stopped target Timers.
Sep 26 14:14:24 dataAnalyzer systemd[1087]: Stopping Sockets.
<output omitted>
```

Nota: Si se ejecuta journalctl como usuario root se mostrará información más detallada.

- Presionen CTRL+C para salir de la pantalla.

Práctica de laboratorio: Leer archivos de registro de un servidor

```
Cybersecurity LabVM Workstation 20250403 [Clement] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
cisco@labvm: ~

File Edit View Search Terminal Help
cisco@labvm: ~ $ journalctl
Hint: You are currently seeing messages from other users and the system.
      The command 'sudo -s' or 'systemctl journalctl' can see all messages.
      Pass -t to turn off this notice.

Feb 10 21:25:19 labvm dbus-daemon[72395]: [session uid=1001 pid=72395] AppArmor D-Bus mediation is enabled
Feb 10 21:25:19 labvm dbus-daemon[72395]: [session uid=1001 pid=72395] Activating service name='ca.desrt.dconf' requested by ':1.0' (uid=1001 pid=72395 comm='dconf load /' label='unconfined')
Feb 10 21:25:19 labvm dbus-daemon[72395]: [session uid=1001 pid=72395] Successfully activated service 'ca.desrt.dconf'
Feb 10 21:27:44 labvm dbus-daemon[72395]: [session uid=1001 pid=72395] Reloading configuration
Feb 10 21:27:44 labvm dbus-daemon[72395]: [session uid=1001 pid=72395] Reloaded configuration
Feb 10 21:27:44 labvm dbus-daemon[72395]: [session uid=1001 pid=72395] Reloading configuration
Feb 10 21:27:44 labvm dbus-daemon[72395]: [session uid=1001 pid=72395] Reloaded configuration
Feb 10 21:27:44 labvm dbus-daemon[72395]: [session uid=1001 pid=72395] Reloading configuration
Feb 10 21:27:44 labvm dbus-daemon[72395]: [session uid=1001 pid=72395] Reloaded configuration
Feb 10 21:30:06 labvm dbus-daemon[72395]: [session uid=1001 pid=72395] Reloading configuration
Feb 10 21:30:06 labvm dbus-daemon[72395]: [session uid=1001 pid=72395] Reloaded configuration
Oct 21 04:26:46 labvm systemd[1157]: Reached target User Application Slice.
Oct 21 04:26:46 labvm systemd[1157]: Created slice User Core System Slice.
Oct 21 04:26:46 labvm systemd[1157]: Reached target Paths.
Oct 21 04:26:46 labvm systemd[1157]: Starting D-Bus User Message Bus Socket...
Oct 21 04:26:46 labvm systemd[1157]: Listening on GnuPG network certificate management daemon.
Oct 21 04:26:46 labvm systemd[1157]: Listening on GnuPG cryptographic agent and passphrase cache (access for web browsers).
Oct 21 04:26:46 labvm systemd[1157]: Listening on GnuPG cryptographic agent and passphrase cache (restricted).
Oct 21 04:26:46 labvm systemd[1157]: Listening on GnuPG cryptographic agent (ssh-agent emulation).
Oct 21 04:26:46 labvm systemd[1157]: Listening on GnuPG cryptographic agent and passphrase cache.
Oct 21 04:26:46 labvm systemd[1157]: Listening on PulseAudio Shared Memory Socket.
Oct 21 04:26:46 labvm systemd[1157]: Listening on Sound System.
Oct 21 04:26:46 labvm systemd[1157]: Listening on Speed Dispatcher Socket.
Oct 21 04:26:46 labvm systemd[1157]: Listening on D-Bus User Message Bus Socket.
Oct 21 04:26:46 labvm systemd[1157]: Reached target Basic System.
Oct 21 04:26:46 labvm systemd[1157]: Starting Sound Service.
Oct 21 04:26:46 labvm systemd[1157]: Started PulseAudio Shared Memory Bus.
Oct 21 04:26:46 labvm dbus-daemon[1171]: [session uid=1001 pid=1171] AppArmor D-Bus mediation is enabled
Oct 21 04:26:46 labvm pulseaudio[1164]: Disabling timer-based scheduling because running inside a VM
Oct 21 04:26:46 labvm pulseaudio[1164]: Disabling timer-based scheduling because running inside a VM
Oct 21 04:26:46 labvm pulseaudio[1164]: Failed to read authentication key '/home/cisco/.config/pulse/cookie': No such file or directory
Oct 21 04:26:46 labvm pulseaudio[1164]: Failed to read authentication key '/home/cisco/.pulse-cookie': No such file or directory
Oct 21 04:26:46 labvm pulseaudio[1164]: Failed to load authentication key '/home/cisco/.pulse-cookie': No such file or directory
Oct 21 04:26:46 labvm pulseaudio[1164]: Failed to read authentication key '/home/cisco/.pulse-cookie': No such file or directory
Oct 21 04:26:46 labvm pulseaudio[1164]: Failed to load authentication key '/home/cisco/.pulse-cookie': No such file or directory
Oct 21 04:26:46 labvm pulseaudio[1164]: Reached target PulseAudio Service.
Oct 21 04:26:46 labvm pulseaudio[1164]: Reached Target Main User Target.
Oct 21 04:26:46 labvm systemd[1157]: Startup finished in 17ms.
Oct 21 04:26:46 labvm org.freedesktop.Notifications[1170]: [session uid=1001 pid=1308 comm='/usr/bin/vBoxClient --checkhvVersion' label='unconfined'] Activating service name='org.freedesktop.Notifications' requested by ':1.0' (uid=1001 pid=1308 comm='/usr/bin/vBoxClient --checkhvVersion' label='unconfined')
Oct 21 04:26:46 labvm org.gtk.vfs.Daemon[1171]: [session uid=1001 pid=1171] Activating via systemd: service name='org.gtk.vfs.Daemon' requested by ':1.0' (uid=1001 pid=1171 comm='org.gtk.vfs.Daemon' label='unconfined')
Oct 21 04:26:46 labvm org.gtk.vfs.Daemon[1171]: [session uid=1001 pid=1171] Successfully activated service 'org.gtk.vfs.Daemon'
Oct 21 04:26:46 labvm org.sshd[1172]: [session uid=1001 pid=1172] Activating via systemd: service name='org.sshd' requested by ':1.0' (uid=1001 pid=1172 comm='org.sshd' label='unconfined')
Oct 21 04:26:46 labvm org.sshd[1172]: [session uid=1001 pid=1172] Successfully activated service 'org.sshd'.
Oct 21 04:26:46 labvm org.libnats[1173]: [session uid=1001 pid=1173] Activating via systemd: service name='org.libnats' requested by ':1.0' (uid=1001 pid=1173 comm='org.libnats' label='unconfined')
Oct 21 04:26:46 labvm org.libnats[1173]: [session uid=1001 pid=1173] Successfully activated service 'org.libnats'.
Oct 21 04:26:46 labvm org.accessibility[1174]: [session uid=1001 pid=1174] Activating via systemd: service name='org.accessibility' requested by ':1.0' (uid=1001 pid=1174 comm='org.accessibility' label='unconfined')
Oct 21 04:26:46 labvm org.accessibility[1174]: [session uid=1001 pid=1174] Successfully activated service 'org.accessibility'.
Oct 21 04:26:46 labvm org.aishiibus[1175]: [session uid=1001 pid=1175] Activating via systemd: service name='org.aishiibus' requested by ':1.0' (uid=1001 pid=1175 comm='org.aishiibus' label='unconfined')
Oct 21 04:26:46 labvm org.aishiibus[1175]: [session uid=1001 pid=1175] Successfully activated service 'org.aishiibus'.
cisco@labvm: ~
```

Paso 2: Journalctl y algunas opciones

Parte de las ventajas de utilizar **journald** radica en sus opciones. Para los siguientes comandos, utilice **CRTL+C** para salir de la pantalla.

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

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

```
Cybersecurity LabVM Workstation 20200409 (Coronado) - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
cisco@labvm: ~

File Edit View Search Terminal Help

lscpu
Linux labvm 5.5.0-50-generic #20-Ubuntu SMP Fri Jan 28 14:29:49 UTC 2022
Build ID: 00000000000000000000000000000000
Processor: Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz
CPU op-mode(s): 32-bit, 64-bit
Byte Order: Little Endian
CPU(s): 12
Thread(s) per core: 2
Core(s) per socket: 6
Socket(s): 1
Hyper-threading: Enabled
L1 Cache: 32K x 8
L2 Cache: 256K x 8
L3 Cache: 16MB x 1
NUMA nodes: 1
Vendor ID: GenuineIntel
CPU family: 6
Model: 107
Model name: Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz
Stepping: 1
Processor ID: 00000000000000000000000000000000
CPU signature: 00000000000000000000000000000000
CPU MHz: 2600.000
BogoMIPS: 5199.99
Flags: fpu vme de pse tsc msr pae mce cx8 apic mmx fxsr sse sse2 sse3 sse4_1 sse4_2 ssse3 sse4_3 sse4 sse5 sse6 sse7 sse8 sse9 sse10 sse11 sse12 sse13 sse14 sse15 sse16 sse17 sse18 sse19 sse100 sse101 sse102 sse103 sse104 sse105 sse106 sse107 sse108 sse109 sse1010 sse1011 sse1012 sse1013 sse1014 sse1015 sse1016 sse1017 sse1018 sse1019 sse10100 sse10110 sse10120 sse10130 sse10140 sse10150 sse10160 sse10170 sse10180 sse10190 sse101000 sse101100 sse101200 sse101300 sse101400 sse101500 sse101600 sse101700 sse101800 sse101900 sse1010000 sse1011000 sse1012000 sse1013000 sse1014000 sse1015000 sse1016000 sse1017000 sse1018000 sse1019000 sse10100000 sse10110000 sse10120000 sse10130000 sse10140000 sse10150000 sse10160000 sse10170000 sse10180000 sse10190000 sse101000000 sse101100000 sse101200000 sse101300000 sse101400000 sse101500000 sse101600000 sse101700000 sse101800000 sse101900000 sse1010000000 sse1011000000 sse1012000000 sse1013000000 sse1014000000 sse1015000000 sse1016000000 sse1017000000 sse1018000000 sse1019000000 sse10100000000 sse10110000000 sse10120000000 sse10130000000 sse10140000000 sse10150000000 sse10160000000 sse10170000000 sse10180000000 sse10190000000 sse101000000000 sse101100000000 sse101200000000 sse101300000000 sse101400000000 sse101500000000 sse101600000000 sse101700000000 sse101800000000 sse101900000000 sse1010000000000 sse1011000000000 sse1012000000000 sse1013000000000 sse1014000000000 sse1015000000000 sse1016000000000 sse1017000000000 sse1018000000000 sse1019000000000 sse10100000000000 sse10110000000000 sse10120000000000 sse10130000000000 sse10140000000000 sse10150000000000 sse10160000000000 sse10170000000000 sse10180000000000 sse10190000000000 sse101000000000000 sse101100000000000 sse101200000000000 sse101300000000000 sse101400000000000 sse101500000000000 sse101600000000000 sse101700000000000 sse101800000000000 sse101900000000000 sse1010000000000000 sse1011000000000000 sse1012000000000000 sse1013000000000000 sse1014000000000000 sse1015000000000000 sse1016000000000000 sse1017000000000000 sse1018000000000000 sse1019000000000000 sse10100000000000000 sse10110000000000000 sse10120000000000000 sse10130000000000000 sse10140000000000000 sse10150000000000000 sse10160000000000000 sse10170000000000000 sse10180000000000000 sse10190000000000000 sse101000000000000000 sse101100000000000000 sse101200000000000000 sse101300000000000000 sse101400000000000000 sse101500000000000000 sse101600000000000000 sse101700000000000000 sse101800000000000000 sse101900000000000000 sse1010000000000000000 sse1011000000000000000 sse1012000000000000000 sse1013000000000000000 sse1014000000000000000 sse1015000000000000000 sse1016000000000000000 sse1017000000000000000 sse1018000000000000000 sse1019000000000000000 sse10100000000000000000 sse10110000000000000000 sse10120000000000000000 sse10130000000000000000 sse10140000000000000000 sse10150000000000000000 sse10160000000000000000 sse10170000000000000000 sse10180000000000000000 sse10190000000000000000 sse101000000000000000000 sse101100000000000000000 sse101200000000000000000 sse101300000000000000000 sse101400000000000000000 sse101500000000000000000 sse101600000000000000000 sse101700000000000000000 sse101800000000000000000 sse101900000000000000000 sse1010000000000000000000 sse1011000000000000000000 sse1012000000000000000000 sse1013000000000000000000 sse1014000000000000000000 sse1015000000000000000000 sse1016000000000000000000 sse1017000000000000000000 sse1018000000000000000000 sse1019000000000000000000 sse10100000000000000000000 sse10110000000000000000000 sse10120000000000000000000 sse10130000000000000000000 sse10140000000000000000000 sse10150000000000000000000 sse10160000000000000000000 sse10170000000000000000000 sse10180000000000000000000 sse10190000000000000000000 sse101000000000000000000000 sse101100000000000000000000 sse101200000000000000000000 sse101300000000000000000000 sse101400000000000000000000 sse101500000000000000000000 sse101600000000000000000000 sse101700000000000000000000 sse101800000000000000000000 sse101900000000000000000000 sse1010000000000000000000000 sse1011000000000000000000000 sse1012000000000000000000000 sse1013000000000000000000000 sse1014000000000000000000000 sse1015000000000000000000000 sse1016000000000000000000000 sse1017000000000000000000000 sse1018000000000000000000000 sse1019000000000000000000000 sse10100000000000000000000000 sse10110000000000000000000000 sse10120000000000000000000000 sse10130000000000000000000000 sse10140000000000000000000000 sse10150000000000000000000000 sse10160000000000000000000000 sse10170000000000000000000000 sse10180000000000000000000000 sse10190000000000000000000000 sse101000000000000000000000000 sse101100000000000000000000000 sse101200000000000000000000000 sse101300000000000000000000000 sse101400000000000000000000000 sse101500000000000000000000000 sse101600000000000000000000000 sse101700000000000000000000000 sse101800000000000000000000000 sse101900000000000000000000000 sse1010000000000000000000000000 sse1011000000000000000000000000 sse1012000000000000000000000000 sse1013000000000000000000000000 sse1014000000000000000000000000 sse1015000000000000000000000000 sse1016000000000000000000000000 sse1017000000000000000000000000 sse1018000000000000000000000000 sse1019000000000000000000000000 sse10100000000000000000000000000 sse10110000000000000000000000000 sse10120000000000000000000000000 sse10130000000000000000000000000 sse10140000000000000000000000000 sse10150000000000000000000000000 sse10160000000000000000000000000 sse10170000000000000000000000000 sse10180000000000000000000000000 sse10190000000000000000000000000 sse101000000000000000000000000000 sse101100000000000000000000000000 sse101200000000000000000000000000 sse101300000000000000000000000000 sse101400000000000000000000000000 sse101500000000000000000000000000 sse101600000000000000000000000000 sse101700000000000000000000000000 sse101800000000000000000000000000 sse101900000000000000000000000000 sse1010000000000000000000000000000 sse1011000000000000000000000000000 sse1012000000000000000000000000000 sse1013000000000000000000000000000 sse1014000000000000000000000000000 sse1015000000000000000000000000000 sse1016000000000000000000000000000 sse1017000000000000000000000000000 sse1018000000000000000000000000000 sse1019000000000000000000000000000 sse10100000000000000000000000000000 sse10110000000000000000000000000000 sse10120000000000000000000000000000 sse10130000000000000000000000000000 sse10140000000000000000000000000000 sse10150000000000000000000000000000 sse10160000000000000000000000000000 sse10170000000000000000000000000000 sse10180000000000000000000000000000 sse10190000000000000000000000000000 sse101000000000000000000000000000000 sse101100000000000000000000000000000 sse101200000000000000000000000000000 sse101300000000000000000000000000000 sse101400000000000000000000000000000 sse101500000000000000000000000000000 sse101600000000000000000000000000000 sse101700000000000000000000000000000 sse101800000000000000000000000000000 sse101900000000000000000000000000000 sse1010000000000000000000000000000000 sse1011000000000000000000000000000000 sse1012000000000000000000000000000000 sse1013000000000000000000000000000000 sse1014000000000000000000000000000000 sse1015000000000000000000000000000000 sse1016000000000000000000000000000000 sse1017000000000000000000000000000000 sse1018000000000000000000000000000000 sse1019000000000000000000000000000000 sse10100000000000000000000000000000000 sse10110000000000000000000000000000000 sse10120000000000000000000000000000000 sse10130000000000000000000000000000000 sse10140000000000000000000000000000000 sse10150000000000000000000000000000000 sse10160000000000000000000000000000000 sse10170000000000000000000000000000000 sse10180000000000000000000000000000000 sse10190000000000000000000000000000000 sse101000000000000000000000000000000000 sse101100000000000000000000000000000000 sse101200000000000000000000000000000000 sse101300000000000000000000000000000000 sse101400000000000000000000000000000000 sse101500000000000000000000000000000000 sse101600000000000000000000000000000000 sse101700000000000000000000000000000000 sse101800000000000000000000000000000000 sse101900000000000000000000000000000000 sse1010000000000000000000000000000000000 sse1011000000000000000000000000000000000 sse1012000000000000000000000000000000000 sse1013000000000000000000000000000000000 sse1014000000000000000000000000000000000 sse1015000000000000000000000000000000000 sse1016000000000000000000000000000000000 sse1017000000000000000000000000000000000 sse1018000000000000000000000000000000000 sse1019000000000000000000000000000000000 sse10100000000000000000000000000000000000 sse10110000000000000000000000000000000000 sse10120000000000000000000000000000000000 sse10130000000000000000000000000000000000 sse10140000000000000000000000000000000000 sse10150000000000000000000000000000000000 sse10160000000000000000000000000000000000 sse10170000000000000000000000000000000000 sse10180000000000000000000000000000000000 sse10190000000000000000000000000000000000 sse101000000000000000000000000000000000000 sse101100000000000000000000000000000000000 sse101200000000000000000000000000000000000 sse101300000000000000000000000000000000000 sse101400000000000000000000000000000000000 sse101500000000000000000000000000000000000 sse101600000000000000000000000000000000000 sse101700000000000000000000000000000000000 sse101800000000000000000000000000000000000 sse101900000000000000000000000000000000000 sse1010000000000000000000000000000000000000 sse1011000000000000000000000000000000000000 sse1012000000000000000000000000000000000000 sse1013000000000000000000000000000000000000 sse1014000000000000000000000000000000000000 sse1015000000000000000000000000000000000000 sse1016000000000000000000000000000000000000 sse1017000000000000000000000000000000000000 sse1018000000000000000000000000000000000000 sse1019000000000000000000000000000000000000 sse10100000000000000000000000000000000000000 sse10110000000000000000000000000000000000000 sse10120000000000000000000000000000000000000 sse10130000000000000000000000000000000000000 sse10140000000000000000000000000000000000000 sse10150000000000000000000000000000000000000 sse10160000000000000000000000000000000000000 sse10170000000000000000000000000000000000000 sse10180000000000000000000000000000000000000 sse10190000000000000000000000000000000000000 sse101000000000000000000000000000000000000000 sse101100000000000000000000000000000000000000 sse101200000000000000000000000000000000000000 sse101300000000000000000000000000000000000000 sse101400000000000000000000000000000000000000 sse101500000000000000000000000000000000000000 sse101600000000000000000000000000000000000000 sse101700000000000000000000000000000000000000 sse101800000000000000000000000000000000000000 sse101900000000000000000000000000000000000000 sse1010000000000000000000000000000000000000000 sse1011000000000000000000000000000000000000000 sse1012000000000000000000000000000000000000000 sse1013000000000000000000000000000000000000000 sse1014000000000000000000000000000000000000000 sse1015000000000000000000000000000000000000000 sse1016000000000000000000000000000000000000000 sse1017000000000000000000000000000000000000000 sse1018000000000000000000000000000000000000000 sse1019000000000000000000000000000000000000000 sse10100000000000000000000000000000000000000000 sse10110000000000000000000000000000000000000000 sse10120000000000000000000000000000000000000000 sse10130000000000000000000000000000000000000000 sse10140000000000000000000000000000000000000000 sse10150000000000000000000000000000000000000000 sse10160000000000000000000000000000000000000000 sse10170000000000000000000000000000000000000000 sse10180000000000000000000000000000000000000000 sse10190000000000000000000000000000000000000000 sse101000000000000000000000000000000000000000000 sse101100000000000000000000000000000000000000000 sse101200000000000000000000000000000000000000000 sse101300000000000000000000000000000000000000000 sse101400000000000000000000000000000000000000000 sse101500000000000000000000000000000000000000000 sse101600000000000000000000000000000000000000000 sse101700000000000000000000000000000000000000000 sse101800000000000000000000000000000000000000000 sse101900000000000000000000000000000000000000000 sse1010000000000000000000000000000000000000000000 sse1011000000000000000000000000000000000000000000 sse10120000000000000000000000000000000000000000000 sse10130000000000000000000000000000000000000000000 sse10140000000000000000000000000000000000000000000 sse10150000000000000000000000000000000000000000000 sse10160000000000000000000000000000000000000000000 sse10170000000000000000000000000000000000000000000 sse10180000000000000000000000000000000000000000000 sse10190000000000000000000000000000000000000000000 sse101000000000000000000000000000000000000000000000 sse101100000000000000000000000000000000000000000000 sse1012000000000000000000000000000000000000000000000 sse10130000
```

- b. Utilicen **journalctl -b** para mostrar las entradas de registro registradas durante el último arranque:

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

```
Feb 07 08:23:13 secOps systemd-journald[172]: Time spent on flushing to /var is
Feb 07 08:23:13 secOps kernel: Linux version 4.8.12-2-ARCH (builduser@andyrtr)
Feb 07 08:23:13 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 fl
Feb 07 08:23:13 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE re
Feb 07 08:23:13 secOps kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX re
Feb 07 08:23:13 secOps kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]
Feb 07 08:23:13 secOps kernel: x86/fpu: Enabled xstate features 0x7, context si
```

Práctica de laboratorio: Leer archivos de registro de un servidor

```
Feb 07 08:23:13 secOps kernel: x86/fpu: Using 'eager' FPU context switches.  
Feb 07 08:23:13 secOps kernel: e820: BIOS-provided physical RAM map:  
<output omitted>
```

- c. Utilicen **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
```

Cybersecurity LabVM Workstation 20250409 [Comended] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

cisco@labvm: ~

```
cisco@labvm:~$ sudo journalctl -u ssh.service --since today
Oct 21 00:27:42 labvm systemd[1]: Starting OpenSSH Secure Shell server...
Oct 21 00:27:42 labvm sshd[193]: Server listening on :: port 22.
Oct 21 00:27:43 labvm systemd[1]: Started OpenSSH Secure Shell server.
Oct 21 00:27:43 labvm sshd[193]: Server listening on :: port 22.
Oct 21 00:27:43 labvm sshd[193]: Started OpenSSH Secure Shell server.
Oct 21 00:27:43 labvm sshd[193]: Listening on :: port 22.
Oct 21 18:20:09 labvm systemd[1]: Starting OpenSSH Secure Shell server...
Oct 21 18:20:09 labvm sshd[719]: Server listening on 0.0.0.0 port 22.
Oct 21 18:20:09 labvm sshd[719]: Server listening on :: port 22.
Oct 21 18:20:09 labvm sshd[719]: Started OpenSSH Secure Shell server.
-- Boot 552356af1f3b00aa7151c8c850e0ebfb --
Oct 21 19:43:32 labvm systemd[1]: Starting OpenSSH Secure Shell server...
Oct 21 19:43:32 labvm sshd[942]: Server listening on :: port 22.
Oct 21 19:43:32 labvm sshd[942]: Server listening on :: port 22.
Oct 21 19:43:32 labvm systemd[1]: Started OpenSSH Secure Shell server.
cisco@labvm:~$
```

- d. Utilicen el switch **-k** para mostrar solo mensajes generados por el kernel:

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

Práctica de laboratorio: Leer archivos de registro de un servidor

```
cisco@labvm:~$ sudo journalctl -k
Oct 21 18:20:06 labvm kernel: Linux version 3.10.0-60-generic (bullseye@lcy02-andd-054) (gcc (Ubuntu 11.3.0-1ubuntu22.04) 11.3.0, GNU ld (GNU Binutils for Ubuntu) 2.38) #66-Ubuntu SMP Fri Jan 20 14:29:49 UTC 2023
Oct 21 18:20:06 labvm kernel: Command line: root=/dev/vda1 ro quiet splash zswap.enabled=1
Oct 21 18:20:06 labvm kernel: KERNEL supported cpus:
Oct 21 18:20:06 labvm kernel: Intel GenuineIntel
Oct 21 18:20:06 labvm kernel: AMD AuthenticAMD
Oct 21 18:20:06 labvm kernel: Centaur Centaurhearts
Oct 21 18:20:06 labvm kernel: zhaoxnt Shanghai
Oct 21 18:20:06 labvm kernel: x86/pni x87 FPU will use FSGNVC
Oct 21 18:20:06 labvm kernel: memory size: 1649
Oct 21 18:20:06 labvm kernel: BIOS-provided physical RAM map:
Oct 21 18:20:06 labvm kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbff] usable
Oct 21 18:20:06 labvm kernel: BIOS-e820: [mem 0x00000000000000fc00-0x000000000000ffff] reserved
Oct 21 18:20:06 labvm kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000000ffff] reserved
Oct 21 18:20:06 labvm kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000007ffff] usable
Oct 21 18:20:06 labvm kernel: BIOS-e820: [mem 0x0000000000000000-0xffffffffffff] ACPI data
Oct 21 18:20:06 labvm kernel: BIOS-e820: [mem 0x0000000000fc0000-0x0000000000fcffff] reserved
Oct 21 18:20:06 labvm kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000000ffff] reserved
Oct 21 18:20:06 labvm kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000000ffff] reserved
Oct 21 18:20:06 labvm kernel: NX (Execute Disable protection) active
Oct 21 18:20:06 labvm kernel: SMBIOS 2.5 present
Oct 21 18:20:06 labvm kernel: SMBIOS v2.6 detected from VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Oct 21 18:20:06 labvm kernel: Hypervisor detected: KVM
Oct 21 18:20:06 labvm kernel: kvm-clock: Using msrs 4b56d4b1 and 4b56d4b0
Oct 21 18:20:06 labvm kernel: kvm-clock: CPU 0 primary cpu clock
Oct 21 18:20:06 labvm kernel: kvm-clock: log2_tsc_offset 704707 cycles
Oct 21 18:20:06 labvm kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dfb, max_idle_ns: 881590591483 ns
Oct 21 18:20:06 labvm kernel: tsc: Detected 2887.999 MHz processor
Oct 21 18:20:06 labvm kernel: e820: Update [mem 0x00000000-0x0000ffff] usable => reserved
Oct 21 18:20:06 labvm kernel: last_pfn = 0xfffff max_arch_pfn = 0x4000000000
Oct 21 18:20:06 labvm kernel: x86/PAT Configuration [0-7]: WC UC UC WB WP UC UC WT
Oct 21 18:20:06 labvm kernel: Found SMM MP-table at [mem 0x00009f7000-0x00009f9bf]
Oct 21 18:20:06 labvm kernel: RAMDISK: [mem 0x306f7000-0x34372fff]
Oct 21 18:20:06 labvm kernel: ACPI: Early table checksum verification disabled
Oct 21 18:20:06 labvm kernel: ACPI: Early table checksum verification disabled
Oct 21 18:20:06 labvm kernel: ACPI: XSDT 0x0000000000000030 000003C {v1 VBOX VBOXXSDT 00000001 ASL 00000001}
Oct 21 18:20:06 labvm kernel: ACPI: FACP 0x0000000000000004 {v04 VBOX VBOXFAC 00000001 ASL 00000001}
Oct 21 18:20:06 labvm kernel: ACPI: DSDT 0x0000000000000010 002353 {v02 VBOX VBOXDSDT 00000002 INTL 20100528}
Oct 21 18:20:06 labvm kernel: ACPI: FACS 0x0000000000000005 00000005 {v01 VBOX VBOXFACS 00000002 INTL 20100528}
Oct 21 18:20:06 labvm kernel: ACPI: APIC 0x0000000000000004 {v02 VBOX VBOXAPIC 00000001 ASL 00000001}
Oct 21 18:20:06 labvm kernel: ACPI: SSDT 0x0000000000000030 000035C {v01 VBOX VBOXSSDT 00000002 INTL 20100528}
Oct 21 18:20:06 labvm kernel: ACPI: Reserved DSDT table memory at [mem 0xfffff8010-0xfffff29e2]
Oct 21 18:20:06 labvm kernel: ACPI: Reserving DSDT table memory at [mem 0xfffff8200-0xfffff023f]
Oct 21 18:20:06 labvm kernel: ACPI: Reserving FACS table memory at [mem 0xfffff8200-0xfffff023f]
Oct 21 18:20:06 labvm kernel: ACPI: Reserving APIC table memory at [mem 0xfffff8100-0xfffff0230]
Oct 21 18:20:06 labvm kernel: ACPI: Reserving ARIC table memory at [mem 0xfffff8100-0xfffff0230]
cisco@labvm:~
```

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

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

```
cisco@labvm:~$ sudo journalctl -f
Oct 21 23:06:15 labvm sudo[2810]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1001)
Oct 21 23:06:16 labvm sudo[2810]: pam_unix(sudo:session): session closed for user root
Oct 21 23:07:34 labvm sudo[2815]: Cisco :TTvpts/0 :Pw0:/home/cisco :USER=root :COMMAND=/usr/bin/journalctl -u ssh.service --since today
Oct 21 23:07:34 labvm sudo[2815]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1001)
Oct 21 23:07:34 labvm sudo[2815]: pam_unix(sudo:session): session closed for user root
Oct 21 23:08:18 labvm sudo[2820]: Cisco :TTvpts/0 :Pw0:/home/cisco :USER=root :COMMAND=/usr/bin/journalctl -k
Oct 21 23:08:18 labvm sudo[2820]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1001)
Oct 21 23:08:18 labvm sudo[2820]: pam_unix(sudo:session): session closed for user root
Oct 21 23:09:03 labvm sudo[2826]: Cisco :TTvpts/0 :Pw0:/home/cisco :USER=root :COMMAND=/usr/bin/journalctl -f
Oct 21 23:09:03 labvm sudo[2826]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1001)
cisco@labvm:~
```

Pregunta de reflexión

Comparen Syslog con Journald. ¿Cuáles son las ventajas y desventajas de cada uno?

Syslog: simple, texto plano, fácil de leer, pero poca información extra y difícil de filtrar.

Journald: más completo, guarda metadatos, fácil de buscar y seguro, pero binario y necesita journalctl para leerlo.