

VxLEARN Networks

Networking & Cybersecurity Track
Simulated Employment Program

Lab Report: Reading Server Logs

Prepared by:
Kudzaishe Majeza
Junior Network Engineer – VxLEARN Networks

Mentor:
Titus Majeza
Senior Network Engineer

Date: 12 January 2026

Contents

Objective.....	3
Tools and Environment.....	3
Part 1: Reading Log Files	3
Step 1: Opening Log Files.	4
Step 2: Actively Following Logs.	8
Part 2: Syslog	10
Part 3: Journald.....	12
Step 1: Running journalctl with no options.	13
Step 2: Journalctl and a few options.	14
Reflection.....	16

Objective

The objective of this lab is to understand how to read, monitor, and analyze server log files using common Linux command-line tools. The lab also explores centralized logging using Syslog and Journald.

Tools and Environment

- Security Workstation Virtual Machine
- Linux Terminal
- Log analysis commands: cat, more, less, tail, journalctl

Part 1: Reading Log Files

In this section, various commands were used to read log files.

Cat Command:

The cat command displays the entire content of a file at once. A drawback of using cat with large files is that the output scrolls quickly, making it difficult to review specific information.

More Command:

The more command displays files page by page. A drawback of more is that it only allows forward navigation and does not support scrolling backward.

Less Command:

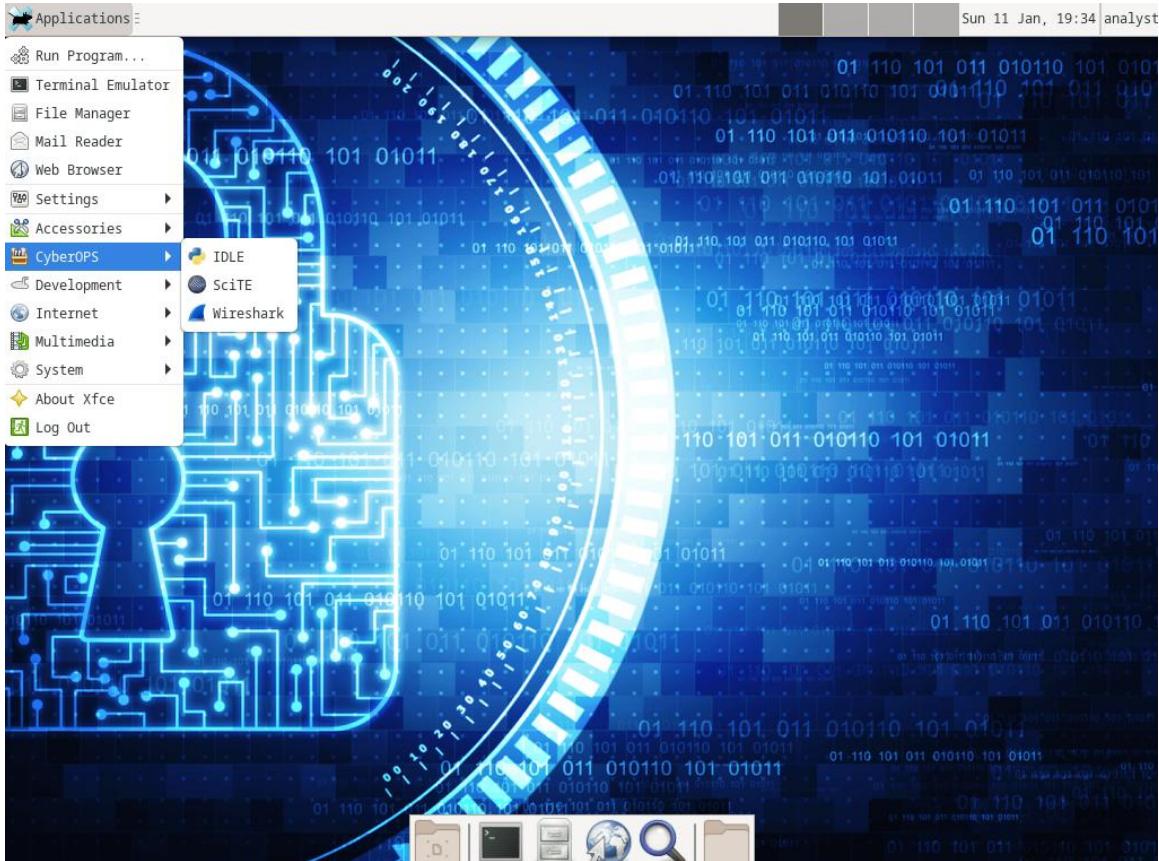
The less command improves usability by allowing both forward and backward navigation. It is ideal for analyzing large log files.

Tail and Tail -f:

The tail command shows the last lines of a file, while tail -f continuously updates the display as new entries are added. Tail -f is useful for real-time log monitoring.

Step 1: Opening Log Files.

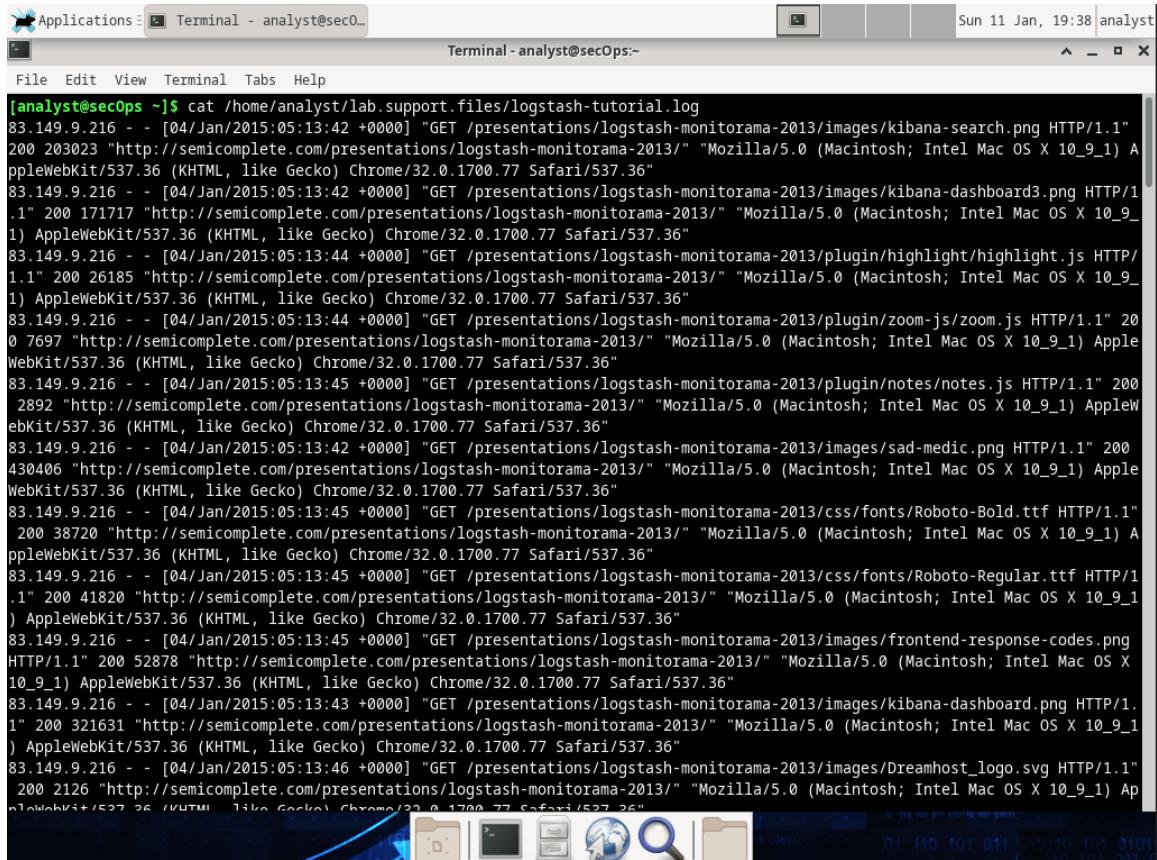
- Start the **CyberOps Worstation VM** and open a terminal window.



- From the terminal window, issue the command below to display the contents of the **logstash-tutorial.log** file, located in the **/home/analyst/lab.support.files/** folder:

A screenshot of a terminal window titled 'Terminal - analyst@secOps:~'. The window shows a standard Linux terminal interface with a black background and white text. At the top, there's a menu bar with 'File', 'Edit', 'View', 'Terminal', 'Tabs', and 'Help'. Below the menu is a command line prompt '[analyst@secOps ~]\$'. A single command is entered: 'cat /home/analyst/lab.support.files/logstash-tutorial.log'. The terminal is currently empty, indicating the file has not been fully read yet.

The contents of the file should scroll through the terminal window until the all contents have been displayed.

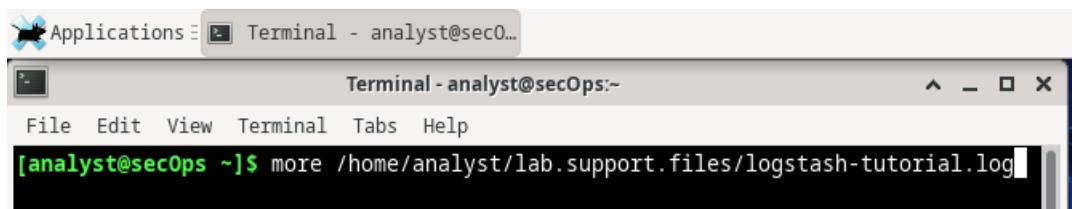


A screenshot of a Mac OS X terminal window titled "Terminal - analyst@secOps:~". The window shows the command `cat /home/analyst/lab.support.files/logstash-tutorial.log` running. The output of the command is a large block of log entries from January 2015, detailing various HTTP requests to a presentation site. The log includes fields like timestamp, method, URL, and user agent information.

```
[analyst@secOps ~]$ cat /home/analyst/lab.support.files/logstash-tutorial.log
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-search.png HTTP/1.1" 200 203023 "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/2015:05:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-dashboard3.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"
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://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/2015:05:13:44 +0000] "GET /presentations/logstash-monitorama-2013/plugin/zoom-js/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"
83.149.9.216 - - [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"
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://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/2015:05:13:45 +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"
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://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/2015:05:13:45 +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"
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://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/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"
```

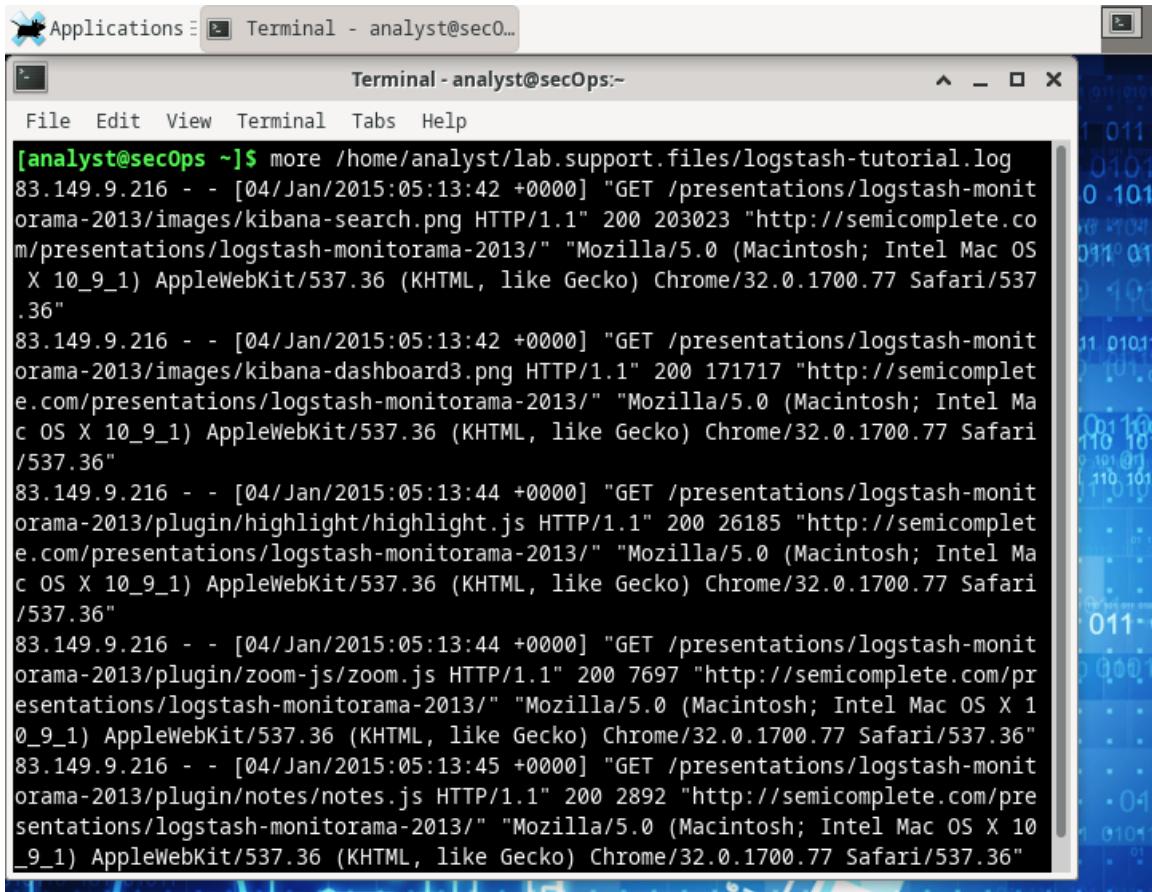
Another popular tool for visualizing log files is **more**. Similar to **cat**, **more** is also a UNIX command-line-based tool that can open a text-based file and display the file contents on the screen. The main difference between **cat** and **more** is that **more** supports page breaks, allowing the user to view the contents of a file, one page at a time. This can be done using the space bar to display the next page.

- From the same terminal window, use the command below to display the contents of the **logstash-tutorial.log** file again. This time using **more**:



A screenshot of a Mac OS X terminal window titled "Terminal - analyst@secOps:~". The window shows the command `more /home/analyst/lab.support.files/logstash-tutorial.log` running. The output is the same log file content as the previous screenshot, but it is displayed in a paginated format where each page of the log is shown on a new line, and the user must press the space bar to see the next page.

The contents of the file should scroll through the terminal window and stop when one page is displayed. Press the space bar to advance to the next page. Press enter to display the next line of text.

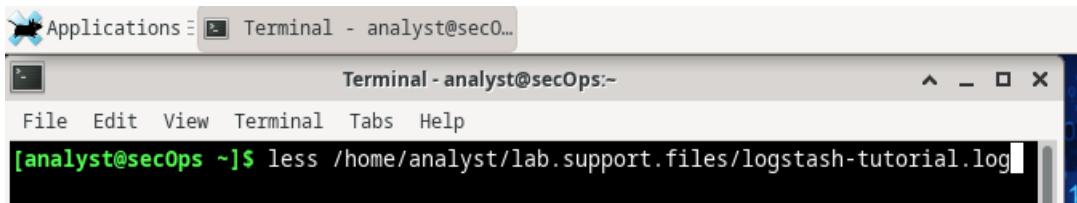


A screenshot of a terminal window titled "Terminal - analyst@secOps:~". The window shows the command "[analyst@secOps ~]\$ more /home/analyst/lab.support.files/logstash-tutorial.log" followed by several lines of log data. The log entries are as follows:

```
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-search.png HTTP/1.1" 200 203023 "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/2015:05:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-dashboard3.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"
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://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/2015:05:13:44 +0000] "GET /presentations/logstash-monitorama-2013/plugin/zoom-js/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"
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://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"
```

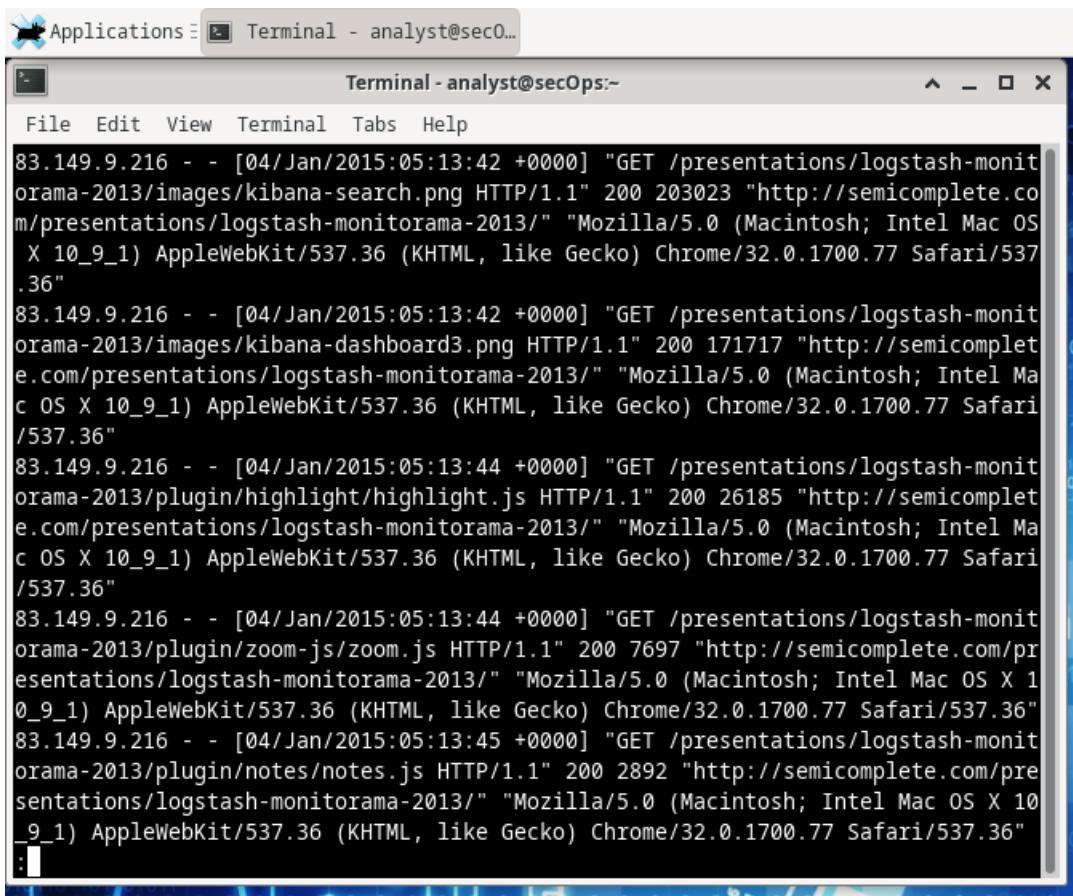
Building on the functionality of **cat** and **more**, the **less** tool allows the contents of a file to be displayed page by page, while also allowing the user the choice of viewing previously displayed pages.

- d. From the same terminal window, use **less** to display the contents the **logstash-tutorial.log** file again:



A screenshot of a terminal window titled "Terminal - analyst@secOps:~". The window shows the command "[analyst@secOps ~]\$ less /home/analyst/lab.support.files/logstash-tutorial.log". The terminal is in a scrollable mode, indicated by the vertical scrollbar on the right side of the window.

The contents of the file should scroll through the terminal window and stop when one page is displayed. Press the space bar to advance to the next page. Press enter to display the next line of text. Use the up and down arrow keys to move back and forth through the text file.



The screenshot shows a terminal window titled "Terminal - analyst@sec0...". The window contains several lines of log entries from the file "/home/analyst/lab.support.files/logstash-tutorial.log". The logs are timestamped at 04/Jan/2015:05:13:42 +0000 and show various HTTP requests being handled by Logstash. The requests include GET requests for images like "kibana-search.png" and "kibana-dashboard3.png", as well as plugin files like "highlight.js" and "notes.js". The clients are identified as 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, indicating they are running on Mac OS X 10.9.1 with Google Chrome.

```
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-search.png HTTP/1.1" 200 203023 "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/2015:05:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-dashboard3.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"
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://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/2015:05:13:44 +0000] "GET /presentations/logstash-monitorama-2013/plugin/zoom-js/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"
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://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"
:
```

- e. The **tail** command displays the end of a text file. By default, **tail** displays the last ten lines of the file.

Use tail to display the last ten lines of the **/home/analyst/lab.support.files/logstash-tutorial.log** file.

```

[analyst@secOps ~]$ less /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%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_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/2015:05:29:48 +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/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" "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"
[analyst@secOps ~]$ 
```

Step 2: Actively Following Logs.

In some situations, it is desirable to monitor log files as log entries are written to the log files. For those cases, the **tail -f** command is very helpful.

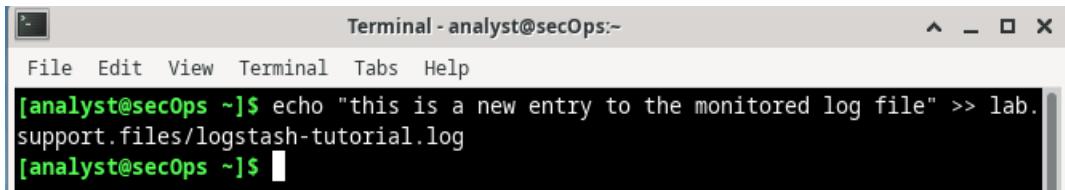
- Use **tail -f** to actively monitor the contents of the **/var/log/syslog** file:

```

[analyst@secOps ~]$ sudo 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.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%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_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/2015:05:29:48 +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/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" "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"
```

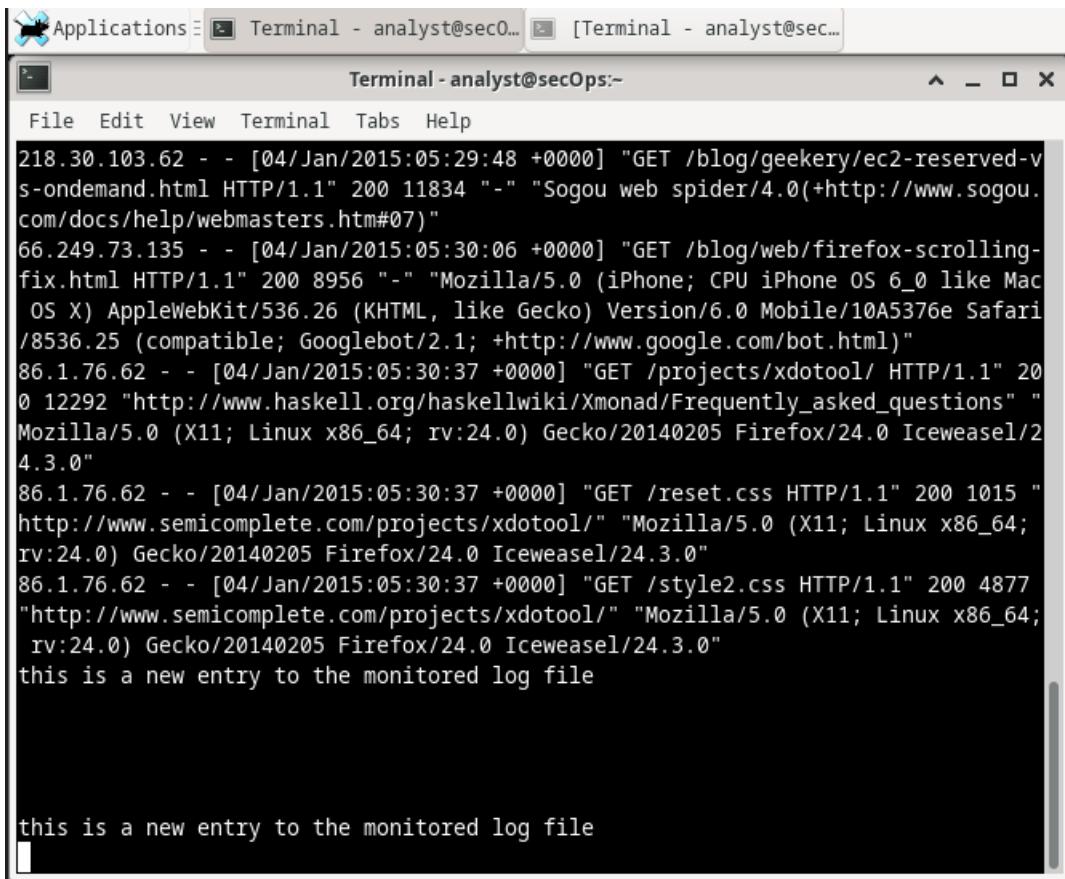
- b. To watch tail -f in action, open a second terminal window. Arrange your display so you can see both terminal windows. Re-size the windows so you can see them both at the same, as shown in the image below:

The terminal window on the top is running **tail -f** to monitor the **/home/analyst/lab.support.files/logstash-tutorial.log** file. Use the terminal window on the bottom to add information to the monitored file.



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

To make it easier to visualize, select the top terminal window (the one running **tail -f**) and press enter a few times. This will add a few lines between the current contents of the file and the new information to be added.



```
Terminal - analyst@sec0... [Terminal - analyst@sec...]  
File Edit View Terminal Tabs Help  
218.30.103.62 - - [04/Jan/2015:05:29:48 +0000] "GET /blog/geekery/ec2-reserved-v  
s-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/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" 20  
0 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/2  
4.3.0"  
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"  
this is a new entry to the monitored log file  
  
this is a new entry to the monitored log file
```

- c. Select the bottom terminal window and enter the following command:

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

The command above appends the #this is a new entry to the monitored log file# message to the **/home/analyst/lab.support.files/logstash-tutorial.log** file. Because tail -f is monitoring the file at the moment a line is added to the file. The top window should display the new line in real-time.

- d. Press CTRL + C to stop the execution of **tail -f** and return to the shell prompt.
e. Close one of the two terminal windows.

Part 2: Syslog

Syslog is a centralized logging system that collects operating system and application logs.

Root Access:

The cat command had to be executed as root because syslog files contain sensitive system information and are protected to prevent unauthorized access.

Log Rotation:

Older syslog files are rotated and renamed (syslog.1, syslog.2, etc.) to prevent files from becoming too large.

Time Synchronization:

Accurate system time is essential for log analysis, troubleshooting, and security investigations. Incorrect timestamps can lead to misinterpretation of events.

Because of their importance, it is common practice to concentrate log files in one monitoring computer. **Syslog** is a system designed to allow devices to send their log files to a centralized server, known as **syslog** server. Clients

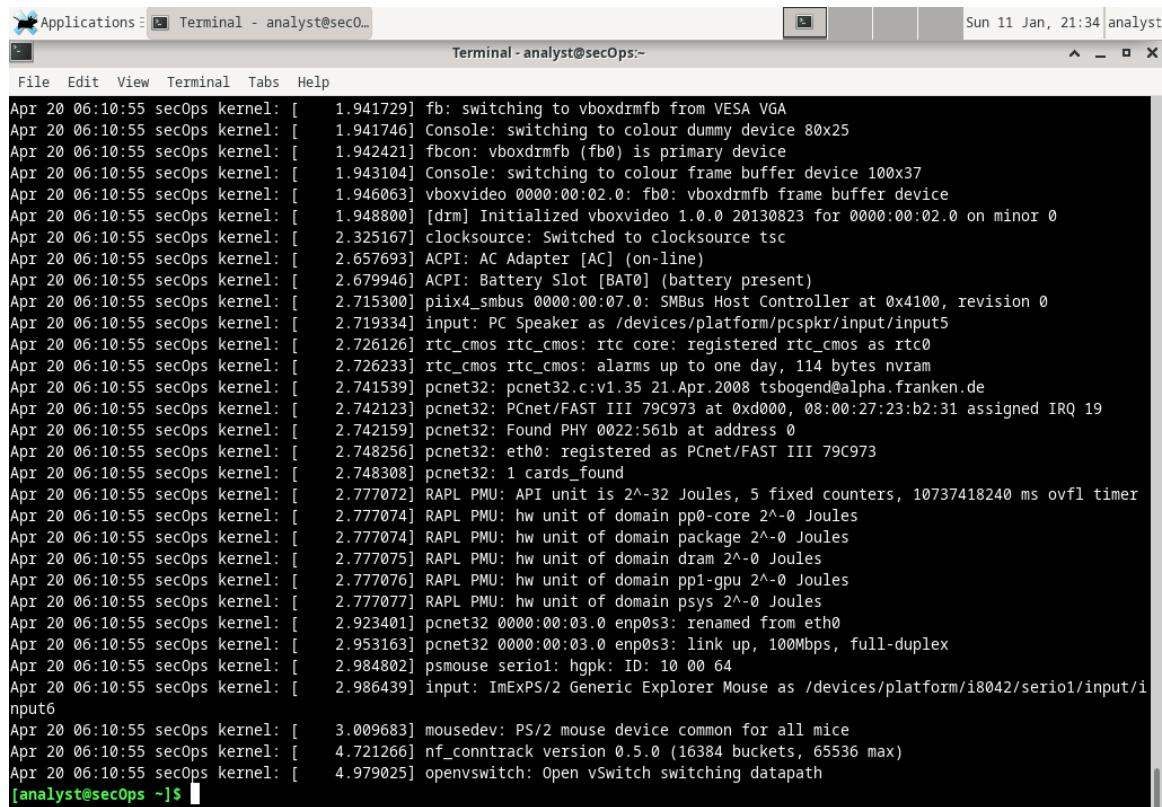
communicate to a syslog server using the **syslog** protocol. **Syslog** is commonly deployed and supports practically all computer platforms.

The CyberOps Workstation VM generates operating system level log files and hands them over to **syslog**.

- Use the **cat** command as **root** to list the contents of the **/var/log/syslog.1** file. This file holds the log entries that are generated by the CyberOps Workstation VM operating system and sent to the **syslog** service.

```
analyst@secOps ~$ sudo cat /var/log/syslog.1
```

[sudo] password for analyst:



A screenshot of a terminal window titled "Terminal - analyst@secOps...". The window shows the command "cat /var/log/syslog.1" being run. The output is a long list of log entries from the kernel, starting with "Apr 20 06:10:55 secOps kernel: [1.941729] fb: switching to vboxdrmfb from VESA VGA" and ending with "[analyst@secOps ~]\$". The terminal window has a standard OS X-style interface with a menu bar and a title bar showing the date and time ("Sun 11 Jan, 21:34").

```
Analyst@secOps ~$ sudo cat /var/log/syslog.1
[sudo] password for analyst:
[ 1.941729] fb: switching to vboxdrmfb from VESA VGA
[ 1.941746] Console: switching to colour dummy device 80x25
[ 1.942421] fbcon: vboxdrmfb (fb0) is primary device
[ 1.943104] Console: switching to colour frame buffer device 100x37
[ 1.946063] vboxvideo 0000:00:02.0: fb0: vboxdrmfb frame buffer device
[ 1.948800] [drm] Initialized vboxvideo 1.0.0 20130823 for 0000:00:02.0 on minor 0
[ 2.325167] clocksource: Switched to clocksource tsc
[ 2.657693] ACPI: AC Adapter [AC] (on-line)
[ 2.679946] ACPI: Battery Slot [BAT0] (battery present)
[ 2.715300] piix4_smbus 0000:00:07.0: SMBus Host Controller at 0x4100, revision 0
[ 2.719334] input: PC Speaker as /devices/platform/pcspkr/input/input5
[ 2.726126] rtc_cmos rtc_cmos: rtc core: registered rtc_cmos as rtc0
[ 2.726233] rtc_cmos rtc_cmos: alarms up to one day, 114 bytes nvram
[ 2.741539] pcnet32: pcnet32.c:v1.35 21.Apr.2008 tsbogend@alpha.franken.de
[ 2.742123] pcnet32: PCnet/FAST III 79C973 at 0xd000, 08:00:27:23:b2:31 assigned IRQ 19
[ 2.742159] pcnet32: Found PHY 0022:561b at address 0
[ 2.748256] pcnet32: eth0: registered as PCnet/FAST III 79C973
[ 2.748308] pcnet32: 1 cards_found
[ 2.777072] RAPL PMU: API unit is 2^-32 Joules, 5 fixed counters, 10737418240 ms ovfl timer
[ 2.777074] RAPL PMU: hw unit of domain pp0-core 2^-0 Joules
[ 2.777074] RAPL PMU: hw unit of domain package 2^-0 Joules
[ 2.777075] RAPL PMU: hw unit of domain dian 2^-0 Joules
[ 2.777076] RAPL PMU: hw unit of domain pp1-gpu 2^-0 Joules
[ 2.777077] RAPL PMU: hw unit of domain psys 2^-0 Joules
[ 2.923401] pcnet32 0000:00:03.0 enp0s3: renamed from eth0
[ 2.953163] pcnet32 0000:00:03.0 enp0s3: link up, 100Mbps, full-duplex
[ 2.984802] psmouse serio1: hpgk: ID: 10 00 04
[ 2.986439] input: ImExPS/2 Generic Explorer Mouse as /devices/platform/i8042/serio1/input/input6
[ 3.009683] mousedev: PS/2 mouse device common for all mice
[ 4.721266] nf_conntrack version 0.5.0 (16384 buckets, 65536 max)
[ 4.979025] openvswitch: Open vSwitch switching datapath
[analyst@secOps ~]$
```

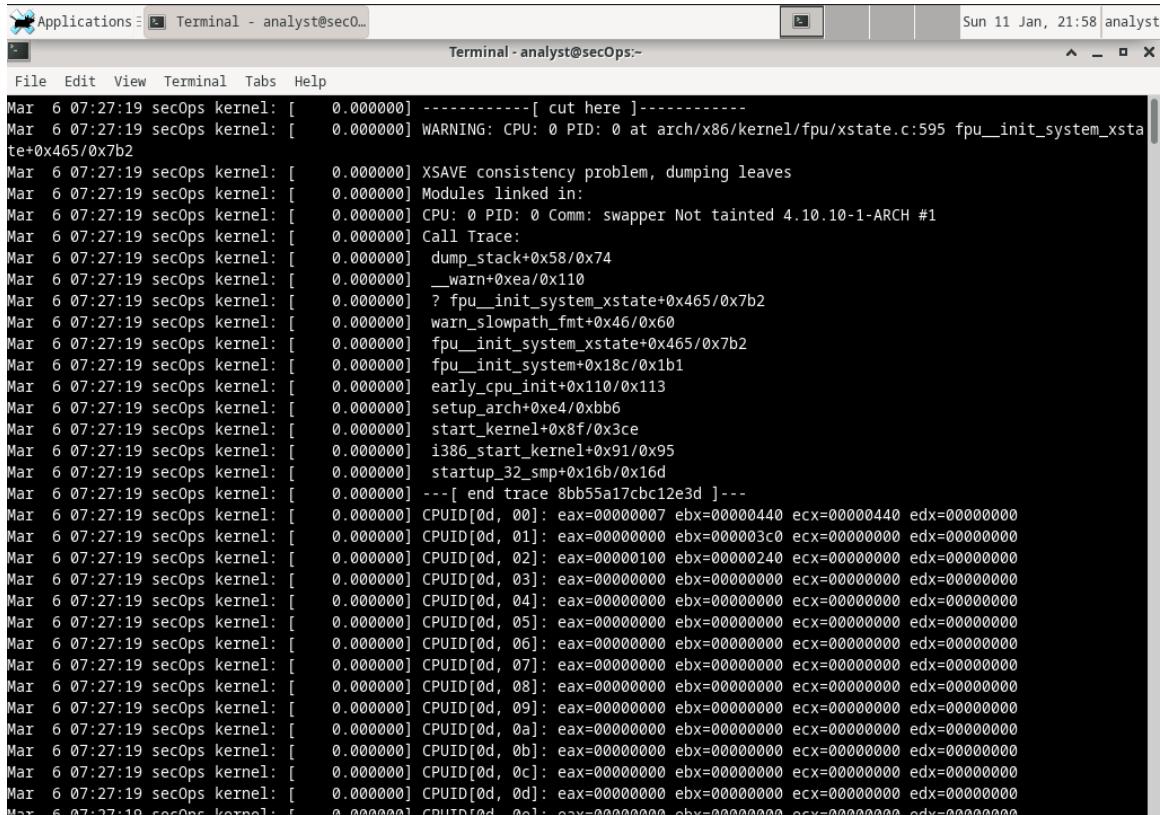
- Notice that the **/var/log/syslog** file only stores the most recent log entries. To keep the syslog file small, the operating system periodically rotates the log files, renaming older log files as **syslog.1**, **syslog.2**, and so on.

Use the **cat** command to list older **syslog** files:

analyst@secOps ~\$ sudo cat /var/log/syslog.2

analyst@secOps ~\$ sudo cat /var/log/syslog.3

analyst@secOps ~\$ sudo cat /var/log/syslog.4



The screenshot shows a terminal window titled "Terminal - analyst@secOps:" with the date "Sun 11 Jan, 21:58" and user "analyst". The window displays a long list of kernel log messages from March 6, 2019, at 07:27:19. The logs are primarily from the "secOps kernel" and show various system initialization and CPUID calls. The text is in a monospaced font and is too long to reproduce here.

Part 3: Journald

Journald manages logs using binary files and centralizes log data from multiple sources.

Journalctl:

The journalctl command allows filtering by boot session, service, kernel messages, and time range.

Advantages:

- Structured logging
- Advanced filtering
- Tamper resistance

Disadvantages:

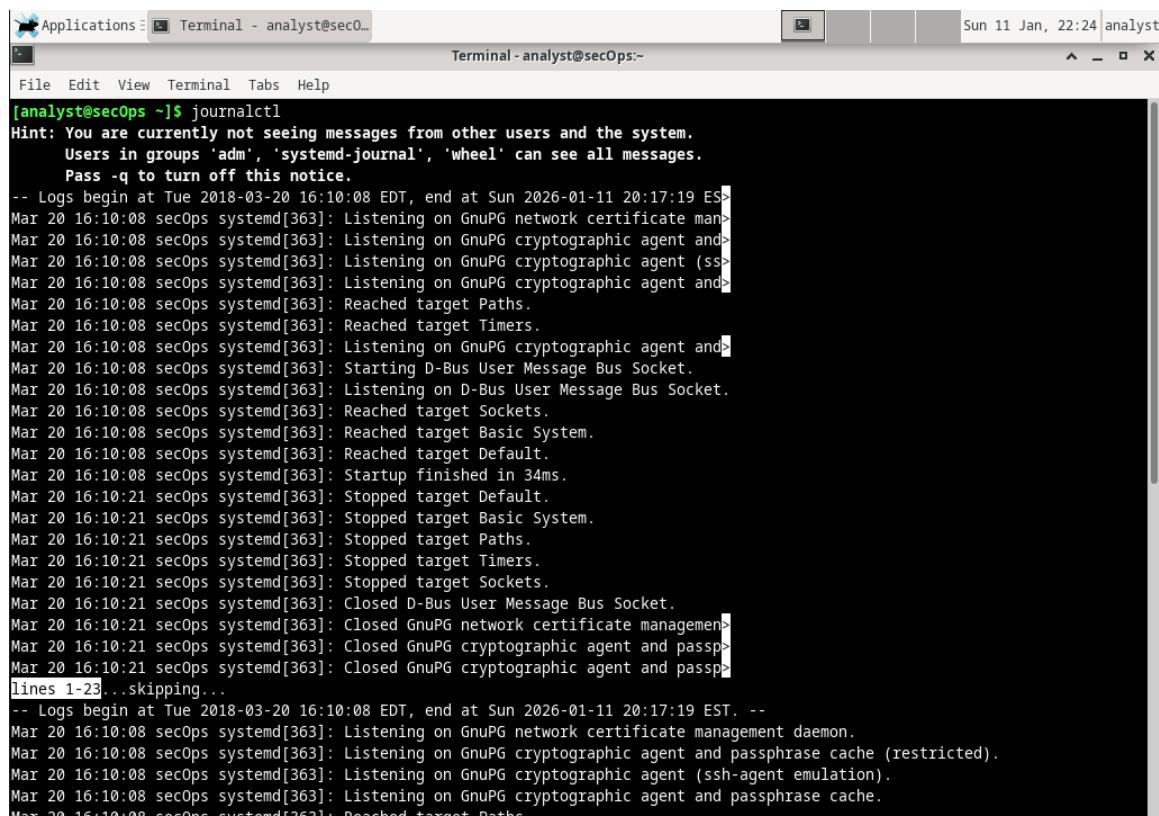
- Binary format is not human-readable without journalctl
- Slightly higher resource usage

In the context of this lab, the most evident feature of the **journal** system daemon is the use of append-only binary files serving as its **log files**.

Step 1: Running journalctl with no options.

- To look at the **journald** logs, use the **journalctl** command.

The **journalctl** tool interprets and displays the log entries previously stored in the **journal** binary log files.



A screenshot of a terminal window titled "Terminal - analyst@sec0...". The window shows the output of the command [analyst@secOps ~]\$ journalctl. The output includes a warning about not seeing messages from other users, followed by a log of GnuPG network certificate management events on March 20, 2018, between 16:10:08 and 16:10:21. The logs show various actions like listening on ports, reaching target Paths, and stopping targets. The terminal window has a standard Linux-style title bar and scroll bars.

```
[analyst@secOps ~]$ journalctl
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal', 'wheel' can see all messages.
      Pass -q to turn off this notice.
-- Logs begin at Tue 2018-03-20 16:10:08 EDT, end at Sun 2026-01-11 20:17:19 EST.
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG network certificate man...
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and...
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent (ss...
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and...
Mar 20 16:10:08 secOps systemd[363]: Reached target Paths.
Mar 20 16:10:08 secOps systemd[363]: Reached target Timers.
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and...
Mar 20 16:10:08 secOps systemd[363]: Starting D-Bus User Message Bus Socket.
Mar 20 16:10:08 secOps systemd[363]: Listening on D-Bus User Message Bus Socket.
Mar 20 16:10:08 secOps systemd[363]: Reached target Sockets.
Mar 20 16:10:08 secOps systemd[363]: Reached target Basic System.
Mar 20 16:10:08 secOps systemd[363]: Reached target Default.
Mar 20 16:10:08 secOps systemd[363]: Startup finished in 34ms.
Mar 20 16:10:21 secOps systemd[363]: Stopped target Default.
Mar 20 16:10:21 secOps systemd[363]: Stopped target Basic System.
Mar 20 16:10:21 secOps systemd[363]: Stopped target Paths.
Mar 20 16:10:21 secOps systemd[363]: Stopped target Timers.
Mar 20 16:10:21 secOps systemd[363]: Stopped target Sockets.
Mar 20 16:10:21 secOps systemd[363]: Closed D-Bus User Message Bus Socket.
Mar 20 16:10:21 secOps systemd[363]: Closed GnuPG network certificate managemen...
Mar 20 16:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent and passphr...
Mar 20 16:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent and passphr...
lines 1-23... skipping...
-- Logs begin at Tue 2018-03-20 16:10:08 EDT, end at Sun 2026-01-11 20:17:19 EST. --
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG network certificate management daemon.
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and passphrase cache (restricted).
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent (ssh-agent emulation).
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and passphrase cache.
Mar 20 16:10:08 secOps systemd[363]: Reached target Paths
```

Note: Running journalctl as root will display more detailed information.

- Use CTRL+C to exit the display.

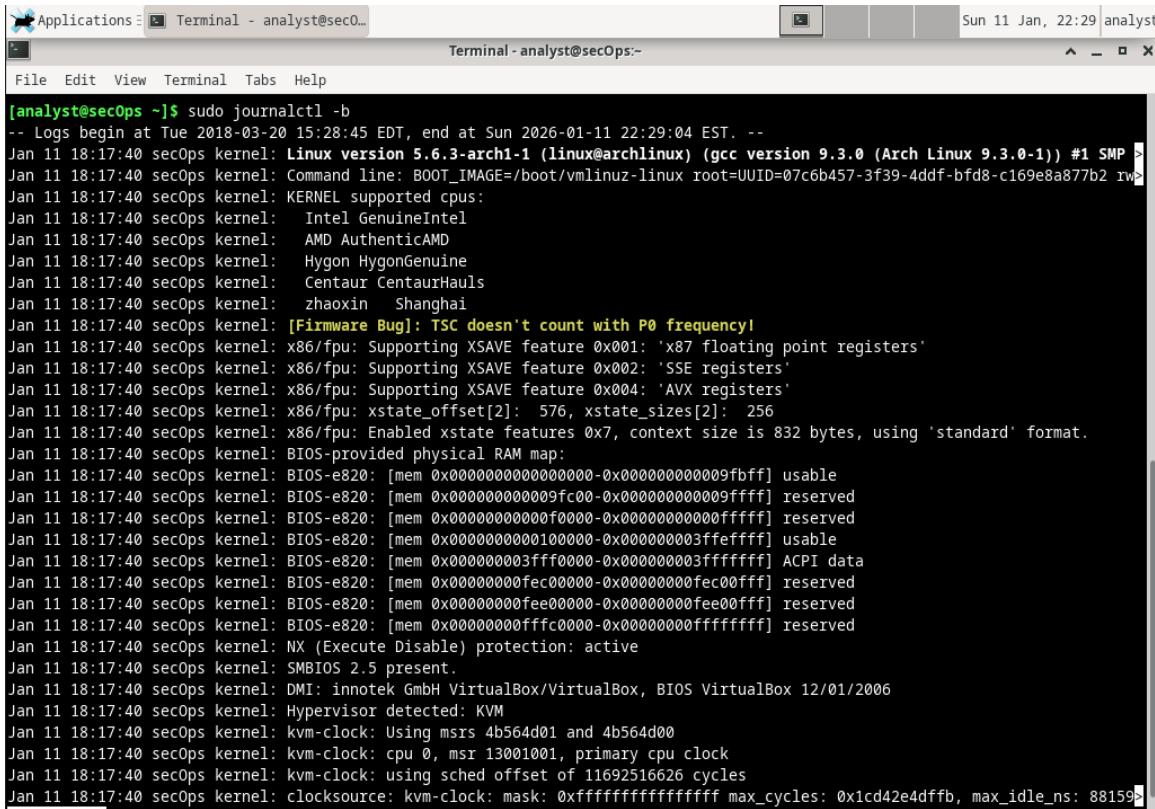
Step 2: Journalctl and a few options.

Part of the power of using journalctl lies in its options. For the following commands, use CRTL+C to exit the display.

- a. Use **journalctl --utc** to display all timestamps in UTC time:

```
[analyst@secOps ~]$ sudo journalctl --utc
[sudo] password for analyst:
-- Logs begin at Tue 2018-03-20 19:28:45 UTC, end at Mon 2026-01-12 03:27:17 UTC. --
Mar 20 19:28:45 secOps kernel: Linux version 4.15.10-1-ARCH (builduser@heftig-18961) (gcc version 7.3.1 20180312 (GCC) #1 SMP
Mar 20 19:28:45 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c169e8a877b2 rw
Mar 20 19:28:45 secOps kernel: KERNEL supported cpus:
Mar 20 19:28:45 secOps kernel: Intel GenuineIntel
Mar 20 19:28:45 secOps kernel: AMD AuthenticAMD
Mar 20 19:28:45 secOps kernel: Centaur CentaurHauls
Mar 20 19:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Mar 20 19:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 20 19:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Mar 20 19:28:45 secOps kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Mar 20 19:28:45 secOps kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using 'standard' format.
Mar 20 19:28:45 secOps kernel: e820: BIOS-provided physical RAM map:
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000fbff] usable
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000000f0000-0x0000000000ffff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x0000000000100000-0x000000003fffffff] usable
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x0000000003fff0000-0x000000003fffffff] ACPI data
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000000fec0000-0x000000000fec00ff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000000fee00000-0x000000000fee00ffff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000000fffc0000-0x000000000ffffffff] reserved
Mar 20 19:28:45 secOps kernel: NX (Execute Disable) protection: active
Mar 20 19:28:45 secOps kernel: random: fast init done
Mar 20 19:28:45 secOps kernel: SMBIOS 2.5 present.
Mar 20 19:28:45 secOps kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Mar 20 19:28:45 secOps kernel: Hypervisor detected: KVM
Mar 20 19:28:45 secOps kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Mar 20 19:28:45 secOps kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Mar 20 19:28:45 secOps kernel: e820: last_pfn = 0x3ffff max_arch_pfn = 0x400000000
Mar 20 19:28:45 secOps kernel: MTRR default type: uncachable
Mar 20 19:28:45 secOps kernel: MTRR variable ranges disabled:
Mar 20 19:28:45 secOps kernel: MTRR fixed ranges disabled:
```

- b. Use `journalctl -b` to display log entries recorded during the last boot:



A screenshot of a terminal window titled "Terminal - analyst@secOps:~". The window shows a log of system events from January 11, 2018, at 18:17:40. The logs include kernel boot information, CPU support (Intel GenuineIntel, AMD AuthenticAMD), processor features (XSAVE, SSE registers, AVX registers), memory maps (BIOS-e820), and various protection settings (NX, Execute Disable). A notable entry is a warning about a TSC frequency bug.

```
[analyst@secOps ~]$ sudo journalctl -b
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Sun 2026-01-11 22:29:04 EST. --
Jan 11 18:17:40 secOps kernel: Linux version 5.6.3-arch1-1 (linux@archlinux) (gcc version 9.3.0 (Arch Linux 9.3.0-1)) #1 SMP ...
Jan 11 18:17:40 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c169e8a877b2 rw ...
Jan 11 18:17:40 secOps kernel: KERNEL supported cpus:
Jan 11 18:17:40 secOps kernel:   Intel GenuineIntel
Jan 11 18:17:40 secOps kernel:   AMD AuthenticAMD
Jan 11 18:17:40 secOps kernel:   Hygon HygonGenuine
Jan 11 18:17:40 secOps kernel:   Centaur CentaurHauls
Jan 11 18:17:40 secOps kernel:   zhaoxin Shanghai
Jan 11 18:17:40 secOps kernel: [Firmware Bug]: TSC doesn't count with P0 frequency!
Jan 11 18:17:40 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Jan 11 18:17:40 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Jan 11 18:17:40 secOps kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Jan 11 18:17:40 secOps kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Jan 11 18:17:40 secOps kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using 'standard' format.
Jan 11 18:17:40 secOps kernel: BIOS-provided physical RAM map:
Jan 11 18:17:40 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Jan 11 18:17:40 secOps kernel: BIOS-e820: [mem 0x00000000000000fc00-0x0000000000009ffff] reserved
Jan 11 18:17:40 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000ffff] reserved
Jan 11 18:17:40 secOps kernel: BIOS-e820: [mem 0x0000000000100000-0x000000003fffffff] usable
Jan 11 18:17:40 secOps kernel: BIOS-e820: [mem 0x000000003fff0000-0x000000003ffffffff] ACPI data
Jan 11 18:17:40 secOps kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Jan 11 18:17:40 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Jan 11 18:17:40 secOps kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Jan 11 18:17:40 secOps kernel: NX (Execute Disable) protection: active
Jan 11 18:17:40 secOps kernel: SMBIOS 2.5 present.
Jan 11 18:17:40 secOps kernel: DMI: innoteck GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Jan 11 18:17:40 secOps kernel: Hypervisor detected: KVM
Jan 11 18:17:40 secOps kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Jan 11 18:17:40 secOps kernel: kvm-clock: cpu 0, msr 13001001, primary cpu clock
Jan 11 18:17:40 secOps kernel: kvm-clock: using sched offset of 11692516626 cycles
Jan 11 18:17:40 secOps kernel: clocksource: kvm-clock: mask: 0xfffffffffffffff max_cycles: 0x1cd42e4dfffb, max_idle_ns: 88159...
```

- c. Use **journalctl** to specify the service and timeframe for log entries. The command below shows all **nginx** service logs recorded today:

```
[analyst@secOps ~]$ sudo journalctl -u nginx.service --since today
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Sun 2026-01-11 22:33:53 EST. --
-- No entries --
```

- d. Use the **-k** switch to display only messages generated by the kernel:

```
[analyst@secOps ~]$ sudo journalctl -k
[sudo] password for analyst:
Sorry, try again.
[sudo] password for analyst:
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Sun 2026-01-11 22:37:28 EST. --
Jan 11 18:17:40 secOps kernel: Linux version 5.6.3-arch1-1 (linux@archlinux) (gcc version 9.3.0 (Arch Linux 9.3.0-1)) #1 SMP >
Jan 11 18:17:40 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c169e8a877b2 rw>
Jan 11 18:17:40 secOps kernel: KERNEL supported cpus:
Jan 11 18:17:40 secOps kernel:   Intel GenuineIntel
Jan 11 18:17:40 secOps kernel:   AMD AuthenticAMD
Jan 11 18:17:40 secOps kernel:   Hygon HygonGenuine
Jan 11 18:17:40 secOps kernel:   Centaur CentaurHauls
Jan 11 18:17:40 secOps kernel:   zhaixin Shanghai
Jan 11 18:17:40 secOps kernel: [Fixme Bug]: TSC doesn't count with P0 frequency!
Jan 11 18:17:40 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Jan 11 18:17:40 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Jan 11 18:17:40 secOps kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Jan 11 18:17:40 secOps kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Jan 11 18:17:40 secOps kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using 'standard' format.
Jan 11 18:17:40 secOps kernel: BIOS-provided physical RAM map:
Jan 11 18:17:40 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000fbfff] usable
Jan 11 18:17:40 secOps kernel: BIOS-e820: [mem 0x00000000000fc00-0x0000000000ffff] reserved
Jan 11 18:17:40 secOps kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000ffff] reserved
Jan 11 18:17:40 secOps kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000003ffff] usable
Jan 11 18:17:40 secOps kernel: BIOS-e820: [mem 0x000000003fff0000-0x000000003ffff] ACPI data
Jan 11 18:17:40 secOps kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Jan 11 18:17:40 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Jan 11 18:17:40 secOps kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Jan 11 18:17:40 secOps kernel: NX (Execute Disable) protection: active
Jan 11 18:17:40 secOps kernel: SMBIOS 2.5 present.
Jan 11 18:17:40 secOps kernel: DMI: innoteck GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Jan 11 18:17:40 secOps kernel: Hypervisor detected: KVM
Jan 11 18:17:40 secOps kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
```

- e. Similar to **tail -f** described above, use the **-f** switch to actively follow the logs as they are being written:

```
[analyst@secOps ~]$ sudo journalctl -f
-- Logs begin at Tue 2018-03-20 15:28:45 EDT. --
Jan 11 22:38:53 secOps audit[1410]: USER_END pid=1410 uid=0 auid=1000 ses=2 msg='op=PAM:session_close grantors=pam_limits,pam_unix,pam_permit acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/2 res=success'
Jan 11 22:38:53 secOps audit[1410]: CRED_DISP pid=1410 uid=0 auid=1000 ses=2 msg='op=PAM:setcred grantors=pam_unix,pam_permit acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/2 res=success'
Jan 11 22:39:15 secOps audit[1423]: USER_ACCT pid=1423 uid=0 auid=1000 ses=2 msg='op=PAM:accounting grantors=pam_unix,pam_permit,pam_time acct="analyst" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/2 res=success'
Jan 11 22:39:15 secOps sudo[1423]: analyst : TTY=pts/2 : PWD=/home/analyst : USER=root : COMMAND=/usr/bin/journalctl -f
Jan 11 22:39:15 secOps kernel: audit: type=1101 audit(1768189155.039:120): pid=1423 uid=1000 auid=1000 ses=2 msg='op=PAM:accounting grantors=pam_unix,pam_permit,pam_time acct="analyst" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/2 res=succes ss'
Jan 11 22:39:15 secOps audit[1423]: CRED_REFR pid=1423 uid=0 auid=1000 ses=2 msg='op=PAM:setcred grantors=pam_unix,pam_permit, pam_env acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/2 res=success'
Jan 11 22:39:15 secOps sudo[1423]: pam_unix(sudo:session): session opened for user root by (uid=0)
Jan 11 22:39:15 secOps audit[1423]: USER_START pid=1423 uid=0 auid=1000 ses=2 msg='op=PAM:session_open grantors=pam_limits,pam_unix,pam_permit acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/2 res=success'
Jan 11 22:39:15 secOps kernel: audit: type=1110 audit(1768189155.046:121): pid=1423 uid=0 auid=1000 ses=2 msg='op=PAM:setcred grantors=pam_unix,pam_permit,pam_env acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/2 res=success'
Jan 11 22:39:15 secOps kernel: audit: type=1105 audit(1768189155.046:122): pid=1423 uid=0 auid=1000 ses=2 msg='op=PAM:session_open grantors=pam_limits,pam_unix,pam_permit acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/2 res=success'
```

Reflection

Syslog is simple, widely supported, and uses plain-text logs, making it easy to integrate with other tools. However, it lacks advanced filtering. Journald provides powerful querying and structured logging but relies on binary files, which require specific tools to read. Both systems are effective depending on use case.