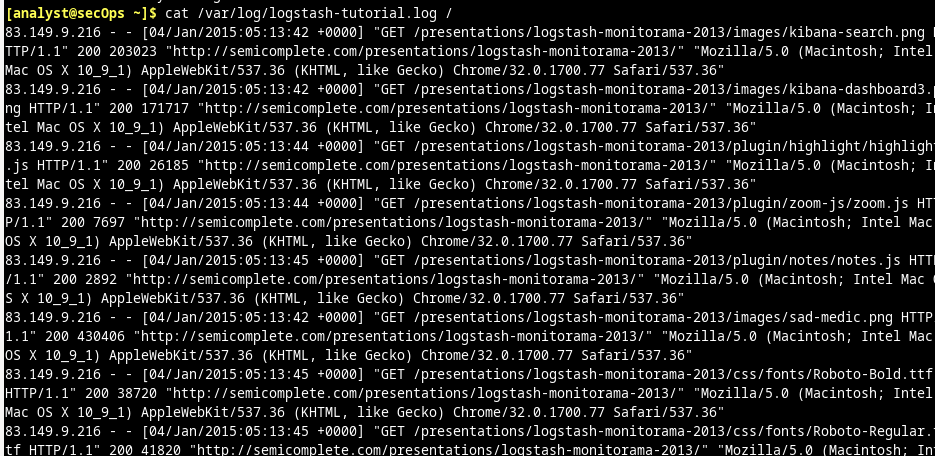
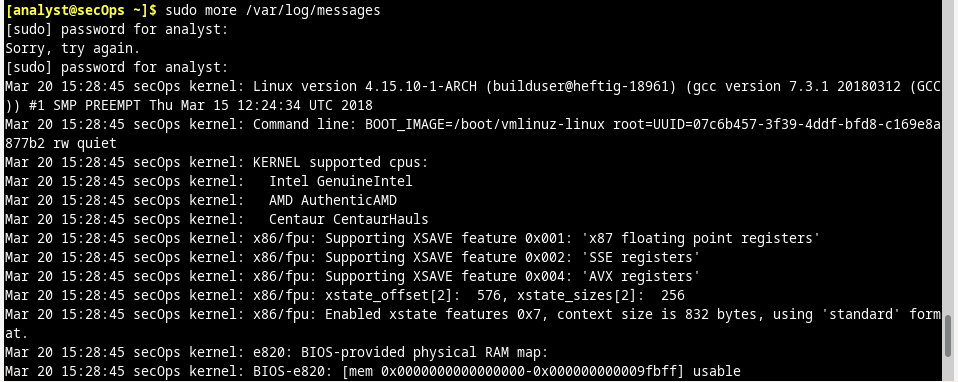
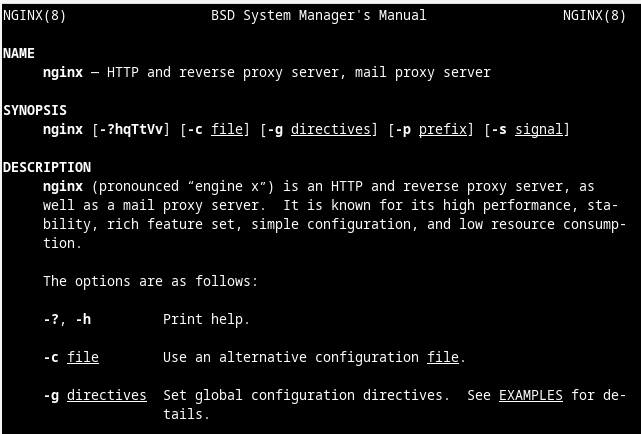
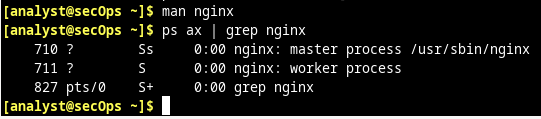
**Part 1: Log File Overview**

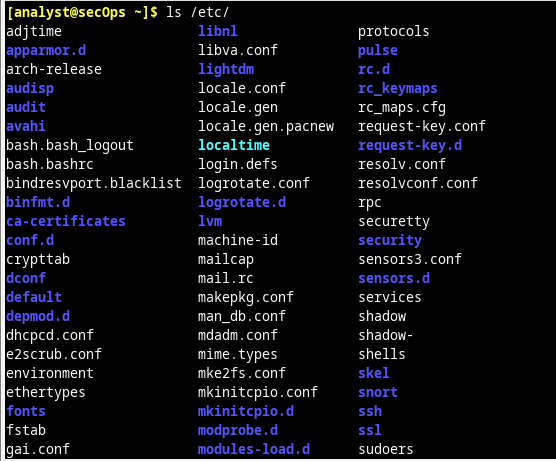
**Step 1: Web server log file example**

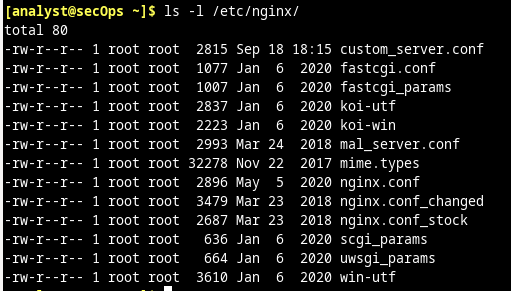
****

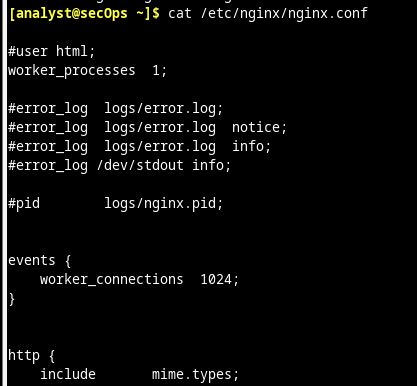
Step 2: Operating system log file example

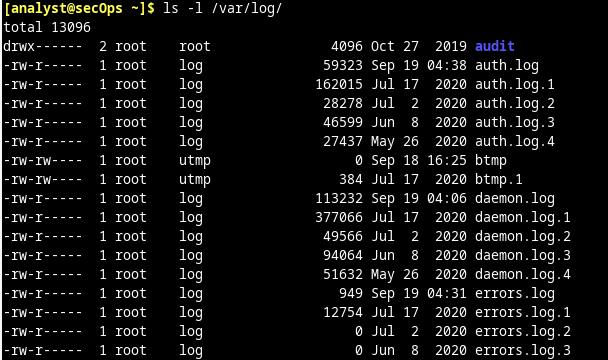
**Part 2: Locating Log Files in Unknown Systems**  
a. [analyst@secOps ~]$ man nginx  


d. [analyst@secOps ~]$ ps ax | grep nginx  


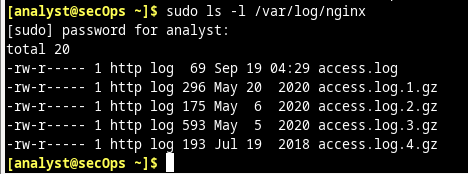
e [analyst@secOps ~]$ ls /etc/  


f.. [analyst@secOps ~]$ ls -l /etc/nginx/  


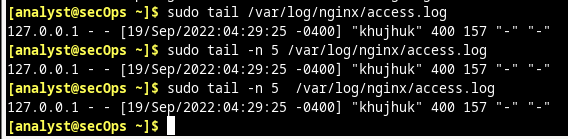
g. [analyst@secOps ~]$ cat /etc/nginx/nginx.conf  


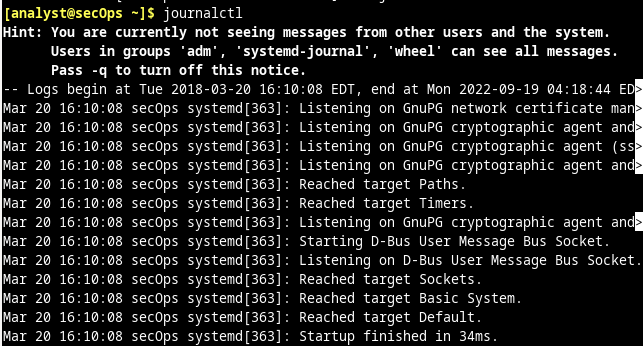
h. [analyst@secOps ~]$ ls -l /var/log/  


i. [analyst@secOps ~]$ sudo ls -l /var/log/nginx

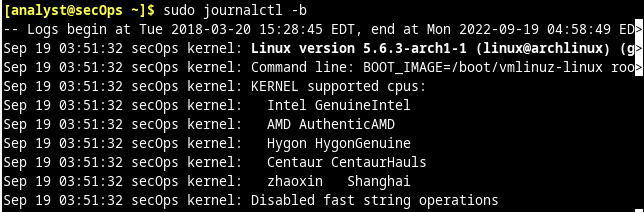


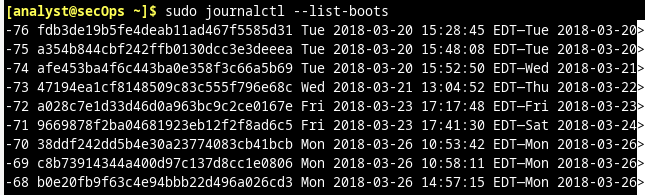
**Part 3: Monitoring Log Files in Real Time**

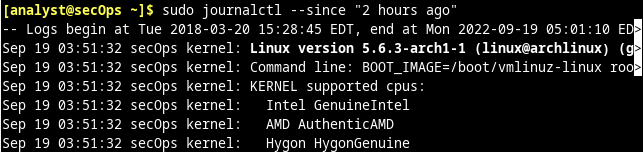
a. Use the tail command to display the end of the /var/log/nginx/access.log.   
[analyst@secOps ~]$ sudo tail /var/log/nginx/access.log  


a. [analyst@secOps ~]$ journalctl  


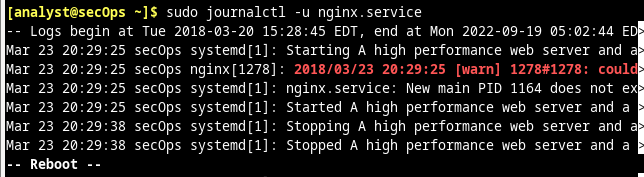
How can you run journalctl and see all log entries  
Running journalctl as the root user will display all entries. To run journalctl as root, prepend the sudo command to journalctl: sudo journalctl.

b. [analyst@secOps ~]$ sudo journalctl –b  


d. Use the --list-boots option to list previous boots:   
[analyst@secOps ~]$ sudo journalctl –-list-boots  


e. [analyst@secOps ~]$ sudo journalctl –-since "2 hours ago"  


[analyst@secOps ~]$ sudo journalctl –u nginx.service



[analyst@secOps ~]$ sudo journalctl –f