<hunter_strategy>

Linux Log Analysis: "Lastlog and Found"

Jake Williams, VP R&D
Jake.Williams@hunterstrategy.net

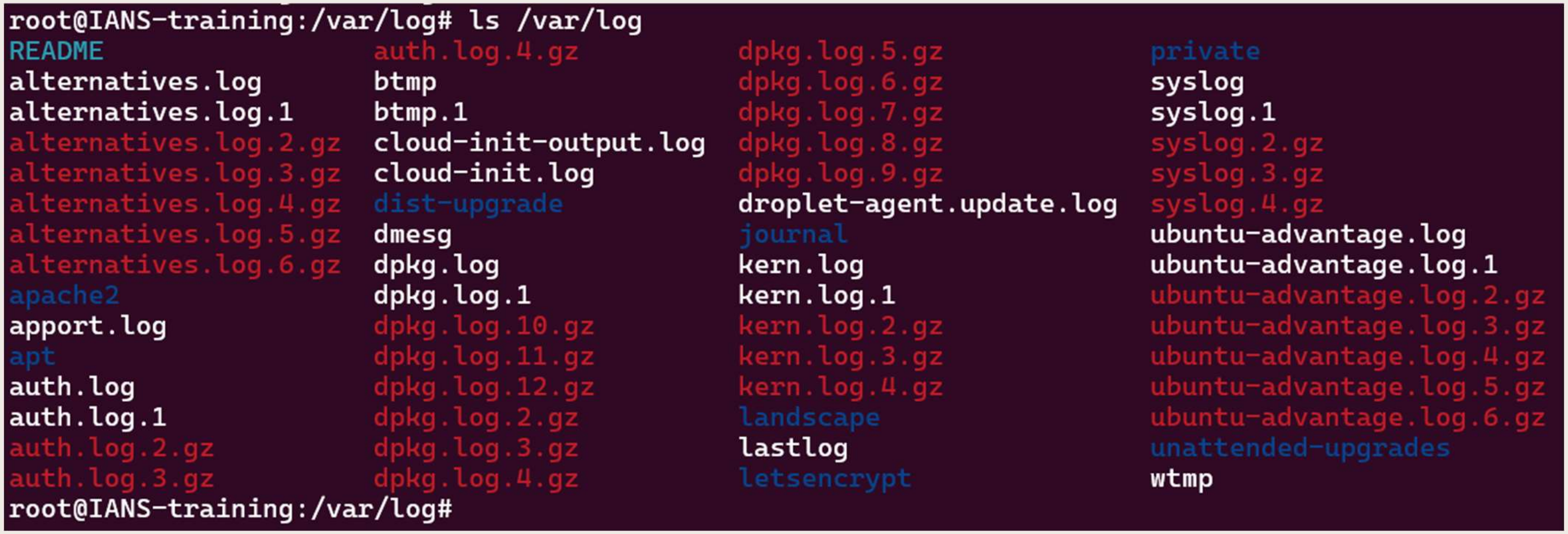
Agenda

Log Discussion

Log Analysis Hands-On

Where are Linux logs?

Linux logs are typically stored in /var/log



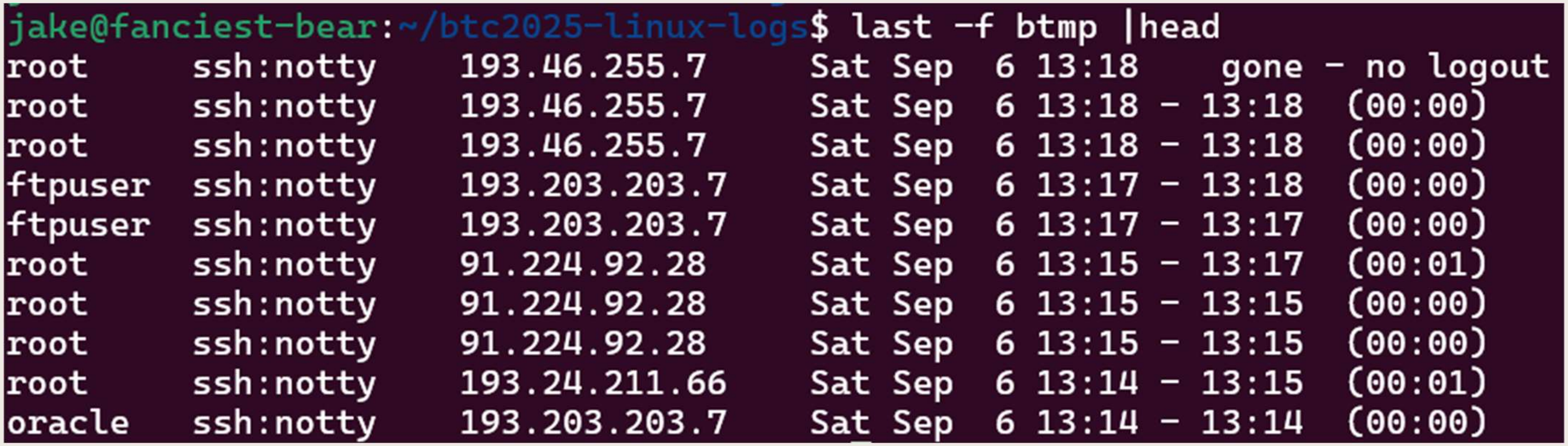
```
root@IANS-training:/var/log# ls /var/log
README                 auth.log.4.gz          dpkg.log.5.gz             private
alternatives.log       btmp                   dpkg.log.6.gz             syslog
alternatives.log.1     btmp.1                 dpkg.log.7.gz             syslog.1
alternatives.log.2.gz  cloud-init-output.log  dpkg.log.8.gz             syslog.2.gz
alternatives.log.3.gz  cloud-init.log         dpkg.log.9.gz             syslog.3.gz
alternatives.log.4.gz  dist-upgrade           droplet-agent.update.log  syslog.4.gz
alternatives.log.5.gz  dmesg                  journal                   ubuntu-advantage.log
alternatives.log.6.gz  dpkg.log               kern.log                  ubuntu-advantage.log.1
apache2                dpkg.log.1             kern.log.1                ubuntu-advantage.log.2.gz
apport.log             dpkg.log.10.gz         kern.log.2.gz             ubuntu-advantage.log.3.gz
apt                    dpkg.log.11.gz         kern.log.3.gz             ubuntu-advantage.log.4.gz
auth.log               dpkg.log.12.gz         kern.log.4.gz             ubuntu-advantage.log.5.gz
auth.log.1             dpkg.log.2.gz          landscape                 ubuntu-advantage.log.6.gz
auth.log.2.gz          dpkg.log.3.gz          lastlog                   unattended-upgrades
auth.log.3.gz          dpkg.log.4.gz          letsencrypt               wtmp
root@IANS-training:/var/log#
```

Log Files

Log file	Purpose
auth.log	Authentication event details (e.g., password or public key, failed or successful).
btmp	Failed logins with source IP.
dmesg	Kernel ring buffer that starts at boot, useful for finding rootkits and troubleshooting hardware errors.
dpkg.log	Software installed through the Debian package manager.
kern.log	Kernel debug messages, useful for finding rootkits and troubleshooting hardware errors.
lastlog	Records the most recent login for each user, helps find dormant accounts.
syslog	Generic system messages that aren't specific to another log (/var/log/messages on many systems).
wtmp	Successful logins with source IP.
	In /var/log/apache2
access.log	Web server access logs. Includes successful and unsuccessful attempts that aren't server errors.
error.log	Web server error logs. Includes 500 error codes (server failures).

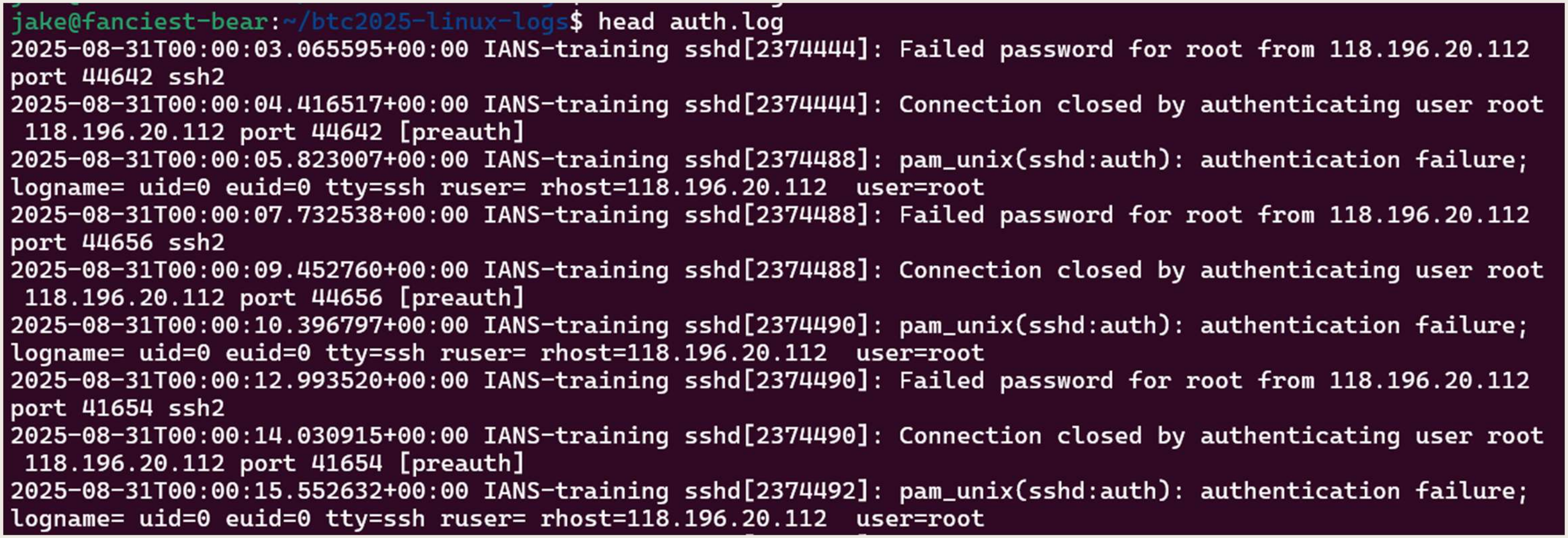
Using last to look at logs

The last command parses the lastlog, btmp, and wtmp files.



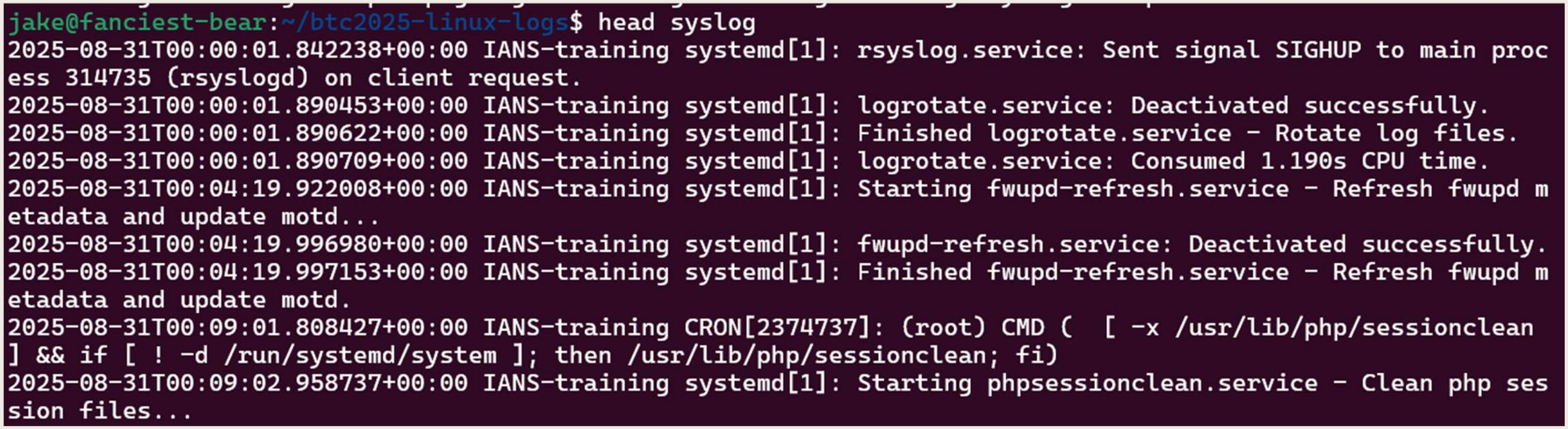
```
jake@fanciest-bear:~/btc2025-linux-logs$ last -f btmp |head
root     ssh:notty    193.46.255.7     Sat Sep  6 13:18   gone - no logout
root     ssh:notty    193.46.255.7     Sat Sep  6 13:18 - 13:18  (00:00)
root     ssh:notty    193.46.255.7     Sat Sep  6 13:18 - 13:18  (00:00)
ftpuser  ssh:notty    193.203.203.7    Sat Sep  6 13:17 - 13:18  (00:00)
ftpuser  ssh:notty    193.203.203.7    Sat Sep  6 13:17 - 13:17  (00:00)
root     ssh:notty    91.224.92.28     Sat Sep  6 13:15 - 13:17  (00:01)
root     ssh:notty    91.224.92.28     Sat Sep  6 13:15 - 13:15  (00:00)
root     ssh:notty    91.224.92.28     Sat Sep  6 13:15 - 13:15  (00:00)
root     ssh:notty    193.24.211.66    Sat Sep  6 13:14 - 13:15  (00:01)
oracle   ssh:notty    193.203.203.7    Sat Sep  6 13:14 - 13:14  (00:00)
```

Auth.log Shows Details



```
jake@fanciest-bear:~/btc2025-linux-logs$ head auth.log
2025-08-31T00:00:03.065595+00:00 IANS-training sshd[2374444]: Failed password for root from 118.196.20.112
port 44642 ssh2
2025-08-31T00:00:04.416517+00:00 IANS-training sshd[2374444]: Connection closed by authenticating user root
 118.196.20.112 port 44642 [preauth]
2025-08-31T00:00:05.823007+00:00 IANS-training sshd[2374488]: pam_unix(sshd:auth): authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=118.196.20.112  user=root
2025-08-31T00:00:07.732538+00:00 IANS-training sshd[2374488]: Failed password for root from 118.196.20.112
port 44656 ssh2
2025-08-31T00:00:09.452760+00:00 IANS-training sshd[2374488]: Connection closed by authenticating user root
 118.196.20.112 port 44656 [preauth]
2025-08-31T00:00:10.396797+00:00 IANS-training sshd[2374490]: pam_unix(sshd:auth): authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=118.196.20.112  user=root
2025-08-31T00:00:12.993520+00:00 IANS-training sshd[2374490]: Failed password for root from 118.196.20.112
port 41654 ssh2
2025-08-31T00:00:14.030915+00:00 IANS-training sshd[2374490]: Connection closed by authenticating user root
 118.196.20.112 port 41654 [preauth]
2025-08-31T00:00:15.552632+00:00 IANS-training sshd[2374492]: pam_unix(sshd:auth): authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=118.196.20.112  user=root
```

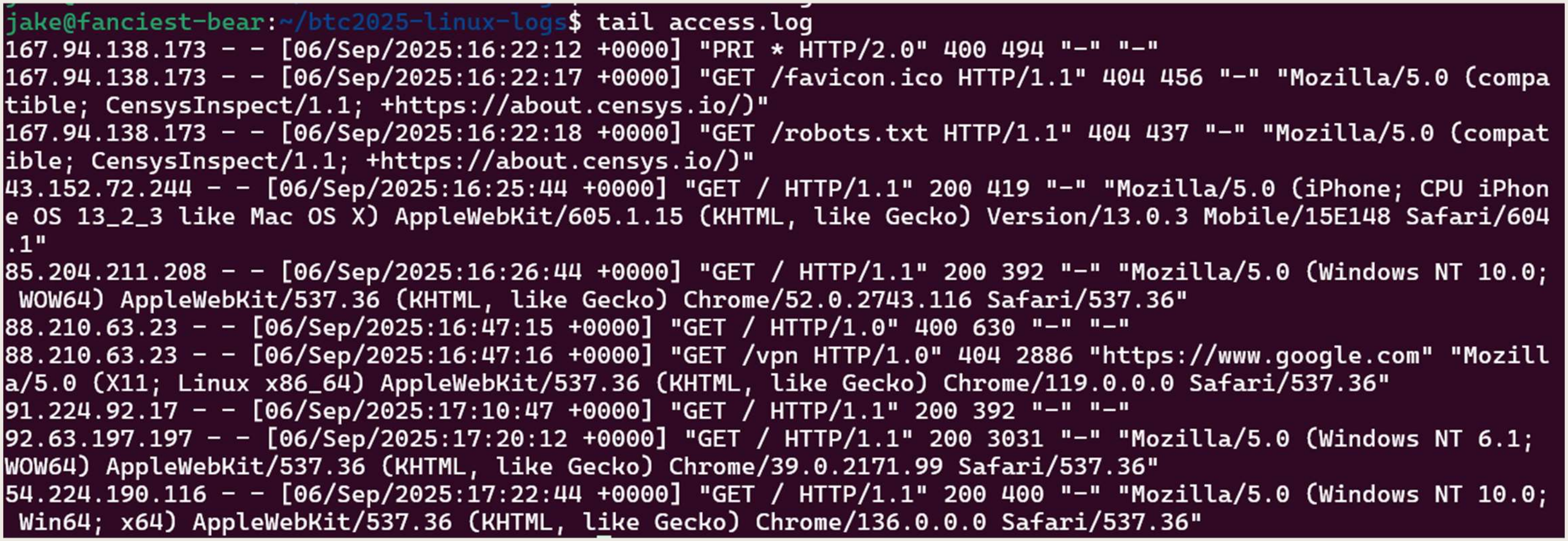
Syslog shows general log messages



```
jake@fanciest-bear:~/btc2025-linux-logs$ head syslog
2025-08-31T00:00:01.842238+00:00 IANS-training systemd[1]: rsyslog.service: Sent signal SIGHUP to main proc
ess 314735 (rsyslogd) on client request.
2025-08-31T00:00:01.890453+00:00 IANS-training systemd[1]: logrotate.service: Deactivated successfully.
2025-08-31T00:00:01.890622+00:00 IANS-training systemd[1]: Finished logrotate.service - Rotate log files.
2025-08-31T00:00:01.890709+00:00 IANS-training systemd[1]: logrotate.service: Consumed 1.190s CPU time.
2025-08-31T00:04:19.922008+00:00 IANS-training systemd[1]: Starting fwupd-refresh.service - Refresh fwupd m
etadata and update motd...
2025-08-31T00:04:19.996980+00:00 IANS-training systemd[1]: fwupd-refresh.service: Deactivated successfully.
2025-08-31T00:04:19.997153+00:00 IANS-training systemd[1]: Finished fwupd-refresh.service - Refresh fwupd m
etadata and update motd.
2025-08-31T00:09:01.808427+00:00 IANS-training CRON[2374737]: (root) CMD (   [ -x /usr/lib/php/sessionclean
] && if [ ! -d /run/systemd/system ]; then /usr/lib/php/sessionclean; fi)
2025-08-31T00:09:02.958737+00:00 IANS-training systemd[1]: Starting phpsessionclean.service - Clean php ses
sion files...
```

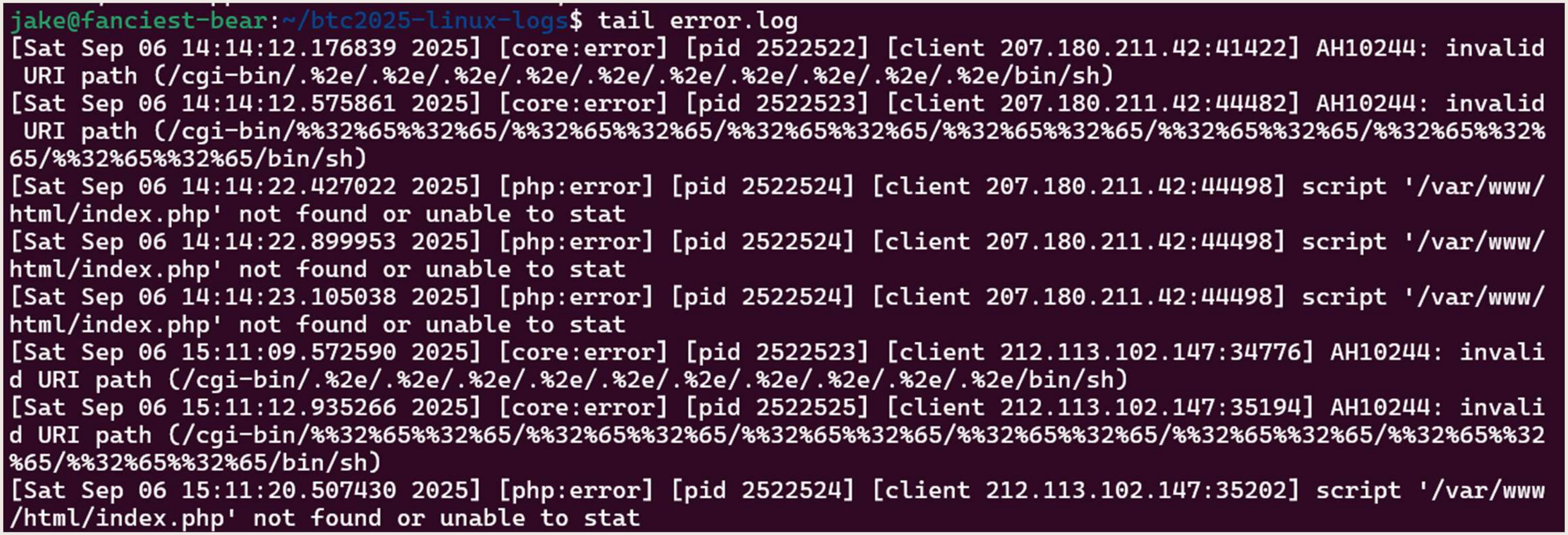
Apache Access Logs

Note the attempted path traversal attack from 212.113.102.147



```
jake@fanciest-bear:~/btc2025-linux-logs$ tail access.log
167.94.138.173 - - [06/Sep/2025:16:22:12 +0000] "PRI * HTTP/2.0" 400 494 "-" "-"
167.94.138.173 - - [06/Sep/2025:16:22:17 +0000] "GET /favicon.ico HTTP/1.1" 404 456 "-" "Mozilla/5.0 (compa
tible; CensysInspect/1.1; +https://about.censys.io/)"
167.94.138.173 - - [06/Sep/2025:16:22:18 +0000] "GET /robots.txt HTTP/1.1" 404 437 "-" "Mozilla/5.0 (compat
ible; CensysInspect/1.1; +https://about.censys.io/)"
43.152.72.244 - - [06/Sep/2025:16:25:44 +0000] "GET / HTTP/1.1" 200 419 "-" "Mozilla/5.0 (iPhone; CPU iPhon
e OS 13_2_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.0.3 Mobile/15E148 Safari/604
.1"
85.204.211.208 - - [06/Sep/2025:16:26:44 +0000] "GET / HTTP/1.1" 200 392 "-" "Mozilla/5.0 (Windows NT 10.0;
 WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36"
88.210.63.23 - - [06/Sep/2025:16:47:15 +0000] "GET / HTTP/1.0" 400 630 "-" "-"
88.210.63.23 - - [06/Sep/2025:16:47:16 +0000] "GET /vpn HTTP/1.0" 404 2886 "https://www.google.com" "Mozill
a/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36"
91.224.92.17 - - [06/Sep/2025:17:10:47 +0000] "GET / HTTP/1.1" 200 392 "-" "-"
92.63.197.197 - - [06/Sep/2025:17:20:12 +0000] "GET / HTTP/1.1" 200 3031 "-" "Mozilla/5.0 (Windows NT 6.1;
WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.99 Safari/537.36"
54.224.190.116 - - [06/Sep/2025:17:22:44 +0000] "GET / HTTP/1.1" 200 400 "-" "Mozilla/5.0 (Windows NT 10.0;
 Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36"
```

Apache Error Logs



```
jake@fanciest-bear:~/btc2025-linux-logs$ tail error.log
[Sat Sep 06 14:14:12.176839 2025] [core:error] [pid 2522522] [client 207.180.211.42:41422] AH10244: invalid
 URI path (/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh)
[Sat Sep 06 14:14:12.575861 2025] [core:error] [pid 2522523] [client 207.180.211.42:44482] AH10244: invalid
 URI path (/cgi-bin/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%
65/%%32%65%%32%65/bin/sh)
[Sat Sep 06 14:14:22.427022 2025] [php:error] [pid 2522524] [client 207.180.211.42:44498] script '/var/www/
html/index.php' not found or unable to stat
[Sat Sep 06 14:14:22.899953 2025] [php:error] [pid 2522524] [client 207.180.211.42:44498] script '/var/www/
html/index.php' not found or unable to stat
[Sat Sep 06 14:14:23.105038 2025] [php:error] [pid 2522524] [client 207.180.211.42:44498] script '/var/www/
html/index.php' not found or unable to stat
[Sat Sep 06 15:11:09.572590 2025] [core:error] [pid 2522523] [client 212.113.102.147:34776] AH10244: invali
d URI path (/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh)
[Sat Sep 06 15:11:12.935266 2025] [core:error] [pid 2522525] [client 212.113.102.147:35194] AH10244: invali
d URI path (/cgi-bin/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32
%65/%%32%65%%32%65/bin/sh)
[Sat Sep 06 15:11:20.507430 2025] [php:error] [pid 2522524] [client 212.113.102.147:35202] script '/var/www
/html/index.php' not found or unable to stat
```

Hands-On Time!

Let's do some command line Kung Fu!