Log Files and Logrotate

Andrew Mallett
LINUX AUTHOR AND TRAINER

@theurbanpenguin web.theurbanpenguin.com

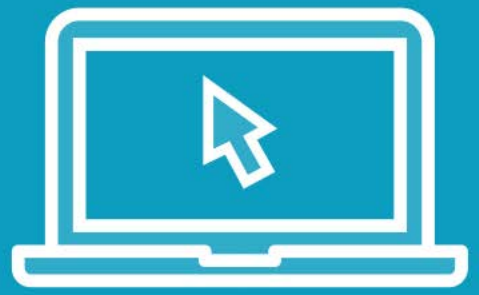
Exam Objectives

Locate and analyze system log files

Monitor security and conduct audits

Script automation tools to make work faster and more accurate

Demo



Audit login events

Audit access sudo and su

Scripting awk to analyze logs

Configuring system logging

Rotating log files with logrotate

Using systemd and journalctl

Auditing Login Events

Auditing Root Access

Scripting awk to Analyse Logs

Configuring System Logging

Rotating Log Files

Using Journalctl

Audit Logins

lastlog

last

lastb

Audit Root Access

/var/log/secure

sudo:

su:

awk

```
awk '/sudo/ { print $5,$6,$14 }' /var/log/secure
```

rsyslogd

/etc/rsyslog.conf

local1.info /var/log/service_log

systemctl restart rsyslogd.service

logger -p local1.warn “Script ended”

Rotate Logs

/etc/logrotate.conf

/etc/cron.daily/

logrotate /etc/logrotate.conf

journalctl

journalctl

journalctl -n

journalctl --since “10 minutes ago”

journalctl -b

mkdir /var/log/journal

Next Up: Introducing SELinux