Introducing SELinux

Andrew Mallett

LINUX AUTHOR AND TRAINER

@theurbanpenguin   web.theurbanpenguin.com
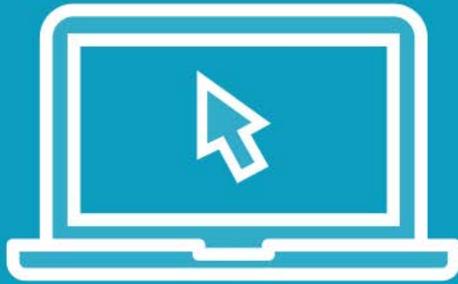
Exam Objectives

List and identify SELinux/AppArmor file and process

Configure and modify SELinux/AppArmor policies

Demo

View SELinux status and understand modes and context

View SELinux logs

Working with SELinux booleans

Working with SELinux ports

View SELinux Modes and Context

View SELinux Logs

Working with SELinux Booleans

Working with SELinux Ports

SELinux Status

sestatus

getenforce

setenforce 0 | 1

/etc/selinux/config

$ ls -Z <file>

$ ps -Z <pid>

$ id -Z

Logs and Commands

/var/log/audit/audit.log

ausearch -m avc

ausearch -m avc -ts recent

restorecon /etc/shadow

chcon -t shadow_t /etc/shadow

Booleans and Ports

```
# getsebool -a

# semanage boolean -l

# setsebool httpd_read_user_content on

# -P To make permanent

# semange port -l

# semange port -at ssh_port_t -p tcp 1111
```

Next Up: Managing Software on CentOS 7