



Auditing Security Related Events

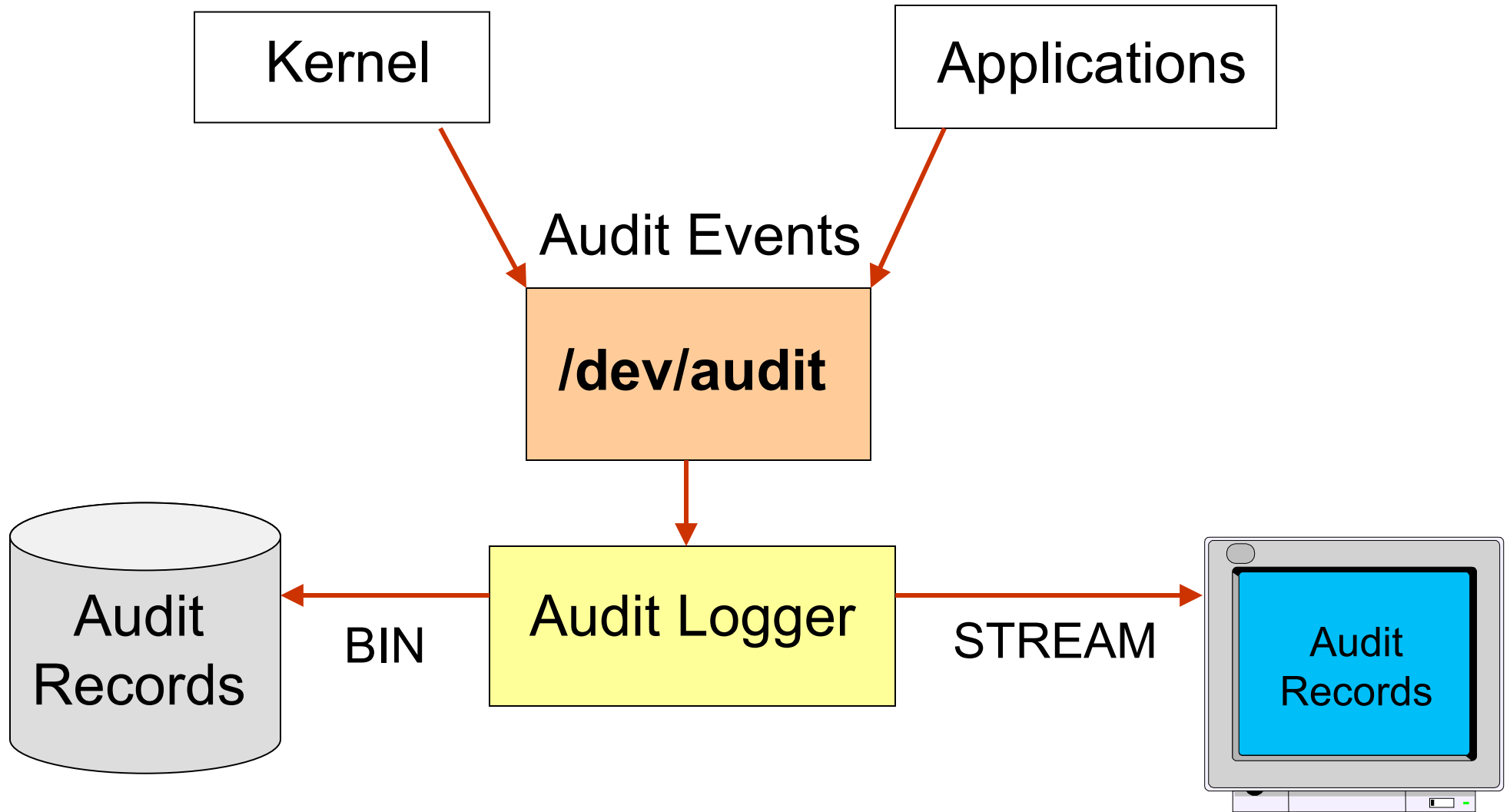


Appendix Objectives

After completing this appendix, you should be able to:

- Configure the auditing subsystem

How the Auditing Subsystem Works



Auditing Configuration Files

/etc/security/audit/objects	Contains the <i>audit events</i> triggered by file access
/etc/security/audit/events	Contains information about system <i>audit events</i> and <i>responses</i> to those events
/etc/security/audit/config	Contains <i>audit configuration</i> information: <ul style="list-style-type: none">- Start Mode- Audit Classes- Audited Users

Audit Configuration: objects

```
# vi /etc/security/audit/objects
```

```
/etc/security/user:
```

```
w = "S_USER_WRITE"
```

```
...
```

```
/etc/filesystems:
```

```
w = "MY_EVENT"
```

```
/usr/sbin/no:
```

```
x = "MY_X_EVENT"
```

Audit Configuration: events

```
# vi /etc/security/audit/events  
auditpr:
```

```
USER_Login    = printf "user: %s tty: %s"  
USER_Logout  = printf "%s"
```

```
...
```

```
MY_EVENT = printf "%s"
```

```
MY_X_EVENT = printf "%s"
```

Audit Configuration: config

```
# vi /etc/security/audit/config
```

start:

```
binmode = off  
streammode = on
```

```
...
```

classes:

```
general = USER_SU, PASSWORD_Change, ...  
tcPIP = TCPIP_connect, TCPIP_data_in, ...  
...  
init = USER_Login, USER_Logout
```

users:

```
root = general  
michael = init
```

Audit Configuration: bin Mode

```
# vi /etc/security/audit/config
```

start:

```
binmode = on
```

```
streammode = off
```

bin:

```
trail = /audit/trail
```

```
bin1 = /audit/bin1
```

```
bin2 = /audit/bin2
```

```
binsize = 10240
```

```
cmds = /etc/security/audit/bincmds
```

...

- Use the **auditpr** command to display the audit records:

```
# auditpr -v < /audit/trail
```

Audit Configuration: stream Mode

```
# vi /etc/security/audit/config

start:
    binmode = off
    streammode = on

stream:
    cmds = /etc/security/audit/streamcmds

...

# vi /etc/security/audit/streamcmds

/usr/sbin/auditstream | auditpr -v > /dev/console &
```

All audit records are displayed on the console

The audit Command

audit start

—————→ Start / Stop auditing

audit shutdown

audit query

—————→ Display audit status

audit off

—————→ Suspend / Restart auditing

audit on

Example Audit Records

Event	Login	Status	Time	Command
MY_X_EVENT	root	OK	Tue Aug 09	no
audit object exec event detected /usr/bin/no				
MY_EVENT	root	OK	Thu Aug 09	vi
audit object write event detected /etc/filesystems				
USER_Logout	michael	OK	Thu Aug 09	logout
/dev/pts/0				

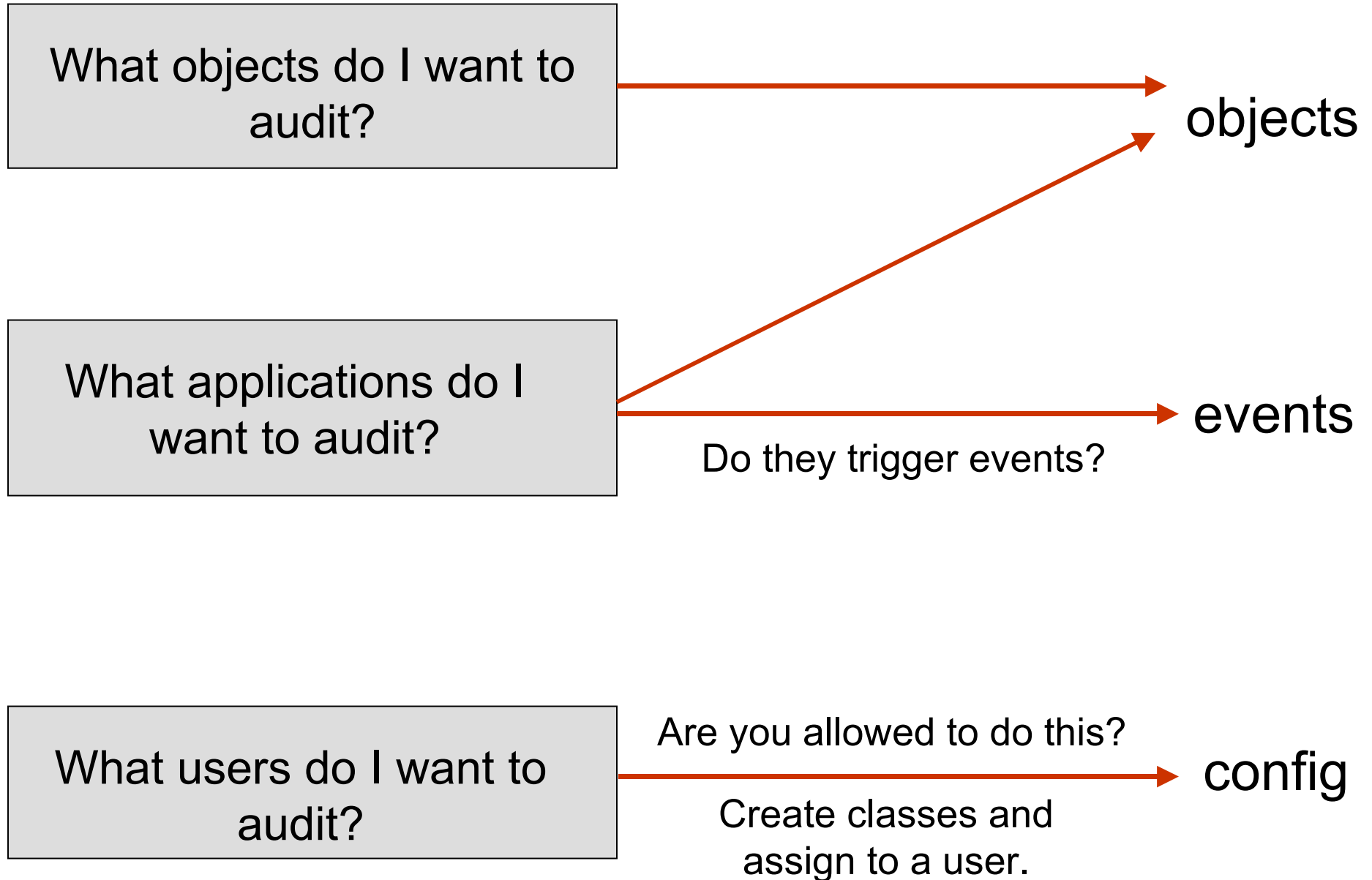


Audit tail

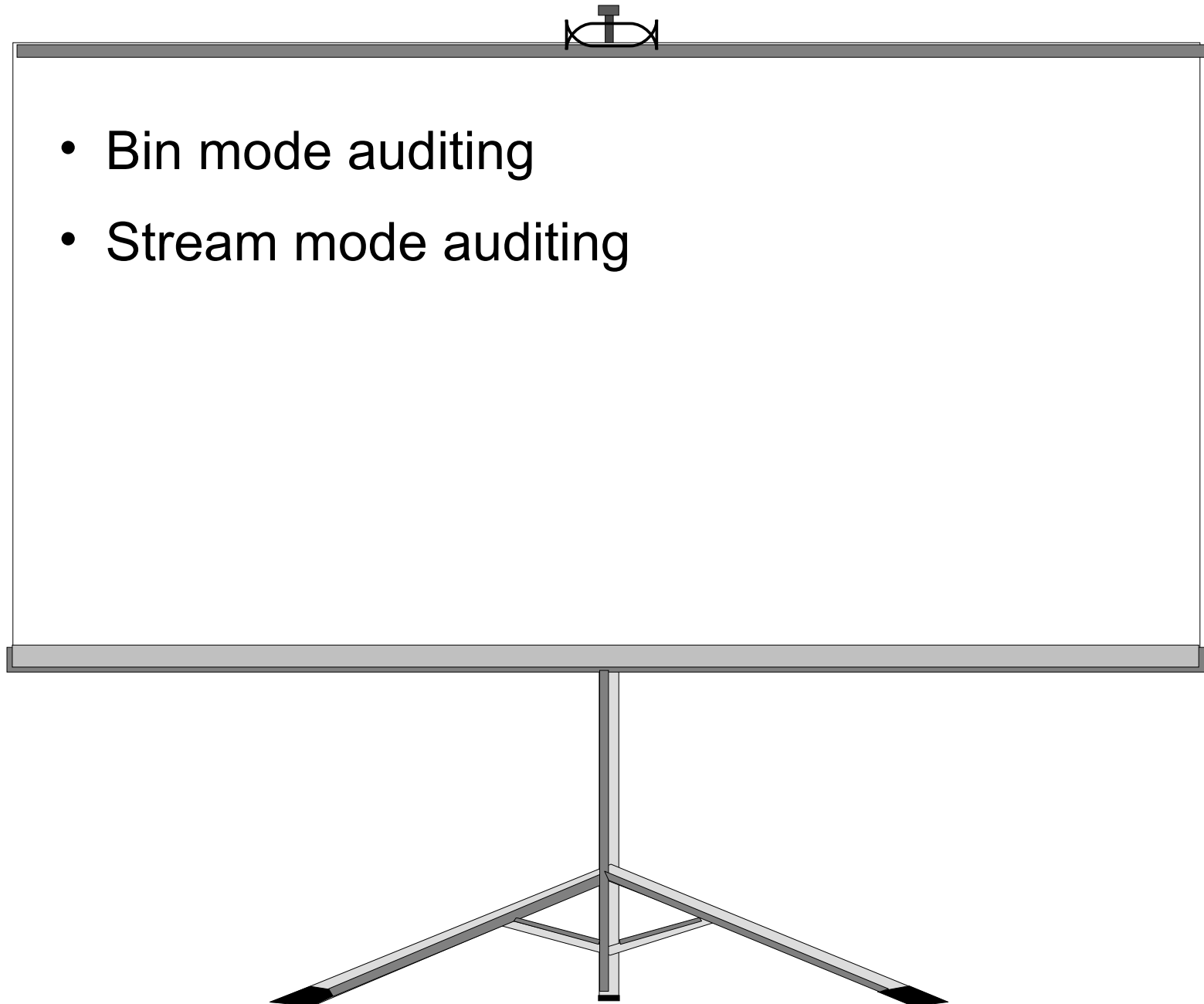


Audit header

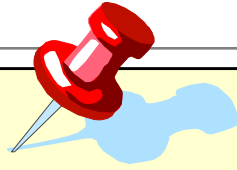
Set Up Auditing in Your Environment



Exercise: Auditing



Appendix Summary



Having completed this appendix, you should be able to:

- Configure the auditing subsystem