**Review**

- Summarize what you learned from the section 2 lectures

**Activity 1**

What is freeRadius?

**Activity 2**

Locate the logs on your computer that show successful and failed authentication. On a Windows system, they can be found by right-clicking My Computer and selecting Manage. Then, in the computer Management dialog box, expand the Event Viewer in the left column. Expand Windows Logs and select Security. On a Ubuntu Linux system (and many other Linux distributions), the authentication logs can be found in /var/log/auth.log.

Locate any failed logon attempts.

Document how you would configure the maximum size of a log file and what the system will do when that maximum size is reached.

**Activity 3**

- [An example of Identity Management from IBM](http://www.microsoft.com/en-us/server-cloud/products/forefront-identity-manager/try.aspx)
- Experimenting with Identity management (if you want to play with it, can’t all do as a class or we overwhelm servers)
  - I was successful using a windows IE and linux ff
  - what is provisioning?

**Activity 4**

First, research what apparmor is:

- [http://askubuntu.com/questions/236381/what-is-apparmor](http://askubuntu.com/questions/236381/what-is-apparmor)
- [https://help.ubuntu.com/community/AppArmor](https://help.ubuntu.com/community/AppArmor)

Questions:

How does this relate to our current topics?

**Activity 5**
• Try apparmor
  ◦ Here
• Using one time passwords
  ◦ https://www.digitalocean.com/community/tutorials/install-and-use-otpw

Activity 5

More Linux user security:

• chage
• ulimit (can’t really test this, but see man page for what it does)
• /etc/security

Activity 6

Encryption?? Labs and help?