CS 409
Quiz 1 Key

1. What does the following sudoers file accomplish?

User_Alias DOGS = terriers, shepards
User_Alias CATS = tabby, siamese
Cmd_Alias BARKING = /usr/sbin/woof, /sbin/yelp
Cmd_Alias MEOWING = /usr/bin/mew, /bin/hiss
DOGS ALL = (watchdog) BARKING, /usr/sbin/skulking
CATS localhost = MEOWING, BARKING, !/usr/sbin/woof
master ALL = (#1) NOPASSWD: ALL, (root) /usr/sbin/useradd, /usr/sbin/userdel

(a) Users terriers and shepards can execute /usr/sbin/woof, /sbin/yelp and /usr/sbin/skulking as watchdog and they can access this systems sudo from any other host.

(b) Users tabby and siamese can execute /usr/sbin/mew, /bin/hiss and /usr/sbin/yelp as root but only from the local host.

(c) User master can access all commands as user UID=1 without a password from any host. master can execute /usr/sbin/useradd and /usr/sbin/userdel as root from any host.

2. What are the things that have to happen to add a user to the system that should be able to log in and work from the host?

The following things need to happen.

- Add the user to the passwd file.
- Add the user to the shadow file (if needed).
- Add a new group (if needed).
- Create a home directory.
- Provide initial configuration files (from skel).
- Set up quotas (if needed).
- Set up a mail file (if needed).
3. Suppose you use shadow passwords but someone gets a copy of your password file. What are four things that they can learn that might lead to your system being vulnerable to attack.

(a) If there are any users equivalent to root.

(b) What users are interactive for password attacks.

(c) The presence of old/unused accounts.

(d) Useful finger information for password testing.

(e) Shared accounts where activity may not be noticed.

(f) Telephone numbers (for modem attacks).

(g) Accounts set up for remote access.

(h) What services might be running.