Kimberly Mackey

Cit220

1. Describe UNIX groups and how they improve access control and security. Give 5 example groups that you think might be useful on a college UNIX system, including the names of the groups and what they control access to. (5 points)

It groups allows it users to be able to run their own processes and not allow other users to interfere in the processes as well as places restrictions on what the user is able to access and what kind of restrictions are put on the user's profile.

On a college unix system I would imagine the college would have multiple different groups. A student group, which I assume would be divided more by the specific program the student is studying. The student might also be in multiple groups depending on if there is a specific group needed for a class. These groups would have basic access for certain files, and limited access on what they can do to prevent any cheating or misconduct, or some accidental failure. I would also imagine the college would have another group for professors. They would be a higher level of access since they would need to check on the students as well as to add, delete users and groups for their students. A college would also need an IT group. They would have different access to allow them to do updates, upgrades, and troubleshooting needs.

1. Log into thompson and use the 'id' command. What groups are you a member of? If you had to guess, what do you think these groups control access to? (2 points)

I am a member of two groups 1001 developers and 1094 cit220. I believe these groups gives us access to be able to modify and download certain programs needed for programing as well as permissions be able to access certain files needed for class assignments.

1. Most UNIX systems have user accounts such as "mail", "mysql", "www-data" and others that have no home directories and their login shell is set to /usr/bin/nologin - In other words, these accounts cannot log in and have no home directories. They are used only by the system to run services such as a mail or web server. How does this help improve security on UNIX systems? (3 points)

They get their own main user account; the user accounts sole purpose is to run the software so when you open the program you don’t have to log in and that’s why it doesn’t have a home directory.

1. Why is it important not to use 'root' as your primary login for normal day-to-day activities? (3 points)

Since root has the most power, it’s also the most vulnerable. You could accidently delete something important that would no longer be recoverable. Also, if the device you are using becomes compromised than that person now has full access and permissions to the entire device, instead of the limited access it would have had, being logged in as a regular user.

1. Scenario: Alice has an account on a FreeBSD system. She tries to use 'su' to become root, but this keeps failing even though she knows the root password and is typing it correctly. What is the reason why she is not succeeding? (2 points)

FreeBSD requires its users to be in a wheel group in order to use the ‘su’ command, more than likely Alices user name isn’t added into that wheel group therefor she wouldn’t have access.