GALGOTIAS UNIVERSITY

School of Computing Science and Engineering

Program: BSC (Hons) CS

Course Code: BSCS3560

Course Name: Linux Administration

Lecture : 19

UNIT III

MONITORING LINUX USERS

- User creating and management commands - /etc/password - /etc/shadow and /etc/group - Users and access permissions – Modifying user and group attributed.

There are three types of accounts on a Linux system

- Root account
- System accounts
- User accounts

- **Root account**

This is also called **superuser** and would have complete and unfettered control of the system. A superuser can run any commands without any restriction. This user should be assumed as a system administrator.

- **System accounts**

System accounts are those needed for the operation of system-specific components for example mail accounts and the **sshd** accounts. These accounts are usually needed for some specific function on your system, and any modifications to them could adversely affect the system.

- **User accounts**

User accounts provide interactive access to the system for users and groups of users. General users are typically assigned to these accounts and usually have limited access to critical system files and directories.

- Unix supports a concept of *Group Account* which logically groups a number of accounts. Every account would be a part of another group account. A Unix group plays important role in handling file permissions and process management.

Managing Users and Groups

- One of the key administrative tasks with Linux is managing users and groups.

- The primary reason for user accounts is to verify the identity of each individual using a computer system.
  - A secondary reason for user accounts is to permit the per-individual tailoring of resources and access privileges.
    - Resources can include files, directories, and devices. Controlling access to these resources is a primary task of an administrator

Groups tie together users that have a common purpose.

– an organization may have persons responsible for accounts payable and others responsible for payroll.

- By placing the user accounts in an accounts payable group then common permissions can be given to all the members of that group.
- Members of the accounts payable group would not have access to the information and resources of the payroll group. Users within the same group have the same read, write or execute privileges of group resources.

etc

- Several files are used when creating users in Linux. The following are four main user administration files.

/etc/passwd

/etc/shadow

/etc/group

/etc/gshadow

/etc/passwd

- The /etc/passwd file contains the user ID, and default home directory. Because this file is used by many tools it needs to be readable by any user.
- To view the /etc/passwd file use the less command.

  less /etc/passwd

  – The /etc/passwd file is a group of fields separated with a colon (**:**). They are username, password (shown as an x), numeric user ID, numeric group ID, full name, user's home directory, and user's shell account.

/etc/shadow

- The /etc/shadow file contains the encrypted passwords and other password information.
  - This file is viewable by the root user only.
- To view the /etc/shadow file use the following commands:

  su – root

  tail /etc/shadow
- The /etc/shadow file is a group of fields separated with a colon (**:**). They are:
  - Username
  - password (13 characters encrypted)
  - the number of days since the password was last changed
  - the number of days before the password may be changed
  - the number of days to warn a user of an expiring password
  - the number of days after a password expires that account is disabled
  - the number of days since an account has bee disabled
  - a reserved field for possible future use.


Thank You