LIMKOKWING UNIVERSITY OF CREATIVE TECHNOLOGY
ESWATINI

Bachelor Degree in Information Technology

Network Administration– BITNA4211

Trimester 6
From Jan2025 to April 2025

Account and Security Administration, and Access Control

INSTRUCTOR: MR S MAMBA

Account and Security Administration, and Access Control

- Nobody in an organization should have free rein to access any resource. Access control is the combination of policies and technologies that decide which authenticated users may access which resources. Security requirements, infrastructure, and other considerations lead companies to choose among the four most common access control models:
  - Mandatory Access Control (MAC)
  - Discretionary Access Control (DAC)
  - Role-Based Access Control (RBAC)
  - Privileged Access Management (PAM)

LIMKOKWING UNIVERSITY OF CREATIVE TECHNOLOGY
ESWATINI

What is mandatory access control (MAC)?

- Mandatory access control uses a centrally managed model to provide the highest level of security. A non-discretionary system, MAC reserves control over access policies to a centralized security administration.

- MAC works by applying security labels to resources and individuals. These security labels consist of two elements:

  - Classification and clearance — MAC relies on a classification system (restricted, secret, top-secret, etc.) that describes a resource's sensitivity. Users' security clearances determine what kinds of resources they may access.

  - Compartment — A resource's compartment describes the group of people (department, project team, etc.) allowed access. A user's compartment defines the group or groups they participate in.

- A user may only access a resource if their security label matches the resource's security label.

What is mandatory access control (MAC)?

- MAC originated in the military and intelligence community. Beyond the national security world, MAC implementations protect some companies' most sensitive resources. Banks and insurers, for example, may use MAC to control access to customer account data.

- Advantages of MAC
  - Enforceability — MAC administrators set organization-wide policies that users cannot override, making enforcement easier.
  - Compartmentalization — Security labels limit the exposure of each resource to a subset of the user base.

- Disadvantages of MAC
  - Collaboration — MAC achieves security by constraining communication. Highly collaborative organizations may need a less restrictive approach.
  - Management burden — A dedicated organizational structure must manage the creation and maintenance of security labels.

LIMKOKWING UNIVERSITY OF CREATIVE TECHNOLOGY
ESWATINI

What is discretionary access control (DAC)?

- Discretionary access control decentralizes security decisions to resource owners. The owner could be a document’s creator or a department’s system administrator. DAC systems use access control lists (ACLs) to determine who can access that resource. These tables pair individual and group identifiers with their access privileges.

- The sharing option in most operating systems is a form of DAC. For each document you own, you can set read/write privileges and password requirements within a table of individuals and user groups. System administrators can use similar techniques to secure access to network resources

LIMKOKWING UNIVERSITY OF CREATIVE TECHNOLOGY ESWATINI

What is discretionary access control (DAC)?..cont

- Advantages of DAC
  - Conceptual simplicity — ACLs pair a user with their access privileges. As long as the user is in the table and has the appropriate privileges, they may access the resource.
  - Responsiveness to business needs — Since policy change requests do not need to go through a security administration, decision-making is more nimble and aligned with business needs.
- Disadvantages of DAC
  - Over/underprivileged users — A user can be a member of multiple, nested workgroups. Conflicting permissions may over- or under privilege the user.
  - Limited control — Security administrators cannot easily see how resources are shared within the organization. And although viewing a resource’s ACL is straightforward, seeing one user’s privileges requires searching every ACL.
  - Compromised security — By giving users discretion over access policies, the resulting inconsistencies and missing oversight could undermine the organization’s security posture.

LIMKOKWING UNIVERSITY OF CREATIVE TECHNOLOGY
ESWATINI

What is role-based access control (RBAC)?

- Role-based access control grants access privileges based on the work that individual users do. A popular way of implementing “least privilege, policies, RBAC limits access to just the resources users need to do their jobs.

- Implementing RBAC requires defining the different roles within the organization and determining whether and to what degree those roles should have access to each resource.

- Accounts payable administrators and their supervisor, for example, can access the company’s payment system. The administrators’ role limits them to creating payments without approval authority. Supervisors, on the other hand, can approve payments but may not create them.

What is role-based access control (RBAC)?..cont

- Advantages of RBAC
  - Flexibility — Administrators can optimize an RBAC system by assigning users to multiple roles, creating hierarchies to account for levels of responsibility, constraining privileges to reflect business rules, and defining relationships between roles.
  - Ease of maintenance — With well-defined roles, the day-to-day management is the routine on-boarding, off-boarding, and cross-boarding of users' roles.
  - Centralized, non-discretionary policies — Security professionals can set consistent RBAC policies across the organization.
  - Lower risk exposure — Under RBAC, users only have access to the resources their roles justify, greatly limiting potential threat vectors.

- Disadvantages of RBAC
  - Complex deployment — The web of responsibilities and relationships in larger enterprises makes defining roles so challenging that it spawned its own subfield: role engineering.
  - Balancing security with simplicity — More roles and more granular roles provide greater security, but administering a system where users have dozens of overlapping roles becomes more difficult.
  - Layered roles and permissions — Assigning too many roles to users also increases the risk of over-privileging users.

LIMKOKWING UNIVERSITY OF CREATIVE TECHNOLOGY ESWATINI

What is Privileged Access Management (PAM)?

- A recent ThycoticCentrify study found that 53% of organizations experienced theft of privileged credentials and 85% of those thefts resulted in breaches of critical systems. Privileged access management is a type of role-based access control specifically designed to defend against these attacks.

- Based on least-privilege access principles, PAM gives administrators limited, ephemeral access privileges on an as-needed basis. These systems enforce network security best practices such as eliminating shared passwords and manual processes.

What is Privileged Access Management (PAM)?..cont

- Advantages of PAM
  - Reduced threat surface — Common passwords, shared credentials, and manual processes are commonplace even in the best-run IT departments. Imposing access control best practices eliminates these security risks.
  - Minimizing permission creep — PAM systems make it easier to revoke privileges when users no longer need them, thus preventing users from “collecting, access privileges.
  - Auditable logging — Monitoring privileged users for unusual behavior becomes easier with a PAM solution.
- Disadvantages of PAM
  - Internal resistance — Just as doctors make the worst patients, IT professionals can be resistant to tighter security measures.
  - Complexity and cost — Implementing PAM requires investments in time and money within already-constrained IT departments.

LIMKOKWING UNIVERSITY OF CREATIVE TECHNOLOGY ESWATINI

Where is access control headed?

- In fact, today’s complex IT environment is the reason companies want more dynamic access control solutions. Even before the pandemic, workplace transformation was driving technology to a more heterogeneous, less centralized ecosystem characterized by:
  - Device diversity — Bring-your-own-device policies and the Industrial Internet of Things create a diverse array of devices with different security profiles connecting to company resources.
  - Cloud and hybrid architectures — IT began leaving the premises decades ago. Getting business done now requires a mix of in-house, hybrid cloud, and X-as-a-Service resources.
  - Remote workforces — Remote working is no longer just for salespeople. Accelerated by the pandemic just about any employee may access sensitive resources from their home network.
  - Blended, dynamic teams — Security administrators must manage a constantly shifting workforce comprising employees, contractors, consultants, suppliers, and other third parties.

LIMKOKWING UNIVERSITY OF CREATIVE TECHNOLOGY ESWATINI

User and Group Concepts, and User Private Group Scheme

- User and group concepts are fundamental to Unix-like operating systems for managing permissions and access control. Here's a brief overview:
    - User: A user is an individual who interacts with the operating system. Each user has a unique username (login name) and a user ID (UID) assigned by the system. Users can own files and processes, and their permissions are used to control access to these resources.
    - Group: A group is a collection of users. It allows you to set permissions for multiple users at once, simplifying access control management. Each group has a unique group name and group ID (GID). Users can belong to one or more groups.
    - User Private Group (UPG) Scheme: The User Private Group scheme is a convention used in some Unix-like systems (like Ubuntu) where a new group with the same name as the user is created automatically when the user is added to the system. This group is the user's primary group, and it simplifies file sharing among users. By default, files created by a user are owned by the user and their primary group, which is the same as their username.
- Each user is associated with a unique numerical identification number called a user ID (UID). Likewise, each group is associated with a group ID (GID). A user who creates a file is also the owner and group owner of that file. The file is assigned separate read, write, and execute permissions for the owner, the group, and everyone else. The file owner can be changed only by root, and access permissions can be changed by both the root user and file owner.

User and Group Concepts, and User Private Group Scheme..cont

- Users must authenticate to any system they need to use. This authentication provides access to resources and a customized, user-specific environment. The user's identity is based on their user account. What skills do sysadmins need to manage user accounts?

- To create a new user in Linux, we can use the useradd command. This command creates a new user account and assigns a UID and GID. The syntax for creating a new user is:
- useradd [options] username
  - For example, to create a new user named "Abebe", we can use the following command:
  - sudo useradd Abebe

LIMKOKWING UNIVERSITY OF CREATIVE TECHNOLOGY ESWATINI

Modifying User Accounts

- To modify a user account in Linux, we can use the usermod command. This command allows us to change the user's password, home directory, shell, and more. The syntax for modifying a user account is:
  - usermod [options] username
- For example, to change the home directory of the user "Abebe", we can use the following command:
  - sudo usermod -d /home/Abebe.

Modifying User Accounts

- To delete a user account in Linux, we can use the userdel command. This command removes the user's account and home directory. The syntax for deleting a user account is:
  - userdel [options] username
- For example, to delete the user "Abebe", we can use the following command:
  - sudo userdel Abebe

LIMKOKWING UNIVERSITY OF CREATIVE TECHNOLOGY
ESWATINI

Managing Groups in Linux

- To create a new group in Linux, we can use the groupadd command. This command creates a new group and assigns a GID. The syntax for creating a new group is:
  - groupadd [options] groupname
- For example, to create a new group named "developers", we can use the following command:
  - sudo groupadd developers

Adding Users to a Group

- To add a user to a group in Linux, we can use the usermod command with the -aG option. This command adds a user to an existing group. The syntax for adding a user to a group is:
  - usermod -aG groupname username
- For example, to add the user "Abebe" to the "developers" group, we can use the following command:
  - sudo usermod -aG developers Abebe

Modifying Group Accounts

- To modify a group account in Linux, we can use the groupmod command. This command allows us to change the group's name and GID. The syntax for modifying a group account is:
  - groupmod [options] groupname
- For example, to change the name of the "developers" group to "devops", we can use the following command:
  - sudo groupmod -n devops developers

LIMKOKWING UNIVERSITY OF CREATIVE TECHNOLOGY ESWATINI

Mounting Additional File systems

- Deleting Group Accounts
- To delete a group account in Linux, we can use the groupdel command. This command removes the group from the system. The syntax for deleting a group account is:
    - groupdel groupname
- For example, to delete the "devops" group, we can use the following command:
    - sudo groupdel devops

Advanced User and Group Management in Linux

- In Linux, permissions define the actions that users and groups can perform on files and directories. Permissions are set using the chmod command and are represented by three categories: read (r), write (w), and execute (x). Each category can be assigned to the owner, group, or others. For example, to grant read and write permissions to the owner and read permission to the group and others for a file named "file.txt", we can use the following command:
  - chmod 644 file.txt.

sudo Access

- sudo is a powerful command that allows users to execute commands with the privileges of another user, typically the superuser (root). To grant sudo access to a user, we need to add the user to the sudoers file using the visudo command. For example, to grant sudo access to the user "Abebe", we can add the following line to the sudoers file:
- AbebeALL=(ALL) ALL
- This line indicates that the user "Abebe" can execute any command as any user on the system.

LIMKOKWING UNIVERSITY OF CREATIVE TECHNOLOGY ESWATINI

Password Aging and Default User Files

- System administration involves numerous tasks including managing users/groups and under user management, some of the minor tasks involved are adding, modifying, suspending, or deactivating user accounts, and many more.
- The chage command is used to modify user password expiry information. It enables you to view user account aging information, change the number of days between password changes and the date of the last password change.
- Once you have set password expiry and aging information, this information is used by the system to determine when a user must change his/her password. Normally, companies or organizations have certain security polices that demand users to change passwords regularly: this can be a simple way to enforce such policies as we explained below.

Managing files and folder permission

- For many users of Linux, getting used to file permissions and ownership can be a bit of a challenge. It is commonly assumed, to get into this level of usage, the command line is a must. Although there is always far more power and flexibility to be had, running seemingly complicated command isn’t always a necessity. With the help of some of the most user-friendly desktop interfaces available, you can get away with little to no command line usage. Even with file permission and ownership.

Command line: File permissions

- The commands for modifying file permissions and ownership are:
  - chmod – change permissions
  - chown – change ownership.
- Neither command is difficult to use. It is important, however, that you understand the only user that can actually modify the permissions or ownership of a file is either the current owner or the root user. So, if you are user Bethany, you cannot make changes to files and folders owned by Jacob without the help of root (or sudo).

LIMKOKWING UNIVERSITY OF CREATIVE TECHNOLOGY ESWATINI

For example

- A new folder was created on a data partition called /DATA/SHARE. Both users Bethany and Jacob need read and write access to this folder. There are a number of ways this can be done (one of which would be to join the users to a special group – we'll go over managing groups in another post). If Bethany and Jacob are the only users on the system (and you know your network is safe – very important), you can change the permissions of the folder to give them access. One way to do this would be to issue the command:
    - `sudo chmod -R ugo+rw /DATA/SHARE`

LIMKOKWING UNIVERSITY OF CREATIVE TECHNOLOGY
ESWATINI

For example..cont

- The breakdown of the above command looks like:
  - sudo – this is used to gain admin rights for the command on any system that makes use of sudo (otherwise you'd have to 'su' to root and run the above command without 'sudo')
  - chmod – the command to modify permissions
  - -R – this modifies the permission of the parent folder and the child objects within
  - ugo+rw – this gives User, Group, and Other read and write access.
- As you can probably surmise, this command opens wide the SHARE folder such that anyone on the system can have access to that folder. As I mentioned earlier, a more secure method would be to use groups. But we're just using this for the purpose of demonstration.

LIMKOKWING UNIVERSITY OF CREATIVE TECHNOLOGY
ESWATINI

For example..cont

- The breakdown of permissions looks like this:
  - u – user
  - g – group
  - o – other
- The ‘other’ entry is the dangerous one, as it effectively gives everyone permission for the folder/file. The permissions you can give to a file or folder are:
  - r – read
  - w – write
  - x – execute
- Using the -R switch is important. If you have a number of sub-folders and files within the SHARE directory, and you want the permissions to apply from the parent object (the containing folder) to the child objects (the sub-folders and files), you must use the -R (recursive) switch so the same permissions are applied all the way to the deepest folder, contained within the parent.

Command line: File ownership

- Changing the ownership of a file or folder is equally as simple. Say Jacob moved a folder for Bethany into the SHARE directory – but Jacob still has ownership. This can be changed with a simple command:
  - sudo chown -R bethany /DATA/SHARE
- Let’s break this down.
  - sudo – admin rights must be used since we are dealing with a folder that belongs to another user
  - chown – the command for changing ownership
  - -R – the recursive switch to make sure all child objects get the same ownership changes
  - bethany – the new owner of the folder
  - /DATA/SHARE – the directory to be modified

LIMKOKWING UNIVERSITY OF CREATIVE TECHNOLOGY
ESWATINI

GUI: File permissions

- Displaying the file contents on the terminal:
  - cat: It is generally used to concatenate the files. It gives the output on the standard output.
  - more: It is a filter for paging through text one screenful at a time.
  - less: It is used to viewing the files instead of opening the file.Similar to more command but it allows backward as well as forward movement.
  - head : Used to print the first N lines of a file. It accepts N as input and the default value of N is 10.
  - tail : Used to print the last N-1 lines of a file. It accepts N as input and the default value of N is 10.

Managing File Ownership

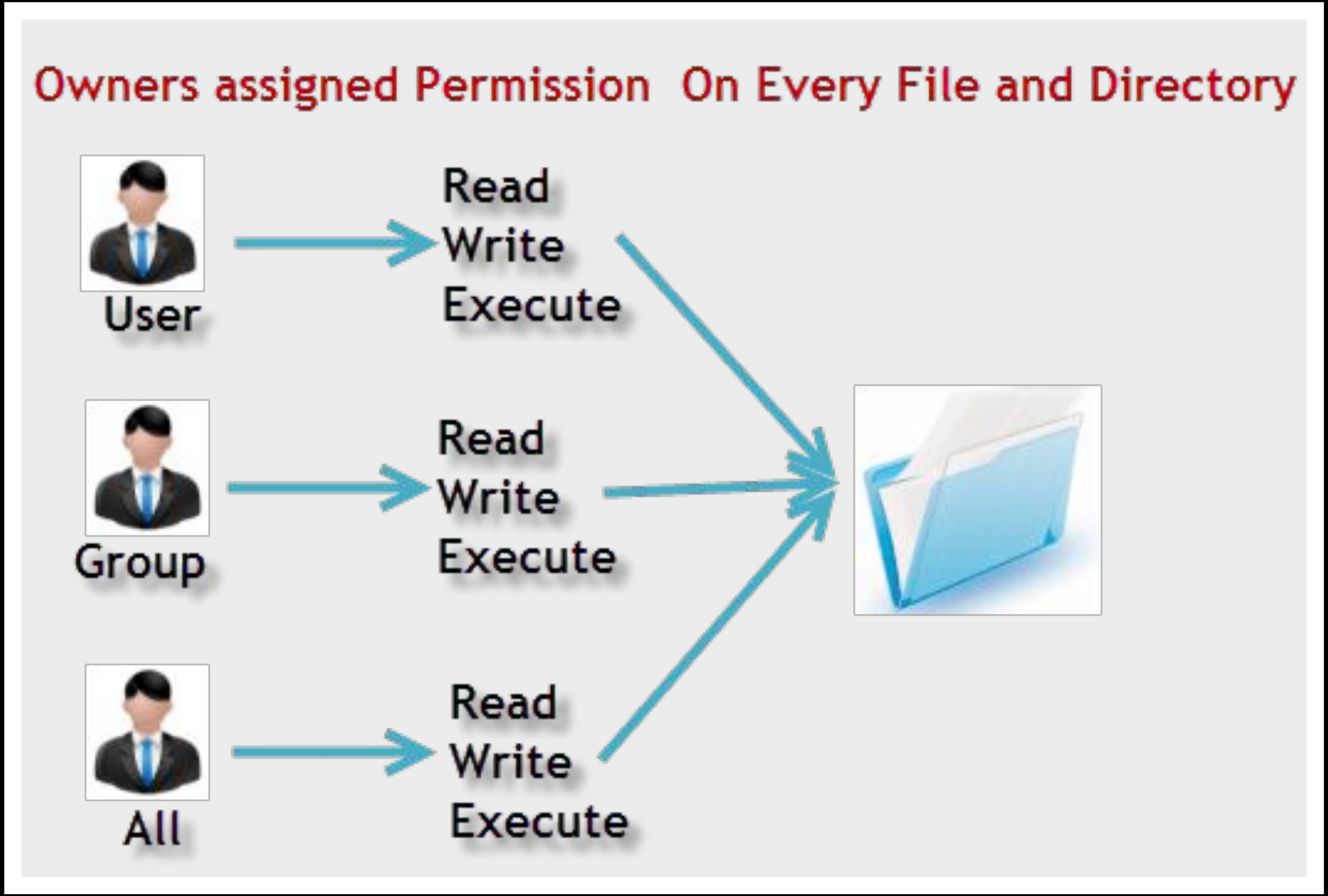
- The Unix files access is controlled. There are three types of access (permissions):
  - read
  - write
  - execute
- Each file belongs to a specific user and group (ownership). Access to the files is controlled by user, group, and what is called other/everyone permission bits and is usually set using a numerical value.
- For example, 644 as permission bit will result in:
  - Owner/User Group Other/Everyone 644

Managing File Ownership…cont

- Read: This permission give you the authority to open and read a file. Read permission on a directory gives you the ability to lists its content.
- Write: The write permission gives you the authority to modify the contents of a file. The write permission on a directory gives you the authority to add, remove and rename files stored in the directory. Consider a scenario where you have to write permission on file but do not have write permission on the directory where the file is stored. You will be able to modify the file contents. But you will not be able to rename, move or remove the file from the directory.
- Execute: In Windows, an executable program usually has an extension ".exe" and which you can easily run. In Unix/Linux, you cannot run a program unless the execute permission is set. If the execute permission is not set, you might still be able to see/modify the program code(provided read & write permissions are set), but not run it.

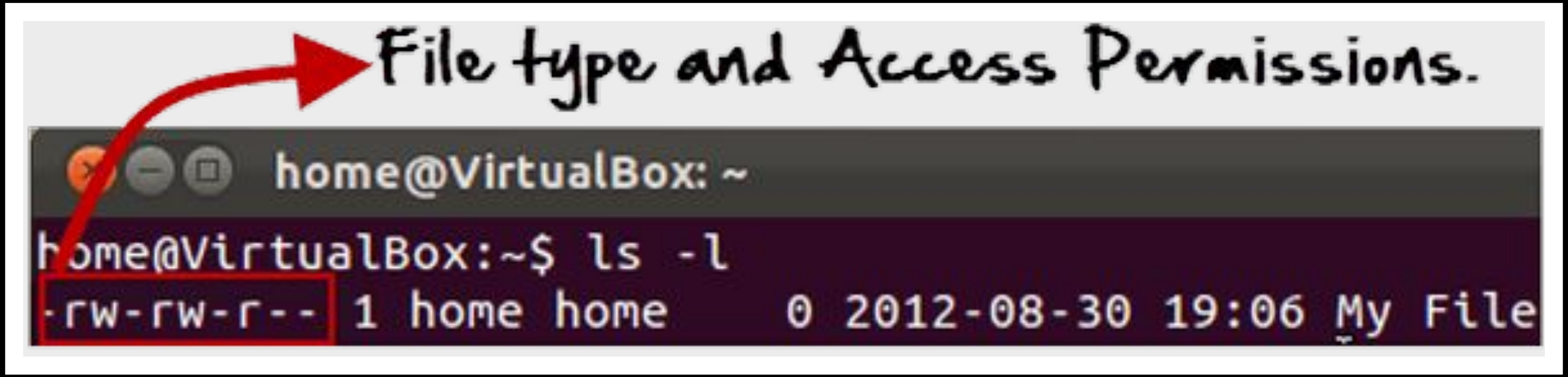
LIMKOKWING UNIVERSITY OF CREATIVE TECHNOLOGY ESWATINI

Managing File Ownership…cont



Managing File Ownership…cont

- Let’s see file permissions in Linux with examples:
  - ls – l on terminal gives
- ls – l



```
home@VirtualBox:~$ ls -l
-rw-rw-r-- 1 home home    0 2012-08-30 19:06 My File
```

- Here, we have highlighted ‘-rw-rw-r–‘and this weird looking code is the one that tells us about the Unix permissions given to the owner, user group and the world.

Different access levels depending on the numbers:

- 0 – no access to the file whatsoever
- 1 – execute permissions only
- 2 – write permissions only
- 3 – write and execute permissions
- 4 – read permissions only
- 5 – read and execute permissions
- 6 – read and write permissions
- 7 – read, write and execute permissions (full permissions)
- Thus the above 644 permissions example will look like this:
    - Owner/User - Read and Write
    - Group - Read only
    - Other/Everyone - Read only

LIMKOKWING UNIVERSITY OF CREATIVE TECHNOLOGY
ESWATINI

Different access levels depending on the numbers:

- To allow a script to be executed and read by everyone but the only one who can write in it is your user, you would need to set 755 as permissions:
  - Owner/User - 7 - Full permissions
  - Group - 5 - read and execute
  - Other/Everyone - 5 - read and execute
- Changing the permissions to 700 will make the file visible only for your username and no one else and setting it to 444 will allow only the file creator to modify it.

LIMKOKWING UNIVERSITY OF CREATIVE TECHNOLOGY
ESWATINI

Controlling Access to files

- To allow a script to be executed and read by everyone but the only one who can write in it is your user, you would need to set 755 as permissions:
  - Owner/User - 7 - Full permissions
  - Group - 5 - read and execute
  - Other/Everyone - 5 - read and execute
- Changing the permissions to 700 will make the file visible only for your username and no one else and setting it to 444 will allow only the file creator to modify it.

LIMKOKWING UNIVERSITY OF CREATIVE TECHNOLOGY
ESWATINI

Managing Disk Quotas

- A disk quota is the amount of space allocated to each user for file storage on a given computer.
- On shared systems such as Unix, every user has a maximum disk quota. This prevents any individual from using more than his or her fair share of disk space. In order to keep from going over your quota, you must be sure to periodically clean out old, unused, and unneeded files.
- Two commands are very helpful in bringing your disk space back under control:
  - The ls -al command shows you the contents of your directory.
  - The rm command removes any unnecessary files.

Managing Disk Quotas

- To use the rm command (which stands for "remove"), enter:
  - rm filename
- Replace filename with the name of the file you want to remove.
- You can also enter:
  - rm -i filename
- The -i flag tells Unix to inquire for confirmation before removing.
- Always be careful when you remove files, because there is no command to retrieve the file. You may create an alias that will move files to a trash can rather than removing them from the system completely, but this is generally not an accepted practice.
- If you are unsure of the content of a file, enter:
  - cat filename