# Understanding Root and Sudo

By: Michael Ilodigwe

M2i
TECH

# Root User

**The root user, often referred to as the "superuser," is the most privileged account on a Linux system. It has the username “root”.**

## Key Characteristics

**Full System Access:**

The root user has unrestricted access to all commands and files on the system.

**Administrative Privileges:**

Can perform administrative tasks such as installing software, modifying system configurations, and managing users.

**Single User:**

There is only one root user account, though users can temporarily gain root privileges via sudo.

# Common Practices and Risk as User root

## Common Tasks for the Root User

- **System Configuration:** Editing system configuration files in directories like /etc.
- **User Management:** Adding, modifying, or deleting user accounts.
- **File System Management:** Creating, deleting, and modifying any files or directories.
- **Software Installation:** Installing and updating software packages.

## Risks and Best Practices

- **Risk of Misuse:** Unrestricted access means that misuse or errors can lead to system-wide issues or security vulnerabilities.
- **Minimal Use:** Limit the use of the root account; prefer using sudo to execute commands with root privileges.
- **Secure Access:** Ensure strong passwords and consider additional security measures such as two-factor authentication.

# Introduction to Sudo

## Sudo stands for "Superuser Do”

- Allows users to execute commands with the security privileges of another user, typically the root user

## The Sudo User

- A regular user granted permission to execute specific commands as the root user
- Configuration in the sudoers file determines which commands the sudo user can run

# Sudo Su – Root user

Sudo su

allows a user to switch to the root user with elevated privileges

Should be used cautiously due to the extensive access it grants

# How to Sudo to Root

**To sudo to root type**

sudo su -  or sudo –i

These two commands are the same.

**If you have root privledges and logged in as another account you can sudo to the account.**

sudo su - <user_account>

To verify if you have been granted sudo prvileges type: sudo –l

# Verify Sudo Prvileges

- If you have root prvileges and logged in as another account you can sudo to the account.
  - sudo su - <user_account>
  - To verify if you have been granted sudo prvileges type: sudo –l

  Prvileges are granted by creating a file inside the /etc/sudoers.d/ directory and providing the commands for the particular user to execute