

**NATIONAL OPEN UNIVERSITY OF NIGERIA**

**FACULTY OF COMPUTING**

**DEPARTMENT OF CYBERSECURITY**

**COURSE CODE: CYB 191**

**COURSE TITLE: CYBERSECURITY PRACTICAL 1**

**Module 1: Practical on System Access Control**

Unit 1: Creation of user Accounts and Password on Operating System

Unit 2: Creation of Password for Microsoft office Document Protection

Unit 3: Configuration of Password Policies in Windows and Unix Based computer

**Module 2: Practical on Network Security**

Unit 1: Configuration of Firewall on Windows

Unit 2: Real-time operating system

Unit 3: Time-Sharing and Object-oriented operating system

**Module 3: Process Management**

Unit 1: Processes

Unit 2: Co-operating Processes

Unit 3: Threads

---

## Module 1: Practical on System Access Control

---

### Module Introduction

This module is about Access Control Practical. The module covers discussion on different types of user accounts. It covers how to create User Accounts and password, Password Creation for Microsoft office Document Protection. The module covers practical on how on how to removal password from Microsoft Office Document. It contains four units as follows:

- Unit 1: Creation of user Accounts on windows Based Computer
- Unit 2: Creation of user Accounts on Unix Based Computer
- Unit 3: Configuration of Password Policies in Windows and Unix Based computer

### Unit 1: Creation of user Accounts on Windows Based Computer

#### Contents

- 1.0 Introduction
- 2.0 Intended Learning Outcomes (ILOs)
- 3.0 Main Content
  - 3.1 Understanding User Accounts in Windows
  - 3.2 Types of User Accounts on Windows Based Personal Computer
  - 3.3 Types of Users Accounts on Unix Based Personal Computer
  - 3.4 Creation of User Account on Windows
  - 3.5 Lab1: Creating user Accounts using “the Settings App” (Win 10 and Win 11)
  - 3.6 Lab2: Creating User Accounts Using “Control Panel”
  - 3.7 Lab3: Creating User accounts Using “Command Prompt”
- 4.0 Self-Assessment Laboratory activity
- 5.0 Conclusion
- 6.0 Summary

#### 1.0 Introduction

In this unit, you will learn about different types of user accounts that can be created on a Microsoft Operating system computer. You will also learn how to create these user accounts and password.



## **2.0 Intended Learning Outcomes (ILOs)**

By the end of this unit, you will be able to:

- Describe how to operate different user account Windows Based Personal Computer.
- Analysis different types of user accounts and their options Windows Based Personal Computer.
- Explain how to protect personal computer with password.



## **3.0 Main Content**

### **3.1 Understanding User Accounts in Windows Based Personal Computer**

To comprehend how different user accounts work in personal computer running Windows Operating System, let discuss general role of user account in personal computer. A user account is a collection of settings and permissions, specific to each user, that determine what the user can and cannot do on the computer User account in Personal Computer is important for managing access and personalizing user experiences on a computer. Each account allows users to have their own settings, files, and applications, ensuring confidentiality and integrity.

### **3.2 Types of User Accounts on Windows Based Personal Computer**

There are Three (3) types of user accounts on Window Based Personal Computer.

#### **3.2.1 Administrator Accounts**

Administrator accounts allow users to have full control over the computer, permit users to install software, change computer settings, and manage other user accounts.

Administrators have access to everything on the computer, and can make changes to anything, such as installing software and changing security settings

#### **3.2.2 Standard User Accounts**

Standard accounts enable users to have limited permissions. Users with standard account will have limited privilege to make changes to the computer, except for personalizing the computer, such as applying a screen saver or changing a theme.

Standard users can run applications and change their settings but require administrator approval for system-wide changes.

### 3.2.2 Guest User Accounts

Guest user accounts are temporary accounts with minimal permissions, typically used for short-term access. Guest accounts exist for temporary users of a computer and only one guest account can exist on a computer. Guest accounts are similar to standard accounts, except there is no privacy, as anybody can log onto a guest account

### 3.3 Creation of User Accounts on Windows Based Computer

Creation of user accounts on a Windows Computer is an easy process that can be done using the Settings app, Control Panel, or the Command Prompt. The laboratory works in the following section give step by step by which user account can be created using the setting app, Control Panel and the command prompt.

#### 3.4 Lab1: Creating user Accounts using “the Settings App” (Win 10 and Win 11)

The aim of this laboratory activity is to create user accounts using the setting App on Windows 10 and Windows 11. Students are to follow the following steps to carry out the activity.

**Step1:** Press “**Win + I**” to open the Settings app

**Step2:** Click on “**Accounts.**”

**Step3:** Click on “**Family & other users**” in the left-hand menu.

**Step4:** Under “Other users,” click “**Add someone else to this PC.**”

**Step5:** Create Account of your choice as follows:

- To create a Microsoft account, enter the email address or phone number.
- To create a local account, click on “**I don’t have this person’s sign-in information,**” then select “**Add a user without a Microsoft account.**”
- Enter the username, password, and security questions.
- then click “**Next.**”

#### 3.5 Lab2: Creating User Accounts Using “Control Panel”

The aim of this laboratory activity is to create user accounts using Control Panel on Windows 10 and Windows 11. Students are to follow the following steps to carry out the laboratory activity.

**Step1:** Press “**Win + R**”, type control, and press Enter.

**Step2:** Click on " **User Accounts.**"

**Step3:** Click on "**Manage another account.**"

**Step4:** Click on "**Add a new user in PC settings**" to be redirected to the Settings app, or

**Step5:** In older versions of Windows, you can directly create a new account here by clicking "**Create a new account,**" then following the prompts to set up the account.

### **3.6 Lab3: Creating User accounts Using “Command Prompt”**

The aim of this laboratory activity is to create user accounts using Control Panel on Windows 10 and Windows 11. Students are to follow the following steps to carry out the laboratory activity.

**Step1:** Press Win + X and select "Command Prompt (Admin)" or "Windows PowerShell (Admin)."

**Step2:** Type the following command and press Enter

```
net user [username] [password] /add
```

**Step3:** Replace [username] with the desired username and [password] with the desired password.

**Step4:** To create new user with administrative privileges, type the following command and press Enter:

```
net localgroup administrators [username] /add
```

### **4.0 Self-Assessment Laboratory activity**

**Activity:** Students are to create user accounts on Windows 10 and Windows 11 using PowerShell.

### **5.0 Conclusion**

You have learnt from this unit about different types of user accounts on both the windows-based computer and Unix based computer. You have also learnt how to create user accounts in windows-based computer. Four (4) methods of creating user accounts have been discussed in this unit.

## 6.0 Summary

This unit covered different types of user account in both windows based computer and unix based computer. The unit also gave step by step by which user accounts can be created in windows based computer.

## 7.0 Further Readings

Krebs, B. (2012). *The Scrap Value of a Hacked PC, Revisited* Retrieved from <http://www.krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/>

Glanz, J. & Markoff, J. (2011). Egypt Leaders Found 'Off' Switch for the Internet', *The New York Times*, 15 February 2011. Retrieved from <http://www.nytimes.com/2011/02/16/technology/16internet.html?>

Matlack, C. (2014). 'Swift Justice: One Way to Make Putin Howl'. *Bloomberg Business*, 4 September 2014, Retrieved from <http://www.bloomberg.com/bw/articles/2014-09-04/ultimate-sanction-barring-russian-banks-from-swiftmoney-system>

## Unit 2: Creation of user Accounts on Unix Based Computer

### Contents

- 1.0 Introduction
- 2.0 Intended Learning Outcomes (ILOs)
- 3.0 Main Content
  - 3.1 Understanding User Accounts in Unix Based Computer
  - 3.2 Types of User Accounts on Unix Based Computer
  - 3.3 Creation of User Account on Unix Based Computer
  - 3.4 Lab1: Creating a user Account **on Unix** Based Computer
  - 3.5 Lab2: Creating password for User Account on Unix Based Computer
  - 3.6 Lab3: Creating User's Home Directory on Unix Based Computer
  - 3.7 Lab4: Setting Default Shell for User on Unix Based Computer
- 4.0 Self-Assessment Laboratory activity
- 5.0 Conclusion
- 6.0 Summary

### 1.0 Introduction

In this unit, you will learn about different types of user accounts that can be created on a Unix Based Computer. You will also learn how to create these user accounts and password.



### 2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- Describe how to operate different user account Unix Based Computer.
- Analysis different types of user accounts and their options Unix Based Computer.
- Explain how to protect personal computer with password.



### 3.0 Main Content

#### 3.1 Understanding User Accounts in Unix Based Computer

To comprehend how different user accounts work in personal computer running Windows Operating System, let discuss general role of user account in personal computer. A user account is a collection of settings and permissions, specific to each user, that determine



what the user can and cannot do on the computer User account in Personal Computer is important for managing access and personalizing user experiences on a computer. Each account allows users to have their own settings, files, and applications, ensuring confidentiality and integrity.

## **3.2 Types of Users Accounts on Unix Based Personal Computer**

In Unix operating systems, user accounts are important for managing access and operations on the computer. Unix operating system has several types of user accounts, each with different levels of access and roles.

### **3.2.1 Root Accounts**

The root account often referred to as the "superuser," is the most powerful user account in Unix and Unix-like systems, including Linux. The user of this account has unrestricted access to all commands and files on the computer.

### **3.2.2 System accounts**

System accounts in Unix and Unix-like systems are special user accounts used to run system services and perform administrative tasks. Unlike regular user accounts, they are not intended for interactive login and are essential for the operation of various system components

### **3.2.3 User Accounts**

User accounts in Unix and Unix-like systems are essential for providing individualized access and control over the system. Each user account represents a single user and has a unique set of permissions, files, and settings

### **3.2.4 Group Accounts**

Group accounts in Unix and Unix-like systems are a fundamental mechanism for managing user permissions and access control. A group is a collection of user accounts that can be assigned specific permissions collectively.

## **3.3 Creation of User Accounts on Unix Based Computer**

Creation of user accounts on a **Unix Based Computer** involves several steps. The steps can vary slightly depending on the specific Unix or Linux distribution one is using. The laboratory activity in the following section gives general step-by-step guide on how user account and password can be created in Unix based Operating System.

## **3.4 Lab1: Creating user Accounts on Unix Based Computer**

**Aim:** The aim of this laboratory activity is to create user account Unix Based Computer using. Students are to follow the following steps to carry out the activity.

**Step1:** Log in to the system as the root user or use “sudo” to gain administrative privileges.

**Step2:** Open the terminal through application menu for graphical user interface.

**Step3:** type the useradd command to create a new user account. The syntax is

```
bash Copy code  
  
sudo useradd [options] username
```

**Step4:** Replace username with the desired username. For example, to create a user named for ‘olalere’

```
bash Copy code  
  
sudo useradd olalere
```

**Step5:** Press Enter to finish creation of user “olalere”

### 3.5 Lab2: Creating password for User Account on Unix Based Computer

**Aim:** The aim of this laboratory activity is to create password for user account on Unix based computer.

To set or create password for user account on Unix based computer, let consider the user account ‘olalere’ created in lab1. The following steps are to be followed.

**Step1:** create a password for ‘olalere’ by typing the ‘passwd’ command

```
bash Copy code  
  
sudo passwd olalere
```

**Step2:** Press ‘Enter’.

**Step3:** Type and confirm the new password.

```
arduino Copy code  
  
Enter new UNIX password:  
Retype new UNIX password:
```

**Step4:** Press 'Enter' to finish password creation.

### 3.6 Lab3: Creating User's Home Directory on Unix Based Computer

A home directory provides privacy and security for user's data. In other words, Other users won't be able to view or modify files unless given explicit permission. When a home directory is created for user, breach of confidentiality and integrity become impossible. In this laboratory activity, steps to create user's home directory will be provided.

**Aim:** The aim of this laboratory activity is to create user home directory on Unix based computer. Students are to follow the following steps to carry out the laboratory activity.

**Step1:** Type '-m' option with useradd.

**Step2:** Press 'Enter' to finish creation of user home directory.

```
bash Copy code  
  
sudo useradd -m olalere
```

### 3.7 Lab4: Setting Default Shell for User on Unix Based Computer

Though it is optional, one can specify the default shell for the user created. Each user on a Unix based computer is associated with a default shell. This default shell determines the command interpreter users use when interacting with the system. The steps to set default shell for user on Unix based computer are presented in this laboratory activity.

**Aim:** The aim of this laboratory activity is to set default shell for user on Unix based computer are presented in this laboratory activity. Students are to follow the following steps to carry out the laboratory activity.

**Step1:** To specify the default shell for the user type '-s' option

```
bash
```

```
Copy code
```

```
sudo useradd -s /bin/bash olalere
```

**Step2:** Press 'Enter' to finish setting default shell.

#### 4.0 Self-Assessment Laboratory activity

**Laboratory Activity:** Students are to create a user named 'olalere', set a password, create a home directory, set the default shell to /bin/bash, in a single line of command

#### 5.0 Conclusion

You have learnt from this unit about different types of user accounts on Unix based computer. You have also learnt how to create user account on Unix based computer. You have also learnt how to **set a password, create a home directory, set the default shell to /bin/bash** on Unix based computer.

#### 6.0 Summary

This unit covered different types of user account on Unix based computer. The unit also gave step by step by which user account can be created on Unix based computer. Also, step by step to **create a home directory, set the default shell to /bin/bash** on Unix based computer.

#### 7.0 Further Readings

Krebs, B. (2012). *The Scrap Value of a Hacked PC, Revisited* Retrieved from <http://www.krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/>

Glanz, J. & Markoff, J. (2011). Egypt Leaders Found 'Off' Switch for the Internet', *The New York Times*, 15 February 2011. Retrieved from <http://www.nytimes.com/2011/02/16/technology/16internet.html?>

Matlack, C. (2014). 'Swift Justice: One Way to Make Putin Howl'. *Bloomberg Business*, 4 September 2014, Retrieved from <http://www.bloomberg.com/bw/articles/2014-09-04/ultimate-sanction-barring-russian-banks-from-swiftmoney-system>

## Unit 3: Configuration of Password Policies in Windows and Unix Based computer

### Contents

- 1.0 Introduction
- 2.0 Intended Learning Outcomes (ILOs)
- 3.0 Main Content
  - 3.1 Understanding Active Directory
  - 3.2 Active Directory Password Policy
  - 3.3 Components of Active Directory Password Policy
  - 3.4 General Security Benefits of Active Directory Password Policy
  - 3.4 Lab1: Creating a user Account **on Unix** Based Computer
  - 3.5 Lab2: Creating password for User Account on Unix Based Computer
  - 3.6 Lab3: Creating User's Home Directory on Unix Based Computer
  - 3.7 Lab4: Setting Default Shell for User on Unix Based Computer
- 4.0 Self-Assessment Laboratory activity
- 5.0 Conclusion
- 6.0 Summary

### 1.0 Introduction

In this unit, you will learn about Active Directory and Active Directory Password Policy. You will have understanding of components of Active Directory Password Policy and Security Benefits of Active Directory Password Policy. You will also learn how to configure Active directory Password policy.



### 2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- Describe how Active Directory and Active Directory Password Policy work.
- Describe key components of Active Directory Password Policy
- Explain benefits of Active Directory Password Policy
- Describe how to configure Active Directory Password Policy.



### 3.0 Main Content

#### 3.1 Understanding Active Directory

**What is Active Directory?** Before we discuss Active Directory Password policy, its component, security benefits and configuration, let's explain what Active Directory is. Active Directory (AD) is a directory service developed by Microsoft for networked Windows environment. Microsoft Active Directory (AD) can be seen as a core component of the Server operating system. Active Directory is a database and set of services that enable secure access to resources in Windows domain networks. Active Directory is a fundamental component of many IT infrastructures for managing user identities and securing access to resources within an enterprise. **Active Directory Password Policy** is One of the key security features of Active Directory.

### **3.2 Active Directory Password Policy**

**Active Directory Password Policy** is One of the key security features of Active Directory. Active Directory Password Policy is an essential aspect of an organization's security posture. If stringent password requirements is enforced, Active Directory Password Policy helps to protect against unauthorized access, mitigates password-based attacks, ensures compliance with security standards, and reduces the risk of compromised passwords. Active Directory Password Policy establishes guidelines for creating passwords, including minimum length, complexity (such as the inclusion of capital letter, alphanumeric and special characters), and life span before the password must be changed. The key components of Active Directory password policy are presented in the following subsection.

### **3.2 Components of Active Directory Password Policy**

In this section, there are Six (6) key component of Active Directory Password Policy to be discussed with their security benefits. The components are what administrator can reconfigure or edit to suit the need of an organization. It is important to note that these components came with their default values.

### **3.3 Security Benefits of Active Directory Password Policy**

In Unix operating systems, user accounts are important for managing access and operations on the computer. Unix operating system has several types of user accounts, each with different levels of access and roles.

### **3.2 Components of Active Directory Password Policy**

In Unix operating systems, user accounts are important for managing access and operations on the computer. Unix operating system has several types of user accounts, each with different levels of access and roles.

### 3.3 Active Directory Password Policy

In Unix operating systems, user accounts are important for managing access and operations on the computer. Unix operating system has several types of user accounts, each with different levels of access and roles.

#### 3.3.1 Enforce Password History

The **Enforce Password History** setting determines the number of unique new passwords that user must have used before an old password can be reused. This setting does not give room for old password recycling by users. The security benefit of this component is that it reduces the risk of compromise from previously exposed passwords.

#### 3.3.2 Maximum Password Age

The **Maximum Password Age** setting determines the life span (in days) that a password can be used before the system requires the user to change it. Changing of password regularly can limit the damage from compromised passwords. The main security benefit of this setting is that periodical change of password reduces the risk of long-term password exposure.

#### 3.3.3 Minimum Password Age

The **Minimum Password Age** setting dictates the minimum period of time (in days) that a password must be used before it can be changed the user. This setting prevents users from changing their password quickly to a previously used password. The security benefit of this component is that users are discouraged from bypassing the password history requirement by enforcing a minimum usage period for each password.

#### 3.3.4 Minimum Password Length

The **Minimum Password Length** setting determines the minimum number of characters a password must contain. The longer the password the harder it becomes to guess or crack. This setting security benefit is that the complexity and strength of passwords are increased and this make the password to be more resistant to brute-force attacks.

#### 3.3.5 Password Complexity Requirements

The **Password Complexity Requirements** setting ensures that passwords contain characters from at least three of the following four categories: uppercase letters, lowercase letters, digits, and special characters. The security benefit of this setting is that it makes passwords to be less susceptible to dictionary and guessing attacks.

#### 3.3.6 Account Lockout Policy

The **Account Lockout Policy** setting is not a direct component of the Password Policy. This policy defines the numbers of failed login attempts (due to the wrong password input) are allowed before the account is locked and for how long.

=

### **3.4 General Security Benefits of Active Directory Password Policy**

In general, Active Directory Password Policy provides significant security benefits by enforcing stringent password requirements that enhance the overall protection of user accounts. Some of the security benefits are discussed in the following subsections.

#### **3.4.1 Enhanced Protection Against Unauthorized Access**

With the enforcement of strong password policies, organizations can significantly reduce the likelihood of unauthorized access to user accounts. Also, enforcing complex and regularly updated passwords make it more difficult for attackers to gain access to user accounts.

#### **3.4.2 Mitigation of Password-Based Attacks**

Security policies that require complex passwords and prevent reuse of old passwords help protect against various password-based attacks, such as brute-force, dictionary attacks, and credential stuffing.

#### **3.4.3 Compliance with Security Standards**

Implementation of strong password and policies is a must for organizations is a must for many regulatory and industry standards. Active Directory Password Policy helps organizations comply with these standards, thereby avoiding potential legal and financial penalties.

#### **3.4.4 Reduced Risk from Compromised Passwords**

By enforcing regular password changes and complexity requirements, Active Directory Password policy reduces attackers' chance of compromised passwords exploitation. Even if a password is compromised, it will soon be rendered useless

#### **3.4.5 Improved User Security Awareness**

Implementing and communicating password policies raises awareness among users about the importance of strong passwords and security practices. This can lead to better overall security behavior within the organization.

#### **3.4.6 Centralized Management and Enforcement**



Active Directory allows for centralized management of password policies, ensuring consistent enforcement across the organization. This centralization simplifies administration and ensures all users adhere to the same security standards.

### 3.5 Lab1: Viewing Default/Current Domain Password Policy

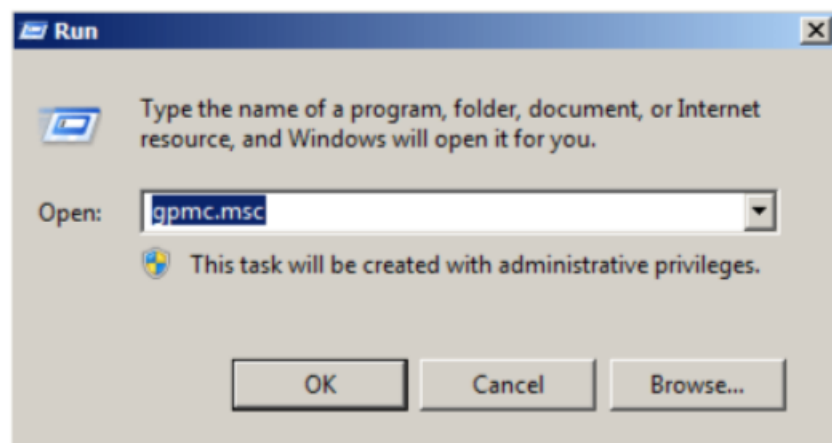
Before carrying out laboratory activity on configuration of Active Directory Domain Password Policy, let carry out laboratory activity on viewing the default/current Active directory password policy.

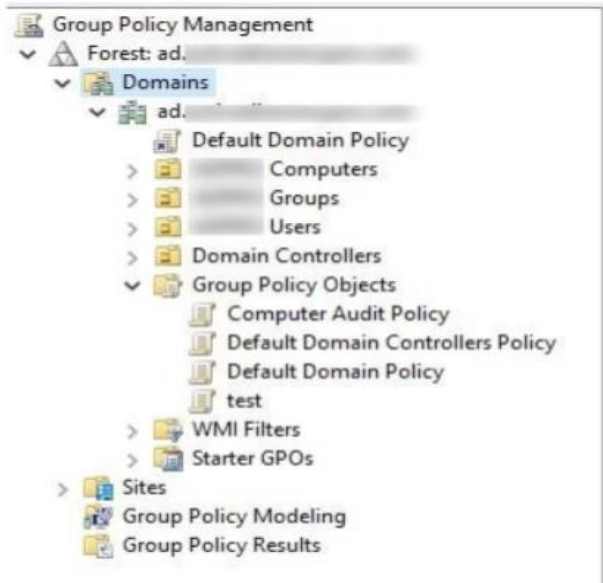
**Aim:** The aim of this laboratory activity is to viewing Default/Current Domain Password Policy.

It is important to note that password policies come under the group policy, which relates to the root domain. To view the current Active Directory Domain Password Policy, follow the following steps:

#### Step1: Open Group Policy Management

- Press Windows + R to open the Run dialog box.
- Type “gpmmc.msc” and press Enter. This will open the Group Policy Management Console.





### Step2: Navigate to the Default Domain Policy

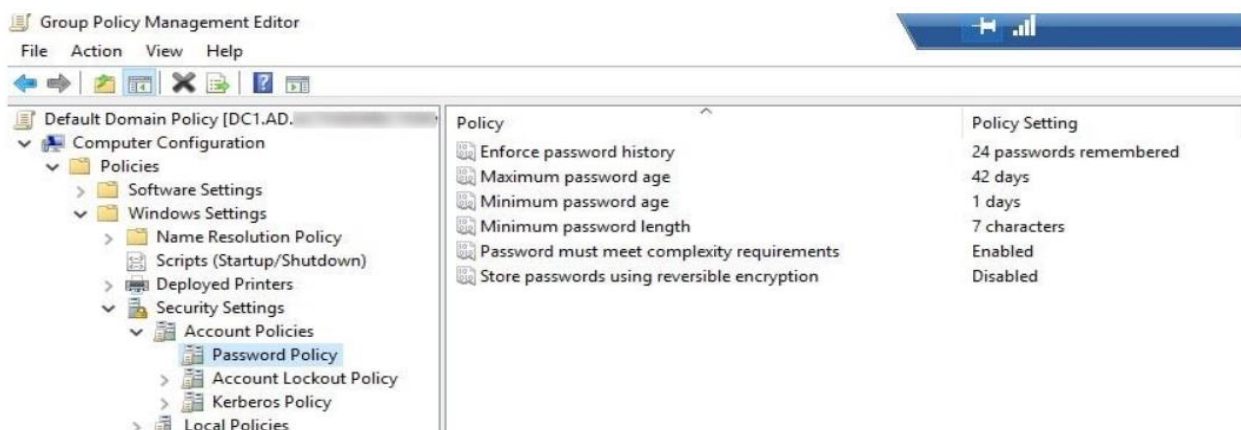
- In the Group Policy Management Console, expand the forest and domain node.
- Expand your domain (e.g., example.com).
- Click on the "Default Domain Policy" under the "Group Policy Objects" node.

### Step3: Edit the Default Domain Policy

- Right-click on "Default Domain Policy" and
- select "Edit."

### Step4: Navigate to the Password Policy Settings

- In the Group Policy Management Editor, navigate to: Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy.



### Step5: Review the Password Policy Settings

- Click on each policy to review the current settings, such as "Minimum password length," "Password must meet complexity requirements," and so on.

### 3.6 Lab2: Creating password for User Account on Unix Based Computer

**Aim:** The aim of this laboratory activity is to create password for user account on Unix based computer.

To set or create password for user account on Unix based computer, let consider the user account 'olalere' created in lab1. The following steps are to be followed.

**Step1:** create a password for 'olalere' by typing the 'passwd' command

```
bash Copy code  
sudo passwd olalere
```

**Step2:** Press 'Enter'.

**Step3:** Type and confirm the new password.

```
arduino Copy code  
Enter new UNIX password:  
Retype new UNIX password:
```

**Step4:** Press 'Enter' to finish password creation.

### 3.6 Lab3: Creating User's Home Directory on Unix Based Computer

A home directory provides privacy and security for user's data. In other words, Other users won't be able to view or modify files unless given explicit permission. When a home directory is created for user, breach of confidentiality and integrity become impossible. In this laboratory activity, steps to create user's home directory will be provided.

**Aim:** The aim of this laboratory activity is to create user home directory on Unix based computer. Students are to follow the following steps to carry out the laboratory activity.

**Step1:** Type '-m' option with useradd.

**Step2:** Press 'Enter' to finish creation of user home directory.

```
bash Copy code  
  
sudo useradd -m olalere
```

### 3.7 Lab4: Setting Default Shell for User on Unix Based Computer

Though it is optional, one can specify the default shell for the user created. Each user on a Unix based computer is associated with a default shell. This default shell determines the command interpreter users use when interacting with the system. The steps to set default shell for user on Unix based computer are presented in this laboratory activity.

**Aim:** The aim of this laboratory activity is to set default shell for user on Unix based computer are presented in this laboratory activity. Students are to follow the following steps to carry out the laboratory activity.

**Step1:** To specify the default shell for the user type '-s' option

```
bash Copy code  
  
sudo useradd -s /bin/bash olalere
```

**Step2:** Press 'Enter' to finish setting default shell.

### 4.0 Self-Assessment Laboratory activity

**Laboratory Activity:** Students are to creates a user named 'olalere', sets a password, creates a home directory, sets the default shell to /bin/bash, in a single line of command

### 5.0 Conclusion

You have learnt from this unit about different types of user accounts on Unix based computer. You have also leant how to create user account Unix based computer. You have also leant how to **set a password, creates a home directory, sets the default shell to /bin/bash** on Unix based computer.

## 6.0 Summary

This unit covered different types of user account on Unix based computer. The unit also gave step by step by which user account can be created on Unix based computer. Also, step by step to **create a home directory, set the default shell to /bin/bash** on Unix based computer.

## 7.0 Further Readings

Krebs, B. (2012). *The Scrap Value of a Hacked PC, Revisited* Retrieved from <http://www.krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/>

Glanz, J. & Markoff, J. (2011). Egypt Leaders Found 'Off' Switch for the Internet', *The New York Times*, 15 February 2011. Retrieved from <http://www.nytimes.com/2011/02/16/technology/16internet.html?>

Matlack, C. (2014). 'Swift Justice: One Way to Make Putin Howl'. *Bloomberg Business*, 4 September 2014, Retrieved from <http://www.bloomberg.com/bw/articles/2014-09-04/ultimate-sanction-barring-russian-banks-from-swiftmoney-system>

---

## Module 2: Practical on Network Security

---

### Module Introduction

This module is about Access Control Practical. The module covers discussion on different types of user accounts. It covers how to create User Accounts and password, Password Creation for Microsoft office Document Protection. The module covers practical on how on how to removal password from Microsoft Office Document. It contains four units as follows:

- Unit 1: Creation of user Accounts on windows Based Computer
- Unit 2: Creation of user Accounts on Unix Based Computer
- Unit 3: Configuration of Password Policies in Windows and Unix Based computer

### Unit 1: Creation of user Accounts on Windows Based Computer

#### Contents

- 1.0 Introduction
- 2.0 Intended Learning Outcomes (ILOs)
- 3.0 Main Content
  - 3.1 Understanding User Accounts in Windows
  - 3.2 Types of User Accounts on Windows Based Personal Computer
  - 3.3 Types of Users Accounts on Unix Based Personal Computer
  - 3.4 Creation of User Account on Windows
  - 3.5 Lab1: Creating user Accounts using “the Settings App” (Win 10 and Win 11)
  - 3.6 Lab2: Creating User Accounts Using “Control Panel”
  - 3.7 Lab3: Creating User accounts Using “Command Prompt”
- 4.0 Self-Assessment Laboratory activity
- 5.0 Conclusion
- 6.0 Summary

#### 1.0 Introduction

In this unit, you will learn about different types of user accounts that can be created on a Microsoft Operating system computer. You will also learn how to create these user accounts and password.



## **2.0 Intended Learning Outcomes (ILOs)**

By the end of this unit, you will be able to:

- Describe how to operate different user account Windows Based Personal Computer.
- Analysis different types of user accounts and their options Windows Based Personal Computer.
- Explain how to protect personal computer with password.



## **3.0 Main Content**

### **3.1 Understanding User Accounts in Windows Based Personal Computer**

To comprehend how different user accounts work in personal computer running Windows Operating System, let discuss general role of user account in personal computer. A user account is a collection of settings and permissions, specific to each user, that determine what the user can and cannot do on the computer User account in Personal Computer is important for managing access and personalizing user experiences on a computer. Each account allows users to have their own settings, files, and applications, ensuring confidentiality and integrity.

### **3.2 Types of User Accounts on Windows Based Personal Computer**

There are Three (3) types of user accounts on Window Based Personal Computer.

#### **3.2.1 Administrator Accounts**

Administrator accounts allow users to have full control over the computer, permit users to install software, change computer settings, and manage other user accounts.

Administrators have access to everything on the computer, and can make changes to anything, such as installing software and changing security settings

#### **3.2.2 Standard User Accounts**

Standard accounts enable users to have limited permissions. Users with standard account will have limited privilege to make changes to the computer, except for personalizing the computer, such as applying a screen saver or changing a theme.

Standard users can run applications and change their settings but require administrator approval for system-wide changes.

### 3.2.2 Guest User Accounts

Guest user accounts are temporary accounts with minimal permissions, typically used for short-term access. Guest accounts exist for temporary users of a computer and only one guest account can exist on a computer. Guest accounts are similar to standard accounts, except there is no privacy, as anybody can log onto a guest account

### 3.3 Creation of User Accounts on Windows Based Computer

Creation of user accounts on a Windows Computer is an easy process that can be done using the Settings app, Control Panel, or the Command Prompt. The laboratory works in the following section give step by step by which user account can be created using the setting app, Control Panel and the command prompt.

#### 3.4 Lab1: Creating user Accounts using “the Settings App” (Win 10 and Win 11)

The aim of this laboratory activity is to create user accounts using the setting App on Windows 10 and Windows 11. Students are to follow the following steps to carry out the activity.

**Step1:** Press “**Win + I**” to open the Settings app

**Step2:** Click on “**Accounts.**”

**Step3:** Click on “**Family & other users**” in the left-hand menu.

**Step4:** Under “Other users,” click “**Add someone else to this PC.**”

**Step5:** Create Account of your choice as follows:

- To create a Microsoft account, enter the email address or phone number.
- To create a local account, click on “**I don’t have this person’s sign-in information,**” then select “**Add a user without a Microsoft account.**”
- Enter the username, password, and security questions.
- then click “**Next.**”

#### 3.5 Lab2: Creating User Accounts Using “Control Panel”

The aim of this laboratory activity is to create user accounts using Control Panel on Windows 10 and Windows 11. Students are to follow the following steps to carry out the laboratory activity.

**Step1:** Press “**Win + R**”, type control, and press Enter.



**Step2:** Click on " **User Accounts.**"

**Step3:** Click on "**Manage another account.**"

**Step4:** Click on "**Add a new user in PC settings**" to be redirected to the Settings app, or

**Step5:** In older versions of Windows, you can directly create a new account here by clicking "**Create a new account,**" then following the prompts to set up the account.

### **3.6 Lab3: Creating User accounts Using “Command Prompt”**

The aim of this laboratory activity is to create user accounts using Control Panel on Windows 10 and Windows 11. Students are to follow the following steps to carry out the laboratory activity.

**Step1:** Press Win + X and select "Command Prompt (Admin)" or "Windows PowerShell (Admin)."

**Step2:** Type the following command and press Enter

```
net user [username] [password] /add
```

**Step3:** Replace [username] with the desired username and [password] with the desired password.

**Step4:** To create new user with administrative privileges, type the following command and press Enter:

```
net localgroup administrators [username] /add
```

### **4.0 Self-Assessment Laboratory activity**

**Activity:** Students are to create user accounts on Windows 10 and Windows 11 using PowerShell.

### **5.0 Conclusion**

You have learnt from this unit about different types of user accounts on both the windows-based computer and Unix based computer. You have also learnt how to create user accounts in windows-based computer. Four (4) methods of creating user accounts have been discussed in this unit.

## 6.0 Summary

This unit covered different types of user account in both windows based computer and unix based computer. The unit also gave step by step by which user accounts can be created in windows based computer.

## 7.0 Further Readings

Krebs, B. (2012). *The Scrap Value of a Hacked PC, Revisited* Retrieved from <http://www.krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/>

Glanz, J. & Markoff, J. (2011). Egypt Leaders Found 'Off' Switch for the Internet', *The New York Times*, 15 February 2011. Retrieved from <http://www.nytimes.com/2011/02/16/technology/16internet.html?>

Matlack, C. (2014). 'Swift Justice: One Way to Make Putin Howl'. *Bloomberg Business*, 4 September 2014, Retrieved from <http://www.bloomberg.com/bw/articles/2014-09-04/ultimate-sanction-barring-russian-banks-from-swiftmoney-system>