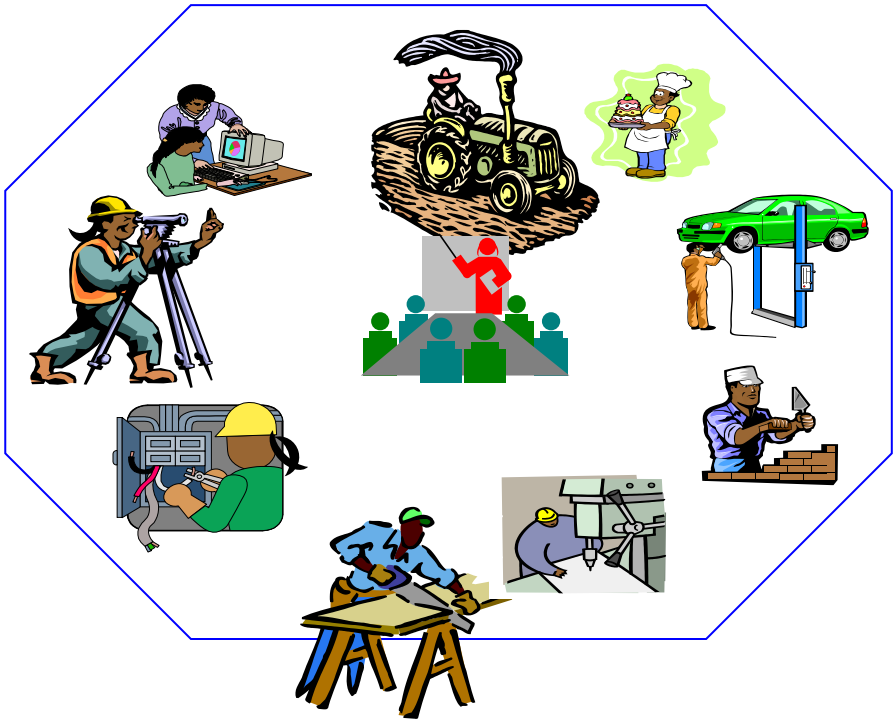

HARD WARE SND NETWORK SERVICING LEVEL III

Based on August, 2011, Version 3

Occupational Standard (OS)

Module Title: Monitoring and Administer System and Network Security

LG Code: EIS HNS3 M07 LO (1-4) LG (23-26)

TTLM Code: EIS HNS3 TTLM 1220v1

December 2020

Bishoftu, Ethiopia

Contents

L G# 7 LO #1- Ensure user accounts are controlled

Instruction sheet

This learning guide is developed to provide you the necessary information regarding the following content coverage and topics:

- Modifying default user settings to confirm security policy
- Modifying previously created user setting to update security policy
- Ensuring Displayed legal notices at logon
- Using appropriate utilities to check strength of passwords and complexity
- Reviewing actions taken to ensure password procedures
- Accessing information services to identify security gaps

This guide will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Modify default user settings to confirm security policy
- Modify previously created user setting to update security policy
- Ensure Displayed legal notices at logon
- Use appropriate utilities to check strength of passwords and complexity
- Review actions taken to ensure password procedures
- Access information services to identify security gaps

Read the specific objectives of this Learning Guide.

1. Follow the instructions described below.
2. Read the information written in the “Information Sheets”. Try to understand what are being discussed. Ask your trainer for assistance if you have hard time understanding them.
3. Accomplish the “Self-checks” which are placed following all information sheets.
4. Ask from your trainer the key to correction (key answers) or you can request your trainer to correct your work. (You are to get the key answer only after you finished answering the Self-checks).
5. If you earned a satisfactory evaluation proceed to “Operation sheets
6. Perform “the Learning activity performance test” which is placed following “Operation sheets” ,
7. If your performance is satisfactory proceed to the next learning guide,
8. If your performance is unsatisfactory, see your trainer for further instructions or go back to ” operation sheets “

Information Sheet 1.1 Modifying default user settings to confirm security policy

Modifying default user settings to confirm security policy

Windows Server 2008 creates a Default Domain Policy GPO for every domain in the forest. This domain is the primary method used to set some security-related policies such as password expiration and account lockout.

You can use fine-grain password and account lockout policy to apply custom password and account lockout policy settings to individual users and global security groups within a domain.

The domain password policy allows you to specify a range of password security options, including how frequently users change their passwords, how long passwords must be, how many unique passwords must be used before a user can reuse one, and how complex passwords must be.

You can use account lockout to prevent successful brute force password guessing. If it's not enabled, someone can keep attempting to guess username/password combinations very rapidly using a software-based attack. The proper combination of settings can effectively block these types of security vulnerabilities.

Using Account Lockout Policy, you can configure the following settings:

Account lockout duration

This option determines the amount of time that a locked-out account will remain inaccessible. Setting this option to 0 means that the account will remain locked out until an administrator manually unlocks it. Select a lockout duration that will deter intruders without crippling your authorized users; 30 to 60 minutes is sufficient for most environments.

Account lockout threshold

This option determines the number of invalid logon attempts that can occur before an account will be locked out. Setting this option to 0 means that accounts on your network will never be locked out.

Reset account lockout counter after

This option defines the amount of time in minutes after a bad logon attempt that the "counter" will reset. If this value is set to 45 minutes, and user jsmith types his password incorrectly two times before logging on successfully, his running tally of failed logon attempts will reset to 0 after 45 minutes have elapsed. Be careful not to set this option too high, or your users could lock themselves out through simple typographical errors.

For each item that you want to configure, right-click the item and select **Properties.** To illustrate, we create an Account lockout threshold of three invalid logon attempts. In the screen shown in the below Figure , place a check mark next to **Define this policy setting,** and then enter the appropriate value.

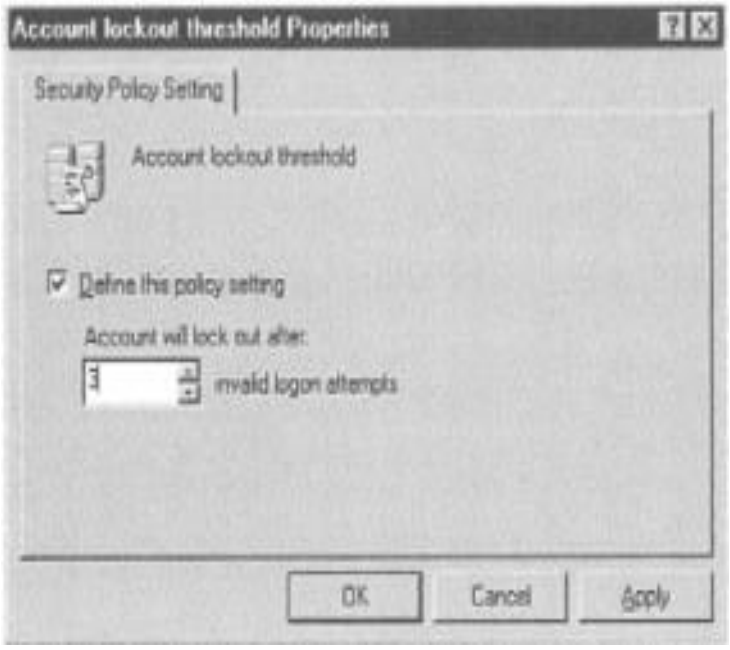

Fig 1.1. Account lockout threshold properties

Self-Check1

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. ___option determines the amount of time that a locked-out account will remain inaccessible.
   A. Reset account lockout counter after
   B. Account lockout duration
   C. Account lockout threshold

2. _____ allows you to specify a range of password security options
   A. The domain password policy
   B. Client password policy
   C. Adding roles

3. _____ Option defines the amount of time in minutes after a bad logon attempt that the "counter" will reset.
   A. Reset account lockout counter after
   B. Account lockout duration
   C. Account lockout threshold

Note: **Satisfactory rating half 100%**

You can ask you teacher for the copy of the correct answers.

Answer Sheet

Score = _____
Rating: _____

Name: _____ Date: _____

Information Sheet 1.2Modifying previously created user setting to update security policy

2.1. Managing user account settings

User accounts are created so that people can identify themselves to the system and receive access to the network resources they need. In Windows Server 2008 with Active Directory enabled, user accounts (often called *user IDs*) are assigned using the Active Directory Users and Computers management console. On standalone Windows Server 2008 computers, user accounts are created using the User Accounts applet in Control Panel.

User Account Settings

In the New User Creation Wizard, the default password settings force the new user to change the password at the first successful logon. This ensures that the administrator does not know the user's credentials and therefore cannot impersonate the user. Also, forcing the user to change his password immediately makes him aware of any password complexity rules the organization has chosen, because if the password is too short or not complex enough, Windows Server 2008 will reject it and force the user's new password to comply with the complexity rules in order to log in.

The second password setting is User Cannot Change Password. Typically, an organization wants users to be able to change their own passwords, but occasionally (as for a visitor account) the password should not be changed.

Next is a setting that allows the administrator to exempt this account from the password-expiration rule. Most organizations want their users to change their passwords regularly (every 60 days, for example) so that if a password has been compromised, its useful period to gain access to the network is limited. The exception to this rule is for service accounts. A service account is used so that applications, such as Microsoft Exchange and Microsoft SQL Server, have access to network resources. These applications expect the password to never be changed, or if it is changed, the change must be performed using the management tool for the application, and not through the ADUC.

Finally, the account can be disabled with the last check box, Account Is Disabled. This feature is generally used in one of two cases: when the account is created before the user is

physically onsite or when the user is temporarily or permanently gone from the organization. In both cases, no one should be able to use the account, so disabling it is an appropriate security precaution.

The account has now been created, and at this point the user could log in. However, there are many properties of the account that we have not yet set, so let's now look at how to modify a user account with Active Directory Users and Computers.

Once the user object has been created, you can select it and review or set its properties. Simply double-clicking the object in the right panel of ADUC opens a Properties dialog box, as shown below

Larger organizations generally have a list of the required information that must be entered for each user account. As an example, it may be mandatory to fill in the Office Location field, and there may be a fixed list of allowable entries. Like all fields in a user object, it is possible to search on the contents of the Office Location field.

Self-Check 2

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. Users are identify themselves to the system and receive access to the network resources they need using:
   A. User accounts
   B. File server
   C. Print server
2. ____setting prevents users to be able to change their own passwords.
   A. Disable password
   B. User Cannot Change Password
   C. Expire password
3. _____ setting that allows the administrator to exempt the account from the password-expiration rule.
   A. Creating password
   B. Password expiration
   C. Changing password

Note: **Satisfactory rating 100%**

You can ask you teacher for the copy of the correct answers.

Answer Sheet

Score = _____
Rating: _____

Name: _____ Date: _____

Information Sheet 1.3 Ensuring Displayed legal notices at logon

1.3.1. Configure Legal Notices on Domain Computers Using Group Policy

In certain sensitive business situations, reminding users of their legal responsibilities with regard to enterprise information technology and systems can be just as important as other security measures. On most operating systems, one of the most effective ways to regularly communicate legal obligations to users is with a login message.

When you configure legal notice, the legal notice message appears when the user hits CTRL+ALT+DEL.

Most of all you can configure legal notices on domain computers in two ways:

- You can write a fancy script and execute it at the every logon
- Configure legal notice using a group policy.

You can use the message display functionality to personalize the logon process, provide news or information, and for other similar purposes. The message appears after the user presses CTRL+ALT+DEL and disappears after the user clicks OK.

Self-Check 3

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. When you configure legal notice, the legal notice message appears when the user hits _____ keys
2. Most of all you can configure legal notices on domain computers in two ways :
   A. _____
   B. _____
3. the most effective ways to regularly communicate legal obligations to users is with a _____message.

Note: **Satisfactory rating 100%**

You can ask you teacher for the copy of the correct answers.

Answer Sheet

Score = _____
Rating: _____

Name: _____ Date: _____

Operation Sheet 1.1 Ensuring Displayed legal notices at logon

1.1.1. **Operation Purpose**

To acquire the trainees the skill of - **Configuring legal notices at logon**

Equipment, tools and materials required:

Supplies and equipment needed or useful for **Configuring legal notices at logon** are:

- Desk top or lap top computer installed with the required operating system
- Local area network installation

Procedures:
To configure Legal Notices on Domain Computers Using Group Policy

1. Login to the domain controller with an administrator account.
2. Click Start > Administrative Tools > Group Policy Management.
3. Under Domains, right click your domain and click **Create a GPO in this domain, and link it here**.

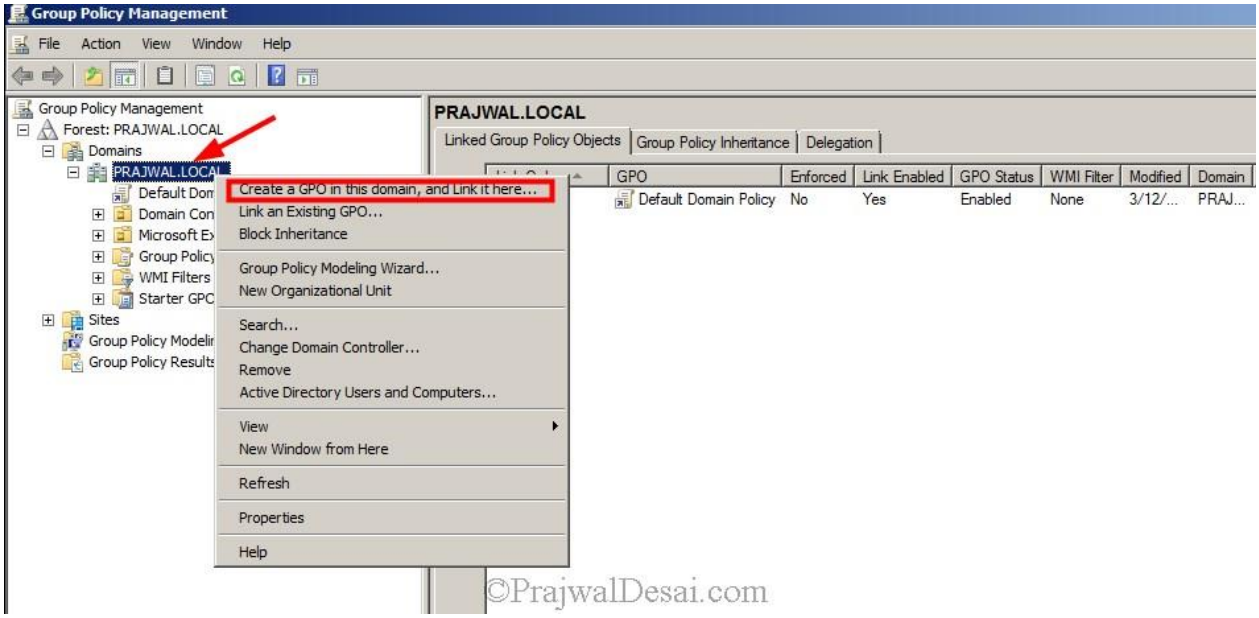

Fig 1.1. 1. Group policy management

Create a policy and name it as **Logon_Banner**. Click **OK**.

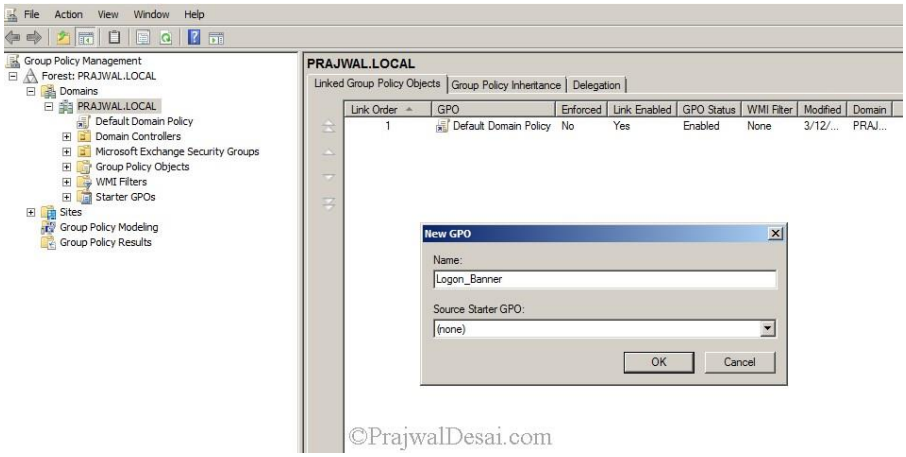

Fig 1.1.2. New group policy

Right click this new policy **Logon Banner** and click **Edit**. You should see Group Policy Management Editor.

In the next step expand **Computer Configuration** > **Policies** > **Windows Settings >Security Settings > Local Policies**. Now click **Security Options.**

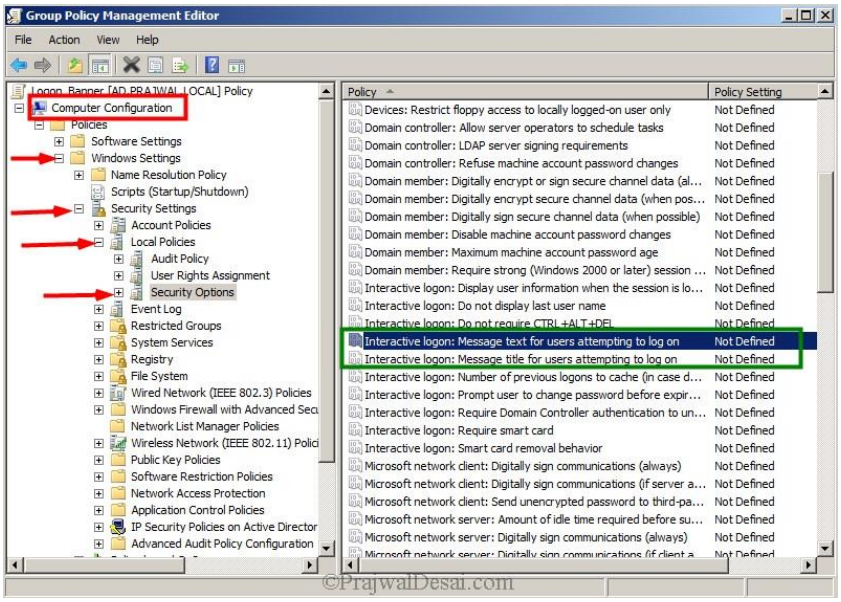

Fig 1.1.3 Group policy management editor

On the right pane look for the policy **Interactive Logon : Message text for users attempting to log on.** This security setting specifies a text message that is displayed to

users when they log on. You can paste the Logon text that is to be displayed to the users before they log in. Click **Apply** and **OK**.

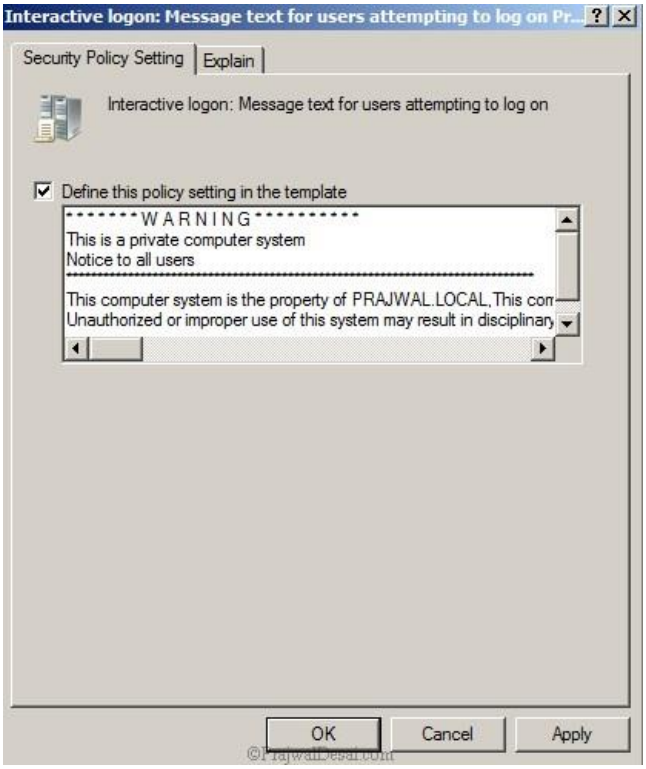

Fig 1.1.4. Interactive logon

On the right pane look for the policy **Interactive Logon: Message title for users attempting to log on.** This security setting allows the title to appear in the title bar of the window that contains the Interactive logon.

Type the title text and click **Apply** and **OK**.

Fig 1.1.5. Interactive logon manager

On the client computer open the command prompt and run the command **gpupdate**.

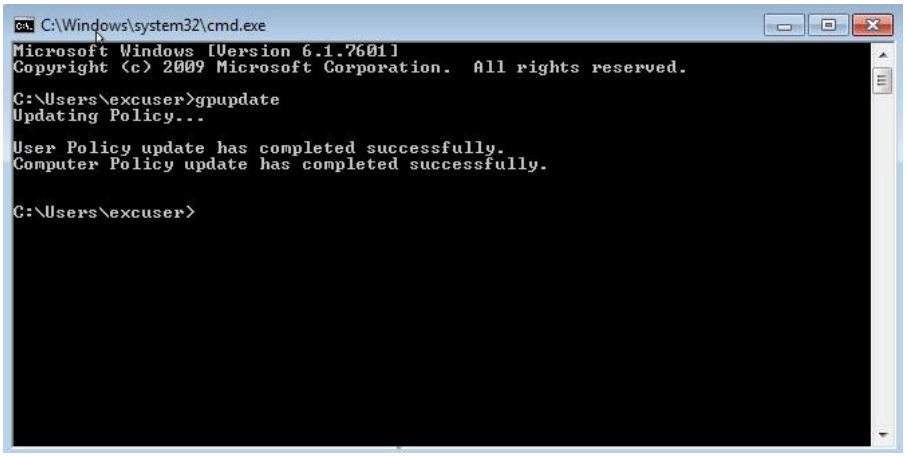

Fig 1.1.6. Gpupdate window

Log off from the client computer. Hold CTRL+ALT and press DEL. You should now see the logon banner. Click OK to login to the computer.

Fig 1.1.7 logon banner

LAP Test 1 : Practical Demonstration on Displaying legal notices at logon

Name: _____ Date: _____

Time started: _____ Time finished: _____

Instructions: Given necessary templates, tools and materials you are required to perform the following tasks within --- hour.

Task 1. Create logon notices

Task 2. Check the created logon notices on the client computer

Information Sheet 1.4: Using appropriate utilities to check strength of passwords and complexity

1.4.1. Utilities used to check strength of passwords and complexity

Currently, password strength checkers and other validation tools flood the web. However, with this bounty of available tools come new challenges. Enterprises need to determine which tools they can trust with their potential and current credentials. Additionally, they also need to understand what these tools can teach their employees about their identity management.

We compiled 6 password validation tools which we consider secure for your identity management strategies. We explore them in-depth below.

Best Practices for Password Strength Checkers

Before you use password strength checkers, you need to understand a critical aspect of identity and access management: password best practices. After all, what good is a password validation tool if you don't know how to compose a strong password?

Critically, most password strength checkers judge credentials based on two key factors: strength and complexity. The longer the password, the more time a cracking program requires to uncover it. A password of twelve characters proves far more secure than a password of eight characters. Therefore, your enterprise should mandate minimum passwords of at least ten characters and allow for longer ones.

As for complexity, most users know the general requirements: include letters both upper and lower case, numbers, and punctuation. However, most identity and password experts recommend not using sequences in your passwords; hackers' cracking programs can identify patterns easily and exploit them. Plus, using phrases and sentences often prove easier to remember and stronger for cyber security. Consider the following recommendations

- **Don't Allow Repeated Passwords**

Often, this proves easier said than done; many employees feel overwhelmed by the number of passwords they must remember to perform their jobs. Regardless, employees should never repeat passwords in either their professional or personal lives. More importantly, they should never cross-use their credentials.

The more a password appears across the web, the more likely it ends up in hackers' hands through other breaches. With these, hackers can conduct largely successful credential stuffing attacks.

- **Don't Allow the Sharing of Passwords**

This remains a persistent problem across enterprises of all sizes. Employees can and will share their passwords with others; often they do so to facilitate business processes and efficiencies. Of course, this leads to more insider threats and a loss of control over users' access. Put severe penalties in place for sharing passwords.

Additionally, forbid employees from writing down their passwords, either on physical paper or in document applications. That almost always leads to significant issues in the long term.

- **Don't Incorporate Personal Information into Your Passwords**

Stereotypically, birthdays often end up in users' passwords. However, this precept extends further than that. Social media research and other kinds of open personal information allow hackers to conduct significant research on their targets with minimal efforts. Obviously, this allows them to inflict subtler social engineering and phishing attacks.

Less obviously, hackers can use this information to guess users' passwords. Usually, users create passwords they can remember easily which means drawing on their interests.

- **Remember Password Expiration Policies Don't Work**

Although many cyber security and identity management providers only now recognize the futility of password expiration policies. In fact, they can actually cloud your identity security protocols, as it creates more long term confusion.

Instead, identity management experts believe it better to mandate strong passwords and secure them rather than constantly expire them.

- **Secure Privileged Access Accounts as Well**

All of the precepts described above apply equally to privileged users and regular ones. In fact, they may apply more to the former; hackers tend to target privileged access credentials more than regular ones because of the network power they wield. At the same time, privileged users are subject to the same identity foibles as their regular counterparts.

- **Select a Next-Gen Identity and Access Management Solution**

Only modern identity security solutions can provide the necessary password security capabilities to survive in the modern digital landscape. Legacy identity solutions remain behind the time both in terms of threat intelligence and capabilities.

The Top 6 Password Strength Checkers and Validation Tools

Of course, you should only use password strength checkers which you can trust. Obviously, a trustworthy validation tool should never store your passwords in any capacity; they should only process your passwords in the browser. Again, you should never input your password into sites you don't trust.

Another important note is that almost all of these password strength checkers and validation tools call themselves educational tools; they provide non-binding advice and exist primarily to help users understand what they need to improve their passwords.

Therefore, you should use these password strength checkers as intended—to demonstrate why typical passwords don't suffice in modern identity management. Provide them to your employees to help them determine how best to write strong passwords and push them away from weaker ones. Additionally, you can use them to help you formulate your own password policies.

We cultivated a clear list of password vaults we believe to be secure. However, you should do your own evaluation of these sites to ensure your users' credentials' safety.

Theft by hackers

Rather than operating like other straightforward password strength checkers, Have I Been Pawned? Actually determines whether a particular email account has been exposed.

"Have I Been Pawned?" details the breach information in which the account appears and what information became exposed in those breaches. It can provide a strong wake-up call to users to change their passwords if they suffered a breach.

1. **Comparitech Password Strength Test**

The Comparitech Password Strength Test provides a strong baseline for other password strength checkers. For example, the test can demonstrate how long hackers need to crack the inputted password.

This test evaluates passwords based on complexity, length, and can determine whether the password appears in the list of most commonly used passwords. As a bonus, this test hashes the passwords automatically, which isn't always the case.

2. **My1Login Password Strength Test**

Much like the password checker above, the My1Login Password automatically hashes the password inputted; this helps establish trust with the validation tool. Also, it too gives an estimate on the time needed to crack the password.

However, My1Login offers much more conservative timeframe estimates. A super complex password labeled as 13 sextillion years to crack only requires hackers two years to crack, according to this tool. If anything, this could be a sobering reminder on the relative security of passwords.

3. **Thycotic Password Strength Checker**

The Thycotic Password Strength Checker can also recognize the most common passwords and warns against them. Further, it can identify dictionary words, recognizes repeated patterns of characters, and suggest ways to improve password strength.

4. **LastPass: How Secure Is My Password?**

From one of the most prominent of password managers, we wanted to include LastPass to emphasize the potential of password management. Such tools when paired with other identity and access management solutions can help employees deal with the myriad password demands of their day-to-day business processes.

5. **JavaScript Password Strength Checkers Code**

Instead of using external password strength checkers, your enterprise could design your own using JavaScript.

Self-Check 4.

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. The two credentials used to check password is:
   A. Strength and complexity.
   B. Hacker and cracker
   C. Password expiration policy
2. Which one not allowed to securing pass word?
   A. Incorporate Personal Information into Your Passwords
   B. Sharing password
   C. All
3. To make our password complex we have to use a combination of:
   A. letters both upper and lower case
   B. Numbers
   C. Punctuation
   D. All

Note: **Satisfactory rating 100%**

You can ask you teacher for the copy of the correct answers.

Answer Sheet

Score = _____
Rating: _____

Name: _____ Date: _____

Information Sheet 1.5 Reviewing actions taken to ensure password procedures

- **Best Practices/Recommendations to implement password procedures**

The successful adoption of a password procedure depends on the ability of the organization to enforce it. Some organizations/authorities have sophisticated technologies that can provide substantial automation and support for a large number of users. Others may have limited resources and will need to develop a procedure that is manageable in a more manual fashion. When creating a password procedure, it is important to consider:

- ✓ Software security settings.
- ✓ Minimum length of a password and expiry cycle for passwords.
- ✓ Issues that would be linked to user education include not having passwords displayed on sticky notes and not sharing passwords.
- ✓ Password retention.

After action review of password procedures Organizational learning requires that teams continuously assess their performance to identify and learn from successes and failures.

The After Action Review (AAR) is a simple but powerful tool to help you do this. Conducting an AAR at the end of a project, program or event can help you and your team learns from your efforts. Furthermore, sharing the results from your AAR can help future teams learn your successful strategies and avoid pitfalls you have worked to overcome.

An AAR is centered on four questions:

1. What was expected to happen?
2. What actually occurred?
3. What went well and why?
4. What can be improved and how?

Self-Check 5

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. When creating a password procedure, it is important to consider Most of all you can configure legal notices on domain computers in two ways :

   _____
   _____
   _____
   _____

4. The four After Action Review question is:

   _____
   _____
   _____
   _____
   _____
   _____

Note: **Satisfactory rating 100%**

You can ask you teacher for the copy of the correct answers.

Answer Sheet

Score = _____
Rating: _____

Name: _____ Date: _____

Information Sheet 1.6 Accessing information services to identify security gaps

1.5.1. Identifying security gap using the required hard ware and software tools

A primary task of any information security professional is to manage or perform an information security gap analysis to find potential security vulnerabilities and risks and to use the information to implement solutions to bridge the gaps.

The main objective of security analysis is to continually improve and move closer to the desired security position and to transition security from its current state to its future improved state. Several critical steps in the process must always be addressed when conducting a useful gap analysis.

Importance of gap analysis

A gap analysis can be performed for various reasons. Generally, no matter the background, it is a tool used for improving the state of something — to raise the performance level of the particular area in question. it can be used at different levels. Also, it can be centered on different perspectives, such as organizational, business process, business direction, and technology perspectives.

An information security gap analysis is an excellent way for an organization to understand where to focus its security efforts for maximum security improvement. Additionally, it's often a compliance requirement, to obtain and maintain compliance with a particular standard or regulation. However, this is not the only reason for performing one. A primary purpose is to help organizations uncover risks and vulnerabilities and to improve their information security posture ultimately.

For every gap analysis, the process should include describing the scope or the area to be analyzed, identifying the improvement areas, defining the targets, identifying the current state and devising a plan of action or steps to achieve the desired future state.

Self-Check 6:

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. The main objective of security analysis is to continually improve and move closer to the desired security position
   A. True
   B. False
2. Gap analysis can be centered on:
   A. Organizational
   B. business process
   C. business direction and technology perspectives
   D. All

Note: **Satisfactory rating 100%**

You can ask you teacher for the copy of the correct answers.

Answer Sheet

Score = _____
Rating: _____

Name: _____ Date: _____

L G# 7	LO #2- Secure file and resource access

Instruction sheet

This learning guide is developed to provide you the necessary information regarding the following content coverage and topics:

- Reviewing and considering inbuilt security and access features of

  operating system

- Developing or reviewing file security categorization scheme

- Understanding the role of users in setting security

- Implementing and scheduling virus checking process on server,

  computer and other components

This guide will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Review and considering inbuilt security and access features of

  operating system

- Develop or reviewing file security categorization scheme

- Understand the role of users in setting security

- Implement and scheduling virus checking process on server,

  computer and other components

Read the specific objectives of this Learning Guide.

1. Follow the instructions described below.
2. Read the information written in the “Information Sheets”. Try to understand what are being discussed. Ask your trainer for assistance if you have hard time understanding them.
3. Accomplish the “Self-checks” which are placed following all information sheets.
4. Ask from your trainer the key to correction (key answers) or you can request your trainer to correct your work. (You are to get the key answer only after you finished answering the Self-checks).

Information Sheet 2.1: Reviewing and considering inbuilt security and access features of operating system

2.1.1. Feature description

Computers that are running a supported version of Windows can control the use of system and network resources through the interrelated mechanisms of authentication and authorization. After a user is authenticated, the Windows operating system uses built-in authorization and access control technologies to implement the second phase of protecting resources: determining if an authenticated user has the correct permissions to access a resource.

Shared resources are available to users and groups other than the resource's owner, and they need to be protected from unauthorized use. In the access control model, users and groups (also referred to as security principals) are represented by unique security identifiers (SIDs). They are assigned rights and permissions that inform the operating system what each user and group can do. Each resource has an owner who grants permissions to security principals. During the access control check, these permissions are examined to determine which security principals can access the resource and how they can access it.

Security principals perform actions (which include Read, Write, Modify, or Full control) on objects. Objects include files, folders, printers, registry keys, and Active Directory Domain Services (AD DS) objects. Shared resources use access control lists (ACLs) to assign permissions. This enables resource managers to enforce access control in the following ways:

- Deny access to unauthorized users and groups
- Set well-defined limits on the access that is provided to authorized users and groups

Object owners generally grant permissions to security groups rather than to individual users. Users and computers that are added to existing groups assume the permissions of that group. If an object (such as a folder) can hold other objects (such as subfolders and files), it is called a container.

In a hierarchy of objects, the relationship between a container and its content is expressed by referring to the container as the parent. An object in the container is referred to as the child, and the child inherits the access control settings of the parent.

Object owners often define permissions for container objects, rather than individual child objects, to ease access control management.

Practical applications

Administrators who use the supported version of Windows can refine the application and management of access control to objects and subjects to provide the following security:

- ✓ Protect a greater number and variety of network resources from misuse.
- ✓ Provision users to access resources in a manner that is consistent with organizational policies and the requirements of their jobs.
- ✓ Enable users to access resources from a variety of devices in numerous locations.
- ✓ Update users' ability to access resources on a regular basis as an organization's policies change or as users' jobs change.
- ✓ Account for a growing number of use scenarios (such as access from remote locations or from a rapidly expanding variety of devices, such as tablet computers and mobile phones).
- ✓ Identify and resolve access issues when legitimate users are unable to access resources that they need to perform their jobs.

Self-Check 1

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. Shared resources use _____ to assign permissions
   A. access control lists (ACLs
   B. Domain name
   C. User account
2. Users and computers that are added to existing groups assume the permissions of that Group.
   A. True
   B. False
3. . In the access control model, users and groups are represented by:
   A. Unique security identifiers (SIDs).
   B. User name
   C. all

Note: **Satisfactory rating 100%**

You can ask you teacher for the copy of the correct answers.

Answer Sheet

Score = _____
Rating: _____

Name: _____ Date: _____

Information Sheet 2.2: Developing or reviewing file security categorization scheme and Role of users

2.2.1. Introduction

Data classification allows organizations to think about data based on sensitivity and business impact, which then helps the organization assess risks associated with different types of data. Reputable standards organizations, such as the International Standards Organization (ISO) and the National Institute of Standards and Technology (NIST), recommend data classification schemes so that information can be more effectively managed and secured according to its relative risk and criticality, advising against practices that treat all data equally.

2.2.2. Principles of data and information categorization

The implementation of information management in general and data classification in particular varies by type of organization and may even vary depending on the individual organization. However, certain fundamental principles are common across governments, nongovernment organizations, and commercial organizations. The following is a refinement of six principles expressed by national (and regional) legal sources and international organizations' instruments for information management. The principles below should be used as guidance rather than a single, standing benchmark in the construction and/or refinement of an information management and data classification strategy

- **The six principles of data and information categorization**

  - ✓ **Openness, transparency, and societal values**: Classification should be used cautiously and in accordance with the sensitivity, value, and criticality of data. Access restrictions should only be chosen for cases where information disclosure may be detrimental to the legitimate interests and legal obligations of the organization itself, its staff, or third parties.
  - ✓ **Content driven, technology neutral approach**: Information should be classified on the basis of its contents and the risks associated with the compromise of the content, regardless of its format, media, or origin. There should be no discrimination based on the format or media of the information – whether analogue (paper) or digital;

stored in an information system, on storage media, on mobile devices, or in the Cloud.

- ✓ **Risk management approach**: Information should be afforded protection in accordance with the level of sensitivity, value, and criticality of the information; this is usually done in a graded approach based on levels corresponding to value and risk. A protection level circumscribes the set of measures to reduce risks to an acceptable level – i.e. the potential severity and likelihood – that information is compromised.
- ✓ **Proportionality**: Information shall be classified to an appropriate level which should be as low as possible, but as high as necessary.
- ✓ **Clear roles and responsibilities**: with regard to data classification, policy and processes should be assigned for information security within the organization and upheld by management awareness and commitment to information security.
- ✓ **Lifecycle approach**: As a part of an information management system, the classification system should have consideration for information throughout its lifecycle: from creation or receipt, storage, retrieval, modifications, transfer, copying, and transmission to destruction

- **Reviewing and Monitoring Data security**

✓ **Periodic review and adjustment**

Beyond the continuous monitoring and assessment, periodic systematic reviews enable adjustments to data access and review of classified data. A reclassification and revision methodology can ensure that security measures are applied that are suited to the current technology and threat/ risk environment, but also the changing value and sensitivity of the classified data. Classified information should be reviewed regularly to prevent legacy information lingering, which is costly to store and manage. It is advisable to likewise review classification policies and procedures on a periodic basis.

- **Role of users in setting security**

✓ **Supervision and quality assurance**

An appropriate entity should be assigned for supervision, advice and consulting, as well as revision of classification decisions – e.g. Chief Information Officer (CIO), Chief Data Officer (CDO, or Chief Information Security Officer (CISO) with dedicated responsibility

for data classification, data risk decisions, and required protection measures. That entity should also be empowered to ensure quality assurance for the implementation of security controls, the suitability and adequacy of existing controls for meeting the desired security objectives, and any compliance requirements.

- ✓ **Continuous improvement and monitoring**

After the data assets have been classified, the security procedures need to be implemented with a view of constant monitoring and assessment in order to continue meeting risk management and compliance requirements. In order to continue meeting the policy's security objectives, it is advisable to develop security standards and implementation guides based on current technical and non-technical capabilities, which can be updated to adopt new innovations more readily without having to update the policy.

Self-Check 2

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. Beyond the continuous monitoring and assessment, _____enable adjustments to data access and review of classified data.
   A. Risk management approach
   B. Supervision and quality assurance
   C. Clear roles and responsibilities
   D. periodic systematic reviews
2. _____Information shall be classified to an appropriate level which should be as low as possible, but as high as necessary.
   A. Classified
   B. Uncategorized data
   C. Proportionality
3. After the data assets have been classified, the security procedures need to be implemented with a view of constant monitoring and assessment in order to continue meeting risk management and compliance requirements.
   A. Proportionality
   B. Risk management approach
   C. Appropriate

Note: **Satisfactory rating 100%**

You can ask you teacher for the copy of the correct answers.

Answer Sheet

Score = _____
Rating: _____

Name: _____ Date: _____

2.3.1. Scheduling and Running antivirus software on domain controllers

Virus Detection Software

Because viruses were the first malware, the software that detects and removes malware is still known as “virus” software, although such programs have been upgraded over time to handle all types of malware. At one time, there were many virus detection software packages available. As with most software arenas, however, time has shaken out the marketplace, leaving several leading products that have shown to have staying power.

You can perform malware detection at two places: on each host or on your servers. In particular, it is well worth the investment to purchase an e-mail server that includes malware detection. Because malware can enter a computer through a vehicle other than e-mail, you should also have virus checkers installed–and preferably set to run automatically–on all computers.

Network firewall security

A firewall is a piece of software or hardware that filters all incoming and outgoing traffic to your business. Firewall devices can:

- ✓ block malicious email relaying
- ✓ prevent malware being downloaded from untrusted websites
- ✓ prevent access to blacklisted websites or unsecure services

- **Hardware firewall**

Is a part of broadband routers, It protects your entire local network from unauthorized external access and is usually effective even with minimal configuration.

- **Software firewall**

Is an application installed on individual computers and devices, It is often part of the operating system and usually needs greater configuration of settings and applications controls.

Because domain controllers provide an important service to clients, the risk of disruption of their activities from malicious code, from malware, or from a virus must be minimized. Antivirus software is the generally accepted way to reduce the risk of infection. Install and configure antivirus software so that the risk to the domain controller is reduced as much as possible and performance is affected as little as possible.

The following list contains recommendations to help you configure and install antivirus software on a Windows Server domain controller.

- Antivirus software must be installed on all domain controllers in the enterprise. Ideally, try to install such software on all other server and client systems that have to interact with the domain controllers. It is optimal to catch the malware at the earliest point, such as at the firewall or at the client system where the malware is introduced. This prevents the malware from ever reaching the infrastructure systems that the clients depend on.
- Use a version of antivirus software that is designed to work with Active Directory domain controllers and that uses the correct Application Programming Interfaces (APIs) to access files on the server
- Do not use a domain controller to browse the Internet or to perform other activities that may introduce malicious code.
- We recommend that you minimize the workloads on domain controllers. When possible, avoid using domain controllers in a file server role. This lowers virus-scanning activity on file shares and minimizes performance overhead.
- Do not put Active Directory or FRS database and log files on NTFS file system compressed volumes.

Turn off scanning of Active Directory and Active Directory-related files

- Exclude the Main NTDS database files. The location of these files is specified in the following registry sub key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters\DSA Database File

The default location is %windir%\Ntds. Specifically, exclude the following files:

Ntds.dit

Ntds.pat

- Exclude the Active Directory transaction log files. The location of these files is specified in the following registry sub key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters\Database Log Files Path

Self-Check 3

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. Firewall devices can:

   A. block malicious email relaying
   B. prevent malware being downloaded from untrusted websites
   C. prevent access to blacklisted websites or unsecure services
   D. All

2. You can perform malware detection on

   A. each host
   B. your servers
   C. A and B

3. _____ is a piece of software or hardware that filters all incoming and outgoing traffic to your business

   A. Antivirus
   B. Firewall
   C. Server

Note: **Satisfactory rating 100%**

You can ask you teacher for the copy of the correct answers.

Answer Sheet

Score = _____
Rating: _____

Name: _____ Date: _____

L G# 7 **LO #3- Determine authentication requirements**

Instruction sheet

This learning guide is developed to provide you the necessary information regarding the following content coverage and topics:

- Determining user and enterprise security requirements
- Identifying and analyzing authentication options
- Selecting most appropriate authentication and authorization processes

This guide will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Determine user and enterprise security requirements
- Identify and analyzing authentication options
- Select most appropriate authentication and authorization processes

Read the specific objectives of this Learning Guide.

1. Follow the instructions described below.
2. Read the information written in the “Information Sheets”. Try to understand what are being discussed. Ask your trainer for assistance if you have hard time understanding them.
3. Accomplish the “Self-checks” which are placed following all information sheets.
4. Ask from your trainer the key to correction (key answers) or you can request your trainer to correct your work. (You are to get the key answer only after you finished answering the Self-checks).

Information Sheet 3.1 Determining user and enterprise security requirements

Identifying Security Threats

The most typical threats to directory security include the following:

- **Eavesdropping.** Information remains intact, but its privacy is compromised. For example, someone could learn your credit card number, record a sensitive conversation, or intercept classified information.
- **Unauthorized access.** This threat includes unauthorized access to data through data-fetching operations. Unauthorized users might also gain access to reusable client authentication information by monitoring the access of others. The Directory Server Enterprise Edition authentication methods, password policies, and access control mechanisms provide effective ways of preventing unauthorized access.
- **Tampering.** Information in transit is changed or replaced and then sent on to the recipient. For example, someone could alter an order for goods or change a person's resume.

  This threat includes unauthorized modification of data or configuration information. If your directory cannot detect tampering, an attacker might alter a client's request to the server. The attacker might also cancel the request or change the server's response to the client. The Secure Socket Layer (SSL) protocol and similar technologies can solve this problem by signing information at either end of the connection.
- **Impersonation.** Information passes to a person who poses as the intended recipient.

Impersonation can take two forms, spoofing and misrepresentation.

- ✓ **Spoofing.** A person or computer impersonates someone else. For example, a person can pretend to have the mail address jdoe@example.com, or a computer can identify itself as a site called www.example.com when it is not.
- ✓ **Misrepresentation.** A person or organization misrepresents itself. For example, suppose the site www.example.com pretends to be a furniture store

when it is really just a site that takes credit-card payments but never sends any goods.

- **Denial of service.** In a denial of service attack, the attacker's goal is to prevent the directory from providing service to its clients. Directory Server Enterprise Edition provides a way of preventing denial of service attacks by setting limits on the resources that are allocated to a particular bind DN.

Security Methods required by users /enterprises

A security policy must be able to prevent sensitive information from being modified or retrieved by unauthorized users, but easy enough to administer.

Directory Server Enterprise Edition provides the following security methods:

- **Authentication.** Provides a means for one party to verify another's identity. For example, a client gives a password to Directory Server during an LDAP bind operation. As part of the authentication process, password policies define the criteria that a password must satisfy to be considered valid, for example, age, length, and syntax. Account inactivation disables a user account, group of accounts, or an entire domain so that all authentication attempts are automatically rejected.
- **Encryption.** Protects the privacy of information. When data is encrypted, the data is scrambled in a way that only the recipient can decode. The Secure Sockets Layer (SSL) maintains data integrity by encrypting information in transit. If encryption and message digests are applied to the information being sent, the recipient can determine that the information was not tampered with during transit. Attribute encryption maintains data integrity by encrypting stored information.
- **Access control.** Tailors the access rights that are granted to different directory users, and provides a means of specifying required credentials or bind attributes.
- **Auditing.** Enables you to determine if the security of your directory has been compromised. For example, you can audit the log files maintained by your directory.

These security tools can be used in combination in your security design. You can also use other features of the directory, such as replication and data distribution, to support your security design.

Self-Check 1:

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. By this threat a person or computer impersonates someone else
   A. Malware
   B. Spoofing
   C. Firewall
2. In _____attack, the attacker's goal is to prevent the directory from providing service to its clients.
   A. a denial of service
   B. Unauthorized access
   C. Authentication
3. _____ protects the privacy of information.
   A. Encryption.
   B. Access control
   C. Malicious

Note: **Satisfactory rating 100%**

You can ask you teacher for the copy of the correct answers.

Answer Sheet

Score = _____
Rating: _____

Name: _____ Date: _____

Information Sheet 3.2 Identifying and analyzing authentication options

3.2.1. Common Authentication Methods: Network Security

In the past few years, we've seen that even the biggest companies are not immune to security breaches. Big wigs like LinkedIn, Target, Home Depot and Sony Pictures have had their systems hacked into, revealing sensitive information of their owners, employees, and clients. With millions of passwords, email addresses and more having been exposed, there has been an increase in pressure on those who handle enterprise security to up their defenses.

Since it is difficult to keep up with how quickly the cyber-criminals can advance their knowledge of systems, network administrators have been facing plenty of challenges and had to start implementing more sophisticated ways of authenticating users. Below we discuss common authentication methods used for network security to beat the savvy cyber-crooks.

- **Authentication, authorization and access control**

Authentication, authorization and access control are three paramount **cyber security** concepts that are often confused and used interchangeably. It might be because these three are usually perceived as one single process by the end user, yet it is critically important to understand the distinction while designing the security framework.

- ✓ **Authentication**

In authentication process, identities of the users are verified. Most of the time this verification process includes a username and a password but other methods such as PIN number, fingerprint scan, smart card and such are adapted as well.

In order to conduct the process of authentication, it is essential that the user has an account in the system so that the authentication mechanism can interrogate that account. Or an account has to be created during the process.

A user is either who they claim to be or someone else. Thus the output of the authentication process is either a yes or no. 'Maybe' is treated as a no for security concerns.

In addition, the 'user' may not be an actual person but an application trying to use a web services API.

Authentication technologies are mainly used with two types of authorization processes:

- Two factor authentication
- Multi-factor authentication

In the past, multi-factor authentication was vastly popular but due to its difficulties in use, password authentication prevailed. **Two factor authentication**, on the other hand, is still a widely used security process that involves two methods of verification. One of them is password verification most of the time.

Frequently used types of authentication technology are username/password, one-time password and biometric authentication.

✓ **Authorization**

In authorization process, it is established if the user (who is already authenticated) is allowed to have access to a resource. In other words, authorization determines what a user is and is not permitted to do.

The level of authorization that is to be given to a user is determined by the metadata concerning the user's account. Such data can indicate if the user is a member of the 'Administrators' or 'Customers,' or it can indicate if the user has paid-subscription for some content.

The processes of authorization also encompass **Authorization Management** which denotes creating authorization rules. For instance, an administrator can be allowed to create such a rule that lets another user to publish content to a web page.

We create authorization policies while using social media: Facebook, LinkedIn, Twitter or Instagram have millions of users but we can authorize (to an extent) which of those users can interact with us.

Authorization technologies empowers businesses by enabling them to control what employees can access, or where and on which device they can access data.

A little level of regulation allows businesses to make sure that their staff can access sensitive data on a secure device operating within the company's firewall.

✓ **Access Control**

In the process of access control, the required security for a particular resource is enforced. Once we establish who the user is and what they can access to, we need to actively prevent that user from accessing anything they should not. Thus we can see access control as the merger of authentication and authorization plus some additional measures like IP-based restrictions.

Most of the time **security vulnerabilities in applications** stem from inadequate access control mechanisms instead of faulty authentication or authorization mechanisms. The reason why is that access control is more complex and intricate than other two. Main types of access control are **DAC (discretionary access control)**, **RBAC (role-based access control)**, **ABAC (attribute based access control)** and **MAC (mandatory access control)**

Self-Check 2

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. Authentication technologies are mainly used with two types of authorization processes:
   A. Two factor authentication
   B. Multi-factor authentication
   C. A and B
2. In the process of ____the required security for a particular resource is enforced.
   A. access control
   B. Security
   C. hacking

Note: **Satisfactory rating 100%**

You can ask you teacher for the copy of the correct answers.

Answer Sheet

Score = _____
Rating: _____

Name: _____ Date: _____

3.3.1. **Choosing the right authentication and authorization processes**

These days, there are so many different authentication methods for so many varied devices that it's hard to know what to choose.

Let's take a look at the new world a little bit. What we're finding when we talk to our customers is that enterprise authentication technologies are really struggling to meet the needs of the business, in a cost-effective secure and usable manner. There are really three principle challenges that have existed in the past but are becoming more acute, and I'll go into some of these in-depth shortly. There are more user constituencies besides employees, for example. We're also exposing more high-security applications over the Internet. They could be patient records in a clinical scenario, in a health care scenario. It could be the exposure of our ERP applications. We're exposing more applications to more users outside the firewall. And finally, not only users, but lines of business are asking for universal device access and we'll talk about what that means as well.

- **Challenges face us during authentication**

✓ **Authentication challenge #1: External users**

So the first challenge: more user constituencies. We all know that employees, partners and contractors are part of this equation. This isn't a surprise. What's happening is that partners and contractors are becoming a larger part of the equation; and they're asking for more and more employee- like access, and they're doing that because we're partnering so much more. We also have the impact of the emerging cloud in place here. So if you're a service provider or you're providing a service, by definition you've got external users coming into the system. The other attribute about these partners and contractors is that they're originating from non-managed work stations. You don't own those work stations, so some of the tricks you could pull in the past in terms of managing the security of that work station, being able to force a specific kind of authentication mechanism that might require software installation, for example, are gone. You can't do that anymore. You don't own those machines. And with these partners and contractors, we're finding that hardware-based authenticators like smart cards and particular hardware-based one-time password devices are a difficult sell to everybody, because of usability concerns, but also cost recovery concerns. So, in the good

old days when you deployed hardware-based tokens, you were able to make sure that you got those back and could re-use them because you were dealing with your employees. Unlike smart cards or other devices, one-time password devices can be re-used. So, there's a cost recovery component that's introduced with these external users. And with respect to usability, we're also hearing that these employees, the other part of the equation, are demanding simple to use authentication types. As we go through some of the other challenges in this new world, you'll start to see that this plays out in a variety of different ways.

- ✓ **Authentication challenge #2: Increased exposure of high identity assurance applications over the Internet**

We're exposing more of our core applications, like ERP, and lines of business units are demanding this. They're demanding that their internal users and their partners and contractors be able to access these things. Purchasing applications would be another example of this. And in the case of challenge No. two, the exposition of these applications is almost always, but not absolutely, over a Web interface.

- ✓ **Authentication challenge #3: Universal device access and what that really means**

The customers really are asking for two different things when they say this, and they're two distinct things. The first is that they want access from unmanaged PCs or Macs, which is readily achievable today, but it limits your hardware-based authentication options. The other thing we're seeing in terms of universal device access being demanded by lines of business and users, is that access from Internet capable devices. So, the idea that we can access anything we want to from our mobile phone. For example an iPhone or a Blackberry or other such device. It's not typically possible, not because of authentication concerns, but because of the issue of modifying the application to interface. And so to make it usable, frequently things need to be done, for example, writing a skin for the application so that it can be exposed. Let's talk about some of the authentication methods that are available here.

Authentication method recommendations

I'd like to move to some recommendations right now. And of course I'll start with the assessed risk recommendation and it sounds like analyst's platitude I know, but it's something that absolutely essential. So, when you're looking at your applications, you need to match the authentication mechanism to the level of risk, user constituency and application protocol

and cost. So you need to measure all of those things. And what you certainly don't want to do is build a $10,000 barn for a $5,000 horse. You don't want to build a security solution that is more expensive than the cost of FROG for example. Some other recommendations, watch for

technological improvements. In this new world, things are going to be getting better, in particular transactional analytics. Expect, as we said, some industry-specific vertical solutions that will come out and help in that space. Also, with OTP's on a mobile device, the platform support is improving over time, and the distribution and binding mechanisms.
Distribution being getting the OTP out to the user, binding being, being able to associate the OTP with the user in an application. Those are continually improving and they must improve and it's logical that they will continue to improve. It's such a valuable technology because again we all carry mobile devices now and so if we can do this in a secure way, this makes a lot of sense.

next recommendations, layer for warmth. As we talked before, there's no single authentication mechanism that's bullet proof; they all have deficiencies. So, if you layer these technologies you get a higher level of identity assurance. We see this frequently as a best practice across many organizations. So for example, you may want to do an OTP-based SMS kind of thing when you set up a device identification. So it's an initial way to do some good identify proofing, that will enable you to be able to set up a good device identification moving forward. Another one would be the example I gave before which is in a case of using transactional analytics in an active modality, you may want to, as the user gets stocked, do an out of band telephone mechanism. That would enable you to validate that the transaction is authorized before they move forward. There's good cost reduction there because you don't have to have the fraud department follow up in a separate instance and chase the user down.

Finally, mix and match technologies. What we've seen for large enterprises is that there's no single one technology that will work, no primary mechanism that will work across the board. So expect to have multiple authentication mechanisms even to the same application based on your user constituencies. It's just going to be that way. It's going to be difficult to do that. So just have that expectation. Finally, our last slide on recommendations, look for easy integration points. So, one example might be radius aware applications. You can bolt a variety of different OTP technologies underneath that. So things like Web applications, VPM, they can leverage these authentication techniques without you having to go through an application development life cycle to make it work.

Another one would be key strokes dynamics authentication. Again that's typing stuff. What we've seen is that these applications integrate pretty well if your application for example, can consume a [SAML] insertion, or a Web-access management cookie. So for example, if you're running Siteminder or Tivoli Access Manager for e-business, these keystroke dynamics products will do the authentication for you and then they issue a cookie so that the user is properly authenticated, and you don't need to modify your Web access management application to make that work. Other things to take a look at are transitional analytics and device identification. These products in the consumer authentication suite are beginning to be integrated with Web-access management systems. So, one of the problems that you have if these things aren't integrated from WAM systems to transitional analytics, is that you have the problem with two police officers being out there, two authorizations police officers. So you need to have systems, transitional, analytic and Web access management systems that are harmonized from an authorization perspective.

Authentication and authorization processes Example

Take the example of an online banking system - where, after logging in, the user can perform certain operations during an active session. When the session expires, the user loses their rights until the next correct login.

What happens inside

During the session, **inside the online banking system**, the user may perform a number of operations such as:

- preview balance,
- review transaction history,
- review personal data,
- edit personal data,
- declare trusted recipients,
- define new transfer.

Some of these operations require additional activity from the user to certify their identity within the session after logging in. In online banking, authorization may be carried out in various ways:

- SMS codes,
- hardware token,
- one-time password list,
- OTP (OCRA) one-time code generator,
- mobile token.

When a user wants to perform an operation that is considered critical (especially important and risk-prone), the system may ask the user to rewrite the authorization code generated in response to the server's request. Most often this code is sent to the user via a separate channel (SMS), or generated on an external device (e.g. OTP token).

Data verification

After the code is rewritten and the order accepted, the data together with the signature is sent to the server. The **data is verified on the server**. If it is correct and the system decides it has not been forged, the operation is sent for execution.

The above scenario aims at ensuring that it's the **user who originates the transfer** – as they know the authorization code which was sent to them via a predefined, separate channel (e.g. via SMS). Such a division makes it difficult for a criminal to carry out an attack on the basis of knowing of the user authorization data which is relatively easy to obtain.

Self-Check 3:

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. write those challenges on authentication

   _____
   _____
   _____

2. write the recommendation given for these challenges

   _____
   _____
   _____

Note: **Satisfactory rating 100%**

You can ask you teacher for the copy of the correct answers.

Answer Sheet

Score = _____
Rating: _____

Name: _____ Date: _____

L G# 7 LO #4- Determine network security

Instruction sheet

This learning guide is developed to provide you the necessary information regarding the following content coverage and topics:

- Sharing resources access via a network
- Monitoring and recording Security threats
- Updating the latest antivirus signatures

This guide will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Sharing resources access via a network
- Monitoring and recording Security threats
- Updating the latest antivirus signatures

Read the specific objectives of this Learning Guide.

1. Follow the instructions described below.
2. Read the information written in the “Information Sheets”. Try to understand what are being discussed. Ask your trainer for assistance if you have hard time understanding them.
3. Accomplish the “Self-checks” which are placed following all information sheets.
4. Ask from your trainer the key to correction (key answers) or you can request your trainer to correct your work. (You are to get the key answer only after you finished answering the Self-checks).

Information Sheet 4.1: Sharing resources access via a network

4.1.1. Sharing resource access

In computing, a **shared resource**, or **network share**, is a computer resource made available from one host to other hosts on a computer network. It is a device or piece of information on a computer that can be remotely accessed from another computer transparently as if it were a resource in the local machine. Network sharing is made possible by inter-process communication over the network.

Some examples of shareable resources are computer programs, data, storage devices, and printers. E.g. shared file access (also known as disk sharing and folder sharing), shared printer access, shared scanner access, etc. The shared resource is called a shared disk, shared folder or shared document.

The term file sharing traditionally means shared file access, especially in the context of operating systems and LAN and Intranet services, for example in Microsoft Windows documentation. Though, as BitTorrent and similar applications became available in the early 2000s, the term file sharing increasingly has become associated with peer-to-peer file sharing over the Internet.

Common file systems and protocols

shared file and printer access require an operating system on the client that supports access to resources on a server, an operating system on the server that supports access to its resources from a client, and an application layer (in the four or five layer TCP/IP reference model) file sharing protocol and transport layer protocol to provide that shared access. Modern operating systems for personal computers include distributed file systems that support file sharing, while hand-held computing devices sometimes require additional software for shared file access.

The most common file systems and protocols are:

Primary operating system	Application protocol	Transport protocol
Mac OS	SMB, Apple Filing Protocol[5]	• TCP, • UDP or • AppleTalk
Unix-like systems	Network File System (NFS), SMB	• TCP or • UDP
MS-DOS, Windows	SMB, also known as CIFS	• TCP, • NBT (includes UDP), • NBF, or • other NetBIOS transports
Novell NetWare (server) MS-DOS, Windows (client)	• NCP and • SAP	• SPX (over IPX), or • TCP

Self-Check 1

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. The Transport protocol work with mac Os is:
   A. TCP
   B. UDP
   C. Apple talk
   D. All
2. The Transport protocol work with MS-DOS, Windows is:
   A. TCP
   B. NBT
   C. NBF
   D. All
3. The Transport protocol work with Unix-like systems is:
   A. TCP
   B. UDP
   C. All

Note: **Satisfactory rating 100%**

You can ask you teacher for the copy of the correct answers.

Answer Sheet

Score = _____
Rating: _____

Name: _____

Information Sheet 4.2: Monitoring and recording Security threats

4.2.1. Managing security threats

The "primary operating system" is the operating system on which the file sharing protocol in question is most commonly used.

On Microsoft Windows, a network share is provided by the Windows network component "File and Printer Sharing for Microsoft Networks", using Microsoft's SMB (Server Message Block) protocol. Other operating systems might also implement that protocol.

Security issues

A network share can become a security liability when access to the shared files is gained (often by devious means) by those who should not have access to them. Many computer worms have spread through network shares. Network shares would consume extensive communication capacity in non-broadband network access. Because of that, shared printer and file access is normally prohibited in firewalls from computers outside the local area network or enterprise Intranet. However, by means of virtual private networks (VPN), shared resources can securely be made available for certified users outside the local network.

A network share is typically made accessible to other users by marking any folder or file as shared, or by changing the file system permissions or access rights in the properties of the folder. For example, a file or folder may be accessible only to one user (the owner), to system administrators, to a certain group of users to public, i.e. to all logged in users. The exact procedure varies by platform.

In operating system editions for homes and small offices, there may be a special pre-shared folder that is accessible to all users with a user account and password on the local computer. Network access to the pre-shared folder can be turned on.

Comparison to file transfer

Shared file access should not be confused with file transfer using the file transfer protocol (FTP), or the Bluetooth IRDA OBject EXchange (OBEX) protocol. Shared access involves automatic synchronization of folder information whenever a folder is changed on the

server, and may provide server side file searching, while file transfer is a more rudimentary service.

Shared file access is normally considered as a local area network (LAN) service, while FTP is an Internet service.

Comparison to file synchronization

Shared file access involves but should not be confused with file synchronization and other information synchronization. Internet-based information synchronization may, for example, use the SyncML language. Shared file access is based on server side pushing of folder information, and is normally used over an "always on" Internet socket. File synchronization allows the user to be offline from time to time, and is normally based on an agent software that polls synchronized machines at reconnect, and sometimes repeatedly with a certain time interval, to discover differences. Modern operating systems often include a local cache of remote files, allowing offline access and synchronization when reconnected.

4.2.2. Security threat monitoring

Threat monitoring refers to a type of solution or process dedicated to continuously monitoring across networks and/or endpoints for signs of security threats such as attempts at intrusions .

Threat monitoring gives technology professionals visibility into the network and the actions of the users who access it, enabling stronger data protection as well as preventing or lessening of the damages caused by breaches. Today companies employ independent contractors, remote workers, and staff who use their own devices for work, posing additional risk to the company’s data and sensitive information and driving the need for threat monitoring at enterprises.

Automated systems should support near real-time analysis and alerting of events (e.g., malicious code, potential intrusions) and integrate intrusion detection into access and flow control mechanisms.

Auditing and monitoring systems should support audit reduction and report generation. The information system should be able to automatically process audit records for events of

interest based on selectable criteria. Alerts should be generated for technical personnel to analyze and investigate suspicious activity or suspected violations.

Secure log-on procedures should be implemented that include:

- a warning notice;
- limits the number unsuccessful attempts;
- records the number of unsuccessful and successful attempts; and
- Does not display the password when being entered.

The **logon procedure** for the OS should minimize the opportunity for unauthorized access
by:

- Disclosing the minimum amount of information about the system;
- limiting the number of unsuccessful logon attempts to three (3) and enforcing the disconnect of the data link connections;
- sending an alarm to the system console;
- setting the number of password retries commensurate with the minimum length of the password and value of the information protected;
- limiting the maximum and minimum time allowed for the log-on procedure;
- not transmitting passwords in clear text over the network;
- not displaying system or application identifiers until the logon process is successfully completed;
- not proving help messages during the procedure;
- validating the long-on information only on completion of all input data; and
- Not indicating which part of the logon was incorrect if an error condition arises.

Network Logging Parameters:

- Account Logon – Success and Failure Auditing
- Account Management – Success and Failure Auditing
- Directory Service Access – Failure Auditing
- Logon Events – Success and Failure Auditing
- Object Access – Success and Failure Auditing

- Policy Change – Success and Failure Auditing
- Privilege Use – Success and Failure Auditing
- Process Tracking – Failure Auditing
- System Events – Success and Failure Auditing

A **System Log (or SysLog) server** should be implemented that can collect all the audit logs from different sources such as internal servers and routers. The SysLog server will aggregate information and produce reports to show suspicious activity or behavior. The SysLog will allow write access from different sources, but read-only access to workforce members to view to prevent any unauthorized manipulation of event logs.

Self-Check 2

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. Secure log-on procedures should be implemented that include:
   A. a warning notice;
   B. limits the number unsuccessful attempts;
   C. records the number of unsuccessful and successful attempts
   D. all
2. _____ collects all the audit logs from different sources such as internal servers and routers.
   A. System Log (or SysLog) server
   B. Secure log
   C. Security issues
   D. All
3. _____refers to a type of solution or process dedicated to continuously monitoring across networks
   A. Threat monitoring
   B. Virus scanning
   C. all

Note: **Satisfactory rating 100%**

You can ask you teacher for the copy of the correct answers.

Answer Sheet

Score = _____
Rating: _____

Name:

Information Sheet 4.3: Updating the latest antivirus signatures

4.3.1. Virus signature

A **virus signature** is the fingerprint of a virus. It is a set of unique data, or bits of code, that allow it to be identified. Antivirus software uses a virus signature to find a virus in a computer file system, allowing detecting, quarantine, and removing the virus. In the antivirus software, the virus signature is referred to as a definition file or DAT file.

Multiple viruses may have the same virus signature, which allows antivirus programs to detect multiple viruses when looking for a single virus signature. Because of this sharing of the same virus signature between multiple viruses, antivirus programs can sometimes detect a virus that is not even known yet. New viruses have a virus signature that are not used by other viruses, but new "strains" of known virus sometimes use the same virus signature as earlier strains.

Antivirus software performs frequent virus signature, or definition, updates. These updates are necessary for the software to detect and remove new viruses. New viruses are being created and released almost daily, which forces antivirus software to need frequent updates.

4.3.2 Updating antivirus signature

To be truly victorious, you must be vigilant in keeping up with antivirus updates. Being current is analogous to keeping supplies and ammunition available at the front lines of a battle. In order to maintain an effective fighting force, an organization must perform four key steps:

1. Retrieval
2. Testing
3. Deployment
4. Monitoring

1. Retrieval

The first and most easily neglected step in managing your multilayer antivirus defense is the timely and consistent retrieval of antivirus signature updates.

Most signature updates are obtained by accessing the FTP site of the antivirus vendor and pulling down the latest update. This process must be automated (and many virus software packages have built-in automation features). Failure to automate will result in updates being skipped simply due to forgetfulness, carelessness, and absenteeism (your holidays).

Gone are the days when updates were merely issued monthly and you had plenty of time to deal with each release. Today, the updates are weekly—if not daily. Having but one automated method of retrieving updates is good but not as good as it can or should be. A fallback or alternate method is also important.

Many FTP sites become overly busy during peak periods and access is then restricted. If your scheduled update is for a time that coincides with a busy period, you may not be getting your updates as regularly as anticipated. I recommend having a backup system, such as the old-fashioned dial-up access for retrieving updates. Not only does it provide a level of redundancy, it can also act as a safety check regarding a signature update.

2. Testing

Having successfully obtained that latest signature update, you should test it before general deployment throughout your organization.

3. Deployment

Deployment is clearly the most crucial phase. Assuming that testing hasn't revealed any major glitches, it is time to automatically roll out the software to the server and client layers. In a large organization, it's not feasible to have all of your client machines pick up their updates from one central location. This would simply saturate your available bandwidth and introduce unnecessary delays for clients.

We have set up our system so that clients always pick up their updates from a server that is local to them. In the background, a master server distributes the tested update to various distribution servers. This process runs at night, when WAN utilization is at its lowest.

4. Monitoring

one phase that is easily forgotten involves monitoring the antivirus health of your environment. You need to monitor whether all your connected computers have the latest software, whether they're at the latest signature level, whether someone has intentionally or inadvertently disabled the "real-time" monitoring, and so on.

Today, many antivirus solutions offer tools for monitoring the state of your antivirus environment, and I would insist on this functionality before purchasing any new product. If you have an existing system without such functionality, you should either consider switching products or write some custom code to capture the pertinent information from your systems as they connect to the network. This won't be a trivial task, so it might be better to simply buy a new antivirus software package.

Self-Check 3

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. _____is the fingerprint of a virus.
   A. virus signature
   B. Testing
   C. Retrieval
   D. All
2. _____ performs frequent virus signature, or definition, updates.
   A. Antivirus software
   B. Monitoring
   C. Virus signature
   D. all

Note: **Satisfactory rating 100%**

You can ask you teacher for the copy of the correct answers.

Score = _____
Rating: _____

Answer Sheet

Name:

Reference

- Network Administration with FreeBSD 7
  (Author Babak Farrokhi)
- Windows NT TCP IP Network Administration
  (Author Craig Hunt
- Analytical Network and System Administration: Managing Human-Computer Systems
  (Author Mark Burgess)
- UNIX Administration: A Comprehensive Sourcebook for Effective Systems & Network Management
  (Author Bozidar Levi)
- Security+ Guide to Network Security Fundamentals, 3rd Edition
  (Author Mark Ciampa)
- Padlipsky, Michael A. (September 1982). A Perspective on the ARPANET Reference Model. IETF. doi:10.17487/RFC0871. RFC 871. Retrieved 15 December 2013.
- ^ Jump up to:a b Walden, David C. (July 1970). A Note on Interprocess in a Resource Sharing Computer Network. IETF. doi:10.17487/RFC0061. RFC 61. Retrieved 15 December 2013.
- ^ Walden, David C. (August 1970). A System for Interprocess Communication in a Resource Sharing Computer Network. IETF. doi:10.17487/RFC0062. RFC 62. Retrieved 15 December 2013.

Acknowledgement

Federal TVET Agency and Oromia TVET Bureau wishes to extend thanks and appreciation to the many representatives of TVET Instructors who donated their time and expertise to the development of this Model Curriculum and TTLM.

Institution name represented by the Trainer

No	Name the Trainer	College Name	Edu. Background	Address	
				Mob.	Email
1	Zerihun Abate	Sebeta Polytechnic College	Msc.	0911858358	zedoabata2017@gmail.com
2	Tsedale Mangiste	Dukem TVET College	Msc.	0912076643	tmmeng2005@gmail.com
3	Frew Atkilt	Bishoftu Polytechnic College	Msc.	0911787374	frew.frikii@gmail.com
4	Abebe Mintefa	Ambo TVET College	Msc.	0929352458	tolabula@gmail.com
5	Tewodiros Girma	Sheno TVET College	Msc.	0912068479	tedimutd@gmail.com

This curriculum was developed on **December 2020** at Bishoftu, Oromia

Answer Key for Module Title: Monitoring and Administer System and Network Security

LO #1 Ensure user accounts are controlled	
Self-Check 1	**Written Test**

Part 1: Choose the best answer

1. **B**
2. **A**
3. **A**

LO #1 Ensure user accounts are controlled	
Self-Check 2	**Written Test**

1.A

2. B

3. B

LO #1 Ensure user accounts are controlled	
Self-Check 3	**Written Test**

1. Ctr l+ Alt + Delete

2.

a. You can write a fancy script and execute it at the every logon

b. Configure legal notice using a group policy.

LO #1 Ensure user accounts are controlled	
Self-Check 4	**Written Test**

1.A

2. C

3. D

LO #1 Ensure user accounts are controlled	
Self-Check 5	**Written Test**

1.

- Software security settings.
- Minimum length of a password and expiry cycle for passwords.
- Issues that would be linked to user education include not having passwords displayed on sticky notes and not sharing passwords.
- Password retention

2.

5. What was expected to happen?
6. What actually occurred?
7. What went well and why?
8. What can be improved and how?

LO #1 Ensure user accounts are controlled	
Self-Check 6	**Written Test**

1. A
2. D

LO #2 Secure file and resource access	
Self-Check 1	**Written Test**

1. A
2. A
3. A

LO #2 Secure file and resource access	
Self-Check 2	**Written Test**

1. D
2. C
3. B

4.

LO #2 Secure file and resource access	
Self-Check 3	**Written Test**

1. D
2. C
3. B

LO #3 Determine authentication requirements	
Self-Check 1	**Written Test**

1. B
2. A
3. A

LO #3 Determine authentication requirements	
Self-Check 2	**Written Test**

1. C
2. A

LO #3 Determine authentication requirements	
Self-Check 3	**Written Test**

1.

- External users
- Increased exposure of high identity assurance applications over the Internet.
- Universal device access and what that really means

2. Recommendations

3.

LO #4 Determine network security	
Self-Check 1	**Written Test**

1. D
2. D
3. C

LO #4 Determine network security	
Self-Check 2	**Written Test**

1. D
2. A
3. A

LO #4 Determine network security	
Self-Check 3	**Written Test**

1. A
2. B

AKNOWLEDGEMENT

We wish to extend thanks and appreciation to the many representatives of TVET instructors who donated their time and expertise to the development of this TTLM.

We would like also to express our appreciation to Federal Technical and Vocational Education and Training Agency (FTVET), Oromia TVET Bureau, TVET College/ Institutes, who made the development of this TTLM with required standards and quality possible.

This TTLM is developed on December 2020 at Bishoftu Bin International hotel.

The trainers who developed the TTLM

No	Name of Trainer	College Name	Edu. Background	Address	
				Mob.	Email
1	Abebe Mintefa	Ambo TVET College	MSc.	0929352458	tolabula@gmail.com
2	Frew Atkilt	Bishoftu Polytechnic College	MSc.	0911787374	frew.frikii@gmail.com
3	Tewodiros Girma	Sheno TVET College	MSc.	0912068479	tedimutd@gmail.com
4	Tsedale Mengiste	Dukem TVET College	MSc.	0912076643	tmmeng2005@gmail.com
5	Zerihun Abate	Sebeta Polytechnic College	MSc.	0911858358	zedoabata2017@gmail.com