የሥራና ክህሎት ሚኒስቴር
Ministry of Labor and Skills

Hardware and Network Servicing

Level-III

Based on November 2023, Curriculum Version - II

Module Title: - **Monitoring and Administering System and Network Security**

Module code: - **EIS HNS3 M04 1123**

Nominal duration: **30Hour**

Prepared by: Ministry of Labor and Skill

August, 2023

Addis Ababa, Ethiopia

Contents

Acknowledgment

The **Ministry of Labor and skill** wishes to thank and appreciation to MoLS leaders and experts, Regional Labor and skill/training Bureaus leader, experts, TVT College Deans, Instructors and industry experts who contribute their time and professional experience to the development of this Curriculum for **Hardware and Network service level III**.

Acronym

RBAC	Role-Based Access Control
MFA	Multi-Factor Authentication
IAM	Centralized Identity and Access Management
OS	Operating System
SIEM	Security Information and Event Management
DAC	Discretionary Access Control
MAC	Mandatory Access Control
DLP	Data Loss Prevention
ACL	Access Control Lists
NTFS	New Technology File System
EXT4	Fourth Extended File System
NFS	Network File Systems
SSO	Single Sign-On
MFA	Multi-Factor Authentication
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention Systems
VPS	Virtual Private Networks
SSL	Secure Sockets Layer
TLS	Transport Layer Security
RDS	Remote Desktop Services
IPP	Internet Printing Protocol
EDR	Endpoint Detection and Response

Introduction to the Module

This module provide you to obtain knowledges, skills and attitudes that required to monitor and administer security functions of a system in general.

This module covers the units:

- User Accounts
- File and Resource Access
- Authentication Requirements
- Network Security

Learning Objective of the Module:

- Modify default user settings
- Explain about inbuilt operating system security and accessing features
- Describe file security categorization scheme
- Determine security requirements
- Monitor and record Security threat
- Update the latest antivirus signatures

Module Instruction

For effective use this modules trainees are expected to follow the following module instruction:

1. Read the specific objectives of this Learning Guide.
2. Read the information that this module contain.
3. Complete the Self-check.
4. Submit your accomplished Self-check.
5. Do the Operations which in the module.
6. Do the LAP test in page (if you are ready) and show your output to your teacher.

Your teacher will assess your result either satisfactory or unsatisfactory. If unsatisfactory, your teacher shall advice you on additional work. But if satisfactory you can proceed to the next topic.

Unit One: User Accounts

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

- Modifying default user settings
- Displaying legal notices at logon
- Checking strength of passwords and complexity
- Reviewing password procedures
- Identifying security gaps

This unit will also support you to accomplish the learning outcomes stated in the cover page. Specifically, upon completion of this module, you will be able to:

- Modify default user settings
- Display legal notices at logon
- Check strength of passwords and complexity
- Review password procedures
- Identify security gaps

1. User Accounts

Overview of user account management

A user account defines the actions a user can perform in Windows. On a stand-alone computer or a computer that is a member of a workgroup, a user account establishes the privileges assigned to each user. On a computer that is part of a network domain, a user must be a member of at least one group. The permissions and rights granted to a group are assigned to its members.

User Account Provisioning: Implement a formal process for user account provisioning. This process should include verifying the user's identity, determining the appropriate level of access based on their role and responsibilities, and creating user accounts with strong passwords or passphrase.

User Account Reviews: Conduct regular reviews of user accounts to ensure they are still required and have appropriate access privileges. This includes reviewing user roles, access levels, and permissions. Remove or modify access for users who no longer require it.

By implementing these and some others control measures, you can effectively manage user accounts and reduce the risk of unauthorized access, data breaches, and insider threats. Regularly review and update your account management processes to adapt to changing security requirements and industry best practices.

1.1.Modifying default user setting

Modifying default user settings is an important step in enhancing system and network security. Default settings often have known vulnerabilities or may not align with your organization's security requirements. Here are some considerations for modifying default user settings:

Operating System Configuration: Review and modify default settings on the operating system (OS) level. This includes disabling unnecessary services, closing unused ports, and enabling security features such as firewalls. This is practically performed on operation sheet 1.1

User Permissions: Adjust default user permissions to follow the principle of least privilege. Limit the abilities of users to install software, modify system settings, or access sensitive files unless necessary for their work. Regular user accounts should not have administrative privileges by default.

Password Policies: Modify default password policies to enforce stronger password requirements. Set minimum length, complexity, and expiration rules that align with best practices. Discourage the use of default or easily guessable passwords.

Application Configuration: Configure default settings in applications to enhance security. This may involve disabling or securing unnecessary features, enabling encryption options, and configuring access controls within applications.

Network Device Settings: Modify default settings on network devices such as routers, switches, and firewalls. Change default passwords and usernames, disable unnecessary services or ports, and apply security patches and firmware updates regularly.

Web Browser Configurations: Adjust default settings in web browsers to enhance security. Enable pop-up blockers, disable or restrict plugins and extensions, and configure privacy and security settings to provide the appropriate level of protection.

Regularly review and update the modified settings as new security threats emerge or as your organization's security requirements evolve. Stay informed about security best practices and consult relevant security guidelines and recommendations provided by software vendors and security organizations.

1.2.Displaying legal notices at logon

Displaying legal notices at logon is a common practice used by organizations to communicate important information, policies, or legal disclaimers to users before they log into a system or network. These notices can serve various purposes, such as informing users of acceptable use policies, confidentiality agreements, or warnings about unauthorized access.

To display legal notices at logon, follow these general steps:

Determine the content: Clearly define the content of the legal notice. It should be concise, informative, and aligned with your organization's policies and legal requirements. Consult with legal and compliance teams to ensure accuracy and appropriateness.

Identify the target audience: Determine which user groups or individuals should see the legal notice. It may be applicable to all users or specific groups based on their roles or access privileges.

Test and deploy: After configuring the legal notice, test it in a controlled environment to ensure it is displayed correctly and is readable. Once validated, deploy the changes to the production environment.

Regularly review and update: Periodically review the content of the legal notice to ensure it remains accurate and relevant. Update it as necessary to reflect any changes in policies, regulations, or legal requirements.

It's important to note that while legal notices can help communicate important information, they should not replace user awareness and training programs. Users should receive proper education and understanding of the policies and agreements mentioned in the legal notice.

1.3.Checking strength of passwords and complexity

Checking the strength and complexity of passwords is an essential practice to ensure that users create strong and secure passwords. By enforcing password strength requirements, you can significantly reduce the risk of password-related vulnerabilities. Here are some key factors to consider when checking password strength and complexity:

Password Strength Criteria:

1. **Length:**
   - A longer password is generally stronger. Aim for a minimum of 12 characters.
   - Passphrases (a sequence of words or a sentence) can be a good alternative for increased length and memorability.
2. **Complexity:**
   - Include a mix of uppercase and lowercase letters.
   - Use numbers and special characters.

- Avoid using easily guessable patterns (e.g., "password123" or "qwerty").

3. **Unpredictability:**
    - Avoid using easily guessable information, such as names, birthdays, or common words.
    - Do not use easily accessible personal information.
4. **Avoiding Common Words:**
    - Avoid using dictionary words or common phrases.
    - Consider misspellings or substitutions.
5. **Avoiding Reuse:**
    - Avoid using the same password across multiple accounts.
    - Regularly update passwords and avoid using previously compromised passwords.

Tools for Checking Password Strength:

1. **Password Strength Meters:**
    - Many websites and applications provide password strength meters during the password creation process.
    - These meters often assess length, complexity, and commonality with known passwords.
2. **Password Managers:**
    - Password managers often include features to generate and assess password strength.
    - They can analyze existing passwords and suggest improvements.

Recommendations for Improving Password Strength:

1. **Use Passphrases**
    - Create long and memorable passphrases.
    - Combine unrelated words or use a sentence.
2. **Avoid Personal Information:**
    - Avoid using easily discoverable personal information (names, birthdays, etc.).
3. **Regularly Update Passwords:**
    - Encourage users to change passwords periodically.

4. **Multi-Factor Authentication (MFA):**
    - Implement multi-factor authentication to add an extra layer of security.
5. **Education and Policies:**
    - Educate users about the importance of strong passwords.
    - Implement and enforce password policies within your organization.

Remember that while strong passwords are essential, they are just one part of a comprehensive security strategy. Regularly review and update security policies to adapt to evolving threats. Additionally, consider implementing other security measures such as account lockout policies and monitoring for unusual login activity.

1.4.Reviewing password procedures

Reviewing password procedures is a critical aspect of maintaining strong cybersecurity practices within an organization. Passwords serve as a primary defense against unauthorized access, and ensuring that password procedures are robust is essential for protecting sensitive information. Here's a comprehensive checklist for reviewing and improving password procedures:

Password Creation Guidelines:

- **Length and Complexity:** Ensure that passwords meet minimum length and complexity requirements (uppercase, lowercase, numbers, and special characters).
- **Avoid Common Patterns:** Discourage the use of easily guessable patterns, such as "password123" or sequential characters (e.g., "abcd" or "1234").

Password Storage and Transmission:

- **Hashing and Encryption:** Implement strong hashing and encryption algorithms for storing and transmitting passwords.
- **Avoiding Plain Text:** Never store passwords in plain text; use secure methods like hashing with salt.

Authentication Policies:

- **Multi-Factor Authentication (MFA):** Encourage or mandate the use of MFA to enhance security.
- **Account Lockout Policies:** Implement account lockout policies to prevent brute-force attacks.

Password Recovery Procedures:

- **Secure Methods:** Ensure that password recovery processes are secure and do not compromise user accounts.
- **Alternate Authentication:** Use alternate methods (e.g., email verification, security questions) for password recovery.

User Education and Training:

- **Security Awareness:** Conduct regular training sessions to educate users about the importance of strong passwords and the risks associated with weak ones.
- **Phishing Awareness:** Train users to recognize and avoid phishing attempts that may compromise their passwords.

Third-Party Services:

- **Vendor Policies:** If using third-party services that involve user authentication, review and ensure alignment with their password security practices.

Response to Security Incidents:

- **Incident Response Plan:** Have a well-defined incident response plan in place in case of a security incident related to compromise passwords.

Regularly reviewing and updating password procedures is crucial to adapting to evolving threats and maintaining a strong security posture. Additionally, consider conducting periodic security assessments and involving security professionals to identify and address potential vulnerabilities.

1.5.Identifying security gaps

Identifying security gaps is a crucial aspect of maintaining a robust cybersecurity posture. Security gaps can be vulnerabilities, weaknesses, or areas of non-compliance that could be exploited by attackers. Here are steps to help you identify security gaps within your organization:

Conduct Regular Security Audits:

- Perform comprehensive security audits to assess the overall security posture.
- Evaluate network configurations, access controls, and adherence to security policies.

Vulnerability Assessments:

- Regularly conduct vulnerability assessments using tools that scan systems and networks for known vulnerabilities.
- Prioritize and address high-risk vulnerabilities promptly.

Review Access Controls:

- Audit user accounts and access permissions regularly.
- Ensure that the principle of least privilege is followed, and users only have the necessary access for their roles.

Network Security Analysis:

- Analyze network traffic to identify anomalies or signs of unauthorized access
- Review firewall configurations and ensure that they effectively control incoming and outgoing traffic.

Continuous Monitoring:

- Implement continuous monitoring solutions to respond to security events in real time.
- Use intrusion detection systems and security information and event management (SIEM).

Document and Prioritize Findings:

- Document all identified security gaps and vulnerabilities.
- Prioritize remediation efforts based on the severity and potential impact.

Regularly reassess and update your security strategy as the threat landscape evolves. Continuous improvement is key to staying ahead of potential security threats and minimizing the risk of security gaps.

Self-check test-1

Instruction: You are required to perform the following questions individually.

I. Write true if the questions are correct and write false if the questions are incorrect.

1. Password policies enforce users that require to create complex passwords or passphrases.
2. A user account defines the actions a user can perform in Windows.
3. Never store passwords in plain text; use secure methods like hashing with salt.
4. Password managers often include features to generate and assess password strength.

II. Choose the best answer from the questions listed below.

1. User Account Provisioning process should include_______________

   A. Verify user's identity
   B. Role and responsibilities
   C. Level of access
   D. All

2. Account monitoring checking user account activities for any signs of __________

   A. Unauthorized access
   B. Multiple failed login attempts
   C. Unusual login patterns or
   D. All

3. Operating system configuration modifying default settings on the operating system level, this include________________

   A. Unnecessary services
   B. Enabling security features
   C. Closing unused ports
   D. All

4. ____________have a well-defined event reaction plan in place in case of a security incident related to compromise passwords.

   A. Incident Response Plan
   B. Alternate Authentication
   C. Third-Party Services
   D. Password Change Policies

III. Matching the following from column "A" into column "B"

A	B
1. Multi-Factor Authentication	A. Use Passphrases
2. Hashing and Encryption	B. Prevent brute-force attacks.
3. Account Lockout Policies	C. For storing and transmitting passwords.
4. References for Password Strength	D. Implement for sensitive data.

IV. List and Fill in the blank space for the following questions.

1. List the password creation guidelines
2. List the authentication policies for reviewing password procedures
3. What are the recommendations for Improving Password Strength?
4. List some of the steps security gaps within your system and network security?

Operation Sheet 1.1

1. Modifying default user settings

Task 1: Modifying Default User Profile (Windows 10):

1. Log in as an administrator.
2. Customize the user settings you want to apply to new users.
3. Open the File Explorer and navigate to C:\Users. Locate the default user profile folder (usually named Default).
4. Copy the customized user profile to the Default folder, replacing existing files. Ensure you copy all necessary settings and configurations.
5. Changes to the default user profile will apply to new users when they log in for the first time.

Task 2: Group Policy Active Directory (Windows Server):

1. Open the Group Policy Management Console (GPMC) on a domain controller.
2. Create or modify a Group Policy Object (GPO) linked to the relevant Organizational Unit (OU).
3. Navigate to Computer Configuration -> Policies -> Administrative Templates -> System/User Profiles.
4. Enable the setting "Set roaming profile path for all users logging onto this computer" or similar, and specify the profile path.
5. Changes to the GPO will apply to new users in the specified OU.

2. Displaying legal notices at logon

Task 1: Windows: Using Group Policy:

1. Open the Group Policy Management Console (GPMC) on a Windows computer.
2. Navigate to **Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options**.
3. Look for the policy named "Interactive logon: Message text for users attempting to log on" and set the desired message text.
4. Similarly, set the message title using "Interactive logon: Message title for users attempting to log on."
   Note: Ensure that you are modifying the appropriate Group Policy Object (GPO) and test the changes in a controlled environment.

Task 2: Registry Edit (Alternative):

1. Open the Registry Editor (**regedit**) as an administrator.
2. Navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**.
3. Create a new String Value named **LegalNoticeCaption** for the title and **LegalNoticeText** for the message.
4. Set the desired text and title for the legal notice.

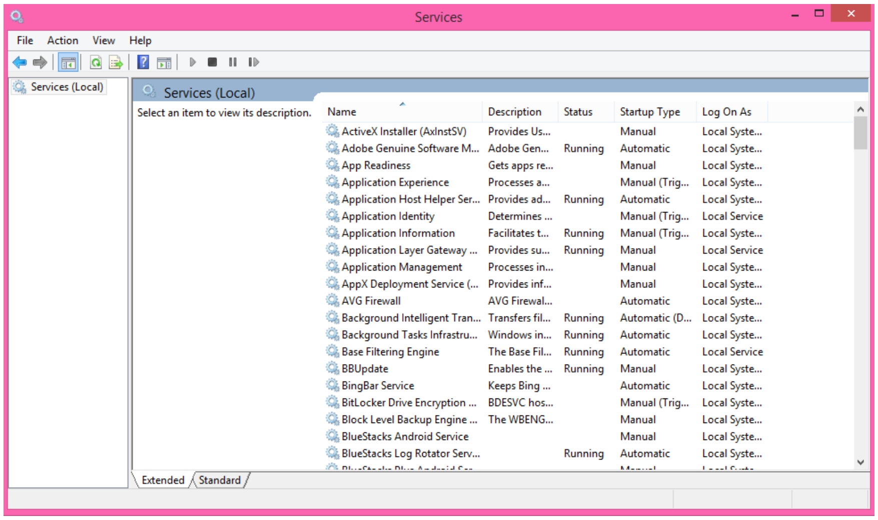
Operation Sheet 1.2

1. Operating System Configuration (Windows 10):

Task 1: Disabling or stop unnecessary services

As with all versions of windows, working in the background are services. While some of them are vital to smooth running, quite a few aren't for day-to-day use. If you disable these services, you can speed up your windows. Performing this follow the steps:

1. Click the Start Menu
2. Type **services.msc** into the search field
3. Open the Services app
4. Find a service you want to disable, and double click
5. Click stop



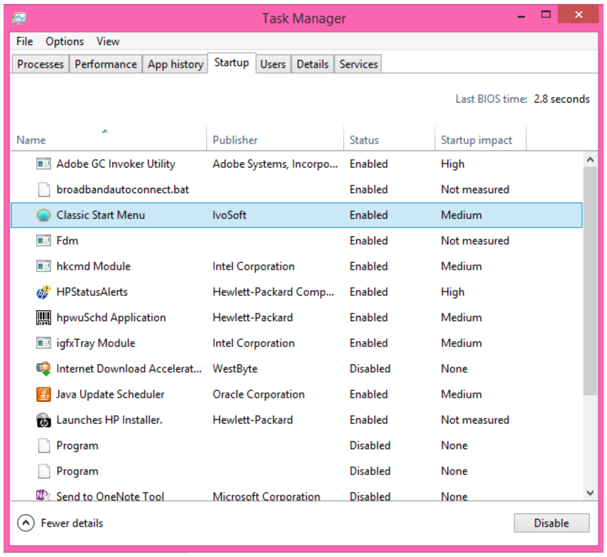
Select an item to view its description.

Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides Us...		Manual	Local Syste...
Adobe Genuine Software M...	Adobe Gen...	Running	Automatic	Local Syste...
App Readiness	Gets apps re...		Manual	Local Syste...
Application Experience	Processes a...		Manual (Trig...	Local Syste...
Application Host Helper Ser...	Provides ad...	Running	Automatic	Local Syste...
Application Identity	Determines ...		Manual (Trig...	Local Service
Application Information	Facilitates t...	Running	Manual (Trig...	Local Syste...
Application Layer Gateway ...	Provides su...	Running	Manual	Local Service
Application Management	Processes in...		Manual	Local Syste...
AppX Deployment Service (...	Provides inf...		Manual	Local Syste...
AVG Firewall	AVG Firewal...		Automatic	Local Syste...
Background Intelligent Tran...	Transfers fil...	Running	Automatic (D...	Local Syste...
Background Tasks Infrastru...	Windows in...	Running	Automatic	Local Syste...
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Service
BBUpdate	Enables the ...	Running	Manual	Local Syste...
BingBar Service	Keeps Bing ...		Automatic	Local Syste...
BitLocker Drive Encryption ...	BDESVC hos...		Manual (Trig...	Local Syste...
Block Level Backup Engine ...	The WBENG...		Manual	Local Syste...
BlueStacks Android Service			Manual	Local Syste...
BlueStacks Log Rotator Serv...		Running	Automatic	Local Syste...

Task 2: Disable startup programs in Windows 10

Virtually every version of Windows allows you to disable startup items, and Windows 10 is no exception. Stopping some programs from starting up will speed up the OS. To find this option follow the steps below:

1. Right click the Taskbar
2. Click Task Manager
3. Click 'More Details'
4. Click the Startup tab
5. Find a program you don't want to load at startup
6. Right click and click Disable



Last BIOS time: 2.8 seconds

Name	Publisher	Status	Startup impact
Adobe GC Invoker Utility	Adobe Systems, Incorpo...	Enabled	High
broadbandautoconnect.bat		Enabled	Not measured
Classic Start Menu	IvoSoft	Enabled	Medium
Fdm		Enabled	Not measured
hkcmd Module	Intel Corporation	Enabled	Medium
HPStatusAlerts	Hewlett-Packard Comp...	Enabled	High
hpwuSchd Application	Hewlett-Packard	Enabled	Medium
igfxTray Module	Intel Corporation	Enabled	Medium
Internet Download Accelerat...	WestByte	Disabled	None
Java Update Scheduler	Oracle Corporation	Enabled	Medium
Launches HP Installer.	Hewlett-Packard	Enabled	Not measured
Program		Disabled	None
Program		Disabled	None
Send to OneNote Tool	Microsoft Corporation	Disabled	None

2. Access and Check the Windows Server Firewall Settings

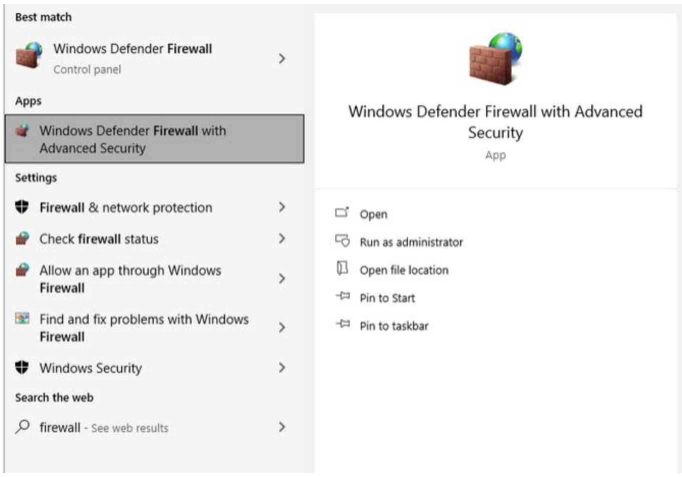
Managing your network traffic is essential in securing any device that handles your workloads. One of the primary tools in doing so is a firewall. The Windows operating system (OS) comes prepackaged with the Windows Defender Firewall to assist with this task.

Note: We have performing the following practice on windows server 2008 and above, to access and check the Firewall Settings but, the procedures are almost the same if we will practice to enable and change Firewall Ports in windows operating system.

Task 1: Access the Windows Firewall Management Console

1. Log into your server via Remote Desktop.
2. Click the **Search** icon on the bottom-left of the taskbar and type **firewall**.

3. Click on **Windows Defender Firewall with Advanced Security**. This action opens the Windows Firewall Management Console.



Best match

Windows Defender Firewall
Control panel

Apps

Windows Defender Firewall with Advanced Security

Settings

Firewall & network protection

Check firewall status

Allow an app through Windows Firewall

Find and fix problems with Windows Firewall

Windows Security

Search the web

firewall - See web results

Windows Defender Firewall with Advanced Security
App

Open

Run as administrator

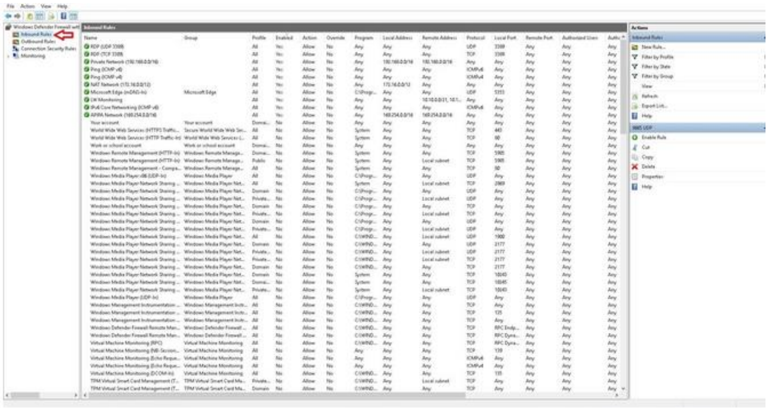
Open file location

Pin to Start

Pin to taskbar

Task 2: View and Configure Inbound Rules in the Console

1. From the left-hand navigation, click **Inbound Rules** to expose the Inbound Rules pane on the right.



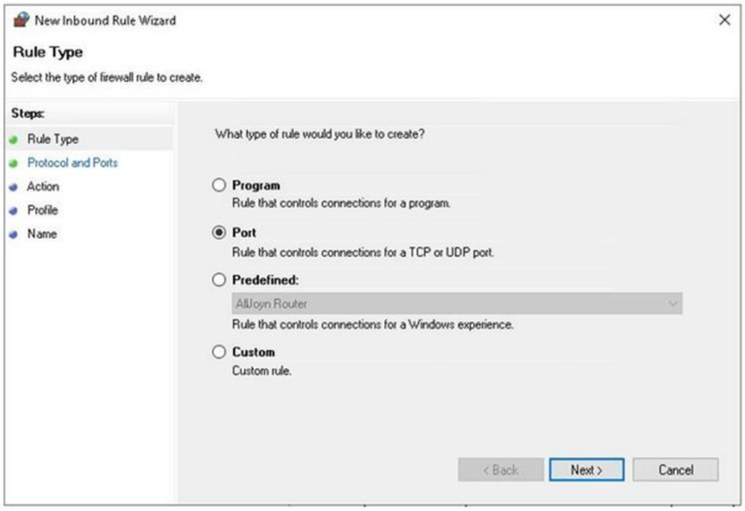
2. Click the **Enabled** column at the top to sort your rules by status until the value of Yes is at the top. Make a note of the preconfigured rules.

   Note: The rules created by Liquid Web allow access to your server. Disabling or editing these rules could cause network disruptions or prevent support from assisting you.

Task 3: Open a Port in Windows Server Firewall

1. Open the firewall manager again.
2. Click **Inbound Rules** from the left pane to reveal the Inbound Rules pane on the right.
3. Click **New Rule** in the right-hand pane to open the New Inbound Rule Wizard.

4. In the New Inbound Rule Wizard, under the Rule Type section, select the Port radio button and click **next**.



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

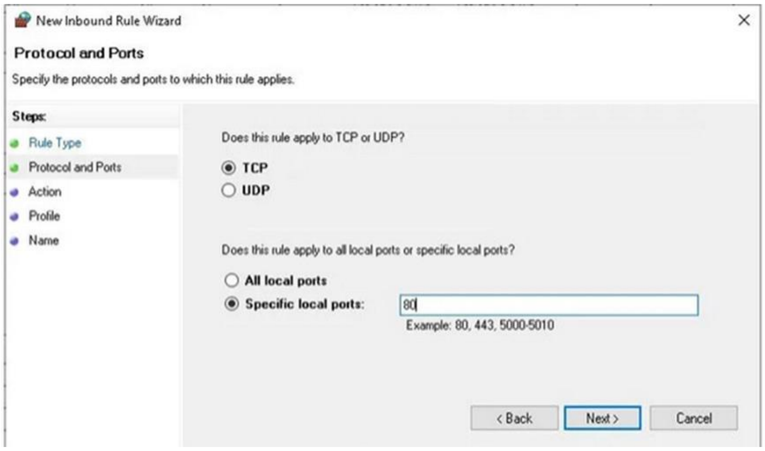
○ **Program**
Rule that controls connections for a program.

● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

5. In the Protocol and Ports section, select TCP or UDP. Next, select the radio button for all local ports or Specific local ports. For this tutorial, choose Specific local ports and enter the corresponding port number. If listing multiple ports, split them with a comma. Once completed, click **next**.



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

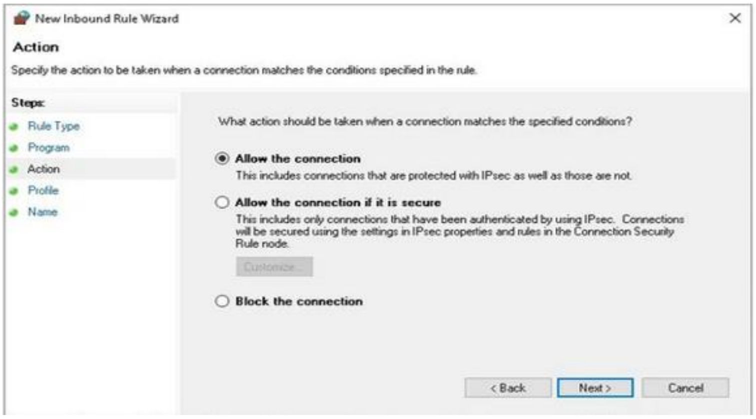
Does this rule apply to TCP or UDP?

● **TCP**
○ **UDP**

Does this rule apply to all local ports or specific local ports?

○ **All local ports**
● **Specific local ports:** 80
Example: 80, 443, 5000-5010

6. In the Action section, select **Allow the connection** (or choose the setting for your requirements) and click **Next**.



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:
- Rule Type
- Program
- Action
- Profile
- Name

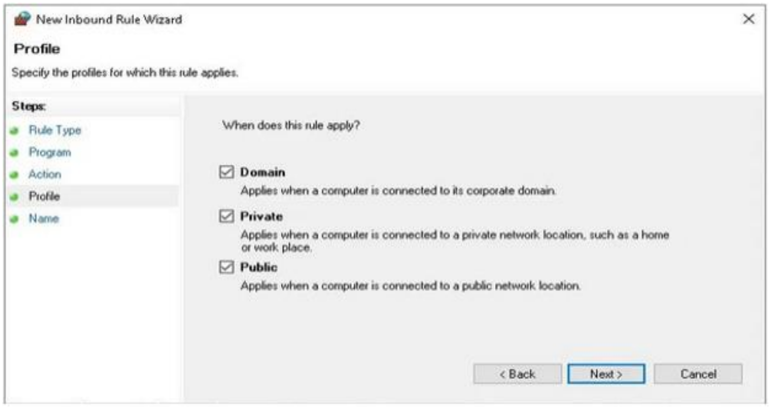
What action should be taken when a connection matches the specified conditions?

● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **Block the connection**

7. In the Profile section, select all appropriate profiles for when this rule applies and click **next**.



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:
- Rule Type
- Program
- Action
- Profile
- Name

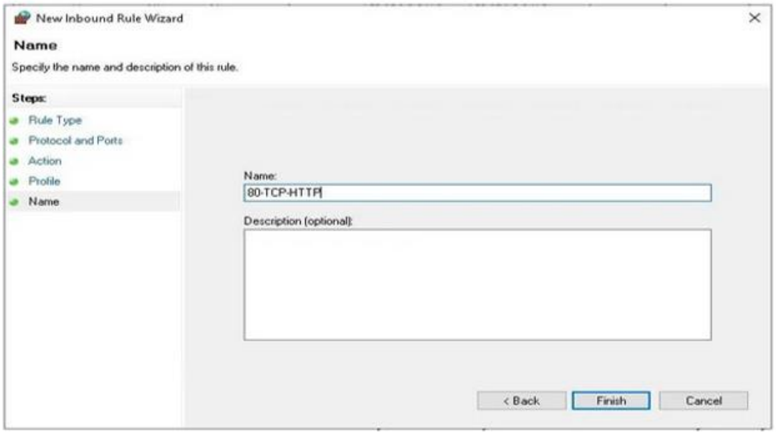
When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**
Applies when a computer is connected to a public network location.

8. Finally, give your new rule a descriptive name so that it is easy to find later, and click **Finish**.



New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Name: 80-TCP-HTTP

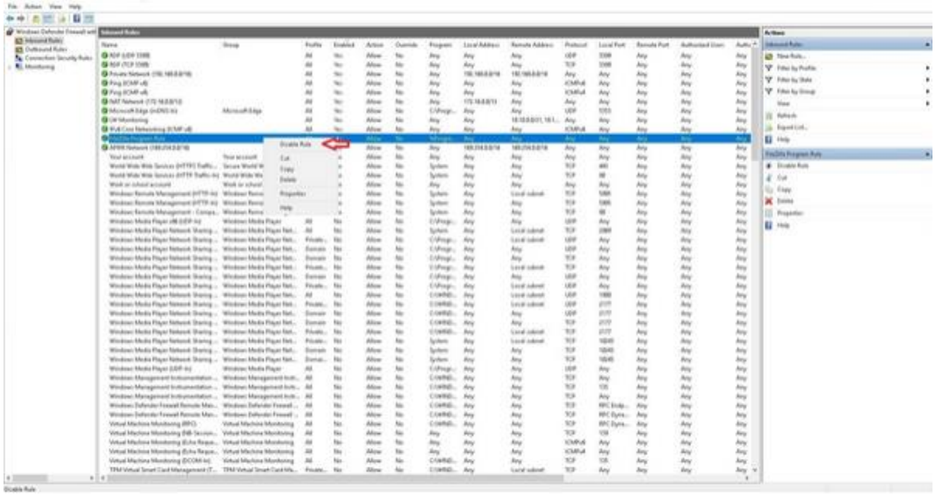
Description (optional):

You should now be able to see your new rule created in the Inbound Rules pane and establish connections to your server with the configured port if a program or service is listening on that port.

Task 4: Close a Port in Windows Server Firewall

If you need to close a previously opened port, find and disable the rule that opens the port using these steps.

1. Open the firewall manager.
2. Click **Inbound Rules** from the left pane to reveal the Inbound Rules pane on the right.
3. Click the **Enabled** column at the top to sort your rules by status until the value of Yes is at the top.
4. Locate the rule for the local port you would like to close.
5. Right-click on the rule and select **Disable**.



The Inbound Rule is disabled, and access to the port is restricted.

3. Web Browser Configurations:

The security settings of web browsers to provide the appropriate level of protection. These measures ensure that your web browsers storing only as much of your information as it needs to function normally. Under the “Privacy” tab, complete the following steps.

Task 1: Configure privacy and security setting

1. Select “Use custom settings for history.”
2. Deselect “Remember my browsing and download history.”
3. Deselect “Remember search and form history.”
4. Deselect “Accept third-party cookies.”

5. Set cookie storage to “Keep until I close Firefox.”
6. Select “Clear history when Firefox closes.”

Task 2: Configure security settings

Under the “Security” tab, choose the following settings. These steps prevent browsers from saving your passwords and keep you from visiting potentially harmful sites.

1. Verify that “Warn me when sites try to install add-ons,” “Block reported attack sites,” and “Block reported web forgeries” are all selected.
2. Deselect “Remember passwords for sites.”

Task 3: Enable pop-up blocking

1. Verify that “Block pop-up windows” is selected under the “Content” tab.
2. This feature should be turned on by default as it protects users from unwarranted advertisements and windows.

Task 4: Turn on automatic updates

1. Verify that “Automatically install updates” is selected in the “Update” tab under “Advanced.”
2. Doing so will ensure that your browser receives critical security updates.
3. Verify that “Automatically update Search Engines” is selected as well.

Lap test 1

Instructions: You are required to perform the following individually with the presence of your teacher.

1. Modifying default user settings
    1.1. Modifying Default User Profile (in Windows 10) and show your task
    1.2. Group Policy Active Directory (in Windows Server) and show your task
2. Displaying legal notices at logon
    2.1. Using Group Policy Windows 10 display legal notice at logon
    2.2. Alternatively show a Registry Edit

Lap test 2

Instructions: You are required to perform the following individually with the presence of your teacher.

1. Operating System Configuration (Windows 10):
    - 1.1. Disabling or stop unnecessary services
    - 1.2. Disable startup programs in Windows 10
2. Access and Check the Windows Server Firewall Settings
    - 2.1. Access and show the Windows Firewall Management Console
    - 2.2. View and Configure Inbound Rules in the Console of windows server
    - 2.3. Open and show a Port in Windows Server Firewall
    - 2.4. Close a Port in Windows Server Firewall
3. Web Browser Configurations:
    - 3.1. Configure privacy and security setting
    - 3.2. Configure security settings
    - 3.3. Enable pop-up blocking
    - 3.4. Turn on automatic updates

Unit Two: File and Resource Access

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

- Reviewing inbuilt operating system security and accessing features
- Reviewing file security categorization scheme
- Role of users in security setting
- Implementing and scheduling virus checking process

This unit will also support you to accomplish the learning outcomes stated in the cover page. Specifically, upon completion of this module, you will be able to:

- Explain about inbuilt operating system security and accessing features
- Describe file security categorization scheme
- Identify role of users in security setting
- Implement and schedule virus checking process

2. File and resource access

File and resource access refers to the ability of users or processes to interact with and retrieve data from files and various system resources. Managing access to files and resources is a critical aspect of maintaining the security and integrity of an organization's data.

Access Control Models:

- **Discretionary Access Control (DAC):** Allows the resource owner to determine who has access to their files or resources. Permissions are typically assigned based on user identity.
- **Mandatory Access Control (MAC):** Access is determined by the system or administrator, often using labels or classifications. Common in government and military environments.

File Permissions:

- **Read:** Allows users to view the contents of a file or directory.
- **Write:** Permits users to modify the contents of a file or create new files within a directory.
- **Execute:** Allows the execution of a file as a program or script.

Access Control Lists (ACLs):

- **Fine-Grained Control:** ACLs extend the basic file permissions by providing more

File System Types:

- **NTFS (New Technology File System):** Used in Windows environments, supports advanced file permissions, encryption, and auditing.
- **EXT4 (Fourth Extended File System):** Commonly used in Linux, supports traditional UNIX permissions and ACLs.

Network File Systems (NFS):

- **Cross-Platform Access:** NFS allows file access over a network and is commonly used in mixed-platform environments.
- **Security Considerations:** Requires careful configuration to ensure secure file access.

By implementing these best practices, organizations can effectively manage file and resource access, reduce the risk of unauthorized access, and protect sensitive data from compromise. Organizations should implement a comprehensive strategy that combines proper access controls, auditing, encryption, and user education to control unauthorized access.

2.1.Reviewing inbuilt operating system security and accessing features

Reviewing the inbuilt security features of an operating system is an essential step in assessing the overall security of your computer or network. Operating systems often include built-in security mechanisms and features that can help protect against various threats. Here are some key aspects to consider when reviewing the inbuilt security features of an operating system:

User Authentication and Access Control:

- Operating systems provide user authentication mechanisms and access controls to secure resources.
- Access these features through the "Control Panel" or "Settings" in Windows..

Update and Patch Management:

- Regular updates and patches fix vulnerabilities in the operating system.
- Assess the operating system's patch management capabilities.
- Determine if it provides automatic updates for security patches and fixes to address vulnerabilities.
- Consider the frequency and reliability of patch releases, as well as the ease of deploying patches across your systems.

Antivirus and Anti-Malware Protection:

- Some operating systems come with built-in antivirus or anti-malware tools.
- Determine if it includes antivirus or anti-malware software with real-time scanning and threat detection capabilities.

Audit and Logging:

- Operating systems log events for auditing and security analysis.

Device Management:

- Control access to external devices and manage hardware settings.

Backup and Restore:

- Built-in backup and restore options help recover from data loss.

Remote Desktop and Remote Management:

- Enable or disable remote access features.

Security Center/Settings:

- Some operating systems have centralized security dashboards.

App Permissions:

- Control what permissions applications have.

Security Updates and Notifications

- Configure how and when security updates and notifications are delivered.

Security Policies:

- Set and enforce security policies for the system.

Remember that while built-in security features are valuable, they should be complemented with additional security measures, such as regular patching, security awareness training, and the use of third-party security tools, to establish a robust security posture.

2.2.Reviewing file security categorization scheme

File security categorization is a critical aspect of information security, helping organizations classify and protect sensitive data appropriately. An effective categorization scheme ensures that data is handled in accordance with its level of sensitivity and importance. Below is a review of key considerations for a file security categorization scheme:

1. Data Classification Levels:

Define clear levels of classification based on sensitivity and criticality.

Typical Levels:

- **Public:** Non-sensitive, public information.
- **Internal:** Sensitive information for internal use.
- **Confidential:** Highly sensitive, restricted to specific individuals or teams.
- **Top Secret:** The most sensitive and critical information.

2. Criteria for Classification:

Establish criteria that determine how data is classified.

- **Examples:**
  - **Legal Requirements:** Compliance with industry regulations or legal standards.

- **Business Impact:** The potential impact on the organization if the data is compromised.
- **Confidentiality Requirements:** The need to restrict access to certain individuals or groups.

Collaboration and Sharing Guidelines:

Define rules for collaborating and sharing classified data.

Examples:

- Public data can be shared openly.
- Internal and confidential data may have restricted sharing policies.

Automated Classification Tools:

Consider using automated tools to classify data based on content and context.

Examples:

- Data Loss Prevention (DLP) tools can automatically classify and control the flow of sensitive information.
- Prevention (DLP) tools can automatically classify and control the flow of sensitive information.

A well-structured file security categorization scheme provides a foundation for a robust information security program. Regular reviews and updates, along with clear communication and training, contribute to the effectiveness of the scheme. Additionally, integrating technology solutions for automated classification and monitoring enhances the overall security posture of the organization.

2.3.Role of users in security setting

Users play a crucial role in the overall security setting of any organization. Their actions, awareness, and adherence to security policies significantly impact the cybersecurity posture. Here are key aspects of the role user's play in security settings:

Password Management:

- **Creation of Strong Passwords:** Users are responsible for creating strong, unique passwords that are not easily guessable.

- **Regular Password Updates:** Adhering to policies that require periodic password changes enhances security.

Phishing Awareness:

- **Recognizing Phishing Attempts:** Users need to be trained to recognize phishing emails and other social engineering tactics.

- **Avoiding Clicking on Suspicious Links:** Refraining from clicking on links or downloading attachments from unknown or suspicious sources is critical.

Device Security:

- **Securing Personal Devices:** If allowed for work-related tasks, users should follow security practices on personal devices, including regular updates and antivirus software.
- **Reporting Lost or Stolen Devices:** Users play a vital role in reporting lost or stolen devices promptly to initiate security measures.

Data Handling and Classification:

- **Understanding Data Sensitivity:** Users must understand the sensitivity of data they handle and apply appropriate security measures.
- **Following Data Classification Policies:** Adherence to data classification policies ensures that sensitive information is handled with the necessary precautions.

Software Updates:

- **Promptly Applying Updates:** Users should apply software updates promptly to ensure that systems are protected against known vulnerabilities.
- **Reporting Software Issues:** Prompt reporting of software-related issues helps in addressing security concerns efficiently.

Physical Security:

- **Securing Workstations:** Users play a role in physically securing their workstations to prevent unauthorized access.
- **Locking Devices When Away:** Adhering to the practice of locking computers when away from the desk contributes to physical security.

Remote Work Security:

- **Securing Home Networks:** Users should take steps to secure their home networks, including updating router passwords and using encryption.
- **Using Virtual Private Networks (VPNs):** Adhering to the use of VPNs for secure remote access to organizational resources.

Reporting Suspicious Activities:

- **Proactive Reporting:** Users are often the first line of defense and should proactively report any suspicious activities or security concerns.
- **Understanding Reporting Procedures:** Users should be aware of and understand the procedures for reporting security incidents.

Data Backups:

- **Adherence to Backup Policies:** Users should follow organizational backup policies, ensuring that critical data is regularly backed up.
- **Understanding Data Recovery Procedures:** Users should be aware of data recovery procedures in case of data loss.

In summary, users are integral to the success of any cybersecurity strategy. Their awareness, proactive involvement, and adherence to security practices contribute significantly to maintaining a secure environment. Continuous education, clear communication, and a collaborative approach between users and IT/security teams are essential for a robust security posture.

2.4.Implementing and scheduling virus checking process

Implementing and scheduling virus checking processes is a critical component of maintaining a secure computing environment. Virus checking, also known as antivirus or anti-malware scanning, helps detect and mitigate potential threats to your systems. Here's a guide on how to implement and schedule virus checking processes:

Enable automatic updates for the antivirus software to ensure it stays current with the latest virus definitions and scanning engine improvements. This helps the system stay resilient against evolving threats. Configure the software to perform email attachment scanning to prevent malware spread through emails, and enable scanning of USB drives and other removable media to thwart potential threats from external sources. Define quarantine actions for detected threats, specifying whether files should be isolated, cleaned, or deleted.

Install and Configure the Antivirus Software:

- **Follow Installation Instructions:** Install the antivirus software according to the vendor's instructions.
- **Configure Settings:** Adjust settings to fit your organization's security policies and requirements.

Configure Real-Time Scanning:

- **Enable Real-Time Protection:** Turn on real-time scanning to monitor files and processes in real-time for potential threats.
- **Configure Settings:** Adjust real-time scanning settings based on your organization's security needs.

Schedule Regular Full System Scans:

- **Select Scan Frequency:** Schedule regular full system scans to check all files and directories.
- **Off-Peak Hours:** Schedule scans during off-peak hours to minimize impact on system performance.

Schedule Quick Scans:

- **Frequent Quick Scans:** Schedule more frequent quick scans for critical system areas and commonly targeted locations.
- **Daily or Weekly:** Perform quick scans daily or weekly to quickly identify and address emerging threats.

Automatic Updates:

- **Enable Automatic Updates:** Ensure that the antivirus software receives automatic updates to its virus definitions and scanning engine.
- **Frequent Updates:** Configure the software to check for updates multiple times per day.

Include Virus Checking in Change Management:

- **Coordinate with IT Changes:** Integrate virus checking into your organization's change management process.
- **Test Updates:** Ensure that antivirus updates are tested before deployment. Ensure that antivirus updates are tested before deployment.

Integration with Security Information and Event Management (SIEM):

- **Integrate with SIEM:** If applicable, integrate antivirus logs with your SIEM solution for centralized monitoring and analysis.
- Automate Responses: Automate response actions based on SIEM alerts.

Self-check test-2

Instruction: You are required to perform the following questions individually.

I. Write true if the questions are correct and write false if the questions are incorrect.

1. Regular updates and patches fix vulnerabilities in the operating system.
2. Some operating systems come with built-in antivirus or anti-malware tools.
3. It is possible to configure the software to check for updates multiple times per day.
4. Users should be aware of and understand the procedures for reporting security incidents.

II. Choose the best answer from the questions listed below.

1. For managing file and resource access which one is access control lists
   A. Read
   B. Write:
   C. Fine-Grained Control
   D. Execute
2. Which one of the following is a typical levels of data classification?
   A. Public
   B. Internal
   C. Top Secret
   D. All
3. Which one of the following role of users in security setting
   A. Password Management
   B. Device Security
   C. Phishing Awareness:
   D. All

III. Matching the following from column “A” into column “B“

A	B
1. Device Management	A. Enforce rules for the system
2. App Permissions	B. Highly sensitive to specific or teams
3. Security Policies	C. Manage hardware settings
4. Confidential	D. Control what permissions app have.

IV. List and Fill in the blank space for the following questions.

1. What is inbuilt security features of an operating system
2. What does user Authentication and Access Control mean
3. What is the importance of Data Backups

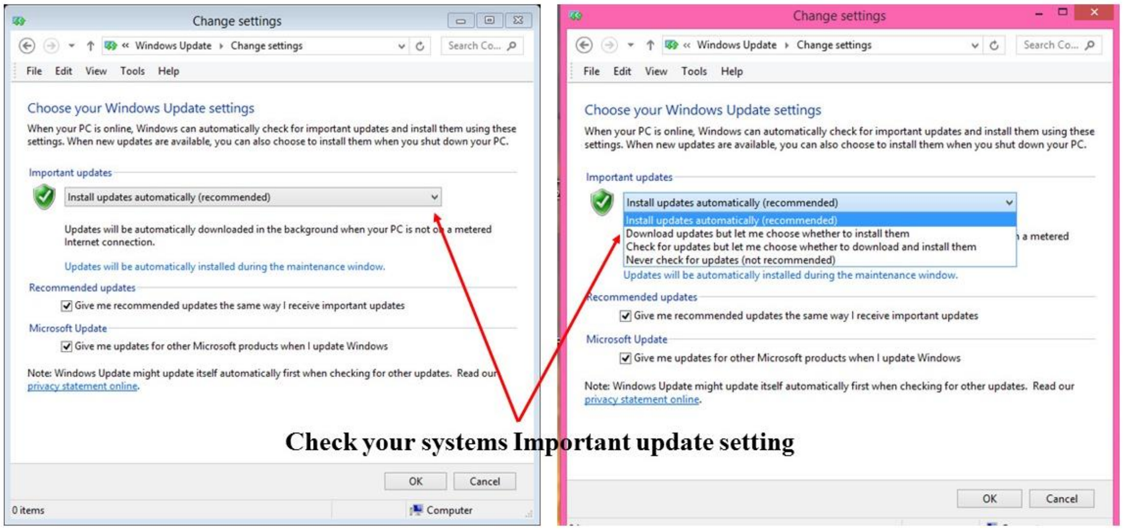
Operation Sheet 2.1

Reviewing inbuilt operating system security and accessing features

1. **Update and Patch Management:**

Check your windows update setting

- Windows updates are managed through for windows 7 and 8 "Control Panel" > "Windows Update" > "Change Setting" for windows 10 "Settings" > "Update & Security."



Choose your Windows Update settings

When your PC is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also choose to install them when you shut down your PC.

Important updates

Install updates automatically (recommended)

Updates will be automatically downloaded in the background when your PC is not on a metered Internet connection.

Updates will be automatically installed during the maintenance window.

Recommended updates

☑ Give me recommended updates the same way I receive important updates

Microsoft Update

☑ Give me updates for other Microsoft products when I update Windows

Note: Windows Update might update itself automatically first when checking for other updates. Read our privacy statement online.

Choose your Windows Update settings

When your PC is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also choose to install them when you shut down your PC.

Important updates

Install updates automatically (recommended)
- Install updates automatically (recommended)
- Download updates but let me choose whether to install them
- Check for updates but let me choose whether to download and install them
- Never check for updates (not recommended)

Updates will be automatically installed during the maintenance window.

Recommended updates

☑ Give me recommended updates the same way I receive important updates

Microsoft Update

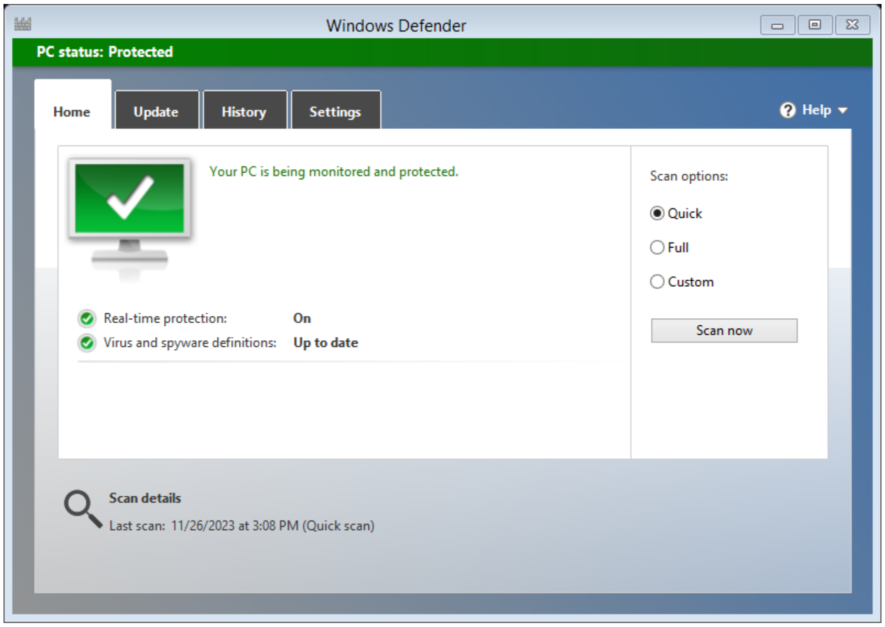
☑ Give me updates for other Microsoft products when I update Windows

Note: Windows Update might update itself automatically first when checking for other updates. Read our privacy statement online.

Check your systems Important update setting

2. **Antivirus and Anti-Malware Protection:**

- Some operating systems come with built-in antivirus or anti-malware tools.
- In Windows, “Windows Defender” is the default; and Click, check your PC status: protected:-
- Check your computer’s status, run a scan and more
- Make sure that your computer is using the latest updates to help protect against potential threat
- Summarized view of the items detected in previous scan and the action that were taken
- Decide how you want to this app to run on your computer



PC status: Protected

Your PC is being monitored and protected.

Real-time protection: On

Virus and spyware definitions: Up to date

Scan options:

● Quick

○ Full

○ Custom

Scan details

Last scan: 11/26/2023 at 3:08 PM (Quick scan)

3. **User Account Controls:**

Evaluate the operating system's user account management capabilities.

- Look for features such as user authentication, password policies, and the ability to assign different user roles and permissions.
- Ensure that strong password policies can be enforced and that user accounts can be easily managed and audited.
- In Windows, access through "Control Panel" > "User Accounts."

4. **Device Management:**

- You can use “Device manager” to view and check a list of hardware devices installed on your computer and set properties for each device.
- In Windows, access device manager through "Control Panel" > "System" > "Device Manager."

5. **Remote Desktop and Remote Management:**

- Enable or disable remote access features.
- In Windows, configure through "Control Panel" > "System" > "Remote Settings."

Lap test 2

Instructions: You are required to perform the following individually with the presence of your teacher.

1. Check your windows update setting
2. Evaluate the operating system's user account management capabilities.
3. View and check a list of hardware devices installed on your computer and set properties for each device.
4. Enable or disable remote access features

Unit Three: Authentication Requirements

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

- Determining security requirements
- Identifying and analyzing authentication options
- Selecting authentication and authorization processes

This unit will also support you to accomplish the learning outcomes stated in the cover page. Specifically, upon completion of this module, you will be able to:

- Determine security requirements
- Identify and analyze authentication options
- Select authentication and authorization processes

3. Authentication Requirements

Overview of authentication requirements

Establishing strong authentication requirements is crucial for safeguarding sensitive information and systems from unauthorized access. The following steps outline key components of effective authentication practices:

Firstly, organizations should enforce robust password policies. This involves defining complex password criteria, including minimum length, character types, and regular updates. Users play a vital role in creating strong, unique passwords.

Authentication requirements should be integrated into incident response plans, ensuring timely investigation and response to authentication-related incidents. Consideration should be given to third-party authentication providers, ensuring secure integration and adherence to security standards. Regular security reviews of third-party providers contribute to maintaining a secure authentication ecosystem.

Access revocation, involving the prompt deactivation of user accounts when access is no longer required, should be included in off boarding procedures for departing employees. This ensures that former employees do not retain unnecessary access rights, reducing the risk of unauthorized entry into systems and data.

3.1.Determining security requirements

Determining security requirements is a critical step in developing a comprehensive cybersecurity strategy that aligns with an organization's needs and goals. The process involves assessing risks, identifying assets, and defining the necessary security controls to protect against potential threats. Here is a step-by-step guide to determining security requirements:

Risk Assessment:

- **Identify Assets:** Begin by identifying and categorizing critical assets, including data, systems, applications, and infrastructure.
- **Threat Analysis:** Conduct a thorough threat analysis to identify potential risks and vulnerabilities.

- **Assess Impact:** Evaluate the potential impact of security incidents on the organization, considering factors such as financial loss, reputational damage, and operational disruptions.

Define Security Objectives:

- **Clarify Objectives:** Clearly define security objectives based on the organization's mission, values, and business goals.
- **Prioritize Objectives:** Prioritize security objectives based on the criticality of assets and potential risks.

Data Encryption:

- **Identify Sensitive Data:** Identify and classify sensitive data that requires encryption.
- **Define Encryption Standards:** Establish encryption standards for data in transit and data at rest.

Incident Response and Reporting:

- **Develop Incident Response Plan:** Create a comprehensive incident response plan outlining steps to be taken in the event of a security incident.
- **Reporting Procedures:** Define reporting procedures for security incidents to ensure timely and accurate communication.

Network Security:

- **Firewall Rules:** Define firewall rules and configurations to control inbound and outbound network traffic.
- **Intrusion Detection/Prevention Systems:** Implement intrusion detection and prevention systems to monitor and protect against malicious activities.

By following these steps, organizations can systematically determine their security requirements, ensuring a robust and effective cybersecurity posture that addresses potential risks and compliance obligations. Regular reviews and updates to security requirements are essential to adapt to the evolving threat landscape.

3.2.Identifying and analyzing authentication options

Identifying and analyzing authentication options is a crucial step in designing a secure and user-friendly access control system for an organization. Authentication is the process of verifying the identity of a user, system, or application before granting access. Here is a comprehensive look at various authentication options and factors to consider during the identification and analysis process:

Username and Password:

- **Identification:** Users provide a username and password.
- **Pros:** Widely used, familiar to users.
- **Cons:** Vulnerable to password-related attacks, user compliance challenges.

Multi-Factor Authentication (MFA):

- **Identification:** Users provide multiple forms of identification (e.g., password, token, biometric).
- **Pros:** Enhanced security, mitigates risks of compromised credentials.
- **Cons:** Implementation complexity, potential user friction.

Biometric Authentication:

- **Identification:** Users provide unique biological features (e.g., fingerprint, facial recognition).
- **Pros:** High accuracy, difficult to forge.
- **Cons:** Privacy concerns, potential for false positives/negatives.

Smart Cards and Tokens:

- **Identification:** Users present a physical card or token.
- **Pros:** Two-factor authentication, portable.
- **Cons:** Cost of implementation, risk of loss or theft.

Time-Based Authentication:

- **Identification:** Users enter a code valid for a specific time.
- **Pros:** Dynamic security, reduces vulnerability to replay attacks.
- **Cons:** Time synchronization challenges.

Device Authentication:

- **Identification:** Devices are authenticated based on unique identifiers.
- **Pros:** Enhances network security, prevents unauthorized devices.
- **Cons:** Device management complexity.

Risk-Based Authentication:

- **Identification:** Authentication adapts based on risk factors.
- **Pros:** Adaptive security, responsive to contextual changes.
- **Cons:** Initial setup complexity.

Password less Authentication:

- **Identification:** Users authenticate without traditional passwords.
- **Pros:** Eliminates password vulnerabilities, enhanced security.
- Cons: Limited adoption, compatibility challenges.

Session Management:

- **Identification:** Users are authenticated for the duration of a session.
- **Pros:** Reduced need for frequent logins, improved user experience.
- **Cons:** Increased risk if sessions are not securely managed.

When identifying and analyzing authentication options, organizations must consider factors such as the level of security required, user experience, regulatory compliance, and the specific use cases for which authentication is needed. A balanced and well-integrated combination of these authentication methods can contribute to a robust and adaptable access control system. Regular reviews and updates to authentication mechanisms are essential to address emerging threats and technological advancements.

3.3.Selecting authentication and authorization processes

Selecting authentication and authorization processes is a crucial aspect of designing a secure and effective access control system. Authentication verifies the identity of users, systems, or applications, while authorization determines the permissions and access levels granted to authenticated entities. Here are considerations and steps to guide the selection of authentication and authorization processes:

1. **Authentication Processes:**

Risk Assessment:

- **Identify Risks:** Conduct a risk assessment to understand the potential threats and vulnerabilities.
- **Risk Tolerance:** Determine the organization's risk tolerance and the sensitivity of the systems and data.

User Authentication Methods:

- **Evaluate Options:** Consider various user authentication methods, such as passwords, multi-factor authentication (MFA), biometrics, and smart cards.
- **User Experience:** Balance security needs with the usability and user experience of the chosen authentication methods.

Compliance Requirements:

- **Regulatory Compliance:** Ensure that the selected authentication processes align with industry and regulatory compliance standards applicable to the organization.

2. **Authorization Processes:**

Access Control Models:

- **Role-Based Access Control (RBAC):** Consider implementing RBAC to assign permissions based on job roles.
- **Attribute-Based Access Control (ABAC):** Explore ABAC for a more dynamic and context-aware access control model.

Granularity of Permissions:

- **Fine-Grained Permissions:** Determine the level of granularity required for access permissions, considering the principle of least privilege.
- **Hierarchical Permissions:** Explore hierarchical permission structures to simplify administration.

Policy Enforcement:

- **Policy Definition:** Clearly define and document access control policies for consistent enforcement.

- **Automation:** Explore automation tools for policy enforcement to reduce manual errors and ensure consistency.

Integration with Authentication:

- **Tight Integration:** Ensure tight integration between authentication and authorization processes to maintain a coherent access control system.
- **Secure Token Exchange:** Implement secure token exchange mechanisms between authentication and authorization components.

Audit Trails and Logging:

- **Logging Requirements:** Establish robust audit trails for tracking access requests, grants, and denials.
- **Analysis Tools:** Implement tools for analyzing access logs to detect and investigate unauthorized activities.

Dynamic Authorization:

- **Contextual Authorization:** Consider dynamic authorization that adapts based on contextual factors such as user location, time, and device.
- **Adaptive Access Controls:** Implement adaptive access controls that adjust permissions based on real-time risk assessments.

Policy Updates:

- **Regular Review:** Regularly review and update access control policies to align with changing business requirements.
- **Incident-Driven Updates:** Update policies in response to security incidents and lessons learned from incidents.

Selecting authentication and authorization processes requires a holistic approach, considering both technical and operational aspects. Organizations should continually assess the effectiveness of these processes and be prepared to adapt to changes in technology, business requirements, and the threat landscape. Regular updates to access control policies and ongoing collaboration with relevant stakeholders are critical for maintaining a secure and efficient access control framework.

Self-check test-3

Instruction: You are required to perform the following questions individually.

I. Write true if the questions are correct and write false if the questions are incorrect.

1. Create a comprehensive incident response plan outlining steps to be taken in the event of a security incident.
2. Define reporting procedures for security incidents to ensure timely and accurate communication.
3. Authentication requirements should be integrated into incident response plans

II. Choose the best answer from the questions listed below.

1. What are the Risk Assessment Metrics______________?

   A. Identify Assets: C. Threat Analysis:

   B. Assess Impact D. All

2. Which of the following is Authentication Processes:

   A. Identify Risks C. Evaluate Options

   B. User Experience D. All

3. Which of the following is Authorization Processes:

   A. Granularity of Permissions C. Access Control Models

   B. Policy Enforcement D. All

III. Matching the following from column "A" into column "B"

A	B
1. Intrusion Detection	A. Provide unique biological features
2. Network Security	B. Incident-Driven Updates
3. Biometric Authentication	C. Firewall Rules
4. Policy Updates	D. Protect against malicious activities

IV. List and Fill in the blank space for the following questions.

1. How to determining security requirements
2. Discuss Risk-Based Authentication
3. Discuss Password less Authentication
4. What is Dynamic Authorization mean?

Unit Four: Network Security

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

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

This unit will also support you to accomplish the learning outcomes stated in the cover page. Specifically, upon completion of this module, you will be able to:

- Share user resources access via a network
- Monitor and record Security threats
- Update the latest antivirus signatures

4. Network security

Overview of network security

Network security is a critical aspect of information technology that focuses on protecting the integrity, confidentiality, and availability of data within a computer network. It involves the implementation of measures and technologies to safeguard the network infrastructure, data, and communication against unauthorized access, attacks, and disruptions. Here is an overview of key components and considerations in network security:

Key Components of Network Security:

1. **Firewalls:**
   - Firewalls are network security devices that monitor and control incoming and outgoing network traffic based on predetermined security rules. They act as a barrier between a trusted internal network and untrusted external networks, such as the internet.
2. **Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):**
   - IDS monitors network and/or system activities for malicious activities or policy violations. IPS goes a step further by actively preventing or blocking detected threats.
3. **Virtual Private Networks (VPNs):**
   - VPNs establish secure and encrypted connections over an untrusted network, such as the internet. They enable secure remote access, allowing users to connect to the organization's network from outside locations.
4. **Secure Sockets Layer (SSL) and Transport Layer Security (TLS):**
   - SSL and TLS protocols provide secure communication over a computer network. They are commonly used to secure web browsing, email, and other data transfer protocols.
5. **Network Access Control (NAC):**
   - NAC systems enforce security policies on devices seeking to access a network. They assess the compliance of devices with security policies before granting access.
6. **Network Segmentation:**
   - Segmentation divides a network into smaller, isolated segments to contain potential security breaches. It limits the impact of an attack by restricting lateral movement within the network.

7. **Wireless Security:**
   - Wireless networks require specific security measures. Protocols like WPA (Wi-Fi Protected Access) and WPA2 provide encryption for wireless communications, while WPA3 is the latest standard.
8. **Encryption:**
   - Encrypting data in transit (e.g., using SSL/TLS) and data at rest (e.g., full-disk encryption) adds a layer of protection, preventing unauthorized access even if data is intercepted.

Considerations in Network Security:

1. **Vulnerability Management:**
   - Regularly identify, assess, and remediate vulnerabilities in network devices, software, and configurations to reduce the attack surface.
2. **Security Policies and Procedures:**
   - Develop and enforce comprehensive security policies and procedures that guide the secure configuration, management, and use of network resources.
3. **Employee Training and Awareness:**
   - Train employees on security best practices, recognizing social engineering attacks, and adhering to security policies to prevent inadvertent security breaches.
4. **Incident Response Planning:**
   - Develop and regularly update an incident response plan to effectively respond to and mitigate the impact of security incidents.
5. **Regular Audits and Assessments:**
   - Conduct regular security audits, vulnerability assessments, and penetration testing to identify and address weaknesses in the network.
6. **Patch Management:**
   - Implement a robust patch management process to promptly apply security patches to network devices and software, reducing the risk of exploitation.
7. **Network Monitoring:**
   - Continuous monitoring of network traffic, log data, and security alerts enables the detection of suspicious activities and rapid response to potential threats.

In summary, network security is a multifaceted discipline that involves a combination of technological solutions, best practices, and organizational policies. It requires a proactive and comprehensive approach to mitigate risks and protect the confidentiality, integrity, and availability of critical data and network resources.

4.1. Sharing user resources access via a network

Sharing user resources access via a network involves providing users with the ability to access and utilize shared resources, such as files, folders, printers, and applications, over a network. This process is fundamental for collaborative work, file sharing, and efficient resource utilization within an organization. Here are key considerations and steps for sharing user resources access:

1. Network File Sharing:

- **Shared Drives and Folders:**
  - ➢ Create shared network drives or folders to centralize documents and files that need collaborative access.
  - ➢ Apply appropriate access controls, specifying who can read, write, or modify shared files.

2. User Authentication and Authorization:

- **User Identification:**
  - ➢ Implement strong user authentication mechanisms to ensure that users are who they claim to be.
  - ➢ Utilize usernames, passwords, and, if possible, multi-factor authentication for secure user identification.
- **Authorization:**
  - ➢ Define access control policies based on user roles or specific permissions.
  - ➢ Ensure that users are only granted access to resources necessary for their roles.

3. Network Print Sharing:

- **Shared Printers:**
  - ➢ Set up shared printers on the network to allow multiple users to print to a single device.
  - ➢ Configure printer permissions to control who can access and use specific printers.

4. Centralized Application Access:

- **Remote Application Access:**
  - ➢ Implement technologies like Remote Desktop Services (RDS) or virtual desktop infrastructure (VDI) to allow users to access applications remotely.
  - ➢ Ensure secure connections and appropriate access controls for remote application access.

5. Collaboration Platforms:

- **File Collaboration Platforms:**
  - ➢ Utilize collaboration platforms such as SharePoint, Google Drive, or Microsoft Teams for seamless file sharing and collaboration.
  - ➢ Leverage version control and document tracking features to manage changes made by different users.

6. Network Protocols:

- **Choose Appropriate Protocols:**
  - ➢ Select secure and efficient network protocols for resource sharing, such as SMB (Server Message Block) for file sharing or IPP (Internet Printing Protocol) for printers.
  - ➢ Consider the use of encrypted protocols like HTTPS or FTPS for enhanced security.

7. Security Measures:

- **Encryption:**
  - Implement encryption for data in transit to protect sensitive information as it travels across the network.
  - Use protocols like SSL/TLS for securing communication channels.
- **Firewall Rules:**
  - Configure firewalls to allow only necessary network traffic and block unauthorized access.
  - Regularly review and update firewall rules to align with security policies.

8. User Training and Awareness:

- **Security Best Practices:**
  - Educate users on security best practices, emphasizing the importance of secure passwords, responsible file sharing, and adherence to access controls.

    - Provide training on recognizing phishing attempts or social engineering attacks that may target shared resources.

Sharing user resources access via a network requires a balanced approach that combines user convenience with robust security measures. Regularly reviewing and updating access controls, monitoring network activities, and staying informed about emerging security threats contribute to a resilient and secure resource sharing environment.

4.2. Monitoring and recording Security threats

Monitoring and recording security threats is a critical aspect of maintaining the cybersecurity posture of an organization. This process involves continuously observing network activities, system logs, and other relevant data to identify and respond to potential security incidents. Here are key elements and best practices for monitoring and recording security threats:

1. Security Information and Event Management (SIEM):

- **Implement SIEM Solutions:**
    - Utilize SIEM tools to collect, aggregate, and analyze log data from various sources across the network.
    - SIEM systems provide real-time monitoring and can correlate events to identify potential security threats.

2. Log Management:

- **Centralized Log Storage:**
    - Centralize log storage to ensure easy access and analysis of logs from various devices and applications.
    - Maintain logs for an appropriate retention period to facilitate forensic analysis and compliance requirements.

3. Network Traffic Analysis:

- **Network Monitoring Tools:**
    - Employ network monitoring tools to analyze patterns of network traffic and detect anomalies.
    - Set up alerts for unusual or suspicious network behavior.

4. Endpoint Detection and Response (EDR):

- **Deploy EDR Solutions:**

    - Use EDR solutions on endpoints to monitor and respond to security incidents at the device level.
    - EDR tools can detect and mitigate threats like malware, ransomware, and unauthorized access.

5. Anomaly Detection:

- **Define Baseline Behavior:**
    - Establish a baseline for normal user and system behavior.
    - Use anomaly detection mechanisms to identify deviations from this baseline, indicating potential security threats.

6. Threat Intelligence Feeds:

- **Integrate Threat Feeds:**
    - ➢ Subscribe to threat intelligence feeds to stay informed about the latest known threats.
    - ➢ Use threat intelligence to enhance threat detection and response capabilities.

7. Incident Detection and Response:

- **Automated Responses:**
    - ➢ Implement automated responses for known and repetitive security incidents.
    - ➢ Define response playbooks to guide incident response teams.

8. Red Team Exercises:

- **Simulated Attacks:**
    - ➢ Conduct red team exercises to simulate realistic cyber-attacks.
    - ➢ Red teaming helps identify weaknesses in security defenses and response capabilities. Defenses and response capabilities.

9. Documentation and Reporting:

- **Incident Documentation:**
    - ➢ Document security incidents, including the timeline of events, actions taken, and outcomes.
    - ➢ Generate reports for management, stakeholders, and regulatory bodies. Management, stakeholders, and regulatory bodies.

By implementing these practices, organizations can establish a robust system for monitoring and recording security threats. This proactive approach enhances the ability to detect, respond to, and mitigate potential security incidents, ultimately contributing to a more resilient cybersecurity posture.

4.3. Updating the latest antivirus signatures

Updating antivirus signatures is a crucial aspect of maintaining the effectiveness of antivirus software in identifying and mitigating new and evolving threats. Antivirus signatures are patterns or definitions that antivirus programs use to recognize known malware and malicious activities. Regularly updating these signatures ensures that the antivirus software can detect and respond to the latest threats. Here's a guide on how to update antivirus signatures:

1. Enable Automatic Updates:

- Most modern antivirus software includes an automatic update feature. Ensure that this feature is enabled to allow the antivirus program to automatically download and install the latest signature updates.

2. Check Update Settings:

- Verify the settings of the antivirus software to confirm that it is configured to check for updates at regular intervals. You may find these settings in the antivirus program's options or settings menu.

4. Connection to Update Servers:

- Ensure that your computer has a reliable and stable internet connection. Antivirus software typically connects to the vendor's update servers over the internet to download the latest signature updates.

5. Scheduled Scans:

- Configure scheduled scans to run regularly. During these scans, the antivirus program not only checks for malware but also updates its signature database. This ensures that the latest definitions are applied to your system.

8. Manual Update Option:

- Some antivirus software provides a manual update option. If automatic updates fail or if you want to ensure an immediate update, use the manual update feature provided by your antivirus program.

10. Alternative Update Methods:

- Some antivirus vendors provide alternative methods for updating signatures, such as using a separate updater tool.

13. Comprehensive Security Strategy:

- Consider antivirus updates as part of a broader cybersecurity strategy. Implement other security measures, such as regular system updates, strong password practices, and employee training, to enhance overall security.

Ensuring that your antivirus signatures are regularly updated is a fundamental step in protecting your system against malware and other security threats. A proactive and vigilant approach to updating signatures enhances the overall security of your computer or network.

Self-check test-4

Instruction: You are required to perform the following questions individually.

I. Write true if the questions are correct and write false if the questions are incorrect.

1. Firewalls are network security devices that monitor and control incoming and outgoing network traffic.
2. IPS goes a step further by actively preventing or blocking detected threats.
3. SSL and TLS protocols provide secure communication over a computer network.

II. Choose the best answer from the questions listed below.

1. Wireless networks require specific security measures. Protocols like_______
   - A. WPA
   - B. WPA2
   - C. WPA3
   - D. All
2. From the following which one is the Considerations in Network Security?
   - A. Security Policies and Procedures
   - B. Incident Response Planning
   - C. Patch Management
   - D. All
3. ____________define access control policies based on user roles or specific permissions.
   - A. Authentication
   - B. Shared Drives
   - C. Authorization
   - D. All

III. Matching the following from column "A" into column "B"

A	B
1. VPN	A. Scheduled scans to run regularly
2. Manual Update Option	B. Known and repetitive security incidents
3. Scheduled Scans	C. Establish secure connections
4. Automated Responses	E. Ensure an immediate update

IV. List and Fill in the blank space for the following questions.

1. What is Vulnerability Management?
2. What is Threat Intelligence Feeds?
3. What is Endpoint Detection and Response?

የሥራና ክህሎት ሚኒስቴር
Ministry of Labor and Skills

Developers Profile

No	Name	Qualification	Field of Study	Organization/ Institution	Mobile number	E-mail
1)	Zerihun Abate	MSc	ITM	Sebata PTC	0911858358	zedoabata2017@gmail.com
2)	Abebe Mintefa	MSc	ITM	Ambo TVETC	0929362458	tolabula@gmail.com
3)	Endale Bereket	Bsc	Computer Science	M/G/M/B/P/T/C	0915439694	zesaron1221@gmail.com
4)	Yinebeb Tamiru	Bsc	Computer Science	APTC	0936325182	Yinebebtamiru07@gmail.com