CM-SUM25_Final-Exam

Start Assignment

- Due Aug 8 by 4:59pm
- Points 100
- Submitting a file upload
- Available Jul 27 at 12am - Aug 8 at 4:59pm

- image.png

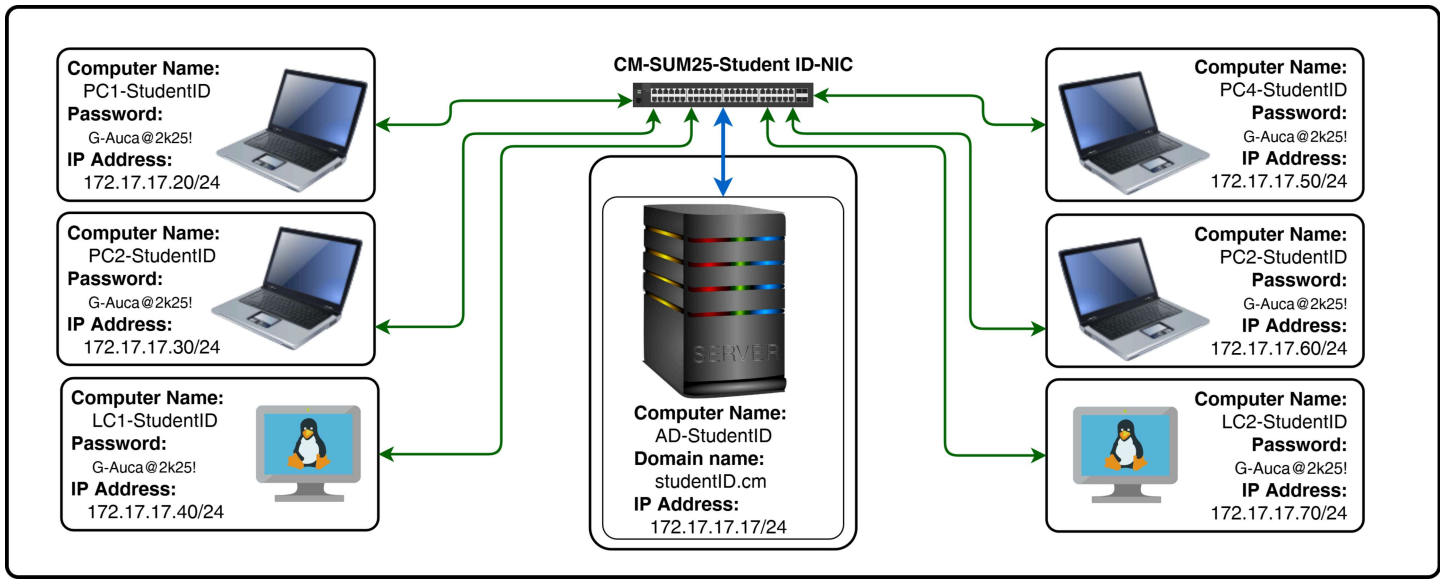
Faculty of Information Technology

Final Exam (Practical) Academic Year: 2024-2025 (3)

Course Code & Name: INSY 8121 & Computer Maintenance

Lecturer: Joshua IRADUKUNDA **Date: From 3rd to 8th Aug, 2025**

MAX/40 **Group Day: (ALL)** **DURATION:** 6 Days



1. Introduction & Executive Summary

1.1 Introduction

In corporate IT environments, IT support officers are tasked with maintenance and upgrading of the functionality of technology systems. Their work most often entails the installation of operating

systems on various devices, ensuring that all the systems are updated and secure. They also recover lost data, which is accomplished through the application of data recovery techniques to access important information that could have been accidentally deleted or compromised.

Additionally, support officers must segment storage to optimize system performance and data management. They accomplish this by dividing drives and implementing storage solutions that optimize speed and efficiency. Another significant activity is troubleshooting Active Directory domain issues, where they must diagnose and fix issues that can affect user access, permissions, and the overall network connectivity.

It is necessary to implement security policies in protecting sensitive data and preventing unauthorized access to them in their role. These include implementing firewall configurations, antivirus, and security updates to protect the company against cyber attacks.
This review will simulate real-world situations in an isolated virtual lab environment so participants may see concrete, real-world applications of the problems with which they will be dealing when employed by your firm. Your product will demonstrate not only your technical acumen but also your capacity to present complex ideas in concise and unambiguous language and your problem-solving skill.

Throughout the exam, you will be employing the software tools provided to you as part of the **CM-SUM25-FinalExamTools** (https://drive.google.com/drive/folders/14mMntbJKF9hiscuxeHVkSyagkyMGfvqu) package, which contains almost all images and tools required to complete the task. The suite gives you the tools to make your expertise and readiness evident to complete the tasks required of a professional IT support position.

1.2 Executive Summary

Task Area	Description
Virtualization & OS Setup	Create two client VMs (PC1-<Student_ID> and PC2-<Student_ID>) and one server VM (AD-<Student_ID>) with recommended CPU, RAM, and disk space.
System Protection & Recovery	Make a system restore point, simulate accidental file deletion with <Student_ID>.txt, recover it as studentid.txt using Recuva.
Disk Partitioning	Create a new 10GB NTFS partition labeled D-<Student_ID> for storing user data separate from system files.
AD Domain & DNS Setup	Manually build an Active Directory forest root named studentid.cm and set up the related DNS zone for domain service discovery.
Policy Configuration	Implement password policies (complexity, expiration, lockout) and describe access control conceptualization for C:\Sensitive folder.

Task Area	Description
Organizational Units & Users	Create three OUs (Student, Lecturer, Registrar) with four user accounts each; set login restrictions per OU/user group.
Shared Folders	Set up department-specific shares and a MasterStorage share accessible to all users with controlled permissions.
HD Video Walkthrough	Provide a detailed narrated video precisely following the grading rubric covering all practical tasks.

2. Objectives & Learning Outcomes

2.1 Core Objectives

Objective	Description
Infrastructure Deployment	Install and configure Windows/Linux OS on virtual machines with appropriate hardware allocation.
Directory Service Setup	Build and configure Active Directory Domain Services (AD DS) with OUs, user accounts, and password policies.
Disaster Recovery	Demonstrate system restore point creation and file recovery using industry-standard tools like Recuva.
Storage Management	Partition and label disks to logically separate system files from user data, improving data safety.
Identity & Access Management	Organize user authentication and authorization within an Active Directory forest with DNS integration.
Policy Design	Define and apply password and login restriction policies; conceptualize folder access restrictions.
Resource Sharing	Architect shared folders with role-based access to facilitate departmental and organizational needs.

2.2 Expected Learning Outcomes

Outcome Category	Description
Technical Proficiency	Master Virtual Machine creation, OS installation, Active Directory configuration, and DNS management.
Conceptual Understanding	Explain security measures like password expiration and login restrictions in an organizational context.
Troubleshooting Acumen	Identify and resolve typical issues such as DNS errors, locked accounts, and restore failures.
Professional Reporting	Create clear, professional-quality instructional videos communicating technical details effectively.

3. Detailed Task Explanations

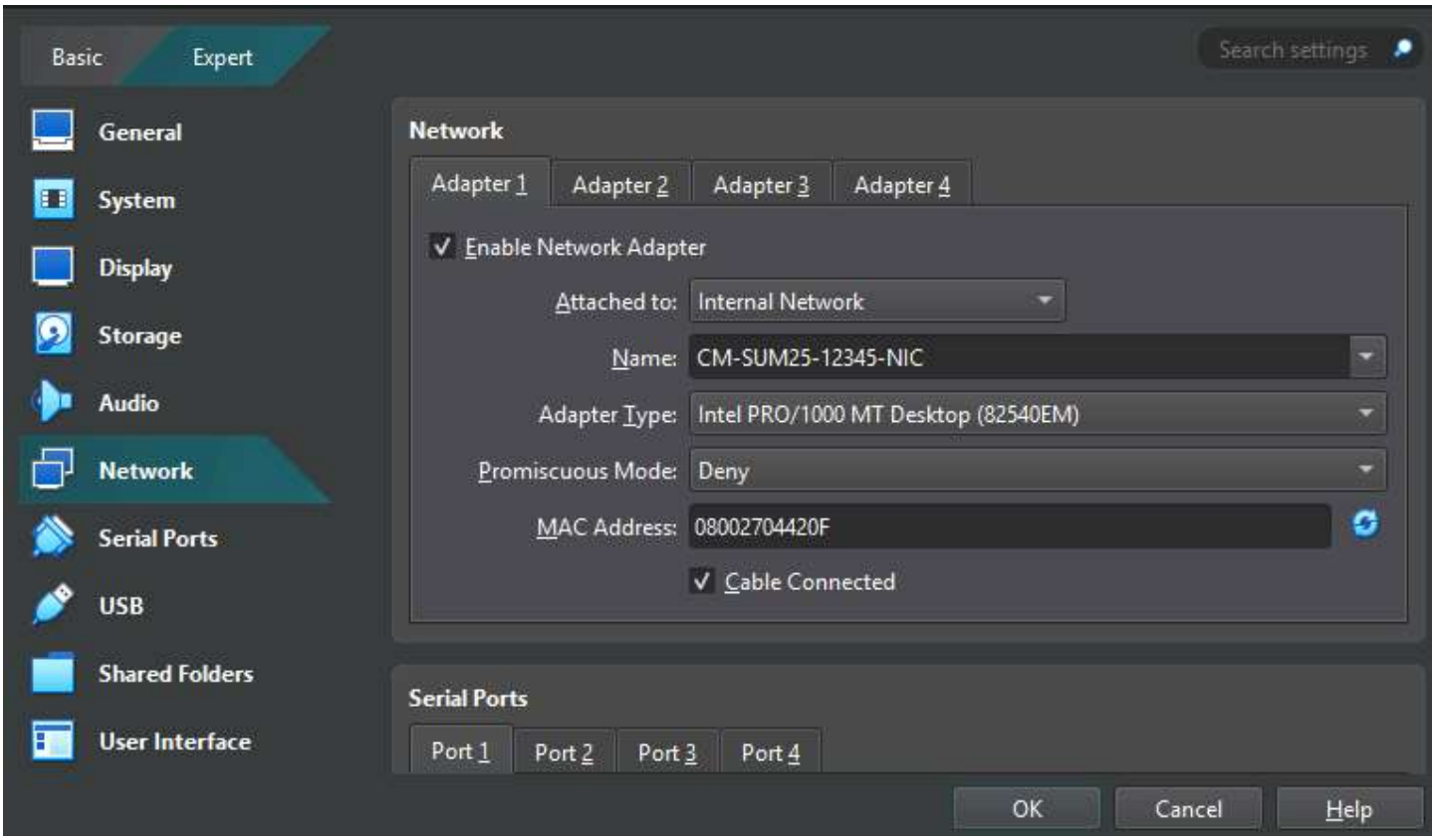
3.1 Virtual Machine Setup

Why Virtualization?

VMs isolate your testing environment from the host system and simulate production environments efficiently, enabling easy snapshots and backups.

Machine Type	RAM	CPU Allocation	Naming Convention	IP Addressing
Server VM	512 MB (minimum)	1 or 2 vCPUs	AD-<Student_ID>	Static IP (example: 172.17.17.17)
Client VM 1	256 MB	1 vCPU	PC1-<Student_ID>	Static IP (example: 172.17.17.20)
Client VM 2	256 MB	1 vCPU	PC2-<Student_ID>	Static IP (example: 172.17.17.30)
Client VM 3	500 MB	1 vCPU	LC1-<Student_ID>	Static IP (example: 172.17.17.40)

Network Adapter: CM-SUM25-Student ID-NIC



- Assign static IPs on all VMs.
- Use appropriate subnet mask and gateway consistent with your lab topology.
- Check connectivity by pinging machines and using Remote Desktop/Screens for Windows Server across all client machines.

3.2 System Restore & File Recovery

System Restore Points

- **Purpose:** A restore point serves as a snapshot of your system files and registry settings at a specific moment in time. This allows you to revert your computer to that previous state in case of system failures or misconfigurations. Using restore points can help to troubleshoot issues caused by software installations, updates, or changes in system settings, ensuring that your system remains stable and functional.
- **Creation Steps:**
  1. **Open System Properties:** Right-click on the **This PC** or **My Computer** icon on your desktop or in File Explorer.
     - Select **Properties** from the context menu.
     - In the left sidebar, click on **System Protection** to access the System Protection settings.
  2. **Select the System Drive:** In the **System Protection** tab, you will see a list of available drives. Select your system drive (usually labeled as **C:**). And Ensure that the **Protection Status** for the selected drive is set to **On**. If it's not, you may need to configure it to enable restore points.
  3. **Create a Restore Point:** Click the Create button located in the bottom right corner of the window. And you will be prompted to enter a description for the restore point. Choose a name that clearly describes its purpose, such as "**<StudentID>_PrePolicyConfig_PC1**," so you can easily identify it later. After entering the name, click **Create** to initiate the process.
  4. **Testing the Restore Point:** You have to delete some system configurations, registry entries, or drivers to demonstrate that you can revert to the restore point created earlier. Before recovering, click on the **test** option to display all changes that have occurred.

File Recovery

- **Background:** When a file is deleted from a computer, the references to that file in the directory are removed, making it seemingly inaccessible. However, the actual data stored on the disk remains intact until the data blocks are overwritten by new information. This means that, in many cases, it is possible to recover deleted files as long as they have not been replaced.

- **Task:**

1. Begin by creating a new text file named **<Student_ID>.txt**, where you will write a concise introduction about yourself. This introduction should include details such as your name, field of study, academic interests, and any relevant experiences or hobbies you would like to share.
2. Once you have finished writing your introduction, proceed to delete the file permanently. Ensure you are using the method that bypasses the recycle bin, which will remove all traces of the file from the usual recovery paths.
3. Next, open the file recovery software, (e.g. **Recuva**). To make the scanning process more efficient, use the filtering feature to specifically search for the deleted file by its name, <Student_ID>.txt. This will help the software locate the file more quickly among the various data sectors.
4. After the scan is complete, follow the prompts to recover the file, saving it as studentid.txt. Take note of the location where the file is restored to make it easier to find later.
5. Finally, confirm the success of the recovery process by opening the newly recovered studentid.txt file. Check to ensure that the contents are intact and reflect the introduction you initially wrote, verifying that the data has been successfully restored without any corruption or loss.

- **Video Tips:** Show scanning progress, successful recovery prompts, and file content validation.

3.3 Disk Partitioning Strategy

Step	Explanation
Shrink System Volume	Reduce the main C: drive size using **Disk Management** to free space for user data partition.
Create New Partition	Create a 10GB partition, format as NTFS, and label as **D-<Student_ID>** for separation.
Verification	Use **Disk Management** and **File Explorer** to confirm partition and label visibility.

Rationale:
Separating OS and user data protects important files during system restores and simplifies backups.

3.4 Active Directory & DNS Fundamentals

Component	Description
AD/DC	Provides centralized authentication and authorization services in a Windows domain environment.

Component	Description
DNS Integration	AD depends on DNS SRV records to enable clients and services to locate domain controllers and resources.

Domain Controller Promotion Steps (Conceptual Description)

1. Add Active Directory Domain Services (AD DS) role via **Server Manager**.
2. Run the domain controller promotion wizard:
   - Select "Add a new forest" and specify the root domain as `studentid.cm`.
   - Set the Directory Services Restore Mode (DSRM) administrator password securely (do not reveal password on-screen).
3. Restart as required and verify AD and DNS services are operational.

Joining Clients to Domain

- On each client PC:
  - Open **System Properties** → **Computer Name** → **Change** → join `studentid.cm` domain.
  - Reboot and log in using created domain accounts to validate.

3.5 OU Architecture & Restrictions

OU Name	Users	Login Restrictions
Student	Stud1 – Stud4	Stud1 & Stud2: Log in 7AM–5PM only
Lecturer	Lect1 – Lect4	Log in only on PC1-<Student_ID> only
Registrar	Reg1 – Reg4	No login allowed during weekends

User Account Setup

- Assign initial passwords: `G-Auca@2k25!`
- Require password change on next login to enforce policy compliance.

Additional Restrictions

- Students can read only their individual "Marks" files (e.g., `Stud1_Marks.txt` in the `Marks` folder), cannot edit or delete them.

- Use Group Policy or logon scripts to enforce these restrictions conceptually.

Remote Desktop Connections

- Use **MSTSC** (Remote Desktop) from client to server and vice versa.
- On Linux, use RDP or VNC clients to connect to Windows machines.
- Demonstrate session persistence and login state visibility remotely.

3.6 Shared Folder Design & Access

Share Name	Purpose	Permissions
MasterStorage	Organization-wide announcements	Read for Domain Users; Write for Domain Admins
StudentStorage	Student OU workspace	Full Control for Student OU; Read-only for others
LecturerStorage	Lecturer OU workspace	Full Control for Lecturer OU; Read-only for others
RegistrarStorage	Registrar OU workspace	Full Control for Registrar OU; Read-only for others

- Conduct a thorough test of share access using accounts both within and outside the organizational unit (OU) to ensure that permissions are correctly configured and functioning as intended.
- Map network drives automatically by group policy or login scripts (demonstrate auto-mapping in video).

3.7 Policy Definitions

Policy Aspect	Configuration	Reasoning & Explanation
Password Length	A minimum requirement of 12 characters	Longer passwords significantly enhance security by making it more challenging for attackers to crack them using brute-force methods, which systematically guess combinations until the correct one is found.
Complexity	Passwords must contain a mix of uppercase letters, lowercase letters, numbers, and special characters	This requirement increases the overall entropy of the password, making it less predictable and more resistant to dictionary attacks where commonly used words and phrases are guessed.

Policy Aspect	Configuration	Reasoning & Explanation
Expiration	Passwords must be renewed every 24 hours	Frequent password changes limit the effective lifespan of any given password, thereby reducing the risk of long-term exploitation if the password is compromised. This approach balances the need for security with user convenience.
History	The system will remember the last 5 passwords used by the user	Implementing a password history policy prevents users from recycling their previous passwords, thereby minimizing the risk of unauthorized access through predictable or familiar combinations.
Lockout	Account will be locked after 3 failed login attempts, with a reset period of 15 minutes	This policy is designed to protect against brute-force attacks by limiting the number of attempts an attacker can make in a short period, while also ensuring that legitimate users are not permanently locked out and can regain access after a short pause.
Folder Access	Only the owners of files and folders can make modifications; all other users are granted read-only access	This restriction is crucial for maintaining data integrity and confidentiality, ensuring that sensitive information cannot be altered by unauthorized individuals while still allowing necessary access for collaboration.
Student Exception	Students are granted access only to their Marks files in a read-only format, with permissions set to disallow any modifications or deletions	This policy is essential for safeguarding the integrity and confidentiality of academic records, ensuring that students have access to their information without the risk of accidental or malicious alterations.

Testing Procedures: In the video demonstration, outline the process for setting up each policy. Provide specific use case scenarios to effectively test the functionality and impact of each policy. For instance, simulate password creation to demonstrate the complexity requirements, and illustrate how the lockout mechanism operates after multiple failed login attempts. This comprehensive approach will emphasize the practical application and importance of these policies in maintaining a secure environment.

4. Video Recording Instructions

Aspect	Detail
Minimum Length	At least **20 minutes**
Content Structure	1. **Introduction & VM Setup**: Show ping tests between machines and Remote Desktop access from Windows XP client and Linux machine into the server. 2. **Disk Partitioning**: Demonstrate creating, shrinking, and extending partitions using Disk Management. 3. **AD/DNS Configuration**: Demonstrate domain join, logging in as domain users on all computers, and removing a client from the domain. 4. **OU/User Creation & Login Restrictions**: Show creating OUs and users, apply login hour and device restrictions. 5. **Shared Folders**: Test permissions from within and outside respective OUs; demonstrate auto-mapped drives. 6. **System Restore & Recuva Recovery**: Create a restore point, delete network drivers, roll back using restore point; create and permanently delete file and folder, recover them using Recuva. 7. **Policy Configurations**: Demonstrate password policies, account lockout, and describe folder permission policies. 8. **Troubleshooting Highlights & Recap**: Simulate failed login attempts causing lockout, then unlock the account explaining the process.
Video Format	- Clear, high-definition screen recording. - Picture-in-picture webcam overlay showing your face. - Clear English voice narration. - Focus on UI elements with zoom and on-screen annotations if possible.
Submission	- Upload the video to **Google Drive**. - Generate a shareable link with appropriate viewing permissions. - Paste the shareable link in the last text field of the **Google Form (https://forms.gle/UHapHdMfpcqKYZrM8)** . - Verify the link is accessible from a different account before submitting. - Invalid or restricted links will be considered non-submission.

Summary Table of Video Section Timing Suggestion

Section	Approximate Duration (minutes)
Introduction & VM Setup	2
Disk Partitioning	2
AD/DNS Demostration	2
OU/User Creation & Restrictions	3
Shared Folders & Permissions	2

Section	Approximate Duration (minutes)
System Restore & Recovery	3
Policy Configurations	3
Troubleshooting & Recap	3
Total	**~20 minutes**

Important Notes

- Follow instructions carefully and document all configuration steps with evidence.
- Ensure that the checked points in the Google Form are clearly demonstrated in the video to avoid mark deductions.
- The video must be a tutorial demonstrating content as if teaching a peer or reporting professionally. It should be in HD, showcasing your screen interface and your face, accompanied by a clear voiceover that explains the content. The video must be a tutorial demonstrating content as if teaching a peer or reporting professionally. It should be in HD, showcasing your screen interface and your face, with a clear voiceover that explains the content. The video should be a demonstrative tutorial as if teaching a peer or reporting professionally, and must be in HD, featuring your screen interface and your face, with a clear voiceover explaining the content.
- Clarity and completeness reflect your command of concepts and communication skills, both critical for IT professionals.

"Dream big and work hard to achieve your goals. Stay strong and keep fighting for your dreams. Do not let anything discourage you; the future looks bright."

Good luck!