# Here is the AI planned result

Course Name: OSYS 1020 Operating Systems Security

Course Outcomes:

1. Articulate the typical hardware components of a computer, and the relationship with the operating system and computer security.

2. Summarize the typical architecture elements of an operating system and its role in controlling computer resources and security.

3. Demonstrate the use of basic operating system shell commands and GUI applications to set up and configure a secure system.

4. Demonstrate approaches to configuring a secure operating system.

5. Document changes and system updates to promote traceability rollback, as needed.

Objectives:

Objective 1:

1. Describe the BIOS, Boot process.

2. Describe typical hardware components and dependencies.

Pros: This objective provides a foundational understanding of computer hardware and its relationship to the operating system. It enables learners to identify potential vulnerabilities and security implications.

Cons: This objective may be too technical for learners who have limited background knowledge in computer hardware.

Objective 2:

1. Describe the layered architecture of modern computer operating systems.

2. Explain file systems: permissions, encryption, sharing.

3. Explain the Principle of Least Privilege.

Pros: This objective provides an understanding of the structure and components of an operating system and how they contribute to security. It also introduces important concepts like permissions, encryption, and the Principle of Least Privilege.

Cons: The objective may require extensive theoretical knowledge and may need additional practical examples to ensure comprehension.

Objective 3:

1. Demonstrate the use of shell commands.

2. Explain and demonstrate creating users.

3. Explain and demonstrate the use of file systems: permissions, encryption, sharing.

4. Demonstrate the Principle of Least Privilege.

Pros: This objective focuses on practical skills and hands-on experience, allowing learners to apply their knowledge to real-world scenarios. It also emphasizes the importance of security practices such as user management and file system security.

Cons: The objective may require learners to have access to a system for hands-on practice, which might not be feasible for all learners.

Objective 4:

1. Explore threats to system security: malware, human engineering, system firewalls.

2. Explore system and patch deployment strategies.

3. Explore system logging services and their use.

4. Document changes and system updates to promote traceability rollback, as needed.

Pros: This objective delves into the practical aspects of securing an operating system, including strategies for threat mitigation, patch management, and system logging. It also highlights the importance of documentation for traceability and rollback purposes.

Cons: The objective may require learners to have a deep understanding of security measures and may be challenging for those with limited technical knowledge.

Objective 5:

1. Document changes and system updates to promote traceability rollback, as needed.

Pros: This objective reinforces the importance of documentation for maintaining a secure operating system environment. It emphasizes the need for accountability and traceability in case of system issues.

Cons: The objective may be repetitive, as it overlaps with Objective 4 in terms of documenting changes and system updates.

Overall, the course objectives provide a comprehensive coverage of operating systems security. They address theoretical knowledge, practical skills, and best security practices. The objectives could benefit from additional clarity and alignment to specific learning activities and assessments to ensure effective instruction and learning.

Based on the course outcomes and objectives, an optimal instructional program for OSYS 1020 Operating Systems Security would include a mix of lectures, hands-on labs, case studies, and assessments. The lectures would cover the theoretical concepts, layered architecture, and security principles. The hands-on labs would provide practical experience with configuring secure systems, using shell commands, and implementing security measures. Case studies and group discussions would allow learners to analyze real-world security threats and devise appropriate solutions. Assessments could include quizzes, lab reports, and a final project that requires learners to document and present a secure system configuration.

Overall, this instructional program would provide a well-rounded learning experience that combines theoretical knowledge and practical skills in operating system security.