UE19CS254: Operating Systems
UNIT 5: Question Bank

	Chapter 13: I/O Systems
1	Explain with a diagram how Direct Memory Access (DMA) technique improves disk I/O performance.
2	Explain in detail the life cycle of an I/O request.
3	How does memory mapped I/O differ from in/out instructions?
4	In most multi-programmed systems, user programs access memory through virtual addresses, while the operating system uses raw physical addresses to access memory. What are the implications of this design for the initiation of I/O operations by the user program and their execution by the operating system?
5	How does DMA increase system concurrency? How does it complicate hardware design?
	Chapter 14: System Protection
6	In a ring-protection system, level 0 has the greatest access to objects, and level n (where n > 0) has fewer access rights. The access rights of a program at a particular level in the ring structure are considered a set of capabilities. What is the relationship between the capabilities of a domain at level j and a domain at level i to an object (for j >i)?
7	What protection problems may arise if a shared stack is used for parameter passing?
8	If all the access rights to an object are deleted, the object can no longer be accessed. At this point, the object should also be deleted, and the space it occupies should be returned to the system. Suggest an efficient implementation of this scheme.
9	Why is it difficult to protect a system in which users are allowed to do their own I/O?

10	Consider a computing environment where a process is given the privilege of accessing an object only n times. Suggest a scheme for implementing this policy.
11	Discuss the strengths and weaknesses of implementing an access matrix using access lists that are associated with objects.
12	Discuss the strengths and weaknesses of implementing an access matrix using capabilities that are associated with domains.
13	Explain the need-to-know principle in the context of system protection requirements. How does it differ from the principle of least privilege?

Chapter 15: System Security

14	What are the four levels where security measures must be taken?
15	What is the most common technique for security attacks?
16	Provide examples of at least three program threats.
17	Provide examples of at least two system and network threats.
16	Buffer-overflow attacks can be avoided by adopting a better programming methodology or by using special hardware support. Discuss these solutions.
17	Make a list of six security concerns for a bank's computer system. Foreach item on your list, state whether this concern relates to physical,human, or operating-system security.
18	What is a distributed denial-of-service attack and how does it work?

Chapter 17: Case Study on Windows

19	List the design goals of Windows. Describe two in detail.
20	How does Windows allocate user memory?
21	Describe the management scheme of the Virtual Memory Manager. How does the VM manager improve performance?
22	Describe the three main architectural layers of the Windows Kernel.