**UNIT I: Information Security and Threats**

**Essay Questions**

1. Define Information Security. Explain the types of information assets and threats to them with examples.
2. Discuss various types of network attacks and their impact with real-time case studies.
3. Explain the fundamentals of Information Security. Describe the principles and concepts of data security.
4. Write a detailed note on Types of Controls and Access Control Models.
5. Explain common vulnerabilities and exposures (CVE) with malware attack case studies.
6. Describe a real-world case study of an organization or system that was impacted by a malware attack. Highlight its causes, impact, and response

**Bit Questions**

* Define information security.
* List different types of worms.
* What are Trojans?
* What is meant by CVE?
* Define Application Security.
* Write two characteristics of critical information.

**UNIT II:**

**Essay Questions**

1. What is data leakage? Explain its classification, location, and pathways.
2. Discuss the different techniques of content awareness and content analysis in data leakage prevention.
3. Explain organisational data protection methods in detail.
4. Write a detailed note on Network Sniffers and Injectors with tools like Tcpdump, Wireshark, Ettercap, Hping.
5. What are filters and qualifiers. Discuss how filters and qualifiers are used in tcpdump with examples

**Bit Questions**

* Define Data Leakage.
* Give two examples of data protection techniques.
* What is content awareness?
* Write full form of Tcpdump.
* Name any two sniffing tools.
* What is the use of Wireshark?