
SECURITY THREATS & VULNERABILITIES**Course Code:** 13CS2209**L P C**
4 0 3**Pre requisites:** Network security**Course Educational Objectives:**

The main objective of this course is that to provide security to various systems by identifying various Types of threats and vulnerabilities.

Course Outcomes:

By the end of the course

1. The Student will gain the knowledge on various security threats and issues and how to overcome those issues.
2. The student will get the capability to handle various attackers and crime issues.
3. Learning various issues involved in threats overcome methods.
4. Learning Forensic analysis and risk analysis.
5. Learn inner security issues involved in mail agents, viruses and worms.

UNIT – I

Introduction: Security threats - Sources of security threats- Motives - Target Assets and Vulnerabilities. Consequences of threats- E-mail threats - Web-threats - Intruders and Hackers, Insider threats, Cyber crimes.

UNIT – II

Network Threats: Active/ Passive – Interference – Interception – Impersonation – Worms – Virus – Spam’s – Ad ware - Spy ware – Trojans and covert channels – Backdoors – Bots - IP Spoofing - ARP spoofing - Session Hijacking - Sabotage-Internal treats- Environmental threats - Threats to Server security.

UNIT – III

Security Threat Management: Risk Assessment - Forensic Analysis - Security threat correlation

– Threat awareness - Vulnerability sources and assessment- Vulnerability assessment tools -

Threat identification - Threat Analysis - Threat Modeling - Model for Information Security Planning.

UNIT – IV

Security Elements: Authorization and Authentication - types, policies and techniques - Security

certification - Security monitoring and Auditing - Security Requirements Specifications - Security Policies and Procedures, Firewalls, IDS, Log Files, Honey Pots

UNIT – V

Access control, Trusted Computing and multilevel security - Security models, Trusted Systems,

Software security issues, Physical and infrastructure security, Human factors – Security awareness, training, Email and Internet use policies.

TEXT BOOKS:

1. Swiderski, Frank and Syndex: “Threat Modeling”, 1st Edition, Microsoft Press, 2004.
2. Joseph M Kizza: “Computer Network Security”, 1st Edition, Springer, 2010.
3. William Stallings and Lawrie Brown: “Computer Security: Principles and Practice”, 2nd Edition Prentice Hall, 2008.

REFERENCES:

1. Lawrence J Fennelly : “Handbook of Loss Prevention and Crime Prevention” 5th Edition, Butterworth-Heinemann,2012.
2. Tipton Ruthbe Rg : “Handbook of Information Security Management”, 6th Edition, Auerbach Publications,2010.
3. Mark Egan : “The Executive Guide to Information Security” , 1st Edition, Addison-Wesley Professional,2004.