# SCHEME OF COURSE WORK

**Course Details:**

| | | | |
|---|---|---|---|
| **Course Title** | **: Security Threats & Vulnerabilities** | | |
| **Course Code** | : 13CS2209 | **L T P C** | **:4 0 0 3** |
| **Program:** | **: M.Tech** | | |
| **Specialization:** | **: Cyber Security** | | |
| **Semester** | **: IInd Semester** | | |
| **Prerequisites** | : Network security | | |
| **Courses to which it is a prerequisite** | **: Forensic Analysis, Risk Analysis** | | |

**Course Outcomes (COs):**

| | |
|---|---|
| 1 | Various security threats and issues and how to overcome those issues. |
| 2 | Capability to handle various attackers and crime issues. |
| 3 | Learning various issues involved in threats overcome. |
| 4 | Learning Forensic analysis and risk analysis. |
| 5 | Learn inner security issues involved in mail agents, viruses and worms. |

**Program Outcomes (POs):**

A graduate of Cyber Security Specialization will be able to

| | |
|---|---|
| 1 | Understand what are the common threats faced today. |
| 2 | The foundational theory behind Cyber security. |
| 3 | The basic principles and techniques when designing a secure system. |
| 4 | How to think adversarial, how today's attacks and defenses work in practice, how to assess threats for their significance, and how to gauge the protections and limitations provided by today's technology. |
| 5 | Learn various security methodologies to enhance the security of web. |
| 6 | Basic principles of cyber laws and security policies. |
| 7 | Various scripting languages to develop programs for security mechanisms. |
| 8 | Various tools and methodologies to analyze the various cyber crimes. |
| 9 | Secure protocols inner mechanisms and their practical implementation. |
| 10 | Various Forensic technologies and methodologies for security measurements analization. |
| 11 | Intrusion detection techniques and image model security aspects in Android application developments. |

**Course Outcome** versus **Program Outcomes:**

| COs | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO8 | PO9 | PO10 | PO11 | PO12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CO-1** | | | S | | | S | | | | | | |
| **CO-2** | M | M | S | | | | | | | S | | M |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CO-3** | | | M | | | | | | | S | | M |
| **CO-4** | | S | | S | | | | | | | | |
| **CO-5** | | | | | | | | | | | | S |

*S* - Strongly correlated, *M* - *Moderately* correlated, *Blank* - *No correlation*

| **Assessment Methods:** | Assignment / Quiz / Seminar / Case Study / Mid-Test / End Exam |
|---|---|

## Teaching-Learning and Evaluation

| **Week** | **TOPIC / CONTENTS** | **Course Outcomes** | **Sample questions** | **TEACHING-LEARNING STRATEGY** | **Assessment Method & Schedule** |
|---|---|---|---|---|---|
| 1 | Introduction: Security threats - Sources of security threats. | CO-1 | 1.EXplain various types of security Threats.<br>2.What are the sources of security Threats. | ▫ Lecture/Discussion | Assignment (Week 3 - 4) |
| 2 | Motives - Target Assets and Vulnerabilities. | CO-1 | 1.Explain the target assets of Security threats. | ▫ Lecture / Discussion | Mid-Test 1 (Week 9) |
| 3 | Consequences of threats- E-mail threats - Web-threats. | CO-2 | 1.Explain about E-mail threats & Web threats. | ▫ Lecture/Discussion | Seminar (Week 3 - 6) |
| 4 | Intruders and Hackers, Insider threats, Cyber crimes. | CO-3,CO-4 | 1.Define Intruders & hackers. Explain Insider threats.<br>2.Explain Cyber crimes. | | |
| 5 | Network Threats: Active/ Passive – Interference – Interception – Impersonation. | CO-3 | 1.Explain Active & Passive attacks With examples. | | |
| 6 | Worms – Virus – Spam's – Ad ware - Spy ware – Trojans and covert channels. | CO-3,CO-4 | 1.Difference between worm and Virus. Explain Ad ware and Spy ware.<br>2.Explain Trojans and Covert Channels. | | |
| 7 | Backdoors – Bots – IP Spoofing - ARP spoofing - Session Hijacking – Sabotage. | C0-4 | 1.Difference between IP spoofing and ARP spoofing.<br>2.Explain about Session Hijacking. | | |
| 8 | Internal treats- Environmental threats - Threats to Server security. | CO-4 | 1.Differentiate Internal threats And Environmental threats with Examples. | | |
| **9** | **Mid-Test 1** | CO-1,CO-2 | | | |

| | | | | | |
|---|---|---|---|---|---|
| 10 | Security Threat Management: Risk Assessment - Forensic Analysis - Security threat correlation. | CO-3 | 1.Explain Risk assessment and Forensic analysis.<br>2.Explain Security threat Correlation. | ▫ Lecture<br>▫ Discussion | Mid-Test 2 (Week 18) |
| 11 | Threat awareness - Vulnerability sources and assessment- Vulnerability assessment tools. | CO-3 | 1.Explain Vulnerability assessment Tools. | | Seminar (Week 10 - 15) |
| 12 | Threat identification - Threat Analysis - Threat Modeling - Model for Information Security Planning. | CO-3 | 1.Explain Threat identification and Threat analysis. | | |
| 13 | Security Elements: Authorization and Authentication - types, policies and techniques – Security certification. | CO-3 | 1.Explain Authorization and Authentication.<br>2.Explain about Security Certification. | | |
| 14 | Security monitoring and Auditing - Security Requirements Specifications. | CO-5 | 1.Explain about security Monitoring & auditing. | | |
| 15 | Security Policies and Procedures, Firewalls, IDS, Log Files, Honey Pots. | CO-5 | 1.Explain about Honey pots.<br>2.Explain security policies & Procedures. | | |
| 16 | Access control, Trusted Computing and multilevel security - Security models, Trusted Systems, Software security issues. | CO-5 | 1.Explain multilevel security.<br>2.What are the Software security Issues.? Explain. | | |
| 17 | Physical and infrastructure security, Human factors – Security awareness, training, Email and Internet use policies. | CO-5 | 1.Explain E-mail and Internet use Policies. | | |
| **18** | **Mid-Test 2** | | | | |
| **19/20** | **END EXAM** | | | | |