Shree Rahul Education Society's (Regd.)
SHREE L. R. TIWARI COLLEGE OF ENGINEERING
An Autonomous Institute Affiliated to University of Mumbai,
Approved by AICTE & DTE, Maharashtra State | NAAC Accredited, NBA Accredited Program | ISO 9001:2015 Certified |
DTE Code No: 3423 | Recognized under Section 2(f) of the UGC Act 1956 | Minority Status (Hindi Linguistic)

# Department of Bachelor of Vocational Studies.
# Curriculum FY to B. Voc Cyber Security and Digital Forensics for A.Y 2025-26

## First Year to Final Year Syllabus

## Prepared by: Board of Studies for Computer Engineering

## Approved By: Academic Council of Shree L.R. Tiwari College of Engineering

## R-2025

## PREAMBLE

**"Think. Design. Innovate. – Learning that Leads the Future."**

SLRTCE is proud to be among the youngest institutions to attain academic autonomy—an achievement that strengthens our commitment to becoming a world-class center for socio- economic development and quality education. It is with great pride and purpose that we introduce the restructured curriculum under academic autonomy at SLRTCE. This initiative marks a significant step toward transforming engineering education by equipping our graduates with strong technical foundations, research acumen, interdisciplinary perspective, and an innovation-driven mindset essential for success in today's evolving professional landscape.

1. **Curriculum Design:** The curriculum design is based on The National Skills Qualifications Framework (NSQF). NSQF in India is a ten-level structure that distinctly integrates both a General Component, covering foundational subjects like communication and IT skills, and a Skill Component, focused on vocational training aligned with industry-specific Qualification Packs (QPs) and National Occupational Standards (NOSs).
2. **Purpose of Autonomy: Empowering Innovation and Real-World Learning** Our pursuit of autonomy is rooted in bridging the gap between academic learning and industry relevance. By integrating undergraduate research through the **On Job Training**—our dedicated innovation and problem-solving hub—students engage with real-world challenges, apply interdisciplinary knowledge, and develop socially impactful solutions. This approach nurtures engineers who are not only technically sound but also responsible and creative thinkers.
3. **Alignment with National Education Policy-2020** Aligned with NEP 2020, the curriculum emphasizes multidisciplinary, hands-on learning. Through theme-based projects, electives, value-added courses, and flexible assessments, SLRTCE ensures holistic student development driven by real-world application and academic rigor. SLRTCE, as a part of Rahul Education, benefits from being in a network of HEIs. All Higher Education Institutions under Rahul Education can collectively contribute to curriculum development, promoting multidisciplinary studies.
4. **About General Component and Skill Component:**

This focuses on **foundational knowledge and transferable skills**, often aligned with **general education goals**. Such as cognitive, communication and analytical abilities. Usually constitutes **30–40% of the total credit load. Skill Component** is aligned to **industry-specific job roles** based on **Qualification Packs (QPs)** developed by Sector Skill Councils (SSCs). Makes up **60–70% of the total credits**— emphasizing hands-on skill acquisition

5. **Empowering Faculty as Mentors and Innovators** SLRTCE believes that the success of academic autonomy lies in the hands of its faculty. By empowering educators to think beyond conventional boundaries, we enable them to instill Knowledge, Skills, and Attitudes (KSA) in students while enriching their own professional growth. Faculty serve as research mentors and project guides, supported through structured training in innovation pedagogy and assessment.

Sincerely,

**IQAC Chairperson** Chief Operating Officer

*Shree L. R. Tiwari College of Engineering* Rahul Education

## Contents

## A. Abbreviations

| | |
|---|---|
| G | General Education Component |
| S | Skill C |
| AEC | Ability Enhancement Course |
| AU | Audit Course |
| BSC | Basic Science Course including Mathematics |
| BSC-LC | Basic Science Laboratory Course |
| ELC | Experiential Learning Course |
| ESC | Engineering Science Course |
| ESC-LC | Engineering Science Laboratory Course |
| HSSM | Humanities Social Sciences and Management Course |
| IKS | Indian Knowledge System Course |
| INTR | Internship |
| L | Lecture |
| LC | Laboratory Course |
| LLC | Liberal Learning Course |
| MDM | Multidisciplinary Minor Course |
| MJP | Major project |
| MP | Mini Project |
| OE | Open Elective Course |
| P | Practical |
| PCC | Program Core Course |
| PE | Program Elective Course |
| SBL | Skill Based Laboratory |
| SEC | Skill Enhancement Course |
| T | Tutorial |
| VEC | Value Education Course |

**B. Voc (CSDF) Curriculum Structure**

**Program Structure for First Year B. Voc Cyber Security and Digital Forensics**

**UNIVERSITY OF MUMBAI (With Effect from 2024-2025) Semester I**

| Course Code | Course Name | Teaching Scheme (Contact Hours) | | | Credits Assignec | | | |
|---|---|---|---|---|---|---|---|---|
| | | Theory | Pract. | Tut. | Theory | Pract. | Tut. | Total |
| **General Education Component** | | | | | | | | |
| 21101 | Professional Skill-I (Soft Skill Development) | 2 | - | 1* | 2 | -- | 1 | 3 |
| 21102 | Applied Mathematics | 2 | - | 1* | 2 | -- | 1 | 3 |
| 21103 | Programming principles with C | | 2*+2 | - | – | 2 | -- | 2 |
| | **Total** | **4** | **4** | **2** | **4** | **2** | **2** | **8** |
| **Skill Component** | | | | | | | | |
| 21104 | Computer Networks | 3 | 2 | - | 3 | 1 | -- | 4 |
| 21105 | Cybersecurity Fundamentals | 3 | 2 | - | 3 | 1 | -- | 4 |
| 21106 | Operating System and Network Security | 3 | 2 | - | 3 | 1 | -- | 4 |
| 21107 | On Job Training/ Skill based Internship | - | 80 | - | -- | 2 | -- | 2 |
| | **Total** | **9** | **86** | **--** | **9** | **5** | **--** | **14** |
| **Grand Total** | | **13** | **90** | **2** | **13** | **7** | **2** | **22** |

| Course Code | Course Name | Examination Scheme | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Theory | | | | | Term Work | Pract. &oral | Total |
| | | Internal Assessment | | | End Sem. Exam | Exam. Duration (in Hrs) | | | |
| | | IAT-I | IAT-II | Total (IAT-I) + IAT-II) | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **General Education Component** | | | | | | | | | |
| 21101 | Professional Skill-I (Soft Skill Development) | 20 | 20 | 40 | 60 | 02 | 25 | -- | 125 |
| 21102 | Applied Mathematics | 20 | 20 | 40 | 60 | 02 | 25 | -- | 125 |
| 21103 | Programming principles with C | - | - | - | - | - | 25 | 25 | 50 |
| **Skill Component** | | | | | | | | | |
| 21104 | Computer Networks | 20 | 20 | 40 | 60 | 02 | 25 | 25 | 150 |
| 21105 | Cybersecurity Fundamentals | 20 | 20 | 40 | 60 | 02 | 25 | 25 | 150 |
| 21106 | Operating System and Network Security | 20 | 20 | 40 | 60 | 02 | 25 | 25 | 150 |
| 21107 | On Job Training/ Skill based Internship | -- | -- | -- | -- | -- | 50# | -- | 50 |
| **Total** | | **--** | **--** | **200** | **300** | -- | **200** | **100** | **800** |

* Two hours of practical class to be conducted for full class as demo/discussion.

# Indicates Practical and Oral Marks includes report and presentation.

2 Credits for 2 weeks or 80 hrs during semester or after semester-(AICTE Internship Polity)

**Program Structure for First Year B. Voc Cyber Security and Digital Forensics**
**UNIVERSITY OF MUMBAI (With Effect from 2024-2025)**

## Semester II

| **Course Code** | **Course Name** | **Teaching Scheme (Contact hours)** | | | **Credits Assigned** | | | |
|---|---|---|---|---|---|---|---|---|
| | | **Theory** | **Pract.** | **Tut.** | **Theory** | **Pract.** | **Tut.** | **Total** |
| **General Education Component** | | | | | | | | |
| 21201 | Professional Skill-II (Business communication Ethics) | 2 | - | 1* | 2 | -- | 1 | 3 |
| 21202 | Statistics for Data Science | 2 | - | 1* | 2 | -- | 1 | 3 |
| 21203 | Indian Knowledge System (IKS) | 2 | - | - | 2 | - | -- | 2 |
| | **Total** | **6** | **0** | **2** | **6** | **0** | **2** | **8** |
| **Skill Component** | | | | | | | | |
| 21204 | Python Programming | 2 | 4 | - | 2 | 2 | -- | 4 |
| 21205 | Web Application Security | 3 | 2 | - | 3 | 1 | -- | 4 |
| 21206 | Database Management and Security | 3 | 2 | - | 3 | 1 | -- | 4 |
| 21207 | Skill based Internship | - | 80 | - | -- | 2 | -- | 2 |
| | **Total** | **8** | **88** | **--** | **8** | **7** | **--** | **14** |
| **Grand Total** | | **14** | **88** | **2** | **14** | **7** | **2** | **22** |

| **Course** | | **Examination Scheme** | | | |
|---|---|---|---|---|---|
| | | **Theory** | **Term Work** | **Pract. &oral** | **Total** |

| Code | Course Name | Internal Assessment | | | End Sem. Exam | Exam. Duration (in Hrs) | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | IAT-I | IAT-II | Total (IAT-I) + IAT-II) | | | | | |
| **General Education Component** | | | | | | | | | |
| 21201 | Professional Skill-II (Business communication Ethics) | 20 | 20 | 40 | 60 | 02 | 25 | -- | 125 |
| 21202 | Statistics for Data Science | 20 | 20 | 40 | 60 | 02 | 25 | -- | 125 |
| 21203 | Indian Knowledge System (IKS) | - | - | - | - | - | 25 | 25 | 50 |
| **Skill Component** | | | | | | | | | |
| 21204 | Python Programming | 20 | 20 | 40 | 60 | 02 | 25 | 25 | 150 |
| 21205 | Web Application Security | 20 | 20 | 40 | 60 | 02 | 25 | 25 | 150 |
| 21206 | Database Management and Security | 20 | 20 | 40 | 60 | 02 | 25 | 25 | 150 |
| 21207 | Skill based Internship | -- | -- | -- | -- | -- | 50# | -- | 50 |
| **Total** | | **--** | **--** | **200** | **300** | **--** | **200** | **100** | **800** |

* Two hours of practical class to be conducted for full class as demo/discussion.

# Indicates Practical and Oral Marks includes report and presentation.

2 Credits for 2 weeks or 80 hrs during semester or after semester-(AICTE Internship Polity)

## Program Structure for Second Year B. Voc Cyber Security and Digital Forensics
## UNIVERSITY OF MUMBAI (With Effect from 2023-2024)
## Semester III

| Course Code | Course Name | Teaching Scheme (Contact Hours) | | | Credits Assigned | | | |
|---|---|---|---|---|---|---|---|---|
| | | **Theory** | **Pract.** | **Tut.** | **Theory** | **Pract.** | **Tut.** | **Total** |
| **General Education Component** | | | | | | | | |
| 21301 | Professional Skill-III (Entrepreneurship) | 2 | - | 1* | 2 | -- | 1 | 3 |
| 21302 | Ethical Hacking | 2 | - | 1* | 2 | -- | 1 | 3 |
| 21303 | Cyber Threat Intelligence | 2 | - | - | 2 | - | -- | 2 |
| | **Total** | **6** | **0** | **2** | **6** | **0** | **2** | **8** |
| **Skill Component** | | | | | | | | |
| 21304 | Cybersecurity Risk Management and Auditing | 3 | 2 | | 3 | 1 | -- | 4 |
| 21305 | Malware Analysis and Reverse Engineering | 3 | 2 | _ | 3 | 1 | -- | 4 |
| 21306 | Machine Learning I | 3 | 2 | - | 3 | 1 | -- | 4 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 21307 | Skill based Internship | - | 80 | - | -- | 2 | -- | 2 |
| | **Total** | **9** | **86** | **--** | **9** | **5** | **--** | **14** |
| **Grand Total** | | **15** | **86** | **2** | **15** | **5** | **2** | **22** |

| **Course Code** | **Course Name** | **Examination Scheme** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | **Theory** | | | | | **Term Work** | **Pract. &oral** | **Total** |
| | | **Internal Assessment** | | | **End Sem. Exam** | **Exam. Duration (in Hrs)** | | | |
| | | IAT-I | IAT-II | Total (IAT-I) + IAT-II) | | | | | |
| **General Education Component** | | | | | | | | | |
| 21301 | Professional Skill-III (Entrepreneurship) | 20 | 20 | 40 | 60 | 02 | 25 | -- | 125 |
| 21302 | Ethical Hacking | 20 | 20 | 40 | 60 | 02 | 25 | -- | 125 |
| 21303 | Cyber Threat Intelligence | - | - | - | - | - | 25 | 25 | 50 |
| **Skill Component** | | | | | | | | | |
| 21304 | Cybersecurity Risk Management and Auditing | 20 | 20 | 40 | 60 | 02 | 25 | 25 | 150 |
| 21305 | Malware Analysis and Reverse Engineering | 20 | 20 | 40 | 60 | 02 | 25 | 25 | 150 |
| 21306 | Machine Learning I | 20 | 20 | 40 | 60 | 02 | 25 | 25 | 150 |
| 21307 | Skill based Internship | -- | -- | -- | -- | -- | 50# | -- | 50 |
| **Total** | | **--** | **--** | **200** | **300** | **--** | **200** | **100** | **800** |

* Two hours of practical class to be conducted for full class as demo/discussion.

\# Indicates Practical and Oral Marks includes report and presentation.

2 Credits for 2 weeks or 80 hrs during semester or after semester-(AICTE Internship Polity)

## Program Structure for Second Year B. Voc Cyber Security and Digital Forensics
## UNIVERSITY OF MUMBAI (With Effect from 2023-2024)
## Semester IV

| **Course Code** | **Course Name** | **Teaching Scheme (Contact Hours)** | | | **Credits Assigned** | | | |
|---|---|---|---|---|---|---|---|---|
| | | **Theory** | **Pract.** | **Tut.** | **Theory** | **Pract.** | **Tut.** | **Total** |
| **General Education Component** | | | | | | | | |
| 21401 | Professional Skill-IV (Aptitude and Logic Building) | 2 | – | - | 2 | – | -- | 2 |
| 21402 | Security Architecture and Engineering | 2 | - | 1* | 2 | -- | 1 | 3 |
| 21403 | Digital Forensics | 2 | - | 1* | 2 | -- | 1 | 3 |
| | **Total** | **6** | **0** | **2** | **6** | **0** | **2** | **8** |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Skill Component** | | | | | | | | |
| 21404 | Penetration Testing and Vulnerability Assessment | 3 | 2 | | 3 | 1 | -- | 4 |
| 21405 | Cybercrime Investigation Techniques | 3 | 2 | _ | 3 | 1 | -- | 4 |
| 21406 | Network Forensics | 3 | 2 | - | 3 | 1 | -- | 4 |
| 21407 | Skill based Internship | - | 80 | - | -- | 2 | -- | 2 |
| | **Total** | **9** | **86** | **--** | **9** | **5** | **--** | **14** |
| **Grand Total** | | **15** | **86** | **2** | **15** | **5** | **2** | **22** |

| **Course Code** | **Course Name** | **Examination Scheme** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | **Theory** | | | | | **Term Work** | **Pract. &oral** | **Total** |
| | | **Internal Assessment** | | | **End Sem. Exam** | **Exam. Duration (in Hrs)** | | | |
| | | IAT-I | IAT-II | Total (IAT-I) + IAT-II) | | | | | |
| **General Education Component** | | | | | | | | | |
| 21401 | Professional Skill-IV (Aptitude and Logic Building) | - | - | - | - | - | 25 | 25 | 50 |
| 21402 | Security Architecture and Engineering | 20 | 20 | 40 | 60 | 02 | 25 | -- | 125 |
| 21403 | Digital Forensics | 20 | 20 | 40 | 60 | 02 | 25 | -- | 125 |
| **Skill Component** | | | | | | | | | |
| 21404 | Penetration Testing and Vulnerability Assessment | 20 | 20 | 40 | 60 | 02 | 25 | 25 | 150 |
| 21405 | Cybercrime Investigation Techniques | 20 | 20 | 40 | 60 | 02 | 25 | 25 | 150 |
| 21406 | Network Forensics | 20 | 20 | 40 | 60 | 02 | 25 | 25 | 150 |
| 21407 | Skill based Internship | -- | -- | -- | -- | -- | 50# | -- | 50 |
| **Total** | | **--** | **--** | **200** | **300** | **--** | **200** | **100** | **800** |

* Two hours of practical class to be conducted for full class as demo/discussion.

# Indicates Practical and Oral Marks includes report and presentation.

2 Credits for 2 weeks or 80 hrs during semester or after semester-(AICTE Internship Polity)

**Program Structure for Third Year B. Voc Cyber Security and Digital Forensics UNIVERSITY OF MUMBAI (With Effect from 2023-2024)**

## Semester V

| **Course Code** | **Course Name** | **Teaching Scheme (Contact Hours)** | | | **Credits Assigne** | | | |
|---|---|---|---|---|---|---|---|---|
| | | **Theory** | **Pract.** | **Tut.** | **Theory** | **Pract.** | **Tut.** | **Total** |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **General Education Component** | | | | | | | | |
| 21501 | Professional Skill-IV (Cloud Forensics) | 2 | - | 1* | 2 | -- | 1 | 3 |
| 21502 | Environmental Management | 2 | - | - | 2 | -- | 1 | 3 |
| 21503 | Cyber Security Laws | 2 | - | 1* | 2 | - | -- | 2 |
| | **Total** | **6** | **0** | **2** | **6** | **0** | **2** | **8** |
| **Skill Component** | | | | | | | | |
| 21504 | Blockchain Forensics and Crypto-currency Investigation | 3 | 2 | | 3 | 1 | -- | 4 |
| 21505 | Ransomware Investigation | 3 | 2 | _ | 3 | 1 | -- | 4 |
| 21506 | Mobile Security and Forensics | 3 | 2 | - | 3 | 1 | -- | 4 |
| 21507 | Skill based Internship | - | 80 | - | -- | 2 | -- | 2 |
| | **Total** | **9** | **86** | **--** | **9** | **5** | **--** | **14** |
| **Grand Total** | | **15** | **86** | **2** | **15** | **5** | **2** | **22** |

| **Course Code** | **Course Name** | **Examination Scheme** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | **Theory** | | | | | **Term Work** | **Pract. &oral** | **Total** |
| | | **Internal Assessment** | | | **End Sem. Exam** | **Exam. Duration (in Hrs)** | | | |
| | | IAT-I | IAT-II | Total (IAT-I) + IAT-II) | | | | | |
| **General Education Component** | | | | | | | | | |
| 21501 | Professional Skill-IV (Cloud Forensics) | 20 | 20 | 40 | 60 | 02 | 25 | -- | 125 |
| 21502 | Environmental Management | - | - | - | - | - | 25 | 25 | 50 |
| 21503 | Cyber Security Laws | 20 | 20 | 40 | 60 | 02 | 25 | -- | 125 |
| **Skill Component** | | | | | | | | | |
| 21504 | Blockchain Forensics and Crypto-currency Investigation | 20 | 20 | 40 | 60 | 02 | 25 | 25 | 150 |
| 21505 | Ransomware Investigation | 20 | 20 | 40 | 60 | 02 | 25 | 25 | 150 |
| 21506 | Mobile Security and Forensics | 20 | 20 | 40 | 60 | 02 | 25 | 25 | 150 |
| 21507 | Skill based Internship | -- | -- | -- | -- | -- | 50# | -- | 50 |
| **Total** | | **--** | **--** | **200** | **300** | **--** | **200** | **100** | **800** |

* Two hours of practical class to be conducted for full class as demo/discussion.

\# Indicates Practical and Oral Marks includes report and presentation.

2 Credits for 2 weeks or 80 hrs during semester or after semester-(AICTE Internship Polity)

**Program Structure for Third Year B. Voc Cyber Security and Digital Forensics**
**UNIVERSITY OF MUMBAI (With Effect from 2023-2024)**

# Semester VI

| Course Code | Course Name | Teaching Scheme (Contact Hours) | | | Credits Assigned | | | |
|---|---|---|---|---|---|---|---|---|
| | | Theory | Pract. | Tut. | Theory | Pract. | Tut. | Total |
| **General Education Component** | | | | | | | | |
| 21601 | Professional Skill-IV (API Pentesting) | 2 | - | 1* | 2 | -- | 1 | 3 |
| 21602 | Information Retrieval System | 2 | - | 1* | 2 | -- | 1 | 3 |
| 21603 | Distributed Computing | 2 | - | - | 2 | - | -- | 2 |
| | **Total** | **6** | **–** | **2** | **6** | – | **2** | **8** |
| **Skill Component** | | | | | | | | |
| 21604 | Cloud Computing Security | 3 | 2 | | 3 | 1 | -- | 4 |
| 21605 | Machine Learning II | 3 | 2 | _ | 3 | 1 | -- | 4 |
| 21606 | Security information and Event Management. | 3 | 2 | - | 3 | 1 | -- | 4 |
| 21607 | Skill based Internship | - | 80 | - | -- | 2 | -- | 2 |
| | **Total** | **9** | **86** | **--** | **9** | **5** | **--** | **14** |
| **Grand Total** | | **15** | **86** | **2** | **15** | **5** | **2** | **22** |

| Course Code | Course Name | Examination Scheme | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Theory | | | | | Term Work | Pract. &oral | Total |
| | | Internal Assessment | | | End Sem. Exam | Exam. Duration (in Hrs) | | | |
| | | IAT-I | IAT-II | Total (IAT-I) + IAT-II) | | | | | |
| **General Education Component** | | | | | | | | | |
| 21601 | Professional Skill-IV (API Pentesting) | - | - | - | - | - | 25 | 25 | 50 |
| 21602 | Information Retrieval System | 20 | 20 | 40 | 60 | 02 | 25 | -- | 125 |
| 21603 | Distributed Computing | 20 | 20 | 40 | 60 | 02 | 25 | -- | 125 |
| **Skill Component** | | | | | | | | | |
| 21604 | Cloud Computing Security | 20 | 20 | 40 | 60 | 02 | 25 | 25 | 150 |
| 21605 | Machine Learning II | 20 | 20 | 40 | 60 | 02 | 25 | 25 | 150 |
| 21606 | Security information and Event Management. | 20 | 20 | 40 | 60 | 02 | 25 | 25 | 150 |
| 21607 | Skill based Internship | -- | -- | -- | -- | -- | 50# | -- | 50 |
| **Total** | | **--** | **--** | **200** | **300** | **--** | **200** | **100** | **800** |

* Two hours of practical class to be conducted for full class as demo/discussion.

\# Indicates Practical and Oral Marks includes report and presentation.

2 Credits for 2 weeks or 80 hrs during semester or after semester-(AICTE Internship Polity)

## (Fourth Year) SEMESTER VII
## B. Voc Cyber Security and Digital Forensics with Honor degree

| Course Code | Course Title | Teaching Scheme (Contact Hours) | | | | EVALUATION SCHEME | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | L | T | P | Credit | Test1 | Test2 | Total | End Sem Exam | Exam duration in hrs. | Term Work | Practical Exam | Total |
| 21701 | Research based Project | - | - | 300 | 10 | - | - | - | - | - | 50 | 100 | 150 |
| 21702 | Industry based Project | | | 300 | 10 | | | | | | | | |
| | **TOTAL** | **-** | | 600 | 20 | **-** | **-** | **-** | **-** | **-** | **50** | **100** | **150** |

## (Fourth Year) SEMESTER VIII
## B. Voc Cyber Security and Digital Forensics with Honor degree

| Course Code | Course Title | Teaching Scheme (Contact Hours) | | | | EVALUATION SCHEME | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | L | T | P | Credit | Test 1 | Test 2 | Total | End Sem Exam | Exam duration in hrs. | Term Work | Practical Exam | Total |
| 21801 | On Job Training | - | - | 600 | 20 | - | - | - | - | - | 50 | 100 | 150 |
| | **TOTAL** | **-** | | 600 | 20 | | | | | | **50** | **100** | **150** |

| Course Code: | Course Title | Credit |
|---|---|---|
| 21101 | Professional Skill-I (Soft Skill Development) | 3 |

**Prerequisite: No Prerequisite**

| Course Objectives: | |
|---|---|
| 1 | To develop effective communication skills (spoken and written). |
| 2 | To develop effective presentation skills. |
| 3 | To conduct effective business correspondence and prepare business reports which produce results. |
| 4 | To become self-confident individuals by mastering interpersonal skills, team management skills, and leadership skills |
| **Course Outcomes:** | |
| 1 | To understand effective communication skills (spoken and written). |
| 2 | To apply effective presentation skills. |
| 3 | To understand effective business correspondence and prepare business reports which produce results. |
| 4 | To implement soft skills for self-confident individuals by mastering inter-personal skills, team management skills, and leadership skills. |
| 5 | To develop all-round personalities with a mature outlook to function effectively in different circumstances. |
| 6 | To develop broad career plans, evaluate the employment market, identify the organizations to get good placement, match the job requirements and skill sets. |

| Module | | Content | Hrs |
|---|---|---|---|
| **1** | | **Mechanics of Communication** | **8** |
| | 1.1 | Concept and Meaning: Etymology, Definition and Process of Communication. Barriers: Linguistic, Semantic, Personal, Socio-Psychological, Physical, Environmental, Mechanical, Cross-Cultural | |
| | 1.2 | Methods of Communication: Verbal Non- Verbal Communication<br>Networks of communications: Understanding Organizational Communication. | |
| **2** | | **Mastering Language Skills** | **8** |
| | 2.1 | Listening: Types of Listening; Process of Listening; Hearing and Listening; Exercises on Listening Skill (Video/ Audio)<br>Speaking: Art of Public Speaking; Activities on Speaking Skill. | |
| | 2.2 | Reading: Concept and Types of Reading, Reading Newspaper articles, Fiction and Non-fiction works; Activities on Reading<br>Writing: Principles; Business Correspondence: Elements, Types and Formats of Letter | |
| **3** | | **Presentation Skills** | **8** |
| | 3.1 | Meaning, Importance and Structure of presentations.<br>Use of ICT tools in presentations. (Various applications like Excel, Word, Flipgrid, Nearpod etc.) | |
| | 3.2 | Effective presentation traits (Verbal-Nonverbal)<br>Types of presentations/ Prezi/MS PPT 1`<br>PDCA of presentation | |
| **4** | | **Written Communication** | **6** |
| | 4.1 | Parts of Speech; Phrases and Clauses<br>Sentence Structures; Types of Sentences<br>Editing and Proofreading: Common Errors in English | |

| | | | |
|---|---|---|---|
| | 4.2 | Comprehension and Summarization Paraphrasing and Précis Writing: Exercises | |
| | | **Total** | **30** |

| **Textbooks:** | |
|---|---|
| 1 | Michael Swan, ***"Practical English Usage, Principles and Practice"***, 4th Edition, OUP, 1995. |
| 2 | F.T. Wood, ***"Remedial English Grammar"***, Macmillan,2007 |
| 3 | William Zinsser,***"On Writing Well"*** Harper Resource Book 25th Anniversary Edition 2001 |

| **Referecebooks:** | |
|---|---|
| 1 | Liz Hamp- Lyons and Ben Heasly, ***"Study Writing",*** Cambridge University Press 2nd Edition 2006 |
| 2 | Sanjay Kumar and Pushp Lata, ***"Communication Skills",*** OUP 1st Edition 2011 |
| 3 | CIEFL, ***"Exercises in Spoken English Parts. I-III",*** 1997 Edition University Press, |

| **Assessment:** | |
|---|---|
| **Internal Assessment:** | |
| Assessment consists of two class tests of 20 marks each. The first class test is to be conducted when approx. 40% syllabus is completed and second class test when additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| **End Semester Theory Examination:** | |
| 1 | Question paper will comprise of total six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only Four question need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mention in the syllabus. |

| **Useful Links** | |
|---|---|
| 1 | https://www.coursera.org/learn/speak-english- professionally. |
| 2 | https://nptel.ac.in/courses/109/106/109106129/ |

**List of Tutorial:**

| **Tutorial Number** | **Tutorial Topic** |
|---|---|
| 1 | Introduction to communication, emotional intelligence |
| 2 | Public Speaking (Practice1) Social |
| 3 | Public Speaking (Practice 2) Technical |

| | |
|---|---|
| 4 | Public Speaking (Practice 3)<br>Extempore |

| | |
|---|---|
| 5 | Activities based on Basic Language Skills. |
| 6 | Perform the tutorial on Writing Skills |
| 7 | Perform the tutorial on Reading Skills |
| 8 | Perform the tutorial on Speaking Skills |
| 9 | Perform the tutorial on Listening Skills |
| 10 | Perform the tutorial on Presentation Practice-I |
| 11 | Perform the tutorial on Presentation Practice-II |
| 12 | Perform the tutorial on Presentation Practice-III |
| 13 | Perform the tutorial on Presentation Practice-IV |

| Course Code: | Course Title | Credit |
|---|---|---|
| 21102 | Applied Mathematics | 3 |

| | |
|---|---|
| **Prerequisite: No Prerequisite** | |
| **Course Objectives:** | |
| 1 | To cultivate clear thinking and creative problem solving. |
| 2 | To Thoroughly prepare for the mathematical aspects of other Computer Engineering courses |
| 3 | To provide detailed of matrices which is applied for solving system of linear equations and useful in various fields of technology. |
| 4 | To understand Matrix algebra for solving engineering problems. |
| 5 | To obtain knowledge of Linear and Non-linear programming problems of optimization. |
| **Course Outcomes: On successful completion of course, learner will be able to** | |
| 1 | To Understand the notion of mathematical thinking, mathematical proofs and to apply them in problem solving. |
| 2 | Apply his ability to reason logically. |
| 3 | Apply the knowledge of matrices to solve the problems. |
| 4 | Define subspace of a vector space |
| 5 | Discuss how those matrices change when the bases are changed and Define the kernel of a linear transformation |
| 6 | To find the optimal set of factors that best predict the outcome. |

| Module | | Content | Hrs |
|---|---|---|---|
| **1** | | **Set Theory and Proofing Techniques** | **8** |
| | 1.1 | Definition of Sets, Venn Diagrams, complements, Cartesian products, power sets, counting principle, cardinality and accountability (Countable and Uncountable sets) | |
| | 1.2 | Laws of set theory, Power set and Products Partitions of sets, The Principle of Inclusion and Exclusion. | |
| | 1.3 | Pigeonhole Principle. | |
| **2** | | **Relation and Functions** | 8 |
| | 2.1 | Relation: Definition, types of relation, composition of relations, pictorial representation of relation (Digraphs), properties of relation, partial ordering relation. Operations on relations, Closures. | |
| | 2.2 | Function: Definition and types of function, composition of functions, Recursive and recursively defined functions, Generating Functions. | |
| **3** | | **Matrices** | **7** |

| | | | |
|---|---|---|---|
| | 3.1 | Rank of a matrix, Row Echelon form, System of linear algebraic equations, | |
| | 3.2 | Eigenvalues, eigenvectors, Caley Hamilton theorem, | |
| | 3.3 | Diagonalization of matrix, Orthogonal transformation, Gram- Schmidt orthogonalization. | |
| **4** | | **Linear algebra** | **7** |
| | 4.1 | Vector space- Examples and Properties,<br>Subspaces-criterion for a subset to be a subspace, linear span of a set, linear combination, linear independent and dependent subsets | |
| | | **Total** | **30** |

| **Textbooks:** | |
|---|---|
| 1 | C. L. Liu and D. P. Mohapatra: *Elements of Discrete Mathematics,* McGraw Hill, Revised Second Edition |
| 2 | K. Hoffmann and R. A. Kunze: *Linear algebra,* PHI Learning, Second Edition. |
| **References:** | |
| 1 | Stephen H Friedberg, *Linear Algebra*, O 'Eastern Economic Edition, fourth edition |
| 2 | B.S. Grewal, *Higher Engineering Mathematics*, Khanna Publishers, Thirty Sixth edition . |
| **Useful Links for E-resources:** | |
| 1 | https://nptel.ac.in/courses/111105123/ |
| 2 | https://www.analyticsvidhya.com/blog/2017/02/lintr oductory-guide-on-linear-programming-explained- in-simple-english/ |
| 3 | https://www.u-aizu.ac.jp/~qf- zhao/TEACHING/AI/AI.html |
| 4 | https://www.udemy.com/course/mathematical- foundation-for-machine-learning-and-ai. |

| **Assessment:** | |
|---|---|
| **Internal Assessment:** | |
| Assessment consists of two class tests of 20 marks each. The first -class test is to be conducted when approx. 40% syllabus is completed and the second-class test when an additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| **End Semester Theory Examination:** | |
| 1 | Question paper will comprise a total of six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |

| | |
|---|---|
| 4 | Only Four questions need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus. |

**List of Tutorials:**

| Sr. No | Topic |
|---|---|
| 1 | Tutorial on Set theory |
| 2 | Tutorial on Principle of Inclusion and Exclusion |
| 3 | Tutorial on Pigeonhole Principle |
| 4 | Tutorial on Relation |
| 5 | Tutorial on Functions |
| 6 | Tutorial on system of linear algebraic equations |
| 7 | Tutorial on Caley Hamilton theorem |
| 8 | Tutorial on diagonalization of matrix |
| 9 | Tutorial on Gram-Schmidt orthogonalization |
| 10 | Tutorial on vector space and subspace |
| 11 | Tutorial on linear dependence and independence of vectors |
| 12 | Tutorial on basis and dimensions of vector space |
| 13 | Tutorial on linear transformation and its matrix |
| 14 | Tutorial on Singular Value Decomposition |
| 15 | Tutorial on normal, adjoin and self-adjoin operators |

| Course Code: | Course Title | Credit |
|---|---|---|
| 21103 | Programming principles with C | 2 |

| | |
|---|---|
| **Prerequisite: No Prerequisite** | |
| **Course Objectives:** | |
| 1 | To explore Problem-solving by developing an algorithm, flowchart and implement the logic using C programming language. |
| 2 | To understand data types in C |
| 3 | To explore mathematical and logical operations. |
| 4 | To explore different statements using if statement and loops and understand arranging data in arrays and implementing pointers. |
| **Course Outcomes:** On successful completion of course, learner will be able | |
| 1 | To formulate simple algorithms for arithmetic, logical problems and translate them to programs in C language. |
| 2 | To ability to handle possible errors during program execution. |
| 3 | To Implement, test and execute programs comprising of control structures. |
| 4 | To decompose a problem into functions and synthesize a complete program. |
| 5 | To demonstrate the use of arrays, strings and structures in C language. |
| 6 | To understand the concept of pointers |

| Module | | Content | Hrs |
|---|---|---|---|
| **1** | | **Introduction to C Programming** | **8** |
| | 1.1 | Introduction to components of a Computer System<br>Introduction to Algorithm and Flowchart. | |
| | 1.2 | Fundamentals of C Programming: Keywords, Identifiers, Constants and Variables , Data types in C , Operators in C , Basic Input and Output Operations , Expressions and Precedence of Operators , In-built Functions | |
| **2** | | **Control Structures** | **8** |
| | 2.1 | Introduction to Control Structures. | |
| | 2.2 | Branching and looping structures: If statement, If-else statement, Nested ifelse, else-if Ladder , Switch statement , For loop, While loop, Do while loop<br>, break and continue | |
| **3** | | **Functions** | **6** |
| | 3.1 | Introduction to functions Function prototype, Function definition, accessing a function and parameter passing. | |
| | 3.2 | Recursion. | |
| **4** | | **Arrays and Strings** | **8** |
| | 4.1 | Introduction to Arrays, Declaration and initialization of one dimensional and two-dimensional arrays. | |
| | 4.2 | Definition and initialization of String, String functions. | |

| | | | |
|---|---|---|---|
| | | **Total** | **30** |

| **Textbooks:** | |
|---|---|
| 1 | E. Balaguruswamy, "**Programming in ANSI C**", McGraw-Hill Third Edition 2014 |
| 2 | Kernighan , Ritchie "**The C programming Language**", Prentice Hall of India second Edition 2015 |
| **References:** | |
| 1 | Byron Gottfried, **"Programing with C",** McGraw Hill ( Schaum"s outline series) Third Edition 2009. |
| 2 | KanetkarYashwant **"Let Us C",** IEEE Press, Wiley Publication BPB Publication Third Edition, 2013. |
| **Useful Links** | |
| 1 | https://www.coursera.org/specializations/c-programming |
| 2 | https://onlinecourses.nptel.ac.in/noc20_cs91/preview |

| **Assessment:** | |
|---|---|
| **Internal Assessment:** | |
| Assessment consists of two class tests of 20 marks each. The first class test is to be conducted when approx. 40% syllabus is completed and second class test when additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| **End Semester Theory Examination:** | |
| 1 | Question paper will comprise of total six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only Four question need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mention in the syllabus. |

**List of Practical/ Experiments**:

| Practical Number | Practical/ Experiment Topic |
|---|---|
| 1 | Basic data types and I/O operations |
| 2 | Branching Statements |
| 3 | Statements using conditional controls |
| 4 | Problem statement for iterative loop structure |
| 5 | Problem statement for nested loop structure |
| 6 | Problem statement on Implementation of One D Array |

| | |
|---|---|
| 7 | Problem statement on Implementation of Two D Array |
| 8 | Implementation of Strings using header file and without header file |
| 9 | Study and Implementation of Functions. |
| 10 | Study and Implementation of Recursion. |



| | |
|---|---|
| 11 | Structure and Union |
| 12 | Array of Structure and Nested Structures. |
| 13 | Implementation of Pointers. |

| Course Code: | Course Title | Credit |
|---|---|---|
| 21104 | Computer Networks | 4 |

| Prerequisite: No Prerequisite | |
|---|---|
| **Course Objectives:** | |
| 1 | To introduce concepts and fundamentals of data communication and computer networks. |
| 2 | To explore the inter-working of various layers of OSI. |
| 3 | To explore the issues and challenges of protocols design while delving into TCP/IP protocol suite. |
| 4 | To assess the strengths and weaknesses of various routing algorithms. |
| 5 | To understand various transport layer and application layer protocols. |
| **Course Outcomes: On successful completion of course, learner will be able to** | |
| 1 | Demonstrate the concepts of data communication at physical layer and compare ISO – OSI model with TCP/IP model. |
| 2 | Introduction to Physical layer Transmission media. |
| 3 | Explore different design issues at data link layer. |
| 4 | Design the network using IP addressing and sub netting / super netting schemes. |
| 5 | Analyze transport layer protocols and congestion control algorithms. |
| 6 | Explore protocols at application layer. |

| Module | | Content | Hrs |
|---|---|---|---|
| **1** | | **Introduction to Networking** | **6** |
| | 1.1 | Introduction to computer network, network application, network software and hardware components (Interconnection networking devices), Network topology, protocol hierarchies, design issues for the layers, connection oriented and connectionless services. | |
| | 1.2 | Reference models: Layer details of OSI, TCP/IP models. Communication between layers. | |
| **2** | | **Physical Layer** | **6** |
| | 2.1 | Introduction to Communication Electromagnetic Spectrum. | |
| | 2.2 | Guided Transmission Media: Twisted pair, Coaxial, Fiber optics. | |

| | | | |
|---|---|---|---|
| **3** | | **Data Link Layer** | **8** |

| | | | |
|---|---|---|---|
| | 3.1 | DLL Design Issues (Services, Framing, Error Control, Flow Control), Error Detection and Correction (Hamming Code, CRC, Checksum), Elementary Data Link protocols, Stop and Wait, Sliding Window (Go Back N, Selective Repeat) | |
| | 3.2 | Medium Access Control sub layer Channel Allocation problem, Multiple access Protocol( Aloha, Carrier Sense Multiple Access (CSMA/CD) | |
| **4** | | **Network layer** | **10** |
| | 4.1 | Network Layer design issues, Communication Primitives: Unicast, Multicast, Broadcast. IPv4 Addressing (class full and classless), Sub netting, Super-netting design problems ,IPv4 Protocol, Network Address Translation (NAT), IPv6. | |
| | 4.2 | Routing algorithms: Shortest Path (Dijkastra's), Link state routing, Distance Vector Routing. | |
| | 4.3 | Protocols - ARP, RARP, ICMP, IGMP | |
| | 4.4 | Congestion control algorithms: Open loop congestion control, Closed loop congestion control, QoS parameters, Token & Leaky bucket algorithms. | |
| **5** | | **Transport Layer** | **8** |
| | 5.1 | The Transport Service: Transport service primitives, Berkeley Sockets, Connection management (Handshake), UDP, TCP, TCP state transition, TCP timers. | |
| | 5.2 | TCP Flow control (sliding Window), TCP Congestion Control: Slow Start. | |
| **6** | | **Application Layer** | **7** |
| | 6.1 | DNS: Name Space, Resource Record and Types of Name Server. HTTP, SMTP, Telnet, FTP, DHCP | |
| | | **Total** | **45** |

**Assessment:**

**Internal Assessment:**

Assessment consists of two class tests of 20 marks each. The first -class test is to be conducted when approx. 40% syllabus is completed and the second-class test when an additional 40% syllabus is completed. Duration of each test shall be one hour.

**End Semester Theory Examination:**

| | |
|---|---|
| 1 | Question paper will comprise a total of six questions. |
| 2 | All question carries equal marks |

| | |
|---|---|
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only Four questions need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus. |

| | |
|---|---|
| **Textbooks:** | |
| 1 | A.S. Tanenbaum: Computer Networks, Pearson Education, 4th Edition. |
| 2 | B.A. Forouzan: Data Communication and Networking, TMH, 5th Edition. |
| **References:** | |
| 1 | James F. Kurose, Keith W. Ross: Computer Networking, A Top-Down Approach Featuring the Internet, Addison Wesley, 6th edition. |
| **Useful Links for E-resources:** | |
| 1 | https://www.udemy.com/course/mta-networking-fundamentals-exam-microsoft-98-366/ |
| 2 | https://onlinecourses.nptel.ac.in/noc21_cs18/preview |

**List of Practical/ Experiments:**

| Practical Number | Practical/ Experiment Topic |
|---|---|
| 1 | Study of RJ45 and CAT6 Cabling and connection using crimping tool. |
| 2 | Use basic networking commands in Linux (ping, tracert, nslookup, netstat, ARP, |
| 3 | Build a simple network topology and configure it for static routing protocol using packet tracer. Setup a network and configure IP addressing, subnetting, masking. |
| 4 | Design VPN and Configure RIP/OSPF using Packet tracer. |
| 5 | Socket programming using TCP or UDP |

| | |
|---|---|
| 6 | Perform Remote login using Telnet server |
| 7 | Perform File Transfer and Access using FTP |
| 8 | Use simulator (Eg. NS2) to understand functioning of ALOHA, CSMA/CD |
| 9 | Study and Installation of Network Simulator (NS3) |
| 10 | a. Set up multiple IP addresses on a single LAN.<br>b. Using nestat and route commands of Linux, do the following:<br>● View current routing table<br>● Add and delete routes ● Change default gateway<br>c. Perform packet filtering by enabling IP forwarding using IPtables in Linux. |

| Course Code: | Course Title | Credit |
|---|---|---|
| 21105 | Cyber Security Fundamentals | 4 |

| | |
|---|---|
| **Prerequisite: No Prerequisite** | |
| **Course Objectives:** | |
| 1 | To introduce classical encryption techniques and concepts of modular arithmetic and number theory. |
| 2 | To explore the working principles and utilities of various cryptographic algorithms including secret key cryptography, hashes and message digests, and public key algorithms |
| 3 | To understand various cryptographic techniques. |
| 4 | To understand various security management issues |
| **Course Outcomes: On successful completion of course, learner will be able to** | |
| 1 | Understand system security goals and concepts, classical encryption techniques and acquire fundamental knowledge on the concepts of modular arithmetic and number theory |
| 2 | Understand, compare and apply different encryption and decryption techniques to solve problems related to confidentiality and authentication |
| 3 | To understand security threats and vulnerabilities present in the system. |
| 4 | Apply different message digest and digital signature algorithms to verify integrity and achieve authentication and design secure applications |
| 5 | Analyze and apply system security concept to recognize malicious code. |
| 6 | Understand and analyze various security management issues. |

| Module | | Content | Hrs |
|---|---|---|---|
| **1** | | **Security Fundamentals** | **5** |
| | 1.1 | An Overview of Information Security: The Basic Components, Threats, Policy and Mechanism, Assumptions and Trust, Assurance, Operational Issues, Human Issues, Security nomenclature. | |
| | 1.2 | Access Control Matrix, Security Policies: Confidentiality, Integrity, Availability Policies and Hybrid Policies, OS Security | |
| **2** | | **Modular Arithmetic and Cryptography Basics** | **10** |
| | 2.1 | Modular Arithmetic: Modular Arithmetic Notations, Modular Arithmetic Operations, Euclid's method of finding GCD, The extended Euclid's algorithm. | |
| | 2.2 | Cryptography : Classical encryption techniques, Block and Chain ciphers, Data Encryption Standard, Advanced Encryption Standard, RC5 | |

| | | | |
|---|---|---|---|
| **3** | | **Security Threats and Vulnerabilities** | **8** |
| | 3.1 | Overview of Security threats<br>Weak / Strong Passwords and Password Cracking<br>Insecure Network connections | |
| | 3.2 | Malicious Code<br>Programming Bugs<br>Cybercrime and Cyber terrorism<br>Information Warfare and Surveillance | |
| **4** | | **Cryptography / Encryption** | **8** |
| | 4.1 | Introduction to Cryptography/ Encryption, Digital Signatures Public Key Infrastructure | |
| | 4.2 | Applications of Cryptography Tools and techniques of Cryptography. | |
| **5** | | **Attacks, Malicious Logic and Countermeasures** | **8** |
| | 5.1 | Phishing, Password Cracking, Key-loggers and Spywares, Types of Virus,<br>Worms, DoS and DDoS, SQL injection, Buffer Overflow, Spyware, Adware and Ransomware | |
| | 5.2 | Antivirus and other security measures Intrusion Detection System: IDS fundamentals, Different types of IDS. Intrusion Prevention. | |
| **6** | | **Issues in Security Management** | **6** |
| | 6.1 | Overview, Risk identification, Risk Assessment, Risk Control Strategies, Quantitative vs. Qualitative Risk Control Practices. | |
| | 6.2 | Risk Management. Laws and Ethics in Information Security, Codes of Ethics, Protecting programs and data. | |
| | | **Total** | **45** |

| | |
|---|---|
| **Textbooks:** | |
| 1 | William Stallings: Computer Security: Principles and Practices, Pearson Publication, 6th Edition. |
| **References:** | |
| 1 | Nina Godbole: Cyber Security- Understanding Cyber Crimes, Wiley India Pvt. Ltd, Third Edition. |
| **Useful Links for E-resources:** | |
| 1 | https://www.udemy.com/course/complete-introduction-to-cybersecurity/ |
| 2 | https://www.coursera.org/learn/cyber-security-fundamentals |
| 3 | https://onlinecourses.nptel.ac.in/noc23_cs127/preview |

| | |
|---|---|
| **Assessment:** | |
| **Internal Assessment:** | |
| Assessment consists of two class tests of 20 marks each. The first -class test is to be conducted when approx. 40% syllabus is completed and the second-class test when an additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| **End Semester Theory Examination:** | |
| 1 | Question paper will comprise a total of six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only Four questions need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus. |

**List of Practicals:**

| Serial No | Name of Practical |
|---|---|
| 1 | To implement Text Encryption Using Cryptographic Algorithms. |
| 2 | To implement Key logger Software. |
| 3 | To implement Image Encryption. |
| 4 | To implement Password Strength Tester. |
| 5 | To implement Web-Based Facial Authentication System |
| 6 | Download and install nmap. Use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, xmas scan etc. |
| 7 | Detect ARP spoofing using nmap and/or open-source tool ARPWATCH and wireshark. Use arping tool to generate gratuitous arps and monitor using wireshark. |
| 8 | Simulate DOS attack using Hping, hping3 and other tools. |
| 9 | Simulate buffer overflow attack using Ollydbg, Splint, Cpp check etc. |
| 10 | Setting up personal Firewall using iptables. |

| Course Code: | Course Title | Credit |
|---|---|---|
| **21106** | **Operating System and Network Security** | **4** |

| | |
|---|---|
| **Prerequisite: No Prerequisite** | |
| **Course Objectives:** | |
| 1 | To introduce basic concepts and functions of operating systems. |
| 2 | To understand the concept of process, thread and resource management. |
| 3 | To understand the concepts of process synchronization and deadlock. |
| 4 | To understand various Memory, I/O and File management techniques. |
| 5 | To Understand security concepts and terminologies in computer network |
| **Course Outcomes: On successful completion of course, learner will be able to** | |
| 1 | Understand the objectives, functions and structure of OS |
| 2 | Analyze the concept of process management and evaluate performance of process scheduling algorithms. |
| 3 | Understand and apply the concepts of synchronization and deadlocks |
| 4 | Evaluate performance of Memory allocation and replacement policies |
| 5 | Understand the concepts of file management |
| 6 | Understand security concepts and terminologies in computer network |

| Module | | Content | Hrs |
|---|---|---|---|
| **1** | | **Operating system Overview** | **7** |
| | 1.1 | Introduction, Objectives, Functions and Evolution of Operating System. | |
| | 1.2 | Operating system structures: Layered, Monolithic and Microkernel. | |
| | 1.3 | Linux Kernel, Shell and System Calls. | |
| **2** | | **Process and Process Scheduling** | **10** |
| | 2.1 | Concept of a Process, Process States, Process Description, Process Control Block. | |
| | 2.2 | Uniprocessor Scheduling-Types: Preemptive and Non-preemptive scheduling algorithms (FCFS, SJF, SRTN, Priority, RR) | |
| | 2.3 | Threads: Definition and Types, Concept of Multithreading | |
| **3** | | **Process Synchronization and Deadlocks** | **10** |
| | 3.1 | Concurrency: Principles of Concurrency, Inter-Process Communication, Process Synchronization | |
| | 3.2 | Mutual Exclusion: Requirements, Hardware Support (TSL), Operating System Support (Semaphores), Producer and Consumer problem | |

| | | | |
|---|---|---|---|
| | 3.3 | Principles of Deadlock: Conditions and Resource, Allocation Graphs, Deadlock Prevention, Deadlock Avoidance: Banker's Algorithm, Deadlock Detection and Recovery, Dining Philosophers Problem | |
| **4** | | **Memory Management** | **7** |
| | 4.1 | Memory Management Requirements, Memory Partitioning: Fixed, Partitioning, Dynamic Partitioning, Memory Allocation Strategies: BestFit, First Fit, Worst Fit, Paging and Segmentation, TLB. | |
| | 4.2 | Virtual Memory: Demand Paging, Page Replacement Strategies: FIFO, Optimal, LRU, Thrashing. | |
| **5** | | **File Management** | **5** |
| | 5.1 | Overview, File Organization and Access, File Directories, File Sharing | |
| **6** | | **Network security** | **6** |
| | 6.1 | Security Concepts and Terminology.<br>TCP/IP and OSI Network Security.<br>Access Control Issues (Packet Filters, Firewalls). | |
| | | **Total** | **45** |

| **Textbooks:** | |
|---|---|
| 1 | William Stallings: Operating System: Internals and Design Principles, Prentice Hall, 2014 8th Edition |

| **References:** | |
|---|---|
| 1 | Abraham Silberschatz: Operating System Concept, John Wiley &Son, 2016 9th Edition. |

| **Useful Links for E-resources:** | |
|---|---|
| 1 | https://www.udemy.com/course/operating-systems-from-scratch-part1/ |
| 2 | https://www.coursera.org/learn/-network-security |
| 3 | https://onlinecourses.nptel.ac.in/noc21_cs88/preview |

**Assessment:**

**Internal Assessment:**

Assessment consists of two class tests of 20 marks each. The first -class test is to be conducted when approx. 40% syllabus is completed and the second-class test when an additional 40% syllabus is completed. Duration of each test shall be one hour.

**End Semester Theory Examination:**

| | |
|---|---|
| 1 | Question paper will comprise a total of six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only Four questions need to be solved. |

| | |
|---|---|
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus. |

**List of Practical/ Experiments:**

| Practi cal Numb er | Practical/ Experiment Topic |
|---|---|
| 1 | Explore usage of basic Linux Commands and system calls for file, directory and process management.<br>For eg: (mkdir, chdir, cat, ls, chown, chmod, chgrp, ps etc. system calls:<br>open, read, write, close, getpid, setpid, getuid, getgid, getegid, geteuid.<br>sort, grep, awk, etc.) |
| 2 | Linux shell script Write shell scripts to do the following: a.<br>Display OS version, release number, kernel version<br>b. Display top 10 processes in descending order<br>c. Display processes with highest memory usage.<br>d. Display current logged in user and log name.<br>Display current shell, home directory, operating system type, current path setting, current working directory. |
| 3 | a. Create a child process in Linux using the fork system call. From the child process obtain the process ID of both child and parent by using getpid and getppid system call.<br>b. Explore wait and waitpid before termination of process. |
| 4 | a. Write a program to demonstrate the concept of non-preemptive scheduling algorithms.<br>b. Write a program to demonstrate the concept of preemptive scheduling algorithms. |
| 5 | a. Write a C program to implement solution of Producer consumer problem through Semaphore |
| 6 | Implement IP Table Security |
| 7 | Write a program to demonstrate the concept of deadlock avoidance through Banker's Algorithm |
| 8 | Write a program demonstrate the concept of Dining Philosopher's Problem |
| 9 | Write a program to demonstrate the concept of MVT and MFT memory management techniques |
| 10 | Write a program to demonstrate the concept of dynamic partitioning placement algorithms i.e. Best Fit, First Fit, Worst-Fit etc |

# Semester II

| Course Code: | Course Title | Credit |
|---|---|---|
| 21201 | Business communication Ethics | 3 |

| | |
|---|---|
| **Prerequisite: Professional Skill-I** | |
| **Course Objectives:** | |
| 1 | To enhance effective communication and interpersonal skills. |
| 2 | To explain / defend his/her ideas to a single person or panel. |
| 3 | To develop creative and impactful presentation skills.. |
| 4 | To understand the dynamics of business communication through group communication. required for career enhancement . |
| 5 | To develop analytical and logical skills for problem-solving. |
| **Course Outcomes:** At the end of the course, the students will be able to | |
| 1 | 1. Prepare effective business/ technical documents apt for managerial roles in social and professional situations. |
| 2 | Deliver effective business and technical presentations. |
| 3 | Develop life skills/interpersonal skills to build a confident personality. |
| 4 | Develop creative thinking and problem solving attitude through group communication. |
| 5 | Organize personal and professional skills to build an impressive professional image for internal or external |
| 6 | Apply the trait of a successful professional with a charismatic personality. |

| Module | | Content | Hrs |
|---|---|---|---|
| **1** | | **Writing Skills ( Part -II) A Report & Proposal Writing** | **12** |
| | 1.1 | Report Writing: Objectives of Report Writing (on General Topics) Language and Style in a report Types: Informative and Interpretative (Analytical, Survey and Feasibility) and Formats of reports( Short Report) Proposal Writing :Short Proposal Writing : Objectives, formats, language style | |
| **2** | | **Writing Skills ( Part -II) B Business/ Trade Letters** | **6** |
| | 2.1 | Order credit and status Enquiry Letters of inquiry, letter of complaints, Claim & adjustment letter Sales Letter, promotional leaflets and fliers | |
| **3** | | **Presentation Skills** | **6** |
| | 3.1 | Technical Presentation Business Presentation. | |
| **4** | | **Introduction to Interpersonal Skills** | **6** |
| | 4.1 | Emotional Intelligence,Leadership and Motivation,Team Building,Assertiveness Conflict Resolution and Negotiation Skills,Time Management,Decision Making | |

| | | | |
|---|---|---|---|
| | | **Total** | **30** |

| | |
|---|---|
| **Textbooks:** | |
| 1 | Bovée, C. L.& amp;Thill, J. V, " ***Business communication today*** NJ: Pearson |
| 2 | Ram Archana, "***Place Mentor, Tests of Aptitude for Placement Readiness***", Oxford University Press |
| **References:** | |
| 1 | Raman Meenakshi, Sharma Sangeeta. Technical Communication, Principles and Practice., Oxford University Press. |
| 2 | Masters, L. A., Wallace, H. R., & Harwood, L., Personal development for life and work, Mason: South-Western Cengage Learning. |

| | |
|---|---|
| **Assessment:** | |
| **Internal Assessment:** | |
| Assessment consists of two class tests of 20 marks each. The first class test is to be conducted when approx. 40% syllabus is completed and the second class test when an additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| **End Semester Theory Examination:** | |
| 1 | Question paper will comprise a total of six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only Four questions need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus. |

| | |
|---|---|
| **Useful Links** | |
| 1 | https://www.ese.iitb.ac.in/sites/default/files/downloads/repot_guide.pdf |
| 2 | https://www.spe.org/en/authors/resources/prepare-presentation. |
| 3 | https://india.oup.com/productPage/5591038/7421214/9780198066217 |
| 4 | https://www.geektonight.com/business-meeting/ |

**Suggested List of Tutorials:**

| Sr. No | Topic |
|---|---|
| 1 | Report writing Or Proposal Writing ( Brief reports on general topics) |
| 2 | Tutorial on letter writing |
| 3 | Tutorial on Business Or Technical presentation |
| 4 | Tutorial on Public Speaking Activity |
| 5 | Tutorial on Role Play & Model Building |
| 6 | Tutorial on Meetings Documentation ( Notice agenda & minutes writing |

| | |
|---|---|
| 7 | Case study on business/ corporate ethics |
| 8 | Group discussion & Debate |

| Course Code: | Course Title | Credit |
|---|---|---|
| **21202** | **Statistics for Data Science** | **3** |

| | |
|---|---|
| **Prerequisite: Applied Mathematics.** | |
| **Course Objectives:** | |
| 1 | To build the fundamentals of data science. |
| 2 | To build a classification model and interpret results. |
| 3 | To learn the intricacies of logistic regression, evaluate its outputs, and comprehend how a link function works. |
| 4 | To handle a data set to produce a specified set of results. |
| **Course Outcomes: On the completion of the course, learners will be able to:** | |
| 1 | To be able to calculate probabilities for continuous and discrete random variables. |
| 2 | To understand the basics of statistics. |
| 3 | To understand Bivariate statistics |
| 4 | To understand theory of sampling |
| 5 | To understand Test of significance |
| 6 | To understand Paired test, chi-square test for goodness of fit. |

| Module | | Content | Hrs |
|---|---|---|---|
| **1** | | **Basic Probability Theory and Distributions** | **12** |
| | 1.1 | Data Representation, Average, Spread, Experiments, Outcomes, Events, Probability, Permutations and Combinations, Random Variables, Probability Distributions, Mean and Variance of a Distribution, Binomial, Poisson, and Hypergeometric Distributions, Normal Distribution, Distributions of Several Random Variables. | |
| | 1.2 | Descriptive Statistics and Inference<br>Types of Statistical Inference, Descriptive Statistics, Inferential Statistics, Descriptive Statistics, Measures of Central Tendency: Mean, Median, Mode, Midrange, Measures of Dispersion: Range, Variance, Mean Deviation, Standard Deviation. Coefficient of variation: Moments, Skewness, Kurtosis, | |
| **2** | | **Statistical Inference-II** | **6** |
| | 2.1 | Estimation-properties, Methods of estimation-Point estimation, Interval estimation, One sample hypothesis testing: hypothesis, Testing of Hypothesis, Binomial distribution and normal distribution, Chi-Square Tests, t-test, Z test, F- test | |
| **3** | | **Analysis of Variance** | **6** |
| | 3.1 | Analysis of Variance: Fixed Effects, Random Effects, Mixed Models, 12 Introducing the Analysis of Variance (ANOVA), Performing the ANOVA, Random Effects ANOVA and Mixed Models, One-Way Random Effects ANOVA, | |

| | | | |
|---|---|---|---|
| **4** | | **Correlation and Regression** | **6** |
| | 4.1 | Correlation: Scatter plot, Karl Pearson coefficient of correlation, Spearman's rank correlation coefficient, multiple and partial correlations (for 3 variates only). Simple Linear Regression-OLS estimates- Properties. | |
| | | **Total** | **30** |

| | |
|---|---|
| **Textbooks:** | |
| 1 | S.C. Gupta & V.K. Kapoor, ***"Fundamentals of Mathematical Statistics",*** Sultan Chand & Co. |
| 2 | P. G. Hoel, S. C. Port and C. J. Ston ,***"Introduction to Probability Theory",*** Universal BookStall |
| **References:** | |
| 1 | Gareth James, Daniela Witten, Trevor Hastie, ***"An Introduction to Statistical Learning: with Applications in R",*** Springer. |
| 2 | Ross, ***"A First Course in Probability",*** Pearson Education India. |
| **Useful Links** | |
| 1 | https://www.statisticssolutions.com/continuous-probability- distribution/ |
| 2 | https://nptel.ac.in/courses/111/106/111106112/ |
| 3 | https://nptel.ac.in/courses/111/105/111105124/ |
| 4 | https://www.youtube.com/watch?v=L-pQtGm3VS8 |
| 5 | https://www.youtube.com/watch?v=vN5cNN2-HWE |

| | |
|---|---|
| **Assessment:** | |
| **Internal Assessment:** | |
| Assessment consists of two class tests of 20 marks each. The first-class test is to be conducted when approx. 40% syllabus is completed and second-class test when additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| **End Semester Theory Examination:** | |
| 1 | Question paper will comprise of total six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only Four question need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mention in the syllabus. |

**Suggested List of Practical/ Experiments:**

| Practical Number | Practical/ Experiment Topic |
|---|---|

| | |
|---|---|
| 1 | Implement conditional probability and Bayes theorem |
| 2 | Perform experiment to plot probabilities for continuous and discrete random variable |

| | |
|---|---|
| 3 | Perform experiment to measure central tendency of a dataset |
| 4 | Perform experiment to measure dispersion of a dataset |
| 5 | Perform experiment to calculate correlation between variables |
| 6 | Implement Regression |
| 7 | Implement curve fitting optimization using SciPy package |
| 8 | Implement Sampling distributions |
| 9 | Implement Statistical Significance tests |
| 10 | Regression analysis on hours spent on internet and time spent to study on academic performance of students |

| Course Code: | Course Title | Credit |
|---|---|---|
| 21203 | Indian Knowledge System(IKS) | 2 |

## Rationale:

The Indian Knowledge System (IKS) is vital for preserving India's rich cultural heritage, fostering holistic and sustainable practices, and integrating ancient wisdom with modern science to address contemporary challenges and enrich global knowledge.

## Course Objectives:

| |
|---|
| 1. To explore and understand the evolution of Indian scientific thought |
| 2. To evaluate the historical and modern educational systems in our country |
| 3. To analyse sustainable practices in in ancient India |
| 4. To know the richness of Indian Arts and Culture |
| 5. To understand the contributions of Indian Scientists and Nobel Laureates |
| 6. To understand the principles of good governance |

## Course Outcomes:

| |
|---|
| 1. Recognize the sources and concepts of the Indian knowledge system |
| 2. Learn about our history of Indian ancient knowledge and its significance in the current scenario. |
| 3. Demonstrate sustainable development in various fields like Science, Technology, agriculture, industry, architecture performing arts, etc. |
| 4. Understand and appreciate the rich heritage that resides in literature |
| 5. Learn about the ancient Bhartiya education system in comparison with the modern era |
| 6. Showcase the multi-dimensional nature of IKS and its importance in modern society |

**Prerequisite:**

1. Students should have the foundational knowledge and skills necessary for a comprehensive understanding of IKS

2. Students should be familiar with the Indian Culture, Language, and History of Science and Technology in India.

| Module | Name of Module | Detailed Content | Ho urs |
|---|---|---|---|
| 1 | **Introduction to the Indian Knowledge System (I.K.S.)** | • Basic knowledge and scope of IKS<br>• IKS in ancient India and modern India,<br>• Bhartiya education system – ancient to modern era,<br>• Sources of Education, Aim of Education, Curriculum, methods of learning,<br>• Educational Institutes, Higher Educational Institutions,<br>• Advantages and Disadvantages of the Gurukul System,<br>• Distinguish between the Gurukul system And the Modern Education System | **5** |
| 2 | **Development of Scientific Thoughts in Ancient India** | Development in Science, Technology, Astronomy, Mathematics, and Life Sciences – Life Science, Physiology, Ayurveda, etc. | **4** |
| 3 | **Development of Arts & Culture in India** | • Introduction to Ancient Architecture (Arts, Forts, Paintings, Sculpture, Temple architecture, etc)<br>• Development in performing arts & culture: Music, Art of singing, Art of dancing, Natyakala Cultural traditions and Folk arts | **4** |
| 4 | **Good Governance in Ancient India** | • Introduction to Indian religions<br>• Moral and Ethical Governance<br>• Vishva Kalyan through Vasudhaiva Kutumbkam<br>• Principles of Good Governance about Ramayana, Mahabharat, Artha Sastra and Kauṭilyan State | **5** |
| 5 | **Contribution of Indian Scientist & Nobel** | Baudhayan, Aryabhatta, Brahmgupta, Bhaskaracharya, Varahamihira, Nagarjuna, Susruta, Kanada & Charak | **3** |
| | **Laureates** | Rabindranath Tagore, C.V. Raman, Har Gobind Khorana, Mother Teresa, Subrahmanyan Chandrasekhar, Amartya Sen, V.S. Naipaul, Venkatraman Ramakrishnan, Kailash Satyarthi and Abhijit Banerjee | **4** |

| | | | |
|---|---|---|---|
| **6** | **Sustainable Practices in Ancient India** | • Agriculture, waste management, water conservation, forest conservation, architecture, urban planning, biodiversity preservation, etc<br>• Yoga, pranayama, and meditation for health and well-being | **5** |
| **Total** | | | **30** |

**Text Books:**


1. **1.** A.K Bag, History of technology in India (Set 3 vol), Indian Nation Science Academy, 1997.
2. An Introduction to Indian Knowledge Systems: Concepts and Applications, B Mahadevan, V R Bhat, and Nagendra Pavana R N; 2022 (Prentice Hall of India).
3. Ancient Indian Knowledge: Implications To Education System, Boski Singh; 2019
4. India's Glorious Scientific Tradition by Suresh Soni; 2010 (Ocean Books Pvt. Ltd.)
5. Indian Art: Forms, Concerns, and Development in Historical Perspective (History of Science, Philosophy and Culture in Indian Civilization), General Editor: D.P. Chattopadhyaya, Ed. By. B.N. Goswamy; 1999 Munshiram Manoharlal Publishers Pvt. Ltd.
6. Indian Knowledge Systems: Vol I and II, Kapil Kapoor and A K Singh; 2005 (D.K. Print World Ltd).
7. Pandey, K.K. Kriya Sarira Comprehensive Human Physiology, Chaukhambha Sanskrit series, Varanasi, 2018
8. Shukla Vidyadhar & Tripathi Ravidatt, Aayurved ka Itihas evam Parichay, Chaukhambha Sanskrit Sansthaan, New Delhi, 2017
9. Textbook on The Knowledge System of Bharata by Bhag Chand Chauhan; 2023 (Garuda Prakashan) 6. Pride of India- A Glimpse of India's Scientific Heritage edited by Pradeep Kohle et al. Samskrit Bharati; 2006
10. Traditional Knowledge System in India, Amit Jha


**Online References:**

| Sr. No. | Website Name |
|---|---|
| 1. | https://swayam.gov.in/explorer?searchText=iks |
| 2. | https://iksindia.org/book-list.php |
| **3.** | https://iksindia.org/index.php |

**Assessment:**

**Suggested Pedagogy and assessment criteria for Teachers:**

1. Project-based activities.
2. Presentation, Group Discussions, and Case studies.
3. Visit historical places.
4. Flip class mode/ Role-play
5. Quiz MCQ
6. Assignment as per the modules: 06
7. Internal Assessment through flipped class and PowerPoint presentation along with documentation

| Course Code: | Course Title | Credit |
|---|---|---|
| **21204** | **Python Programming** | **4** |

| | |
|---|---|
| **Prerequisite: Programming principles with C** | |
| **Course Objectives:** | |
| 1 | Implementing data types, statement, operators and strings |
| 2 | Implementing OOPs concept in Python |
| 3 | To learn exception & file handling in Python. |
| 4 | Connecting with databases |
| **Course Outcomes: On successful completion of course, learner will be able to** | |
| 1 | Apply the concept of Program structure, Interactive Shell. |
| 2 | To understand Data Structures and Program control flow, |
| 3 | Apply the concept Functions and Modules & Packages for list manipulation and string manipulation. |
| 4 | Understand Classes & Objects for User Defined Data Type, Objects as Instances of Classes. |
| 5 | Test Exception Handling & File Operations for Default Exception and Errors. |
| 6 | Apply the concept of Database, GUI & Turtle Programming. |

| Module | | Content | Hrs |
|---|---|---|---|
| **1** | | **Introduction to Python** | **4** |
| | 1.1 | History & need of Python, Application of Python, Advantages of Python, Disadvantages of Python, | |
| | 1.2 | Installing Python, Program structure, Interactive Shell, Executable or script files, 1.3 User Interface or IDE Working with Interactive mode, Working with Script mode, 1.4 Python Character Set, Python Tokens, Keywords, Identifiers, Literals, Operators, Variables and Assignments, Input and Output in Python, Data Types. | |
| **2** | | **Data Structures and Program control flow** | **5** |
| | 2.1 | Data Structures**:** String Manipulation, List Manipulation, Tuples and Dictionaries, Set and Frozenset. | |
| | 2.2 | Program Control Flow: | |
| | 2.3 | Conditional Statements: if Statement, if-else Statement, if-elif Statement, Nested if Statements, Python Indentation. | |

| | | | |
|---|---|---|---|
| | 2.4 | Looping and Iteration: For Loop, While Loop, Loop else Statement, Nested Loops, Break and Continue. | |
| | 2.5 | Range Function: Introduction to range(), Types of range() function, Use of range() function. | |
| **3** | | **Functions and Modules & Packages** | **5** |
| | 3.1 | Built-In Functions: Introduction to Functions, Python Function Types, Structure of Python Functions,<br>E.g. - map, zip, reduce, filter, any, chr, ord, sorted, globals, locals, all, etc. | |
| | 3.2 | User Defined Functions: Structure of a Python Program w.r.t. UDF, Types of Functions, Invoking UDF, Flow of Execution, Arguments and Parameters, Default Arguments, Named Arguments, Scope of Variables, Lambda function | |
| | 3.3 | Recursion Function: Use of recursion function | |
| | 3.4 | Modules & Packages: Importing Modules in Python Programs,<br>Working with Random Modules, E.g. - builtins, os, time, datetime, calendar, sys, etc | |
| **4** | | **Classes & Objects** | **6** |
| | 4.1 | Introduction to OOP's: Procedural Vs Modular Programming, Object Oriented Programming, Data Abstraction, Data Hiding, Encapsulation, Modularity, Inheritance, Polymorphism | |
| | 4.2 | Classes & Objects: Classes as User Defined Data Type, Objects as Instances of Classes, Creating Class and Objects, Creating Objects By Passing Values, Variables & Methods in a Class | |
| **5** | | **Exception Handling & File Operations** | **6** |
| | 5.1 | Exception Handling: Default Exception and Errors, Catching Exceptions, Raise an exception, Try<br>- except statement, Raise, Assert,<br>Finally blocks, User defined exception. | |
| | 5.2 | File Operations: opening a file, Reading and Writing Files, Other file tools, Regular Expressions. | |
| **6** | | **Database, GUI & Turtle Programming** | **4** |
| | 6.1 | Database, GUI & Turtle Programming. | |
| | 6.2 | Database: Introduction to MySQL, PYMYSQL Connections, Executing queries, Transactions, Handling error. | |
| | 6.3 | GUI Programming: Introduction, Tkinter programming, Tkinter widgets, Frame, Button, Label, Entry<br>Turtle **Programming:** Introduction to Turtle, Controlling Turtle, Animation Programming | |
| | | **Total** | **30** |

| | |
|---|---|
| **Textbooks:** | |
| 1 | Dr. R. Nageswara Rao: Core Python Programming, Dreamtech Press Wiley Publication, 2018 2nd Edition. |
| 2 | Zed A. Shaw: Learn Python 3 The Hard Way, Pearson Education, 2017 1st Edition. |
| **References:** | |
| 1 | Paul Barry: Head First Python: A Brain- Friendly Guide, Shroff/ O. Reilly, 2016 2nd Edition. |
| 2 | Charles Dierbach: Introduction to Computer Science Using Python: A Computational Problem-Solving Focus, Wiley Publication, 2012 1st Edition. |
| **Useful Links for E-resources:** | |
| 1 | https://www.tutorialspoint.com/python/python_basi c_syntax.html |
| 2 | https://machinelearningmastery.com/machine- learning-in-python-step-by-step/ |
| 3 | https://towardsdatascience.com/beginners-guide-to- machine-learning-with-pythonb9ff35bc9c51 |

| | |
|---|---|
| **Assessment:** | |
| **Internal Assessment:** | |
| Assessment consists of two class tests of 20 marks each. The first class test is to be conducted when approx. 40% syllabus is completed and second class test when additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| **End Semester Theory Examination:** | |
| 1 | Question paper will comprise of total six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only Four question need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mention in the syllabus. |

**List of Practical/ Experiments:**

| Sr. No | Topic |
|---|---|
| 1 | To implement Python program to check whether the given number is even or not. |
| 2 | To implement Python program to convert the temperature in degree centigrade to Fahrenheit |
| 3 | Python program to find the area of a triangle whose sides are given |
| 4 | To Python program to find out the average of a set of integers |

| | |
|---|---|
| 5 | Python program to find the product of a set of real numbers |
| 6 | To implement Python program to find the circumference and area of a circle with a given radius. |
| 7 | Python program to check whether the given integer is a multiple of 5 |
| 8 | To implement Python program to check whether the given integer is a multiple of both 5 and 7. |
| 9 | To implement Python program to find the average of 10 numbers using while loop. |
| 10. | To implement Python program to display the given integer in a reverse manner. |
| 11 | To implement Python program to find the geometric mean of n numbers. |
| 12 | To implement Python program to find the sum of the digits of an integer using a while loop. |
| 13 | To implement Python program to display all the multiples of 3 within the range 10 to 50. |

| Course Code: | Course Title | Credit |
|---|---|---|
| **21205** | **Web Application Security** | **4** |

| | |
|---|---|
| **Prerequisite: No Prerequisite** | |
| **Course Objectives:** | |
| 1 | To reveal the underlying in web application. |
| 2 | To understand SSDLC for secure coding |
| 3 | To identify and aid in fixing any security vulnerabilities during the web development process. |
| 4 | To understand the security principles in developing a reliable web application. |
| **Course Outcomes: On successful completion of course, learner will be able to** | |
| 1 | Identify the vulnerabilities in the web applications. |
| 2 | Identify the various types of threats and mitigation measures of web applications. |
| 3 | Apply the security principles in developing a reliable web application. |
| 4 | Use industry standard tools for web application security. |
| 5 | Apply penetration testing to improve the security of web applications. |
| 6 | Detecting and responding to web application security incidents. |

| Module | | Content | Hrs |
|---|---|---|---|
| **1** | | **Introduction to Web Application Security** | **6** |

| | | | |
|---|---|---|---|
| | 1.1 | Understanding the importance of web application security | |
| | 1.2 | Overview of common web application vulnerabilities | |
| | 1.3 | Introduction to secure coding practices | |
| **2** | | **Web Application Architecture and Technologies** | **10** |
| | 2.1 | Client-server architecture and web application components | |
| | 2.2 | HTTP protocol and web application communication | |
| | 2.3 | Common web application technologies (HTML, CSS, JavaScript, etc.) | |

| | | | |
|---|---|---|---|
| **3** | | **Secure Software Development Lifecycle (SDLC)** | **7** |
| | 3.1 | Overview of the software development process. | |
| | 3.2 | Integrating security into the SDLC | |
| | 3.3 | Secure coding guidelines and best practices. | |
| **4** | | **Web Application Threats and Attacks** | **8** |
| | 4.1 | Injection attacks (SQL injection, OS command injection) | |
| | 4.2 | Cross-Site Scripting (XSS) attacks | |
| | 4.3 | Cross-Site Request Forgery (CSRF) attacks | |
| | 4.4 | Session hijacking and session management vulnerabilities | |
| **5** | | **Web Application Security Testing** | **8** |
| | 5.1 | Manual and automated security testing techniques | |
| | 5.2 | Vulnerability scanning and penetration testing | |
| | 5.3 | Fuzzing and input validation techniques | |
| | 5.4 | Web application security assessment tools | |
| **6** | | **Web Application Security Incident Response** | **6** |
| | 6.1 | Detecting and responding to web application security incidents | |
| | 6.2 | Incident handling and forensics | |
| | 6.3 | Incident response planning and coordination | |

| | | | |
|---|---|---|---|
| | | **Total** | **45** |

| **Textbooks:** | |
|---|---|
| 1 | Bryan Sullivan and Vincent Liu: Web Application Security: A Beginner's Guide, McGraw Hill LLC, 2011 1st Edition |
| | Prakhar Prasad: Mastering Modern Web Penetration Testing, Packt Publishing, 2016 1st Edition. |
| **References:** | |
| 1 | Mark Dowd: The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities, Addison-Wesley Professional, 2006 1st Edition. |
| **Useful Links for E-resources:** | |
| 1 | https://onlinecourses.nptel.ac.in/noc23_cs32/preview |
| 2 | https://www.coursera.org/projects/googlecloud-securing-web-applications-with-web-security-scanner-uqqj1 |
| 3 | https://www.coursera.org/learn/codio-data-security-for-web-developers |

| **Assessment:** | |
|---|---|
| **Internal Assessment:** | |
| Assessment consists of two class tests of 20 marks each. The first -class test is to be conducted when approx. 40% syllabus is completed and the second-class test when an additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| **End Semester Theory Examination:** | |
| 1 | Question paper will comprise a total of six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only Four questions need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus. |

**List of Practical/ Experiments:**

| **Practical Number** | **Practical/ Experiment Topic** |
|---|---|

| | |
|---|---|
| 1 | Recon for bug hunting |
| 2 | Advanced SQL Injection |
| 3 | Command Injection |
| 4 | Session Management and Broken Authentication Vulnerability |
| 5 | CSRF - Cross-Site Request Forgery |
| 6 | SSRF - Server Site Request Forgery |
| 7 | XSS - Cross-Site Scripting |
| 8 | IDOR - Insecure Direct Object Reference |
| 9 | Sensitive Data Exposure and Information Disclose |
| 10 | SSTI - Server Site Template Injection |
| 11 | Case Studies |

| Course Code: | Course Title | Credit |
|---|---|---|
| 21206 | Database Management and Security | 4 |

| | |
|---|---|
| **Prerequisite: No Prerequisite** | |
| **Course Objectives:** | |
| 1 | The role of security in the design and implementation of databases |
| 2 | Use best practices for data input, output, and encryptions |
| 3 | Maintain database management systems, including conducting security audits and keeping software updated. |
| **Course Outcomes: On successful completion of course, learner will be able to** | |
| 1 | Master the basic concepts and appreciate the applications of database systems. |
| 2 | Be familiar with the relational database theory, and be able to write relational algebra expressions for queries. |
| 3 | Mater sound design principles for logical design of databases, including the E-R method and normalization approach. |
| 4 | To understand Database Security Fundamentals. |
| 5 | To understand Database Access Control and Privileges. |
| 6 | To understand Emerging Trends in Database Security. |

| Module | | Content | Hrs |
|---|---|---|---|
| **1** | | **Introduction to Database Management Systems (DBMS)** | **6** |
| | 1.1 | Overview of DBMS concepts and architecture | |
| | 1.2 | Relational database model and relational algebra | |
| | 1.3 | Data models and database design principles | |
| **2** | | **SQL and Database Querying** | **8** |
| | 2.1 | Structured Query Language (SQL) fundamentals | |
| | 2.2 | Data definition and manipulation using SQL | |

| | | | |
|---|---|---|---|
| | 2.3 | Query optimization and performance tuning | |

| | | | |
|---|---|---|---|
| **3** | | **Database Design and Normalization** | **8** |
| | 3.1 | Entity-Relationship (ER) modeling | |
| | 3.2 | Functional dependencies and normalization | |
| | 3.3 | De normalization and trade-offs | |
| **4** | | **Database Security Fundamentals** | **6** |
| | 4.1 | Security models and access control mechanisms | |
| | 4.2 | Security models and access control mechanism | |
| | 4.3 | User authentication and authorization | |
| **5** | | **Database Access Control and Privileges** | **12** |
| | 5.1 | Granting and revoking user privileges | |
| | 5.2 | Role-based access control (RBAC) | |
| | 5.3 | Fine-grained access control | |
| **6** | | **Emerging Trends in Database Security** | **5** |
| | 6.1 | Cloud databases and security considerations | |
| | 6.2 | Big Data and NoSQL databases security challenges | |
| | 6.3 | Privacy and data protection in databases | |
| | | **Total** | **45** |

| | |
|---|---|
| **Textbooks:** | |
| 1 | Avi Silberschatz , Henry F. Korth , and S. Sudarshan: Database System Concepts, McGraw-Hill, 2019 Seventh Edition. |
| 2 | Raghu Ramakrishnan: Database Management Systems, McGraw-Hill, 2014 3rd Edition. |
| **References:** | |
| 1 | Thomas Connolly and Carolyn Begg: Database Systems: Design, Implementation, and Management, Pearson Publication, 2019 6th Edition |
| **Useful Links for E-resources:** | |
| 1 | https://onlinecourses.nptel.ac.in/noc21_cs04/preview |
| 2 | https://www.coursera.org/learn/database-management |

**List of Practical/ Experiments:**

| **Assessment:** | |
|---|---|
| **Internal Assessment:** | |
| Assessment consists of two class tests of 20 marks each. The first -class test is to be conducted when approx. 40% syllabus is completed and the second-class test when an additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| **End Semester Theory Examination:** | |
| 1 | Question paper will comprise a total of six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only Four questions need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus. |

| **Practical Number** | **Practical/ Experiment Topic** |
|---|---|
| 1 | To study and execute the DDL commands in RDBMS. |
| 2 | To study DML commands in RDBMS. |
| 3 | To implement PL/SQL program using control structures, procedures and functions. |
| 4 | To study and execute Triggers in RDBMS. |
| 5 | Implementation of views |
| 6 | To create queries using Procedures. |
| 7 | To implement RDBMS using JDBC connectivity. |
| 8 | Granting and revoking user privileges |
| 9 | To implement Role-based access control (RBAC) |
| 10 | To Demonstrate Fine-grained access control |
| 11 | Course Case Study/Project |

**Program Structure for Second Year B. Voc Cyber Security and Digital Forensics UNIVERSITY OF MUMBAI (With Effect from 2025-2026)**

**Semester III**

| Course Code: | Course Title | Credit |
|---|---|---|
| **21 301** | **Professional Skill-III (Entrepreneurship)** | **3** |

| | |
|---|---|
| **Prerequisite: Business Communication Ethics** | |
| **Course Objectives:** | |
| 1 | To provide a detailed overview of entrepreneurship as the foundation of business growth |
| 2 | To teach to adopt entrepreneurship as value creation in the national economy. |
| 3 | It provides multiple constructs for entrepreneurs to be successful. |
| 4 | It provides multiple pathways for their companies to achieve sustainable growth. |
| **Course Outcomes:** | |
| 1 | To understand key concepts underpinning entrepreneurship |
| 2 | To apply knowledge in the recognition and exploitation of product/ service/ process opportunities |
| 3 | To demonstrate key concepts underpinning innovation and the issues associated with developing and sustaining innovation within organizations |
| 4 | To understand, how to design creative strategies for pursuing, exploiting and further developing new opportunities |
| 5 | To understand Issues associated with securing and managing financial resources in new and established organizations. |

| Module | | Content | Hrs |
|---|---|---|---|
| **1** | | **Introduction to Entrepreneurial Journey** | **6** |
| | 1.1 | Entrepreneurial Journey | |
| | 1.2 | Entrepreneurial Discovery | |
| **2** | | **Ideation and Prototyping** | **6** |
| | 2.1 | Ideation and Prototyping. | |
| | 2. | Testing, Validation and Commercialization, Disruption as a Success Driver | |
| | 2 | | |
| **3** | | **Technological Innovation and Entrepreneurship** | **6** |

| | | | |
|---|---|---|---|
| | 3.1 | Technological Innovation and Entrepreneurship – 1 | |
| | 3.2 | Technological Innovation and Entrepreneurship – 2 ,Raising Financial Resources | |
| **4** | | **Education and Entrepreneurship** | **5** |
| | 4.1 | Education and Entrepreneurship. | |
| | 4.2 | Beyond Founders and Founder-Families, India as a Start-up Nation | |
| **5** | | **National Entrepreneurial Culture** | **4** |
| | 5.1 | National Entrepreneurial Culture. | |
| | 5.2 | Entrepreneurial Thermodynamics, Entrepreneurship and Employment. | |
| **6** | | **Start-up Case Studies.** | **3** |
| | 6.1 | Discuss at least five case studies. | |
| **Total** | | | **30** |

| **Textbooks:** | |
|---|---|
| 1 | Peter Thiel "Zero to One: Notes on Startups, or How to Build the Future", Crown, 16 Sept 2014 - Business & Economics - 224 pages. |
| 2 | Eric Ries "The Lean Startup: How Today's Entrepreneurs Use Continuous Innovation to Create Radically Successful Businesses" published January 1, 2011, Board Book |

| **Referecebooks:** | |
|---|---|
| 1 | C B Rao "India as Global Start-up Hub: Mission with Passion" Notion Press, 2018, |
| 2 | Ashlee Vance ,"Elon Musk: Tesla, SpaceX, and the Quest for a Fantastic Future", Ecco Press, Publish Year: 2015 |
| 3 | Walter Isaacson "Steve Jobs", October 1, 2011 |

**Assessment:**

**Internal Assessment:**

| | |
|---|---|
| Assessment consists of two class tests of 20 marks each. The first class test is to be conducted when approx. 40% syllabus is completed and second class test when additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| **End Semester Theory Examination:** | |
| 1 | Question paper will comprise of total six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only Four question need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mention in the syllabus. |

| **Useful Links** | |
|---|---|
| 1 | https://onlinecourses.nptel.ac.in/noc20_mg35/preview. |
| 2 | https://www.business-school.ed.ac.uk/msc/entrepreneurship-innovation/overview/learningoutcomes |

**List of Tutorial:**

| **Tutorial Number** | **Tutorial Topic** |
|---|---|
| 1 | Field study of Industries offices in vicinity. |
| 2 | Visit to Atal incubation Center. |
| 3 | Create Business Model on any project. |

| **Course Code:** | **Course Title** | **Credit** |
|---|---|---|
| **21302** | **Ethical Hacking** | **3** |

| **Prerequisite:** | |
|---|---|
| **Course Objectives:** | |
| 1 | To describe Ethical hacking and fundamentals of computer Network. |
| 2 | To understand about Network security threats, vulnerabilities assessment and social engineering. |
| 3 | To discuss cryptography and its applications. |

| | |
|---|---|
| 4 | To implement the methodologies and techniques of Sniffing techniques, tools, and ethical issues. |
| 5 | To implement the methodologies and techniques of hardware security. |
| 6 | To demonstrate systems using various case studies. |
| **Course Outcomes:** | |
| 1 | Articulate the fundamentals of Computer Networks, IP Routing and core concepts of ethical hacking in real world scenarios. |
| 2 | Apply the knowledge of information gathering to perform penetration testing and social engineering attacks |
| 3 | Demonstrate the core concepts of Cryptography, Cryptographic checksums and evaluate the various biometric authentication mechanisms. |
| 4 | Apply the knowledge of network reconnaissance to perform Network and web application-based attacks. |
| 5 | Apply the concepts of hardware elements and endpoint security to provide security to physical devices. |
| 6 | Simulate various attack scenarios and evaluate the results. |

| | | | |
|---|---|---|---|
| I | **Introduction to Ethical Hacking** | Fundamentals of Computer Networks/IP protocol stack, IP addressing and routing, Routing protocol, Protocol vulnerabilities, Steps of ethical hacking, Demonstration of Routing Protocols using Cisco Packet Tracer<br><br>**Self-learning Topics**:TCP/IP model, OSI model | **6** |
| II | **Introduction to Cryptography** | Private-key encryption, public key-encryption, key Exchange Protocols, Cryptographic Hash Functions & applications, steganography, biometric authentication, lightweight cryptographic algorithms.Demonstration of various cryptographic tools and hashing algorithms<br><br>**Self-learning Topics**: Quantum cryptography, Elliptic curve cryptography | **6** |
| III | **Introduction to network security** | Information gathering, reconnaissance, scanning, vulnerability assessment, Open VAS, Nessus, System hacking: Password cracking, penetration testing, Social engineering attacks, Malware threats, hacking wireless networks (WEP, WPA, WPA- 2), Proxy network, VPN security, Study of various tools for Network Security such as Wireshark, John the Ripper, Metasploit, etc.<br><br>**Self-learning Topics**: Ransomware(Wannacry), Botnets, Rootkits, Mobile device security | **7** |

| | | | |
|---|---|---|---|
| IV | **Introduction to web security and Attacks** | OWASP, Web Security Considerations, User Authentication, Cookies, SSL, HTTPS, Privacy on Web, Account Harvesting, Web Bugs, Sniffing, ARP poisoning, Denial of service attacks, Hacking Web Applications, Clickjacking, Cross-Site scripting and Request Forgery, Session Hijacking and Management, Phishing and Pharming Techniques, SSO, Vulnerability assessments, SQL injection, Web Service Security, OAuth 2.0, Demonstration of hacking tools on Kali Linux such as SQLMap, HTTrack, hping, burp suite,Wireshark etc.<br>**Self-learning Topics**: Format string attacks | **6** |
| V | **Elements of Hardware Security** | Side channel attacks, physical unclonable functions, Firewalls,Backdoors and trapdoors, Demonstration of Side Channel Attacks on RSA, IDS and Honeypots.<br>**Self-learning Topics**: IoT security | **3** |
| VI | **Case Studies** | Various attacks scenarios and their remedies. Demonstration of attacks using DVWA.<br>**Self-learning Topics**: Session hijacking and man-inmiddle attacks | **2** |
| **Total** | | | **30** |

| Textbooks: | |
|---|---|
| 1 | Computer Security Principles and Practice --William Stallings, Seventh Edition, Pearson Education, 2017 |
| 2 | Security in Computing -- Charles P. Pfleeger, Fifth Edition, Pearson Education, 2015 |
| 3 | Network Security and Cryptography -- Bernard Menezes, Cengage Learning, 2014 |
| 4 | Network Security Bible -- Eric Cole, Second Edition, Wiley, 2011 |
| 5 | Mark Stamp's Information Security: Principles and Practice --Deven Shah, Wiley, 2009 |
| References: | |
| 1 | UNIX Network Programming –Richard Steven,Addison Wesley, 2003 |
| 2 | Cryptography and Network Security -- Atul Kahate, 3rd edition, Tata Mc Graw Hill, 2013 3.TCP/IP Protocol Suite -- B. A. Forouzan, 4th Edition, Tata Mc Graw Hill, 2017 |
| 3 | Applied Cryptography, Protocols Algorithms and Source Code in C -- Bruce Schneier, 2nd Edition / 20th Anniversary Edition, Wiley, 2015 |
| 4 | UNIX Network Programming –Richard Steven,Addison Wesley, 2003 |

| | |
|---|---|
| 5 | Cryptography and Network Security -- Atul Kahate, 3rd edition, Tata Mc Graw Hill, 2013 3.TCP/IP Protocol Suite -- B. A. Forouzan, 4th Edition, Tata Mc Graw Hill, 2017 |

| Assessment: | |
|---|---|
| Internal Assessment: | |
| Assessment consists of two class tests of 20 marks each. The first class test is to be conducted when approximately 40% syllabus is completed and the second class test when an additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| End Semester Theory Examination: | |
| 1 | Question paper will comprise a total of six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only Four questions need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus. |

| Useful Digital Links | |
|---|---|
| 1 | https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project |
| 2 | https://dvwa.co.uk/ |
| 3 | http://testphp.vulnweb.com/ |

| **Suggested List of Tutorials** | |
|---|---|
| **Sr. No.** | **Title of Tutorials** |
| 1 | To implement Break a Caesar Cipher code. |
| 2 | Develop a network analyzer to monitor incoming and outgoing data packets on a specific network. |
| 3 | To explore **H4cker software** |
| 4 | Create a tool that records and stores every keystroke. |
| 5 | Set up your own lab environment with vulnerable web apps (e.g., DVWA, Mutillidae, or OWASP Juice Shop). |
| 6 | Explore platforms like Metasploit, Immunity Debugger, and IDA Pro. |
| 7 | Study smart contracts and blockchain vulnerabilities. |
| 8 | Learn about WPA/WPA2 cracking, rogue access points, and deauthentication attacks. |

| Course Code: | Course Title | Credit |
|---|---|---|
| **21303** | **Cyber Threat Intelligence** | **2** |

| | |
|---|---|
| **Prerequisite: No Prerequisite** | |
| **Course Objectives:** | |
| 1 | Provide a comprehensive understanding of the cyber threat landscape and the importance of threat intelligence. |
| 2 | Equip students with essential skills in gathering, analyzing, and interpreting threat data. |
| 3 | Develop proficiency in utilizing threat intelligence tools and frameworks through handson exercises. |
| 4 | Introduce advanced methods for predicting and mitigating cyber threats. |
| 5 | Enhance the ability to effectively communicate threat intelligence findings and collaborate with cybersecurity teams. |
| **Course Outcomes: On Successful completion of course, learner will be able to** | |

| | |
|---|---|
| 1 | Demonstrate a thorough understanding of cyber threats, threat actors, and their tactics, techniques, and procedures (TTPs). |
| 2 | Apply various methodologies to gather and analyze cyber threat intelligence data. |
| 3 | Utilize threat intelligence platforms and tools to identify and assess threats. |
| 4 | Develop strategies to predict and mitigate potential cyber threats based on intelligence data. |
| 5 | Produce comprehensive threat intelligence reports and effectively communicate findings to various stakeholders. |

| Module | | Content | Hrs |
|---|---|---|---|
| **1** | | **Introduction to Cyber Threat Intelligence** | **6** |
| | 1.1 | Definition and Importance of CTI, History and Evolution of Cyber Threat Intelligence, Types of Threat Intelligence (Strategic, Operational, Tactical, Technical) | |
| | 1.2 | Understanding Key CTI Concepts and Terminology, The Intelligence Lifecycle, Practical Exercise: CTI Scenario Analysis | |
| | 1.3 | Types of Cyber Threats, Common Attack Vectors, Threat Actors and Their Motivations | |
| **2** | | **Threat Data Collection and Sources** | **6** |
| | 2.1 | Threat Data Collection Techniques:- Passive and Active Data Collection Methods, Open Source Intelligence (OSINT), Human Intelligence (HUMINT) | |
| | 2.2 | Practical Exercise: Collecting Threat Data, Hands-on Exercise in Collecting Data from Various Sources, Ensuring Data Quality and Relevance | |
| | 2.3 | Overview of Popular TIPs, Integrating Data Sources with TIPs, Practical Exercise: Setting Up a TIP | |
| **3** | | **Analyzing Cyber Threat Intelligence** | **5** |
| | 3.1 | Threat Analysis Techniques:- Qualitative and Quantitative Analysis Methods, Indicators of Compromise (IoCs), Analyzing Tactics, Techniques, and Procedures (TTPs) | |
| | 3.2 | Practical Exercise: Threat Analysis, Hands-on Analysis of Collected Threat Data, Using Analytical Tools and Techniques | |
| | 3.3 | Advanced Threat Analysis:- Pattern Recognition and Trend Analysis, Attribution and Profiling Threat Actors, Case Studies of Major Cyber Incidents | |
| **4** | | **Threat Intelligence Frameworks and Models** | **3** |

| | | | |
|---|---|---|---|
| | 4.1 | Introduction to Popular CTI Frameworks | |
| | 4.2 | (MITRE ATT&CK, Diamond Model), Understanding the Kill Chain Model | |
| | 4.3 | Conducting Threat Intelligence Operations, Planning and Executing CTI Operations, Threat Hunting and Incident Response Integration, Case Studies of Successful CTI Operations | |
| **5** | | **Communicating Threat Intelligence** | **5** |
| | 5.1 | Reporting and Disseminating Intelligence:- Writing Effective Threat Intelligence Reports, Visualizing Data for Better Understanding, Communicating Findings to Different Audiences | |
| | 5.2 | Practical Exercise: Reporting Threat Intelligence:- Creating and Presenting Threat Intelligence Reports, Peer Review and Feedback | |
| | 5.3 | Collaboration and Sharing Intelligence:- Information Sharing and Analysis Centers (ISACs), Legal and Ethical Considerations in Sharing Intelligence, Best Practices for Collaboration | |
| **6** | | **Advanced Threat Intelligence Techniques** | **5** |
| | 6.1 | Predictive Intelligence and Threat Forecasting:- Predictive Analytics in CTI, Tools and Techniques for Threat Forecasting, Practical Exercise: Predicting Future Threats | |
| | 6.2 | Cyber Threat Intelligence Automation:- Leveraging AI and Machine Learning in CTI, Automating Data Collection and Analysis, Practical Exercise: Implementing Automation in CTI | |
| | 6.3 | Capstone Project: Real-World CTI Analysis, Comprehensive Threat Intelligence Analysis Project, Presentation of Findings and Recommendations, Whole Review and Doubts Session | |
| **Total** | | | **30** |

| **Textbooks:** | |
|---|---|
| 1 | **Cyber Threat Intelligence: From Strategy to Implementation by Henry Dalziel, 1st Edition** |
| **References:** | |
| 1 | **The Threat Intelligence Handbook:** A Practical Guide for Security Teams to Unlocking the Power of Intelligence by Chris Poulin, et al., 1st Edition |
| **Useful Link for E-Resources:** | |
| 1 | Certified Cyber Threat Intelligence Analyst \| Udemy |
| 2 | Cyber Threat Intelligence Course by IBM \| Coursera |
| 3 | Threat Intelligence Training \| CTIA Certification \| EC-Council (eccouncil.org) |
| 4 | https://medium.com/@ivancmoliveira/reverse-engineering-and-analyzingmalware-wannacry-3ce8b3f6406a |
| 5 | https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf |

| **Assessment:** |
|---|
| **Internal Assessment:** |
| No Internal Assesments |
| **End Semester Theory Examination: No End Semester Exams**<br>**Conduct Oral and Practical Examinations with Term Work Marks.** |

**Suggested List of Experiments**

| **Sr. No.** | **Title of Experiment** |
|---|---|
| 1 | Study on threat modeling for an Organisaton. |
| 2 | Study on the threat intelligence lifecycle, |
| 3 | Study on frameworks like MITRE ATT&CK and STRIDE. |
| 4 | Study about log aggregation tools, |
| 5 | Study vulnerability scanners, |
| 6 | How to evaluate cyber risk using frameworks like CVSS. |
| 7 | Study on threat modeling for an Organisaton. |
| 8 | Study on the threat intelligence lifecycle, |
| 9 | Study on frameworks like MITRE ATT&CK and STRIDE. |

| Course Code: | Course Title | Credit |
|---|---|---|
| **21304** | **Cybersecurity Risk Management and Auditing** | **4** |

| | |
|---|---|
| **Prerequisite: No Prerequisite** | |
| **Course Objectives:** | |
| 1 | Gain a solid understanding of essential cyber security principles and their importance in protecting organizational assets. |
| 2 | Learn the risk management lifecycle and effectively apply risk assessment methodologies, both qualitative and quantitative. |
| 3 | Recognize various types of cyber threats and common attack vectors, and analyze vulnerabilities through real-world case studies. |
| 4 | Create and enforce comprehensive cyber security policies and procedures, ensuring compliance and regular updates. |
| 5 | Develop a robust incident response plan, manage incidents effectively, and perform post-incident activities to enhance organizational resilience. |
| **Course Outcomes: On Successful completion of course, learner will be able to** | |
| 1 | Demonstrate a strong grasp of essential cyber security concepts and their role in protecting organizational assets. |
| 2 | Perform risk assessments using qualitative and quantitative methods, applying frameworks like NIST and ISO/IEC 27005. |
| 3 | Recognize various cyber threats and attack vectors, and analyze vulnerabilities through real-world case studies. |
| 4 | Create, implement, and enforce comprehensive cyber security policies and procedures, ensuring compliance and regular updates. |
| 5 | Develop a robust incident response plan, manage incidents from detection to recovery, and conduct post-incident reviews to enhance resilience. |

| Module | | Content | Hrs |
|---|---|---|---|
| **1** | | **Introduction to Cyber Security and Risk Management** | **8** |
| | 1.1 | Introduction to Cyber Security, Understanding Cyber Security, Importance of Risk Management. | |
| | 1.2 | Key Concepts and Terminology, The Risk Management Lifecycle, Practical Exercise: Risk Management Scenario Analysis. | |
| | 1.3 | Types of Cyber Threats, Common Attack Vectors. | |
| **2** | | **Identifying Threats and Vulnerabilities** | **8** |
| | 2.1 | Understanding Vulnerabilities, Case Studies of Major Cyber Incidents | |
| | 2.2 | Practical Exercise: Identifying Threats and Vulnerabilities | |
| | 2.3 | Introduction to Risk Assessment, Qualitative vs. Quantitative Risk Assessment | |
| **3** | | **Risk Assessment Methodologies** | **8** |
| | 3.1 | Risk Assessment Frameworks:- NIST, ISO/IEC 27005,etc | |
| | 3.2 | Practical Exercise: Understanding Different Frameworks | |
| | 3.3 | Conducting Risk Assessments | |
| **4** | | **Identifying, Analyzing, and Mitigating Risks** | **6** |
| | 4.1 | Identifying and Analyzing Risks, Practical Exercise: Performing a Risk Assessment | |
| | 4.2 | Risk Mitigation Strategies, Risk Avoidance, Risk Reduction | |
| | 4.3 | More on Risk Mitigation, Risk Sharing and Transfer, Risk Acceptance | |
| **5** | | **Implementing Security Controls and Policies** | **7** |
| | 5.1 | Implementing Security Controls, Practical Exercise: Developing a Risk Mitigation Plan | |
| | 5.2 | Developing Cyber Security Policies, Implementing Cyber Security Procedures | |
| | 5.3 | Policy Enforcement and Compliance, Regular Review and Updates, Practical Exercise: Drafting Cyber Security Policies | |
| **6** | | **Cyber Security Frameworks and Incident Response** | **8** |
| | 6.1 | Overview of Key Cyber Security Frameworks, NIST Cybersecurity Framework | |
| | 6.2 | More on Frameworks and Standards, ISO/IEC 27001 and 27002, CIS Controls, Industry-Specific Standards, Practical Exercise: Mapping Organizational Controls to Frameworks | |
| | 6.3 | Incident Response Planning, Incident Detection and Analysis, Containment, Eradication, and Recovery, Post-Incident Activities. Developing an Incident Response Team, Practical Exercise: Simulating an Incident Response | |
| **Total** | | | **45** |

| Textbooks: | |
|---|---|
| 1 | **Information Security Risk Assessment Toolkit:** Practical Assessments through Data Collection and Data Analysis by Mark Talabis, Jason Martin, 1st Edition |
| **References:** | |
| 1 | **Risk Management Framework:** A Lab-Based Approach to Securing Information Systems by James Broad, Kelly Stewart, 1st Edition |
| **Useful Link for E-Resources:** | |
| 1 | Cyber Security Risk Management \| Udemy |
| 2 | Introduction to Cybersecurity & Risk Management Specialization [3 courses] (UC Davis) \| Coursera |
| 3 | Cybersecurity Audit Certificate \| ISACA |
| 4 | https://onlinecourses.nptel.ac.in/noc23_cs127/preview |
| 5 | https://onlinecourses.nptel.ac.in/noc24_cs85/preview |

| **Assessment:** | |
|---|---|
| **Internal Assessment:** | |
| Assessment consists of two class tests of 20 marks each. The first-class test is to be conducted when approx. 40% syllabus is completed and the second-class test when an additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| **End Theory Examination:** | |
| 1 | Question paper will comprise a total of six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only four questions need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus. |

**Suggested List of Experiments**

| Sr. No. | Title of Experiment |
|---|---|
| 1 | Case Studies to be done on each Module for at least five Organizations/Company/Corporate. |

| Course Code: | Course Title | Credit |
|---|---|---|
| **21305** | **Malware Analysis and Reverse Engineering** | **4** |

| | |
|---|---|
| **Prerequisite: No Prerequisite** | |
| **Course Objectives:** | |
| 1 | Provide a comprehensive understanding of the various types of malware and their impact on computer systems. |
| 2 | Equip students with essential skills in static and dynamic malware analysis techniques. |
| 3 | Develop proficiency in reverse engineering and understanding malicious code through hands-on exercises. |
| 4 | Introduce advanced methods for detecting, analyzing, and mitigating sophisticated malware threats. |
| 5 | Enhance the ability to effectively communicate findings and collaborate with cybersecurity teams. |
| **Course Outcomes: On Successful completion of course, learner will be able to** | |
| 1 | Demonstrate a thorough understanding of malware types, behaviors, and the threats they pose. |
| 2 | Apply static and dynamic analysis techniques to dissect and understand malware samples. |
| 3 | Utilize reverse engineering tools to deconstruct and analyze executable files. |
| 4 | Identify and bypass obfuscation and anti-analysis techniques used by advanced malware. |
| 5 | Produce comprehensive analysis reports and effectively communicate technical findings to various stakeholders. |

| Module | | Content | Hrs |
|---|---|---|---|
| **1** | | **Introduction to Malware Analysis** | **8** |
| | 1.1 | Definition and Types of Malware, Historical Perspective and Evolution of Malware, Impact and Consequences of Malware Attacks | |

| | | | |
|---|---|---|---|
| | 1.2 | Goals and Objectives of Malware Analysis, Ethical and Legal Considerations, Malware Analysis Methodologies (Static vs. Dynamic Analysis) | |
| | 1.3 | Creating Isolated Sandboxes, Tools for Malware Analysis (Virtual Machines, Snapshots), Network Simulation and Monitoring Tools | |
| **2** | | **Static Malware Analysis** | **8** |
| | 2.1 | Understanding File Formats (PE, ELF, Mach-O), Hashing and File Fingerprinting, Identifying Packing and Obfuscation Techniques | |
| | 2.2 | Extracting Metadata with Tools (e.g., PEiD, Exeinfo PE), Strings Analysis and Indicators of Compromise (IoCs), File Signature Analysis | |
| | 2.3 | Disassembly with IDA Pro and Ghidra, Code Analysis and Reverse Engineering, Recognizing and Understanding Common Code Constructs | |
| **3** | | **Dynamic Malware Analysis** | **8** |
| | 3.1 | Behavioral Analysis:- Setting Up Dynamic Analysis Tools (e.g., Cuckoo Sandbox), Monitoring File System, Registry, and Network Activity, Identifying Behavioral Indicators | |
| | 3.2 | Memory Analysis: - Introduction to Volatility Framework, Capturing and Analyzing Memory Dumps, Extracting Artifacts from Memory | |
| | 3.3 | Advanced Dynamic Analysis: - Debugging Malware with OllyDbg and x64dbg, API Call Monitoring and Analysis, Identifying Anti-Analysis Techniques and Countermeasures | |
| **4** | | **Reverse Engineering Fundamentals** | **6** |
| | 4.1 | Introduction, Objectives and Use Cases of Reverse Engineering, Legal and Ethical Considerations, Overview of Reverse Engineering Tool | |
| | 4.2 | Assembly Language Basics: - Understanding CPU Architectures (x86, x64), Assembly Language Syntax and Instructions, Converting High-Level Code to Assembly | |
| | 4.3 | Analyzing Executables, Examining Executable Headers, Function Identification and Analysis, Control Flow Graphs and Call Graphs | |
| **5** | | **Advanced Reverse Engineering Techniques** | **7** |
| | 5.1 | Code Obfuscation and Anti-Reversing Techniques, Common Obfuscation Methods (e.g., Packing, Encryption), Identifying and Bypassing Anti-Debugging Mechanisms, Techniques for Deobfuscating Code | |
| | 5.2 | Reversing Network Protocols, Capturing and Analyzing Network Traffic, Understanding Custom Protocols, Reconstructing Protocol Specifications | |
| | 5.3 | Reversing Malicious Code, Case Studies of Reversing RealWorld Malware, Techniques for Extracting Decryption Keys, Analyzing Polymorphic and Metamorphic Malware | |
| **6** | | **Practical Malware Analysis and Reporting** | **8** |

| | | | |
|---|---|---|---|
| | 6.1 | Comprehensive Malware Analysis, End-to-End Analysis of Malware Samples, Documenting Findings and IoCs, Developing Mitigation and Response Strategies | |
| | 6.2 | Reporting and Communication, Writing Detailed Malware Analysis Reports, Communicating Technical Findings to NonTechnical Audiences, Collaboration with Incident Response Teams | |
| | 6.3 | Capstone Project: Real-World Malware Analysis, Practical Exercise: Analyzing a Complex Malware Sample, Presentation of Findings and Defense Strategies, Peer Review and Feedback Session | |
| **Total** | | | **45** |

| **Textbooks:** | |
|---|---|
| 1 | **Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software**, Michael Sikorski and Andrew Honig, 1st Edition. |
| **References:** | |
| 1 | **Malware Analyst's Cookbook and DVD:** Tools and Techniques for Fighting Malicious Code, Michael Ligh, Steven Adair, Blake Hartstein, and Matthew Richard, 1st Edition |
| **Useful Link for E-Resources:** | |
| 1 | Reverse Engineering & Malware Analysis in 21 Hours \| REMAC+ \| Udemy |
| 2 | FREE Intro to Malware Analysis & Reverse Engineering Online Training Course \| Cybrary |
| 3 | MARE- Malware Analysis and Reverse Engineering Certification Course (hackerassociate.com) |
| 4 | https://blog.securitybreak.io/my-top-books-to-learn-malware-analysis-andreverse-engineering-2ae1c6e209b9 |
| 5 | https://medium.com/@ivancmoliveira/reverse-engineering-and-analyzingmalware-wannacry-3ce8b3f6406a |

| **Assessment:** | |
|---|---|
| **Internal Assessment:** | |
| Assessment consists of two class tests of 20 marks each. The first-class test is to be conducted when approx. 40% syllabus is completed and the second-class test when an additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| **End Theory Examination:** | |
| 1 | Question paper will comprise a total of six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only four questions need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus. |

| **Suggested List of Experiments** |
|---|

| Sr. No. | Title of Experiment |
|---|---|
| 1 | Packet sniffing with Wire shark |
| 2 | Capturing intruders through packet inspection |
| 3 | Analysis of various Malware types and behavior |
| 4 | Basic Static Analysis |
| 5 | Basic Dynamic Analysis |
| 6 | Analyzing windows programs |
| 7 | Android malware analysis |
| 8 | Data encoding and malware countermeasures |
| 9 | Comparative study of various malware analysis tools |
| 10 | Tools available in Antivirus Application. |
| | |

| Course Code: | Course Title | Credit |
|---|---|---|
| **21306** | **Machine Learning I** | **4** |

| Prerequisite: Engineering Mathematics, Data Structures, Algorithms | |
|---|---|
| Course Objectives: | |
| 1 | To introduce the basic concepts and techniques of Machine Learning. |
| 2 | To acquire in depth understanding of various supervised and unsupervised algorithms |

| | |
|---|---|
| 3 | To be able to apply various ensemble techniques for combining ML models. |
| 4 | To demonstrate dimensionality reduction techniques. |
| Course Outcomes: | |
| 1 | To acquire fundamental knowledge of developing machine learning models. |
| 2 | To select, apply and evaluate an appropriate machine learning model for the given |
| 3 | To demonstrate ensemble techniques to combine predictions from different models. |
| 4 | To demonstrate the dimensionality reduction techniques. |

| Module | | Content | Hrs |
|---|---|---|---|
| 1 | | Introduction to Machine Learning | 5 |
| | 1.1 | Machine Learning, Types of Machine Learning, Issues in Machine Learning, Application of Machine Learning, Steps in developing a Machine Learning Application. | |
| | 1.2 | Training Error, Generalization error, Overfitting, Underfitting, Bias-Variance trade-off. | |
| 2 | | Learning with Regression and Trees | 10 |
| | 2.1 | Learning with Regression: Linear Regression, Multivariate Linear Regression, Logistic Regression. | |
| | 2.2 | Learning with Trees: Decision Trees, Constructing Decision Trees using Gini Index (Regression), Classification and Regression Trees (CART) | |
| | 2.3 | Performance Metrics: Confusion Matrix, [Kappa Statistics], Sensitivity, Specificity, Precision, Recall, F-measure, ROC curve | |
| 3 | | Ensemble Learning | 7 |
| | 3.1 | Understanding Ensembles, K-fold cross validation, Boosting, Stumping, | |
| | | XGBoost | |
| | 3.2 | Bagging, Subagging, Random Forest, Comparison with Boosting, Different ways to combine classifiers | |
| 4 | | Learning with Classification | 08 |
| | 4.1 | Support Vector Machine<br>Constrained Optimization, Optimal decision boundary, Margins and support vectors, SVM as constrained optimization problem, Quadratic Programming, SVM for linear and nonlinear classification, Basics of | |
| | | Kernel trick. | |
| | 4.2 | Support Vector Regression, Multiclass Classification | |
| 5 | | Learning with Clustering | 8 |

| | | | |
|---|---|---|---|
| | 5.1 | Introduction to clustering with overview of distance metrics and major clustering approaches. | |
| | 5.2 | Graph Based Clustering: Clustering with minimal spanning tree<br>Model based Clustering: Expectation Maximization<br>Algorithm, Density Based Clustering: DBSCAN | |
| 6 | | Dimensionality Reduction | 7 |
| | 6.1 | Dimensionality Reduction Techniques, Principal Component Analysis,<br>Linear Discriminant Analysis, Singular Valued Decomposition. | |
| **Total** | | | **45** |

| | |
|---|---|
| Textbooks: | |
| 1 | Peter Harrington, ―Machine Learning n Action‖, DreamTech Press |
| 2 | Ethem Alpaydın, ―Introduction to Machine Learning‖, MIT Press |
| 3 | Tom M. Mitchell, ―Machine Learning‖ McGraw Hill |
| 4 | Stephen Marsland, ―Machine Learning An Algorithmic Perspective‖, CRC Press |
| References: | |
| 1 | Han Kamber, ―Data Mining Concepts and Techniques‖, Morgan Kaufmann Publishers |
| 2 | Margaret. H. Dunham, ―Data Mining Introductory and Advanced Topics, Pearson Education |
| 3 | Kevin P. Murphy , Machine Learning ― A Probabilistic Perspective‖ |
| 4 | Samir Roy and Chakraborty, ―Introduction to soft computing‖, Pearson Edition. |
| 5 | Richard Duda, Peter Hart, David G. Stork, ―Pattern Classification‖, Second Edition, Wiley Publications. |
| Assessment: | |
| Internal Assessment: | |
| Assessment consists of two class tests of 20 marks each. The first class test is to be conducted when approximately 40% syllabus is completed and the second class test when an additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| End Semester Theory Examination: | |
| 1 | Question paper will comprise a total of six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |

| | |
|---|---|
| 4 | Only Four questions need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus. |

| Useful Digital Links | |
|---|---|
| 1 | Data sets for Machine Learning algorithms: https://www.kaggle.com/datasets |
| 2 | Machine Learning repository- https://archive.ics.uci.edu/ml/index.php |
| 3 | Machine Learning from Coursera |
| 4 | https://towardsdatascience.com/machine-learning/home |
| 5 | https://onlinecourses.nptel.ac.in/noc21_cs85/preview |

| **Suggested List of Experiments** | |
|---|---|
| **Sr. No.** | **Title of Experiment** |
| 1 | To implement Linear Regression. |
| 2 | To implement Logistic Regression. |
| 3 | To implement Ensemble learning (bagging/boosting) |
| 4 | To implement multivariate Linear Regression. |
| 5 | To implement SVM |
| 6 | To implement PCA/SVD/LDA |
| 7 | To implement Graph Based Clustering |
| 8 | To implement DB Scan |
| 9 | To implement CART |
| 10 | To implement LDA |

## Program Structure for Second Year B. Voc Cyber Security and Digital Forensics

## UNIVERSITY OF MUMBAI (With Effect from 2025-2026)

## Semester IV

| **Course Code:** | **Course Title** | **Credit** |
|---|---|---|
| **21401** | **Professional Skill-IV (Aptitude and Logic Building)** | **2** |

| Prerequisite: | |
|---|---|
| Course Objectives: | |
| 1 | This course aims to provide an exposure in creating and delivering effective multimedia presentations that convey the key points. |
| 2 | Analyzing data in spreadsheet |
| 3 | How to write technical report |

| Course Outcomes: | |
|---|---|
| 1 | Understand Programs and Computers |
| 2 | Learn how programs and codes operate by using code and scratch. |
| 3 | To develop your critical thinking and reasoning skills. |
| 4 | The capacity to comprehend searching and sorting |
| 5 | Capacity to use formal mathematics to define computer programs (such as recursive functions) |
| 6 | Determine the truth value of unquantified phrases by using logical principles to define sets using the list or set builder notation and connecting symbolic laws of logic. |

| | | | |
|---|---|---|---|
| I | **Introduction to Computers** | Computer Systems, Computer Languages, Software Development, Operating System, Number Systems and their conversion, Crypt arithmetic Problems, Pseudocode and Flowchart | **8** |
| II | **Introduction to Code and Scratch** | Introduction to code (Sequence, if..else and Loops) Design a small code in scratch(animation) | **4** |
| III | **Critical thinking and logical reasoning** | Critical Thinking: What does it mean to think critically? An overview of definition, Computer programming and logical thinking | **5** |
| IV | **Searching and Sorting Techniques** | Searching Techniques: Linear Search, Binary Search Sorting Techniques: Selection, Insertion, | **5** |
| V | **Quantitative Abilities** | Problems on Ages Problems on Profit and Loss<br>Problems on Simple and Compound Interest Problems on Time and Distance | **4** |
| VI | **Logical Reasoning & Verbal Reasoning** | Number Series Alpha Numerical, Letter & Symbol Series Numerical and Alphabet Puzzles Seating Arrangement<br>Para – Jumble, Text Completion | **4** |
| **Total** | | | **30** |

| Textbooks: | |
|---|---|
| 1 | Computational Thinking, Karl Beecher BCS, The Chartered Institute for IT, 1th Edition,2017 |
| 2 | Introduction to Algorithm ,Thomas Corman,PHI,3th Edition,2010 |

| References: | |
|---|---|
| 1 | Think Smarter: Critical Thinking to Improve Problem-Solving and Decision-Making Skills Michael Kallet, Wiley, 2nd Edition, 2014 |

Assessment:

Internal Assessment:

No Internal Assessment

**End Semester Theory Examination: No End Semester Exams**
**Conduct Oral and Practical Examinations with Term Work Marks.**

| Useful Digital Links | |
|---|---|
| 1 | https://www.tutorialspoint.com/basics_of_computers/basics_of_computers_introduction.htm |
| 2 | https://plato.stanford.edu/entries/critical-thinking/ |
| 3 | https://studio.code.org/s/courseb-2020 |
| 4 | https://scratch.mit.edu/projects/editor/?tutorial=getStarted |
| 5 | https://www.careerride.com/mcq/logical-reasoning-quantitative-aptitude-questions-319.aspx |

| Course Code: | Course Title | Credit |
|---|---|---|
| **21402** | **Security Architecture and Engineering** | **3** |

| | |
|---|---|
| Prerequisite: | |
| Course Objectives: | |
| 1 | The course introduces to security engineering process and design. |
| 2 | The students should get exposer to older and modern Security Models. |
| 3 | They shall learn to Information Security, assess and mitigate the vulnerabilities. |
| Course Outcomes: | |
| 1 | Implement and manage engineering processes using secure design principles |
| 2 | Understand the fundamental concepts of security models. |
| 3 | Select controls based upon systems security requirements. |
| 4 | Understand the security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption) |
| 5 | Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements. |
| 6 | Understand Modern Security Model and their use. |

| | | | |
|---|---|---|---|
| I | **Secure System Design Principles** | Secure System Design Principles, Integrated Systems, Journey Towards Zero Trust<br>Security Models: Security Models, Biba Integrity Model Bell LaPadula model, TCSEC, Common criteria. | **5** |

| | | | |
|---|---|---|---|
| II | **Select System Security Controls** | The security controls, seven different types: preventative(preventing unauthorized action on an information system), corrective(correcting an information system after an unauthorized action), detective(detecting unauthorized action), compensating(compensate an information system for a risk or vulnerability) , deterrent(controls that are used to deter would-be attackers), directive(controls that guide the subjects to comply with a security policy) and recovery(controls that are needed to recover from a disaster) | **8** |
| III | **Assessment of Traditional Security Architectures** | Assessment of Traditional Security Architectures, Distributed Systems, Assessment of Non-traditional Security Architectures<br>Securing Embedded Devices, High Performance Systems | **5** |
| | | | |
| IV | **Security of Information System** | Access control mechanisms, secure memory management, layering and virtualization which can be used to protect systems without disrupting the system. | **4** |
| V | **Assess and mitigate the vulnerabilities** | Client security issues: 'Applets', server security issues: Vulnerabilty mitigaton, database Security: Data breach, 'inference', 'aggregation' are other database risks, Cryptographic systems: DES, 3DES, AES, Blowfish, RSA, cloud-based systems, IoT and distributed systems of security architecture and knows how to mitigate them. | **4** |
| VI | **Moderm Security Models** | Time Based Security, Cyber Kill Chain, TBS + Kill Chain + MITRE ATT&CK, Architecting for Visibility & Detection,<br>Architecting for Incident Response, Zero Trust Model | **4** |
| | | **Total** | **30** |

| | |
|---|---|
| Textbooks: | |
| 1 | Securing Systems: Applied Security Architecture and Threat Models by Brook S E Schoenfield, CRC Press. |
| 2 | Security Architecture How & Why by Author: Tom Madsen, Accenture, Denmark, River Publishers Series in Digital Security and Forensics |
| References: | |
| 1 | Information Security Architecture: An Integrated Approach to Security in the Organization, Second Edition by Jan Killmeyer. |
| 2 | Practical Cybersecurity Architecture: A guide to creating and implementing robust designs for cybersecurity architects by Ed Moyle (Author), Diana Kelley (Author) |

| Assessment: | |
|---|---|
| Internal Assessment: | |
| Assessment consists of two class tests of 20 marks each. The first class test is to be conducted when approximately 40% syllabus is completed and the second class test when an additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| End Semester Theory Examination: | |
| 1 | Question paper will comprise a total of six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only Four questions need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus. |

| Useful Digital Links | |
|---|---|
| 1 | https://www.educba.com/security-architecture/ |
| 2 | https://www.pluralsight.com/courses/security-architecture-engineering-designprinciples-cissp |
| 3 | https://www.infosecinstitute.com/skills/learning-paths/security-architecture/ |
| 4 | http://www.ndl.iitkgp.ac.in/he_document/nptel/courses_106_106_106106141_video_lec7 |

| **Suggested List of Tutorials** | |
|---|---|
| **Sr. No.** | **Title of Tutorials** |
| 1 | Study on Security Architecture: Types, Benefits https://www.geeksforgeeks.org/security-architecture-types-elements-frameworkand-benefits/ |
| 2 | Study on Elements of Security Architecture |
| 3 | Examples of Security Architecture Framework |
| 4 | Zero Trust Architecture in Security, https://www.geeksforgeeks.org/zero-trustarchitecture-in-security/ |
| 5 | Zero Security Model, https://www.geeksforgeeks.org/zero-security-model/ |
| 6 | How to Use Docker Content Trust to Verify Docker Container Images, https://www.geeksforgeeks.org/how-to-use-docker-content-trust-to-verify-dockercontainer-images/ |

| Course Code: | Course Title | Credit |
|---|---|---|
| **21403** | **Digital Forensics** | **3** |

| | |
|---|---|
| Prerequisite: | |
| Course Objectives: | |
| 1 | To understand the various computer and cyber-crimes in the digital world. |
| 2 | To understand a significance of digital forensics life cycle, underlying forensics principles and investigation process. |
| 3 | To understand the importance of File system management with respect to computer forensics. |
| 4 | To be able to identify the live data in case of any incident handling and application of appropriate tools and practices for the same. |
| 5 | To Develop the skills in application of various tools and investigation report writing with suitable evidences. |
| 6 | To be able to identify the network and mobile related threats and recommendation of suitable forensics procedures for the same. |
| Course Outcomes: | |
| 1 | Identify and define the class for various computer and cyber-crimes in the digital world. |
| 2 | Understand the need of digital forensic and the role of digital evidence. |
| 3 | Understand and analyze the role of File systems in computer forensics. |
| 4 | Demonstrate the incident response methodology with the best practices for incidence response with the application of forensics tools. |
| 5 | Generate/Write the report on application of appropriate computer forensic tools for investigation of any computer security incident . |
| 6 | Identify and investigate threats in network and mobile. |

| | | | |
|---|---|---|---|
| I | **Prerequisite** | Computer Hardware: Motherboard, CPU, Memory: RAM, Hard Disk Drive (HDD), Solid State Drive (SSD), Optical drive<br>Computer Networks: Introduction CN Terminology: Router, Gateway, OSI and TCP/IP Layers<br>Operating Systems: Role of OS in file management, Memory management utilities, Fundamentals of file systems used in Windows and Linux. | **5** |

| | | | |
|---|---|---|---|
| II | **Introduction to Cybercrime and Computercrime** | Definition and classification of cybercrimes: Definition, Hacking, DoS Attacks, Trojan Attacks, Credit Card Frauds, Cyber Terrorism, Cyber Stalking.<br>Definition and classification of computer crimes: Computer Viruses, Computer Worms.<br>Prevention of Cybercrime: Steps that can be followed to prevent cybercrime, Hackers, Crackers, Phreakers. | **5** |
| II<br>I | **Introduction to Digital Forensics and Digital Evidences** | Introduction to Digital Forensics: Introduction to Digital Forensics and lifecycle, Principles of Digital Forensic.<br>Introduction to Digital Evidences: Challenging Aspects of Digital Evidence, Scientific Evidence, Presenting Digital Evidence.<br>Digital Investigation Process Models: Physical Model, Staircase Model, Evidence Flow Model. | **6** |
| I<br>V | **Computer Forensics** | OS File Systems Review:<br>Windows Systems- FAT32 and NTFS, UNIX File Systems, MAC File Systems<br>Windows OS Artifacts: Registry, Event Logs<br>Memory Forensics : RAM Forensic Analysis, Creating a RAM Memory Image, Volatility framework, Extracting Information<br>Computer Forensic Tools: Need of Computer Forensic Tools, Types of Computer Forensic Tools, Tasks performed by Computer Forensic Tools | **6** |
| V | **Incident Response Management, Live Data Collection and Forensic Duplicatio n** | Incidence Response<br>Methodology: Goals of Incident Response, Finding and Hiring IR Talent<br>IR Process: Initial Response, Investigation, Remediation, Tracking of Significant Investigative Information.<br>Live Data Collection: Live Data Collection on Microsoft Windows,<br>Forensic Duplication: Forensic Duplicates as Admissible Evidence, Forensic Duplication Tools: Creating a Forensic evidence,<br>Duplicate/Qualified Forensic<br>Duplicate of a Hard Drive. | **4** |
| V<br>I | **Forensic Tools and Report Writing** | Forensic Image Acquisition in Linux: Acquire an Image with dd Tools, Acquire an Image with<br>Forensic Formats, Preserve Digital<br>Evidence with Cryptography, Image Acquisition over a Network, Acquire Removable Media<br>Forensic Investigation Report Writing: Reporting Standards, Report Style and Formatting, Report Content and Organization. | **4** |
| **Total** | | | **30** |

Textbooks:

| | |
|---|---|
| 1 | Digital Forensics by Dr. Dhananjay R. Kalbande Dr. Nilakshi Jain, Wiley Publications, First Edition, 2019. |
| 2 | Digital Evidence and Computer Crime by Eoghan Casey, Elsevier Academic Press, Third Edition, 2011. |
| 3 | Incident Response & Computer Forensics by Jason T. Luttgens, Matthew Pepe and Kevin Mandia, McGraw-Hill Education, Third Edition (2014). |
| 4 | Network Forensics : Tracking Hackers through Cyberspace by Sherri Davidoff and Jonathan Ham, Pearson Edu,2012 |
| 5 | Practical Mobile Forensic by Satish Bommisetty, Rohit Tamma, Heather Mahalik, PACKT publication, Open source publication, 2014 ISBN 978-1-78328-831-1 6. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory by Michael Hale Ligh (Author), Andrew Case (Author), Jamie Levy (Author), AAron Walters (Author), Publisher : Wiley; 1st edition (3 October 2014), |

References:

| | |
|---|---|
| 1 | Scene of the Cybercrime: Computer Forensics by Debra Littlejohn Shinder, Syngress Publication, First Edition, 2002. |
| 2 | Digital Forensics with Open Source Tools by Cory Altheide and Harlan Carvey, Syngress Publication, First Edition, 2011. |
| 3 | Practical Forensic Imaging Securing Digital Evidence with Linux Tools by Bruce Nikkel, NoStarch Press, San Francisco,(2016) |
| 4 | Android Forensics : Investigation, Analysis, and Mobile Security for Google Android by Andrew Hogg, Elsevier Publication,2011 |
| 5 | Scene of the Cybercrime: Computer Forensics by Debra Littlejohn Shinder, Syngress Publication, First Edition, 2002. |

Assessment:

Internal Assessment:

Assessment consists of two class tests of 20 marks each. The first class test is to be conducted when approximately 40% syllabus is completed and the second class test when an additional 40% syllabus is completed. Duration of each test shall be one hour.

End Semester Theory Examination:

| | |
|---|---|
| 1 | Question paper will comprise a total of six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only Four questions need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus. |

| |
|---|
| https://www.pearsonitcertification.com/articles/article.aspx?p=462199&seqNum=2 |
| https://flylib.com/books/en/3.394.1.51/1/ |
| https://www.sleuthkit.org/autopsy/ |
| http://md5deep.sourceforge.net/md5deep.html |
| https://tools.kali.org/ |
| https://kalilinuxtutorials.com/ |
| https://accessdata.com/product-download/ftk-imager-version-4-3-0 |
| https://www.amazon.in/Art-Memory-Forensics-Detecting-Malware/dp/1118825098 |

| **Suggested List of Experiments** | |
|---|---|
| **Sr. No.** | **Title of Experiment** |
| 1 | Case Studies |
| 2 | Research Papers study |
| 3 | Learn white papers fromComputer Forensics Resource Center: NIST Draft Special Publication 800-101 : |
| 4 | Make a bootable pen drive. |
| 5 | forensic duplication or mirroring :Disk Imaging |

| **Course Code:** | **Course Title** | **Credit** |
|---|---|---|
| **21404** | **Penetration Testing and Vulnerability Assessment** | **4** |

| |
|---|
| **Prerequisite: No Prerequisite** |
| **Course Objectives:** |

| | |
|---|---|
| 1 | Equip learners with essential skills in penetration testing, starting with Information Gathering to understand targeted systems. |
| 2 | Instruct learners on how to leverage vulnerabilities to gain unauthorized system access. |
| 3 | Offer knowledge on maintaining access, extracting data, and covering tracks after gaining unauthorized access. |
| 4 | Focus on common vulnerabilities in web applications and effective strategies to mitigate them. |
| 5 | Provide a comprehensive understanding of the entire cyberattack process, from initial information gathering to exploitation and post-exploitation techniques. |
| **Course Outcomes: On Successful completion of course, learner will be able to** | |
| 1 | Demonstrate ability to gather information and detect open ports and services effectively. |
| 2 | Successfully exploit system vulnerabilities to gain unauthorized access and execute payloads. |
| 3 | Master post-exploitation tactics, including maintaining access, data extraction, and employing social engineering. |
| 4 | Identify and mitigate common web application vulnerabilities, ensuring secure data transactions and user authentication. |
| 5 | |
| | Gain a thorough understanding of cybersecurity, from initial penetration testing phases to practical exploitation and post-exploitation strategies. |

| Module | | Content | Hrs |
|---|---|---|---|
| **1** | | **Information Gathering** | **6** |
| | 1.1 | Introduction to Penetration Testing Skills, Overview of Penetration Testing, Key Skills and Tools for Penetration Testers | |
| | 1.2 | Information Gathering: Whois and Dmitry, Google and GHDB, Shodan CLI, DNS Reconnaissance, Online Databases | |

| | | | |
|---|---|---|---|
| **2** | | **Scanning and Enumeration** | **8** |
| | 2.1 | Scanning Techniques, Introduction to Scanning, Nmap Scanning, NSE Scripting (Nmap Scripting Engine) | |
| | 2.2 | Enumeration and Vulnerability Detection, Enumeration Concepts, Common Services and Ports, Msfconsole (Metasploit Framework), Enumeration Tools, Vulnerability Detection Methods, Nessus (Vulnerability Scanner) | |
| **3** | | **Exploitation** | **9** |
| | 3.1 | Introduction to Exploitation Techniques | |
| | 3.2 | Exploitation Methods: Brute Force Tools, Exploits Database, Msfconsole, Exploiting Manually | |
| | 3.3 | Payloads: Msfvenom Payloads, Payloads Automation, Meterpreter | |
| **4** | | **Post Exploitation** | **6** |
| | 4.1 | Introduction to Post Exploitation Tactics | |
| | 4.2 | Post Exploitation Techniques: Local vs. Remote Exploits, Privilege Escalation, Persistence, Disabling Security | |
| | 4.3 | Social Engineering, Online Services, BeEF, Phishing Frameworks, Advanced Techniques | |
| **5** | | **Web Application Security Fundamentals** | **9** |
| | 5.1 | Introduction to Web Application Security, Overview of Web Application Security, Importance and Impact of Web Security | |
| | 5.2 | Web Application Vulnerabilities and Mitigation, Understanding Common Web Vulnerabilities, HTML Basics, Introduction to OWASP (Open Web Application Security Project), Cross-Site Scripting (XSS), Local File Inclusion (LFI) / Remote File Inclusion (RFI), Brute Force Attacks | |
| | | | |
| **6** | | **Advanced Web Security Techniques** | **7** |
| | 6.1 | Web Application Vulnerabilities and Mitigation (Continued), SQL Injection, Web Payloads, Reverse Shell | |
| | 6.2 | Burp Suite, Introduction to Burp Suite, Proxy, Repeater, Intruder, Encoder | |
| | | **Total** | **45** |

**Textbooks:**

| | |
|---|---|
| 1 | **The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws by** Dafydd Stuttard, Marcus Pinto**, 2nd Edition** |
| **References:** | |
| 1 | **Advanced Penetration Testing: Hacking the World's Most Secure Networks:** by Wil Allsopp, 1st Edition |
| **Useful Link for E-Resources:** | |
| 1 | Cybersecurity course \| Vulnerability Assessment \| VAPT \| Udemy |
| 2 | Vulnerability Assessment and Penetration Testing Certification - IIT Kanpur (simplilearn.com) |
| 3 | Vulnerability Assessment and Penetration Testing (VAPT) Courses \| Koenig Solutions (koenig-solutions.com) |

| **Assessment:** | |
|---|---|
| **Internal Assessment:** | |
| Assessment consists of two class tests of 20 marks each. The first-class test is to be conducted when approx. 40% syllabus is completed and the second-class test when an additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| **End Theory Examination:** | |
| 1 | Question paper will comprise a total of six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only four questions need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus. |

| **Suggested List of Experiments** | |
|---|---|
| **Sr. No.** | **Title of Experiment** |
| 1 | Learn and Understanding the Attack Surface: |
| 2 | Learn to Adapting to Evolving Threats: |
| 3 | Learn to Reducing Attack Vectors: |
| 4 | Learn to Enhancing Security Measures |
| 5 | Case Study on Risk Management |

| Course Code: | Course Title | Credit |
|---|---|---|
| **21405** | **Cybercrime Investigation Techniques** | **4** |

| | |
|---|---|
| **Prerequisite: No Prerequisite** | |
| **Course Objectives:** | |
| 1 | Provide an in-depth understanding of the techniques and tools used in cybercrime investigations. |
| 2 | Equip students with practical skills in digital forensics and evidence collection. |
| 3 | Develop proficiency in analysing and interpreting digital evidence. |
| 4 | Introduce methodologies for tracking and identifying cybercriminals. |

| | |
|---|---|
| 5 | Enhance the ability to prepare and present comprehensive cybercrime investigation reports. |
| **Course Outcomes: On Successful completion of course, learner will be able to** | |
| 1 | Demonstrate knowledge of cybercrime investigation techniques and digital forensics principles. |
| 2 | Apply digital forensics tools to collect and analyze electronic evidence. |
| 3 | Conduct thorough investigations of cyber incidents and identify perpetrators. |
| 4 | Develop and document a step-by-step investigative process for cybercrime cases. |
| 5 | Produce detailed and accurate reports on cybercrime investigations and present findings effectively. |

| Module | | Content | Hrs |
|---|---|---|---|
| **1** | | **Digital Data Handling** | **9** |
| | 1.1 | Introduction to Digital Data Handling, File and Disk Handling, Viewing File Contents, Examining Disk Structures, Hexadecimal Editor, Manipulating Offsets | |
| | 1.2 | Encoding and Numeric Systems: Data Encoding Techniques, Numeric Representations, Digital Storage Capacities, Features of Solid State Drives (SSDs) | |
| | 1.3 | Automated Extraction and Metadata Examination: Automated Data Extraction, Techniques for Extracting Data, Automated Data Carving Methods, Analysis of Windows System Files | |
| | 1.4 | Metadata Examination, Metadata Inspection, Modified, Accessed, Created (MAC) Timestamps, Editing Metadata Information | |
| **2** | | **Advanced File Forensics** | **7** |
| | 2.1 | Introduction to File Forensics Techniques,<br>Techniques: Methods of Concealing Information, Identifying Concealed Files, Extracting Concealed Files, Generating Hidden Files | |
| | 2.2 | Hard Drive Analysis: Examination of Hard Disk Drives, Analysis of System Files, Master File Table (MFT) Review | |
| | 2.3 | Utilizing Forensic Toolkit (FTK): Application of Forensic Toolkit (FTK) | |
| **3** | | **Evidence Collection Techniques** | **8** |

| | | | |
|---|---|---|---|
| | 3.1 | Introduction to Analysis of Digital Artifacts: Overview of Digital Artifacts, Directories Containing Artifacts, Examination of Browser Artifacts, Investigating Shadow Copies | |
| | 3.2 | Registry Data Analysis: Scrutiny of Registry Data, Retrieving Information, NTUSER.DAT File Analysis, Conducting General Searches, Employing Registry Viewing Tools | |
| **4** | | **Comprehensive Analysis** | **7** |
| | 4.1 | Memory Examination: In-Depth Memory Analysis, Creation of Memory Images, Utilizing Volatility for Analysis, Data Carving from RAM | |
| | 4.2 | Event Analysis: Analysis of System Events, Utilizing Event Viewing Tools, Establishing Audit Policies, Customized Search Techniques | |
| | 4.3 | Network Analysis: Analysis of Network Traffic, Examination of Service Protocols, Identification of Darknet Connections | |
| | 4.4 | Malware Investigation: Investigation of Malicious Software, Basic Static Analysis, Fundamental Dynamic Analysis | |
| **5** | | **Incident Response** | **7** |
| | 5.1 | Introduction to Incident Response and Reporting, Developing Incident Response Plans, Roles and Responsibilities, Incident Handling Procedures | |
| | 5.2 | Live Response Techniques: Conducting Live Forensics, Capturing System State, Preserving Evidence | |
| **6** | | **Forensic Reporting and Analysis** | **7** |
| | 6.1 | Forensic Reporting, Documenting Findings, Writing Forensic Reports, Legal Considerations in Reporting | |
| | 6.2 | Case Studies and Practical Exercises, Analyzing Case Studies, Practical Forensic Exercises | |
| | | **Total** | **45** |

| **Textbooks:** | |
|---|---|
| 1 | **Investigating the Cyber Breach: The Digital Forensics Guide for the Network Engineer:** by Joseph Muniz, Aamir Lakhani, **1st Edition** |
| **References:** | |
| 1 | **Incident Response & Computer Forensics:** by Jason T. Luttgens, Matthew Pepe, Kevin Mandia, 3rd Edition |
| 2 | **Cyber Crime and Digital Evidence: Materials and Cases:** by Thomas K. Clancy, Susan W. Brenner, **1st Edition** |
| **Useful Link for E-Resources:** | |
| 1 | Cybersecurity course \| Vulnerability Assessment \| VAPT \| Udemy |
| 2 | Vulnerability Assessment and Penetration Testing Certification - IIT Kanpur (simplilearn.com) |
| 3 | Vulnerability Assessment and Penetration Testing (VAPT) Courses \| Koenig Solutions (koenig-solutions.com) |

| **Assessment:** |
|---|
| **Internal Assessment:** |

| | |
|---|---|
| Assessment consists of two class tests of 20 marks each. The first-class test is to be conducted when approx. 40% syllabus is completed and the second-class test when an additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| **End Theory Examination:** | |
| 1 | Question paper will comprise a total of six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only four questions need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus. |

| **Suggested List of Experiments** | |
|---|---|
| **Sr. No.** | **Title of Experiment** |
| 1 | Learn Understanding Physical Evidence |
| 2 | Learn Documentation and Photography |
| 3 | Learn Bloodstain Pattern Analysis |
| 4 | Learn Special Scene Considerations |
| 5 | Learn Emerging Technology |

| Course Code: | Course Title | Credit |
|---|---|---|
| **21406** | **Network Forensics** | **4** |

| | |
|---|---|
| **Prerequisite: No Prerequisite** | |
| **Course Objectives:** | |
| 1 | Equip learners with a deep understanding of network protocols, packet structures, and advanced networking tools. |
| 2 | Teach methodologies for detecting intrusions using tools like Wireshark, TShark, and Scapy. |
| 3 | Provide insights into network analysis using frameworks like Zeek, focusing on log monitoring and packet replay for investigations. |
| 4 | Instruct learners on network investigations, anomaly detection, and the use of tools like Network Miner and file carvers. |
| 5 | Focus on configuring and operating IPS/IDS systems, Sysmon, and Snort for effective network security. |
| **Course Outcomes: On Successful completion of course, learner will be able to** | |
| 1 | Learners will demonstrate proficiency in analyzing network protocols and detecting intrusions using advanced tools. |
| 2 | Learners will gain the ability to automate processes, monitor data logs, and use Zeek for detailed network analysis. |

| | |
|---|---|
| 3 | Learners will acquire skills in conducting thorough network investigations, identifying anomalies, and analyzing wireless traffic. |
| 4 | Learners will develop competence in configuring and using Sysmon, Snort, and other IPS/IDS systems for network security. |
| | |
| 5 | Learners will achieve a thorough understanding of network security mitigation strategies, including the operation and configuration of IDS/IPS systems. |

| Module | | Content | Hrs |
|---|---|---|---|
| **1** | | **Intrusion Detection** | **8** |
| | 1.1 | Networking: Overview of Network Protocols, Understanding Packet Structure, Utilizing Netstat and ProcMon, Exploring SysInternal Tools | |
| | 1.2 | Intrusion Detection Methods: Advanced Wireshark for Network Attacks, TShark Analysis Techniques, Integrating GeoIP for Enhanced Detection, Applying the Scapy Module | |
| | 1.3 | Crafting and Analyzing Packets: Techniques for Crafting Packets, Analyzing Packet Data, Working with IPv6 Protocols | |
| **2** | | **Network Analysis** | **7** |
| | 2.1 | Introduction to Zeek: Understanding Zeek and Its Capabilities, Managing Output Logs, Automating Processes with Zeek | |
| | 2.2 | Monitoring and Parsing: Monitoring Data into Logs with Zeek, ZeekCut Parsing Techniques | |
| | 2.3 | Investigative Techniques: Replaying Packets for Investigation, Creating Detailed Timelines from Data | |
| **3** | | **Case Investigation** | **9** |
| | 3.1 | Investigation Process: Understanding the Investigation Process, Identifying and Mitigating MiTM Attacks, Finding Network Anomalies | |
| | 3.2 | Flow Analysis and Network File Carving: Conducting Flow Analysis, Techniques for Network File Carving, Using NetworkMiner, Employing File Carvers | |
| | 3.3 | Wireless Traffic and Access: Capturing and Analyzing Wireless Traffic, Gaining Access Through Wi-Fi Networks, Investigating HTTPS Traffic | |
| **4** | | **Mitigation** | **6** |

| | | | |
|---|---|---|---|
| | 4.1 | IPS and IDS Systems: Introduction to IPS and IDS Systems, Understanding IDS/IPS Operation Processes, Configuring IDS/IPS for Optimal Performance | |
| | 4.2 | Sysmon: Installing and Configuring Sysmon, Capturing and Analyzing Network Events | |
| | 4.3 | Tools for Intrusion Detection: Using Snort for Intrusion Detection | |
| **5** | | **Introduction to Incident Response (IR)** | **8** |
| | 5.1 | Overview of Incident Response Frameworks, Incident Response Lifecycle, Preparation, Detection, Containment, Eradication Recovery, Role of Incident Response Teams (IRTs) and Responsibilities | |
| | 5.2 | Incident Detection and Analysis, Techniques for Detecting Security Incidents, Incident Triage and Initial Assessment, Log Analysis and Correlation | |
| | 5.3 | Incident Containment and Eradication: Strategies for Containing Incidents, Steps for Eradicating Threats, Post-Incident Recovery and Lessons Learned | |
| **6** | | **Threat Hunting** | **7** |
| | 6.1 | Threat Hunting Fundamentals, Introduction to Threat Hunting, Proactive vs. Reactive Threat Hunting Approaches, Using Threat Intelligence for Hunting | |
| | 6.2 | Advanced Threat Hunting Techniques (New Section), HypothesisDriven Threat Hunting, Indicators of Compromise (IoCs), Threat<br>Hunting Tools and Techniques | |
| | 6.3 | Integration of Threat Hunting with Incident Response (New Section), How Threat Hunting Supports Incident Response, Developing a Threat Hunting Program, Case Studies and Best Practices | |
| | | **Total** | **45** |

| **Textbooks:** | |
|---|---|
| 1 | **Network Forensics: Tracking Hackers through Cyberspace** by Sherri Davidoff and Jonathan Ham, 2nd Edition |
| **References:** | |
| 1 | **Zeek (formerly known as Bro):** A Powerful Network Analysis Framework **by** James R. Burgess |
| **Useful Link for E-Resources:** | |
| 1 | Certified Network Forensics Examiner : CNFE (Part1 of Part2) \| Udemy |
| 2 | Network Forensics Examiner \| Free Online Course \| Alison |
| 3 | Getting Started with Network Forensics \| EC-Council Learning (eccouncil.org) |

| **Assessment:** | |
|---|---|
| **Internal Assessment:** | |
| Assessment consists of two class tests of 20 marks each. The first-class test is to be conducted when approx. 40% syllabus is completed and the second-class test when an additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| **End Theory Examination:** | |
| 1 | Question paper will comprise a total of six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only four questions need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus. |

| **Suggested List of Experiments** | |
|---|---|
| **Sr. No.** | **Title of Experiment** |
| 1 | Study EMailTrackerPro: |
| 2 | Study Web Historian: |
| 3 | Study Wireshark for Network Forensics |

## Semester V

| Course Code: | Course Title | Credit |
|---|---|---|
| 21501 | Professional Skill-IV (Cloud Forensics) | 3 |

| | |
|---|---|
| **Prerequisite: Business Communication Ethics** | |
| **Course Objectives:** | |
| 1 | To provide a detailed overview of entrepreneurship as the foundation of business growth |
| 2 | To teach to adopt entrepreneurship as value creation in the national economy. |
| 3 | It provides multiple constructs for entrepreneurs to be successful. |
| 4 | It provides multiple pathways for their companies to achieve sustainable growth. |
| **Course Outcomes:** | |
| 1 | To understand key concepts underpinning entrepreneurship |
| 2 | To apply knowledge in the recognition and exploitation of product/ service/ process opportunities |
| 3 | To demonstrate key concepts underpinning innovation and the issues associated with developing and sustaining innovation within organizations |
| 4 | To understand, how to design creative strategies for pursuing, exploiting and further developing new opportunities |
| 5 | To understand Issues associated with securing and managing financial resources in new and established organizations. |

| Module | | Content | Hrs |
|---|---|---|---|
| **1** | | **An Overview of Cloud Computing** | **8** |
| | 1.1 | Cloud Service Levels and Deployment Methods, Cloud Vendors | |
| | 1.2 | Basic Concepts of Cloud Forensics | |
| **2** | | **Legal Challenges in Cloud Forensics** | **8** |
| | 2.1 | Service Level Agreements. | |
| | 2.2 | Jurisdiction Issues, Accessing Evidence in the Cloud | |
| **3** | | **Technical Challenges in Cloud Forensics** | **8** |
| | 3.1 | Architecture, Analysis of Cloud Forensic Data | |
| | 3.2 | Anti-Forensics, Incident First Responders, Role Management | |
| **4** | | **Encryption in the Cloud** | **7** |

| | | | |
|---|---|---|---|
| | 4.1 | Conducting a Cloud Investigation, Investigating CSPs, Investigating Cloud Customers, Understanding Prefetch Files, | |
| | 4.2 | Examining Stored Cloud Data on a PC, Windows Prefetch Artifacts | |
| **5** | | **Tools for Cloud Forensics** | **7** |
| | 5.1 | Google Cloud Forensics Utils. | |
| | 5.2 | Sleuthkit, Cado Security. | |
| **6** | | **Cloud Forensics Case Studies.** | **7** |
| | 6.1 | Discuss at least five case studies. | |
| **Total** | | | **45** |

| **Textbooks:** | |
|---|---|
| 1 | Clint P. Garrison, Digital Forensics for Network, Internet, and Cloud Computing: A Forensic Evidence Guide for Moving Targets and Data, Syngress Publishing, Inc., 1st Edition (2010).. |
| 2 | Ronald L. Krutz and Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Wiley Publishing, Inc., 1st Edition. |

| **Reference books:** | |
|---|---|
| 1 | Nihad A. Hassan, Digital Forensics Basics - A Practical Guide Using Windows OS, Apress, 1st Edition. |
| 2 | Chris Dotson, Practical Cloud Security: A Guide for Secure Design and Deployment, O'Reilly Media, 1st Edition. |
| 3 | Tim Mather, Subra Kumaraswamy, and Shahed Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'Reilly Media, 1st Edition. |
| **Assessment:** | |
| **Internal Assessment:** | |
| Assessment consists of two class tests of 10 marks each. The first class test is to be conducted when approx. 40% syllabus is completed and second class test when additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| **End Semester Theory Examination:** | |
| 1 | Question paper will comprise of total six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only Four question need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mention in the syllabus. |
| **Useful Links** | |
| 1 | https://archive.nptel.ac.in/courses/128/106/128106006/. |
| 2 | https://www.youtube.com/watch?v=VBQbmpBMJMM |

**List of Tutorial:**

| Tutorial Number | Tutorial Topic |
|---|---|
| 1 | Understand digital forensics and incident response as it applies to the cloud |
| 2 | Identify malicious activities within the cloud |
| 3 | Study on Cost-effectively use cloud-native tools and services for DFIR |
| 5 | Study on decrease adversary dwell time in compromised cloud deployments. |
| 4 | Study on to ensure the business is adequately prepared to respond to cloud incidents |

| Course Code: | Course Title | Credit |
|---|---|---|
| **21502** | **Environmental Management** | **3** |

| **Prerequisite:** | |
|---|---|
| **Course Objectives:** | |
| 1 | To describe knowledge of natural systems which make life possible on Earth. |
| 2 | To understand that humans are part of these systems and depend on them. |
| 3 | To discuss an understanding of sustainable development to meet the needs of the present, without compromising the ability of future generations to meet their own needs. |

| | |
|---|---|
| 4 | To imbibe a sense of responsibility and concern for the welfare of the environment and all organisms. |
| 5 | To promote awareness of their own values concerning environmental issues. |
| 6 | To demonstrate a sound basis for further study, personal development and participation in local and global environmental concerns. |
| **Course Outcomes:** | |
| 1 | A willingness to review their own attitudes in the light of new knowledge and experiences. |
| 2 | Apply the knowledge of information gathering an awareness of the need to manage natural systems |
| 3 | Demonstrate appreciation of the diverse influences of human activity on natural systems. |
| 4 | Apply the knowledge to evaluate strategies, to conserve the biodiversity of a named ecosystem |
| 5 | Apply the concepts of an awareness strategies for managing climate change. |
| 6 | Apply the concepts of an awareness strategies for managing the atmosphere. |

| **Module** | | **Content** | |
|---|---|---|---|
| 1 | **Introduction to environmental management** | Continents and oceans, Country classification by income level, Sustainability, The water cycle, The structure and composition of the atmosphere, Ecosystems, | **8** |
| 2 | **Environmental research and data collection** | The scientific method, Environmental research in the context of climate change, Collection of environmental data, Data collection techniques and data analysis, The use of technology in data collection and analysis,<br>Case study: Plan an environmental management investigation of your choosing. The investigation should include a research aim, methodology, how the | **8** |
| | | data would be collected and how this data could be processed. | |
| 3 | **Managing human population** | Human population dynamics and structure, Impacts of human population change, Managing human population change, | **12** |

| | | | |
|---|---|---|---|
| 4 | **Managing ecosystems and biodiversity** | Ecosystems, Managing the conservation of biodiversity, Impacts of human activity on ecosystems,<br><br>Case study: Evaluate the strategies in place to conserve the biodiversity of a named ecosystem | **10** |
| 5 | **Managing resources and Climate Change** | Food security, Energy resources, Waste management, Managing climate change, strategies for managing climate change | **4** |
| 6 | **Managing water supplies and atmosphere** | Global water distribution, Managing the atmosphere, Acid deposition, Photochemical smog, Managing air pollution, Ozone depletion, | **3** |
| **Total** | | | **45** |

| | |
|---|---|
| Textbooks: | |
| 1 | "The End of Nature" -- Bill McKibben, Published in 1989. |
| 2 | "Braiding Sweetgrass,"-- Robin Wall Kimmerer, 2014. |
| 3 | "The Uninhabitable Earth"-- David Wallace Wells', Penguin Random House |
| 4 | Merchants of Doubt Naomi Oreskes and Erik M. Conway, Wiley, 2011 |
| 5 | "Eating Animals"-- Jonathan Safran Foer's, |
| **Reference books:** | |
| 1 | "The Sixth Extinction," Elizabeth Kolbert |
| 2 | "An Inconvenient Truth," authored by former Vice President Al Gore. |
| 3 | "Losing Earth: The Decade We Could Have Stopped Climate Change" Nathaniel Rich's |
| **Assessment:** | |
| Internal Assessment: | |
| Assessment consists of two class tests of 20 marks each. The first class test is to be conducted when approximately 40% syllabus is completed and the second class test when an additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| End Semester Theory Examination: | |
| 1 | Question paper will comprise a total of six questions. |

| | |
|---|---|
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only Four questions need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus. |

| Useful Digital Links | |
|---|---|
| 1 | https://www.youtube.com/watch?v=0Puv0Pss33M&t=149s |
| 2 | https://www.globalcitizen.org/en/content/11-environmental-documentaries/ |
| 3 | https://www.youtube.com/playlist?list=PLm_MSClsnwm8MoP52arwKP5kdKHyGylWy |

| **Suggested List of Tutorials** | |
|---|---|
| **Sr. No.** | **Title of Tutorials** |
| 1 | Plan an environmental management investigation of your choosing. The investigation should include a research aim, methodology, how the data would be collected and how this data could be processed. |
| 2 | Compare and contrast the population dynamics of a HIC and a LIC. |
| 3 | Evaluate the strategies in place to conserve the biodiversity of a named ecosystem |
| 4 | Compare and contrast the impacts of future energy insecurity on a HIC and a LIC. |
| 5 | Study the impacts that the lack of water security has had on a region and evaluate the strategies in place to improve the water security of that region. |
| 6 | Study the causes and impacts of a named atmospheric pollution event and evaluate the |
| | management of the pollution event. |
| 7 | Evaluate the impacts climate change may have on a named country or location.. |

\

| Course Code: | Course Title | Credit |
|---|---|---|
| **21 503** | **Cyber Security Laws** | **2** |

| Prerequisite: Engineering Mathematics, Data Structures, Algorithms | |
|---|---|
| Course Objectives: | |
| 1 | To introduce the basic concepts and techniques of Machine Learning. |
| 2 | To acquire in depth understanding of various supervised and unsupervised algorithms |
| 3 | To be able to apply various ensemble techniques for combining ML models. |
| 4 | To demonstrate dimensionality reduction techniques. |
| Course Outcomes: | |
| 1 | To acquire fundamental knowledge of developing machine learning models. |
| 2 | To select, apply and evaluate an appropriate machine learning model for the given |
| 3 | To demonstrate ensemble techniques to combine predictions from different models. |
| 4 | To demonstrate the dimensionality reduction techniques. |

| Module | | Content | Hrs |
|---|---|---|---|
| 1 | | **Introduction to Cyber security** | **5** |
| | 1.1 | Defining Cyberspace and Overview of Computer and Webtechnology, Architecture of cyberspace, Communication and web technology, Internet, World wide web, | |
| | 1.2 | Advent of internet, Internet infrastructure for data transfer and governance, Internet society, Regulation of cyberspace, Concept of cyber security, Issues and challenges of cyber Security | |
| 2 | | **Cyber crime and Cyber law** | **10** |
| | 2.1 | Classification of cyber crimes, Common cyber crimes- cyber crime targeting computers and mobiles, | |
| | 2.2 | Cyber crime against women and children, financial frauds, social engineering attacks, malware and ransomware attacks, zero day and zero click attacks, | |
| | 2.3 | Cybercriminals modus-operandi , Reporting of cyber crimes, Remedial and mitigation measures, Legal perspective of cyber crime, IT Act 2000 and its amendments, Cyber crime and offences, Organisations dealing with Cyber crime and Cyber security in India, Case studies. | |

| | | | |
|---|---|---|---|
| 3 | | **Social Media Overview and Security** | **7** |
| | 3.1 | Introduction to Social networks. Types of Social media, Social media platforms, Social media monitoring, Hashtag, Viral content, Social media marketing, Social media privacy, Challenges, opportunities and pitfalls in online social network | |
| | 3.2 | Security issues related to social media, Flagging and reporting of inappropriate content, Laws regarding posting of inappropriate content, Best practices for the use of Social media, Case studies | |
| 4 | | **Tools and Methods Used in Cyber line** | **8** |
| | 4.1 | Phishing, Password Cracking, Key loggers and Spywares, Virus and Worms, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Over Flow | |
| | 4.2 | Attacks on Wireless Networks, Phishing, Identity Theft (ID Theft) | |
| 5 | | **The Concept of Cyberspace** | **8** |
| | 5.1 | E-Commerce , The Contract Aspects in Cyber Law ,The Security Aspect of Cyber Law ,The Intellectual Property Aspect in Cyber Law, The Evidence Aspect in Cyber Law , The Criminal Aspect in Cyber Law, Global Trends in Cyber Law | |
| | 5.2 | Legal Framework for Electronic Data Interchange Law Relating to Electronic Banking , The Need for an Indian Cyber Law | |
| 6 | | **Indian IT Act** | **7** |
| | 6.1 | Cyber Crime and Criminal Justice : Penalties, Adjudication and Appeals Under the IT Act, 2000, IT Act. 2008 and its Amendments. Information Security Standard compliances SOX, GLBA, HIPAA, ISO, FISMA, NERC, PCI. | |
| **Total** | | | **45** |

| **Textbooks:** | |
|---|---|
| 1 | Cyber Crime Impact in the New Millennium, by R. C Mishra, Auther Press. Edition 2010. |
| 2 | Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd. (First Edition, 2011) |
| 3 | Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform. (Pearson , 13th November, 2001). |
| 4 | Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers. |
| 5 | Network Security Bible, Eric Cole, Ronald Krutz, James W. Conley, 2nd Edition, Wiley India Pvt. Ltd. |
| References: | |
| 1 | Fundamentals of Network Security by E. Maiwald, McGraw Hill. |

| | |
|---|---|
| 2 | Cyber Law & Cyber Crimes By Advocate Prashant Mali; Snow White Publications, Mumbai |
| 3 | William Stallings, Cryptography and Network Security, Pearson Publication |
| 4 | Kennetch J. Knapp, Cyber Security &Global Information Assurance Information Science Publishing. |
| 5 | The Indian Cyber Law by Suresh T. Vishwanathan; Bharat Law House New Delhi |

**Assessment:**

**Internal Assessment:**

Assessment consists of two class tests of 20 marks each. The first class test is to be conducted when approximately 40% syllabus is completed and the second class test when an additional 40% syllabus is completed. Duration of each test shall be one hour.

**End Semester Theory Examination:**

| | |
|---|---|
| 1 | Question paper will comprise a total of six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only Four questions need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus. |

| **Useful Digital Links** | |
|---|---|
| 1 | Websites for more information is available on : The Information Technology ACT, 2008- TIFR : https://www.tifrh.res.in |
| 2 | Website for more information , A Compliance Primer for IT professional https://www.sans.org/reading-room/whitepapers/compliance/compliance-primerprofessionals- 33538 |

**Suggested List of Experiments**

| **Sr. No.** | **Title of Experiment** |
|---|---|
| 1 | Study Platforms for reporting cyber crimes. Prepare Checklist for reporting cyber crimes online. |
| 2 | Setting, configuring and managing three password policy in the computer (BIOS, Administrator and Standard User). |
| 3 | Setting and configuring two factor authentication in the Mobile phone. |
| 4 | Security patch management and updates in Computer and Mobiles. |
| 5 | Managing Application permissions in Mobile phone. |
| 6 | Setting privacy settings on social media platforms. |
| 7 | Do’s and Don’ts for posting content on Social media platforms. |

| | |
|---|---|
| 8 | Registering complaints on a Social media platform. |
| 9 | Prepare password policy for computer and mobile device. |
| 10 | List out security controls for computer and implement technical security controls in the personal computer. |
| 11 | List out security controls for mobile phone and implement technical security controls in the personal mobile phone. |
| 12 | Log into computer system as an administrator and check the security policies in the system |

| **Course Code:** | **Course Title** | **Credit** |
|---|---|---|
| **21504** | **Blockchain Forensics and Crypto-currency Investigation** | **4** |

| |
|---|
| **Prerequisite: No Prerequisite** |
| **Course Objectives:** |

| | |
|---|---|
| 1 | Develop a solid foundation in blockchain technology, its components, and the role of cryptocurrencies in modern digital systems. |
| 2 | Learn to trace, decode, and analyze cryptocurrency transactions using blockchain explorers and forensic tools. |
| 3 | Recognize common cryptocurrency-related threats such as fraud, money laundering, and scams, and understand how to address these challenges effectively. |
| 4 | Gain hands-on experience with blockchain forensic tools like Etherscan, Bitquery, and Chainalysis for investigating suspicious activities. |
| 5 | Understand the regulatory landscape, ethical considerations, and future trends in blockchain forensics to prepare for advanced investigations and industry roles. |

**Course Outcomes: On Successful completion of course, learner will be able to**

| | |
|---|---|
| 1 | Students will be able to explain the core principles of blockchain technology and its role in enabling secure and transparent transactions. |
| 2 | Students will demonstrate the ability to trace and interpret cryptocurrency transactions using blockchain explorers and forensic methodologies. |
| 3 | Students will be capable of identifying cryptocurrency-related threats such as fraud and money laundering and applying mitigation strategies. |
| 4 | Students will gain practical experience in using forensic tools like Chainalysis and Bitquery to investigate suspicious activities on the blockchain. |
| 5 | Students will understand and apply relevant legal frameworks, ethical principles, and industry best practices in conducting blockchain investigations. |

| Module | | Content | Hrs |
|---|---|---|---|
| **1** | | **Fundamentals of Blockchain Technology** | **7** |
| | 1.1 | **Introduction to Blockchain: -**<br>• Basics of blockchain technology: Definition and purpose<br>• Structure of blockchain: Blocks, transactions, and chains<br>• Types of blockchains: Public, private, and consortium | |

| | | | |
|---|---|---|---|
| | 1.2 | **Cryptographic Principles: -**<br>• Hashing and its role in blockchain<br>• Digital signatures and public-key cryptography<br>• Consensus mechanisms: Proof-of-Work (PoW) and Proof-of-Stake (PoS) | |

| | | | |
|---|---|---|---|
| | 1.3 | **Blockchain Transactions: -**<br>• How transactions are processed and recorded<br>• Anatomy of a blockchain transaction: Inputs, outputs, and transaction IDs<br>• Understanding smart contracts and their applications | |
| **2** | | **Understanding Cryptocurrencies** | **7** |
| | 2.1 | **Introduction to Cryptocurrencies**<br>• Overview of cryptocurrencies: Definition and characteristics<br>• Popular cryptocurrencies: Bitcoin, Ethereum, and others<br>• Differences between cryptocurrencies and traditional currencies | |
| | 2.2 | **Cryptocurrency Wallets**<br>• Wallet types: Hot wallets vs. cold wallets<br>• Key concepts: Public and private keys<br>• Wallet addresses and their role in transactions | |
| | 2.3 | **Transaction Mechanics**<br>• How cryptocurrency transactions work<br>• Transaction fees and their importance<br>• Exploring transaction data on blockchain explorers | |
| **3** | | **Risks and Challenges in Cryptocurrencies** | **7** |
| | 3.1 | **Cryptocurrency Threats**<br>• Fraud, scams, and phishing attacks<br>• Money laundering techniques in cryptocurrencies<br>• Real-world examples of crypto-related crimes | |
| | 3.2 | **Anonymity and Pseudonymity**<br>• How blockchain provides pseudonymity<br>• Techniques used to obscure transactions (mixing, tumblers)<br>• Challenges of tracking cryptocurrency crimes | |
| | 3.3 | **Regulatory and Ethical Considerations**<br>• Overview of cryptocurrency regulations in India and globally<br>• Ethical considerations in blockchain investigations<br>• Compliance with AML (Anti-Money Laundering) and KYC (Know Your Customer) standards | |
| **4** | | **Blockchain Forensics Basics** | **8** |

| | | | |
|---|---|---|---|
| | 4.1 | **Blockchain Traceability**<br>• Understanding blockchain transparency and traceability<br>• Tools for analysis: Blockchain explorers (e.g., Etherscan, Blockchain.info)<br>• Steps for tracing a transaction | |
| | 4.2 | **Investigative Techniques**<br>• Identifying sources and destinations in transactions<br>• Wallet clustering and transaction chains<br>• Recognizing patterns in suspicious activities | |

| | | | |
|---|---|---|---|
| | 4.3 | **Forensic Tools**<br>• Introduction to beginner-friendly tools (e.g., Bitquery, Blockcypher)<br>• How to gather evidence from blockchain transactions<br>• Preparing reports based on blockchain analysis | |
| **5** | | **Advanced Blockchain Forensics** | 8 |
| | 5.1 | **Intermediate Investigation Techniques**<br>• Analyzing transaction histories for anomalies<br>• Using forensic tools: Chainalysis, CipherTrace, and Elliptic<br>• Tracking stolen or laundered cryptocurrency | |
| | 5.2 | **Case Study: Cryptocurrency Fraud**<br>• Real-world example of a fraudulent transaction<br>• Step-by-step breakdown of investigation process<br>• Lessons learned and best practices | |
| | 5.3 | **Hands-On Lab**<br>• Tracing a mock transaction using blockchain explorers<br>• Identifying suspicious wallets and tracing funds<br>• Report generation and presentation | |
| **6** | | **Emerging Trends and Future Directions** | **8** |
| | 5.1 | **Future of Blockchain Forensics**<br>• Emerging challenges in blockchain investigations<br>• Investigating DeFi (Decentralized Finance) platforms<br>• New forensic tools and AI integration | |
| | 5.2 | **Cryptocurrency Ecosystem Trends**<br>• Growth of privacy-focused cryptocurrencies (e.g., Monero, Zcash)<br>• Trends in crypto scams and fraud detection<br>• Role of governments and international organizations | |
| | 5.3 | **Hands-On Lab**<br>• Tracing a mock transaction using blockchain explorers<br>• Identifying suspicious wallets and tracing funds | |
| | | • Report generation and presentation | |
| **Total** | | | **45** |

| **Textbooks:** | |
|---|---|
| 1 | *Investigating Cryptocurrencies: Understanding, Extracting, and Analyzing Blockchain Evidence,* Nick Furneaux, 1st Edition, Wiley. |
| **References:** | |
| 1 | *Blockchain and Cryptocurrency Legal Framework: An In-Depth Look at the Legal and Ethical Challenges,* **:** Dean Armstrong QC, Daniel Davies, and Sam Thomas, Bloomsbury Professional. |
| 2 | *Mastering Blockchain: Unlocking the Power of Cryptocurrencies and Smart Contracts,* Imran Bashir, Packt Publishing |

| Useful Link for E-Resources: | |
|---|---|
| 1 | Certified Cryptocurrency Expert™ (CCE) \| Crypto Certification |
| 2 | Bitcoin and Cryptocurrency Forensic Investigation (OSINT) \| Udemy |
| 3 | Free Cryptocurrency Tutorial - Introduction to Cryptocurrencies and Blockchain \| Udemy |

| Assessment: | |
|---|---|
| **Internal Assessment:** | |
| Assessment consists of two class tests of 20 marks each. The first-class test is to be conducted when approx. 40% syllabus is completed and the second-class test when an additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| **End Theory Examination:** | |
| 1 | Question paper will comprise a total of six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only four questions need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus. |

| Suggested List of Experiments | |
|---|---|
| **Sr. No.** | **Title of Experiment** |
| 1 | Understanding the structure and functioning of blockchain technology. |
| 2 | Analyzing wallet addresses and transaction histories. |
| 3 | Using tools to trace cryptocurrency transactions across the blockchain. |
| 4 | Detecting patterns of fraud or illegal activities in blockchain transactions. |
| 5 | Hands-on experience with blockchain forensic tools like Chainalysis or Elliptic. |
| 6 | **Case Studies**: Solving real-world cases involving cryptocurrency fraud or theft. |

| Course Code: | Course Title | Credit |
|---|---|---|
| **21505** | **Ransomware Investigation** | **4** |

| Prerequisite: No Prerequisite | |
|---|---|
| **Course Objectives:** | |
| 1 | Understand the lifecycle and impact of ransomware attacks on organizations. |
| 2 | Learn how to collect, analyze, and preserve evidence during ransomware investigations. |
| 3 | Develop practical skills to mitigate ransomware threats and recover encrypted data. |
| 4 | Explore legal, ethical, and regulatory considerations related to ransomware incidents. |

| | |
|---|---|
| 5 | Use advanced tools and techniques to trace ransomware activities and attribute attacks. |

**Course Outcomes: On Successful completion of course, learner will be able to**

| | |
|---|---|
| 1 | Explain the mechanisms and lifecycle of ransomware attacks. |
| 2 | Conduct effective ransomware investigations using forensic techniques. |
| 3 | Identify and apply best practices for ransomware prevention and recovery. |
| 4 | Demonstrate understanding of legal and ethical issues in ransomware cases. |
| 5 | Use forensic and analytical tools to attribute ransomware attacks to threat actors. |

| Module | | Content | Hrs |
|---|---|---|---|
| **1** | | **Introduction to Ransomware** | **7** |
| | 1.1 | **Introduction to Ransomware:**<br>• Evolution and history of ransomware<br>• Types of ransomware (Crypto, Locker, Scareware, etc.) | |
| | 1.2 | **Ransomware Lifecycle**<br>• Infection vectors (phishing, drive-by downloads, etc.)<br>• Encryption and ransom demand phases | |
| | | • Data exfiltration and double extortion tactics | |
| | 1.3 | **Impact of Ransomware**<br>• Economic and operational consequences<br>• Case studies: Major ransomware attacks | |
| **2** | | **Ransomware Investigation Techniques** | **8** |
| | 2.1 | **Incident Response Basics**<br>• Initial response to ransomware incidents<br>• Identifying affected systems and isolating infections | |

| | | | |
|---|---|---|---|
| | 2.2 | **Collecting Evidence**<br>• Techniques for gathering digital evidence<br>• Preserving system integrity during investigation | |
| | 2.3 | **Malware Analysis**<br>• Tools for analyzing ransomware samples<br>• Reverse engineering basics: Understanding encryption methods | |
| **3** | | **Ransomware Mitigation Strategies** | **8** |
| | 3.1 | **Prevention and Protection**<br>• Best practices for endpoint security<br>• Role of backups and disaster recovery plans | |
| | 3.2 | **Decryption and Recovery**<br>• Identifying available decryption tools<br>• Limitations of ransomware recovery | |
| | 3.3 | **Negotiation and Payment (Ethical Considerations)**<br>• When and how to engage with attackers<br>• Risks and legal implications of ransom payments | |
| **4** | | **Ransomware Forensics** | **8** |
| | 4.1 | **Digital Forensic Analysis & Attribution Techniques** • Investigating ransomware footprints | |
| | | • Analyzing logs and network traffic<br>• Identifying threat actors<br>• Tracing cryptocurrency payments (e.g., Bitcoin tracking) | |
| | 4.2 | Report Writing and Presentation<br>• Documenting findings<br>• Creating incident analysis reports | |
| **5** | | **Legal and Ethical Aspects** | **7** |

| | | | |
|---|---|---|---|
| | 5.1 | Ransomware Regulations & Ethical Challenges<br>• Overview of cybercrime laws<br>• Reporting requirements and compliance<br>• Balancing transparency and confidentiality<br>• Navigating moral dilemmas in ransomware cases | |
| | 5.2 | Coordination with Law Enforcement<br>• How to collaborate with agencies during investigations<br>• Case examples of law enforcement success | |
| **6** | | **Advanced Topics and Trends** | **7** |
| | 6.1 | **Emerging Ransomware Tactics**<br>• Evolving attack techniques (e.g., RaaS – Ransomwareas-a-Service)<br>• Multi-extortion ransomware | |
| | 6.2 | **AI and Machine Learning in Ransomware Detection**<br>• Role of AI in detecting and mitigating attacks<br>• Automated investigation tools | |
| | 6.3 | **Future of Ransomware Investigation**<br>• Predicting trends in ransomware development<br>• Preparing for next-generation ransomware attacks | |
| **Total** | | | **45** |

| **Assessment:** | |
|---|---|
| **Internal Assessment:** | |
| Assessment consists of two class tests of 20 marks each. The first-class test is to be conducted when approx. 40% syllabus is completed and the second-class test when an additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| **End Theory Examination:** | |
| 1 | Question paper will comprise a total of six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only four questions need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus. |

| Suggested List of Experiments | |
|---|---|
| **Sr. No.** | **Title of Experiment** |
| 1 | Understanding the stages of a ransomware attack, from initial access to encryption. |
| 2 | Using tools like Autopsy or Velociraptor to analyze infected systems and recover data. |
| 3 | Role-playing exercises to handle ransomware incidents effectively. |
| 4 | Investigating payment methods and tracing transactions related to ransomware. |
| 5 | Analyzing memory dumps to identify ransomware processes and artifacts. |
| 6 | **Case Studies**: Examining real-world ransomware attacks and their investigation strategies. |

| Course Code: | Course Title | Credit |
|---|---|---|
| **21 506** | **Mobile Security and Forensics** | **4** |

| **Prerequisite: No Prerequisite** | |
|---|---|
| **Course Objectives:** | |
| 1 | Understand the core architecture and security mechanisms of mobile platforms, including<br>Android and iOS. |
| 2 | Learn to identify, analyze, and mitigate vulnerabilities in mobile applications, networks, and devices. |
| 3 | Gain practical expertise in forensic tools and techniques for mobile device investigation and evidence extraction. |
| 4 | Explore cutting-edge topics in mobile security, such as cloud integration, IoT security, and AI-driven solutions. |
| 5 | Develop critical skills to detect, investigate, and respond to advanced threats targeting mobile environments. |

| **Course Outcomes: On Successful completion of course, learner will be able to** | |
|---|---|
| 1 | Demonstrate a solid understanding of mobile platform architecture, security challenges, and mitigation strategies. |
| 2 | Analyze and secure mobile applications, APIs, and networks using advanced tools and best practices. |
| 3 | Employ forensic methodologies to collect, preserve, and analyze digital evidence from mobile devices. |
| 4 | Investigate cloud and app-based data with a focus on maintaining legal and ethical standards. |
| 5 | Effectively identify and respond to emerging threats, including mobile ransomware, IoT integration risks, and AI-driven malware. |

| Module | | Content | Hrs |
|---|---|---|---|
| **1** | | **Mobile Security Essentials** | **7** |
| | 1.1 | **Mobile Platform Architecture**<br>• Android and iOS architectural differences<br>• Security models of mobile operating systems | |
| | | • Sandboxing and permission models | |
| | 1.2 | **Threat Landscape in Mobile Devices**<br>• Advanced mobile malware (trojans, spyware, adware)<br>• Attack vectors: Application-based, network-based, and hardware-based<br>• Case studies of high-profile mobile security breaches | |
| | 1.3 | **Mobile Device Security Best Practices**<br>• Implementing device encryption and biometric authentication<br>• Hardening Android and iOS devices<br>• Security policies and Mobile Device Management (MDM) | |
| **2** | | **Mobile Application Security** | **8** |
| | 2.1 | **Vulnerability Assessment for Mobile Apps**<br>• OWASP Mobile Top 10 vulnerabilities<br>• Identifying insecure data storage and code injection issues<br>• Automated app scanning tools (e.g., MobSF, Drozer) | |

| | | | |
|---|---|---|---|
| | 2.2 | **Advanced API Security**<br><br>• Secure authentication and authorization in APIs (OAuth, JWT)<br>• Testing APIs for flaws using Postman and Burp Suite<br>• Protecting APIs from injection attacks and data exposure | |
| | 2.3 | **Dynamic Mobile App Analysis**<br><br>• Setting up mobile app analysis environments (Android Studio, Genymotion)<br>• Analyzing runtime behavior of apps<br>• Debugging and code instrumentation | |
| **3** | | **Mobile Network Security** | **8** |
| | 3.1 | **Wireless Communication Security**<br><br>• Security of mobile network protocols: GSM, LTE, 5G<br>• Exploiting vulnerabilities in Wi-Fi and Bluetooth connections<br>• Countermeasures for wireless attacks | |
| | 3.2 | **Mobile Network Traffic Analysis**<br><br>• Tools for capturing and analyzing network traffic (Wireshark, tcpdump) | |

| | | | |
|---|---|---|---|
| | | • Identifying suspicious patterns in mobile traffic<br>• SSL/TLS decryption techniques | |
| | 3.3 | **Network-Based Attacks**<br><br>• Man-in-the-Middle (MitM) attacks in mobile environments<br>• DNS spoofing and ARP poisoning on mobile devices<br>• Protection against rogue access points | |
| **4** | | **Intermediate Mobile Forensics** | **7** |
| | 4.1 | **Evidence Collection and Chain of Custody**<br><br>• Legal considerations and preserving evidence<br>• Imaging Android and iOS devices<br>• Tools for bypassing screen locks | |
| | 4.2 | **Forensic Analysis of Mobile Artifacts**<br><br>• Understanding app data storage: SQLite databases, shared preferences<br>• Extracting and analyzing browser history, call logs, and messages<br>• Analyzing iCloud and Google Drive backups | |

| | | | |
|---|---|---|---|
| | 4.3 | **Mobile File System Examination**<br>• Navigating Android and iOS file systems<br>• Recovering deleted data using forensic tools<br>• Examining encrypted data storage | |
| **5** | | **Advanced Mobile Forensics Techniques** | 7 |
| | 5.1 | **Advanced Data Recovery**<br>• Techniques for recovering deleted data and multimedia<br>• Forensic tools for recovering app-specific data (WhatsApp, Signal)<br>• Challenges in encrypted data recovery | |
| | 5.2 | **App-Specific Forensics**<br>• Investigating social media apps (Facebook, Instagram)<br>• Forensic analysis of financial apps and wallets<br>• Analyzing ransomware on mobile devices | |
| | 5.3 | **Forensics in the Cloud Era**<br>• Investigating cloud-synced mobile data<br>• Tools for analyzing Google Drive and iCloud data<br>• Challenges of cross-device cloud forensics | |
| **6** | | **Emerging Trends and Tools** | **8** |
| | 6.1 | **IoT Security and Mobile Integration** | |
| | | • Analyzing IoT data from mobile devices<br>• Security challenges with IoT-connected mobile devices<br>• Case studies of IoT-mobile integration attacks | |
| | 6.2 | **Advanced Threats in Mobile Security**<br>• Mobile ransomware and spyware evolution<br>• Mobile-based cryptocurrency mining malware<br>• Zero-day exploits in mobile applications | |
| | 6.3 | **AI and Automation in Mobile Forensics**<br>• AI-based mobile malware detection tools<br>• Automated forensic investigation workflows<br>• Future trends in mobile forensics | |
| **Total** | | | **45** |

| **Textbooks:** | |
|---|---|
| 1 | Mobile Forensics – Advanced Investigative Strategies, Satish Bommisetty, Rohit Tamma, Heather Mahalik, Packt Publishing |
| **References:** | |
| 1 | Practical Mobile Forensics, Rohit Tamma, Oleg Skulkin, Heather Mahalik, Packt Publishing. |

| | |
|---|---|
| 2 | Android Malware Analysis: Detecting and Mitigating Android Malware and Spyware , Ken Dunham, CRC Press |
| **Useful Link for E-Resources:** | |
| 1 | Mobile Computer Forensics Fundamentals \| Udemy |
| 2 | Certified Mobile Forensics Certification \| EC-Council iClass |
| 3 | Free mobile forensics training & courses - MSAB |

| **Assessment:** | |
|---|---|
| **Internal Assessment:** | |
| Assessment consists of two class tests of 20 marks each. The first-class test is to be conducted when approx. 40% syllabus is completed and the second-class test when an additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| **End Theory Examination:** | |
| 1 | Question paper will comprise a total of six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only four questions need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus. |

| **Suggested List of Experiments** | |
|---|---|
| **Sr. No.** | **Title of Experiment** |
| 1 | Understanding the internal structure and file systems of Android and iOS devices. |
| 2 | Extracting data from mobile devices using forensic tools. |
| 3 | Investigating mobile applications for security flaws and data leakage. |
| 4 | Analyzing Wi-Fi and cellular data usage for forensic purposes. |
| 5 | Identifying and mitigating mobile malware threats. |
| 6 | Recovering and analyzing data stored in mobile cloud services. |
| 7 | Solving real-world cases involving mobile security breaches or forensic investigations. |

| Course Code: | Course Title | Credit |
|---|---|---|
| 21504 | Skill Based Internship | 2 |

| |
|---|
| **Assessment:** |
| **Internal Assessment:** |
| Term Work marks are based on Two Project Reviews and Final Presentation. Project should done based on Subjects learned in the Syllabus. |
| **End Theory Examination: No Practical and Oral Examinations** |

## Semester VI

| Course Code: | Course Title | Credit |
|---|---|---|
| **21601** | **Professional Skill-IV (API Pentesting)** | **3** |

| | |
|---|---|
| Prerequisite: | |
| Course Objectives: | |
| 1 | Understanding API Security Concepts |
| 2 | Identifying and Exploiting Vulnerabilities |
| 3 | Performing Advanced Pentesting Techniques |
| 4 | Reporting and Remediation |
| Course Outcomes: | |
| 1 | Gaining practical knowledge of API vulnerabilities and how to defend against them. |
| 2 | Developing the ability to conduct thorough assessments of API security using professional tools and techniques. |
| 3 | Learning how to identify and address risks in API designs and implementations. |
| 4 | Becoming adept at documenting findings and suggesting remediation strategies. |
| 5 | Applying pentesting skills to secure APIs in real-world scenarios across various industries. |
| 6 | Applyiny Best practices for API Security. |

| | | | |
|---|---|---|---|
| I | **Introduction** | Methodical approach to identify vulnerabilities within APIs, assess their security posture, and mitigate potentialrisks.<br>API penetration testing methodology,delving into key concepts, attack vectors, and best practices. | **10** |
| II | **Understanding APIs** | Fundamental concepts of APIs. Define protocols and tools for building software applications, interaction with external services. | **8** |
| III | **Importance of API Security** | Attractive targets for cybercriminals. Breaches in API security, proactive approach to API security, with penetration testing being akey component. | **8** |

| | | | |
|---|---|---|---|
| IV | **API Penetration Testing Methodology** | **Information Gathering:** Identifying the API endpoints, Analyzing API documentation. Understanding the authentication mechanisms in place.<br>**Threat Modeling:**<br>Identifying potential threats and attack vectors.<br>Prioritizing threats based on impact and likelihood.<br>Creating a threat model specific to the API under test.<br>**Vulnerability Analysis:**<br>Conducting manual testing to identify common vulnerabilities like SQLinjection, XSS (Cross-Site Scripting), and CSRF (Cross-Site Request Forgery).<br>Utilizing automated tools to scan for common issues. Assessing the API for insecure direct object references and brokenauthentication mechanisms.<br>Authentication and Authorization Testing, Input Validation and Output Encoding, Error Handling and Logging, Security Misconfigurations, Data Protection , API Rate Limiting and Throttling, Post-Testing Analysis and Reporting | **6** |
| V | **Common API Attack Vectors** | SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Insecure Direct Object References (IDOR), Authentication Bypass, API Rate Limiting Bypass, XML External Entity (XXE) Attack, Insecure Deserialization. | **7** |
| VI | **Best Practices for API Security** | Least Privilege Principle, Secure Authentication, Input Validation, Regular Security Updates, API Versioning, Secure Communication, Rate Limiting and Throttling, Security Monitoring and Incident Response. | **6** |
| **Total** | | | **45** |

| | |
|---|---|
| Textbooks: | |
| 1 | Pentesting APIs: A Practical Guide to Discovering, Fingerprinting, and Exploiting APIs by Maurício Harley |
| 2 | The Hacker Playbook 3: Practical Guide to Penetration Testing by Peter Kim |
| References: | |
| 1 | Hacking APIs: Breaking Web Application Programming Interfaces by Corey J. Ball. |
| Assessment: | |
| Internal Assessment: | |
| Assessment consists of two class tests of 10 marks each. The first class test is to be conducted when approximately 40% syllabus is completed and the second class test when an additional 40% | |
| syllabus is completed. Duration of each test shall be one hour. | |

| End Semester Theory Examination: | |
|---|---|
| 1 | Question paper will comprise a total of six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only Four questions need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus. |

| Useful Digital Links | |
|---|---|
| 1 | https://www.youtube.com/watch?v=2_lswM1S264 |
| 2 | https://www.youtube.com/watch?v=MFxk5BZulVU |
| 3 | https://www.youtube.com/watch?v=apoxlzW2abg |

**List of Tutorial:**

| Tutorial Number | Tutorial Topic |
|---|---|
| 1 | Discovering and analyzing API endpoints using tools like Postman or Burp Suite. |
| 2 | Testing for excessive data exposure and business logic flaws in API responses. |
| 3 | Performing password brute force, password spraying, and MFA bypass techniques. |
| 5 | Identifying broken object-level authorization (BOLA) vulnerabilities. |
| 4 | Conducting SQL, NoSQL, and XSS injection attacks on APIs. |
| 5 | Evaluating APIs for rate-limiting vulnerabilities. |
| 6 | Detecting mass assignment vulnerabilities in API requests. |
| 7 | Testing for misconfigurations and improper asset management in APIs. |
| 8 | Discovering and analyzing API endpoints using tools like Postman or Burp Suite. |

| Course Code: | Course Title | Credit |
|---|---|---|
| **21602** | **Information Retrieval System** | **3** |

**Prerequisite:** Data Structures and Algorithms or Database Management Systems

| Course Objectives: | |
|---|---|
| 1 | To introduce students to the principles and techniques of information retrieval in digital systems. |
| 2 | To develop skills in designing and evaluating retrieval models for text and multimedia data. |
| 3 | To explore indexing, searching, and ranking mechanisms used in modern information retrieval systems. |
| 4 | To familiarize students with applications of IRS, including web search engines and recommender systems. |
| 5 | To provide hands-on experience with tools and algorithms for efficient information retrieval. |

| Course Outcome: | |
|---|---|
| 1 | Explain the architecture and components of an information retrieval system. |
| 2 | Design and implement basic retrieval models for structured and unstructured data. |
| 3 | Evaluate the performance of IRS using metrics like precision, recall, and F-measure. |
| 4 | Apply indexing and querying techniques to optimize retrieval efficiency. |
| 5 | Analyze real-world IRS applications, such as search engines and content recommendation. |

| Module | | Detailed Contents | Hours |
|---|---|---|---|
| **1** | | **Introduction to Information Retrieval** | |
| | 1.1 | Overview of IRS: Definition, Scope, and Importance. | **7** |
| | 1.2 | Types of Information Retrieval: Text, Image, Audio, Video. | |
| | 1.3 | IRS vs. Database Systems: Key Differences. | |
| | 1.4 | Basic Retrieval Process: Querying, Matching, and Ranking. | |
| **2** | | **Information Retrieval Models** | **8** |
| | 2.1 | Boolean Retrieval Model: Concepts and Limitations. | |
| | 2.2 | Vector Space Model: Term Weighting (TF-IDF), Cosine Similarity. | |
| | 2.3 | Probabilistic Models: BM25 and Relevance Feedback. | |
| | 2.4 | Evaluation Metrics: Precision, Recall, MAP (Mean Average Precision) | |
| **3** | | **Indexing and Data Structures** | **8** |
| | 3.1 | Inverted Index: Construction and Optimization. | |
| | 3.2 | Text Preprocessing: Tokenization, Stemming, Stop Words. | |
| | 3.3 | Data Structures for IRS: Tries, Suffix Trees, Hashing. | |
| | 3.4 | Compression Techniques for Indexes. | |
| **4** | | **Query Processing and Search Algorithms** | **7** |
| | 4.1 | Query Parsing and Reformulation. | |
| | 4.2 | Search Algorithms: Exact Match, Approximate Match. | |
| | 4.3 | Ranking Algorithms: PageRank, HITS. | |
| | 4.4 | Spell Correction and Autocompletion in Queries | |
| **5** | | **Advanced Topics in IRS** | **7** |

| | | | |
|---|---|---|---|
| | 5.1 | Web Information Retrieval: Crawling, Indexing, and Link Analysis. | |
| | 5.2 | Multimedia Retrieval: Image and Video Search Techniques. | |
| | 5.3 | Recommender Systems: Collaborative Filtering, Content-Based Filtering. | |
| | 5.4 | Natural Language Processing in IRS: Word Embeddings, BERT | |
| **6** | | **Practical Implementation and Evaluation** | **8** |
| | 6.1 | Tools and Frameworks: Apache Lucene, Elasticsearch. | |
| | 6.2 | Building a Simple Search Engine: Hands-On Project. | |
| | 6.3 | Performance Evaluation: Benchmarking and User Studies. | |
| | 6.4 | Challenges in IRS: Scalability, Latency, and Relevance. | |
| **Total** | | | **45** |

| **Textbooks:** | |
|---|---|
| 1 | "Information Retrieval" by G.G. Chowdhury and Sudatta Chowdhury, PHI Learning (India). |
| 2 | "Introduction to Information Retrieval and Text Mining" by R. Rajendra Prasad, S. Chand Publishing. |
| 3 | "Introduction to Information Retrieval" by Christopher D. Manning, Prabhakar Raghavan, and Hinrich Schütze, Cambridge University Press. |
| 4 | "Search Engines: Information Retrieval in Practice" by Bruce Croft, Donald Metzler, and Trevor Strohman, Pearson. |

| **References:** | |
|---|---|
| 1 | "Modern Information Retrieval" by Ricardo Baeza-Yates and Berthier Ribeiro-Neto, Addison-Wesley. |
| 2 | "Information Retrieval: Algorithms and Heuristics" by David A. Grossman and Ophir Frieder,Springer. |
| 3 | "Text Data Management and Analysis" by ChengXiang Zhai and Sean Massung, Morgan & Claypool. |
| 4 | Data Science for Dummies Paperback, Wiley Publications, Lillian Pierson |

**Assessment:**
**Internal Assessment:**

Assessment consists of two class tests of 20 marks each. The first-class test is to be conducted when approx. 40% syllabus is completed and second-class test when additional 40% syllabus is completed. Duration of each test shall be one hour.

**End Semester Theory Examination:**

| | |
|---|---|
| 1 | Question paper will comprise a total of six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only Four questions need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus. |

| Useful Links | |
|---|---|
| 1 | https://nlp.stanford.edu/IR-book/ |
| 2 | https://www.elastic.co/guide/en/elasticsearch/ |

**List of Practical/ Tutorials:**

| Sr. No | Topic |
|---|---|
| 1 | Use NLTK to preprocess a text dataset (e.g., news articles) with tokenization and stemming. |
| 2 | Build an inverted index in Python for a small document collection (e.g., 20 text files). |
| 3 | Implement a Boolean retrieval system for a dataset (e.g., Wikipedia snippets) with AND/OR/NOT queries. |
| 4 | Compute TF-IDF scores and retrieve top documents for a query (e.g., movie descriptions). |
| 5 | Use the vector space model to rank documents based on cosine similarity (e.g., blog posts) |
| 6 | Create a basic web crawler with BeautifulSoup to collect data (e.g., news headlines). |
| 7 | Index a text corpus (e.g., research abstracts) and perform searches using Lucene. |
| 8 | Enhance a retrieval system with synonym expansion using WordNet and compare results. |
| 9 | Calculate precision, recall, and MAP for a retrieval system on a labeled dataset (e.g., TREC). |
| 10. | Build an end-to-end search engine for a small corpus (e.g., articles) with indexing and ranking. |

| Course Code: | Course Title | Credit |
|---|---|---|
| **21603** | **Distributed Computing** | **2** |

| | |
|---|---|
| **Prerequisite:** Computer Networks and Operating Systems. | |
| **Course Objectives:** | |
| 1 | To introduce students to the concepts and architectures of distributed computing systems. |
| 2 | Develop an understanding of communication, synchronization, and coordination in distributed environments. |
| 3 | Equip students with skills to design and implement distributed applications. |
| 4 | Explore fault tolerance and scalability in distributed systems. |
| 5 | Provide hands-on experience with distributed computing frameworks and tools. |
| **Course Outcomes:** | |
| 1 | Students will be able to explain the characteristics and models of distributed systems. |
| 2 | Implement inter-process communication and synchronization mechanisms. |
| 3 | Design distributed algorithms for real-world applications. |
| 4 | Evaluate the performance and reliability of distributed systems. |
| 5 | Develop a distributed application using modern tools or frameworks. |

| Module | | Content | Hrs |
|---|---|---|---|
| **1** | | **Introduction to Distributed Computing** | **8** |
| | 1.1 | Distributed Systems: Definition, Goals, Challenges. | |
| | 1.2 | Characteristics: Concurrency, Scalability, Fault Tolerance. | |
| | 1.3 | Architectures: Client-Server, Peer-to-Peer, Multi-Tier. | |
| | 1.4 | Examples: Cloud Computing, Blockchain, CDN. | |
| **2** | | **Communication in Distributed Systems** | **8** |
| | 2.1 | Inter-Process Communication (IPC): Message Passing, RPC. | |
| | 2.2 | Middleware: CORBA, RMI, gRPC. | |

| | | | |
|---|---|---|---|
| | 2.3 | Network Protocols: TCP/IP, UDP, Sockets. | |
| | 2. | Time and Clock Synchronization: Lamport Clocks, NTP. | |
| | 4 | | |
| **3** | | **Synchronization and Coordination** | **7** |
| | 3.1 | Mutual Exclusion: Centralized, Distributed Algorithms. | |
| | 3.2 | Election Algorithms: Bully, Ring. | |
| | 3.3 | Deadlock Detection and Prevention in Distributed Systems. | |
| | 3.4 | Consistency Models: Eventual, Strong, Causal. | |

| | | | |
|---|---|---|---|
| **4** | | **Distributed Algorithms** | **8** |
| | 4.1 | Distributed Consensus: Paxos, Raft. | |
| | 4.2 | Leader Election and Replication. | |
| | 4.3 | Distributed Transactions: Two-Phase Commit (2PC). | |
| | 4.4 | Load Balancing: Round-Robin, Least Connection. | |
| **5** | | **Fault Tolerance and Recovery** | **7** |
| | 5.1 | Fault Models: Crash, Byzantine Failures. | |
| | 5.2 | Replication Techniques: Primary-Backup, Active Replication. | |
| | 5.3 | Checkpointing and Rollback Recovery. | |
| | 5.4 | Distributed File Systems: NFS, GFS. | |
| **6** | | **Distributed Computing Frameworks and Applications** | **7** |
| | 6.1 | Frameworks: Apache Hadoop, Spark, MPI. | |
| | 6.2 | Cloud-Based Distributed Systems: AWS Lambda, Azure Functions. | |
| | 6.3 | Security in Distributed Systems: Authentication, Encryption. | |
| | 6.4 | Project: Building a Distributed Application (e.g., Chat System). | |
| **Total** | | | **45** |

**Textbooks:**

| | |
|---|---|
| 1 | "Distributed Computing" by Sunita Mahajan and Seema Shah, Oxford University Press (India) |
| 2 | "Distributed Systems" by Dr. R.K. Singla, S.K. Kataria & Sons |
| 3 | "Distributed Systems: Concepts and Design" by George Coulouris, Jean Dollimore, and Tim Kindberg, Pearson |
| **References:** | |
| 1 | "Distributed Systems: Principles and Paradigms" by Andrew S. Tanenbaum and Maarten Van Steen, Pearson |
| 2 | "Designing Data-Intensive Applications" by Martin Kleppmann, O'Reilly Media |
| **Useful Links for E-resources:** | |
| 1 | https://ocw.mit.edu |
| 2 | https://hadoop.apache.org/docs/ |

| | |
|---|---|
| **Assessment:** | |
| **Internal Assessment:** | |
| Assessment consists of two class tests of 20 marks each. The first class test is to be conducted when approx. 40% syllabus is completed and second class test when additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| **End Semester Theory Examination:** | |
| 1 | Question paper will comprise of total six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only Four question need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lectures hours as mention in the syllabus. |

**List of Practical/ Experiments:**

| Sr. No | Topic |
|---|---|
| 1 | Implement a simple client-server chat application using TCP sockets in Python. |
| 2 | Use gRPC or Java RMI to create a distributed calculator service. |
| 3 | Simulate Lamport's logical clocks in a multi-process system. |
| 4 | Implement the Ricart-Agrawala algorithm for mutual exclusion in Python. |
| 5 | Code the Bully algorithm to elect a leader among distributed nodes. |

| | |
|---|---|
| 6 | Build a basic file-sharing system using sockets or a P2P framework. |
| 7 | Write a MapReduce program in Hadoop to count words in a large text file. |
| 8 | Use Apache Spark to process a dataset (e.g., movie ratings) and compute averages. |
| 9 | Simulate node failures in a distributed system and implement recovery. |
| 10. | Develop a real-time chat system using a distributed framework (e.g., MPI or Spark). |

| | |
|---|---|
| **Term Work:** | |
| 1 | Term work should consist of 10 experiments. |
| 2 | Journal must include at least 2 assignments on content of theory and practical of "Software Engineering" |
| 3 | The final certification and acceptance of term work ensures that satisfactory performance of laboratory work and minimum passing marks in term work. |
| 4 | Total 25 Marks (Experiments: 15-marks, Attendance Theory & Practical: 05-marks, Assignments: 05-marks) |
| **Oral & Practical exam** | |
| | Based on the entire syllabus. |

| Course Code: | Course Title | Credit |
|---|---|---|
| 21604 | Cloud Computing Security | 4 |

| Prerequisite: No Prerequisite | |
|---|---|
| **Course Objectives:** | |
| 1 | Understand the principles of cloud computing and the associated security challenges. |
| 2 | Develop skills to secure cloud infrastructure, applications, and APIs against modern threats. |
| 3 | Gain hands-on experience with tools for monitoring, securing, and auditing cloud environments. |
| 4 | Learn to design robust incident response and disaster recovery strategies for cloud platforms. |
| 5 | Explore emerging cloud security trends and advanced solutions like zero trust and AIdriven security. |
| **Course Outcomes: On Successful completion of course, learner will be able to** | |
| 1 | Demonstrate a comprehensive understanding of cloud security models, tools, and best practices. |
| 2 | Analyze and mitigate vulnerabilities in cloud applications and network configurations. |
| 3 | Use forensic and monitoring tools to detect, respond to, and recover from cloud security incidents. |
| 4 | Implement secure development and deployment pipelines in cloud environments. |
| 5 | Evaluate emerging cloud security technologies and adapt them to organizational needs. |

| Module | | Content | Hrs |
|---|---|---|---|
| **1** | | **Fundamentals of Cloud Computing Security** | **7** |

| | | | |
|---|---|---|---|
| | 1.1 | **Overview of Cloud Computing**<br><br>• Service models (IaaS, PaaS, SaaS)<br>• Deployment models (Public, Private, Hybrid) | |

| | | | |
|---|---|---|---|
| | | • Shared responsibility model | |
| | 1.2 | **Cloud Security Challenges**<br><br>• Threats specific to cloud environments<br>• Common vulnerabilities and misconfigurations<br>• Case studies of cloud security incidents | |
| | 1.3 | **Basics of Cloud Security Tools**<br><br>• Introduction to key tools (AWS Security Hub, Azure Security Center)<br>• Features of cloud-native security tools<br>• Setting up a secure cloud environment | |
| **2** | | **Cloud Identity and Data Security** | **8** |
| | 2.1 | **Identity and Access Management (IAM)**<br><br>• Role-based access control (RBAC)<br>• Configuring Multi-Factor Authentication (MFA)<br>• IAM policy management and best practices | |
| | 2.2 | **Data Security in the Cloud**<br><br>• Data classification and encryption techniques<br>• Key Management Service (KMS) in cloud platforms<br>• Securing data at rest and in transit | |
| | 2.3 | **Secure Data Backups and Recovery**<br><br>• Automated backup strategies<br>• Recovery from accidental or malicious deletion<br>• Cloud storage access control | |
| **3** | | **Cloud Infrastructure and Network Security** | **7** |
| | 3.1 | **Securing Virtual Machines and Containers**<br><br>• Hardening virtual machines (VMs)<br>• Security considerations for containerized applications • Managing vulnerabilities in Kubernetes clusters | |

| | | | |
|---|---|---|---|
| | 3.2 | **Cloud Network Security**<br>• Configuring Virtual Private Clouds (VPCs)<br>• Implementing firewalls and security groups<br>• Preventing network-based attacks in the cloud | |
| | 3.3 | **Monitoring and Auditing Cloud Infrastructure**<br>• Real-time monitoring using tools (CloudTrail, Azure Monitor) | |

| | | | |
|---|---|---|---|
| | | • Setting up alerts for suspicious activities<br>• Log analysis and forensic auditing | |
| **4** | | **Application and API Security in the Cloud** | **7** |
| | 4.1 | **Securing Cloud Applications**<br>• Secure application development practices<br>• Cloud-specific vulnerabilities and mitigations<br>• Tools for automated security testing | |
| | 4.2 | **API Security in Cloud Environments**<br>• Authentication mechanisms (OAuth, JWT)<br>• Common API vulnerabilities and their exploitation<br>• Best practices for securing APIs | |
| | 4.3 | **DevSecOps in Cloud Applications**<br>• Integrating security into CI/CD pipelines<br>• Tools for automated security in DevOps (Jenkins, GitLab)<br>• Continuous security assessment practices | |
| **5** | | **Incident Response and Disaster Recovery in the Cloud** | 8 |
| | 5.1 | **Cloud Incident Response**<br>Identifying and responding to security incidents<br>• Containment, eradication, and recovery processes<br>• Case study of a cloud data breach | |
| | 5.2 | **Business Continuity and Disaster Recovery (BC/DR)**<br>• Designing disaster recovery plans for cloud environments<br>• Testing recovery strategies using cloud tools<br>• Using snapshots and backups for rapid recovery | |
| | 5.3 | **Legal and Compliance Considerations**<br>• GDPR, HIPAA, and other regulatory requirements<br>• Cloud provider compliance certifications<br>• Audit frameworks for cloud services | |
| **6** | | **Emerging Trends in Cloud Security** | **8** |

| | | | |
|---|---|---|---|
| | 6.1 | **Zero Trust Security for the Cloud**<br>• Principles of zero trust architecture<br>• Implementing zero trust in hybrid and multi-cloud setups<br>• Advantages and limitations of zero trust | |
| | 6.2 | **AI-Driven Threat Detection**<br>• Machine learning techniques for anomaly detection<br>• AI-based tools for identifying cloud-specific threats • Automating threat responses using AI | |
| | 6.3 | **Future of Cloud Security**<br>• Challenges with quantum computing and post-quantum encryption<br>• Advanced serverless architecture and its security concerns<br>• Innovations in cross-cloud security tools | |
| **Total** | | | **45** |

| **Textbooks:** | |
|---|---|
| 1 | Practical Cloud Security: A Guide for Secure Design and Deployment, Chris Dotson, O'Reilly Media |
| **References:** | |
| 1 | AWS Security Cookbook, Heartin Kanikathottu, Dylan Shields, Packt Publishing. |
| 2 | Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Ronald L. Krutz, Russell Dean Vines, Wiley. |
| **Useful Link for E-Resources:** | |
| 1 | Introduction to Cloud Identity \| Coursera |
| 2 | Cloud Security Training Courses \| Learn Cloud Security Online Today |
| 3 | Cloud Security Essentials Course \| CSE Certification \| EC-Council |

| **Assessment:** | |
|---|---|
| **Internal Assessment:** | |
| Assessment consists of two class tests of 20 marks each. The first-class test is to be conducted when approx. 40% syllabus is completed and the second-class test when an additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| **End Theory Examination:** | |
| 1 | Question paper will comprise a total of six questions. |

| | |
|---|---|
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only four questions need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus. |

**List of Practical/ Experiments:**

| Sr. No | Topic |
|---|---|
| 1 | Understanding the components of cloud infrastructure (IaaS, PaaS, SaaS) and their security implications. |
| 2 | Configuring and managing IAM policies to ensure secure access control. |
| 3 | Implementing encryption techniques for data at rest and in transit within cloud environments. |
| 4 | Using tools to identify and mitigate vulnerabilities in cloud systems. |
| 5 | Simulating and responding to security breaches in a cloud environment. |
| 6 | Ensuring cloud setups meet regulatory and compliance standards. |
| 7 | Designing and testing disaster recovery strategies for cloud-based systems. |

| Course Code: | Course Title | Credit |
|---|---|---|
| **21 605** | **Machine Learning-II** | **4** |

| | |
|---|---|
| **Prerequisite:** Machine Learning Part-1 or equivalent (Supervised/Unsupervised Learning, Python proficiency). | |
| **Course Objectives:** | |
| 1 | To deepen students' understanding of advanced machine learning algorithms and techniques. |
| 2 | To introduce ensemble methods, neural networks, and reinforcement learning concepts. |
| 3 | To develop skills in handling complex datasets and optimizing ML models for real-world applications. |
| 4 | To provide hands-on experience with deep learning frameworks. |
| 5 | To explore ethical considerations and practical challenges in deploying machine learning systems. |
| **Course Outcomes:** | |
| 1 | Implement and compare advanced ML algorithms like ensemble methods and neural networks. |
| 2 | Design solutions for complex problems using dimensionality reduction and feature engineering. |
| 3 | Optimize and deploy ML models using modern frameworks and techniques. |
| 4 | Analyze the trade-offs and limitations of advanced ML approaches in practical scenarios. |
| 5 | Demonstrate an understanding of reinforcement learning and its applications. |

| Module | | Content | Hrs |
|---|---|---|---|
| **1** | | **Advanced Supervised Learning** | **8** |
| | 1.1 | Ensemble Methods: Bagging, Boosting (AdaBoost, Gradient Boosting). | |
| | 1.2 | Support Vector Machines (SVM): Kernels, Margin Maximization. | |
| | 1.3 | Regularization Techniques: L1 (Lasso), L2 (Ridge). | |
| | 1.4 | Evaluation: ROC Curves, AUC, Confusion Matrix Analysis. | |
| **2** | | **Advanced Unsupervised Learning** | **8** |
| | 2.1 | Advanced Clustering: DBSCAN, Gaussian Mixture Models (GMM) | |
| | 2.2 | Dimensionality Reduction: t-SNE, UMAP. | |
| | 2.3 | Anomaly Detection: Isolation Forest, One-Class SVM. | |

| | | | |
|---|---|---|---|
| | 2.4 | Applications: Customer Segmentation, Fraud Detection. | |
| **3** | | **Introduction to Neural Networks** | **7** |
| | 3.1 | Perceptrons and Multi-Layer Perceptrons (MLP). | |
| | 3.2 | Activation Functions: Sigmoid, ReLU, Tanh. | |
| | 3.3 | Backpropagation and Gradient Descent Variants (SGD, Adam). | |
| | 3.4 | Overfitting Prevention: Dropout, Weight Decay. | |

| | | | |
|---|---|---|---|
| **4** | | **Deep Learning Basics** | **8** |
| | 4.1 | Convolutional Neural Networks (CNN): Architecture, Convolution Layers. | |
| | 4.2 | Recurrent Neural Networks (RNN): LSTM, GRU. | |
| | 4.3 | Frameworks: TensorFlow, PyTorch Introduction. | |
| | 4.4 | Applications: Image Classification, Time Series Prediction. | |
| **5** | | **Reinforcement Learning Fundamentals** | **7** |
| | 5.1 | Markov Decision Processes (MDP): States, Actions, Rewards. | |
| | 5.2 | Q-Learning and Value Iteration. | |
| | 5.3 | Exploration vs. Exploitation: Epsilon-Greedy, UCB. | |
| | 5.4 | Practical Examples: Game Playing, Robotics. | |
| **6** | | **Model Optimization and Deployment** | **7** |
| | 6.1 | Hyperparameter Tuning: Bayesian Optimization, Genetic Algorithms. | |
| | 6.2 | Model Interpretability: SHAP, LIME. | |
| | 6.3 | Deployment: Flask for ML APIs, Model Serving with Docker. | |
| | 6.4 | Ethical Issues: Bias, Fairness, Privacy in ML. | |
| **Total** | | | **45** |

| | |
|---|---|
| **Textbooks:** | |
| 1 | "Advanced Machine Learning" by Dr. Sunita Jahirabadkar and Dr. Parag Kulkarni, Wiley India. |
| 2 | "Machine Learning and Deep Learning" by Dr. S. Sridhar and Dr. M. Chandrasekaran,PHI Learning (India). |
| 3 | "Deep Learning" by Ian Goodfellow, Yoshua Bengio, and Aaron Courville, MIT Press |
| **References:** | |
| 1 | "Pattern Recognition and Machine Learning" by Christopher M. Bishop, Springer |

| | |
|---|---|
| 2 | "Reinforcement Learning: An Introduction" by Richard S. Sutton and Andrew G. Barto, MIT Press. |
| **Useful Links for E-resources:** | |
| 1 | http://cs231n.stanford.edu |
| 2 | https://machinelearningmastery.com/machine- learning-in-python-step-by-step/ |
| 3 | https://towardsdatascience.com/beginners-guide-to- machine-learning-with-pythonb9ff35bc9c51 |
| 4 | https://nptel.ac.in/courses/106106145 |

| | |
|---|---|
| **Assessment:** | |
| **Internal Assessment:** | |
| Assessment consists of two class tests of 20 marks each. The first class test is to be conducted when approx. 40% syllabus is completed and second class test when additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| **End Semester Theory Examination:** | |
| 1 | Question paper will comprise of total six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only Four question need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lectures hours as mention in the syllabus. |

**List of Practical/ Experiments:**

| Sr. No | Topic |
|---|---|
| 1 | Implement a random forest classifier on a dataset (e.g., spam detection) and analyze feature importance. |
| 2 | Use XGBoost to predict a target variable (e.g., customer churn) and tune hyperparameters. |
| 3 | Train an SVM with different kernels (linear, RBF) on a dataset (e.g., digits) and compare performance. |
| 4 | Detect outliers in a dataset (e.g., credit card fraud) and evaluate with precision-recall. |
| 5 | Apply t-SNE to visualize high-dimensional data (e.g., gene expression) in 2D/3D. |
| 6 | Implement an MLP in PyTorch/TensorFlow for a classification task (e.g., fashion MNIST). |
| 7 | Train a CNN on a small image dataset (e.g., CIFAR-10) and analyze accuracy. |

| | |
|---|---|
| 8 | Implement Q-learning to solve a grid-world problem or a game like Frozen Lake. |
| 9 | Use SHAP to explain predictions of a gradient boosting model on a dataset (e.g., loan approval). |
| 10. | Create a REST API to serve predictions from a trained model (e.g., sentiment analysis). |
| 11 | Design and train a CNN or RNN for a real-world task (e.g., handwritten digit recognition). |

| **Term Work:** | |
|---|---|
| 1 | Term work should consist of 10 experiments. |
| 2 | Journal must include at least 2 assignments on content of theory and practical of "Software Engineering" |
| 3 | The final certification and acceptance of term work ensures that satisfactory performance of laboratory work and minimum passing marks in term work. |
| 4 | Total 25 Marks (Experiments: 15-marks, Attendance Theory & Practical: 05-marks, Assignments: 05-marks) |
| **Oral & Practical exam** | |
| | Based on the entire syllabus. |

| Course Code: | Course Title | Credit |
|---|---|---|
| 21606 | Security Information and Event Management | 4 |

| | |
|---|---|
| **Prerequisite: No Prerequisite** | |
| **Course Objectives:** | |
| 1 | To understand the architecture and functioning of SIEM systems. |
| 2 | To gain knowledge about log collection, event correlation, and threat detection processes. |
| 3 | To explore real-time monitoring and alerting capabilities of SIEM solutions. |
| 4 | To learn to configure and analyze SIEM dashboards for actionable insights. |
| 5 | To gain hands-on experience in deploying and managing SIEM tools in various environments. |
| **Course Outcomes: On Successful completion of course, learner will be able to** | |
| 1 | Demonstrate the ability to deploy and configure SIEM systems for real-time threat monitoring. |
| 2 | Analyze logs and events to identify and respond to potential security incidents. |
| 3 | Utilize SIEM dashboards to generate actionable insights and reports. |
| 4 | Understand advanced use cases like threat hunting and compliance management using SIEM. |
| 5 | Apply SIEM tools in enterprise environments to ensure security and compliance. |

| Module | | Content | Hrs |
|---|---|---|---|

| | | | |
|---|---|---|---|
| **1** | | **Introduction to SIEM** | **7** |
| | 1.1 | **Overview of SIEM Systems** | |
| | | • Purpose and benefits of SIEM.<br>• Components of a SIEM system (log collectors, correlation engines, dashboards).<br>• Use cases in security monitoring. | |
| | 1.2 | **Fundamentals of Log Management**<br>• Log collection processes.<br>• Parsing and normalization of logs.<br>• Common log sources (OS, applications, network devices). | |
| | 1.3 | **Event Correlation** • Correlation rules and their importance.<br>• Examples of correlation logic (brute force, lateral movement). | |
| **2** | | **SIEM Deployment and Configuration** | **8** |
| | 2.1 | **SIEM Architecture**<br>• Deployment models (on-premise vs. cloud-based SIEM).<br>• Integration with other security tools. | |
| | 2.2 | **Data Onboarding**<br>• Configuring log sources.<br>• Managing log storage and retention policies.<br>• Common challenges in data ingestion. | |
| | 2.3 | **Configuring SIEM Alerts**<br>• Setting thresholds and triggers.<br>• Avoiding false positives and negatives. | |
| **3** | | **Monitoring and Threat Detection** | **7** |
| | 3.1 | **Real-Time Monitoring**<br>• Analyzing live data streams.<br>• Identifying unusual patterns and behaviors. | |

| | | | |
|---|---|---|---|
| | 3.2 | **Incident Detection and Response** • Understanding SOC workflows with SIEM. • Automating responses using SOAR (Security Orchestration, Automation, and Response). | |
| | 3.3 | **Threat Intelligence Integration** • Incorporating threat feeds into SIEM. • Enriching alerts with contextual data. | |
| **4** | | **Advanced Analytics in SIEM** | 7 |
| | 4.1 | **Machine Learning in SIEM** • Behavioral analytics for anomaly detection. • Building baselines and detecting deviations. | |
| | 4.2 | **Advanced Use Cases** • Threat hunting with SIEM. • Compliance auditing and reporting. | |
| | 4.3 | **Case Studies**Analysis of real-world SIEM deployments. • Lessons learned from security incidents. | |
| **5** | | **SIEM Tools and Technologies** | 8 |
| | 5.1 | **Popular SIEM Solutions** • Overview of tools like Splunk, QRadar, ArcSight, and Elastic Stack. • Feature comparison and selection criteria. | |
| | 5.2 | **Customization and Scripting** • Writing custom dashboards and reports. • Using APIs to extend SIEM functionalities. | |
| | 5.3 | **Hands-On Labs** • Deploying a SIEM solution in a lab environment. • Configuring log sources and setting up alerts. | |
| **6** | | **Challenges and Future of SIEM** | **8** |
| | 6.1 | **Common Challenges** • Scalability, performance, and cost considerations. • Managing noisy alerts and alert fatigue. | |

| | | | |
|---|---|---|---|
| | 6.2 | **Emerging Trends & Future Directions** • <br><br> SIEM in cloud-native environments. <br><br> • Integration with XDR (Extended Detection and Response). <br> • Role of AI and ML in enhancing SIEM capabilities. <br> • Transition towards hybrid SIEM architectures. | |
| **Total** | | | **45** |

| **Textbooks:** | |
|---|---|
| 1 | Mastering Splunk, James D. Miller, Packt Publishing. |
| **References:** | |
| 1 | Practical Threat Intelligence and Data-Driven Threat Hunting, Valentina Costa-Gazcon, Packt Publishing |
| 2 | Cybersecurity Attack and Defense Strategies, Yuri Diogenes, Dr. Erdal Ozkaya, Packt Publishing |
| **Useful Link for E-Resources:** | |
| 1 | Introduction to SIEM (Splunk) \| Coursera |
| 2 | Security Onion Solutions |
| 3 | Cyber Security SOC Analyst Training - SIEM (Splunk) \| Udemy |

| **Assessment:** | |
|---|---|
| **Internal Assessment:** | |
| Assessment consists of two class tests of 20 marks each. The first-class test is to be conducted when approx. 40% syllabus is completed and the second-class test when an additional 40% syllabus is completed. Duration of each test shall be one hour. | |
| **End Theory Examination:** | |
| 1 | Question paper will comprise a total of six questions. |
| 2 | All question carries equal marks |
| 3 | Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3) |
| 4 | Only four questions need to be solved. |
| 5 | In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus. |

**List of Practical/ Experiments:**

| **Sr. No** | **Topic** |
|---|---|

| | |
|---|---|
| 1 | Gathering and analyzing log data from various sources like firewalls, servers, and applications. |
| 2 | Using SIEM tools to identify anomalies and potential security threats. |
| 3 | Practicing responses to simulated security incidents using SIEM systems. |
| 4 | Setting up and customizing dashboards for real-time monitoring. |
| 5 | Creating rules to correlate events and detect complex attack patterns. |
| 6 | Generating reports to meet regulatory and compliance requirements. |
| 7 | **Case Studies**: Investigating real-world scenarios using SIEM tools like Splunk, IBM QRadar, or ArcSight. |

| **Course Code:** | **Course Title** | **Credit** |
|---|---|---|
| **21607** | **Skill based Internship** | **2** |

| |
|---|
| **Assessment:** |
| **Internal Assessment:** |
| Term Work marks 50 are based on Two Project Reviews and Final Presentation. Project should done based on Subjects learned in the Syllabus. |
| **End Theory Examination: No Practical and Oral Examinations** |