# UNIVERSITY OF MUMBAI

## Syllabus

## Honours/ Minor Degree Program

## in

## Cyber Security

## FACULTY OF SCIENCE & TECHNOLOGY

(As per AICTE guidelines with effect from the academic year 2022-2023)

| University of Mumbai<br>Cyber Security<br>(With effect from 2022-23) | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Year & Sem | Course Code and Course Title | Teaching Scheme Hours / Week | | | Examination Scheme and Marks | | | | | Credit Scheme |
| | | Theory | Seminar/ Tutorial | Pract | Internal Assessment | End Sem Exam | Term Work | Oral/ Pract | Total | Credits |
| TE Sem V | **HCSC501: Ethical Hacking** | 04 | -- | -- | 20 | 80 | -- | -- | 100 | 04 |
| | **Total** | **04** | **-** | **--** | **100** | | **-** | **-** | **100** | **04** |
| | | | | | | | | | | **Total Credits = 04** |
| | | | | | | | | | | |
| TE Sem. VI | **HCSC601: Digital Forensic** | 04 | -- | -- | 20 | 80 | -- | -- | 100 | 04 |
| | **Total** | **04** | **-** | **-** | **100** | | **-** | **-** | **100** | **04** |
| | | | | | | | | | | **Total Credits = 04** |
| | | | | | | | | | | |
| BE Sem. VII | **HCSC701: Security Information Management** | 04 | -- | -- | 20 | 80 | -- | -- | 100 | 04 |
| | **HCSSBL601: Vulnerability Assessment Penetration Testing (VAPT) Lab (SBL)** | -- | -- | 04 | -- | -- | 50 | 50 | 100 | 02 |
| | **Total** | **04** | **-** | **04** | **100** | | **50** | **50** | **200** | **06** |
| | | | | | | | | | | **Total Credits = 06** |
| | | | | | | | | | | |
| BE Sem. VIII | **HCSC801: Application Security** | 04 | - | -- | 20 | 80 | -- | -- | 100 | 04 |
| | **Total** | **04** | **-** | **-** | **100** | | **-** | **-** | **100** | **04** |
| | | | | | | | | | | **Total Credits = 04** |
| | | | | | | | | | | |
| **Total Credits for Semesters V,VI, VII &VIII = 04+04+06+04=18** | | | | | | | | | | |

| Cyber Security: Sem V | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Course Code** | **Course Title** | **Theory** | **Practical** | **Tutorial** | **Theory** | **Practical/Oral** | **Tutorial** | **Total** |
| **HCSC501** | **Ethical Hacking** | **04** | **--** | **--** | **04** | **--** | **--** | **04** |

| **Course Code** | **Course Title** | **Examination Scheme** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | **Theory Marks** | | | | **Term Work** | **Practical** | **Oral** | **Total** |
| | | **Internal assessment** | | | **End Sem. Exam** | | | | |
| | | **Test1** | **Test 2** | **Avg.** | | | | | |
| **HCSC501** | **Ethical Hacking** | **20** | **20** | **20** | **80** | **--** | **--** | **--** | **100** |

**Course Objectives:**

| **Sr. No.** | **Course Objectives** |
|---|---|
| The course aims: | |
| 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:**

| **Sr. No.** | **Course Outcomes** | **Cognitive levels of attainment as per Bloom's Taxonomy** |
|---|---|---|
| On successful completion, of course, learner/student will be able to: | | |
| 1 | Articulate the fundamentals of Computer Networks, IP Routing and core concepts of ethical hacking in real world scenarios. | L1,L2 |
| 2 | Apply the knowledge of information gathering to perform penetration testing and social engineering attacks. | L3 |
| 3 | Demonstrate the core concepts of Cryptography, Cryptographic checksums and evaluate the various biometric authentication mechanisms. | L1,L2 |
| 4 | Apply the knowledge of network reconnaissance to perform Network and web application-based attacks. | L3 |
| 5 | Apply the concepts of hardware elements and endpoint security to provide security to physical devices. | L3 |
| 6 | Simulate various attack scenarios and evaluate the results. | L4,L5 |

**DETAILED SYLLABUS:**

| **Sr. No.** | **Module** | **Detailed Content** | **Hours** | **CO Mapping** |
|---|---|---|---|---|
| 0 | **Prerequisite** | Computer Networks, Databases, system security | **2** | - |

| | | | | |
|---|---|---|---|---|
| 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 | **10** | CO1 |
| 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 | **08** | CO3 |
| 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 | **12** | CO2 |
| 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 | **10** | CO4 |
| 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><br>**Self-learning Topics**: IoT security | **6** | CO5 |
| VI | **Case Studies** | Various attacks scenarios and their remedies. Demonstration of attacks using DVWA.<br><br>**Self-learning Topics**: Session hijacking and man-in-middle attacks | **4** | CO6 |

**Text Books:**

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
4. Applied Cryptography, Protocols Algorithms and Source Code in C -- Bruce Schneier, 2nd Edition / 20th Anniversary Edition, Wiley, 2015

**Online Resources:**

| Sr. No. | Website Name |
|---|---|
| 1. | https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project |
| 2. | https://dvwa.co.uk/ |
| 3. | http://testphp.vulnweb.com/ |

**Assessment:**

**Internal Assessment (IA) for 20 marks:**

- IA will consist of Two Compulsory Internal Assessment Tests. Approximately 40% to 50% of syllabus content must be covered in First IA Test and remaining 40% to 50% of syllabus content must be covered in Second IA Test

➢ **Question paper format**

- Question Paper will comprise of a total of **six questions each carrying 20 marks Q.1** will be **compulsory** and should **cover maximum contents of the syllabus**
- **Remaining questions** will be **mixed in nature** (part (a) and part (b) of each question must be from different modules. For example, if Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)
- A total of **four questions** need to be answered

| Cyber Security: Sem VI | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Course Code** | **Course Title** | **Theory** | **Practical** | **Tutorial** | **Theory** | **Practical/Oral** | **Tutorial** | **Total** |
| **HCSC601** | **Digital Forensic** | **04** | **--** | **--** | **04** | **--** | **--** | **04** |

| **Course Code** | **Course Title** | **Examination Scheme** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | **Theory Marks** | | | | **Term Work** | **Practical** | **Oral** | **Total** |
| | | **Internal assessment** | | | **End Sem. Exam** | | | | |
| | | **Test1** | **Test 2** | **Avg.** | | | | | |
| **HCSC601** | **Digital Forensic** | **20** | **20** | **20** | **80** | **--** | **--** | **--** | **100** |

**Course Objectives:**

| **Sr. No.** | **Course Objectives** |
|---|---|
| The course aims: | |
| 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:**

| **Sr. No.** | **Course Outcomes** | **Cognitive levels of attainment as per Bloom's Taxonomy** |
|---|---|---|
| On successful completion, of course, learner/student will be able to: | | |
| 1 | Identify and define the class for various computer and cyber-crimes in the digital world. | L1,L2 |
| 2 | Understand the need of digital forensic and the role of digital evidence. | L1,L2 |
| 3 | Understand and analyze the role of File systems in computer forensics. | L1,L2,L3 |
| 4 | Demonstrate the incident response methodology with the best practices for incidence response with the application of forensics tools. | L3 |
| 5 | Generate/Write the report on application of appropriate computer forensic tools for investigation of any computer security incident . | L5 |
| 6 | Identify and investigate threats in network and mobile. | L4 |

**DETAILED SYLLABUS:**

| **Sr. No.** | **Module** | **Detailed Content** | **Hours** | **CO Mapping** |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| 0 | **Prerequisite** | **Computer Hardware**: Motherboard, CPU, Memory: RAM, Hard Disk Drive (HDD), Solid State Drive (SSD), Optical drive<br><br>**Computer Networks:** Introduction CN Terminology: Router, Gateway, OSI and TCP/IP Layers<br><br>**Operating Systems:** Role of OS in file management, Memory management utilities, Fundamentals of file systems used in Windows and Linux. | **2** | -- |
| I | **Introduction to Cybercrime and Computer-crime** | **1.1 Definition and classification of cybercrimes:** Definition, Hacking, DoS Attacks, Trojan Attacks, Credit Card Frauds, Cyber Terrorism, Cyber Stalking.<br><br>**1.2 Definition and classification of computer crimes:** Computer Viruses, Computer Worms.<br><br>**1.3 Prevention of Cybercrime**: Steps that can be followed to prevent cybercrime, Hackers, Crackers, Phreakers.<br><br>**Self-learning Topics:** Steps performed by Hacker | **4** | CO1 |
| II | **Introduction to Digital Forensics and Digital Evidences** | **2.1 Introduction to Digital Forensics:** Introduction to Digital Forensics and lifecycle, Principles of Digital Forensic.<br><br>**2.2 Introduction to Digital Evidences:** Challenging Aspects of Digital Evidence, Scientific Evidence, Presenting Digital Evidence.<br><br>**2.3 Digital Investigation Process Models:** Physical Model, Staircase Model, Evidence Flow Model.<br><br>**Self-learning Topics:** Digital Investigation Process Models comparison and its application, Rules of Digital Evidence. | **5** | CO2 |
| III | **Computer Forensics** | **3.1 OS File Systems Review:** Windows Systems- FAT32 and NTFS, UNIX File Systems, MAC File Systems<br><br>**3.2 Windows OS Artifacts:** Registry, Event Logs<br><br>**3.3 Memory Forensics :** RAM Forensic Analysis, Creating a RAM Memory Image, Volatility framework, Extracting Information<br><br>**3.4 Computer Forensic Tools:** Need of Computer Forensic Tools, Types of Computer Forensic Tools, Tasks performed by Computer Forensic Tools<br><br>**Self-learning Topics:** Study of 'The Sleuth Kit' Autopsy tool for Digital Forensics | **7** | CO3 |
| IV | **Incident Response Management, Live Data Collection and Forensic Duplication** | **4.1 Incidence Response Methodology:** Goals of Incident Response, Finding and Hiring IR Talent<br><br>**4.2 IR Process:** Initial Response, Investigation, Remediation, Tracking of Significant Investigative Information.<br><br>**4.3 Live Data Collection:** Live Data Collection on Microsoft Windows, | **10** | CO4 |

| | | | | |
|---|---|---|---|---|
| | | **4.4 Forensic Duplication:** Forensic Duplicates as Admissible Evidence, Forensic Duplication Tools: Creating a Forensic evidence, Duplicate/Qualified Forensic Duplicate of a Hard Drive.<br><br>**Self-learning Topics:** Live Data Collection on Unix-Based Systems | | |
| V | **Forensic Tools and Report Writing** | **5.1 Forensic Image Acquisition in Linux :** Acquire an Image with dd Tools, Acquire an Image with Forensic Formats, Preserve Digital Evidence with Cryptography, Image Acquisition over a Network, Acquire Removable Media<br><br>**5.2 Forensic Investigation Report Writing:** Reporting Standards, Report Style and Formatting, Report Content and Organization.<br><br>**Self-learning Topics:** Case study on Report Writing | **10** | CO5 |
| VI | **Network Forensics and Mobile Forensics** | **6.1 Network Forensics:** Sources of Network-Based Evidence, Principles of Internetworking, Internet Protocol Suite, Evidence Acquisition, Analyzing Network Traffic: Packet Flow and Statistical Flow, Network Intrusion Detection and Analysis, Investigation of Routers, Investigation of Firewalls<br><br>**6.2 Mobile Forensics:** Mobile Phone Challenges, Mobile phone evidence extraction process, Android OS Architecture, Android File Systems basics, Types of Investigation, Procedure for Handling an Android Device, Imaging Android USB Mass Storage Devices.<br><br>**Self-learning Topic:** Elcomsoft iOS Forensic Toolkit, Remo Recover tool for Android Data recovery | **14** | CO6 |



**Text Books:**

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

**Online References:**

| Sr. No. | Website Name |
|---|---|
| 1. | https://www.pearsonitcertification.com/articles/article.aspx?p=462199&seqNum=2 |
| 2. | https://flylib.com/books/en/3.394.1.51/1/ |
| 3. | https://www.sleuthkit.org/autopsy/ |
| 4. | http://md5deep.sourceforge.net/md5deep.html |
| 5. | https://tools.kali.org/ |
| 6. | https://kalilinuxtutorials.com/ |
| 7. | https://accessdata.com/product-download/ftk-imager-version-4-3-0 |
| 8. | https://www.amazon.in/Art-Memory-Forensics-Detecting-Malware/dp/1118825098 |

**Research Papers: Mobile Forensics/Guidelines on Cell Phone Forensics**

1. Computer Forensics Resource Center: NIST Draft Special Publication 800-101 : https://csrc.nist.gov/publications/detail/sp/800-101/rev-1/final
2. https://cyberforensicator.com/category/white-papers
3. https://www.magnetforensics.com/resources/ios-11-parsing-whitepaper/
4. Samarjeet Yadav , Satya Prakash , Neelam Dayal and Vrijendra Singh, "Forensics Analysis WhatsApp in Android Mobile Phone", Electronic copy available at: https://ssrn.com/abstract=3576379

**Assessment:**

**Internal Assessment (IA) for 20 marks:**

- IA will consist of Two Compulsory Internal Assessment Tests. Approximately 40% to 50% of syllabus content must be covered in First IA Test and remaining 40% to 50% of syllabus content must be covered in Second IA Test

➢ **Question paper format**

- Question Paper will comprise of a total of **six questions each carrying 20 marks Q.1** will be **compulsory** and should **cover maximum contents of the syllabus**
- **Remaining questions** will be **mixed in nature** (part (a) and part (b) of each question must be from different modules. For example, if Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)
- A total of **four questions** need to be answered

| Cyber Security: Sem VII | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Course Code** | **Course Title** | **Theory** | **Practical** | **Tutorial** | **Theory** | **Practical/Oral** | **Tutorial** | **Total** |
| **HCSC701** | **Security Information Management** | **04** | **--** | **--** | **04** | **--** | **--** | **04** |

| **Course Code** | **Course Title** | **Examination Scheme** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | **Theory Marks** | | | | **Term Work** | **Practical** | **Oral** | **Total** |
| | | **Internal assessment** | | | **End Sem. Exam** | | | | |
| | | **Test 1** | **Test 2** | **Avg.** | | | | | |
| **HCSC701** | **Security Information Management** | **20** | **20** | **20** | **80** | **--** | **--** | **--** | **100** |

**Course Objectives:**

| **Sr. No.** | **Course Objectives** |
|---|---|
| The course aims: | |
| **1** | The course is aimed to focus on cybercrime and need to protect information. |
| **2** | Understand the types of attacks and how to tackle the amount of risk involved. |
| **3** | Discuss the role of industry standards and legal requirements with respect to compliance. |
| **4** | Distinguish between different types of access control models, techniques and policy. |
| **5** | Awareness about Business Continuity and Disaster Recovery. |
| **6** | Awareness about Incident Management and its life cycle. |

**Course Outcomes:**

| **Sr. No.** | **Course Outcomes** | **Cognitive levels of attainment as per Bloom's Taxonomy** |
|---|---|---|
| On successful completion, of course, learner/student will be able to: | | |
| **1** | Understand the scope of policies and measures of information security to people. | L1,L2 |
| **2** | Interpret various standards available for Information security. | L1,L2 |
| **3** | Apply risk assessment methodology. | L3 |
| **4** | Apply the role of access control to Identity management. | L3 |
| **5** | Understand the concept of incident management**,** disaster recovery and business continuity. | L1,L2 |
| **6** | Identify common issues in web application and server security. | L3 |

**DETAILED SYLLABUS:**

| **Sr. No.** | **Module** | **Detailed Content** | **Hours** | **CO Mapping** |
|---|---|---|---|---|
| 0 | **Prerequisite** | Vulnerability Assessment for Operating Systems, Network (Wired and Wireless). Tools for conducting Reconnaissance. | **2** | -- |

| | | | | |
|---|---|---|---|---|
| I | **Basics of Information Security** | **1.1** What is Information Security & Why do you need it? –<br>**1.2** Basics Principles of Confidentiality, Integrity<br>**1.3** Availability Concepts, Policies, procedures, Guidelines, Standards<br>**1.4** Administrative Measures and Technical Measures, People, Process, Technology, IT ACT 2000, IT ACT 2008<br><br>**Self-learning Topics:** Impact of IT on organizations, Importance of IS to Society | **6** | CO1, CO2 |
| II | **Current Trends in Information Security** | **2.1** Cloud Computing: benefits and Issues related to information Security.<br>**2.2** Standards available for InfoSec: Cobit, Cadbury, ISO 27001, OWASP, OSSTMM.<br>**2.3** An Overview, Certifiable Standards: How, What, When, Who.<br><br>**Self-learning Topics:** Cloud Threats, Impact of cloud computing on users, examples of cloud service providers: Amazon, Google, Microsoft, Salesforce etc. | **8** | CO2 |
| III | **Threat & Risk Management** | **3.1** Threat Modelling**:** Threat, Threat-Source, Vulnerability, Attacks.<br>**3.2** Risk Assessment Frameworks**:** ISO 31010, NIST-SP-800-30, OCTAVE<br>**3.3** Risk Assessment and Analysis: Risk Team Formation, Information and Asset Value, Identifying Threat and Vulnerability, Risk Assessment Methodologies<br>**3.4** Quantification of Risk, Identification of Monitoring mechanism, Calculating Total Risk and Residual Risk.<br><br>**Self-learning Topics:** Risk management trends today and tomorrow. | **8** | CO3 |
| IV | **Identity and Access Management** | **4.1** Concepts of Identification, Authentication, Authorization and Accountability.<br>**4.2** Access Control Models: Discretionary, Mandatory, Role based and Rule-based.<br>**4.3** Access Control Techniques: Constrained User, Access control Matrix, Content-dependent, Context – dependent<br>**4.4** Access Control Methods: Administrative, Physical, Technical, Layering of Access control<br>**4.5** Access Control Monitoring: IDS and IPS and anomaly detection.<br>**4.6** Accountability: Event-Monitoring and log reviews. Log Protection<br>**4.7** Threats to Access Control: Various Attacks on the Authentication systems.<br><br>**Self-learning Topics:** challenges and solutions in identity and access management | **10** | CO4 |
| V | **Operational Security** | **5.1** Concept of Availability, High Availability, Redundancy and Backup.<br>**5.2** Calculating Availability, Mean Time Between Failure (MTBF), Mean Time to Repair (MTTR) | **10** | CO5 |

| | | | | |
|---|---|---|---|---|
| | | **5.3** Incident Management**:** Detection, Response, Mitigation, Reporting, Recovery and Remediation<br>**5.4** Disaster Recovery:<br>Metric for Disaster Recovery, Recovery Time Objective (RTO), Recovery Point Objective (RPO), Work Recovery Time (WRT), Maximum Tolerable Downtime (MTD), Business Process Recovery, Facility Recovery (Hot site, Warm site, Cold site, Redundant site), Backup & Restoration<br><br>**Self-learning Topics:** Challenges and Opportunities of Having an IT Disaster Recovery Plan | | |
| VI | **Web Application, Windows, and Linux security** | **6.1** Types of Audits in Windows Environment<br>**6.2** Server Security, Active Directory (Group Policy), Anti-Virus, Mails, Malware<br>**6.3** Endpoint protection, Shadow Passwords, SUDO users, etc.<br>**6.4** Web Application Security: OWASP, Common Issues in Web Apps, what is XSS, SQL injection, CSRF, Password Vulnerabilities, SSL, CAPTCHA, Session Hijacking, Local and Remote File Inclusion, Audit Trails, Web Server Issues, etc.<br>**Self-learning Topics:**, Network firewall protection,Choosing the Right Web Vulnerability Scanner | **8** | CO6 |

**Textbooks:**


1. Shon Harris, Fernando Maymi, CISSP All-in-One Exam Guide, McGraw Hill Education, 7th Edition, 2016.
2. Andrei Miroshnikov, Introduction to Information Security - I, Wiley, 2018
3. Ron Lepofsky, The Manager's Guide to Web Application Security, Apress; 1st ed. edition, 2014


**References:**


1. Rich-Schiesser, IT Systems Management: Designing, Implementing and Managing World - Class Infrastructures, Prentice Hall; 2 edition, January 2010.
2. NPTEL Course: - Introduction to Information Security – I (URL: https://nptel.ac.in/noc/courses/noc15/SEM1/noc15-cs03/)
3. Dr. David Lanter – ISACA COBIT – 2019 Framework - Introduction and Methodology
4. Pete Herzog, OSSTMM 3, ISECOM
5. NIST Special Publication 800-30, Guide for Conducting Risk Assessments, September 2012


**Online References:**

| Sr. No. | Website Name |
|---|---|
| 1. | https://www.ultimatewindowssecurity.com/securitylog/book/Default.aspx |
| 2. | http://www.ala.org/acrl/resources/policies/chapter14 |
| 3. | https://advisera.com/27001academy/what-is-iso-27001/ |

| | |
|---|---|
| 4. | https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf |
| 5. | http://www.diva-portal.org/smash/get/diva2:1117263/FULLTEXT01.pdf |

**Assessment:**

**Internal Assessment (IA) for 20 marks:**

- IA will consist of Two Compulsory Internal Assessment Tests. Approximately 40% to 50% of syllabus content must be covered in First IA Test and remaining 40% to 50% of syllabus content must be covered in Second IA Test

➢ **Question paper format**

- Question Paper will comprise of a total of **six questions each carrying 20 marks Q.1** will be **compulsory** and should **cover maximum contents of the syllabus**
- **Remaining questions** will be **mixed in nature** (part (a) and part (b) of each question must be from different modules. For example, if Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)
- A total of **four questions** need to be answered

| Cyber Security: Sem VII | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Teaching Scheme (Contact Hours) | | | Credits Assigned | | | |
| Course Code | Course Title | Theory | Practical | Tutorial | Theory | Practical & Oral | Tutorial | Total |
| HCSSBL701 | Vulnerability Assessment Penetration Testing (VAPT) Lab (SBL) | -- | 4 | -- | -- | 2 | -- | 2 |

| Course Code | Course Title | Examination Scheme | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Theory Marks | | | | Term Work | Practical/ Oral | Total |
| | | Internal assessment | | | End Sem. Exam | | | |
| | | Test1 | Test 2 | Avg. | | | | |
| HCSSBL701 | Vulnerability Assessment Penetration Testing (VAPT) Lab (SBL) | -- | -- | -- | -- | 50 | 50 | 100 |

**Lab Objectives:**

| Sr. No. | Lab Objectives |
|---|---|
| The Lab aims: | |
| 1 | To identify security vulnerabilities and weaknesses in the target applications. |
| 2 | To discover potential vulnerabilities which are present in the system in network using vulnerability assessment tools. |
| 3 | To identify threats by exploiting them using penetration test attempt by utilizing the vulnerabilities in a system |
| 4 | To recognize how security controls can be improved to prevent hackers gaining access controls to database. |
| 5 | To test and exploit systems using various tools and understands the impact in system logs. |
| 6 | To write a report with a full understanding of current security posture and what work is necessary to both fix the potential threat and to mitigate the same source of vulnerabilities in the future |

**Lab Outcomes:**

| Sr. No. | Lab Outcomes | Cognitive levels of attainment as per Bloom's Taxonomy |
|---|---|---|
| On successful completion, of lab, learner/student will be able to: | | |
| 1 | Understand the structure where vulnerability assessment is to be performed. | L1,L2 |
| 2 | Apply assessment tools to identify vulnerabilities present in the system in network. | L3 |
| 3 | Evaluate attacks by executing penetration tests on the system or network. | L4 |
| 4 | Analyse a secure environment by improving security controls and applying prevention mechanisms for unauthorised access to database. | L5 |
| 5 | Create security by testing and exploit systems using various tools and remove the impact of hacking in system. | L6 |

| | | |
|---|---|---|
| 6 | Formation of documents as per applying the steps of vulnerabilities of assessment and penetration testing. | L3, L4, L5 |

**Prerequisite:** Computer Networks, Basic of Network Security.

**Hardware & Software Requirements:**

| Hardware Requirements | Software Requirements | Other Requirements |
|---|---|---|
| PC With Following Configuration<br>1. Intel PIV Processor<br>2. 4 GB RAM<br>3. 500 GB Harddisk<br>4. Network interface card | 1. Windows or Linux Desktop OS<br>2. Security Software and tools | 1. Internet Connection. |

**DETAILED SYLLABUS:**

| Sr. No. | Module | Detailed Content | Hours | CO Mapping |
|---|---|---|---|---|
| **0** | **Prerequisite** | Computer Network, Basics of Network Security, Ethical Hacking, Digital Forensics | **2** | |
| I | **Human Security (Social Engineering) Assessment** | **Visibility Audit: C**ollecting information through social media and internet. Collecting contact details (like phone number, email ID, What's App ID, etc)<br>**Active Detection Verification:** Test if the phone number, email id etc are real by test message. Test whether the information is filtered at point of reception. Test if operator / another person assistance can be obtained.<br>**Device Information:** IP Address, Port details, Accessibility, Permissions, Role in business<br>**Trust Verification:** Test whether the information can be planted in form of note / email / Message (Phishing)<br>**Test Subjects:** College Staff, Reception, PA to Director / Principal. To conduct information gathering to conduct social engineering audit on various sections in your college.<br>**Self-Learning Topics:** Networking Commands | **8** | LO1 |
| II | **Network & Wireless Security Assessment** | **Network Discovery:** Using various tools to discover the various connected devices, to get device name, IP Address, relation of the device in network, Detection of Active port, OS Fingerprinting, Network port and active service discovery<br>**Tools:** IP Scanner, Nmap etc<br>**Network Packet Sniffing:** Packet Sniffing to detect the traffic pattern, Packet capturing to detect protocol specific traffic pattern, Packet capturing to reassemble packet to reveal unencrypted password<br>**Tools:** Wireshark<br>**Self-Learning Topics:** Learning the CVE database for vulnerabilities detected. | **8** | LO2 |
| III | **Setting up Pentester lab** | Including an attacker machine preferably Kali and in the same subnet victim machines either DVWA/ SEEDlabs/ multiple | **9** | LO3 |

| | | | | |
|---|---|---|---|---|
| | | VULNHUB machines as and when required. Understanding Categories of pentest and legalities/ ethics.<br>Installed Kali machine on VM environment with some VULNHUB machines and we can find out vulnerability of Level 1-VULNHUB machine like deleted system files, permissions of files.<br>**Self learning Topics:** Vulnerability exploitation for acquire root access of the Kioptrx machine | | |
| IV | **Database and Access Control Security Assessment** | **Database Password Audit:** Tool based audit has to be performed for strength of password and hashes.<br>**Tools:** DBPw Audit<br>**Blind SQL Injection:** Test the security of the Database for SQL Injection<br>**Tools:** BSQL Hacker<br>**Password Audit:** Perform the password audit on the Linux / Windows based system<br>**Tools:** Cain & Able, John the ripper, LCP Password Auditing tools for Windows.<br>**Active Directory and Privileges Audit:** Conduct a review of the Active Directory and the Group Policy to assess the level of access privileges allocated.<br>**Tools:** SolarWinds<br>**Self-Learning Topics:** Federated Database security challenges and solutions. | **9** | LO4 |
| V | **Log Analysis** | Conduct a log analysis on Server Event Log / Firewall Logs / Server Security Log to review and obtain insights<br>Tools: graylog, Open Audit Module.<br>**Self-Learning Topics:** Python and R-Programming scripts | **6** | LO5 |
| VI | **Compliance and Observation Reporting** | **License Inventory Compliance:**<br>Identify the number of licenses and its deployment in your organization.<br>Tools: Belarc Advisor, Open Audit Report<br>Writing: NESSUS tool<br>Report should contain:<br>a. Vulnerability discovered<br>b. The date of discovery<br>c. Common Vulnerabilities and Exposure (CVE) database reference and score; those vulnerabilities found with a medium or high CVE score should be addressed immediately<br>d. A list of systems and devices found vulnerable<br>e. Detailed steps to correct the vulnerability, which can include patching and/or reconfiguration of operating systems or applications<br>f. Mitigation steps (like putting automatic OS updates in place) to keep the same type of issue from happening again<br>**Purpose of Reporting:** Reporting provides an organization with a full understanding of their current security posture and what work is necessary to both fix the potential threat and to mitigate the same source of vulnerabilities in the future.<br>**Self-Learning Topics:** Study of OpenVAS, Nikto, etc. | **10** | LO6 |

**Text & Reference Books and Links:**


1. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws Paperback – Illustrated, 7 October 2011 by Dafydd Stuttard
2. Hacking: The Art of Exploitation, 2nd Edition 2nd Edition by Jon Erickson
3. Important links of Vulnhub: Vulnhub Kioptrix
   Download Link: https://www.vulnhub.com/entry/basic-pentesting-1,216/
   https://www.vulnhub.com/entry/kioptrix-level-1-1,22/
   Installation Video: https://youtu.be/JupQRHtfZmw
   Walkthrough/solutions Video: https://youtu.be/Qn2cKYZ6kBI
4. OWASP Broken Web Application Projects
   https://sourceforge.net/projects/owaspbwa/
5. Mastering Modern Web Penetration Testing By Prakhar Prasad, October 2016, Packt Publishing.
6. Kali Linux Revealed: Mastering the Penetration Testing Distribution – June 5, 2017 by Raphael Hertzog (Author), Jim O'Gorman (Author), Offsec Press Publisher


**Term Work:**

The Term work shall consist of at least 10 to 12 practical based on the above syllabus. The term work Journal must include at least 2 assignments. The assignments should be based on real world applications which cover concepts from all above syllabus**.**

**Term Work Marks:** 50 Marks (Total marks) = 40 Marks (Experiment) + 5 Marks (Assignments/tutorial/write up) + 5 Marks (Attendance)

**Practical & Oral Exam: An Oral & Practical exam will be held based on the above syllabus.**

| Cyber Security: Sem VIII | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Course Code** | **Course Title** | **Theory** | **Practical** | **Tutorial** | **Theory** | **Practical/Oral** | **Tutorial** | **Total** |
| **HCSC801** | **Application Security** | **04** | **--** | **--** | **04** | **--** | **--** | **04** |

| **Course Code** | **Course Title** | **Examination Scheme** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | **Theory Marks** | | | | **Term Work** | **Practical** | **Oral** | **Total** |
| | | **Internal assessment** | | | **End Sem. Exam** | | | | |
| | | **Test1** | **Test 2** | **Avg. of 2 Tests** | | | | | |
| **HCSC801** | **Application Security** | **20** | **20** | **20** | **80** | **--** | **--** | **--** | **100** |

**Course Objectives:**

| **Sr. No.** | **Course Objectives** |
|---|---|
| The course aims: | |
| 1 | The terms and concepts of application Security, Threats, and Attacks |
| 2 | The countermeasures for the threats wrt Application security. |
| 3 | The Secure Coding Practices |
| 4 | The Secure Application Design and Architecture |
| 5 | The different Security Scanning and testing techniques |
| 6 | The threat modeling approaches |

**Course Outcomes:**

| **Sr. No.** | **Course Outcomes** | **Cognitive levels of attainment as per Bloom's Taxonomy** |
|---|---|---|
| On successful completion, of course, learner/student will be able to: | | |
| 1 | Enumerate the terms of application Security, Threats, and Attacks | L1 |
| 2 | Describe the countermeasures for the threats with respect to Application security. | L1 |
| 3 | Discuss the Secure Coding Practices. | L2 |
| 4 | Explain the Secure Application Design and Architecture. | L2 |
| 5 | Review the different Security Scanning and testing techniques. | L2 |
| 6 | Discuss the threat modeling approaches. | L2 |

**DETAILED SYLLABUS:**

| **Sr. No.** | **Module** | **Detailed Content** | **Hours** | **CO Mapping** |
|---|---|---|---|---|
| 0 | **Prerequisite** | Operating System, DBMS, Computer Network, Web Programming, OOP | **02** | - |

| | | | | |
|---|---|---|---|---|
| I | **Introduction to Application Security, Threats, and Attacks** | Introduction to Web Application Reconnaissance, Finding Subdomains, API Analysis, Identifying Weak Points in Application Architecture<br>**Offense:** Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), XML External Entity (XXE) Injection, Injection Attacks, Denial of Service (DoS), Cross-Origin Resource Sharing Vulnerabilities<br>**Self-learning Topics: Simulate the attacks using open-source tools in virtual environment** | **05** | CO1 |
| II | **Defence and tools** | Securing Modern Web Applications, Secure Application Architecture, Reviewing Code for Security, Vulnerability Discovery, Defending Against XSS Attacks, Defending Against CSRF Attacks, Defending Against XXE, Defending Against Injection attacks, Defending Against DoS, Defending against CORS based attacks<br>**Self-learning Topics: Implement the countermeasures to the attacks using open-source tools** | **09** | CO2 |
| III | **Secure Coding Practices** | Security Requirements, Encryption, Never Trust System Input, Encoding and Escaping, Third-Party Components, Security Headers: Seatbelts for Web Apps, Securing Your Cookies, Passwords, Storage, and Other Important Decisions, HTTPS Everywhere, Framework Security Features, File Uploads, Errors and Logging, Input Validation and Sanitization, Authorization and Authentication, Parameterized Queries, Least Privilege, Requirements Checklist<br>**Self-learning Topics: OWASP Secure Coding Practices** | **09** | CO3 |
| IV | **Secure Application Design and Architecture** | **Secure Software Development Lifecycle**<br>Averting Disaster Before It Starts, Team Roles for Security, Security in the Software Development Lifecycle,<br>**Design Flaw vs. Security Bug,**<br>**Secure Design Concepts,**<br>**Segregation of Production Data,**<br>**Application Security Activities**<br>**Self-learning Topics: Secure Hardware architecture** | **09** | CO4 |
| V | **Security Scanning and testing** | Testing Your Code, Testing Your Application, Testing Your Infrastructure, Testing Your Database, Testing Your APIs and Web Services, Testing Your Integrations, Testing Your Network, Dynamic Web Application Profiling<br>**Self-learning Topics: Open-source Application Security Tools, IAST, RASP and WAF, Selenium** | **09** | CO5 |
| VI | **Threat Modeling** | **Objectives and Benefits of Threat Modeling**,<br>Defining a Risk Mitigation Strategy, Improving Application Security, Building Security in the Software Development Life Cycle | **09** | CO6 |

| | | | | |
|---|---|---|---|---|
| | | **Existing Threat Modeling Approaches**<br><br>Security, Software, Risk-Based Variants<br><br>**Threat Modeling Within the SDLC**<br><br>Building Security in SDLC with Threat Modeling, Integrating Threat Modeling Within the Different Types of SDLCs,<br><br>**Self-learning Topics: The Common Vulnerability Scoring System (CVSS)** | | |

**Text Books:**

1. Alice and Bob Learn Application Security, by Tanya Janca Wiley; 1st edition (4 December 2020)
2. Web Application Security, A Beginner's Guide by Bryan Sullivan McGraw-Hill Education; 1st edition (16 January 2012)
3. Web Application Security: Exploitation and Countermeasures for Modern Web Applications by Andrew Hoffman Shroff/O'Reilly; First edition (11 March 2020)
4. The Security Development Lifecycle by Michael Howard Microsoft Press US; 1st edition (31 May 2006)
5. Risk Centric Threat Modeling Process for Attack Simulation And Threat Analysis, Tony Ucedavélez and Marco m. Morana, Wiley
6. Iron-Clad Java: Building Secure Web Applications (Oracle Press) 1st Edition by Jim Manico

**References:**


1. Software Security: Building Security In by Gary McGraw Addison-Wesley Professional; 1st edition (January 23, 2006)
2. A Guide to Securing Modern Web Applications by Michal Zalewski
3. Threat Modeling: A Practical Guide for Development Teams by Izar Tarandach and Matthew J. Coles Dec 8, 2020


**Online References:**

| Sr. No. | Website Name |
|---|---|
| 1. | https://owasp.org/www-project-top-ten/ |
| 2. | https://owasp.org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v2.pdf |
| 3. | https://pentesterlab.com/ |
| 4. | https://app.cybrary.it/browse/course/advanced-penetration-testing |
| 5. | https://www.udemy.com/ |
| 6. | https://www.coursera.org/ |

**Assessment:**

**Internal Assessment (IA) for 20 marks:**

- IA will consist of Two Compulsory Internal Assessment Tests. Approximately 40% to 50% of syllabus content must be covered in First IA Test and remaining 40% to 50% of syllabus content must be covered in Second IA Test

➢ **Question paper format**

- Question Paper will comprise of a total of **six questions each carrying 20 marks Q.1** will be **compulsory** and should **cover maximum contents of the syllabus**
- **Remaining questions** will be **mixed in nature** (part (a) and part (b) of each question must be from different modules. For example, if Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)
- A total of **four questions** need to be answered