**M. Sc. Cyber Security**

Syllabus

UNIVERSITY DEPARTMENT

**2022– 2023 onwards**

**BHARATHIAR UNIVERSITY**

**(A State University, Accredited with “A” Grade by NAAC, Ranked 13th among Indian Universities by MHRD-NIRF,**

**World Ranking: Times -801-1000,Shanghai -901-1000, URAP - 982)**

**Coimbatore - 641 046, Tamil Nadu, India**



|  |
| --- |
| **Program Educational Objectives (PEOs)** |
| The **M.Sc. Cyber Security** program describe accomplishments that graduates are expected to attain within five to seven years after graduation |
| PEO1 | To equip with the technical knowledge and skills needed to protect and defend computer systems and networks |
| PEO2 | To assimilate and use state of the art computing technologies, tools and techniques necessary to provide security to the computing platforms. |
| PEO3 | To equip with skill to design a system, component, or process to meet desired needs within realistic constraints such as economic, environmental, social and ethical contexts. |
| PEO4 | To develop graduates that can identify, analyze, and remediate computer security breaches. |
| PEO5 | To prepare, report and effectively communicate with the stakeholders about Information security process, standards and controls. |
| PEO6 | To practice managing security relevant projects and function effectively in cyber space as an individual, and as a member or leader in diverse teams. |
| PEO7 | To plan, implement, and monitor cyber security mechanisms to help ensure the protection of information technology assets. |
| PEO8 | To appeal self-learning for continual development as a cyber professional for the betterment of individuals, organizations, research community and society. |
| PEO9 | To select suitable ethical principles and commit to professional responsibilities and human values and also contribute value and wealth for the benefit of the society. |
| PEO10 | To systematically educate the necessity to understand the impact of cyber crimes and threats with solutions in a global and societal context |



|  |
| --- |
| **Program Specific Outcomes (PSOs)** |
| After the successful completion of M.Sc. Cyber Security program, the students are expected to |
| PSO1 | To understand the cyber space and frame the foundations of security principles, enterprise and models to suit the needs of the industry. |
| PSO2 | To select and operate the cloud infrastructure and enterprise system based on the security and storage needs. |
| PSO3 | To ensure the credibility of the information systems by managing the security standards and protocols. |
| PSO4 | To enumerate system vulnerability and provide solutions for vulnerabilities and other potential threats. |
| PSO5 | To code and execute python programming with a higher level of expertise. |
| PSO6 | To develop and assist in designing security software architecture and testing its credibility against threats. |
| PSO7 | To understand and carry out the digital forensics process for evidence collection under investigative techniques. |
| PSO8 | To develop basic understandings of IoT structures and develop familiarity with basic security attacks and its measures. |
| PSO9 | To develop a deeper understanding and familiarity with various types of cyber attacks and vulnerable frames to tackle them. |
| PSO10 | To raise skill in dealing with advanced web technologies allied with complex and sophisticated IT infrastructure. |



|  |
| --- |
| **Program Outcomes (POs)** |
| On successful completion of the M. Sc. Cyber Security program |
| PO1 | Analyze and evaluate the cyber security needs of an organization |
| PO2 | Conduct a cyber security risk assessment |
| PO3 | Perform Network and Application Vulnerability Assessment |
| PO4 | Implement sustainable cyber security solutions for various cyber threats as per business requirements. |
| PO5 | Articulated reporting and effective communication with the stakeholders, about security process, standards and controls. |
| PO6 | Spear head and run cyber security relevant projects and function effectively in cyber space as an individual, and as a member or leader in diverse teams. |
| PO7 | Design and Develop secure architecture for an organization |
| PO8 | Habit of self-learning for continual development as a cyber professional for the betterment of individuals, organizations, research community and society. |
| PO9 | Implementation of ethical principles and commit to professional responsibilities and human values and also contribute value and wealth for the benefit of the society. |
| PO10 | Evaluate the impact of cyber crimes and threats in a global and societal context. |

## M.Sc. CYBER SECURITY 2022-2023

**Univ.Dept. in collaboration with CSCC Lab**

***(Effective from the academic Year 2022-2023)***

## SCHEME OF EXAMINATIONS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Course Code** | **Title of the Course** | **Credits** | **Hours** | **Maximum Marks** |
| **Theory** | **Practical** | **CIA** | **ESE** | **Total** |
| **FIRST SEMESTER** |
| 21CSESC01 | Core I: Security Principles and Governance | 4 | 62 | 0 | 50 | 50 | 100 |
| 21CSESC02 | Core II: Network Technologies and Security | 4 | 62 | 0 | 50 | 50 | 100 |
| 21CSESC03 | Core III: Basics of Ethical Hacking for CyberSecurity | 4 | 32 | 60 | 50 | 50 | 100 |
| 21CSESC04 | Core IV: Python & Shell Programming | 4 | 32 | 60 | 50 | 50 | 100 |
| 21CSESC05 | Core V: Operating Systems | 4 | 32 | 30 | 50 | 50 | 100 |
|  | Elective I |  |  |  |  |  |  |
| Supportive | Offered by other Departments | 2 | 31 |  | 25 | 25 | 50 |
|  | **Total** | **22** | **220** | **150** | **275** | **275** | **550** |
| **SECOND SEMESTER** |
|  |  |  |  |  |  |  |  |
| 21CSESC07 | Core VI: Secure Software Design & Analysis | 4 | 62 | 0 | 50 | 50 | 100 |
| 21CSESC08 | Core VII: Digital Forensics & Best Practices | 4 | 62 | 0 | 50 | 50 | 100 |
| 21CSESC09 | Core VIII: Mobile & IoT | 4 | 32 | 60 | 50 | 50 | 100 |
| 21CSESC10 | Core IX: Advanced Ethical Hacking &Penetration Testing | 4 | 32 | 60 | 50 | 50 | 100 |
| 21CSESC11 | Core X: Information Systems RiskManagement | 4 | 62 | 0 | 50 | 50 | 100 |
|  | Elective II |  |  |  |  |  |  |
|  | **Total** | **20** | **250** | **120** | **300** | **300** | **600** |
| **THIRD SEMESTER** |
| 21CSESC12 | Core XI: Evolving Technologies and Threats | 4 | 62 | 0 | 50 | 50 | 100 |
| 21CSESC13 | Core XII: Security Standards and Compliance | 4 | 62 | 0 | 50 | 50 | 100 |
| 21CSESC14 | Core XIII: Case studies of Cyber Security – Paper 1 | 6 | 0 | 0 | 50 | 100 | 150 |
| 21CSESC15 | Core XIV: Case studies of Cyber Security – Paper 2 | 6 | 0 | 0 | 50 | 100 | 150 |
|  | Elective III |  |  |  |  |  |  |
|  | Elective IV |  |  |  |  |  |  |
| Supportive | Offered by other Departments | 2 | 31 |  | 25 | 25 | 50 |
|  | **Total** | **22** | **124** | **0** | **225** | **325** | **550** |
| **FOURTH SEMESTER** |
|  | Project / Dissertation + Viva-voce | 14 |  |  | 175 | 175 | 350 |
| **Total** | **14** |  |  | **175** | **175** | **350** |
| **Grand Total** | **94** | **594** | **270** | **975** | **1075** | **2050** |

|  |
| --- |
| **CO-SCHOLASTIC COURSES** |
| **ONLINE COURSES** |
|  | Swayam, MOOC Course etc., | 2 | - | - | - | - | - |
| **VALUE ADDED COURSES** |
|  | Value Added Course - I | 2 | 30 | - | 50 | - | 50 |
|  | Value Added Course - II | 2 | 30 | - | 50 | - | 50 |
| **CERTIFICATE COURSES** |
|  | Certificate Course - I | 4 | 30-40 | - | 100 | - | 100 |
|  | Certificate Course - II | 4 | 30-40 | - | 100 | - | 100 |
| The scholastic courses are only counted for the final grading and ranking. However, for theaward of the degree, the completion of co-scholastic courses is also mandatory. |

**Electives for M.Sc Cyber Security(CBCS)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Elective** | **Suggested Code** | **Title OfthePaper** | **L** | **P** |
| Elective | 21CSESE01 | IT Infrastructure and Cloud Security | 0 | 4 |
| Elective | 21CSESE02 | Malware Analysis | 2 | 2 |
| Elective | 21CSESE03 | Incident Response and Handling | 4 | 0 |
| Elective | 21CSESE04 | Cyber Threat and Intelligence | 4 | 0 |
| Elective | 21CSESE05 | Cyber Law | 4 | 0 |
| Elective | 21CSESE06 | Artificial Intelligence & Machine Learning | 4 | 0 |



First Semester



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Course code** | **21CSESC01** | **SECURITY PRINCIPLES & GOVERNANCE** | **L** | **T** | **P** | **C** |
|  | **Core/Elective/Supportive** | **Core** | **4** |  |  | **4** |
|  | **Pre-requisite** | **Terminologies and fundamentals of****Risk Management** | **Syllabus****Version** | **2022-****2023** |
|  | **Course Objectives:** |
|  | The main objectives of this course are to:1. To understand the fundamental functioning of securitypatterns.
2. To understand the Enterprise Security and Risk Management, AssetSecurity.
3. To understand the need for Authentication, Access controls, Securityoperations.
4. To understand Security Assessment andTesting.
 |
|  |  |
|  | **Expected Course Outcomes:** |
|  | On the successful completion of the course, student will be able to: |
|  | 1 | Understand the fundamental functioning of security patterns | K2 |
|  | 2 | Understand the Enterprise Security and Risk Management, Asset Security | K2 |
|  | 3 | Understand the Authentication, Access controls, Security operations | K2 |
|  | 4 | Understand the Security Assessment and Testing | K2 |
|  | 5 | Analyze, Apply, Create and Evaluate the Security Assessment and Testing | K3 –K6 |
|  | **K1** - Remember; **K2** - Understand; **K3** - Apply; **K4** - Analyze; **K5** - Evaluate; **K6** – Create |
|  |  |
|  | **Unit:1** | **Foundations of Security** | **10hours** |
|  | Overview of Security, Security Taxonomy, General Security Resources, Security Patterns-The History of Security Patterns, Scope of Pattern Characteristics of Security Patterns, Sources for Security Pattern Mining and Types of Patterns. |
|  |  |
|  | **Unit:2** | **Enterprise Security and Risk Management, Asset****Security** | **12 hours** |
|  | Security Needs Identification for Enterprise Assets, Asset Valuation, Threat Assessment, Vulnerability Assessment, Risk Determination, Enterprise Security Approaches, Enterprise Security Services and Enterprise Partner Communication. Identification and Authentication– Requirements, Automated Identification and Authentication Design Alternatives, Password Design and Use, Biometrics DesignAlternatives. |
|  |  |
|  | **Unit:3** | **Access Control Models** | **12 hours** |
|  | Authorization, Role-Based Access Control, Multilevel Security, Reference Monitor, Role Rights Definition, System Access Control Architecture - Access Control Requirements, Single Access Point, Check Point, Security Session, Full Access with Errors, Limited Access. Operating System Access Control – Authenticator, Controlled Process Creator, ControlledObjectFactory,ControlledObjectMonitor,ControlledVirtualAddressSpace,Execution Domain, Controlled Execution Environment and File Authorization. |
|  |  |
|  | **Unit:4** | **Security Operations** | **12hours** |
|  | Investigations, Investigation Types, Logging and Monitoring, Provisioning of Resources, Foundational Security Operations Concepts, Resource Protection Techniques, IncidentResponse,Preventative Measures, Patch and Vulnerability Management, Change Management Processes, Recovery Strategies,Disaster Recovery Processes,Disaster |



|  |  |
| --- | --- |
|  | Recovery Plans, Business Continuity Planning and Exercising Physical Security andPersonnel Safety. Recovery Plans, Business Continuity Planning and Exercising Physical Security and Personnel Safety |
|  |  |
|  | **Unit:5** | **Security Assessment & Testing** | **14hours** |
|  | Assessment and Test Strategies, Security Control, Collect Security Process Data, Test Output, Conduct or Facilitate Internal and Third-Party Audits. Software security – Security in the software development life cycle, Security controls in the development environment, Theeffectivenessofsoftwaresecurity,Assesssoftwareacquisitionsecurity.Casestudies-Web Security and Mobile Security. |
|  |  |
|  | **Unit:6** | **Contemporary Issues** | **2 hours** |
|  | Security Challenges in Robotics, Security challenges in Distributed Networks. |
|  |  |
|  |  | **Total Lecture hours** | **62 hours** |
| **Text Book(s)** |
| 1 | Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Frank Buschmann, Peter Sommerlad,“Security Patterns: Integrating Security andSystemsEngineering”, Wiley Publications, 2013. |
| 2 | Adam Gordon, Official (ISC)2 Guide to the CISSP CBK, Apple Academic Press Inc., Fourth Edition,2015 |
| 3 | Tony Hsiang-Chih Hsu,„Practical Security Automation and Testing‟,Packt Publishing,2019 |
| **Reference Books : EBooks** |
| 1 | [https://repo.zenk-](https://repo.zenk-security.com/Techniques%20d.attaques%20%20.%20%20Failles/The%20Art%20of%20Software%20Security%20Assessment%20-%20Identifying%20and%20Preventing%20Software%20Vulnerabilities.pdf) [security.com/Techniques%20d.attaques%20%20.%20%20Failles/The%20Art%20of%20](https://repo.zenk-security.com/Techniques%20d.attaques%20%20.%20%20Failles/The%20Art%20of%20Software%20Security%20Assessment%20-%20Identifying%20and%20Preventing%20Software%20Vulnerabilities.pdf) [Software%20Security%20Assessment%20-](https://repo.zenk-security.com/Techniques%20d.attaques%20%20.%20%20Failles/The%20Art%20of%20Software%20Security%20Assessment%20-%20Identifying%20and%20Preventing%20Software%20Vulnerabilities.pdf)[%20Identifying%20and%20Preventing%20Software%20Vulnerabilities.pdf](https://repo.zenk-security.com/Techniques%20d.attaques%20%20.%20%20Failles/The%20Art%20of%20Software%20Security%20Assessment%20-%20Identifying%20and%20Preventing%20Software%20Vulnerabilities.pdf) |

|  |
| --- |
| **Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]** |
|  | **Course Title** | **Duration** | **Provider** |
| 1 | IBM Cyber security Analyst Professional Certificate( 8-courses) |  | Coursera |
| **Web link** |  |  |
| 1. <http://softwaretestingfundamentals.com/security-testing/>
2. <https://www.ibm.com/in-en/cloud/devops/>
 |
| Course Designed by: Dr.M. Punithavalli & CSCC Labs |

|  |
| --- |
| **Mapping with Programme Outcomes** |
| **COs** | **PO 1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** | **PO8** | **PO9** | **PO10** |
| **CO1** | L | L | M | M | L | L | L | L | M | M |
| **CO2** | L | S | M | M | L | L | M | L | M | S |
| **CO3** | L | M | M | M | L | L | M | L | M | M |
| **CO4** | L | M | S | S | M | L | L | L | M | S |
| **CO5** | L | M | S | S | M | L | L | L | M | S |

\*S-Strong; M-Medium; L-Low

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Course code** | **21CSESC03** | **Network Technologies and Security** | **L** | **T** | **P** | **C** |
| **Core/Elective/Supportive** | Core | **4** | **0** | **0** | **4** |
| **Pre-requisite** | **Nil** | **Syllabus Version** | **2022-2023** |
| **Course Objectives:** |
| The main objectives of this course are to: 1. To understand the basics of networks, and reference models
2. To understand the types protocols and its usage
3. To discuss about the network security attacks and network security assessment
4. To know about assessment of network security and remote Information Services
5. To understand the security techniques used in cryptography
 |
|  |
| **Expected Course Outcomes:** |
| On the successful completion of the course, student will be able to: |
| 1 | Learn basics of computer networks and hardware | K1,K2 |
| 2 | Explain the Reference Models (OSI and TCP/IP) | K2,K4 |
| 3 | Understand network security and identify protocols | K2,K4 |
| 4 | Illustrate the security attacks  | K4,K5 |
| 5 | Explain Network Security Assessment and RIS | K2,K5 |
| 6 | Demonstrate about Cryptography algorithms | K2,K3,K5 |
| **K1** - Remember; **K2** - Understand; **K3** - Apply; **K4** - Analyze; **K5** - Evaluate; **K6**– Create |
|  |
| **Unit:1** | **Introduction to Computer Networks and Reference Models** | **12 hours** |
| **Overview of Computer Networks:** Introduction – Business and Home Applications – Mobile Users – Social Applications. Network Hardware: PAN – LAN – MAN – WAN. **Reference Models:** OSI – TCP/IP - Comparisons of OSI and TCP/IP. **Example Networks:** Internet – Arpanet – NSFNET – Mobile Phone Networks – Wireless LAN – RFID and Sensor Networks. |
|  |
| **Unit:2** | **Network and Transport Layer Protocols** | **12 hours** |
| **Network Layer Protocols:** Routing algorithms Congestion control: Principles –policies–Congestion control in VC subnets –congestion control in datagram subnets-Network layer in Internet: Architecture– IP protocol -IP Address – IPv6. **Firewalls:** Need – Characteristics – Types – Basing – Location and Configuration – IP Security Transport Protocols: Transport service – **Transport Layer Protocols**: TCP and UDP – Transport Level Security |
|  |
| **Unit:3** | **Challenges of Security attacks**  | **12 hours** |
| **Security Attacks:** Challenges of Securing Information – Threat Actors – Defending against Attacks. Attacking using Malware – Social Engineering Attacks. Networking based attacks -Server Attacks. Wireless Network Security Attacks and solutions. Types of mobile devices – mobile device risks – securing mobile devices – embedded systems and Internet of Things. |
|  |
| **Unit:4** | **Assessment of Network security and Remote Information Services** | **12 hours** |
| **Network Security Assessment:** Assessment Standards – Network Security Assessment and Platform. Assessing IP VPN Services: IPsec VPNs – Attacking IPsec VPNs. **Assessing Remote Information Services:** Remote Information Services – DNS – Finger – Auth – NTP – SNMP – LDAP – rwho – RPC rusers – Remote Information Services Countermeasures. |
|  |
| **Unit:5** | **Basics of Cryptography Algorithms** |  **12 hours** |
| **Overview of Cryptography:** Computer Security Concepts – OSI Security Architecture – Security Attacks – Security Services – Security Mechanisms. **Symmetric Ciphers:** Traditional Block Cipher Structure – DES – AES. **Asymmetric Ciphers:** Public Key Cryptography and RSA. **Hash Functions:** – SHA – SHA 3. **Message Authentication:** Requirements – Functions– codes - CCM and GCM. **Digital Signatures and Scheme**: (EDSS &SDSS) - Algorithms - NIST – ECDS – RSA-PSS. |
|  |
| **Unit:6** | **Contemporary Issues** | **2 hours** |
|  Submit an assignment by on cryptography algorithms or Resolve 4 Box in Hackthebox |
|  |
|  | **Total Lecture hours** | **62 hours** |
| **Text Book(s)** |
| 1 | Computer Networks (5th Edition), Andrew S.Tanenbaum David J. Wetherall, 2014. |
| 2 | Behrouz A. Forouzan, ― Data communication and Networking, Tata McGraw Hill, 4th Edition, 2006 |
| 3 | Cryptography and Network Security: Principles and Practice (6th Edition), William Stallings, Prentice Hall Press, 2013. |
| 4 | CompTIASecurity+ Guide to Network Security Fundamentals (6th Edition), Mark Ciampa, CENGAGE, 2017. |
| 5 | Network Security Assessment (2nd Edition), Chris McNab, O’REILLY, 2008. |
|  |
| **Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]** |
| 1 | <https://onlinecourses.swayam2.ac.in/ugc19_hs25/preview> |
| 2 | <https://www.coursera.org/learn/introduction-cybersecurity-cyber-attacks> |
| 3 | <https://www.udemy.com/course/cisco-networking-introduction/> |
|  | <https://nptel.ac.in/noc/courses/noc20/SEM1/noc20-cs33/> |
| Web Link1. [https://www.cisco.com/c/en\_in/solutions/small-business/resource-](https://www.cisco.com/c/en_in/solutions/small-business/resource-center/networking/networking-basics.html) [center/networking/networking-basics.html](https://www.cisco.com/c/en_in/solutions/small-business/resource-center/networking/networking-basics.html)
2. <https://docs.microsoft.com/en-us/learn/modules/network-fundamentals/>
3. <https://www.hackthebox.com/>
 |
| Course Designed By: Mr. S.Palanisamy |
|  **Mapping with Programme Outcomes** |
| **Cos** | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** | **PO8** | **PO9** | **PO10** |
| **CO1** | S | S | M | S | S | L | L | M | M | M |
| **CO2** | S | M | M | S | S | L | L | M | M | M |
| **CO3** | S | M | L | M | S | L | M | M | M | M |
| **CO4** | M | L | L | M | M | M | M | M | S | S |
| **CO5** | M | S | M | S | M | M | M | M | S | S |
| **CO6** | S | S | S | S | S | S | S | S | S | S |

\*S-Strong; M-Medium; L-Low





|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Course code** | **21CSESC03** | **BASICS OF ETHICAL HACKING FOR CYBER SECURITY** | **L** | **T** | **P** | **C** |
| **Core/Elective/Supportive** | **Core** | **2** |  | **2** | **4** |
| **Pre-requisite** | **Basics of Computers, Network, Linux****Usage and Cyber Security Terminology** | **Syllabus****Version** | **2022-2023** |
| **Course Objectives:** |
| The main objectives of this course are to:1. To understand Information Security, Cyber threats, attacks, websecurity.
2. To know about different modes of hacking tools and phases of penetration tests and Methodologies.
 |
| **Expected Course Outcomes:** |
| On the successful completion of the course, student will be able to: |
| 1 | Understand the basics of information security, threats and its attacks | K1, K2 |
| 2 | Understand the fundamentals of ethical hacking with the hackingMethodologies | K6 |
| 3 | Analyze the phases of the penetration test with the methods | K4 |
| 4 | Understand the vulnerabilities and use the frameworks to identifyvulnerabilities by service scan | K2-K4 |
| 5 | Understand the web security issues with the fundamentals of OWASP | K4-K5K6 |
| **K1** - Remember; **K2** - Understand; **K3** - Apply; **K4** - Analyze; **K5** - Evaluate; **K6** –Create |
|  |
| **Unit:1** | **Fundamentals of Ethical Hacking** | **18--hours** |
| Introduction to Ethical Hacking – Terminologies – Phases – Ethical Hacking – Lab Setup : Virtualization – kali Linux Installation – Installation of Pre-Vulnerable OS – OS Fundamentals: Windows, Linux, Mac OS – kali Linux Configurations – Adding Repository – apt – dpkg – rpm – Exploring Editors – nano - Vi – kali linux walkthrough |
|  |
| **Unit:2** | **Hacking Methodology Reconnaissance** | **18--hours** |
| **Foot printing:** Reconnaissance - Footprinting theory – Penetration test – Phases of Penetration test - Methods of Footprinting – Network Information gathering process – Terminologies of Foot printing –Footprinting through search engine directives – Whois tool–NetCraft – Extract Information from DNS - Foot printing from Email servers – Shodan – Dig – MetaGooFil – Social Engineering. |
|  |
| **Unit:3** | **Scanning and Enumeration** | **18--hours** |
| **Scanning:** Concept of Nmap - Port scanning with Nmap – Subnet - Scanning IPs with Nmap Pings and Ping sweeps – Port - Three way handshake – Nmap Syn scanning – Nmap TCP Scan – Nmap UDP Scan - Bypass of IPS and IDS – Nmap Script Engine **Enumeration:** Service Fingerprinting – Vulnerability Scanners – Basic Banner Grabbing– Common Network services – SMTP – DNS – RPCBIND Enumeration – SMB – NetBIOS |
|  |
| **Unit:4** | **System and Network Vulnerability** | **18--hours** |
| Metasploit – Penetration testing with framework Metasploit – Scan services to identify vulnerabilities – Scan FTP services – Scan HTTP services – Exploitation – PostExploitation techniques–Meterpreter–Rootkit–Backdoor–Password Hashes–Privilege Escalation - Nessus – Installation – Configuration – Importing Scanning Module – Scanning Vulnerable Service with Nessus |



|  |  |  |
| --- | --- | --- |
| **Unit:5** | **Software Vulnerability (OWASP 10)** | **18--hours** |
| Fundamentals of OWASP Zed Attack Proxy (ZAP) – Installation – Configuration – Scanning HTTP / HTTPS Packets – Walkthrough of OWASP ZAP Tool – Burp Suite – Maltego – Sn1per – WPScan |
|  |
| **Unit:6** | **Contemporary Issues** | **2 hours** |
| Seminar, Workshop, Training andWebinars |
|  |
| **Text Book(s)** |
| 1 | McClure, S., Scambray, J. and Kurtz, G., 2012. Hacking Exposed 7Network Security Secrets and Solutions. New York: McGraw-Hill. |
| 2 | Engebretson, P., 2013. The Basics Of Hacking And Penetration Testing. Amsterdam: Syngress, an imprint of Elsevier. |
| **Reference Books : EBooks** |
| 1 | Zaid Sabih, Learn Ethical Hacking from Scratch, 2018, PACKT publishing, ISBN: 978-1-78862-205-9 |
| 2 | Harsh Bothra, Hacking be a hacker with ethics, Khanna Publishing, 2016, ISBN: 978-03-86173-05-8 |
| **Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]** |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Course Title** | **Duration** | **Provider** |
| 1. | Ethical Hacker (Free) | 6 hours | Alison |
| 2. | The Complete Ethical Hacking Course Bundle | 22 hours | StationX |
| 3. | Learn Ethical Hacking From Scratch | 14 hours | Udemy |
| 4. | The Complete Cyber Security and Hacking Course | 5 Weeks | EH Academy |
| 5. | Introduction to Ethical Hacking and Cyber Security (Free) | 5 hours | Udemy |
| 6. | The Art of Exploitation (Free) | 3 hours | Cybrary |
| **Web link** |  |  |
| 1. <https://www.guru99.com/what-is-hacking-an-introduction.html>
2. <https://www.besanttechnologies.com/ethical-hacking-tutorial>
3. <https://www.edureka.co/blog/ethical-hacking-tutorial/>
4. <https://www.hackingtutorials.org/>
 |
| Course Designed by: Prof. T. Devi and CSCC Labs |

|  |
| --- |
| **Mapping with Programme Outcomes** |
| **COs** | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** | **PO8** | **PO9** | **PO10** |
| **CO1** | S | L | M | L | L | L | L | L | L | L |
| **CO3** | L | L | L | L | S | M | L | L | L | L |
| **CO3** | L | S | M | L | L | L | L | S | L | L |
| **CO4** | L | L | L | L | L | L | L | L | L | M |
| **CO5** | L | L | L | L | L | L | L | M | S | S |

\*S-Strong; M-Medium; L-Low



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Course****code** | **21CSESC04** |  **PYTHON & SHELL PROGRAMMING** | **L** | **T** | **P** | **C** |
| **Core/Elective/Supportive** | **Core** | **2** |  | **2** | **4** |
| **Pre-requisite** | **Understanding of Programming Concepts** | **Syllabus Version** | **2022-****2023** |
| **Course Objectives:** |
| The main objectives of this course are:1. To understand the basics of Python and Ethical Hacking fromScratch.
2. To strengthen fundamental skills in NetworkCommunication.
 |
|  |
| **Expected Course Outcomes:** |
| On the successful completion of the course, student will be able to: |
| 1 | To describe the environment setup and program basics. | K1 |
| 2 | To understand the Python data structures and data types. | K2 |
| 3 | To demonstrate modular programming and to explain network concepts | K1/K3 |
| 4 | To design working environment of virtual environment and understandvarious library in python | K3/K4 |
| 5 | To understand testing methods and analyze the use cases with suitabletechniques. | K5/K6 |
| **K1**–Apply; **K2** - Understand; **K3** - Setup; **K4** - Analyze; **K5** - Evaluate; **K6** – Create |
|  |
| **Unit:1** | **Python – An Overview** | **15 hours** |
| Python – Introduction – History of Python – Python Features - Python Interpreter – Installation and Setup: Windows – Linux – macOS – Installing/Updating Python Packages - Essential Python Libraries - Basic Data Types – Python Built-in Functions – IDEs – Text Editors –IPython – Jupyter Notebook - Importing and Exporting Files: CSV File – JSON File – txt File- Excel File – Xml File – DelimitedFormats – GitHub - Environment Setup - Lifecycle - Create Operation - Perform Changes - Review Changes - Commit Changes - Push, update , stash, move , rename ,delete , tag Operations -Managing Branches - Online Repositories |
| **Unit:2** | **Python Data Structure** | **20 hours** |
| Data Structures: Introduction – NumPy Package - Python List: Introduction – Accessing values– List Manipulation – List Operations - Python Tuples: Creating Tuples - Operation in Tuples – Accessing and Functions in Tuples – Python Dictionary: Accessing – Functions in Dictionary – Functions – Namespaces - Indexing – Slicing – Matrices – Arrays Functions – Exception Handling -Global and Local Variables. |
| **Unit:3** | **Modular Programming** | **15 hours** |
| Modular Programming - TCP Server- Client – UDP Server- Client – HTTP Server- Retrieving hostname IP – Banner grabbing - Socket Server Framework – Scapy: Syn Flood attack Scapy – Ping Sweep – Sniffing with Scapy – Buffer Overflow – exploit writing. |
| **Unit:4** | **Python Environment Setup** | **20 hours** |
| **Python Environment Setup** - Introduction –Virtual Environment - Setting Up Virtual Box – Setting Up VMWare –Kali Linux Installation - Installation Visual Studio Code – IRC Client Installation.**Networking Setup:** Introduction – Basic Socket Library – Urllib Library: Access URL Resources/Download Files – ftplib Library: Develop an FTP Client - smtplib Library:SMTP Client - Paramiko Library: Interactive SSH Shell |



|  |  |  |
| --- | --- | --- |
| **Unit:5** | **Penetration Testing** | **20 hours** |
| Penetration Test Introduction – Categories – Pentesting Process – Use Cases:Developing Ethical Hacking Tools: Automating Information Gathering – Keylogger – Bruteforcing ZIP Passwords. |
| **Unit:6** | **Contemporary Issues** |  **2Hours** |
| **Write an Assignment on any of the following:**1. Create a Cyber Security tool using Python or bash code .
2. Use Google Colabs and Develop a Bash tool.
 |
|  | **Total Lecture hours** | **92hours** |
| **Text Book(s)** |
| **References** |
| 1 | Wesley J. Chun, “Core Python Programming”, 2nd Edition, Pearson Education. |
| 2 | Andrew S. Tanenbaum, “Computer Networks”, PHI, Fourth Edition, 2003 |
| 3 | Mark Summerfield, “Programming in Python”, Pearson Education. |
| 4 | Behrouz A. Forouzan, “Data communication and Networking”, Tata McGraw-Hill, 2004. |
|  |
| **Reference Books** |
| 1 | Fred L. Drake, Guido Van Russom, “An Introduction to Python”, Network Theory Limited. |
| 2 | William Stallings, “Data and Computer Communication”, Sixth Edition, Pearson Education,2000 |
| 3 | TeerawatUssaruyakul, Ekram Hossain, Introduction to Network Simulator NS2, Springer, 2009 |
| 4 | Magnus Lie Hetland, “Beginning Python: From Novice to Professional”, 2nd Edition. |
| **Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]** |
|  | [www.onlinecourses.swayam2.ac.in](http://www.onlinecourses.swayam2.ac.in/) [Introduction to Cyber Security – Uttarakhand OpenUniversity, Haldwani] – 12 weeks |
|  | [www.coursera.com](http://www.coursera.com/) [Penetration Testing, INCIDENT Response and Forensics] – 4 weeks |
|  | [www.coursera.com](http://www.coursera.com/) [Python for Everybody] – 17 weeks |
| **Web Link**1. [http://python.org](http://python.org/)
2. <https://www.computer-pdf.com/programming/802-tutorial-python-tuturial.html>
3. htt[ps://www.pdfdrive.c](http://www.pdfdrive.com/penetration-testing-a-hands-on-introduction-to-hacking)o[m/penetration-testing-a-hands-on-introduction-to-hacking](http://www.pdfdrive.com/penetration-testing-a-hands-on-introduction-to-hacking)
 |
| Course Designed By: Dr. V. Bhuvaneswari |

|  |
| --- |
| **Mapping with Programme Outcomes** |
| **COs** | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** | **PO8** | **PO9** | **PO1 0** |
| **CO1** | L | L | L | L | L | L | M | L | L | M |
| **CO2** | L | L | L | L | L | L | M | L | L | M |
| **CO3** | S | M | M | S | L | L | S | L | M | S |
| **CO4** | S | M | M | S | L | L | S | L | M | S |
| **CO5** | M | M | L | S | L | L | S | L | L | S |

\*S-Strong; M-Medium; L-Low

.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Course****code** | **21CSESC05** |  **OPERATING SYSTEMS** | **L** | **T** | **P** | **C** |
| **Core/Elective/Supportive** | **Core** | **2** |  | **2** | **4** |
| **Pre-requisite** | Fundamentals of operating systems | **Syllabus Version** | **2022-****2023** |
| **Course Objectives:** |
| The main objectives of this course are to:1. To impart knowledge to make the students
2. 1. To understand the operating system overview.
3. 2. To understandthe different types of operating systems, servers, DNS and administrative tools.
4. 3. To learn using case studies in different OS.
 |
|  |
| **Expected Course Outcomes:** |
| On the successful completion of the course, student will be able to: |
| 1 | Develop knowledge in basics of the operating system overview | K2 |
| 2 |  Develop knowledge in different types of operating systems, servers, DNS and administrative tools. | K2 |
| 3 | Develop a vast knowledge in Linux ,windows and Mobile Operating Systems | K3 |
| 4 | Improve skills in Android for further Application development  | K3 |
| 5 | Practice technical programming, cracking code, simple logic and concepts | K1/K4 |
| **K1** - Remember; **K2** - Understand; **K3** - Apply; **K4** - Analyze; **K5** - Evaluate; **K6**– Create |
|  |
| **Unit:1** |  **Introduction to Operating System.** | **12 hours** |
| Basics of Operating Systems: Process Management: Process Scheduling and Operations; Interprocess Communication,CPU Scheduling, Deadlock, Memory Management,Storage Management, File and Input/Output Systems |
|  |
| **Unit:2** |  **Windows Os** | **12 hours** |
| Windows Operating Systems: Design Principles, System Components, Terminal Services and Fast User Switching; File System, NetworkingWindows-Hardware Basics, Operating System overview and Windows,Windows 7 Essential, ClientOS-Windows 7-Users and Groups-IP Configuration, Client OS-Windows 7Tools and Utilities-ClientOS Windows 7- Installation-Features-Disk Management-File Systems. |
|  |
| **Unit:3** | **Linux Operating Systems:** | **14 hours** |
| Linux Operating Systems: Design Principles, Kernel Modules, Process Management, Scheduling, Memory Management, File Systems, Input and Output; Interprocess Communication, Network Structure. |
|  |
| **Unit:4** |  **Mobile Operating Systems:** | **12 hours** |
| Introduction to Mobile Applications: Native and web applications - Mobile OS and Databases. Introduction to Android: History - Features – OSS – OHA - Versions - Android devices - Setting up software – IDE - XML. Introduction to Objective C and iOS – iOS features –user interface - Using Wifi – iPhone marketplace. |
|  |



|  |  |  |
| --- | --- | --- |
| **Unit:5** | **Real Time Operating Systems** | **10 hours** |
| Introduction – Applications of Real Time Systems – Basic Model of Real Time System – Characteristics – Safety and Reliability - Real Time Task Scheduling |
|  |
| **Unit:6** | **Contemporary Issues** | **2 hours** |
| Write a deatiled assignment on the following:1. All the Os Versions of windows
2. All the Os Versions of Linux
3. All the Versions of Android & IOS
 |
|  |
|  | **Total Lecture hours** | **62 hours** |
| **Text Book(s)** |
| 1 | 1. Barry Burd, “Android Application Development – All-in-one for Dummies”, 2ndEdition, Wiley India, 2016. |
| 2 | Operating System Conceptsby Abraham Silberschatz, Peter Baer Galvin, Greg Gagne |
|  |
| **Reference Books** |
| 1 | “Operating Systems: Internals and Design Principles” by William Stallings |
|  |
| **Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]** |
| 1 | <https://www.coursera.org/courses?languages=en&query=operating+system> |
| 2 | <https://www.udacity.com/course/advanced-operating-systems--ud189> |
| **Web Links** |
| 1 | <https://www.tutorialspoint.com/operating_system/index.html> |
| Course Designed By:Dr. M. Punithavalli |

|  |
| --- |
| **Mapping with Programme Outcomes** |
| **COs** | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** | **PO8** | **PO9** | **PO10** |
| **CO1** | L | M | L | S | S | S | S | M | M | L |
| **CO2** | L | M | L | S | S | S | S | M | M | M |
| **CO3** | M | M | M | M | L | M | M | L | S | L |
| **CO4** | S | L | M | L | L | M | M | L | L | L |
| **CO5** | S | L | M | L | L | M | M | L | L | L |

\*S-Strong; M-Medium; L-Low



Second Semester



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Course code** | **21CSESC06** | **SECURE SOFTWARE DESIGN AND ANALYSIS** | **L** | **T** | **P** | **C** |
|  | **Core/Elective/Supportive** | **Core** | **4** |  |  | **4** |
|  | **Pre-requisite** | **Basic Coding Knowledge, Security Concepts, SDLC Process** | **Syllabu s****Version** | **2022-****2023** |
|  | **Course Objectives:** |
|  | The main objectives of this course are to:1. To understand the fundamentals of security requirement, architecture andprinciples
2. To understand the threats and issues insecurity
3. To understand the secure coding, testing anddeployment
 |
|  |  |
|  | **Expected Course Outcomes:** |
|  | On the successful completion of the course, student will be able to: |
|  | 1 | Could understand the security principles | K2 |
|  | 2 | Can analyze the problems with secure coding and testing | K4 |
|  | 3 | Could apply the secure techniques in coding and testing | K3 |
|  | 4 | Understand the security violations thatcompromisessecure software implementation | K2 |
|  | 5 | Could apply the secure techniques in secure software deployment | K3 |
|  | **K1** - Remember; **K2** - Understand; **K3** - Apply; **K4** - Analyze; **K5** - Evaluate; **K6** – Create |
|  |  |
|  | **Unit:1** | **Need of Secure Software** | **12hours** |
|  | The Need for Secure Systems, Security Requirements, The Proactive Security DevelopmentProcess, Security Principles: SD3 - Secure by Design, by Default, and in Deployment. |
|  |  |
|  | **Unit:2** | **Secure Design and Secure Architecture** | **12hours** |
|  | The security development Life Cycle Process, Comparing the secure software Life cycleModels, Adaptation of secure software lifecycle, assessing the secure development lifecycle. |
|  |  |
|  | **Unit:3** | **Threat Modeling** | **12 hours** |
|  | Secure Design Through Threat Modeling, Security Techniques- Authentication, Authorization, Tamper-Resistant and Privacy-Enhanced Technologies, Encryption, Hashes, MACs, and Digital Signatures, Auditing, Filtering, Throttling, andQuality of Service,Protecting Against Denial of Service Attacks. |
|  |  |
|  | **Unit:4** | **Secure Coding** | **14 hours** |
|  | The Buffer Overrun, Determining Appropriate Access Control, Running with Least Privilege, Cryptographic Foibles, Protecting Secret Data. Issues in secure coding: Canonical Representation Issues, Database Input Issues, Web-Specific Input Issues andInternationalization Issues. Security Issues in Documentation and Security Issues in Error Messages. |
|  |  |



|  |  |  |  |
| --- | --- | --- | --- |
|  | **Unit:5** | **Security Testing and Test Plans** | **10 hours** |
|  | Security Testing - The Role of the Security Tester, Security Testing Is Different, Building Security Test Plans from a Threat Model, Testing Clients with Rogue Servers, Testing withSecurity Templates, Test the End-to-End Solution, Determining Attack Surface. Secure Deployment: Secure Software Installation. Case Study: Socket Security. |
|  |  |
|  | **Unit:6** | **Contemporary Issues** | **2 hours** |
|  | Challenges in Secure Web Applications, Application of Penetration Testing in Software. |
|  |  |
|  |  | **Total Lecture hours** | **62 hours** |
| **Text Book(s)** |
| 1 | [Michael Howard,](https://www.google.co.in/search?tbo=p&tbm=bks&q=inauthor%3A%22Michael%2BHoward%22&source=gbs_metadata_r&cad=6)[Steve Lipner](https://www.google.co.in/search?tbo=p&tbm=bks&q=inauthor%3A%22Steve%2BLipner%22&source=gbs_metadata_r&cad=6), “The Security Development Lifecycle: SDL, a Process forDeveloping Demonstrably More Secure Software”, Microsoft Press, 2006 |
| 2 | [Michael Howard,](https://www.google.co.in/search?tbo=p&tbm=bks&q=inauthor%3A%22Michael%2BHoward%22&source=gbs_metadata_r&cad=6)[David LeBlanc,](https://www.google.co.in/search?tbo=p&tbm=bks&q=inauthor%3A%22David%2BLeBlanc%22&source=gbs_metadata_r&cad=6) “Writing Secure Code”, Microsoft Press, 2002 |
| **Reference Books : EBooks** |
| 1 | [https://www.cybok.org/media/downloads/Secure\_Software\_Lifecycle\_KA\_-](https://www.cybok.org/media/downloads/Secure_Software_Lifecycle_KA_-_draft_for_review_April_2019.pdf)[\_draft\_for\_review\_April\_2019.pdf](https://www.cybok.org/media/downloads/Secure_Software_Lifecycle_KA_-_draft_for_review_April_2019.pdf) |
| 2 | [https://safecode.org/wp-](https://safecode.org/wp-content/uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf)[content/uploads/2018/03/SAFECode\_Fundamental\_Practices\_for\_Secure\_Software\_Development\_March\_2018.pdf](https://safecode.org/wp-content/uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf) |
| 3 | <https://www.csiac.org/wp-content/uploads/2016/02/stn8_2.pdf> |
| **Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]** |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Course Title** | **Duration** | **Provider** |
| 1 | Foundations of Cyber security | 8 weeks | Coursera |
| 2 | Fundamentals of Computer Network SecuritySpecialization ( 4- Courses) |  | Coursera |
| **Web link** |  |  |
| 1. <https://www.ptsecurity.com/ww-en/analytics/knowledge-base/how-to-approach-secure-software-development/>
2. <https://www.synopsys.com/blogs/software-security/secure-sdlc/>
 |
| Course Designed by: Dr.M. Punithavalli and CSSC Labs |

|  |
| --- |
| **Mapping with Programme Outcomes** |
| **COs** | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** | **PO8** | **PO9** | **PO10** |
| **CO1** | L | S | L | L | M | M | M | S | S | S |
| **CO2** | M | M | S | S | S | M | M | M | M | S |
| **CO3** | M | M | S | S | L | M | L | M | M | S |
| **CO4** | M | M | S | S | L | M | L | M | M | S |
| **CO5** | M | M | S | S | L | L | M | L | L | S |

\*S-Strong; M-Medium; L-Low



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Course code** | **21CSESC07** | **DIGITAL FORENSICS & BEST PRACTICES** | **L** | **T** | **P** | **C** |
| **Core/Elective/Supportive** | **Core** | **4** |  |  | **4** |
| **Pre-requisite** | **Operating Systems and Computer Networks** | **Syllabus Version** | **2022-****2023** |
| **Course Objectives:** |
| The main objectives of this course are to:1. To understand the concepts and vocabulary of digital forensics and understand how computers create and store digital information is a perquisite for the study of digitalforensics.
2. To understand what tools exist for use when performing Digital Forensics and howthe digital evidence is handled will play a major role in getting that evidence admitted intocourt.
3. To understand the system artifacts and anti forensicsconcepts.
4. To understand the legal aspect of digitalforensics.
5. To understand the network and mobile deviceforensics.
 |
|  |
| **Expected Course Outcomes:** |
| On the successful completion of the course, student will be able to: |
| 1 | Understand the concepts and vocabulary of digital forensics. | K2 |
| 2 | Understand what tools exist for use when performing Digital Forensics and How the digital evidence is handled will play a major role in getting thatevidence admitted into court. | K2, K4 |
| 3 | Understand the system artifacts and anti forensics concepts | K2 |
| 4 | Examines the reasonable expectations of privacy, private searches, searchingwith and without a warrant. | K2 |
| 5 | To understand the network and mobile device forensics. | K2 |
| **K1** - Remember; **K2** - Understand; **K3** - Apply; **K4** - Analyze; **K5** - Evaluate; **K6** – Create |
|  |
| **Unit:1** | **Digital Forensics** | **12hours** |
| Introduction – Uses of Digital Forensics – Organizations of Note – Locard‟s Exchange Principles – Scientific Method. Key Technical Concepts: Bits, Bytes and Numbering Schemes – File Extensions and File Signatures – Storage and Memory – Computing Environments – DataTypes – File Types – Allocated and Unallocated Space. |
|  |
| **Unit:2** | **Evidence Collection, Labs and Tools** | **12hours** |
| Labs and Tools:Introduction – Forensic Laboratories - Policies and Procedures – Quality Assurance – Digital Forensic Tools – Accreditation. Collecting Evidence: Crime Scenes And Collecting Evidence - Documenting The Scene - Chain Of Custody – Cloning – Live SystemVersus Dead System – Hashing – Final Report. |
|  |
| **Unit:3** | **System Artifacts, Anti Forensics** | **12hours** |
| System Artifacts:Deleted Data - Hibernation File – Registry – Print Spooling Recycle Bin – Metadata - Restore Points And Shadow Copy –Link Files.Anti Forensics:Introduction – HidingData – Password Attacks – Data Destruction. |
| **Unit:4** | **Legal Aspect, Internet and E-Mail** | **12hours** |
| Legal Aspect: Criminal Law-Searches Without a Warrant – Search with a Warrant – ElectronicDiscovery – Internet and E-mail: Internet Overview – Web Browsers – EMail – Social Networking Sites. |



|  |  |  |
| --- | --- | --- |
| I | Digital Forensic | 16 Weeks |
| II | Introduction of Forensic Science Services &Police Organization | 8 Weeks |

|  |  |  |
| --- | --- | --- |
| **Unit:5** | **Network and Device Forensics** | **12hours** |
| Network Fundamentals – Network Security Tools – Network Fundamentals – Incident Responses– Network Evidence and Investigations – Mobile Cellular Networks – Operating Systems – Cell Phone Evidence - Cell Phone forensic tools - Global Positioning Systems. Challenges and Concerns**:** Standards And Controls - Cloud Forensics - Solid State Drives. |
| **Unit:6** | **Contemporary Issues** | **2 hours** |
| Write an assignment on any one of the following:1. Legal and privacy issues in computerforensics
2. Open and Proprietary tools for DigitalForensics
 |
|  | **Total Lecture hours** | **62hours** |
| **Text Book(s)** |
| 1 | John Sammons, “The Basics of Digital Forensics, The Primer for Getting Started in DigitalForensics”, Syngress, 2012. |
| 2 | Tony Sammes, Brian Jenkinson, “Forensic Computing”, Second edition, Springer, 2007. |
|  |
| **Reference Books** |
| 1 | Cory Altheide and Harlan Carvey, “Digital Forensics with Open Source Tools”, Elsevier,2011. |
| 2 | Bill Nelson, Amelia Philips, Chris Steuart, “Guide to Computer Forensics andInvestigations”, 5th Edition, CENGAGE Learning, 2015. |
| **Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]** |
|  | https://onlinecourses.swayam2.ac.in (2 courses) - University of Illinois] |
|  | htt[ps://www.classc](http://www.classcentral.com/course/edx-computer-forensics-7857)e[ntral.com/course/edx-computer-forensics-7857](http://www.classcentral.com/course/edx-computer-forensics-7857) [Computer Forensics] |
| **Web Link**1. <https://www.guru99.com/digital-forensics.html>
2. <https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html>
 |
| Course Designed By: Dr. S. Gavaskar and CSSC Labs |

|  |
| --- |
| **Mapping with Programme Outcomes** |
| **Cos** | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** | **PO8** | **PO9** | **PO1****0** |
| **CO1** | S | S | M | L | L | M | L | M | S | L |
| **CO2** | S | S | M | L | M | M | L | S | S | L |
| **CO3** | S | S | M | L | L | M | L | M | S | L |
| **CO4** | S | S | M | L | L | M | L | M | S | L |
| **CO5** | S | S | M | L | L | M | L | M | S | L |

\*S-Strong; M-Medium; L-Low



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Course code** | **21CSESC08** | **Mobile and IoT** | **L** | **T** | **P** | **C** |
| **Core/Elective/Supportive** | **Core** | **2** | **0** | **2** | **4** |
| **Pre-requisite** | **Computer Networks, GITHUB and****OWASP Concepts** | **Syllabus Version** | **2022-****2023** |
| **Course Objectives:** |
| The main objectives of this course are to:1. To understand the basics of mobile computing, Principles andTechniques.
2. To discuss the Introduction of IoT, Architecture and ParticipatorySensing.
3. To understand the basics of mobile securitytechniques
 |
|  |
| **Expected Course Outcomes:** |
| On the successful completion of the course, student will be able to: |
| 1 | Learn basics of mobile computing principles and techniques | K1,K2 |
| 2 | Understand middleware and proposed applications | K2 |
| 3 | Explain the IoT Standard and Reference Architecture. | K2,K4 |
| 4 | Illustrate the mobile security and prevention techniques | K1,K4 |
| 5 | Explain Commercial Building Automation and Demonstrate simplebuilding automation | K2,K3,K6 |
| **K1** - Remember; **K2** - Understand; **K3** - Apply; **K4** - Analyze; **K5** - Evaluate; **K6** – Create |
|  |
| **Unit:1** | **Introduction to Mobile Computing** | **18 hours** |
| Mobile Computing: Introduction – Adaptability – Mechanisms for Adaptation – Develop or Incorporate Adaptations – Support for Building Adaptive Mobile Applications. Mobility Management: Location Management Principles and Techniques. Data Dissemination and Management: Challenges - Data Dissemination - Data Caching - Cache maintenance Schemes -Web Caching. |
|  |
| **Unit:2** | **Mobile middleware and Networking Challenges** | **18 hours** |
| Mobile Middleware: Introduction - Adaptation - Agents - Service Discovery. Ad Hoc and Sensor Networks: Properties of an Ad Hoc Network - Unique Features of Sensor Networks - Proposed Applications. Challenges: Constrained Resources - Security - Mobility. Approaches and Solutions: Deployment and Configuration - Routing - Fault Tolerance and Reliability -Energy Efficiency. |
|  |
| **Unit:3** | **Mobile and IoT** | **18 hours** |
| Introduction - From M2M to IoT - M2M towards IoT the global context. An Architectural Overview: Building an Architecture - Main design Principles and Needed Capabilities - An IoT Architecture Outline. Standards Considerations. IoT Architecture: Introduction - State of theArt. |
| **Unit:4** | **IoT Reference Architecture Views** | **18 hours** |
| IoT Reference Architecture: Introduction - Functional View - Information View - Deployment and Operational View - Other Relevant Architectural Views. Participatory Sensing: Introduction- Roles, Actors, Engagement - Participatory Sensing Process - Technology Overview - An early Scenario - Recent Trends - A modern Example. |
|  |

|  |  |  |
| --- | --- | --- |
| **Unit:5** | **Mobile communication and Security** | **18 hours** |
| Mobile Security: Overview of Mobile Communication: Introduction - Basics of Mobile Communications - Wireless Vulnerabilities and Threats - Attacks in Mobile Environments -Mobile Malware - Prevention Techniques in Mobile Systems - Intrusion Detection in Wireless Communications. |
|  |
| **Unit:6** | **Contemporary Issues** | **2 hours** |
| Study: Commercial Building Automation: Phase one - Phase Two. |
|  |
|  | **Total Lecture hours** | **92 hours** |
| **Text Book(s)** |
| 1 | Fundamentals of Mobile and Pervasive Computing, Golden G. Richard III, FrankAdelstein, Sandeep K. S. Gupta, Loren Schweibert, McGraw-Hill 2005 |
| 2 | . From Machine-to-Machine to the Internet of Things: Introduction to New Age ofIntelligence, Jan Ho¨ller, VlasiosTsiatsis, Catherine Mulligan, StamatisKarnouskos, Stefan Avesand, David Boyle, Elsevier,2014 |
| 3 | Security Of Mobile Communication, NoureddineBoudriga, CRC Press, 2010 |
|  |
| **Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]** |
| 1 | <https://onlinecourses.nptel.ac.in/noc20_cs21/preview> |
| 2 | <https://nptel.ac.in/courses/106/105/106105166/> |
| 3 | <https://www.coursera.org/learn/security-awareness-training> |
| Web Link1. <https://us.norton.com/internetsecurity-iot-securing-the-internet-of-things.html>
2. <https://www.allot.com/service-providers/iot-security-solutions/>
 |
| Course Designed By: Mr. S.Palanisamy& CSCC Labs |

|  |
| --- |
| **Mapping with Programme Outcomes** |
| **Cos** | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** | **PO8** | **PO9** | **PO10** |
| **CO1** | S | S | M | S | L | M | S | M | M | S |
| **CO2** | S | M | M | M | L | M | S | M | M | S |
| **CO3** | S | M | M | M | S | M | S | M | M | S |
| **CO4** | S | S | S | S | S | M | S | M | S | S |
| **CO5** | S | S | S | S | S | S | S | S | S | S |
| **CO6** | S | S | S | S | S | S | S | S | S | S |

\*S-Strong; M-Medium; L-Low



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Course code** | **21CSESC09** | **ADVANCED ETHICAL HACKING AND PENETRATION TESTING** | **L** | **T** | **P** | **C** |
| **Core/Elective/Supportive** | **Core** | **4** | **2** | **2** | **4** |
| **Pre-requisite** | **Computer Networks, OWASP****Concepts, and Wireless Standards** | **Syllabus****Version** | **2022-2023** |
| **Course Objectives:** |
| The main objectives of this course are to:1. To understand the basics of penetration tools andmethodologies
2. Acquired knowledge in analyzing the vulnerabilities and attacks ofsystem
3. To get familiar on the process of phishingattacks
 |
|  |
| **Expected Course Outcomes:** |
| On the successful completion of the course, student will be able to: |
| 1 | Understand and find out the vulnerabilities and the weakness of system using penetration testing | K1, K2 |
| 2 | Understand the basic scripting for connecting to a port for scanning thenetwork and host. | K6 |
| 3 | Analyze and scan the vulnerabilities with wireless attacks andconnection process | K4 |
| 4 | Understand the process of phishing attacks and the security levels | K2-K4 |
| 5 | Understand and Evaluate the web application vulnerabilities and thetesting with SQL Injection. | K4-K5K6 |
| **K1** - Remember; **K2** - Understand; **K3** - Apply; **K4** - Analyze; **K5** - Evaluate; **K6** –Create |
|  |
| **Unit:1** | **Introduction to Penetration Testing** | **18—hours** |
| Introduction – Preparation and Creating a Penetration Testing Lab – The use and creation of hacking lab – Setting up Virtual Lab – Using Kali Linux – Programming – Using the Metasploit framework – Phases of Penetration testReconnaissance – Scanning – Exploitation – Maintaining Access – Web based Exploitation – Maintaining Access withbackdoors and rootkits. |
|  |
| **Unit:2** | **Information Gathering and Vulnerabilities** | **18—hours** |
| Netcraft – WhoisLookUp – DNS Reconnaissance – Searching for Email Addresses - Maltego. **Host and Network Scanning:** Manual port scanning – Port scanning with Nmap. Nessus policies – Exporting Nessus results – Researching Vulnerabilities –TheNmap Scripting Engines – Metasploit Scanner Modules. |
|  |
| **Unit:3** | **Wires and Wireless Attacks** | **18—hours** |
| Exploitation – Metasploit payloads – Reverse TCP -Injecting Malware into original file – attacking outside network using port forwarding – Post exploitation techniques – Server Side Attack – Defending against malware - Running a script on the target web server – Password attacks – Client side exploitation – HTTP and HTTPS Payloads – Wireless attacks: Viewing and scanning for available access points – Capturing packets – Wired equivalent privacy – WiFi Protected access – WPA2 – The Enterprise Connection Process– The personal connection process – WiFi protected setup. |
|  |
| **Unit:4** | **Social Engineering** | **18—hours** |
| The Social Engineering toolkit – Spear Phishing attacks – choosing a payload – creating atemplate – single or mass mail – setting up target and listener – web attacks – Mass email attacks – Multipronged attacks |



|  |
| --- |
|  |
| **Unit:5** | **Web Application Vulnerabilities** | **18—hours** |
|  Generate VAPT Report .Bug Reporting Procedure - Responsible Disclosure Form- Vulnerability Labs – PortSwigger- TryHackme – Hackerone – BugCrowd – Hack the Box |
|  |
| **Unit:6** | **Contemporary Issues** | **2 hours** |
| The stage of risk, Data Asset, Affect the confidentiality, Integrity – Destruction – Disclosure– Modification – Corruption of Data – Viruses and Malwares – Cyber Attacks – Misconfiguration – Risk Assessment- Darkweb - Deep web - Surface Web – TOR |
|  |
|  | **Total Lecture hours** | **92—hours** |

|  |
| --- |
| **Text Book(s)** |
| 1 | DafyddStuttard, Marcus Pinto, “The Web Application Hacker‟s Handbook” Findingand Exploiting Security Flaws, Second edition, Wiley Publishing, Inc.,2011 |
| 2 | Georgia Weidman, “Penetration Testing”, A Hands-On Introduction to Hacking, 2014. |
| **Reference Books : EBooks** |
| 1 | Patrick Engenretson, “The Basics of Hacking Penetration Testing” Ethical Hacking and Penetration Testing Made Easy, Second Edition, Syngress, 2013. |
| 2 | Stuart McClure, Joel Scambray, George Kurtz, “Hacking Exposed 7: Network Security Secrets and Solutions,2012. |
| **Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]** |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Course Title** | **Duration** | **Provider** |
| 1. | Advanced Ethical Hacking | 6 hours | Udemy |
| 2. | Penetration Testing and Ethical Hacking(Free) | 23 hours | Cybrary |
| 3. | Ethical Hacking | 12 Weeks | SWAYAM |
| 4. | Hacking and Patching Certification by Universityof Colorado | 5 Weeks | Coursera |
| 5. | The complete Ethical Hacking Course | 24.5 hours | Udemy |
| 6. | Become an Ethical Hacker (Free) | 32 hours | LinkedInLearning |
| **Web link** |  |  |
| 1. <http://www.cybersecurityafrica.com/advanced-ethical-hacking.html>
2. <https://www.digital4nxgroup.com/advanced-ethical-hacking/>
3. <https://gicseh.com/blog.php>
4. <https://www.isoeh.com/exclusive-blog.html>
 |
| Course Designed by: Prof. T. Devi and CSCC Labs |

|  |
| --- |
| **Mapping with Programme Outcomes** |
| **Cos** | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** | **PO8** | **PO9** | **PO10** |
| **CO1** | M | L | S | L | L | L | L | L | L | L |
| **CO2** | L | M | S | S | L | L | L | L | L | L |
| **CO3** | L | L | S | S | M | L | L | L | L | L |
| **CO4** | L | L | L | S | S | L | L | L | L | L |
| **CO5** | L | L | L | L | L | L | S | L | L | L |

\*S-Strong; M-Medium; L-Low



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Course code** | **21CSESC10** | **Information Systems Risk Management** | **L** | **T** | **P** | **C** |
| **Core/Elective/Supportive** | **Core** | **4** |  |  | **4** |
| **Pre-requisite** | **Security Standards, Threat, Vulnerability,****Risk and Audit Frameworks** | **Syllabus****Version** | **2022-****2023** |
| **Course Objectives:** |
| The main objectives of this course are to:1. To understand the impacts of Information Systems.
2. To identify the Risk factors by using Information Security.
 |
|  |
| **Expected Course Outcomes:** |
| On the successful completion of the course, student will be able to: |
| 1 | Understand the basic knowledge in Information Systems Risk ManagementSecurity | K1 |
| 2 | Analyze your integrity & availability of information system risks. | K2 |
| 3 | Demonstrate the organization and system level securities and explain riskmanagement framework concepts | K3 |
| 4 | Understand the basic knowledge in Information Security and basicunderstanding of Hardware, Software Protocols. | K3/K6 |
| 5 | Understand the risk methods and analyse security factors and implement theuse cases with suitable techniques. | K4/K5 |
| **K1** - Understand; **K2**- Remember; **K3** – Analyze; **K4** - Apply; **K5** - Evaluate; **K6** – Create |
|  |
| **Unit:1** | **Information: An overview** | **12hours** |
| Information: An overview - Life Cycle - Who Should Use Information Risk Management - Introduction Risk – Information Risk Management Needs – Categorizing Risk – Simple Statistical calculation and Parameters - PERT Technique - Analysing and Assessing Risks - Risk Assessments - Risk Management Process - Risk Assessment Components - Key Risk Concepts - Risk Models - Risk Factors: Threats - Vulnerabilities and Predisposing Conditions – Likelihood – Impact – Risk – Aggregation - Assessment Approaches - Application ofRiskAssessments: Risk Management Hierarchy |
| **Unit:2** | **Risk Assessment** | **12hours** |
| Maintaining Risk Assessment - Information Risk Management Criteria - Risk Identification - Risk Analysis and Risk Evaluation - Risk Treatment - Risk Reporting and Presentation – Risk Monitoring and Review - Organization-Wide Risk Management Approach - Risk Management Framework- Executing RMF Tasks - Prepare Task: Organization / System Level - Categorize Task -Select Task - Implement Task - Assess Task - Authorize Task - Monitor Task - Information Security and Privacy in RMF - Requirements and Controls - Security and PrivacyPosture - Supply Chain Risk Management |
| **Unit:3** | **Information Security** | **14hours** |
| Information Security Knowledge - Brief History - SystemAdministration **-** System Administration Utilities - Operating System Structure - The command-line interface -Files and Directories -Moving around the filesystem – pwd, cd - Listing files and directories - ShellExpansions - File Management - Viewing Files- Searching for files |
| **Unit:4** | **Information Security Model** | **12hours** |
| Basic Information Security Model - Vulnerabilities, Threats and Controls - Access control and User Management - Access Control Lists - System Profiling - Encryption Controls - Identityand Access Management - Incident Analysis - Hardware and Software Controls - Policies, Standards, and Guidelines |

|  |  |  |
| --- | --- | --- |
| **Unit:5** | **Critical Thinking - Use Cases** | **10hours** |
| Critical Thinking **-** Use Cases- Google Executives sentenced to Prison over Video - Offensive Cyber Effects Operations (OCEO) - Risk Estimation Biases - Iraq cyber war plans in 2003 -Uses of a Hacked PC - Deepfake Attack in 2017 – Social Engineering Attacks in 2020 – Twitter Hack in 2020 – Zoom Credentials up for Sale in 2020 - Zero-day Attacks. |
| **Unit6: ContemporaryIssues 2 hours** |
| Write an assignment on Social network security: Issues, challenges, threats, and solution |
|  | **Total Lecture hours** | **62hours** |
| **Text Book(s)** |
| 1 | Bruce Newsome, “A Practical Introduction to Security and Risk Management”, FirstEdition, ISBN: 9781483313405, 2013 |
| 2 | David Sutton, “Information Risk Management:A practitioner'sguide”, bcsCharteredInstitute for IT, ISBN: 978-1- 78017-266-1, 2014 |
| 3 | Refsdal, Atle, Sohaug, “Cyber - Risk Management”, First Edition, Springer InternationalPublishing, ISBN: 978-3-319-23570-7, 2015 |
| 4 | Manish Agrawal, Alex Campoe, Eric Pierce, Information Security and IT Risk |
| Management, First Edition, Wiley Publisher,ISBN-13: | 978-1118335895, 2014 |
| **Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]** |
|  1 | [www.coursera.com](http://www.coursera.com/)– Information Security and Risk Management in Context – 10 weeks |
|  2  |  [www.udamey.com](http://www.udamey.com)– Risk Management for Cybersecurity and IT Managers |
| **Web Link**1. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
2. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf>
 |
| Course Designed By: Prof. M.Punithavalli and CSCC Labs |

|  |
| --- |
| **Mapping with Programme Outcomes** |
| **Cos** | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** | **PO8** | **PO9** | **PO10** |
| **CO1** | L | L | L | L | L | L | M | L | L | M |
| **CO2** | L | L | L | L | L | L | M | L | L | M |
| **CO3** | S | M | M | S | L | L | S | L | M | S |
| **CO4** | S | M | M | S | L | L | S | L | M | S |
| **CO5** | M | M | L | S | L | L | S | L | M | S |

\*S-Strong; M-Medium; L-Low



Third Semester



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Course code** | **21CSESC11** | **EVOLVING TECHNOLOGIES AND THREATS** | **L** | **T** | **P** | **C** |
|  | **Core/Elective/Supportive** | **Core** | **4** |  |  | **4** |
|  | **Pre-requisite** | **Current and Future Technology Trends** | **Syllabus Version** | **2022-****2023** |
|  | **Course Objectives:** |
|  | The main objectives of this course are to:1. To understand Web Technology, Robotics and AutonomousSystems
2. To analyze security problems associated with bigdata
3. To analyze and Build Big dataApplications
 |
|  |  |
|  | **Expected Course Outcomes:** |
|  | On the successful completion of the course, student will be able to: |
|  | 1 | Could understand the security in web technology | K2 |
|  | 2 | Can analyze the security problems associated with big data | K4 |
|  | 3 | Could apply the secure techniques in Big data Applications | K3 |
|  | 4 | Understand the security violations in Robotics | K2 |
|  | 5 | Understand the security violations in Autonomous Systems | K2 |
|  | **K1** - Remember; **K2** - Understand; **K3** - Apply; **K4** - Analyze; **K5** - Evaluate; **K6** – Create |
|  |  |
|  | **Unit:1** | **Advances in web technologies** | **12hours** |
|  | Improving Security in Web Sessions- Special Management of Cookies, Proposed mechanism for web session, management, Implementation and experiments. Leveraging Semantic Web Technologies for Access Control- Implementing RBAC with ontologies, semantically extending the XACML attribute model, Ontology-based context awareness, Ontological specification of user preferences, Semantic access control in online social networks, DEMONS ontological access controlmodel. |
|  |  |
|  | **Unit:2** | **Complex & Distributed IT infrastructure** | **12hours** |
|  | System Security Engineering for Information Systems, System security engineering history,Established system security engineering methods, processes, and tools, Modern and emerging system security engineering methods, processes, and tools – Example of New Technology : Block Chain |
|  |  |
|  | **Unit:3** | **Privacy and Identity Theft** | **12hours** |
|  | Fundamental Concepts, Definitions, Statistics, Data Privacy Attacks, Data linking and profiling, access control models, role based access control, privacy policies, their specifications, languages and implementation, privacy policy languages, privacy in different domains- medical, financial, etc Medical privacy legislation, policies and best practices, Examination of privacy matters specific to the World Wide Web, Protections provided by the Freedom of Information Act or the requirement for search warrants. |
|  |  |



|  |  |  |  |
| --- | --- | --- | --- |
|  | **Unit:4** | **Threats of Big Data** | **14hours** |
|  | An Approach to Facilitate Security Assurance for Information Sharing and Exchange in Big- Data Applications, UML extensions for XML security, Extensions for policy modeling and integration, Integrating local security policies into a global security policy, Real-time Network Intrusion Detection Using Hadoop-Based Bayesian Classifier, Overview on Hadoop based technologies, Survey of Intrusion Detection Systems, Hadoop-based real-time Intrusion Detection: System architecture, Practical application scenario and system evaluation. CSRF and Big Data: Rethinking Cross-Site Request Forgery in Light of Big - Defenses against CSRF: Server and browser Sides, Experiment results: CSRF in social media and networking sites, Analysis of test framework with popular Web/URL scanningtools. |
|  |  |
|  | **Unit:5** | **Robotics & Autonomous Systems** | **10hours** |
|  | Emerging Security Challenges in Cloud Computing, from Infrastructure-Based Security to Proposed Provisioned Cloud Infrastructure - Infrastructure security, Cloud service models, Provisioned access control infrastructure (DACI). |
|  | **Unit:6** | **Contemporary Issues** | **2 hours** |
|  |  Challenges in the development of Chabot, Discuss the issues in Autonomous System |
|  |  |
|  |  | **Total Lecture hours** | **62 hours** |
| **Text Book(s)** |
| 1 | Babak Akhgar Hamid Arabnia, “Emerging Trends in ICT Security”, Morgan Kaufmann, 2013 |
| 2 | [Divya Gupta Chowdhry,](https://www.google.co.in/search?tbo=p&tbm=bks&q=inauthor%3A%22Divya%2BGupta%2BChowdhry%22&source=gbs_metadata_r&cad=7) [Rahul Verma,](https://www.google.co.in/search?tbo=p&tbm=bks&q=inauthor%3A%22Rahul%2BVerma%22&source=gbs_metadata_r&cad=7)[Manisha Mathur,](https://www.google.co.in/search?tbo=p&tbm=bks&q=inauthor%3A%22Manisha%2BMathur%22&source=gbs_metadata_r&cad=7) “The Evolution of Business in the Cyber Age: Digital Transformation, Threats, and Security”, CRC Press, 2020 |
| 3 | Seema Acharya, SubhashniChellappan, “Big Data Analytics”, Wiley, 2015. |
| 4 | Errol Simon, “Distributed information systems from client / server to distributed multimedia“,Mcgraw-Hill, 1996 |
| 5 | Vladlena Benson John McAlaney, ” Emerging Cyber Threats and Cognitive Vulnerabilities, Academic Press,2019 |
| **Reference Books : EBooks** |
| 1 | <https://cyber-edge.com/wp-content/uploads/2019/10/RecordedFutureSecondEditioneBook.pdf> |
| 2 | <https://paper.bobylive.com/Security/threat-intelligence-handbook-second-edition.pdf> |
| **Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]** |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Course Title** | **Duration** | **Provider** |
| 1. | Big Data Fundamentals (3 – courses) Specialization | 6 weeks | IBM |
| 2. | Big Data Specialization (6 – courses) | 30 weeks | Coursera |
| 3. | Cyber Threat Intelligence (IBM) | 5 weeks | Coursera |

|  |  |  |
| --- | --- | --- |
| **Web link** |  |  |
| 1. <https://cognitiveclass.ai/learn/big-data>
2. <https://www.fireeye.com/>
3. <https://www.ibm.com/in-en/security>
4. <https://cognitiveclass.ai/courses/robots-are-coming>
 |
| Course Designed by: Dr.M. Punithavalli and CSCC Labs |

|  |
| --- |
| **Mapping with Programme Outcomes** |
| **COs** | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** | **PO8** | **PO9** | **PO10** |
| **CO1** | L | S | L | M | M | L | S | S | M | S |
| **CO2** | M | S | S | S | M | L | L | M | M | M |
| **CO3** | M | M | S | S | M | L | M | S | S | S |
| **CO4** | M | M | S | S | M | L | M | S | S | S |
| **CO5** | S | S | S | S | M | M | M | S | S | S |

\*S-Strong; M-Medium; L-Low



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Course code** | **21CSESC12** | **SECURITY STANDARDS AND COMPLIANCE** | **L** | **T** | **P** | **C** |
| **Core/Elective/Supportive** | **Core** | **4** |  |  | **4** |
| **Pre-requisite** | **Basic knowledge of Policy, Process,****Standard, Procedure and Compliance** | **Syllabus****Version** | **2022-****2023** |
| **Course Objectives:** |
| The main objectives of this course are to:1. To understand the risk management process for allorganizations.
2. To understand the security standards, compliance, security controls and accesscontrols.
3. To learn what PCI DSS is and understand how it applies to theorganizations.
4. To understand the technologies referenced by PCIDSS
5. To understand how to building and maintaining a SecureNetwork.
 |
|  |
| **Expected Course Outcomes:** |
| On the successful completion of the course, student will be able to: |
| 1 | Understand the risk management process for all organizations | K2 |
| 2 | Understand the security standards, security controls and control libraries. | K2 |
| 3 | Understand what PCI DSS is and understand how it applies to theorganizations. | K2 |
| 4 | Understand how to building and maintaining a Secure Network | K2,K3 |
| 5 | Develop a case study for organization using PCI DSS. | K3 |
| **K1** - Remember; **K2** - Understand; **K3** - Apply; **K4** - Analyze; **K5** - Evaluate; **K6** – Create |
|  |
| **Unit:1** | **Security Risk Management** | **14hours** |
| Organizational Security Risk Management: Risk is Inevitable – Strategic Governance and Risk Management – Elements of Risk Management – Risk Types and Risk Handling Strategies – Overview of the Risk Management Process. Existing Risk Management Frameworks: Standard Best Practice –Risk Management Tangible – Formal Architecture – General Shape of the RMF Process – RMF Implementation – Other Frameworks and Models for Risk Management – International Organization for Standardization – NIST SP 800-30 and NIST SP 800-39Standards. |
|  |
| **Unit:2** | **Security Controls and Control Library** | **12hours** |
| Select Security Controls: Understanding Control Selection - Federal Information Processing Standard Publication 200 – Document Collection and Relationship Building - Control Libraries:Control Objectives for Information and Related Technologies – CIS Critical Security Controls – Industrial Automation and Control Systems Security Life Cycle – ISO/IEC 27001. |
|  |
| **Unit:3** | **Payment Card Industry Data Security Standard (PCI DSS)** | **12hours** |
| PCI Introduction – Electronic Card Payment Ecosystem – Compliance Deadlines –Compliance and Validation – History of PCI DSS – PCI Council – QSAs, PFIs, PCIPs, QIRs, ASVs – PCI Requirements – PCI DSS and Risk – Benefits of Compliance – Case Study. |
| **Unit:4** | **PCO Scope and Secure Network** | **10hours** |
| Determining and Reducing the PCI Scope: Basics – Scope Reduction Tips – Planning PCI Project. Building and Maintaining a Secure Network: Establishing FirewallConfigurationStandards – Tools and Best Practices – Common Mistakes and Pitfalls – Case Study. |

|  |  |  |
| --- | --- | --- |
| **Unit:5** | **Strong Access Controls** | **12hours** |
| DMCA - Social Media Attacks and Complaint - VOIP Complaint - Reporting Form for Various Crimes - Parental Control - Mobile Security Options - Google Security – Factor Authentication – USB Authentication – Permissions – Ad Settings, ID, - App Permissions – Dashboard – Takeout. |
| **Unit:6** | **Contemporary Issues** | **2 hours** |
| Write an assignment on any one of the following:1.Report any 5 Real time bug and submit POC Document2.List some protocol OSI Layer Level Attack and its mitigation |
|  | **Total Lecture hours** | **62hours** |
| **Text Book(s)** |
| 1 | Anne Kohnke, Ken Sigler, Dan Shomaker, “Implementing Cybersecurity: A Guide to theNational Standards and Technology Risk Management Framework” CRC Press, 2017. |
| 2 | Branden R. Williams, Anton A. Chuvakin, “PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance”, Fourth Edition,Syngress,2015. |
|  |
| **Reference Books** |
| 1 | Barry L. Williams “Information Security Policy Development for Compliance: ISO/IEC 27001, NIST SP 800-53, HIPAA Standard, PCI DSS V2.0, and AUP V5.0”, CRC Press,2013 |
| **Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]** |
| 1 | [www.coursera.com](http://www.coursera.com/)[Cybersecurity Compliance Framework & System Administration] |
| **Web Link**1. https://resources.infosecinstitute.com/step-step-guide-data-security-compliance- industry/#gref
2. htt[ps://www.tutorialspoint.com/computer\_securit](http://www.tutorialspoint.com/computer_security/computer_security_legal_compliance.ht)y[/computer\_security\_legal\_compliance.ht](http://www.tutorialspoint.com/computer_security/computer_security_legal_compliance.ht)m
3. <https://www.akamai.com/uk/en/resources/security-compliance.jsp>
 |
| Course Designed By: Dr. S. Gavaskar and CSCC Labs |
|  | **Mapping with Programme Outcomes** |  |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **COs** | **P O1** | **P O2** | **P O3** | **P O4** | **P O5** | **P O6** | **P O7** | **P O8** | **P O9** | **PO 10** |
|  | **CO1** | S | S | L | L | M | L | L | S | S | L |
|  | **CO2** | S | M | L | M | M | L | S | S | S | L |
|  | **CO3** | S | M | S | S | S | S | S | S | S | S |
|  | **CO4** | S | M | S | S | M | S | S | S | S | M |
|  | **CO5** | S | S | M | S | M | S | S | S | S | M |

\*S-Strong; M-Medium; L-Low

## Course Title: Case studies of Cyber Security - Paper 1

**No. of Credits :6**

**Course Code :21CSESC13**

Every person would be doing 2 case studies with help of CSSC GSOC & Professors

## Course Title: Case studies of Cyber Security - Paper 2

**No. of Credits : 6**

**Course Code :21CSESC14**

Every person would be doing 2 case studies with help of CSSC GSOC & Professors

## Course Title: Practice School

**No. of Credits : 14**

**Course Code :21CSESC15**

Every person would be doing a Cyber Security Based Project



Elective Papers



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Course****code** | **21CSESE01** | **IT Infrastructure and Cloud Security** | **L** | **T** | **P** | **C** |
| **Core/Elective/Supportive** | **Elective** | **4** |  |  | **4** |
| **Pre-requisite** | **Cloud, Networking Basics** | **Syllabus Version** | **2022-****2023** |
| **Course Objectives:** |
| The main objectives of this course are to:1. To understand the concepts of Internet of Things
2. To learn how to use CloudServices.
3. To implementVirtualization
4. To understand complex technologies leading to the development of current and future cloud computingsecurity
 |
|  |
| **Expected Course Outcomes:** |
| On the successful completion of the course, student will be able to: |
| 1 | Understand the nature of malware, its capabilities, and how it is combatedthrough detection and classification. | K2 |
| 2 | Understand the social, economic, and historical context in which malwareoccurs. | K2 |
| 3 | Analyze malicious in windows programs. | K4 |
| 4 | Apply the tools and methodologies used to perform static and dynamic analysison unknown executable. | K3 |
| 5 | Apply techniques and concepts to unpack, extract, decrypt, or bypass new anti-analysis techniques in future malware samples. | K3 |
| **K1** - Remember; **K2** - Understand; **K3** - Apply; **K4** - Analyze; **K5** - Evaluate; **K6** – Create |
|  |
| **Unit:1** | **Introduction to Networking & Communication Protocols** | **10hours** |
| **Networking:** Introduction to Corporate Infrastructure – LAN, MAN and WAN. **Internet of Things:** Introduction – Definition Evolution – IoT Architecture – Resource Management – IoT Data Management and Analytics – Communication Protocols – Identity Management and Authentication – Privacy. Device Collaboration Framework. |
| **Fog Computing** |
| **Unit:2** |  | **14hours** |
| **Fog Computing:** Introduction – Characteristics – Reference Architecture – Applications – Research Directions and Enables – Commercial Products. **Stream Processing in IoT:** Foundation of Stream Processing in IoT – Continuous Logic Processing System – Challenges and Future Direction. |
| **Cloud Computing Influences** |
| **Unit:3** |  | **12hours** |
| **Cloud Computing**: Introduction – Characteristics – Architectural Influences – Technological Influences – Operational Influences. **Cloud Computing Architecture**: Delivery Model – Deployment Model – Benefits. Cloud SecurityServices. |
| **Unit:4** | **Virtualization & Data Center** | **12hours** |
| **Cloud, Virtualization, andDataStorage & Data Center NetworkingFundamentals:**Server and Storage I/O Fundamentals – I/O Connectivity and Networking Fundamentals – IT Clouds – Virtualization: Servers, Storage and Networking – Virtualization and Storage Services |



|  |
| --- |
| – Data and Storage Access. **Infrastructure Resource Management:** Introduction - Managing Data Infrastructure for Cloud Virtual Environments – Understanding IT Resources – Managing IT Resources |
| **Unit:5** | **Security Threats and Risks** | **12hours** |
| **Data and Storage Networking Security:** Security Threat Risks and Challenges – Securing Networks – Securing Storage – Securing Clouds. **Data Protection:** Data Protection Challenges and Opportunities – Protect, Preserve, and Serve Information Services – Virtual – Physical, and Cloud Data Protection – Modernizing and Protection and Backup. |
| **Unit:6** | **Contemporary Issues** | **2 hours** |
| Internet of Robotic Things - Cloud-enabled Robotics. |
|  | **Total Lecture hours** | **62hours** |
| **Text Book(s)** |
| 1 | Rajkumar Buyya, Amir Vahid Dastjerdi, “Internet of Things: Principles and Paradigms”,Morgan Kaufmann Publications, 2016. |
| 2 | Ronald L.Krutz, Russell Dean Vines, “Cloud Security: A Comprehensive Guide to SecureCloud Computing”, Wiley Publishing, Inc, 2010. |
|  |
| **Reference Books** |
| 1 | Fei Hu, “Security and Privacy in Internet of Things: Models, Algorithm andImplementations”, CRC Press, 2016. |
| 2 | John R.Vacca, “Cyber Security and IT Infrastructure Protection”, Syngress, 2013. |
| 3 | Chris Dotson, “Practical Cloud Security: A Guide for Secure Design and Deployment”,O‟Reilly Media Publications, 2019. |
| **Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]** |
|  | https://onlinecourses.nptel.ac.in [Two Courses] |
| 1 | Components And Applications Of Internet Of Things | 15 Weeks |  |
| 2 | Introduction to Industry 4.0 and Industrial Internet of Things. | 12 Weeks |  |
|  | <https://www.classcentral.com/course/cloud-computing-security-11754>[Cloud Computing Security] |
| **Web Link** |
| Course Designed By: Dr. S. Gavaskar & CSSC Labs |

|  |
| --- |
| **Mapping with Programme Outcomes** |
| **COs** | **P O1** | **P O2** | **P O3** | **P O4** | **P O5** | **P O6** | **P O7** | **P O8** | **P O9** | **PO 10** |
| **CO1** | M | L | L | L | L | L | L | S | L | M |
| **CO2** | L | L | L | L | L | L | L | S | L | M |
| **CO3** | S | S | S | M | S | M | M | S | S | S |
| **CO4** | S | S | M | S | M | S | S | S | M | M |
| **CO5** | M | M | M | S | M | S | S | S | M | M |

\*S-Strong; M-Medium; L-Low



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Course code** | **21CSESE02** | **MALWARE ANALYSIS** | **L** | **T** | **P** | **C** |
| **Core/Elective/Supportive** | **Elective** | **4** |  |  | **4** |
| **Pre-requisite** | **Operating System, Basics of Malware, Security Concepts and Algorithms** | **Syllabus Version** | **2022-****2023** |
| **Course Objectives:** |
| The main objectives of this course are to:1. To understand the nature of malware, its capabilities, and how it is combatedthrough detection andclassification.
2. To able apply the tools and methodologies used to perform static and dynamicanalysis on unknownexecutable.
3. To understand the social, economic, and historical context in which malwareoccurs.
4. To be able to apply techniques and concepts to unpack, extract, decrypt, or bypass new anti-analysis techniques in future malwaresamples.
 |
|  |
| **Expected Course Outcomes:** |
| On the successful completion of the course, student will be able to: |
| 1 | Understand the nature of malware, its capabilities, and how it is combatedthrough detection and classification. | K2 |
| 2 | Understand the social, economic, and historical context in which malwareoccurs. | K2 |
| 3 | Analyze malicious in windows programs. | K4 |
| 4 | Apply the tools and methodologies used to perform static and dynamic analysison unknown executable. | K3 |
| 5 | Apply techniques and concepts to unpack, extract, decrypt, or bypass new anti-analysis techniques in future malware samples. | K3 |
| **K1** - Remember; **K2** - Understand; **K3** - Apply; **K4** - Analyze; **K5** - Evaluate; **K6** – Create |
|  |
| **Unit:1** | **Malware Analysis Overview** | **12hours** |
| Introduction:Definition of Malware – Goals of .Malware Analysis– Malware Analysis Techniques - Types of Malware Analysis – General Rules for Malware Analysis. Analyzing malicious windows programs:Windows API – Windows Registry – Networking APIs – FollowingRunning Malwares – Kernel vs User Mode- Native API. |
|  |
| **Unit:2** | **Basic Analysis** | **14hours** |
| Basic Static Techniques – Antivirus Scanning – Hashing – Finding Strings – Packed and Obfuscated Malware – Portable Executable File Format – Linked Libraries and Function – Static Analysis in Practice – PE File Headers and Sections. Basic Dynamic Analysis: Quality and Dirty Approach – Running Malware – Monitoring with Process Monitor – Viewing Process with Process Explorer: The Process Explorer Display, Using the Verify Option, Comparing Strings, Using Dependency Walker, Analyzing Malicious Documents – Comparing Registry Snapshots withRegshot–FakingaNetwork–PacketSniffingwithWireshark–UsingINetSim–BasicDynamic Tools in Practice. |
|  |
| **Unit:3** | **Advanced Analysis** | **10hours** |
| x86 Architecture: Memory, instructions, opcodes, operands, registers, functions, stack. IDA ProInference – Cross Reference – Analyzing Functions – Using Graphing Options – Enhancing Disassembly – Extending IDA with Plug-ins. |



|  |  |  |
| --- | --- | --- |
| **Unit:4** | **Advanced Dynamic Analysis** | **12hours** |
| Source-Level vs Assembly Level Debuggers –Kernel vs User-Mode Debugging – Using Debugger – Exceptions – Modifying Execution with a Debugger.OllyDbg:Loading Malware – OllyDbg Interface – Memory MapViewing Threads and Stacks – Executing Code – Breakpoints –Loading DLLs – Tracing – Exception Handling – Patching – Analyzing Shellcode – Assistance Features – Plug-ins – Scriptable Debugging. Using WinDbg – Microsoft Symbols. |
| **Unit:5** | **Anti-Disassembly and Anti-Debugging** | **12hours** |
| Anti-Disassembly:Understanding Anti-Disassembly – Defeating Disassembly Algorithm – Anti- Disassembly Techniques – Obscuring Flow Control – Thwarting Stack-Frame Analysis. Anti-Debugging:Windows Debugger Detection – Identifying Debugger Behaviour – Interfering with Debugger Functionality – Debugger Vulnerabilities. Defeat Malware. |
| **Unit:6** | **Contemporary Issues** | **2 hours** |
| Write an assignment on any one of the following:1. Malware AnalysisTools
2. Malicious in WindowsPrograms.
 |
|  | **Total Lecture hours** | **62hours** |
| **Text Book(s)** |
| 1 | Michael Sikorski, Andrew Honig, “Practical Malware Analysis”, No Strach Press, 2012. |
| 2 | Michael Hale Ligh, Steven Adair, Blake Hartstein, Matthew Richard “Malware Analyst‟s Cookbook and DVD: Tools and Techniques for Fighting Malicious Code”, Wiley PublishingInc, 2011. |
| 3 | Chris Eagle, The IDA Pro Book”, 2nd Edition, No Strach Press, 2011. |
|  |
| **Reference Books** |
| 1 | Eldad Eilam, “Reversing: Secrets of Reverse Engineering”, Wiley Publishing Inc, 2005. |
| 2 | Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters, “The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory”, Wiley,2014. |
| **Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]** |
| 1 | <https://www.cybrary.it/course/malware-analysis/>[Intro to Malware Analysis and ReverseEngineering |
| 2 | htt[ps://www.elearnse](http://www.elearnsecurity.com/course/malware_analysis_professional/)c[urity.com/course/malware\_analysis\_professional/](http://www.elearnsecurity.com/course/malware_analysis_professional/) [Malware AnalysisProfessional] |
| **Web Link**1. htt[ps://www.ha](http://www.hackingtutorials.org/category/malware-analysis-tutorials/)c[kingtutorials.org/category/malware-analysis-tutorials/](http://www.hackingtutorials.org/category/malware-analysis-tutorials/)
2. https://gbhackers.com/malware-analysis-cheat-sheet-and-tools-list/
 |
| Course Designed By: Dr. S. Gavaskar and CSCC Labs |

|  |
| --- |
| **Mapping with Programme Outcomes** |
| **COs** | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** | **PO8** | **PO9** | **PO10** |
| **CO1** | M | L | L | L | L | L | L | S | L | M |
| **CO2** | L | L | L | L | L | L | L | S | L | M |
| **CO3** | S | S | S | M | S | M | M | S | S | S |
| **CO4** | S | S | M | S | M | S | S | S | M | M |
| **CO5** | M | M | M | S | M | S | S | S | M | M |

\*S-Strong; M-Medium; L-Low



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Course code** | **21CSESE03** | **INCIDENT RESPONSE** | **L** | **T** | **P** | **C** |
|  | **Core/Elective/Supportive** | **Elective** | **4** |  |  | **4** |
|  | **Pre-requisite** | **Forensics, Networks & Penetration Testing** | **Syllabus Version** | **2022-2023** |
|  | **Course Objectives:** |
|  | The main objectives of this course are to:1. To understand Incident Response Policy, Plan andProcedure.
2. To understand Incident Handling, Coordination and InformationSharing.
3. To analyze and Build methods for Data Exfiltration Detection andPrevention.
 |
|  |  |
|  | **Expected Course Outcomes:** |
|  | On the successful completion of the course, student will be able to: |
|  | 1 | Understand the Incident Response needs and structure. | K2 |
|  | 2 | Understand the Incident Handling techniques | K2 |
|  | 3 | Understand the Coordination and Information Sharing in Incident Response | K2 |
|  | 4 | Understand and analyze the scenarios in Incidence Response | K2-K4 |
|  | 5 | Analyze and Apply the Incident Response issues. | K3-K4 |
|  | **K1** - Remember; **K2** - Understand; **K3** - Apply; **K4** - Analyze; **K5** - Evaluate; **K6** – Create |
|  |  |
|  | **Unit:1** | **Introduction to Incident Response** | **12hours** |
|  | Need for Incident Response, Incident Response Policy, Plan, and Procedure Creation,Incident Response Team Structure, Incident Response Team Services. |
|  |  |
|  | **Unit:2** | **Incident Handling** | **10 hours** |
|  | Preparation, Detection and Analysis, Containment, Eradication, and Recovery, Post-IncidentActivity, Incident Handling Checklist. |
|  |  |
|  | **Unit:3** | **Coordination and Information Sharing** | **12hours** |
|  | Coordination, Information Sharing Techniques, Granular Information Sharing. |
|  |  |
|  | **Unit:4** | **Scenarios in Incidence Response** | **14hours** |
|  | Domain Name System (DNS), Server Denial of Service (DoS), Compromised Database Server, Worm and Distributed Denial of Service (DDoS) Agent Infestation, Stolen Documents, Unknown Exfiltration, Unauthorized Access to Payroll Records, Disappearing Host, Telecommuting Compromise Anonymous Threat, Peer-to-Peer File Sharing, Unknown Wireless Access Point. |
|  |  |
|  | **Unit:5** | **Incident Response Use Cases** | **12hours** |
|  | Data Exfiltration Detection and Prevention. Mitigation of Internet of Things (IoT) Threats. |
|  |  |
|  | **Unit:6** | **Contemporary Issues** | **2hours** |
|  | Issues in Dark Reading, Issues in Cyber espionage. Problems with Logic Bomb. |
|  |  |
|  |  | **Total Lecture hours** | **62hours** |

|  |
| --- |
| **Text Book(s)** |
| 1 | Paul Cichonski, Tom Millar, TimGrance, Karen Scarfone, “Computer Security Incident Handling Guide”, National Institute of Standards and Technology SpecialPublication,2012. |
| 2 | Chris Sanders and Jason Smith, “Applied Network Security Monitoring: Collection,Detection, and Analysis”, Syngress- Elsevier, 2014. |
| 3 | [Don Murdoch,](https://www.google.co.in/search?tbo=p&tbm=bks&q=inauthor%3A%22Don%2BMurdoch%22&source=gbs_metadata_r&cad=3) “Blue Team Handbook: Incident Response Edition : a Condensed Field Guide for the Cyber Security Incident Responder”, Create Space Independent Publishing,2014 |
| **Reference Books : EBooks** |
| 1 | <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> |
| 2 | Security Operations Center - Analyst Guide: SIEM Technology, Use Cases and Practicesby Arun E Thomas |
| 3 | Security Operations Center - Tools & Practices by Arun E Thomas |
| **Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]** |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Course Title** | **Duration** | **Provider** |
| 1. | Penetration Testing, Incident Response and Forensics | 4 weeks | Coursera(IBM) |
| 2. | Cyber Security Capstone: Breach Response CaseStudies | 4 weeks | Coursera(IBM) |
| **Web link** |  |  |
| 1. <https://security.ucop.edu/files/documents/policies/incident-response-standard.pdf>
2. <https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-EN.pdf>
 |
| Course Designed by: Dr.M. Punithavalli and CSCC Labs |

|  |
| --- |
| **Mapping with Programme Outcomes** |
| **COs** | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** | **PO8** | **PO9** | **PO10** |
| **CO1** | L | M | M | L | M | M | L | S | M | S |
| **CO2** | L | M | M | L | M | M | L | S | M | S |
| **CO3** | L | L | L | L | M | M | M | S | M | S |
| **CO4** | L | L | L | L | M | M | M | S | M | S |
| **CO5** | M | M | S | S | M | S | S | M | S | S |

\*S-Strong; M-Medium; L-Low



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Course code** | **21CSESE04** | **THREAT INTELLIGENCE** | **L** | **T** | **P** | **C** |
|  | **Core/Elective/Supportive** | **Elective** | **4** |  |  | **4** |
|  | **Pre-requisite** | **Information Security Assets, Attacks and Vulnerabilities** | **Syllabu s Version** | **2022-2023** |
|  | **Course Objectives:** |
|  | The main objectives of this course are to:1. To understand Threat Intelligence, Threat Intelligence types and LifeCycle.
2. To understand and apply Threat detection andprevention.
3. To analyze and build secure methods to preventthreats.
 |
|  |  |
|  | **Expected Course Outcomes:** |
|  | On the successful completion of the course, student will be able to: |
|  | 1 | Understand threats, threats, intelligence types. | K2 |
|  | 2 | Understand the stages of a threat intelligence life cycle. | K2 |
|  | 3 | Understand various types of threats and its features. | K2 |
|  | 4 | Understand, analyze and evaluate the efficiency of secure methods todetect and prevent threats. | K2-K5 |
|  | 5 | Analyze and implement the secure methods in real life scenarios. | K3-K6 |
|  | 6 | Understand and evaluate the effective detection and prevention methods. | K2, K5 |
|  | **K1** - Remember; **K2** - Understand; **K3** - Apply; **K4** - Analyze; **K5** - Evaluate; **K6** - Create |
|  |  |
|  | **Unit:1** | **Introduction to Threat Intelligence** | **12hours** |
|  | Define TI, Importance of TI, Benefits and challenges of Threat Information Sharing, Creating Cyber Threat Information. |
|  |  |
|  | **Unit:2** | **Threat Intelligence Life Cycle** | **12hours** |
|  | Phases of Life cycle, Direction, Collection, Processing, Analysis, DisseminationandFeedback. |
|  |  |
|  | **Unit:3** | **Types of Threat Intelligence** | **12hours** |
|  | Strategic Threat Intelligence, tactical Threat Intelligence, operational Threat Intelligence,and technical Threat Intelligence. |
|  |  |
|  | **Unit:4** | **Applications of Threat Intelligence** | **14hours** |
|  | Threat Intelligence for Security Operations, Threat Intelligence for Incident Response, Threat Intelligence for Vulnerability Management, Threat Intelligence for Security Leaders, Risk Analysis, Threat Intelligence for Fraud Prevention, Threat Intelligence for ReducingThird Party Risk, Threat Intelligence for Digital Risk Protection. |
|  |  |
|  | **Unit:5** | **Threat Intelligence Use cases** | **10hours** |
|  | Machine learning for better Threat Intelligence, Threat Intelligence use cases:Paymentfraud, Compromised data, Typo squatting and fraudulent domains. |
|  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Unit:6** | **Contemporary Issues** | **2 hours** |
|  | Advantages of Threat Hunting, Cyber Kill Chain, The role of private Channels and theDark web. |
|  |  |
|  |  | **Total Lecture hours** | **62hours** |
| **Text Book(s)** |
| 1 | Christopher Ahlberg, “The Threat Intelligence Handbook : Moving Toward a securityIntelligence Program, Second Edition”, CyberEdge Group, 1997 |
| 2 | [Florian Skopik](https://www.google.co.in/search?tbo=p&tbm=bks&q=inauthor%3A%22Florian%2BSkopik%22&source=gbs_metadata_r&cad=8), “Collaborative Cyber Threat Intelligence: Detecting and Responding toAdvanced Cyber Attacks at the National Level”, CRC Press, 2017 |
| 3 | Christopher Ahlberg, “The Threat Intelligence Handbook : A Practical GuideforSecurity Teams to Unlocking the Power of Intelligence”, CyberEdge Group,1997 |
| **Reference Books : EBooks** |
| 1 | https://paper.bobylive.com/Security/threat-intelligence-handbook-second-edition.pdf |
| 2 | https://cyber-edge.com/wp-content/uploads/2018/11/Recorded-Future-eBook.pdf |
| 3 | https://books.google.co.in/books?id=cyE6DwAAQBAJ&printsec=frontcover&source=gbs\_ge\_summary\_r&cad=0#v=onepage&q&f=false |
| **Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]** |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Course Title** | **Duration** | **Provider** |
| 1. | Cyber Threat Intelligence | 5 weeks | Coursera(IBM) |
| **Web link** |  |  |
| 1. <https://www.fireeye.com/>
2. <https://www.ibm.com/in-en/security>
 |
| Course Designed by: Dr.M. Punithavalliand CSCC Labs |

|  |
| --- |
| **Mapping with Programme Outcomes** |
| **COs** | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** | **PO8** | **PO9** | **PO10** |
| **CO1** | L | M | M | M | L | M | L | S | M | S |
| **CO2** | M | M | S | S | M | L | L | S | M | S |
| **CO3** | M | M | S | S | M | L | L | S | M | S |
| **CO4** | S | M | S | S | S | M | M | S | M | S |
| **CO5** | S | S | S | S | M | M | M | S | M | S |

\*S-Strong; M-Medium; L-Low



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Course code** | **21CSESE05** | **Cyber Law** | **L** | **T** | **P** | **C** |
| **Core/Elective/Supportive** | **Core** | **4** | **0** | **0** | **4** |
| **Pre-requisite** | **IPC, IT ACT and Criminal ACT** | **Syllabus Version** | **2022-2023** |
| **Course Objectives:** |
| The main objectives of this course are to:1. Understand the basics of Cyber Crime.
2. Discuss International Law and Regulation of Cyberspace and HumanRights.
3. Understand the Cyber Security Policy ofIndia.
 |
|  |
| **Expected Course Outcomes:** |
| On the successful completion of the course, student will be able to: |
| 1 | Understand Basics of Cyber Crime | K2 |
| 2 | Understand International Law and Regulation of Cyberspace and Human Rights | K2 |
| 3 | Legal Issues of Intercepting WiFi Transmissions | K4 |
| 4 | Conducting Cyber Investigation | K4 |
| 5 | A model case study “Live versus Post-mortem” | K3 |
| **K1** - Remember; **K2** - Understand; **K3** - Apply; **K4** - Analyze; **K5** - Evaluate; **K6**– Create |
| **Unit:1** | **Basics of Cybercrime** | **12 hours** |
| Cyber Criminology and Psychology: Introduction – Cyberbullying, cyber –Harassment and Cyberstalking – Revenge Pornography, Sexting, Sextortion and Related Offences - Tackling Offensive Online Communications and Abuse. Why Cybercrime Occurs: Introduction - Rational Choice Theories: Deterrence Theory and Routine Activity Theory - Self-Control Theory - General Strain Theory - Social Learning Theory and Related Concepts - Subcultural Theories. |
| **Unit:2** | **Human Rights and International Law** | **10 hours** |
| Introduction: Perspectives of Various Stakeholders and Challenges for International Law: Perspectives of Stakeholders - General Introduction to Public International Law - Jurisdiction and Attribution of State Responsibility in Cyberspace: Jurisdiction - Attribution of State Responsibility. Regulation of Cyberspace and Human Rights: General Background - Human Rights in Cyberspace – Exceptions - Territorial Scope of Human Rights Protection. |
| **Unit:3** | **Cybercrime Roles** | **14 hours** |
| Cyber Investigative Roles - Understanding Your Role as a Cyber Crime Investigator - The Role of Law Enforcement Officers - The Role of the Prosecuting Attorney. Incident Response: LiveForensicsandInvestigations-Post-mortem versusLiveForensics-Today‘sLiveMethods.Legal Issues of Intercepting WiFi Transmissions: WiFi Technology - Understanding WiFi RF - Scanning RF - Eavesdropping on WiFi - Fourth Amendment Expectation of Privacy inWLANs. |
| **Unit:4** | **Cybercrime investigations** | **12 hours** |
| Conducting Cyber Investigations: Demystifying Computer/Cyber Crime - Understanding IP Addresses - The Explosion of Networking - The Explosion of Wireless Networks - Interpersonal Communication. Digital Forensics and Analyzing Data: The Evolution of Computer Forensics - Phases of Digital Forensics – Examination – Analysis – Reporting. |



|  |  |  |
| --- | --- | --- |
| **Unit:5** | **Cyber Security Policy in India** | **12 hours** |
| Cyber Security Policy in India-2013 – Cyber Hacking – Cyber Fraud – Cyber Crime: Introduction – Against Economy – Preventive steps for organizations and Government – Problems Related with Cyber Crime – Indian Case studies – Types of Cyber Crime – Threat Perceptions – tools Used for Cyber Crime – Other Cyber Crime Methods – Connection between Terrorism and Cyber Crime. Cyber Crime and Punishment. |
| **Unit:6** | **Contemporary Issues** | **2 hours** |
| Case Study:Live versus Post-mortem |
|  |
|  | **Total Lecture hours** | **62 hours** |
| **Reference Books:** |
| 1 | National Cyber Crime Reference Handbook, AICTE, National Cyber Safety and Security Standards, Ministry of Social Justice and Empowerment, MSME, Govt of India. |
| 2 | Cyber Criminology, Series Editor, Anthony J. Masys, Humanitarian Assistance and Homeland Security, University of South Florida, Tampa, USA, Springer (2018) |
| 3 | Public International Law of Cyberspace - Law, Governance and Technology Series 32, Series editors, Pompeu Casanovas, Giovanni Sartor, Springer(2017) |
| 4 | Cyber Crime Investigations, Anthony Reyes, Syngress Publishing, Inc (2007). |
|  |
| **Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]** |
| 1 | <https://onlinecourses.swayam2.ac.in/cec20_cs09/preview> |
| 2 | [https://www.coursera.org/lecture/cyber-conflicts/introduction-to-cybercrime-and-](https://www.coursera.org/lecture/cyber-conflicts/introduction-to-cybercrime-and-fundamental-issues-xndSq)[fundamental-issues-xndSq](https://www.coursera.org/lecture/cyber-conflicts/introduction-to-cybercrime-and-fundamental-issues-xndSq) |
| 3 | [https://www.bu.edu/online/programs/certificate-programs/cybercrime-investigation-](https://www.bu.edu/online/programs/certificate-programs/cybercrime-investigation-cybersecurity/)[cybersecurity/](https://www.bu.edu/online/programs/certificate-programs/cybercrime-investigation-cybersecurity/) |
| 4 | <https://www.edureka.co/post-graduate/cybersecurity> |
| 5 | <https://www.udemy.com/course/ifci-expert-cybercrime-investigators-course/> |
| Web Link1. <https://cybercrime.gov.in/>
2. <https://www.meity.gov.in/cyber-security>
3. <https://cybercrime.gov.in/>
 |
| Course Designed By: MrS.Palanisamy |

|  |
| --- |
| **Mapping with Programme Outcomes** |
| **COs** | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** | **PO8** | **PO9** | **PO1 0** |
| **CO1** | M | S | M | S | M | M | M | S | M | S |
| **CO2** | S | L | S | S | S | M | M | S | S | M |
| **CO3** | S | S | M | S | M | M | S | L | S | S |
| **CO4** | M | S | S | S | S | S | S | S | S | L |
| CO5 | S | S | S | S | S | S | S | S | S | M |

\*S-Strong; M-Medium; L-Low



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Course code** | **21CSESE06** | **ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING** | **L** | **T** | **P** | **C** |
| **Core/Elective/Supportive** | **Elective** | **4** |  |  | **4** |
| **Pre-requisite** | **Basics of Mathematical Probabilities and Computer Programming** | **Syllabus Version** | **2022-2023** |
| **Course Objectives:**1. To articulate key problems, both technical and philosophical, in the development of artificialintelligence
2. To apply the machine learning algorithms for variousapplications.
3. To understand the Concepts of Machine learning algorithms of different probabilistic,rE
 |
| **Expected Course Outcomes:** |
| CO1 | Understand and Apply AI technique in the development of problem-solving and learning systems | K1 |
| CO2 | Understand the problems where artificial intelligence techniques areapplicable | K2 |
| CO3 | Apply the concepts of machine learning | K2 |
| CO4 | Understand the theoretical concepts of probabilistic and linearmethods | K4 |
| CO5 | Distinguish Supervised, Unsupervised and semi supervised learning | K4, K3,K5 |
|  | **K1** - Remember; **K2** - Understand; **K3** - Apply; **K4** - Analyze; **K5** - Evaluate; **K6**– Create |
|  |  |
|  | **Unit:1** | Artificial Intelligence | **12—hours** |
|  | Introduction to Artificial Intelligence – Intelligent Agents – Problem solving – Solving problems by searching – search in complex environments – Adversarial Search and Games –Constraints Satisfaction Problems |
|  |  |
|  | **Unit:2** | Knowledge, reasoning and planning | **12—hours** |
|  | Logical Agents – First –Order Logic – Inference in First –Order Logic – Knowledge Representation – Automated Planning – Uncertain knowledge and reasoning – Quantifying Uncertainty – Probabilistic Reasoning – Probabilistic Programming – Multi Agent DecisionMaking |
|  |  |
|  | **Unit:3** | Machine Learning | **12—hours** |
|  | Machine Learning Foundations –Overview – applications - Types of machine learning - basic concepts in machine learning Examples of Machine Learning -Applications - Linear Models for Regression - Linear Basis Function Models - The Bias-Variance Decomposition-Bayesian Linear Regression - Bayesian Model Comparison |
|  |  |
|  | **Unit:4** | Models for Classification | **12—hours** |
|  | Supervised Learning Linear Models for Classification - Discriminant Functions - Probabilistic Generative Models - Probabilistic Discriminative Models - Bayesian Logistic Regression. Decision Trees - Classification Trees- Regression Trees - Pruning. Neural Networks -Feed-forward Network Functions - Error Back propagation - Regularization - Mixture Density and Bayesian Neural Networks - Kernel Methods - Dual Representations - Radial Basis Function Networks. Support Vector Machines - Ensemble methods- BaggingBoosting – Evaluation Methods |



|  |  |  |  |
| --- | --- | --- | --- |
|  | **Unit:5** | Clustering | **12—hours** |
|  | Unsupervised Learning Clustering- K-means - EM - Mixtures of Gaussians - The EM Algorithm in General - Model selection for latent variable models - high-dimensional spaces -- The Curse of Dimensionality - Dimensionality Reduction - Factor analysis - Principal Component Analysis - Probabilistic PCA- Independent components analysis |
|  |  |
|  | **Unit:6** | **Contemporary Issues** | **2 hours** |
|  | Ethical Considerations in Machine Learning Applications – Ethics and Challenges of AI andML as disruptive technology Use cases – Webinars |
|  |  | **Total Lecture hours** | **62—hours** |
| **Text Books:** |
| 1 | Christopher Bishop, “Pattern Recognition and Machine Learning” Springer, 2006 |
| 2 | Kevin P. Murphy, “Machine Learning: A Probabilistic Perspective”, MIT Press, 2012 |
| 3 | EthemAlpaydin, “Introduction to Machine Learning 3(Adaptive Computation and MachineLearning Series)”, Third Edition, MIT Press, 2014 |
| 4 | Tom M Mitchell, “Machine Learning”, First Edition, McGraw Hill Education, 2013. |
| 5 | Stuart Russell and Peter Norvig, “Artificial Intelligence: A Modern Approach”, Fourthedition, 2020. |
| **Reference Books** |
| 1 | JannesKlaas, “Machine Learning for Finance”, ISBN: 978178936364, 2019 [Packt] |
| 2 | Giuseppe Bonaccorso, “Machine Learning Algorithms”, Second Edition, ISBN: 9781789347999, 2018 [Packt] |
| 3 | Stephen Marsland, “Machine Learning –An Algorithmic Perspective”, CRC Press, 2009 |
| 4 | Hastie, Tibshirani, Friedman, “The Elements of Statistical Learning”, Second Edition,Springer, 2008 |
| 5 | Yuxi Liu, “Python Machine Learning By Example”, 2017 [Packt] |
| 6 | [John Paul Mueller](https://www.amazon.in/s/ref%3Ddp_byline_sr_book_1?ie=UTF8&field-author=John%2BPaul%2BMueller&search-alias=stripbooks), [Luca Massaron](https://www.amazon.in/Luca-Massaron/e/B00RW7GV02/ref%3Ddp_byline_cont_book_2), “Machine Learning (in Python and R) For Dummies”,First Edition, Wiley Publisher, ISBN: 9788126563050, 2016 |
| 7 | [U Dinesh Kumar](https://www.amazon.in/s/ref%3Ddp_byline_sr_book_1?ie=UTF8&field-author=U%2BDinesh%2BKumar%2BManaranjan%2BPradhan&search-alias=stripbooks) [ManaranjanPradhan](https://www.amazon.in/s/ref%3Ddp_byline_sr_book_1?ie=UTF8&field-author=U%2BDinesh%2BKumar%2BManaranjan%2BPradhan&search-alias=stripbooks),,“Machine Learning using Python”. )Publisher: Wiley, ISBN: 9788126579907, 2019 |
|  | **Online Course:** |  |  |
|  | **S.****No** | **Course Title** | **Duration** | **Provider –Free** |
|  | 1. | AI for Everyone | 4 Weeks | Coursera |
|  | 2. | AI for Everyone: Master the Basics | 4 Weeks | edX |
|  | 3. | Introduction to Artificial Intelligence | 16 Weeks | Udacity |
|  | 4. | Machine Learning : Regression | 6 Weeks | Coursera |
|  | 5. | Introduction to Machine Learning | 12 Weeks | Swayam – NPTEL |
|  | 6 | Deep Learning Specialization | 4 Courses | Coursera |

**Web Link - Video:**

1. htt[ps://www.pa](http://www.packtpub.com/data/hands-on-machine-learning-with-scikit-learn-and-tensorflow-2-)c[ktpub.com/data/hands-on-machine-learning-with-scikit-learn-and-tensorflow-2-](http://www.packtpub.com/data/hands-on-machine-learning-with-scikit-learn-and-tensorflow-2-)0-video
2. htt[ps://www.pa](http://www.packtpub.com/data/machine-learning-projects-with-tensorflow-2-0-video)c[ktpub.com/data/machine-learning-projects-with-tensorflow-2-0-video](http://www.packtpub.com/data/machine-learning-projects-with-tensorflow-2-0-video)3.https:/[/www.pa](http://www.packtpub.com/application-development/complete-machine-learning-course-python-)c[ktpub.com/application-development/complete-machine-learning-course-python-](http://www.packtpub.com/application-development/complete-machine-learning-course-python-)video

|  |
| --- |
| Mapping with Programme Outcomes |
| **COs** | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** | **PO8** | **PO9** | **PO10** |
| **CO1** | M | S | M | S | L | L | M | L | S | L |
| **CO2** | M | S | L | S | M | M | L | L | S | S |
| **CO3** | S | S | L | L | L | L | L | L | L | L |
| **CO4** | S | S | S | S | L | L | M | M | M | L |
| **CO5** | S | S | S | L | L | L | L | L | L | L |

\*S-Strong; M-Medium; L-Low

## Students have to undergo One Job Oriented Course and one Value added course every year.



Annexure

**M.Sc. Cyber Security**

# Syllabus

**With effect from 2022-23**



## DEPARTMENT OF COMPUTER APPLICATIONS

**Bharathiar University**

**(A State University, Accredited with “A“ Grade by NAAC and 13th Rank among Indian Universities by MHRD-NIRF) Coimbatore 641 046, INDIA**

**BHARATHIAR UNIVERSITY, COIMBATORE–641 046 DEPARTMENT OF COMPUTER APPLICATIONS**

**M.Sc. CYBER SECURITY 2022-2023 – (CBCS) University Dept.**

**in collaboration with CSCC Labs (Effective from the academic Year 2022-2023)**

1. **Eligibility forAdmission**

A pass in any Bachelors degree of minimum 3 years duration with Mathematics or Statistics as any one of the subjects at Graduate level.

## Duration

The programme shall be offered on a full-time basis for two years. The students will undergo the programme in Bharathiar University campus for the first three semesters and will undertake project work in the fourthsemester.

## Regulations

The general Regulations of the Bharathiar University Choice Based Credit System Programme are applicable to theseprogrammes.

## The Medium of Instruction andExaminations

The medium of instruction and Examinations shall be in English.

## Submission of Record Notebooks for Practical Examinations & Project Viva- Voce.

Candidates taking the Practical Examinations should submit bonafide Record Note Books prescribed for the Examinations. Otherwise the candidates will not be permitted to take the Practical Examinations. Candidates taking the practice School / Project & Viva -Voce Examination should submit Project Report prescribed for the Examinations. Otherwise the candidates will not be permitted to take up the Project & Viva-voceExamination.

Students carry out Case Studies /Mini-projects and finishing school / major project and the schedule for review meetings are as givenbelow:

Table: Schedule for Review Meetings

|  |  |  |
| --- | --- | --- |
|  | First Review | Second Review |
| Case Studies /Mini Projects | Thursday of firstweek in June | Thursday of firstweek in August |
| PracticeSchool / MajorProject | Friday of first week of February | Friday of first week of April |

## Ranking

A candidate who qualifies for the PG Degree Course passing all the Examinations in the first attempt, within the minimum period prescribed for the Course of Study from the date of admission to the Course and secures 1stor 2ndClass shall be eligible for ranking and such ranking will be confined to 10% of the total number of candidates qualified in that particular subject to a maximum of 10ranks.

## Revision of Regulations and Curriculum

The above Regulation and Scheme of Examinations will be in vogue without any change for a minimum period of three years from the date of approval of the Regulations. The University may revise/amend/ change the Regulations and Scheme of Examinations, if foundnecessary.

## BHARATHIAR UNIVERSITY : : COIMBATORE 641046 DEPARTMENT OF COMPUTER APPLICATIONS

**MISSION**

* + To impart practical knowledge and professional skills in the area of computer applications to students to make them industryready.
	+ To contribute to the advancement of knowledge in the field of Computer Applications throughresearch.
* To involve the students in societal contributions to make them aware of the society and itsneeds.