|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **B.E. COMPUTER SCIENCE AND ENGINEERING / INFORMATION SCIENCE & ENGINEERING**  Choice Based Credit System (CBCS) applicable for 2022 Scheme  **SEMESTER – VI** | | | | |
| **Cyber Security** (3:0:0) 3  (Effective from the academic year 2024-25) | | | | |
| Course Code | | BCS604A | CIE Marks | 50 |
| Teaching Hours/Week (L: T:P) | | (3:0:0) | SEE Marks | 50 |
| Total Number of Contact Hours | | 40 | Exam Hours | 3 |
| **Course Objectives:**  This course will enable students to:   1. Understand the fundamental concepts of cybersecurity, cryptography, network security, and cloud security. 2. Develop practical skills in Cyber threat intelligence, Vulnerability Scanning and Data Protection. 3. Learn about cyber laws, compliance standards, and risk management frameworks. 4. Gain hands-on experience with security tools and real-world case studies. 5. Self-Learning for industry certifications such as CEH, CISSP, and Security+. | | | | |
| **Preamble:**  In today’s digital age, network and cybersecurity are crucial for safeguarding information systems by ensuring data confidentiality, integrity, and availability. As cyber threats rapidly evolve, organizations and individuals must implement robust security measures to protect networks from malicious actors, unauthorized access, and data breaches. Understanding key principles such as secure communication protocols, firewalls, intrusion detection and prevention systems (IDS/IPS), and Virtual Private Networks (VPNs) is essential. Additionally, adopting cybersecurity frameworks, cryptographic techniques, and vulnerability management strategies strengthens defences against cyber threats. By enforcing strong security policies, access controls, and proactive monitoring, we can establish a secure digital environment, fostering trust and reliability in cyberspace. | | | | |
| **Module – 1** | | | | |
| **Importance of cyber security:** Scenarios for security, Understanding the attack surface, the threat landscape, the importance of securing the network and Applications, the history of breaches, how security helps to build trust.  Legacy cybersecurity systems, Transformations in cybersecurity, Advancements in security technology to security 2.0, How ML and Al will play a larger role in cybersecurity,  (Chapter 1 & 2 from Textbook1)  (8 Hours) | | | | |
| **Module – 2** | | | | |
| Learning cybersecurity Technologies Mobile security, advanced data security, cloud security, Modern day regulations, Incidence response and forensic, Enterprise security at scale, penetration testing, DevSecOps, IoT Security, User behaviour analytics (UBA), Endpoint detection and response (EDR).  Attacker Mindset, the category of hackers, the traits of hackers, Social Characteristics of hackers, How hackers think (Motivators), What can be learned from the psychology of hackers?  (Chapter 3 & 5 from Textbook1)  (8 Hours) | | | | |
| **Module – 3** | | | | |
| **Authentication:** one way authentication (password based, certificate based), Mutual authentication (shared secret based, Asymmetric key-based, Authentication and key Agreement, use of Timestamps), Dictionary attacks (attack types, defeating Dictionary attacks).  **Firewalls:** firewall basics-firewall functionality, policies and access control lists, firewall types; practical issues-placement of firewalls, firewall configuration.  Textbook 2: Chapter 11 (11.1-11.3), Chapter 21 (21.1- 21.2)  (8 Hours) | | | | |
| **Module – 4** | | | | |
| **Non-Cryptographic Protocol Vulnerabilities:** DoS and DDoS (attack types, impact of SYN flooding), Session Hijacking and Spoofing (impersonation and session Hijacking, ARP spoofing); cross-site scripting (XSS): Vulnerabilities, SQL injection.  **Intrusion Prevention and Detection:** Introduction, Prevention versus Detection, Types of Intrusion Detection Systems,  Cyber Kill Chain: what is a kill chain, applying the cyber kill chain to detection  Textbook 2: Chapter 17 ,18,22 (17.1, 17.2, 18.4, 22.1- 22.4,)  Textbook 4: Chapter 16  (8 Hours) | | | | |
| **Module – 5** | | | | |
| **Web Application Security:** This Site Is Secure, The Core Security Problem: Users Can Submit Arbitrary Input, Key Problem Factors, The New Security Perimeter, Core Defense Mechanisms: Handling User Access, Handling User Input, Handling Attackers.  **Penetration Testing of Web Applications:** Using tools like BURP Suit and OWASP ZAP to find vulnerabilities in a web application.  https://portswigger.net/burp , https://owasp.org/  (Chapters 1 & 2 from TextBook 3)  (8 Hours) | | | | |
| **Course Outcomes:**  The students will be able to: **(List the COs as per the course requirements)** | | | | |
| **CO1**: | Examine cybersecurity fundamental concepts, including cyber threats, attack types, cryptography, security frameworks and advanced security technologies while solving problems addressing threat detection, regulatory, data protection and regulatory compliance. | | | |
| **CO2** | Analyze the psychology of hackers, including their traits and motivations, and their influence on security strategies. | | | |
| **CO3:** | Analyze security mechanisms including authentication, firewalls, intrusion detection and prevention systems, and secure communication protocols for the given problems. | | | |
| **CO4:**  **CO5:** | Investigate network vulnerabilities, including DoS/DDoS attacks, session hijacking, SQL injection, and cross-site scripting to propose the solution to overcome the attacks.  Demonstrate hands-on skills using cybersecurity tools for Web applications vulnerability Assessment. | | | |
| **Textbooks:**   1. Cybersecurity: The Beginner's Guide by Dr. Erdal Ozkaya 1st Edition 2019, Published by Packt Publishing Ltd. ([Click Here - e-book](https://www.jre-training.com/WebSecurity/Cybersecurity.pdf)) 2. Bernard L. Menezes, Ravinder Kumar, **Cryptography, Network Security, and Cyber Laws**, 2018 Cengage Learning India Pvt. Ltd. 3. The Web Application Hacker’s Handbook Finding and Exploiting Security Flaws by Dafydd   Stuttard Marcus Pinto 2nd Edition 2011 ( [Click Here - e-book](https://www.beiruteyecenter.com/uploads/3794_1008_4334.pdf) )   1. Ira Winkler and Araceli Treu Gomes- Advanced Persistent Security, A Cyberwarfare Approach to Implementing Adaptive Enterprise Protection, Detection, and Reaction Strategies  [ISBN: 978-0-12-809316-0](ISBN:%20978-0-12-809316-0) , Publisher: Todd Green   **References:**   1. Thoms J. Mowbray, Cybersecurity, managing systems, Conducting Testing, and Investigating Instrusions 2. The Cyber Security Body of Knowledge (CyBok)- Awais Rashid, Howard Chivers, George Danezis, Emil Lupu, Andrew Martin 3. Cybersecurity and Cyberwar" by P.W. Singer for policy/ethics or "Blue Team Handbook" for incident response 4. Sunit Belapure, Nina Godbole, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives Wiley India Pvt Ltd 2013 5. Surya Prakash Tripathi, Ritendra Goyal, Praveen Kumar Shukla, Introduction to information security and cyber laws, Dreamtech Press 2015 6. Thomas J. Mowbray, Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions John Wiley & Sons 2013 7. James Graham, Ryan Olson, Rick Howard, Cyber Security Essentials CRC Press 2010 | | | | |
| **Tools for Cyber Security Demonstration**   1. OpenSSH, Hydra, Wireshark, Squid Proxy **(Module 3)** 2. MITRE ATT&CK Navigator, Metasploit Framework, Atomic Red Team, Snort, Hping3, UFONet , Nessus Essentials **(Module 4)** 3. BURP suite and OWASP Zap (**Module 5**) 4. Threat Modeling Tool, Threat Dragon, TMT (Threat Modeling Tool by IriusRisk) SIEM (Security Information and Event Management), Sysmon (Windows), OpenVAS, Nmap, Virus Total 5. **Indian Digital Signature Providers** –  * eMudhra * SafeScrypt * Capricorn CA  1. Autopsy, The Sleuth Kit (TSK), FTK Imager   **Alternate Assessment Tools (AATs) suggested:**   1. **Practical demonstration of Tools in a team of two-three members choosing any 4-5 tools in the given list or any other tools in consultation with the course coordinator and report submission)**  * Network Intrusion Detection and Analysis - (Tool: **Snort**) * Event Log Aggregation, Correlation, and analysis- (Tool: **Splunk Enterprises/IBM Q radar**) * Web Proxies – (caching, URI Filtering, Content Filtering, Squid Configuration, Squid Access Logfiles, Squid Cache, Web proxy analysis, Encrypted Web Traffic,)- (Tool: **Squid**) * Traffic Analysis – Protocol Analysis, Packet Analysis, Higher-layer Traffic analysis- (Tool: **Wireshark**) * Vulnerability Scanning and Management (Tools: **Nessus Essentials, Burp suite**) * Servers Configuration – DHCP server, Name servers, Authentication Servers, Firewalls, Application Servers * SMTP, Fishing Email Analysis – Tool: **Mx Toolbox, Virus Total, IP Void, URL Void, OpenVAS** * Incident response Management, Cyber Kill Chain, MITRE ATT&CK Framework * AI-driven cyberattacks, zero-trust security models, blockchain for security, and deepfake threats * Penetration testing, ethical hacking tools (Metasploit, Nmap, Aircrack-ng, etc.) * Cyber laws (GDPR, HIPAA, India’s IT Act), compliance frameworks. * Incident response lifecycle (NIST SP 800-61), forensics tools (Autopsy, FTK). * Risk management (ISO 27001, NIST CSF). | | | | |
| **Web links / e – resources:**  <https://www.snort.org/documents>  <https://docs.splunk.com/Documentation>  <https://www.ibm.com/docs/en/qradar-common>  <https://www.squid-cache.org/Doc/config/>  <https://www.wireshark.org/docs/>  <https://docs.tenable.com/nessus/Content/GettingStarted.htm>  <https://portswigger.net/web-security>  <https://bind9.readthedocs.io/en/v9.20.5/>  <https://docs.netgate.com/pfsense/en/latest/>  <https://www.freeradius.org/documentation/>  <https://mxtoolbox.com/SuperTool.aspx>  <https://www.virustotal.com/gui/home/upload>  <https://attack.mitre.org/>  <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>  <https://csrc.nist.gov/pubs/sp/800/61/r2/final>  <https://www.nist.gov/cyberframework> | | | | |