RAMAKRISHNA MISSION VIDYAMANDIRA

CBCS Syllabus B.Sc. Computer Science Honours

Semester-V

Credit: 6

Course Type: Discipline Specific Elective

Course Outcome:

i) Determine and analyze software vulnerabilities and security solutions to reduce the risk of exploitation.
ii) Comprehend and execute risk management processes, risk treatment methods, and key risk and performance indicators.
iii) Develop understanding of cyber security laws.
iv) Develop and manage an information security program.
v) Implantation and setup of ethical hacking laboratory using Kali Linux.
vi) To develop practical knowledge of using various open source framework for Cybersecurity.

CMSA DSE T: Cybersecurity

Credit: 4 **Marks: 50**

Introduction to Cyber Security: Overview of Cyber Security, Internet Governance – Challenges and Constraints, Cyber Threats: - Cyber Warfare-Cyber Crime-Cyber Terrorism-Cyber Espionage, need for a Comprehensive Cyber Security Policy, Need for a Nodal Authority, Need for an International convention on Cyberspace. [3 L]

Cyber Security Vulnerabilities and Cyber Security Safeguards: Cyber Security Vulnerabilities Overview, Vulnerabilities in software, System administration, Complex Network Architectures, Open Access to Organizational Data, Weak Authentication, Unprotected Broadband communications, Poor Cyber Security Awareness, Cyber Security Safeguards- Overview, Access control, Audit, Authentication, Biometrics, Cryptography, Deception, Denial of Service Filters, Ethical Hacking, Firewalls, Intrusion Detection Systems, Response, Scanning, Security policy, Threat Management. [7 L]

Securing Web Application, Services and Servers: Introduction, Basic security for HTTP Applications and Services, Basic Security for SOAP Services, Identity Management and Web Services, Authorization Patterns, Security Considerations, Challenges. [5 L]

Intrusion Detection and Prevention: Intrusion, Physical Theft, Abuse of Privileges, Unauthorized Access by Outsider, Malware infection, Intrusion detection and Prevention Techniques, Anti-Malware software, Network based Intrusion detection Systems, Network based Intrusion Prevention Systems, Host based Intrusion prevention Systems, Security Information Management, Network Session Analysis, System Integrity Validation. [7 L]

Malware Analysis & Reverse Engineering: Fundamentals of Malware Analysis (MA), Reverse Engineering Malware (REM) Methodology, Brief Overview of Malware analysis lab setup and configuration, Introduction to key MA tools and techniques. [4 L]

Cryptography and Network Security: Introduction to Cryptography, Symmetric key Cryptography, Asymmetric key Cryptography, Message Authentication, Digital Signatures, Applications of Cryptography. Overview of Firewalls- Types of Firewalls, User Management, VPN Security, Security Protocols: - security at the Application Layer- PGP and S/MIME, Security at Transport Layer- SSL and TLS, Security at Network Layer-IPSec.

[10 L]

Cyberspace and the Law: Concept of Cyberspace, Issues of Jurisdiction in Cyberspace: Jurisdiction Principles under International law, Jurisdiction in different states, Position in India. Conflict of Laws in Cyberspace, International Efforts for harmonization Privacy in Cyberspace, Electronic Commerce, Cyber Contract, Intellectual Property Rights and Cyber Laws UNCITRAL Model Law, E-Governance and Records, The INDIAN Cyberspace, National Cyber Security Policy 2013. [4 L]

Ethical Hacking and Response: Ethical hacking process, Hackers behaviour & mindset, Maintaining Anonymity, Hacking Methodology, Information Gathering, Active and Passive Sniffing, Physical security vulnerabilities and countermeasures. Internal and External testing. Preparation of Ethical Hacking and Penetration Test Reports and Documents, Social Engineering attacks and countermeasures. Password attacks, Privilege Escalation and Executing Applications, Network Infrastructure Vulnerabilities, IP spoofing, DNS spoofing, Wireless Hacking: Wireless footprint, Wireless scanning and enumeration, Gaining access (hacking 802.11), WEP, WPA, WPA2, DoS attacks. Web server and application vulnerabilities, SQL injection attacks, Vulnerability Analysis and Reverse Engineering, Buffer overflow attacks. Client-side browser exploits, Exploiting Windows Access Control Model for Local Elevation Privilege. Exploiting vulnerabilities in Mobile Application, Introduction to Metasploit, Metasploit framework, Metasploit Console, Payloads, Metrpreter, Introduction to Armitage, Installing and using Kali Linux Distribution, Introduction to penetration testing tools in Kali Linux. Case Studies of recent vulnerabilities and attacks.

[15 L]

Cyber Forensics: Introduction to Cyber Forensics,Computer forensics,digital forensics and mobile forensic,conducting disk-based analysis, Investigating Information-hiding, Scrutinizing E-mail, Validating E-mail header information, Tracing Internet access, Tracing memory in real-time, Image Capturing, Authenticating Evidence, Hidden Data Extraction, Data Storage, File Systems, Recovery of deleted files, Cracking Passwords. [5 L]

CMSA DSE P: Cybersecurity Laboratory

Credit: 2 **Marks: 25**

- Set up of virtual ethical hacking lab, Introduction to key MA tools and techniques, Introduction to Network based Intrusion Prevention Systems. [5 L]

- Kali Linux: Installing and using of Kali Linux Distribution, Kali Linux command line, working with files, directories, key strokes, shell variables, vi, vim, nano, bash shell scripting, user management, group management, file permission, networking, password breaking, ethical hacking tools in Kali linux, Introduction to penetration testing tools in Kali Linux, social engineering attacks such as phishing, malware, spyware, adware, ransomware and Bluetooth attacks, Case Studies of recent vulnerabilities and attacks. [10 L]

- Ethical hacking tools: Penetration testing and collecting data for exploration using Sniper,nmap scan using Brutex, XSS scanner using Dalfox,web application security testing using OWASP Zed Attack Proxy (ZAP), Footprining tools, Location tracer, Website copier, Foca, Whois, IP and DNS Lookup. [10 L]

- Metasploit framework, Metagoofil: How to install Metagoofil, information gathering Metagoofil, Maltego: Find IP, location, domain using Maltego; Different kinds of system attack,Introduction to Cyber Forensics tools. [15 L]

Recommended Books:

1. Baloch, R., Ethical Hacking and Penetration Testing Guide, CRC Press, 2015.
2. Beaver, K., Hacking for Dummies, 3rded. John Wiley & sons., 2013.
3. Forouzan, B.A., Cryptography & Network Security. Tata McGraw-Hill Education, 2010
4. Michael Sikorski, Andrew Honig, Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software publisher William Pollock, 2012.
5. John Sammons, The Basics of Digital Forensics, Elsevier, 1st Edition, 2015
6. Davidoff, Sherri, Network forensics: Tracking hackers through cyberspace, Pearson education India private limited, 2017.
7. Dr. Farooq Ahmad, Cyber Law in India, Allahbad Law Agency- Faridabad.
8. J.P. Sharma, Sunaina Kanojia, Cyber Laws.