PARUL UNIVERSITY - Faculty of IT & Computer Science

Department of Computer Application

SYLLABUS FOR 4th Sem B.Sc. (IT), BCA, IMCA (A.Y.-IV) PROGRAMME

Cyber Security (05101386)

Type of Course: B.Sc. (IT), BCA, IMCA (A.Y.-IV)

Prerequisite: Basic knowledge of Computers, Basic knowledge of networking and Internet, Hands on Windows operating system

Rationale: Understand, appreciate, employ, design and implement appropriate security technologies and policies to protect computers and digital information, Identify & Evaluate Information Security threats and vulnerabilities in Information Systems and apply security measures to real time scenarios, Identify common trade-offs and compromises that are made in the design and development process of Information Systems, Demonstrate the use of standards and cyber laws to enhance information security in the development process and infrastructure protection

Teaching and Examination Scheme:

Teaching Scheme			Credit	Examination Scheme					Total
Lect Hrs/ Week	Tut Hrs/ Week	Lab Hrs/ Week		External		Internal			
				T	P	T	CE	P	
3	1	0	4	60	0	20	20	0	100

Lect - Lecture, **Tut** - Tutorial, **Lab** - Lab, **T** - Theory, **P** - Practical, **CE** - CE, **T** - Theory, **P** - Practical

Contents:

Sr.	Topic	Weightage	Teaching Hrs.
1	**Cyber Security Concepts**: Essential Terminologies: CIA, Risks, Breaches, Threats, Attacks, Exploits. Information Gathering (Social Engineering, Foot Printing & Scanning). Open Source/ Free/ Trial Tools: nmap, zenmap, Port Scanners, Network scanners.	10%	6
2	**Cryptography and Cryptanalysis**: 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. Open Source/ Free/ Trial Tools: Implementation of Cryptographic techniques, OpenSSL, Hash Values Calculations MD5, SHA1, SHA256, SHA 512, Steganography (Stools)	15%	7

3	**Infrastructure and Network Security**: Introduction to System Security, Server Security, OS Security, Physical Security, Introduction to Networks, Network packet Sniffing, Network Design Simulation. DOS/ DDOS attacks. Asset Management and Audits, Vulnerabilities and Attacks. Intrusion detection and Prevention Techniques, Host based Intrusion prevention Systems, Security Information Management, Network Session Analysis, System Integrity Validation. Open Source/ Free/ Trial Tools: DOS Attacks, DDOS attacks, Wireshark, Cain & abel, iptables/ Windows Firewall, snort, suricata, fail2ban	15%	7
4	**Cyber Security Vulnerabilities & Safe Guards**: Internet Security, Cloud Computing &Security, Social Network sites security, Cyber Security Vulnerabilities-Overview, vulnerabilities in software, System administration, Complex Network Architectures, Open Access to Organizational Data, Weak Authentication, Authorization, Unprotected Broadband communications, Poor Cyber Security Awareness. Cyber Security Safeguards- Overview, Access control, IT Audit, Authentication. Open Web Application Security Project (OWASP), Web Site Audit and Vulnerabilities assessment.	15%	7
5	**Malware**: Explanation of Malware, Types of Malware: Virus, Worms, Trojans, Rootkits, Robots, Adware's, Spywares, Ransom wares, Zombies etc., OS Hardening (Process Management, Memory Management, Task Management, Windows Registry/ services another configuration), Malware Analysis. Open Source/ Free/ Trial Tools: Antivirus Protection, Anti Spywares, System tuning tools, Anti Phishing	15%	7
6	**Security in Evolving Technology**: Biometrics, Mobile Computing and Hardening on android and ios, IOT Security, Web server configuration and Security. Introduction, Basic security for HTTP Applications and Services, Basic Security for Web Services like SOAP, REST etc., Identity Management and Web Services, Authorization Patterns, Security Considerations, Challenges. Open Source/ Free/ Trial Tools: adb for android, xcode for ios, Implementation of REST/ SOAP web services and Security implementations	15%	7
7	**Cyber Laws and Forensics**: Introduction, Cyber Security Regulations, Roles of International Law, the state and Private Sector in Cyberspace, Cyber Security Standards. The INDIAN Cyberspace, National Cyber Security Policy 2013. Introduction to Cyber Forensics, Need of Cyber Forensics, Cyber Evidence, Documentation and Management of Crime Sense, Image Capturing and its importance, Partial Volume Image, Web Attack Investigations, Denial of Service Investigations, Internet Crime Investigations, Internet Forensics, Steps for Investigating Internet Crime, Email Crime Investigations. Open Source/ Free/ Trial Tools: Case Studies related to Cyber Law, Common Forensic Tools like dd, md5sum, sha1sum, Ram dump analysis, USB device	15%	7

*Continuous Evaluation:

It consists of Assignments/Seminars/Presentations/Quizzes/Surprise Tests (Summative/MCQ) etc.

Reference Books:

1. Cryptography and Network Security
   William Stallings; Pearson Education

2. Cryptography and Network Security
   V.K. Jain; Khanna Publishing House

3. Information and Cyber Security
   Gupta Sarika; Khanna Publishing House

4. Cryptography and Network Security
   Atul Kahate; TMH

5. Cryptography and Information Security
   V.K. Pachghare; PHI Learning

6. Information System Security
   Nina Godbole; Wiley

7. Hacking
   Bothra Harsh; Khanna Publishing House