

CS383: CYBER SECURITY AND CYBER LAWS

Credit and Hours:

Teaching Scheme	Theory	Practical	Total	Credit
Hours/week	3	2	5	4
Marks	100	50	150	

A. Objective of the Course:

The main objective to give the course is

- To be able to identify vulnerabilities in system, software or web application
- To be able to identify security risks and take preventive steps
- To be able investigate cybercrime and collect evidences by understanding cyber laws.
- Able to use knowledge of forensic tools and software

B. Outline of the Course:

Sr No.	Title of the unit	Minimum number of Hours
1	Introduction to Cyber Security	06
2	Cyber Security Vulnerabilities and Cyber Security Safeguards	11
3	Securing Web Application, Services and Servers	06
4	Intrusion Detection and Prevention	11
5	Introduction to Cyber Crime and law	06
6	Introduction to Cyber Crime Investigation	05

Total Hours (Theory): 45

Total Hours (Lab): 30

Total Hours: 75

C. Detailed Syllabus:

1	Introduction to Cyber Security	06 hours	12%
1.1	Overview of Cyber Security		
1.2	Internet Governance – Challenges and Constraints		
1.3	Cyber Threats:- Cyber Warfare-Cyber Crime-Cyber terrorism-Cyber Espionage		
1.4	Need for a Comprehensive Cyber Security Policy, Need for a Nodal Authority, Need for an International convention on Cyberspace.		
2	Cyber Security Vulnerabilities and Cyber Security Safeguards	11 hours	25%
2.1	Cyber Security Vulnerabilities-Overview		
2.2	Vulnerabilities in software, System administration, Complex Network Architectures, Open Access to Organizational Data, Weak Authentication, Unprotected Broadband communications, Poor Cyber Security Awareness.		
2.3	Cyber Security Safeguards- Overview		
2.4	Access control, Audit, Authentication, Biometrics, Cryptography, Deception, Denial of Service Filters		
2.5	Ethical Hacking, Firewalls, Intrusion Detection Systems, Response, Scanning, Security policy, Threat Management.		
3	Securing Web Application, Services and Servers	06 hours	13%
3.1	Introduction, Basic security for HTTP Applications and Services, Basic Security for SOAP Services		
3.2	Identity Management and Web Services, Authorization Patterns		
3.3	OWASP Top 10 ,Security Considerations, Challenges		
4	Intrusion Detection and Prevention	11 hours	25%
4.1	Introduction of Intrusion Detection and Prevention, Physical Theft, Abuse of Privileges, Unauthorized Access by Outsider, Malware infection		
4.2	Intrusion detection and Prevention Techniques, Anti-Malware software		
4.3	Network based Intrusion detection Systems, Network based Intrusion Prevention Systems		
4.4	Host based Intrusion prevention Systems, Security Information Management		
4.5	Network Session Analysis, System Integrity Validation		
5	Introduction to Cyber Crime and law	06 hours	13%
5.1	Cyber Crimes, Types of Cybercrime, Hacking, Attack vectors		

- 5.2 Cyberspace and Criminal Behaviour, Clarification of Terms, Traditional Problems Associated with Computer Crime .
- 5.3 Introduction to Incident Response, Digital Forensics, Realms of the Cyber world, Recognizing and Defining Computer Crime
- 5.4 Contemporary Crimes, Contaminants and Destruction of Data
- 5.5 Indian IT ACT 2000
- 6 Introduction to Cyber Crime Investigation 05 hours 12%**
- 6.1 Key loggers and Spyware, Virus and Worms, Trojan and backdoors
- 6.2 DOS and DDOS attack
- 6.3 Steganography, SQL injection, Buffer Overflow

D. Instructional Methods and Pedagogy:

- At the start, of course, the course delivery pattern, prerequisite of the subject will be discussed.
- Faculty would use coached problem-solving method as it is the class format in which faculty provide a structured, guided context for students working collaboratively to solve problems.
- Assignments based on topic content will be given to the students at the end of each unit/topic.
- Surprise tests/Quizzes will be conducted.
- The course includes a laboratory, where students have an opportunity to build an appreciation for the concepts being taught in lectures.

E. Student Learning Outcomes / Objectives:

Upon completion of this course, students will be able to do the following:

- After learning the course, students should be able to learn about cyber-attack, type of cybercrimes
- Learn cyber security vulnerabilities and security safeguard.
- Learn hands-on on how to prevent the web using different web application tools.
- Learn about how to protect the network using different network tools and Intrusion detection and prevention techniques,
- Learn basic of Cryptography and network security

- Understand about cyber laws
- Learn about cyber Forensics and investigation of information hiding.
- Learn about how to protect them self and ultimately society from cyber-attacks.

F. Recommended Study Material:

❖ Text Books:

1. Cybersecurity: The Beginner's Guide Dr.Erdal Ozkaya

❖ Reference Books:

1. Digital Privacy and Security Using Windows: A Practical Guide ByNihad Hassan, Rami Hijazi, Apress
2. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Nina Godbole and SunitBelpure, Publication Wiley