CS472: CYBER SECURITY AND CYBER LAW

Credit and Hours:

Teaching Scheme	Theory	Practical	Total	Credit
Hours/week	4	2	6	5
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	13
3	Securing Web Application, Services and Servers	10
4	Intrusion Detection and Prevention	14
5	Cryptography and Network Security	07
6	Introduction to Cyberspace and the Law	04
7	Cyber Forensic	06

Total Hours (Theory): 60

Total Hours (Lab): 30

Total Hours: 90

C. Detailed Syllabus:

1	**Introduction to Cyber Security**	**06 hours**	**10%**
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**	**13 hours**	**22%**
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**	**10 hours**	**15%**
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**	**14 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	**Cryptography and Network Security**	**07 hours**	**12%**

5.1 Introduction to Cryptography

5.2 Symmetric key Cryptography, Asymmetric key Cryptography,

5.3 Message Authentication, Digital Signatures,Applications of Cryptography.

5.4 Overview of Firewalls- Types of Firewalls, User Management

5.5 VPN Security Protocols: - security at the Application Layer- PGP and S/MIME

5.6 Security at Transport Layer- SSL and TLS, Security at Network Layer-IPSec

6 Introduction to Cyberspace and the Law 04 hours 06%

6.1 Introduction, Cyber Security Regulations

6.2 Roles of International Law, the state and Private Sector in Cyberspace, Cyber Security Standards

6.3 The INDIAN Cyberspace, National Cyber Security Policy 2013.

7 Cyber Forensics 06 hours 10%

7.1 Introduction to Cyber Forensics, Handling Preliminary Investigations, Controlling an Investigation

7.2 Conducting disk-based analysis, Investigating Information-hiding

7.3 Scrutinizing E-mail, Validating E-mail header information, Tracing Internet access, Tracing memory in real-time.

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 able to learn about cyber-attack, type of cybercrimes
- Learn cyber security vulnerabilities and security safeguard.
- Learn hand-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.ErdalOzkaya

❖ **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