15	Cascading style sheet (css) and other manipulations

Assessment Methods

Written tests, assignments, quizzes, presentations as announced by the instructor in the class.

Keywords

network topologies, data communication, OSI model, TCP/IP model, HTML, web design.

Information Security and Cyber Laws (CSGE401) Generic Elective - (GE) Credit: 06

Course Objectives

This course introduces the students to the concepts of information security and different type of attacks in the cyber space. The course also introduces countermeasures to mitigate attacks and different existing cyber laws.

Course Learning Outcomes

On successful completion of the course, students will be able to:

1. Learn, structure, mechanics and evolution of various crime threats
2. Learn to protect information systems from external attacks by developing skills in enterprise security, wireless security and computer forensics.
3. Analyse the risks involved while sharing their information in cyber space and numerous related solutions like sending protected and digitally signed documents
4. Insights of ethical hacking and usage of password cracking tools
5. Get an overview of different ciphers used for encryption and decryption.

Detailed Syllabus

Unit 1

Definitions :Protection, Security, risk, threat, vulnerability, exploit, attack, confidentiality, integrity, availability, non-repudiation, authentication , authorization, codes, plain text, encryption, decryption, cipher text, key, ciphers, Symmetric and asymmetric cryptography, Public key , private key ,Crypt analysis,, Cyber forensics. Substitution cipher (Caesar), Transposition cipher (Rail-Fence),

Unit 2

Risk analysis, process, key principles of conventional computer security, security policies, data protection, access control, internal vs external threat, security assurance, passwords, access control, computer forensics and incident response.

Unit 3

CYBER ATTACKS (definitions and examples): Denial-of-service attacks, Man-in-the-middle attack, Phishing, spoofing and spam attacks, Drive-by attack, Password attack, SQL injection attack, Cross-site scripting attack, Eavesdropping attack, Birthday attack, Malware attacks, Social Engineering attacks

Unit 4

Brief Introduction of handling the attacks described in UNIT 3. Firewalls, logging and intrusion detection systems, e-mail security, security issues in operating systems, ethics of hacking and cracking.

Unit 5

Definitions: Digital Signature and Electronic Signature, Digital Certificate

i. [Section 43] Penalty and compensation for damage to computer etc.
ii. [Section 65] Tampering with computer source documents
iii. [Section 66A] Punishment for sending offensive messages through communication service etc.
iv. [Section 66B] Punishment for dishonestly receiving stolen computer resource or communication device
v. [Section 66C] Punishment for identity theft
vi. [Section 66D] Punishment for cheating by impersonation by using computer resource
vii. [Section 66E] Punishment for violation of privacy
viii. [Section 66F] Punishment for cyber terrorism
ix. [Section 67] Punishment for publishing or transmitting obscene material in electronic form
x. [Section 67A] Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form
xi. [Section 67B] Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form
xii. [Section 72] Breach of confidentiality and privacy

Unit 6

Brief introduction of IT infrastructure in India, National agencies handling IT.

Practical

1. Demonstrate the use of Network tools: ping, ipconfig, ifconfig, tracert, arp, netstat, whois
2. Use of Password cracking tools : John the Ripper, Ophcrack. Verify the strength of passwords using these tools.
3. Perform encryption and decryption of Caesar cipher. Write a script for performing these operations.
4. Perform encryption and decryption of a Rail fence cipher. Write a script for performing these operations.
5. Use nmap/zenmap to analyse a remote machine.
6. Use Burp proxy to capture and modify the message.
7. Demonstrate sending of a protected word document.
8. Demonstrate sending of a digitally signed document.
9. Demonstrate sending of a protected worksheet.
10. Demonstrate use of steganography tools.
11. Demonstrate use of gpg utility for signing and encrypting purposes.

References

1. Merkow, M., & Breithaupt, J.(2005) *Information Security Principles and Practices*. 5th edition. Prentice Hall.

2. Snyder, G.F. (2010). *Network Security*, Cengage Learning.

3. Whitman, M. E. & Mattord, H. J. (2017) *Principles of Information Security*. 6th edition. Cengage Learning.

Additional Resources:

1. Basta, A., & Halton, W., (2010) *Computer Security: Concepts, Issues and Implementation*, Cengage Learning India.

2. Anderson, R. (2008) *Security engineering: A guide to building dependable Distributed Systems*. 2nd edition. John Wiley & Sons.

Web Resources:

1. https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

2. https://www.ibef.org/industry/infrastructure-sector-india.aspx

Course Teaching Learning Process

- Use of ICT tools in conjunction with traditional class room teaching methods
- Interactive sessions
- Class discussions

Tentative weekly teaching plan is as follows:

Week	**Topics**
1-2	Definitions : Protection , Security, risk, threat, vulnerability, exploit, attack, confidentiality, integrity, availability, non-repudiation, authentication, authorization, codes, plain text, encryption, decryption, cipher text, key, ciphers, Symmetric and asymmetric cryptography
3	Public key, private key,Crypt analysis, Cyber forensics. Substitution cipher (Caeser), Transposition cipher (Rail-Fence)
4	Risk analysis, process, key principles of conventional computer security, security policies
5-6	Data protection, access control, internal vs external threat, security assurance, Passwords, access control, computer forensics and incident response
7-8	Cyber attacks, types and examples)
9	Brief Introduction of handling the attacks described in UNIT 3.
10	Firewalls, logging and intrusion detection systems, e-mail security
11	Security issues in operating systems, ethics of hacking and cracking.
12-14	Digital Signature and Electronic Signature, Digital Certificate, Penalty and compensation, Punishment for various attacks
15	Brief introduction of IT security infrastructure in India. National agencies handling IT security.

Assessment Methods

Written tests, assignments, quizzes, presentations as announced by the instructor in the class.

Keywords

Information security, cyber laws, risk analysis, attacks.

5. Generic Elective Courses: Computer Applications for Non Hons Courses

IT Fundamentals (CSGE501) Generic Elective - (GE)

Credit: 06

Course Objectives

This course introduces the students to the basic concepts of computers. The aim is to bridge the fundamental concepts of computers with the present level of knowledge of the students. The course also aims to skill the students so that they can make use of information technology effectively in all walks of life.

Course Learning Outcomes

On successful completion of this course, students will be able to:

1. develop a vocabulary of key terms related to the computer and to software program menus, identify the components of a personal computer system and use the interface deftly.
2. organize files and documents on storage devices.
3. compose, format and edit a word document.
4. use spreadsheet for storing data and performing preliminary analysis.
5. acquire fundamental knowledge of networking and distinguish between different types of networks.
6. acquire knowledge of internet applications and use them.

Detailed Syllabus

Unit 1

Introduction: Introduction to logical organization of computer, input and output devices, keyboard, mouse, joystick, scanner, OCR, OMR, monitor, Printer, Plotter.

Unit 2

Storage Devices: Primary memory, secondary memory, auxiliary memory.

Unit 3

User Interface: Operating system as user interface, system tools, control panel settings.