**Midterm**

**Exam**

**Course Information**

**Program :** B.Sc. Engineering in CSE

**Course Code :** CSE 413

**Course Title :** Cyber Security and Digital Forensic

## Course Credit : 3.00

**Contact Hours :** 3hrs

**Semester :** Fall 2021-22 and Summer 2022

**Intake :** 39

## Section 2

**Prerequisites :** N/A

This course introduces the fundamental concepts of Cyber security and Ethical Hacking. In this course the students get the opportunity to learn about different ethical hacking concepts, web server concepts, Malware, Denial-of-service attacks,Man-in-the-middle attack, Social engineering attacks, Spoofing, Phishing are some common cyber-attacks etc.This course focuses on various forensic tools and techniques in Ethical hacking and security and practically apply some of the tools.

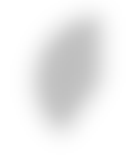
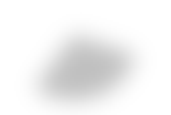
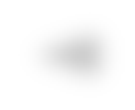
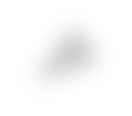
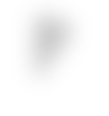
**Course Objectives**

Networking Scanning,Mobile and Web Application Security,Web Servers,Cloud and IoT Security,Cyber Threats and Attacks,Firewall Design principles, VPNs, Worms, Viruses, Security of Network Layer, Security of Application layer protocols, BSD sockets, Elementary and Advanced system calls.

**Course Synopsis**

**Assessment**

|  |  |  |
| --- | --- | --- |
| Class Participation and Quiz | **:** | 10% |
| Assignment/Presentation | **:** | 10% |
| Class Test | **:** | 10% |
| Midterm Examination | **:** | 30% |
| Final Examination | **:** | 40% |



**30%**

**Outcomes (COs)**

**Course**

**Class Test**

**10%**

**Assign/Pres**

**10%**

**Final Exam**

**40%**

**Class Part.**

**10%**

|  |  |  |
| --- | --- | --- |
| After | of this course students will be able to: |  |
| **CO1:** | **Understand** the fundamental aspects of Cyber Security & the nature of secure  software development, operating systems. |  |
| **CO2:** | **Explain** different types of technical specifications of computer systems such as  assemble, disassemble & configure in a secure way. |  |
| **CO3:** | **Analyze** the nature and effect of cybercrime in society & threats posed by cyber  criminals to national infrastructure. |  |
| **CO4:** | **Design** an applications for cyber-attack using various programming language &  apply national laws and regulations for ensuring self-protection. |  |

**Mapping of Course Outcomes (COs) to Program Outcomes (POs)**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| CO | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO8 | PO9 | PO10 | PO11 | PO12 |
| CO1 | √ |  |  |  |  |  |  |  |  |  |  |  |
| CO2 | √ |  |  |  |  |  |  |  |  |  |  |  |
| CO3 |  |  |  |  |  | √ |  |  |  |  |  |  |
| CO4 |  |  | √ |  |  |  |  |  |  |  |  |  |

**Descriptions of Program Outcomes (POs)**

|  |  |
| --- | --- |
| PO1 | **Engineering Knowledge (Cognitive):** Apply the knowledge of mathematics, science,  engineering fundamentals and an engineering specialization to the solution of complex engineering problems. |
| PO2 | **Problem Analysis (Cognitive):** Identify, formulate, research the literature and analyze  complex engineering problems and reach substantiated conclusions using first principles of mathematics, the natural sciences and the engineering sciences. |
| PO3 | **Design/Development of Solutions (Cognitive, Affective):** Design solutions for complex  engineering problems and design system components or processes that meet the specified needs with appropriate consideration for public health and safety as well as cultural,  societal and environmental concerns. |
| PO4 | **Investigation (Cognitive, Psychomotor):** Conduct investigations of complex problems,  considering design of experiments, analysis and interpretation of data and synthesis of information to provide valid conclusions. |
| PO5 | **Modern Tool Usage (Psychomotor, Cognitive):** Create, select and apply appropriate  techniques, resources and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations. |
| PO6 | **The Engineer and Society (Affective):** Apply reasoning informed by contextual  knowledge to assess societal, health, safety, legal and cultural issues and the consequent |

|  |  |
| --- | --- |
|  | responsibilities relevant to professional engineering practice. |
| PO7 | **Environment and Sustainability (Affective, Cognitive):** Understand the impact of  professional engineering solutions in societal and environmental contexts and  demonstrate the knowledge of, and need for sustainable development. |
| PO8 | **Ethics (Affective):** Apply ethical principles and commit to professional ethics,  responsibilities and the norms of the engineering practice. |
| PO9 | **Individual Work and Teamwork (Psychomotor, Affective):** Function effectively as an  individual and as a member or leader of diverse teams as well as in multidisciplinary settings. |
| PO10 | **Communication (Psychomotor, Affective):** Communicate effectively about complex  engineering activities with the engineering community and with society at large. Be able  to comprehend and write effective reports, design documentation, make effective presentations and give and receive clear instructions. |
| PO11 | **Project Management and Finance (Cognitive, Psychomotor):** Demonstrate  knowledge and understanding of the engineering and management principles and apply these to one’s own work as a member or a leader of a team to manage projects in multidisciplinary environments. |
| PO12 | **Life-Long Learning (Affective, Psychomotor):** Recognize the need for and have the  preparation and ability to engage in independent, life-long learning in the broadest  context of technological change. |

# Weekly Schedule

**Teaching-Learning Method:** Lecture, Class Discussion, Discussion Outside Class with Instructor

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Week** | **Lecture** | **Topics** | **Chapter** | **Remarks** | **CO** | **Exam (Mark)** |
| 1 | 1 | **Introduction to Cyber security**: Definition of cyber  security, Key issues plaguing the information security  world, incident management process, and penetration testing. | 01 | CEH | **CO1** |  |
| 2 | **Information Security Terminology:** Hack Value: Notion among hackers that something is worth doing  or interesting | 01 | CEH |
| 3 | **Information Security Terminology:** Vulnerability: Existence of a weakness, design, or implementation error that can  lead to an expected event  compromising the security of the system | 01 | CEH |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 2 | 4 | **Ethical Hacking Concepts, Types, and Phases:**  Hacking: Exploiting system vulnerabilities and compromising security | 04 | CSX | **CO1** | **Mid- Term Exam (30)** |
| 5 | **Information Security Threats and Attack Vectors**:  Viruses and Worms: Capable of infecting a network within seconds | 03 | CSX |
| 6 | **Information Security Threats and Attack Vectors**:  Mobile Threats: Many attackers see mobile phone as a  way to gain access, Botnet: huge network of compromised systems | 01 | CEH |
| 3 | 7 | **Web server Concepts** : Why are web servers  compromised, Improper file/directory permissions | 03 | CSX |
| 8 | **Web server Concepts** : Installing the server with  default settings, Unnecessary services enabled | 03 | CSX |
| 9 | **Webserver Attacks** : Lack of proper security policy,  Improper Authentication, Default Accounts, Bugs in  OS | 03 | CSX | **CO2** |
| 4 | 10 | **Webserver Attacks:** DoS/DDoS Attacks, Phishing  Attacks: | 03 | CEH |
| 11 | **Webserver Attacks** : Man-in-the middle Sniffing  Attack | 05 | CEH |
| 12 | **Webserver Attacks:** Website Defacement: | 05 | CEH |
| 5 | 13 | **Webserver Attacks:** HTTP Responses Splitting  Attack | 02 | CEH |
| 14 | **Web Cache Poisoning:** An attacker forces the web  server’s cache to flush its actual cache content and sends a specially  crafted requests, which will be stored in cache | 06 | CEH |
| 15 | **SSH Brute force Attack:** SSH protocols are used to  create encrypted S  SH Tunnel between two hosts. Attackers can brute force the SSH login credentials | 07 | CEH |
| 6 | 16 | **Webserver Password Cracking:** An attacker tries to  exploit the weaknesses to hack well-chosen passwords (social engineering, spoofing, phishing) ,digital forensic tools | 07 | CEH |
| 17 | **Webserver Attacke** r: Race condition and deadlocks, The heartbleed vulnerability | 18 | CEH |
| 18 | ***Review class for Mid-term Examination: Fall 2019-***  ***20*** |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 7 | 19 | **Mid Term Examination: *Fall 2019-20*** |  |  |  |  |
| 20 |  |  |  |
| 21 |  |  |  |
| 8 | 22 | **Web Server Configuration:** Refers configuration  weaknesses in infrastructure such as directory traversal | 07 | CEH | **CO2** | **Final Exam (40)** |
| 23 | **Hacking Web Applications:**   * Detecting Web App Firewalls and Proxies on target site * Hidden Content discovery: Web spidering automatically finds hidden   content   * Launch web server attack to exploit identified   vulnerabilities, launch DoS | 07 | CEH | **CO3** |
| 24 | **Hacking Web Applications:**   * Cookie Poisoning: by changing info in a cookie, attackers can bypass authentication process * Directory Traversal: Gives access to unrestricted directories * Unvalidated Input: Tempering http request   s, form field, hidden fields, query strings, so on. Example of these attacks include SQL injection, XSS, buffer overflows | 07 | CEH |
| 9 | 25 | **Hacking Web Applications:**   * Cross Site Scripting: Bypassing client-ID mechanisms to gain privileges,   injecting malicious scripts into web pages   * Injection Flaws: Injecting malicious code,   commands, scripts into input gates of flawed apps | 08 | CEH |
| 26 | **Hacking Web Applications** :   * Cross-Site Request Forgery: * Information Leakage * Improper Error Handling | 08 | CEH |
| 27 | **Hacking Web Applications:**   * Log Tampering:   hide their identities   * Buffer Overflow * Broken Session management | 08 | CEH |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 10 | 28 | **Pen Testing:**   * Info Gathering * Config Management Testing * Authentication Testing * Session Management testing | 08 | CEH |  |  |
| 29 | **Pen Testing:**   * Data Validation Testing * DoS Testing * Web Services Testing * AJAX Testing | 08 | CEH |
| 30 | **SQL Injection:** SQL injection is a technique, virtual box security. | 08 | CEH |
| 11 | 31 | **Error based SQL Injection:** Attacker puts  intentional bad input into app to see the database-level error messages. Uses this to create carefully designed SQL Injections | 08 | CEH |
| 32 | **Blind SQL Injection:** Attacker has no error messages  from the system with which to work. Instead, attack simply sends a malicious SQL query to the database | 08 | CEH |
| 33 | Architecture and Design Issues for Web Applications  Top issues need to address with secure design practices Web Application Vulnerabilities due to Bad design, Input Validation | 09 | CEH |
| 12 | 34 | **Designing Secure Web Application:** Authentication,  Authorization | 09 | CEH | **CO4** |
| 35 | **Designing Secure Web Application:** Configuration  Management, Sensitive Data | 09 | CEH |
| 36 | **Designing Secure Web Application:** Session  Management, Cryptography | 10 | CEH |
| 13 | 37 | **Designing Secure Web Application:**  Parameter Manipulation, Exception Management,  Auditing and Logging | 10 | CEH |
| 38 | **Information Security Laws & Standards:** Payment  card Industry Data Security Standard (PCI-DSS) - Payment Systems, Sarbanes Oxley Act (SOX) -Protect investors and public by increasing reliability  of corporate disclosures. | 3 | CSX |
| 39 | Review class for Semester Final Examination |  |  |  |

**Descriptions of Cognitive Domain (Anderson and Krathwohl’s Taxonomy 2001):**

The **cognitive domain** involves the development of our mental skills and the acquisition of

knowledge.

|  |  |  |  |
| --- | --- | --- | --- |
| **Level** | **Category** | **Meaning** | **Keywords** |
| C1 | Remembering | Recognizing or recalling knowledge from memory.  Remembering is when memory is used to produce or retrieve definitions, facts, or lists, or to recite previously learned information. | Define, describe,  draw, find, identify, label, list, match, name, quote, recall,  recite, tell, write |
| C2 | Understanding | Constructing meaning from different types of  functions be they written or graphic messages or activities like interpreting, exemplifying, classifying, summarizing, inferring, comparing, or explaining. | Classify, compare,  exemplify, conclude, demonstrate, discuss, explain, identify,  illustrate, interpret,  paraphrase, predict, report |
| C3 | Applying | Carrying out or using a procedure through executing, or implementing. Applying relates to or refers to situations where learned material is used through products like models, presentations, interviews or simulations. | Apply, change,  choose, compute, dramatize, implement, interview, prepare, produce, role play, select, show, transfer, use |
| C4 | Analyzing | Breaking materials or concepts into parts,  determining how the parts relate to one another or how they interrelate, or how the parts relate to an overall structure or purpose. Mental actions included in this function are differentiating, organizing, and attributing, as well as being able to distinguish between the components or parts. When one is analyzing, he/she can illustrate this mental function by creating spreadsheets, surveys, charts, or diagrams, or graphic representations. | Analyze,  characterize, classify, compare, contrast, debate, deconstruct, deduce, differentiate, discriminate, distinguish,  examine, organize, outline, relate, research, separate,  structure |
| C5 | Evaluating | Making judgments based on criteria and standards  through checking and critiquing. Critiques, recommendations, and reports are some of the products that can be created to demonstrate the processes of evaluation. | Appraise, argue,  assess, choose,  conclude, critique,  decide, evaluate, judge, justify, predict, prioritize, prove, rank,  rate, select, monitor |

|  |  |  |  |
| --- | --- | --- | --- |
| C6 | Creating | Putting elements together to form a coherent or  functional whole; reorganizing elements into a new pattern or structure through generating, planning, or producing. Creating requires users to put parts together in a new way, or synthesize parts into something new and different creating a new form or  product. This process is the most difficult mental function. | Construct, design,  develop, generate, hypothesize, invent, plan, produce,  compose, create, make, perform, plan, produce |

# Teaching Materials/Equipment

## Text Book:

1. CSX Cybersecurity Fundamentals- ISACA

Reference Book:

1. Penetration Testing: A Hands-On Introduction to Hacking
2. CEH module - EC-Council
3. Hacking er golokdhadha – Moniruz Zaman

# Overall Assessment Scheme

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Assessment Area** | **CO** | | | | **Assessment Area Mark** |
|  | **CO1** | **CO2** | **CO3** | **CO4** |  |
| Class Attendance |  |  |  |  | 10 |
| Class Test |  |  |  |  | 10 |
| Assignment/viva voce |  |  |  |  | 10 |
| Midterm Exam | 10 | 10 | 10 |  | 30 |
| Final Exam | 10 | 10 | 10 | 10 | 40 |
| **Total Mark** | **20** | **20** | **20** | **10** | **100** |

**Rubrics**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **COs**  **(Bloom’s Level)** | **Excellent**  **(80%-100%)** | **Good**  **(70%-79%)** | **Satisfactor**  **y (60%-69%)** | **Poor**  **(40%-**  **59%)** | **Unsatisfacto**  **ry**  **(0-39%)** | **Marks**  **(70)** |
| CO1  (Understandi ng) | Answer is  complete and sufficient detail provided to support issues related to the question. And also deals fully with the entire question. | Answer is  brief with sufficient detail provided to support issues were introduced. And most of the basic details are included but some are missing. | Answer is  brief with insufficient detail provided to support issues were introduced. | Answer is  incomplet e and excessive discussion of unrelated issues.  And serious gaps in the basic details. | None of the  relevant details were included or didn’t answer. | **10** |
| CO2  (Explaining) | The question  is answered appropriately explaining the problem solving strategy to a specific programming problem described in the question. | The  question is answered briefly explaining the problem solving strategy to a specific programmin g problem described in the  question. | The  question is answered correctly by the problem solving strategy to a specific programmin g problem described in the question but some points are | The  question is answered incomplet ely explaining the problem solving strategy to a specific programm ing problem described | No attempt  to explain the problem solving strategy to a specific programming problem described in the question method. | **20** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  | missing. | in the  question but some points are correct. |  |  |
| CO3  (Analyzing) | A clear,  complete, and properly ordered chain of analyzing steps (i.e. perceive the problem scenario, relate the problem to the programming perception, explore the programming strategy to solve it) is followed to answer the question. | The chain of  analyzing steps is complete and correctly ordered but lack of some expectedplo ds. | One or more  intermediate analyzing steps are missing or unclear, but the correctness of the analysis is not compromise d. | One or  more intermedia te analyzing steps are missing or unclear to answer the question. | The stated  chain of analysis does not lead to the stated question. | **20** |
| CO4  (Applying) | The answer  shows the complete and appropriate application of conceptual programming  strategies to | The answer  shows appropriate application of conceptual programmin  g strategies | The answer  shows partially appropriate butcomplete application of  conceptual | The  answer shows partially appropriat eapplicati on of  conceptual | The answer  shows the incomplete and inappropriate application | **20** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | solve a  problem. | incompletel  y to solve a problem. | programmin  g strategiesto solve a problem. | programm  ing strategies incomplet ely to solve a problem. | of conceptual  programming strategies to solve a problem. |  |

# Assessment

## Course Evaluation:

|  |  |  |
| --- | --- | --- |
| Class Attendance | **:** | 10% |
| Class Test | **:** | 10% |
| Assignment/viva voce | **:** | 10% |
| Midterm Examination | **:** | 30% |
| Final Examination | **:** | 40% |

**Course Grade:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Numerical Grade** | **Letter Grade** | | **Grade Pont** |
| 80% and above | A+ | (A Plus) | 4.00 |
| 75% to less than 80% | A | (A Regular) | 3.75 |
| 70% to less than 75% | A- | (A Minus) | 3.50 |
| 65% to less than 70% | B+ | (B Plus) | 3.25 |
| 60% to less than 65% | B | (B Regular) | `3.00 |
| 55% to less than 60% | B- | (B Minus) | 2.75 |
| 50% to less than 55% | C+ | (C Plus) | `2.50 |
| 45% to less than 50% | C | (C Regular) | 2.25 |
| 40% to less than 45% | D |  | 2.00 |
| Less than 40% | F |  | 0.00 |

|  |  |
| --- | --- |
| **Instructor In**  **Instructor :** | **formation**  Dr.Dr.Abdullah  Lecturer  Department of Computer Science & Engineering, BUBT |
| **Office :** | Room No-321 (B-1) |
| **Phone :** | 9024266 Ext- 193 |
| **Email :** | Dr.almus@bubt.edu.bd |

|  |  |  |  |
| --- | --- | --- | --- |
| **Class Schedule** | | | |
| **Day** | **Time** | **Room No** |  |
| Sunday | Sunday - CSE 413 - | Room 318(Building 2) -28/1+2 |
| Wednesday | CSE 414 - Room 417 (Building 2) -28/1+2 | Room 417 (Building 2) -28/1+2 |

# Special Instructions

* Students are expected to attend all classes and examinations. A student MUST have at least 70% class attendance to sit for the final exam.
* Students will not be allowed to enter into the classroom after 20 minutes of the starting time.
* For plagiarism, the grade will automatically become zero for that exam/assignment.
* All mobile phones MUST be turned to silent mode during class and exam period.

## Prepared by: Checked by: Approved by: