BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI
WORK INTEGRATED LEARNING PROGRAMMES

COURSE HANDOUT

Part A: Content Design

Course Title	**Cyber Security**
Course No(s)	SS ZG681/SE ZG681
Credit Units	4
Course Author	ASHUTOSH BHATIA
Version No	1.0
Date	23/07/2020

Course Objectives.

No	Objective
CO1	To learn the basic principles of cybersecurity and develop a thorough understanding of confidentiality, integrity, and availability (CIA) triad
CO2	To develop knowledge about cyber security environments and architectures, and to learn about various types of security policies, models, and mechanisms
CO3	To develop a basic understanding about various types of security threats, attacks, and vulnerabilities, and to learn various ways of managing risks involved in cyber security
CO4	To have an overview of various kinds of cybercrimes using malware, ransomware, phishing, hacking, and social engineering; and implementation of various cyber security solutions

Text Book(s)

T1	William Stallings & Lawrie Brown, **Computer Security: Principles and Practice**, 4th Edition, Pearson, 2018
T2	Matt Bishop, **Computer Security**, 2nd Edition, Pearson, 2019

Reference Book(s)

R1	William (Chuck) Easttom II, **Computer Security Fundamentals**, 4th Edition, Pearson, 2020
R2	Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, **Security in Computing**, 5th edition Pearson, 2015
R3	Bill Nelson, A. Philips, F. Enfinger, C. K. Steuart, Guide to Computer Forensics and Investigations, Course Technology (Cengage Learning), Indian edition, 2019.
R4	Joshua B. Hill and Nancy E. Marion, Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century (Praeger Security International) Hardcover – Import, 22 February 2016.

Content Structure

1. **Introduction**
   - 1.1. Fundamentals of Computer Security and Network Security
   - 1.2. CIA Triad
   - 1.3. Threats
   - 1.4. Attacks
   - 1.5. Vulnerabilities.
   - 1.6. Controls.

2. **Security Architecture**
   - 2.1. Overview of Security Policies
   - 2.2. Security Policies – Confidentiality Policies
   - 2.3. Security Policies – Integrity Policies
   - 2.4. Security Policies – Availability Policies
   - 2.5. Security Models
   - 2.6. Security Mechanisms
   - 2.7. Security Risk Analysis and Management
3. **Introduction to Networks and the Internet**
   - 3.1. Network Basics
   - 3.2. How the Internet Works
   - 3.3. History of the Internet
   - 3.4. Basic Network Utilities
   - 3.5. Network Devices
   - 3.6. Advanced Network Communications Topics
4. **Cyber Threat Landscape and Cyber Attacks**
   - 4.1. The Threat Landscape
   - 4.2. Targeted and Un-targeted attacks
   - 4.3. Understanding Vulnerabilities
   - 4.4. Common Cyber Attacks – Stages and Patterns
   - 4.5. Essential Cyber Security Controls
5. **Common Cyber Attacks – Practical Strategies for Identification, Containment and Mitigation**
   - 5.1. Malware Attacks
   - 5.2. Denial of Service Attacks
   - 5.3. Session Hijacking and Man-in-the-Middle Attacks
   - 5.4. Phishing and Spear Phishing Attacks
   - 5.5. SQL Injection Attacks
   - 5.6. Zero Day Exploits
   - 5.7. DNS Tunneling Attacks
6. **Cyber Crimes and Offenses**
   - 6.1. Introduction to Cyber Crimes, motives
   - 6.2. Classification of crimes and criminals
   - 6.3. Cyber Crime Modus-Operandi and Social Engineering
   - 6.4. Cybercrimes against individuals, organizations, and nations
   - 6.5. Cyber Crime Techniques
   - 6.6. Cyber Crime Monitoring and Prevention
7. **Strategic Defense Mechanisms and Defense-in-Depth (DiD)**
   - 7.1. Technical Defense Mechanisms
   - 7.2. Operational, Managerial and Physical Defenses
   - 7.3. Defense-in-Depth Approach and Layered Security Model
8. **Case Studies on Cyber Security**
   - 8.1. Credit Card Skimmer Targets Microsoft ASP.NET sites (July 2020)
   - 8.2. Malicious Google Chrome Extensions (June, 2020)
   - 8.3. Phishing campaigns impersonate popular video conference platforms, Aarogya Setu App and WHO (May, 2020)

Learning Outcomes:

No	Learning Outcomes
LO1	Learn the security landscape, including the nature of the threat, the vulnerabilities, and the probable consequences of failures in security mechanisms
LO2	To acquire the knowledge of computer system misuse and strategic defense against cyber criminals to secure the computer systems and infrastructure
LO3	To analyse and evaluate various case studies related to cyber threats, attacks, and misalignment of security policies in a methodical way.
LO4	Estimate the possible consequences of cyber-attacks and methods to detect, prevent, and recover from the attacks

Part B: Contact Session Plan

Academic Term	First Semester 2023-2024
Course Title	**Cyber Security**
Course No	SS ZG681/SE ZG681
Lead Instructor	ASHUTOSH BHATIA

Course Contents

Contact Session	List of Topics	Reference
01 02	1. **Introduction**: 1.1. Computer Security Concepts 1.2. Threats, Attacks, and Assets 1.3. Security Functional Requirements 1.4. Fundamental Security Design Principles 1.5. Attack Surfaces and Attack Trees 1.6. Computer Security Strategy 1.7. Standards	**T1: Chapter 01**
03 04	2. **Security Architecture: Policies, Models and Mechanisms**: 2.1. Introduction to security policies, models and mechanisms 2.2. The Nature of Security Policies 2.3. Types of Security Policies 2.4. The Role of Trust 2.5. Types of Access Control 2.6. Policy Languages 2.6.1. Example: Academic Computer Security Policy, Security and Precision 2.7. The CIA Classification: 2.7.1. Confidentiality Policies: 2.7.1.1. Goals of Confidentiality Policies, The Bell-LaPadula Model 2.7.2. Integrity Policies: 2.7.2.1. Goals of Integrity Policies, The Biba Model, Lipner's Integrity Matrix Model, Clark-Wilson Integrity Model, Trust Models 2.7.3. Availability Policies: 2.7.3.1. Goals of Availability Policies, Deadlock, Denial of Service Models 2.7.3.2. Example: Availability and Network Flooding Security, Hybrid Models	**T2: Chapter 01, 04, 05, 06, 07, 08**
05	3. **Introduction to Networks and the Internet:** 3.1. Introduction 3.2. Network Basics 3.3. How the Internet Works 3.4. History of the Internet 3.5. Basic Network Utilities 3.6. Other Network Devices 3.7. Advanced Network Communications Topics: 3.7.1. Network communication types 3.7.2. Types of Networks 3.7.3. OSI Model 3.7.4. Network Protocols	**R1: Chapter 2** **R2: Chapter 6 6.1**

06 07	4. **Cyber Threat Landscape and Common Cyber Attacks:** 4.1. The Threat Landscape 4.2. Understanding Vulnerabilities 4.3. Common Cyber Attacks 4.3.1. Stages and Patterns 4.3.2. Targeted and Non-targeted Attacks 4.3.3. Reducing exposure to Cyber Attacks 4.4. Essential Cyber Security Controls 4.4.1. Boundary firewalls and Internet gateways 4.4.2. Secure configuration 4.4.3. Whitelisting and execution control 4.4.4. User access control 4.4.5. Password policy 4.4.6. Content checking	**T1: Chapter 05 5.4** **R2: Chapter 04 4.4** **CERT-UK document**
08 09 10 11	5. **Most Common Cyber Attacks – Practical Strategies for Identification, Containment and Mitigation:** 5.1. Malware Attacks 5.1.1. E.g., Ransomware Attacks 5.2. Denial of Service Attacks 5.3. Session Hijacking and Man-in-the-Middle Attacks 5.4. Phishing and Spear Phishing Attacks 5.5. SQL Injection Attacks 5.6. Zero Day Exploits 5.7. DNS Tunneling Attacks	**T1: Chapter 06, 07, Chapter 10** **T2: Chapter 23** **R1: Chapter 04, 05**
12 13	6. **Cyber Crimes and Offenses:** 6.1. Introduction to Cyber Crimes 6.2. Motives 6.3. Classification of crimes and criminals 6.4. Types, frequency and amount of Cyber Crime 6.5. Organized Cyber Crime 6.6. Cyber terrorism 6.7. Cyber war 6.8. Cyber Crime Modus-Operandi and Social Engineering 6.9. Cybercrimes against individuals, organizations, and nations 6.10. Cyber Crime Techniques 6.11. Cyber Crime Monitoring and Prevention 6.12. Domestic and International Response	**T1: Chapter 19 19.1** **R1: Chapter 03,** **R4: Chapter 03,07,08**
14	7. **Strategic Defense Mechanisms and Defense-in-Depth (DiD):** 7.1. Technical Defense Mechanisms 7.2. Operational, Managerial and Physical Defenses 7.3. Defense-in-Depth Approach and Layered Security Model 7.4. Defense mechanisms like 7.4.1. Encipherment, digital signatures, access control, intrusion detection, authentication exchange, routing control, 7.5. Pervasive mechanisms like 7.5.1. Security audit trail, event detection, security recovery, trusted functionality, anti-malware solutions, VPNs.	**T1: Chapter 02 2.1, 2.2, 2.3, 2.4** **R1: Chapter 08** **R2: Chapter 06 6.6**
15 16	8. **Case Studies on Cyber Security:** 8.1. Credit Card Skimmer Targets Microsoft ASP.NET sites (July 2020) 8.2. Malicious Google Chrome Extensions (June, 2020) 8.3. Phishing campaigns impersonate popular video conference platforms, Aarogya Setu App and WHO (May, 2020),	https://www.cert-in.org.in/

Important Information:

- Assignment questions can be based on self-study syllabus.
- Syllabus for Mid-Semester Test (Closed Book): Topics in CS 1-8.
- Syllabus for Comprehensive Exam (Open Book): All topics given in plan of study

Evaluation Scheme:

Legend: EC = Evaluation Component; AN = After Noon Session; FN = Fore Noon Session

No	Name	Type	Duration	Weight	Day, Date, Session, Time
EC-1	Quiz-1		*	5%	September 1-10, 2023
	Quiz-2		*	5%	October 1-10, 2023
	Assignment		*	10%	November 1-10, 2023
EC-2	Mid-Semester Test	Open Book	2 hours	30%	Sunday, 24/09/2023 (Evening)
EC-3	Comprehensive Exam	Open Book	2 ½ hours	50%	Sunday, 26/11/2023 (Evening)

Notes:

- ✓ The release dates of Quiz-1/2 and assignments will be 5 days (for Quiz) and 10 days (for assignments) before the completion/submission deadline.
- ✓ **Deadlines will NOT be extended for whatever reason** and the student is requested not to wait for the deadline to start working on Quiz/Assignment
- ✓ Syllabus for Quiz-I: Sessions: 1 to 3 / Quiz-II : Session 9 to 12
- ✓ Syllabus for Assignment: Hands-on Python-based Exercise (real-world problem, for individual group of 3 / 4 students). Group formation procedure will be announced before Assignment release
- ✓ All Quiz/Assignments will be released and to be answered/submitted in Canvas LMS
- ✓ Syllabus for Mid-Semester Test (Closed Book): Topics in Session Nos. 1 to 8
- ✓ Syllabus for Comprehensive Exam (Open Book): All topics (Session Nos. 1 to 16)
- ✓ The student is strictly advised to stick to regular schedule of Mid-Sem and Compre examinations, and Makeup examinations will be only for those students with business-related absence/health related issues.
- ✓ Strictly NO MAKEUPS for Quiz and Assignments and all submissions after the above stated deadlines will not be considered/evaluated.
- ✓ All students should conform to BITS students' ethical code-of-conduct and all assignments will be subjected to plagiarism check, and if violated will be subject to disciplinary action apart from nullifying all the marks/grades assigned.

Important links and information:

Canvas LMS: All materials/announcements/discussions forums/Online Quizzes/Assignment submissions will be via Canvas LMS portal. Students are expected to monitor this portal regularly for any content or announcements.

Contact sessions: Students should attend the online lectures as per the schedule provided in the Course Handout (posted on Canvas LMS)

Evaluation Guidelines:

1. EC-1 consists of 2 Quizzes and 1 Assignments. Students will attempt them through the course pages on the Canvas portal. Announcements will be made on the portal, in a timely manner.

2. For Closed Book tests: No books or reference material of any kind will be permitted.

3. For Open Book exams: Use of books and any printed / written reference material (filed or bound) is permitted. However, loose sheets of paper will not be allowed. Use of calculators is permitted in all exams. Laptops/Mobiles of any kind are not allowed. Exchange of any material is not allowed.

4. If a student is unable to appear for the Regular Test/Exam due to genuine exigencies, the student should follow the procedure to apply for the Make-Up Test/Exam which will be made available on the Elearn portal. The Make-Up Test/Exam will be conducted only at selected exam centers.

It shall be the responsibility of the individual student to be regular in attending the contact-session schedule as given in the course handout, and take all the prescribed evaluation components such as Assignment/Quiz, Mid-Semester Test and Comprehensive Exam according to the evaluation scheme provided in the handout