Government Polytechnic, Pune

'180 OB' – Scheme

Programme	**Diploma in Computer Engineering**
Programme code	01/02/03/04/05/**06**/07/08/15/16/17/18/19/21/22/23/24/**26**
Name of Course	**Computer Security**
Course Code	**CM4110**
Prerequisite course code and name	**NA**
Class Declaration	**No**

1. TEACHING AND EXAMINATION SCHEME

Teaching Scheme (In Hours)			Total Credits (L+T+P)		Examination Scheme				
					Theory		Practical		Total Marks
L	T	P	C		ESE	PA	$ESE	PA	
03	00	02	05	Marks	80	20	25	25	150
				Exam Duration	3 Hrs	1 Hr			

Legends: L- Lecture, P- Practical, T- Tutorial, C- Credit, ESE-End Semester Examination, PA- Progressive Assessment (Test I, II/Term Work), *- Practical Exam, $- Oral Exam, #- Online Examination each Lecture/Practical period is of one clock hour

2. RATIONALE

In today's Digital Era, due to various threats, designing security in organization is an important consideration. It is essential to understand basic security principles, various threats to security and techniques to address these threats. The student will be able to recognize potential threats to Computer Security and also able to implement various computer security policies. This course will introduce basic cryptographic techniques, fundamentals of computer/network security, Biometrics, Public Key Infrastructure. It focuses on concepts and methods associated with planning managing and auditing security at all levels including networks.

3. COMPETENCY

The aim of this course is to help the student to attain the following industry identified competency through various teaching learning experiences:

- **Maintain system and network security of organization.**

4. COURSE OUTCOMES (COs)

The theory, practical experiences and relevant soft skills associated with this course are to be taught and implemented, so that the student demonstrates the following industry-oriented COs associated with the above-mentioned competency:

1. Know the basics of Computer Security and identify various software threats and attacks on operating system.
2. Adopt security measures for vital data and identify role of people in security.
3. Apply cryptographic algorithms to maintain Computer Security.
4. Know the procedure to obtain digital certificate and PKI.
5. Apply various Security mechanisms to provide security of network and system.

5. SUGGESTED PRACTICALS/ EXERCISES

Sr. No.	Unit No.	Practical Exercises (Outcomes in Psychomotor Domain)	Relevant CO	Approximate Hours Required.
1.	1	Study of IT Act and Cyber Laws	1	02
2.	2	Install and configure Antivirus software on system (any).	2	02
3.	2	Practice use of data recovery tools	2	04
4.	3	Write a program to implement any Substitution/Transposition Technique.	3	04
5.	3	Install any Cryptographic tool (For. Eg. Cryptool Software)	3	02
6.	3	Perform various Encryption/Decryption techniques using Cryptographic Tool.	3	04
7.	4	Install and Configure firewall settings on any operating system	4	04
8.	4	Create and verify Digital Certificate using tool (e.g., Cryptool)	4	04
9.	5	Trace the origin of email using any tool (e.g., emailTrackerPro)	5	02
10.	5	Trace the path of web site using Tracert Utility	5	02
11.	All	Micro-project (Refer point 11 for micro project list)	All COs	02
		Total Hrs		**32**

S.No.	Performance Indicators	Weightage in %
a.	Correctness of the flow of procedure.	30
b.	Application of basic security design principle and techniques to address threats.	20
c.	Use of various security tools and utilities.	10
d.	Quality of input and output displayed (messaging and formatting)	10
e.	Answer to sample questions	20
f.	Submit report in time	10
	Total	**100**

6. MAJOR EQUIPMENT/ INSTRUMENTSREQUIRED

The major equipment with broad specification mentioned here will usher in uniformity in conduct of practical, as well as aid to procure equipment by authorities concerned**.**

Sr.No.	Major Equipment/ Instruments Required	Experiment Sr. No.
1	Any Anti-Virus Software	2
2	Cryptographic Tool (For. E.g. Cryptool software)	5,6,7
3	Email Tracing Utility (For eg. Email TrakerPro)	8

7. THEORY COMPONENTS

Unit Outcomes (UOs) (in cognitive domain)	Topics and Sub-topics
Unit - I. Introduction to computer security (Weightage -16, Hours-12**)**	
1a. Explain the importance of given pillars of computer security. 1b.Explain the characteristics of given type of threat. 1c.Explain types of attacks related with security.	1.1 Foundations of Computer Security: Definition and Need of computer security, Security basics: Confidentiality, Integrity, Availability, Accountability, Non-repudiation, Reliability, Authentication. 1.2 Risk and Threat Analysis: Assets, Vulnerability, Threats, Risks, Counter measures. 1.3 Threat to Security: Viruses, Phases of Viruses, Types of Virus, Dealing with Viruses, Worms, Trojan horse, Intruders, Insiders, Ransomware. 1.4 Type of attacks: Active and Passive attacks, Denial of service, DDOS, backdoors and trapdoors, sniffing, phishing, spoofing, man in the middle, replay, TCP/IP Hacking, encryption attacks. Steps in Attacks.
Unit - II. User Authentication & Access Control (Weightage-14, Hours-08**)**	
2a. Explain how to construct good/strong password) 2b. Explain the given method of Biometric. 2c. Explain Authentication and Authorization with example. 2d. Describe the features of given access control policy.	2.1 Identification and Authentication: User name & Password, Guessing password, Password attacks-Piggybacking, Shoulder surfing, Dumpster diving 2.2 Biometrics: finger prints, hand prints, Retina, patterns, voice patterns, signature and writing patterns, keystrokes. 2.3 Access controls: Definition, Authentication Mechanism, principle Authentication, Authorization, Audit, Policies: DAC, MAC, RBAC 2.4 Social Engineering.
Unit - III. Cryptography (Weightage- 20 , Hours- 12**)**	
3a. Define terms related to cryptography. 3b. Encrypt/Decrypt the given text using different substitution/transposition techniques. 3c. Describe various encryption algorithms 3d. Explain Hashing with properties.	3.1 Introduction: Plain Text and Cipher Text, Cryptography, Cryptanalysis, Cryptology, Encryption, Decryption. 3.2 Substitution techniques: Caesar's cipher, mono alphabetic, poly alphabetic, Vigenere cipher 3.3 Transposition techniques: Rail fence technique, simple columnar, Vernam Cipher (One-Time Pad) 3.4 Steganography: Procedure, Hashing: Definition , Hashing Algorithms: MD-5, SHA 3.5 Symmetric and Asymmetric cryptography: Introduction to Symmetric encryption, DES (Data encryption Standard) algorithm, Asymmetric key cryptography: Digital Signature

Unit Outcomes (UOs) (in cognitive domain)	Topics and Sub-topics
Unit - IV. Public Key Infrastructure (Weightage-14, Hours- 08**)**	
4a. Explain working of PKI. 4b. Describe Public Key Infrastructure 4c. Describe steps for obtaining digital certificate 4d. Explain digital certificate life cycle	4.1 Public key infrastructures: basics, digital certificates, certificate authorities, registration authorities 4.2 Steps for obtaining a digital certificate 4.3 Trust and certificate verification 4.4 Digital certificates: certificate attributes, certificate extensions 4.5 Certificate life cycles: registration & generations, renewal, revocation, CRL distribution, suspension, key destruction 4.6 Centralized and decentralized infrastructure
Unit - V. System Security & Network Security (Weightage-16, Hours-08**)**	
5a. Explain need of firewalls. 5b. Explain Intrusion Detection system. 5c. Classify IDS techniques. 5d. Explain different ways to implement IP Security 5e. Explain protocols related to Email security	5.1 Firewall: Need of firewall, types of firewall- packet filters, application gateways, circuit gateways 5.2 Kerberos. Intrusion Detection: Network-Based IDS, Host-Based IDS 5.3 Honeypots. 5.6 Operating system security: Operating system updates : hot fix, patch, service pack 5.7 IP security: overview, Protocols- AH, ESP, Modes- transport & Tunnel 5.8 Email security: SMTP, PEM, and PGP.

8. SUGGESTED SPECIFICATION TABLE FORQUESTION PAPER DESIGN

Unit No.	Unit Title	Teaching Hours	Distribution of Theory Marks			
			R Level	U Level	A Level	Total Marks
I	Introduction to computer security	12	06	06	04	16
II	User Authentication & Access Control	08	04	06	04	14
III	Cryptography	12	04	08	08	20
IV	Public key infrastructure	08	04	06	04	14
V	Network Security and System Security	08	04	06	06	16
Total		48	**22**	**32**	**26**	**80**

9. SUGGESTED STUDENT ACTIVITIES

Other than the classroom and laboratory learning, following are the suggested student-related ***co-curricular*** activities which can be undertaken to accelerate the attainment of the various outcomes in this course: Students should conduct following activities in group and prepare reports of about 5 pages for each activity, also collect/record physical evidences for their (student's) portfolio which will be useful for their placement interviews:

a. Prepare journal of practicals.
b. Use Cryptographic Tools and Utilities.

10. SUGGESTED SPECIAL INSTRUCTIONAL STRATEGIES (if any)

These are sample strategies, which the teacher can use to accelerate the attainment of the various outcomes in this course:

a. Massive open online courses (***MOOCs***) may be used to teach various topics/sub topics.
b. About ***15-20% of the topics/sub-topics*** which is relatively simpler or descriptive in nature is to be given to the students for ***self-directed learning*** and assess the development of the COs through classroom presentations.
c. With respect to item No.9, teachers need to ensure to create opportunities and provisions for ***co-curricular activities***.
d. Use different Audio-Visual media for Concept understanding.
e. Guide student(s) in undertaking micro-projects.
f. Demonstrate students thoroughly before they start doing the practice.
g. Observe continuously and monitor the performance of students in Lab.

11. SUGGESTEDMICRO-PROJECTS

Only one micro-project is planned to be undertaken by a student that needs to be assigned to him/her. In special situations where groups have to be formed for micro-projects, the number of students in the group should ***not exceed three.***The micro-project could be industry application based, internet-based, workshop-based, laboratory-based or field-based. Each micro-project should encompass two or more COs which are in fact, an integration of PrOs, UOs and ADOs. (Affective Domain Outcomes). Each student will have to maintain activity chart consisting of individual contribution in the project work and give a seminar presentation of it before submission. The student ought to submit micro-project by the end of the semester to develop the industry-oriented COs.

A suggestive list of micro-projects is given here. Similar micro-projects could be added by the concerned faculty:

a. Study of any Real Case of Malware Attacks:
    i. Understand Computer Virus and Malware Attack
    ii. Analyze Phases of Virus
    iii. Study and Analyze any Real Case of Malware Attacks for. eg CryptoLocker , ransomware, 2013, ILOVEYOU, worm, 2000,11. Melissa, virus, 1999 etc

b. Study and Analyze Small Business Cyber security Case Study:
    i. Understand the type of attack,
    ii. Analyze the Response and Impact of the attack

iii. Find Preventive /curative measures against damages by attack

c. Study and analyze Social Site cyber attack case study:
   i. Understand the type of attack,
   ii. Analyze the Response and Impact of the attack
   iii. Find Preventive /curative measures against damages by attack

d. Any other Relevant Case Study of Student's / Faculty's Choice.

12. SUGGESTED LEARNING RESOURCES

S.N.	Title	Author	Publisher, Edition and Year of publication, ISBN Number
1	Principles of computer security Security+and Beyond	Wm.Arthur Conklin Dwayne Williams Gregory B. White Roger L.Davis Chuck Cothren,	McGraw Hill Technology Education International Edition2005 • ISBN-13: 978-0072255096 • ISBN-10: 0072255099
2	Cryptography And Network Security	Behrouz A Forouzan, De Anza College, Deepak Mukopadhay	McGraw Hill Technology Education International 2nd Edition • ISBN- 9780070702080.
3	Computer Security Third Edition	Dieter Gollmann	Wiley Publication • ISBN : 978-0-470-74115-3
4	Cryptography and Network Security Third Edition	Atul Kahate	McGraw Hill Education, New Delhi • ISBN 13: 978-1-25-902988-2

13. SOFTWARE/LEARNING WEBSITES

1. https://www.tutorialspoint.com//computer_security/computer_security_quick_guide.htm
2. https://freevideolectures.com/course/3027/cryptography-and-network-security
3. https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_process.htm
4. https://www.cybrary.it/
5. https://www.tutorialspoint.com/cryptography/index.htm
6. https://www.geeksforgeeks.org/ip-security-ipsec/
7. https://www.open.edu/openlearn/ocw/mod/oucontent/view.php?id=48325&section=1

14. PO - COMPETENCY- CO MAPPING

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	2	-	-	-	3	-	2
CO2	2	3	2	-	3	1	3
CO3	3	3	3	3	3	3	2
CO4	2	1	2	2	3	1	2
CO5	2	3	3	1	2	2	2

	PSO1	PSO2
CO1	-	1
CO2	1	2
CO3	-	3
CO4	1	2
CO5	3	3

Sign: Name: Smt. S.P. Ambavane Smt. K. S. Sathawane (Course Expert /s)	Sign: Name: Shri.U. V. Kokate Dr.S.B.Nikam (Head of Department) (Department of Computer Engineering)
Sign: Name: Shri.U. V. Kokate Dr.S.B.Nikam (Programme Head) (Department of Computer Engineering)	Sign: Name: Shri A.S.Zanpure (CDC Incharge)