<u>Course Plan</u>

B.E. (ECS) (Semester VIII)

Subject name: System security

Subject code: ECCDO802

Teacher-in-charge: Prajakta Bhangale **Academic Term: 2022-2023**

Module No.	Unit No	Contents	Hrs.
1		**The Need for System Security**	04
	1.1	Risks, Threats, and Vulnerabilities,Tenets of Information Systems Security (Confidentiality,Integrity ,Availability)	
	1.2	Malicious Attack Birthday Attacks ,Brute-Force Password Attacks ,Dictionary Password Attacks, IP Address Spoofing,Hijacking ,Replay Attacks ,Man-in-the-Middle Attacks Masquerading ,Eavesdropping ,Social Engineering, Phreaking ,Phishing ,Pharming .	
2		**Cryptography**	06
	2.1	Cryptography : Overview of Cryptography : What is cryptography , encryption and decryption techniques ,Symmetric and asymmetric key cryptography : AES, DES, RSA, Knapsack cryptosystem.	
3		**Network Security**	09
	3.1	Firewall: Need of Firewall, types of firewall- Packet Filters, Stateful Packet Filters, Application Gateways, Circuit gateways. Firewall Policies, Configuration, limitations, DMZ, VPN.	
	3.2	Intrusion Detection System Vulnerability Assessment, Misuse detection, Anomaly Detection, Network Based IDS, Host-Based IDS, Honeypots	
	3.3	Kerberos: Working, AS, TGS, SS	
	3.4	IP Security- Overview, Protocols- AH, ESP, Modes- transport and Tunnel.	
	3.5	Public key infrastructure Introduction, Certificates, (PKI): Certificate Authority, authority, Registration	
	3.6	X.509/PKIX certificate format.	
	3.7	Basic concepts of SNMP, SNMPv1 Community facility and SNMPv3	
4		**Web Security**	07
	4.1	Web Security Considerations, User Authentication and Session Management, Cookies, SSL, HTTPS, SSH, Privacy on Web, Web Browser Attacks, Account	

		Harvesting, Web Bugs, Clickjacking, CrossSite Request Forgery, Session Hijacking and Management, Secure Electronic Transaction, Email Attacks, DNS Attacks, Web Service Security.	
5		**Infrastructure Security**	09
	5.1	Physical Security: Managerial, Technical And Physical Controls, Environmental Exposures And Controls, Physical Access Controls	
	5.2	Wireless network Security: IEEE 802.11xWireless LAN Security, Wireless Intrusion Detection System (WIDS)	
	5.3	Mobile Security: Security Threats, Device Security, Cloud Security: Cloud Security Risks and Countermeasures, Cloud Identity and Access Management, Cloud Security as a Service, SAML, OAuth	
	5.4	IOT Security: IoT Concepts, IoT Attacks, IoT Hacking Methodology, IoT Hacking Tools, IoT Countermeasures	
6		**Security Auditing and Analysis**	04
	6.1	How to define your audit plan? What auditing benchmarks are ? How to collect audit data? Which post-audit activities you need to perform? How to perform security monitoring? Which types of log information you should capture? How to verify security controls ? • How to monitor and test your security systems?	
		Total	39

Course Objectives:

1. To understand the fundamentals of system security.
2. To explore the working principles and utilities of various crypto algorithms including Secret key Cryptography and public key algorithms
3. To understand the various controls available for protection against internet attacks, including integrity check, firewalls, intruder detection systems.
4. To understand, and evaluate different attacks on Open Web Applications and Web services
5. To describe the mechanisms used to provide security in different infrastructure and networks.
6. To perform Security Auditing and Analysis

Course Outcomes:

At the end of the course student will be able to

1. Understand the concept of vulnerabilities, attacks and protection mechanisms and working of various crypto algorithms.
2. Analyze various controls available for protection against internet attacks.
3. Evaluate different attacks on Open Web Applications and Web services
4. Analyze mechanisms used to provide security in different infrastructure and networks
5. Perform security monitoring and testing of system

CO-PO-PSO Mapping:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	2	2						1						
CO2	1	2	2					2						
CO3		2	2					2						
CO4	2							1						
CO5	1	2						2						1

CO-PO Mapping:(BL – Bloom's Taxonomy, C – Competency, PI – Performance Indicator)

Example:

CO	BL	C	PI	PO
ECC602.1	2	1.2 1.3 1.4	1.2.1 1.3.1 1.4.1	PO1
		2.1	2.1.1 2.1.2 2.1.3 2.1.4	PO2
		8	8.1.1	PO8
ECC602.2	3	1.1 1.2 1.3 1.4	1.1.1 1.2.1 1.3.1 1.4.1	PO1
		2.1	2.1.3 2.1.4	PO2
		3.2	3.2.1 3.2.2	PO3

		4.4 4.5 4.6	4.4.2 4.5.1 4.6.1	PO4
	8	8.1	8.1.1	
ECC602.3	3	1.2 1.3 1.4	1.2.1 1.3.1 1.4.1	PO1
		2.1 2.2	2.1.1 2.1.3 2.2.2 2.2.3 2.2.4	PO2
		3.2	3.2.1	PO3
		4.2	4.2.1	PO4
	8	8.1	8.1.1	
ECC602.4	3	1.1 1.2 1.3 1.4	1.1.1 1.2.1 1.3.1 1.4.1	PO1
		2.4	2.4.1	PO2
ECC602.5	1	1.2 1.3 1.4	1.2.1 1.3.1 1.4.1	PO1
	2	2.1 2.2	2.2.3 2.1.3	PO2
	9	9.1	9.1.1 9.1.2	PO9
	8	8.2	**8.2.2**	PO8

Provide justification of PO to CO mapping

CO1	PO1	Students will apply basic engineering laws and concepts to understand real world problems in System security
	PO2	Understand the difference between various attacks and impacts of it.
	PO3	Apply knowledge to solve real world problem.
CO2	PO1	Students will apply basic engineering laws and concepts to understand real world problems and various countermeasures in System security

	PO2	Understand difference between various technologies for protection mechanism
	PO3	students will able to explore alternate solution for given real word problem
CO3	PO1	Students will apply basic engineering laws and concepts to solve real world problems in System security
	PO2	Various attacks on web applications will be identified based on scenario.
	PO3	students will able to explore alternate solution for given real word problem
	PO4	Students will able to Examine relevant methods, tools and techniques of experiment design,data acquisition, analysis and presentation in web app. attacks
CO4	PO2	Understand difference between various technologies for protection mechanism
CO5	PO1	Engineering Principles in expert system for a given real world problem will be understood.
	PO2	Students will compare existing working principles of Intelligent agents algorithms with expert system.
	PO9	Recognize a variety of working and learning preferences; appreciate the value ofdiversity on a team and Implement the norms of practice (e.g. rules, roles, charters, agendas,etc.) ofeffective team work, to accomplish a goal byProject of Auditing website or any application.

CO Assessment Tools:

Course Outcome	***Assessment Method***							
	Direct Method (80 %)							***Indirect Method (20%)***
	Unit Tests		**Quizzes**		**Activity(Auditing report)**	**University Results**		**Course exit survey**
	1	2	1	2		**Theory**	**Oral/Pract.**	
CO1	20	-	10	-	10	30	30	100
CO2	20	-	10	--	10	30	30	100
CO3	-	20	-	10	10	30	30	100
CO4	-	20	-	10	10	30	30	100
CO5	-	20	-		20	30	30	100

CO calculation= (0.8 *Direct method + 0.2*Indirect method)

Rubrics for Auditing report

Indicator	Very Poor	Poor	Average	Good	Excellent
On time Submission (2)	Assignment not submitted (0)	More than two session late (0.5)	Two sessions late (1)	One session late (1.5)	Early or on time (2)
Organization (2)	N/A	Very poor readability and not structured (0.5)	Poor readability and somewhat structured (1)	Readable with one or two mistakes and structured (1.5)	Very well written and structured without any mistakes (2)
Level of content (4)	N/A	Major points are omitted / addressed minimally (1)	All major topics are covered, the information is accurate. (2)	Most major and some minor criteria are included. Information is Accurate (3)	All major and minor criteria are covered and are accurate. (4)
Depth and breadth of discussion (2)	N/A	None in evidence; superficial at most (0.5)	Minor points/information may be missing and discussion is minimal (1)	Discussion centers on some of the points and covers them adequately (1.5)	Information is presented in depth and is accurate (2)

Content beyond syllabus:

Curriculum gap:

Modes of content delivery

Modes of Delivery	**Brief description of content delivered**	**Attained COs**	**Attained Pos**
Class room lecture	Lectures are taken online and offline both modes as per Timetable		
Online videos Assignments/ Quiz	Quiz 1 Quiz 2 Activity of Audit report		

Text Books:

1. Computer Security Principles and Practice, William Stallings, Sixth Edition, Pearson Education
2. Security in Computing, Charles P. Pfleeger, Fifth Edition, Pearson Education .
3. Fundamentals of Information system security, Third Edition, David Kim,Michael G. Solomon
4. Jones & Bartlett Learning
5. Network Security and Cryptography, Bernard Menezes, Cengage Learning
6. Network Security Bible, Eric Cole, Second Edition, Wiley

Reference Books:

1. Web Application Hackers Handbook by Wiley.
2. . Information Security The Complete Reference, 2nd Edition ,Mark Rhodes-Ousley,McGraw Hill Education
3. Computer Security, Dieter Gollman, Third Edition, Wiley
4. CCNA Security Study Guide, Tim Boyle, Wiley
5. Introduction to Computer Security, Matt Bishop, Pearson.
6. Cloud Security and Privacy, Tim Mather, Subra Kumaraswamy, Shahed Latif ,O’Reilly

Lectures	3 per week	
	Hours	Marks
Theory examination	3	80
Internal Assessment	-	20
Total	--	100

Day	Time
Tuesday	09.00-10.00pm
Wednesday	09.00-10.00pm
Thursday	09.00-10.00pm

Lecture No.	Dates		Topic	Remarks
	Planned	Actual		
1	11/1	11/1	Risks, Threats, and Vulnerabilities,Tenets of Information Systems Security (Confidentiality,Integrity ,Availability)	
2	12/1	12/1	alicious Attack Birthday Attacks ,Brute-Force Password Attacks ,Dictionary Password Attacks	
3	13/1	13/1	, IP Address Spoofing,Hijacking ,Replay attacks ,Man-in-the-Middle Attack	
4	18/1	18/1	Masquerading ,Eavesdropping ,Social Engineering,Phreaking ,Phishing ,Pharming .	
5	19/1	19/1	Cryptography : Overview of Cryptography : What is cryptography ,encryption and decryption techniques ,Symmetric and asymmetric key cryptography	
6	20/1	20/1	AES	
7	24/1	24/1	DES	
8	25/1	25/1	RSA	
9	26/1	26/1	Knapsack	
10	31/1	31/1	firewall: Need of Firewall, types of firewall- Packet Filters, Stateful Packet Filters, Application Gateways, Circuit gateways. Firewall Policies, Configuration, limitations, DMZ, VPN.	
11	1/2	1/2	Intrusion Detection System Vulnerability Assessment, Misuse detection,	

			Anomaly Detection, Network Based IDS, Host-Based IDS, Honeypots	
12	2/2	2/2	Kerberos: Working, AS, TGS, SS	
13	7/2	7/2	Kerberos: Working, AS, TGS, SS	
14	8/2	8/2	Public key infrastructure Introduction, Certificates, (PKI): Certificate Authority, authority, Registration	
15	9/2	9/2	X.509/PKIX certificate format.	
16	14/2	14/2	Basic concepts of SNMP, SNMPv1 Community facility and SNMPv3	
17	15/2	15/2	IP Security- Overview, Protocols- AH, ESP,.	
18	16/2	16/2	Modes- transport and Tunnel.	
19	21/2	21/2	Basic concepts of SNMP, SNMPv1 C	
20	22/2	22/2	Basic concepts of SNMP, SNMPv1 Community facility and SNMPv3	
21	23/2	23/2	Web Security Considerations, User Authentication and Session Management	
22	8/3	/3	Cookies, SSL, HTTPS, SSH, Privacy on Web, Web Browser Attacks, Account Harvestin	
23	9/3	9/3	Web Bugs, Clickjacking, CrossSite Request Forgery, Session	
24	14/3	14/3	Email Attacks, DNS Attacks, Web Service Security.	
25	15/3		Quiz1	
26	16/3		Hijacking and Management, Secure Electronic Transaction,	
27	21/3		Physical Security: Managerial, Technical And Physical Controls, Environmental Exposures And Controls, Physical Access Controls	
28	23/3		Wireless network Security: IEEE 802.11xWireless LAN Security, Wireless Intrusion Detection System (WIDS)	
29	28/3		Mobile Security: Security Threats, Device Security, Cloud Security: Cloud Security Risks and Countermeasures, Cloud Identity and Access Management, Cloud Security as a Service, SAML, OAuth	

30	29/3		IOT Security: IoT Concepts, IoT Attacks, IoT Hacking Methodology, IoT Hacking Tools, IoT Countermeasures	
31	5/4		How to define your audit plan? What auditing benchmarks are ? How to collect audit data? Which post-audit activities you need to ?	
32	6/4		How to perform security monitoring? Which types of log information you should capture? How to verify security controls ? • How to monitor and test your security systems	
33	11/4		Activity on Auditing	
34	12/4		Activity on Auditing	
35	13/4		Guest Lecture	
36	13/4			

Examination Scheme

Module		Lec e Hou	Marks distribution in Test (For internal assessment/TW)		Approximate Marks distribution in Sem. End Examination
			Test 1	Test 2	
1	**The Need for System Securit(CO1**	3	5		10
2	**Cryptography(CO2)**	5	5		10
3	**Network Security(CO2)**	12	10		20
4	**Web Security(CO3)**	10		10	20
5	**Infrastructure Security(CO4)**	5		5	10
6	**Security Auditing and Analysis(CO5)**	5		5	10

Submitted By	Approved By
Sign:	Sign:
Date of Submission:	Date of Approval:
Remarks by PAC (if any):	