Practical Plan

Branch: Computer Engineering
Semester: VI **Year: 2022-23**

Course Title: Cryptography and System Security lab (CSL602)	SEE: 2 Hours – Practical
Total Contact Hours: 20 Hours	
Practical Plan Author: Prof. Monali Shetty	Date: 5-1-23
Checked By: Dr. Sujata Deshmukh	Date:9-1-23

Prerequisites: Computer Networks

Course Outcomes (CO):

On successful completion of course learner will be able to:

CSL602.1	Apply knowledge of cryptographic techniques to implement simple cipher.
CSL602.2	Explore different network reconnaissance, and packet sniffing tools to gather information about networks, and packets, respectively.
CSL602.3	Explore various attacks on the system security.
CSL602.4	Set up firewalls and explore email security.

List of Experiments		
Sr. No.	***Title***	***Attained COs***
1	Design and Implementation of a product cipher using Substitution and Transposition ciphers	CSL602.1
2	Implementation of Diffie- Hellman Key exchange algorithm	CSL602.1
3	Implementation and analysis of RSA cryptosystem.	CSL602.1
4	Download and install nmap. Use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, xmas scan etc	CSL602.2
5	For varying message sizes, test integrity of message using MD-5, SHA-1, and analyse the performance of the two protocols	CSL602.1
6	Study of packet sniffer tools: Wireshark to explore how the packets can be traced based on different filters like ICMP, TCP, and HTTP	CSL602.2
7	Implementation of Salt and Pepper password protection technique	CSL602.1
8	Explore GPG tool of Linux to implement email security.	CSL602.4
9	Simulation of SQL injection attack	CSL602.3
10	Case study/Presentation/Project	CSL602.1 CSL602.2 CSL602.3
Newly Added Experiments		
1	Explore GPG tool of Linux to implement email security.	

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

CO	BL	C	PI	PO	Mapping
CSL602.1.	3	2.4	2.4.1 2.4.2	PO2	1
		5.2	5.2.2	PO5	1
		6.1	6.1.1	PO6	3
		8.1	8.1.1	PO8	2
		9.1	9.1.1	PO9	3
		9.1	9.1.2		
		9.2	9.2.1		
		9.2	9.2.2		
		9.2	9.2.3		
		9.2	9.2.4		
		10.2	10.2.1	PO10	2
		10.2	10.2.2		
		12.3	12.3.1	PO12	2
		12.3	12.3.2		
CSL602.2.	2, 3	5.2	5.2.2	PO5	1
		6.1	6.1.1	PO6	3
		8.1	8.1.1	PO8	2
		9.1	9.1.1	PO9	3
		9.1	9.1.2		
		9.2	9.2.1		
		9.2	9.2.2		
		9.2	9.2.3		
		9.2	9.2.4		
		10.2	10.2.1	PO10	2
		10.2	10.2.2		
		12.3	12.3.1	PO12	2
		12.3	12.3.2		
CSL602.3.	3	5.2	5.2.2	PO5	1
		6.1	6.1.1	PO6	3
		8.1	8.1.1	PO8	2
		9.1	9.1.1	PO9	3
		9.1	9.1.2		
		9.2	9.2.1		
		9.2	9.2.2		
		9.2	9.2.3		
		9.2	9.2.4		
		10.2	10.2.1	PO10	2
		10.2	10.2.2		
		12.3	12.3.1	PO12	2
		12.3	12.3.2		
CSL602.4.	3	5.2	5.2.2	PO5	1
		6.1	6.1.1	PO6	3

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CSL602.1		1			1							
CSL602.2					1	1						
CSL602.3					1	1						
CSL602.4					1	1						

CO-PSO Mapping:

CO	BL	C	PI	PO	Mapping
CSL602.2.	2, 3	2.2	2.2.1	PSO2	1
CSL602.3.	3	2.2	2.2.1	PSO2	1
CSL602.4.	3	2.3	2.3.3	PSO2	1

	PSO1	PSO2
CSL602.1.	--	--
CSL602.2.	--	1
CSL602.3.	--	1
CSL602.4.	--	1

Competencies and PIs for POs	
2.4 Demonstrate an ability to execute a solution process and analyze results	2.4.1 Applies engineering mathematics to implement the solution. 2.4.2 Analyze and interpret the results using contemporary tools.
5.2 Demonstrate an ability to select and apply discipline-specific tools, techniques and resources	5.2.2 Demonstrate proficiency in using discipline-specific tools
6.1 Demonstrate an ability to describe engineering roles in a broader context, e.g. pertaining to the environment, health, safety, legal and public welfare	6.1.1 Identify and describe various engineering roles; particularly as pertains to protection of the public and public interest at the global, regional and local level
8.1 Demonstrate an ability to recognize ethical dilemmas	8.1.1 Identify situations of unethical professional conduct and propose ethical alternatives
8.2 Demonstrate an ability to apply the Code of Ethics	8.2.2 Examine and apply moral & ethical principles to known case studies
9.1 Demonstrate an ability to form a team and define a role for each member	9.1.1 Recognize a variety of working and learning preferences; appreciate the value of diversity on a team 9.1.2 Implement the norms of practice (e.g. rules, roles, charters, agendas, etc.) of effective team work, to accomplish a goal.
9.2 Demonstrate effective individual and team operations–communication, problem-solving, conflict resolution and leadership skills	9.2.1 Demonstrate effective communication, problem-solving, conflict resolution and leadership skills 9.2.2 Treat other team members respectfully 9.2.3 Listen to other members 9.2.4 Maintain composure in difficult situations
10.1 Demonstrate an ability to comprehend technical literature and document project work	10.1.1 Read, understand and interpret technical and non-technical information 10.1.2 Produce clear, well-constructed, and well-supported written engineering documents 10.1.3 Create flow in a document or presentation – a logical progression of ideas so that the main point is clear
10.2 Demonstrate competence in listening, speaking, and presentation	10.2.1 Listen to and comprehend information, instructions, and viewpoints of others

	10.2.2 Deliver effective oral presentations to technical and non-technical audiences
12.3 Demonstrate an ability to identify and access sources for new information	12.3.1 Source and comprehend technical literature and other credible sources of information 12.3.2 Analyze sourced technical and popular information for feasibility, viability, sustainability, etc.
Competencies and PIs for PSOs	
2.2 Demonstrate an ability to identify potential threats and attacks to the information technology assets.	2.2.1 Analyse the static and web vulnerabilities.
2.3 Demonstrate an ability to identify tools and measures to protect the assets from cyber-attacks.	2.3.3 Choose appropriate tools and methods to protect the assets from cyber-attacks.

CO Measurement Weightages for Tools:

Course Outcomes	***Direct Methods (80%)***				***Indirect Method (20%)***
	Lab Performance	Assignments/Post Lab Questions	Quizzes	End Sem Exam (TW)	Course exit survey
CSL602.1	30%	10%	10%	50%	100%
CSL602.2	30%	10%	10%	50%	100%
CSL602.3	30%	10%	10%	50%	100%
CSL602.4	30%	10%	10%	50%	100%

Attainment:

CO CSL602.1:

Direct Method

$$A_{\text{CSL602.1}D} = 0.3 * Lab\ Performance + 0.1 * Assignment/Post\ Lab + 0.1 * Quizzes + 0.6 * SEE\_TW$$

Final Attainment:

$$A_{\text{CSL602.1}} = 0.8 * A_{\text{CSL602.1}D} + 0.2 * A_{\text{CSL602.1}I}$$

CO CSL602.2:

Direct Method

$$A_{\text{CSL602.2}D} = 0.3 * Lab\ Performance + 0.1 * Assignment/Post\ Lab + 0.1 * Quizzes + 0.6 * SEE\_TW$$

Final Attainment:

$$A_{\text{CSL602.2}} = 0.8 * A_{\text{CSL602.2}D} + 0.2 * A_{\text{CSL602.2}I}$$

CO CSL602.3:

Direct Method

$$A_{\text{CSL602.3}D} = 0.3 * Lab\ Performance + 0.1 * Assignment/Post\ Lab + 0.1 * Quizzes + 0.6 * SEE\_TW$$

Final Attainment:

$$A_{\text{CSL602.3}} = 0.8 * A_{\text{CSL602.3}D} + 0.2 * A_{\text{CSL602.3}I}$$

CO CSL602.4:

Direct Method

$$A_{\text{CSL602.4}D} = 0.3 * Lab\ Performance + 0.1 * Assignment/Post\ Lab + 0.1 * Quizzes + 0.6 * SEE\_TW$$

Final Attainment:

$$A_{\mathrm{CSL602.4}} = 0.8 * A_{\mathrm{CSL602.4}D} + 0.2 * A_{\mathrm{CSL602.4}I}$$

Resourses:

1. https://www.youtube.com/watch?v=FvstbO787Qo
2. https://www.tutorialspoint.com/nmap-cheat-sheet

Practical Session Plan

Batch	***Dates***		***Remarks***
	Planned	***Actual***	
Experiment No. 1 Design and Implementation of a product cipher using Substitution and Transposition ciphers			
A	25/01/2023	25/01/2023	
B	24/01/2023	24/01/2023	
C	23/01/2023	23/01/2023	
D	27/01/2023	27/01/2023	
Experiment No. 2 Implementation of Diffie- Hellman Key exchange algorithm			
A	01/02/2023	01/02/2023	
B	31/01/2023	31/01/2023	
C	30/01/2023	30/01/2023	
D	03/02/2023	03/02/2023	
Experiment No. 3 Implementation and analysis of RSA cryptosystem.			
A	08/02/2023	08/02/2023	
B	07/02/2023	07/02/2023	
C	06/02/2023	06/02/2023	
D	10/02/2023	10/02/2023	
Experiment No. 4 Download and install nmap. Use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, xmas scan etc			
A	15/02/2023	15/02/2023	
B	14/02/2023	14/02/2023	
C	13/02/2023	13/02/2023	
D	17/02/2023	17/02/2023	
Experiment No.5 For varying message sizes, test integrity of message using MD-5, SHA-1, and analyze the performance of the two protocols			
A	22/02/2023	22/02/2023	
B	21/02/2023	21/02/2023	
C	20/02/2023	13/03/2023	
D	24/02/2023	24/02/2023	
Experiment No. 6 Implementation of Salt and Pepper password protection technique.			
A	08/03/2023	08/03/2023	
B	14/03/2023	21/02/2023	
C	13/03/2023	13/03/2023	
D	03/03/2023	17/03/2023	
Experiment No. 7 Study the use of network reconnaissance tools like WHOIS, dig, traceroute, ns lookup to gather information about networks and domain registrars.			

A	15/03/2023	15/03/2023	
B	21/03/2023	14/03/2023	
C	20/03/2023	13/03/2023	
D	10/03/2023	24/03/2023	
Experiment No. 8 Explore GPG tool of Linux to implement email security.			
A	29/03/2023	5/4/2023	
B	28/03/2023	28/03/2023	
C	27/03/2023	3/4/2023	
D	17/03/2023	12/04/2023	
Experiment No. 9 Simulation of SQL injection attack.			
A	05/04/2023	5/4/2023	
B	28/03/2023	11/04/2023	
C	03/04/2023	10/04/2023	
D	24/03/2023	12/4/2023	
Experiment No. 10 Project Implementation			
A	1/03/23	20/4/23	
B			
C			
D			