Lesson Plan

Advanced System Security and Digital Forensics

SEM VII

2019-2020

Subject Incharge

Prof.Mahendra Mehra

FR. Conceicao Rodrigues College of Engineering
Department of Computer Engineering
Lesson plan

SUBJECT: Advanced System Security and Digital Forensics
ACADEMIC YEAR: 2019-20 **SUBJECT CODE: CSDLO7031**
SEM: IV **FACULTY NAME: Prof. Mahendra Mehra**

1. Time table
2. Syllabus-text books, reference books, online resources
3. Course objectives
4. Course outcomes (level in blooms taxonomy-knowledge, skill, attitude)
5. CO-PO mapping , CO-PSO Mapping
6. CO attainment tools
7. CO attainment targets
8. Lecture plan (lectures, presentations, homework, videos, case study, social media)
9. Lab/assignments/mini-project plan
10. Curriculum gap (topic, action taken, mapped co or po)
11. Content beyond syllabus (topic, action taken, mapped co or po)
12. Guest lecture(invitation letter, attendance, thanks letter)
13. List of experiments
14. List of assignments/quiz/presentations
15. Rubrics for experiment/ assignment/mini project.. Tools used
16. Lab manual
17. Unit test question papers with marking scheme
18. Sample answer sheets for unit test/sample answer script
19. University question papers
20. Mini project list with some sample reports
21. Course exit survey form
22. Result analysis of previous semester (no. Of students appeared, passed, percentage, students> 60%)
23. Co attainment summary
24. Co attainment excel prints
25. Identified strong and weak students on the basis of test/assignment (>90% and <50%)
26. Assistance to weak students with remedial classes (attendance-contents)
27. Student feedback
28. Audit report
29. Attendance sheets
30. Attendance defaulters till test1/test2
31. Lecture notes
32. Proof of any claim made in SAR related to your subject like innovation in teaching learning and assignments and other pedagogical methods.(please refer final SAR)

TIME TABLE

Fr. Conceicao Rodrigues College of Engineering, Bandra
Computer Engineering Department
July-Nov 2019

Prof. Mahendra Mehra						With Effect From: 15th July 2019				
	8.45 a.m.-09.45 a.m.	9.45 a.m.-10.45 a.m.	10.45 a.m.-11 a.m.	11 a.m. – 12 p.m.	12 p.m.-01 p.m.	1 p.m.-1.30 p.m.	1.30 p.m. - 2.30 p.m.	2.30 p.m.-3.30 p.m.	3.30 p.m.-4.30 p.m.	4.30 p.m.-5.30 p.m.
Monday			BREAK			Lunch Time		WT TEC-B		
Tuesday				ASS&DF BEC			WT TEC-B			
Wednesday								ASS&DF BEC		
Thursday		ASS&DF BEC						WT TEC-A		
Friday	ASS&DF BEC			WT TEC-A				CL TEC-A		
Saturday										
Total load: 04Th+10P = 14										

FR. Conceicao Rodrigues College Of Engineering

Father Agnel Ashram, Bandstand, Bandra-west, Mumbai-50

Department of Computer Engineering

B.E. (Computer) (semester VII) (2019-20)

Course Outcomes & Assessment Plan

Subject: Advanced System Security and Digital Forensics (CSDLO7031)

Course Outcomes:

Upon completion of this course students will be able to:

CSDLO7031.1: understand cyber attacks and defense strategies through access control mechanisms. . **[B2: Understanding]**
CSDLO7031.2: Explore software vulnerabilities, attacks and protection mechanisms of 802.11 standards, mobile devices and web applications. **[B3: Application]**
CSDLO7031.3: understand various security management and policies. . **[B3: Understanding]**
CSDLO7031.4: Explore and demonstrate techniques used in digital forensics. **[B3: Application]**

Mapping of CO and PO/PSO

Relationship of course outcomes with program outcomes: Indicate 1 (low importance), 2 (Moderate Importance) or 3 (High Importance) in respective mapping cell.

	PO1 (Engg Know)	PO2 (Analysis)	PO3 (Design)	PO4 (investigation)	PO5 (tools)	PO6 (engg Soci)	PO7 (Env)	PO8 (Eth)	PO9 (ind Team)	PO10 (comm.)	PO11 (PM)	PO12 (life Long)
CSDLO7031.1	2				1							
CSDLO7031.2	3			2	3							
CSDLO7031.3	1					1		2		2		
CSDLO7031.4	3			3	3							
Course To PO	2.25			2.5	2.33	1		2		2		

CO	PSO1	PSO2
CSDLO7031.1	3	
CSDLO7031.2	3	2
CSDLO7031.3	1	
CSDLO7031.4	3	3
Course to PSO	2.5	2.5

Justification for CO-PO Mapping

PO1:

All COs are mapped to PO1 because engineering graduates will be able to apply the knowledge of mathematics, Operating System , computer networks and its functionalities to solve engineering problems

PO4:

CSDLO7031.2 and CSDLO7031.4 is mapped to PO4 because students will conduct investigations using penetration testing/digital forensic tools as part of lab exercises

PO5:

CSDLO7031.1, CSDLO7031.2 and CSDLO7031.4 is mapped to PO5 because the students will use different ethical hacking tools, penetration testing and forensic tools for security audits and examining evidence.

PO6:

CSDLO7031.3 is mapped to this PO6 because the students will learn various security policies and management ethics to assess legal issues in cyber space.

PO8:

CSDLO7031.3 is mapped to this PO8 because the students will learn various security policies and management ethics.

PO10:

CSDLO7031.3 is mapped to this PO10 because the students will deliver presentations on casestudy of ethics

PSO1:

All COs are mapped to PSO1 because the graduates will be able to apply fundameAdvanced System Security and Digital Forensics knowledge of computer networks , Operating System and best programming practices to build solutions for real world problems.

PSO2: CSDLO7031.2 and CSDLO7031.4 is mapped to PSO2 because student will learn about Zero day attacks and how to safe guard systems against them in this changing world of technology.

CO Assessment Plan

CSDLO7031.1	*CSDLO7031.1:* understand cyber attacks and defense strategies through access control mechanisms. . **[B2: Understanding]**		
Delivery Methods	Black Board, lecture notes and video		
Target	**2.5**		
Sr.no	**CO Assessment Tools**	**Target (Tool wise)**	**Weightage**
1.	Test 1	60% student score more than 60%	0.2
	Questions	TEST1(Q1 (a OR b) total 05 marks)	
	Date		
2.	Lab Experiments	60% students will score minimum 70% marks	0.3
	Experiment nos	1,2	
3.	Assignment 1	60% student score more than 70%	0.2
	Date	8/7/2019	
4.	Semester End Exams	60% students score more than 60%	0.3
	Date		
5.	Course Exit Survey	75% student rate above average (4 & 5)	0.2
	Date		

CO Assessment Tools:

CSDLO7031.1: Direct Methods(80%): Test(1) , Assignment1, Quiz1, Lab_Exp(1-5), Uni_Exam(TH+PR)

CO1dm = 0.2(T1) +0.3LAB(1-2) + 0.2A1 + (0.2UTh+0.1UPr)

Indirect Methods(20%): Course exit survey

CO3idm =Course_Exit_Survey

CSDLO7031.1 = 0.8*CO1dm + 0.2* CO1idm

CSDLO7031.2		**CSDLO7031.2:** Explore software vulnerabilities, attacks and protection mechanisms of 802.11 standards, mobile devices and web applications. **[B3: Application]**	
Delivery Methods		Black Board, lecture notes and video	
Target		**2.5**	
Sr.no	**CO Assessment Tools**	**Target (Tool wise)**	**Weightage**
1.	Test 1	60% student score more than 70%	0.2
	Questions no	TEST1(Q2 for 05M) & TEST1(Q3 for 10M)	
	Date		
2.	Lab Experiments	60% students will score minimum 70% marks	0.3
	Experiment nos	3,4,5,6,7,11	
3.	Assignment 2	60% student score more than 70%	0.2
	Date	5/8/19	
4.	Semester End Exams	60% students score more than 60%	0.3
	Date		
5.	Course Exit Survey	75% student rate above average (4 & 5)	0.2
	Date		

CO Assessment Tools:

CSDLO7031.2: Direct Methods(80%): Test1 , Assignment2, , Lab_Exp(3,4,5,6,7,11), Uni_Exam(TH+PR)

CO1dm = 0.2T1 +0.3LAB(3,4,5,6,7,11) + 0.2A2 + (0.2UTh+0.1UPr)

Indirect Methods(20%): Course exit survey

CO3idm =Course_Exit_Survey

CSDLO7031.1 = 0.8*CO1dm + 0.2* CO1idm

CSDLO7031.3	*CSDLO7031.3:* understand various security management and policies. . **[B3: Understanding]**		
Delivery Methods		Black Board, lecture notes and video	
Target		**2.7**	
Sr.no	**CO Assessment Tools**	**Target (Tool wise)**	**Weightage**
1.	Test 2	60% student score more than 70%	0.2
	Question no	Test2 (Q2 a for 05marks) Test2(Q2 b for 05 marks)	
	Date	9/4/19	
2.	Class Presentation	60% students will score minimum 70% marks	0.3
	Exp no	12	
3.	Assignment 3	60% student score more than 70%	0.2
	Date	22/8/2019	
4.	Semester End Exams	60% students score more than 60%	0.3
	Date		
5.	Course Exit Survey	75% student rate above average (4 & 5)	0.2
	Date		

CO Assessment Tools:

CSDLO7031.3: Direct Methods(80%): Test(2), Assignment3, class_presentation(), Uni_Exam(TH)

CO1dm = 0.2(T2) +0.3class_presentation(12) + 0.2A3 + (0.2UTh+0.1UPr)

Indirect Methods(20%): Course exit survey

CO3idm =Course_Exit_Survey

CSDLO7031.1 = 0.8*CO1dm + 0.2* CO1idm

CSDLO7031.4	*CSDLO7031.4:* Explore and demonstrate techniques used in digital forensics. **[B3: Application]**		
	Delivery Methods	Black Board, lecture notes and video	
Target		**2.7**	
Sr.no	**CO Assessment Tools**	**Target (Tool wise)**	**Weightage**
1.	Test 2	60% student score more than 70%	0.2
	Question no	Test2 (Q1 for 10 marks) and (Q3 for 5marks)	
	Date		
2.	Lab Experiments	60% students will score minimum 70% marks	0.3
	Experiment nos	8,9,10,11	
3.	Assignment 4	60% student score more than 70%	0.2
	Date	9/9/19	
4.	Semester End Exams	60% students score more than 60%	0.3
	Date		
5.	Course Exit Survey	75% student rate above average (4 & 5)	0.2
	Date		

CO Assessment Tools:

CSDLO7031.4: Direct Methods(80%): Test2 , Assignment4, Lab_Exp(8,9), Uni_Exam(TH+PR)

CO1dm = 0.2(T2) +0.3LAB(8,9,10,11) + 0.2A4 + (0.2UTh+0.1UPr)

Indirect Methods(20%): Course exit survey

CO3idm =Course_Exit_Survey

CSDLO7031.1 = 0.8*CO1dm + 0.2* CO1idm

Course Outcomes Target:

Upon completion of this course students will be able to:

CSDLO7031.1: understand cyber attacks and defense strategies through access control mechanisms. . **[B2: Understanding]**

Target level: 2.5

CSDLO7031.2: Explore software vulnerabilities, attacks and protection mechanisms of 802.11 standards, mobile devices and web applications. **[B3: Application]**

Target level: 2.5

CSDLO7031.3: understand various security management and policies. . **[B3: Understanding]**

Target level: 2.7

CSDLO7031.4: Explore and demonstrate techniques used in digital forensics. **[B3: Application]**

Target level: 2.7

Content Beyond Syllabus:

In order understand current applications, trends and new directions in Open Source OS AND TOOLS following topics will be covered

Sr.no.	Content beyond syllabus	Action Plan	CO MAPPED
1.	Burpsuite web penetration testing tool	Assignment , demonstration	C02
2.	Best programming practices	Experiment	CO2

Curriculum Gap:

No gap identified

Rubrics for assessment of Experiment:

FR. Conceicao Rodrigues College Of Engineering

Father Agnel Ashram, Bandstand, Bandra-west, Mumbai-50

Department of Computer Engineering

B.E. (Computer) (semester VII)

(2019-2020)

Class : BE Computer

Subject Name: ADVANCED SYSTEM SECURITY AND DIGITAL FORENSICS

Subject Code: CSDLO7031

Experiment No:	**1 TO 11**
Title:	
Date of Performance:	
Date of Submission:	
Roll No:	
Name of the Student:	

Evaluation:

Sr. No	Rubric	Grade
1	On time Submission & Completion (2)	
2	Preparedness (2)	
3	Skill(4)	
4	Output (2)	
	TOTAL	

Signature of the Teacher:

Explanation of Rubrics: Experiments

Sr. No	Performance Indicator	Excellent	Good	Below Average
1.	On-time completion and submission	Completed between 90-100% of the requirements. Delivered on time, and in correct format. Creatively organized work. [2 marks]	Completed between 70-80% of the requirements. Delivered on time and in correct format. [1 mark]	Completed between 50% of the requirements. Not delivered on time and not in correct format. [0 mark]
2.	Preparedness	Awareness about experiment to be performed, Knows the theory. Seeks information from multiple sources. [2 marks]	Awareness about experiment to be performed, knows the basic concept. Seeks information from few sources mainly textbook. [1 mark]	Not aware of the experiment to be performed. Unable to perform independently. Seeks no extra information other than what is provided by instructor. [0 mark]
3.	Skill	Installation of tools , Exploring different options available with proper demonstration of various modules [4 marks]	Completeness of code, installation, integration inconsistent usage of tools or error. [2 marks]	In Complete code, unformatted, lacks comments, Demonstrates no proficiency in understanding technology, no output is obtained. [0 mark]
4.	Output	Completed with clear conceptualization [2 marks]	Completed with partial conceptualization [1 mark]	Copied (with no understanding) [0 mark]

FR. Conceicao Rodrigues College Of Engineering

Father Agnel Ashram, Bandstand, Bandra-west, Mumbai-50

Department of Computer Engineering

B.E. (Computer) (semester VII)

(2019-2020)

Class : B.E. (COMPUTER)

Subject Name: Advanced System Security and Digital Forensics

Subject Code: CSDLO7031

Experiment No:	**Assignments (1-4)**
Title:	
Date of Performance:	
Date of Submission:	
Roll No:	
Name of the Student:	

Evaluation:

Sr. No	Rubric	Grade
1	On time Submission (2)	
2	Organization (2)	
3	Level of content(4)	
4	Depth and breadth of discussion (2)	
	Total	

Signature of the Teacher:

Rubrics for the Assignments:

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)

FR. Conceicao Rodrigues College Of Engineering

Father Agnel Ashram, Bandstand, Bandra-west, Mumbai-50

Department of Computer Engineering

B.E. (Computer) (semesterVII)

(2019-2020)

Lesson Plan: Advanced System Security and Digital Forensics

Semester VII **Year: 2019-20**

Subject Incharge: Prof. Mahendra Mehra

Course Objectives:

CSDLO7031.1: understand cyber attacks and defense strategies through access control mechanisms. . **[B2: Understanding]**

CSDLO7031.2: Explore software vulnerabilities, attacks and protection mechanisms of 802.11 standards, mobile devices and web applications. **[B3: Application]**

CSDLO7031.3: understand various security management and policies. . **[B3: Understanding]**

CSDLO7031.4: Explore and demonstrate techniques used in digital forensics. **[B3: Application]**

Modes of Content Delivery:

i	Class Room Teaching	v	Self Learning Online Resources	Ix	Industry Visit
ii	Tutorial	vi	Slides	X	Group Discussion
iii	Remedial Coaching	vii	Simulations/Demonstrations	xi	Seminar
iv	Lab Experiment	viii	Expert Lecture	xii	Case Study

Lect. No.	Portion to be covered	Planned date	Actual date	Content Delivery Method
1.	**Introduction & Access Control**	2/7/19		I, vi
2.	Cyber-attacks, Vulnerabilities, Defence Strategies and Techniques	3/7/19		I, vi
3.	Authentication Methods and Protocols,	4/7/19		I, vi

4.	Defence in Depth Strategies.	5/7/19		i, vi
5.	Access Control Policies: DAC, MAC,	9/7/19		i, iv , vi
6.	Multi-level Security Models: Biba Model, Bell La Padula Model,	10/7/19		I,
7	Single Sign on	11/7/19		i
8	Federated Identity Management.	12/7/19		i

Books:

1. Computer Security Principles and Practice, William Stallings, Sixth Edition, Pearson Education
2. Security in Computing, Charles P. Pfleeger, Fifth Edition, Pearson Education .

Lect. No.	Portion to be covered	Planned date	Actual date	Content Delivery Method
9	**Program & OS Security :** Malicious and Non-Malicious programming errors,	16/7/19		i , iv
10	Targeted Malicious codes: Salami Attack, Linearization Attack, Covert Channel	17/7/19		i
11	Control against Program threats	18/7/19		i , iv
12.	Operating System Security: Memory and Address protection	19/7/19		i , iv
13.	Operating System Security: Memory and Address protection	23/7/19		i , iv
14.	File Protection Mechanism,	24/7/19		i , iv

15.	User Authentication.	25/7/19		i
16.	Linux and Windows: Vulnerabilities	26/7/19		i

Books:

1. Computer Security Principles and Practice, William Stallings, Sixth Edition, Pearson Education
2. Security in Computing, Charles P. Pfleeger, Fifth Edition, Pearson Education .

Lect. No.	Portion to be covered	Planned date	Actual date	Content Delivery Method
17	**Web Application Security** OWASP,	30/7/19		i
18	Web Security Considerations	31/7/19		i, iv, vi
19	User Authentication and Session management, Cookies,	1/8/19		i, iv, vi
20	SSL, HTTPS, SSH, Privacy on Web,	2/8/19		i, iv
21	Web Browser Attacks, Account Harvesting, Web Bugs, Clickjacking	6/8/19		i, iv
22	Cross-Site Request Forgery,	7/8/19		i , iv
23	Session Hijacking and Management,	8/8/19		
24	Phishing and Pharming Techniques,	9/8/19		i , vii
25	Web Service Security	20/8/19		i, vi
26	OAuth 2.0	21/8/19		I, vi

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. Cyber Security. Nina Godbole, Sunit Belapure, Wiley

Lect. No.	Portion to be covered	Planned date	Actual date	Content Delivery Method
27.	**Wireless Security** Wi-Fi Security, WEP, WPA, WPA-2,	22/8/19		I, vi
28.	Mobile Device Security-Security Threats,	23/8/19		i, iv, vi
29.	Device Security, GSM and UMTS Security	27/8/19		i
30	IEEE 802.11/802.11i Wireless LAN Security	28/8/19		i, vii
31.	IEEE 802.11/802.11i Wireless LAN Security	29/8/19		i, vi
32	VPN Security.	30/8/19		I, iv

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. Cyber Security. Nina Godbole, Sunit Belapure, Wiley

Lect. No.	Portion to be covered	Planned date	Actual date	Content Delivery Method
33	**Legal and Ethical issues** Cybercrime and its types, Intellectual property	11/9/19		i,, ix, xii
34	Privacy, Ethical issues. Protecting Programs and Data, Information and the Law,	12/9/19		i,, ix, xii
35	Rights of Employees and Employers, Redress for Software Failures	13/9/19		i,, ix, xii
36	Computer Crime, Ethical Issues in Computer Security, case studies of ethics.	17/9/19		i,, ix, xii

Books:

4. Computer Security Principles and Practice, William Stallings, Sixth Edition, Pearson Education
5. Security in Computing, Charles P. Pfleeger, Fifth Edition, Pearson Education .
6. Cyber Security. Nina Godbole, Sunit Belapure, Wiley

Lect. No.	Portion to be covered	Planned date	Actual date	Content Delivery Method
37	**Digital Forensics** Introduction to Digital Forensics, Acquiring Volatile Data from Windows and Unix systems,	18/9/19		i, iv, vi
38	Forensic Duplication Techniques	19/9/19		i iv, vi
39	, Analysis of forensic images using open source tools like Autopsy and SIFT,	20/9/19		I, iv, vi
40	Analysis of forensic images using open source tools like Autopsy and SIFT,	24/9/19		I, iv, vi
41	Investigating logs from Unix	25/9/19		I, iv, vi
42	Investigating logs from windows systems	26/9/19		I, iv, vi
43	Investigating Windows Registry.	3/10/19		I, iv, vi
44	Defaulters remedial session	4/10/19		I, iv, vi
45	Defaulters remedial session	9/10/19		I, iv, vi

Books:

1. Digital Forensics by Nilakshi Jain & Kalbande, Wiley.
2. Incident Response & Computer Forensics by Kevin Mandia, Chris Prosise, Wiley.

FR. Conceicao Rodrigues College Of Engineering
Department Of Computer Engineering
ASSDF: List of Experiments (2019-2020)

Sr.no	Concept	CO	Experiment
01	Access control list	CO1	Exploring Router and VLAN security, setting up access lists using Cisco Packet tracer(student edition)
02			Exploring Authentication and access control using RADIUS, TACACS and TACACS+
03	Penetration testing tools	CO2	Static code analysis using open source tools like CPPCHECK & SPLINT
04			Vulnerability scanning using Nessus, Nikto (Kali Linux)
05			Performing a penetration testing using Metasploit (Kali Linux)
06			Detect SQL injection vulnerabilities in a website database using SQLMap
07			Install and use a security app on an Android mobile
08	Digital Forensics tools	CO4	Explore forensics tools in Kali Linux for acquiring, analyzing and duplicating data: dd, dcfldd, foremost, scalpel, debugfs, wireshark, tcptrace, tcpflow
09			Analysis of forensic images using open source tools like Autopsy, SIFT, FKT Imager
10			Use of steganographic tools like OpenStego, to detect data hiding or unauthorized file copying
11		CO1,4	Use Password cracking using tools like John the Ripper/Cain and Abel/ Ophcrack to detect weak passwords
12	Legal and Ethical issues	CO3	**Class Presentation**

FR. CONCEICAO RODRIGUES COLLEGE OF ENGINEERING

Department of Computer Engineering

B.E. (Computer) (semester VII) (2019-20)

Subject Incharge: Prof. Mahendra Mehra

Advanced System Security and Digital Forensics

EXPERIMENTS – Date of Performance

Sr.no.	Experiments	CO MAPPING	BATCH Friday
1	Exploring Router and VLAN security, setting up access lists using Cisco Packet tracer(student edition)	CO1	15/07/19- 19/07/19
2	Exploring Authentication and access control using RADIUS, TACACS and TACACS+	CO1	22/07/19- 26/07/19
3	Static code analysis using open source tools like CPPCHECK & SPLINT	CO2	29/07/19 to 02/08/19
4	Vulnerability scanning using Nessus, Nikto (Kali Linux)	CO2	5/08/19 to 9/08/19
5	Performing a penetration testing using Metasploit (Kali Linux)	CO2	19/8/19 to 23/8/19
6	Detect SQL injection vulnerabilities in a website database using SQLMap	CO2	26/8/19 to 30/8/19
7	Install and use a security app on an Android mobile	CO2	27/8/19 to 31/8/19
8	Explore forensics tools in Kali Linux for acquiring, analyzing and duplicating data: dd, dcfldd, foremost, scalpel, debugfs, wireshark, tcptrace, tcpflow	CO4	9/9/19 to 13/9/19
9	Analysis of forensic images using open source tools like Autopsy, SIFT, FKT Imager	CO4	16/9/19 to 20/9/19
10	Use of steganographic tools like OpenStego, to detect data hiding or unauthorized file copying	CO4	23/9/19 to 27/9/19
11	Use Password cracking using tools like John the Ripper/Cain and Abel/ Ophcrack to detect weak passwords	CO2&CO4	30/09/19 to 11/10/19
12	Legal and Ethical issues (Class Presentations)	CO3	09/09/19 to 13/09/19

FR. CONCEICAO RODRIGUES COLLEGE OF ENGINEERING

Department of Computer Engineering

B.E. (Computer) (semester VII) (2019-20)

Subject Incharge: Prof. Mahendra Mehra

Advanced System Security and Digital Forensics

Assignments – Date of Performance

Assignment	DOP	DOS
ASSIGNMENT NO 1	8/7/2019	22/7/2019
ASSIGNMENT NO 2	5/8/2019	18/8/2019
ASSIGNMENT NO 3	22/8/2019	5/9/2019
ASSIGNMENT NO 4	9/9/2019	16/9/2019

FR. Conceicao Rodrigues College Of Engineering

Department Of Computer Engineering
OS-LAB (CSDLO7031)
(2019-2020)

Class Presentation Plan

CSDLO7031.3: understand various security management and policies. . [B3: Understanding]

Date	Activity
18/07/2019	Group formation, Topic Submission through Google Form
01/08/2019	Presentation list will be declared
09/09/19 to 13/09/19	Class presentation + ppt

FR. Conceicao Rodrigues College Of Engineering

Father Agnel Ashram, Bandstand, Bandra-west, Mumbai-50

Computer Engineering Department

Course Exit Form

Advanced System Security and Digital Forensics

(2019 - 2020)

1. **I am able to understand cyber attacks and defense strategies through access control mechanisms..**
    a. Strongly Agree
    b. Agree
    c. Neutral
    d. Disagree
    e. Strongly Disagree

2. **I am able to explore software vulnerabilities, attacks and protection mechanisms of 802.11 standards, mobile devices and web applications.**
    a. Strongly Agree
    b. Agree
    c. Neutral
    d. Disagree
    e. Strongly Disagree

3. **I am able to understand various security management and policies.**
    a. Strongly Agree
    b. Agree
    c. Neutral
    d. Disagree
    e. Strongly Disagree

4. **I am able to Explore and demonstrate techniques used in digital forensics.**
    a. Strongly Agree
    b. Agree
    c. Neutral
    d. Disagree
    e. Strongly Disagree