COURSE FILE

NTAL-LAB

2018-2019

FR. Conceicao Rodrigues College of Engineering
Department of Computer Engineering
COURSE FILE INDEX

SUBJECT: Network threats and attacks Laboratory ACADEMIC YEAR:2018-19
SUBJECT CODE:CPL701 SEM:VII
FACULTY NAME: 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

Prof. Mahendra Mehra						With Effect From: 16th July 2018				
	08.45 – 09.45	09.45 – 10.45	10.45 – 11.00	11.00 – 12.00	12.00 – 13.00	13.00 – 13.30	13.30 – 14.30	14.30 – 15.30	15.30 – 16.30	16.30 – 17.30
Monday			Break	WT TEC-B		Lunch Time	AOS TEC			
Tuesday		AOS TEC		WT TEC-B			NTAL BEC-D		Mentoring	
Wednesday	AOS TEC								NTAL BEC-D	
Thursday		AOS TEC					NTAL BEC-B			
Friday							NTAL BEC-B			
Saturday										
Total load: 4hrs(Th)+12hrs(Pract)=16hrs+ Mentoring										

FR. Conceicao Rodrigues College Of Engineering

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

Department of Computer Engineering

B.E. (Computer) (semester VII) (2018-2019)
Course Outcomes & Assessment Plan

Subject: Network threats and attacks Laboratory: CPL701

Credits-2

Course Outcomes:

Upon completion of this course students will be able to:

CPL701.1: Analyze Network infrastructure by using different reconnaissance and port scanning tools. **[B2: Analysis]**

CPL701.2: Demonstrate various network and distributed system attacks by exploiting common vulnerabilities **[B3: Application]**

CPL701.3: Apply and validate solutions to computer network security challenges using common network security tools and formal methods. **[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)
CPL701.1	2	2		2	2	1						
CPL701.2	2				2	1						
CPL701.3	2		2	2	3	1			2		2	
Course To PO	2	2	2	2	2.33	1			2		2	

CO	PSO1	PSO2
CPL701.1	3	
CPL701.2	3	
CPL701.3	3	3
Course to PSO	3	3

Justification

PO1: This subject all Cos are mapped to PO1 because engineering graduates will be able to apply the knowledge of Network Threats and attack laboratory fundamentals to solve complex engineering problems and identify various security issues within them .

PO2: CPL701.1is mapped to this PO2 because the students analyze the network Infrastructure with the help of various reconnaissance tools and derive useful information out of it about the victim/target.

PO3: CPL701.3 is mapped to this PO3 because the students design and develop various security solutions to prevent breach of network infrastructure.

PO4: CPL701.1 and CPL701.3 are mapped to this PO4 because the students use the knowledge gained to do analysis and synthesis based on the information gathered also to conclude if the solutions are effective.

PO5: CPL701.1, CPL701.2 and CPL701.3 are mapped to this PO5 because the students use the tools like zenmap, whois domain tools, Wireshark, Kali Linux, tripwire, graylag to scan attack and defend the network infrastructure.

PO6: CPL701.1, CPL701.2 and CPL701.3 are mapped to this PO6 because the students need to be aware of the consequences and legal bindings of misusing the tools for ill motives.

PO9: CPL701.3 is mapped to this PO9 because the students will develop a mini-project by working in a team and present the same

PO11: CPL701.3 is mapped to this PO11 because the students will follow project guidelines as given by the teacher

PSO1: All COs are mapped to PSO1 because the graduates will be able to apply fundamental knowledge of NTAL to provide computer base solution to real world problems.

PSO2: CPL701.3 is mapped to this PSO2 because the students design and implement a networking infrastructure with appropriate considerations to security solutions.

CO1 Assessment Plan

CPL701.1	CPL701.1: Analyze Network infrastructure by using different reconnaissance and port scanning tools. **[B2: Analysis]**		
	Delivery Methods	PRACTICALS	
	Target	**2.7**	
Sr.no	**CO Assessment Tools**	**Target (Tool wise)**	**Weightage**
1.	MCQ'S Quiz on Moodle Test 1	60% of students will score minimum 80%	0.2
	Date	6/08/2017 to 10/08/17	
2.	Lab Experiments	70% students will score minimum 80% marks	0.4
	Experiment nos:	01,02 & 03	
3.	Semester End Exams (orals)	70% of students will minimum score 70% marks	0.4
	Date	To be announced	
4.	Course Exit Survey	60% students strongly agree and agree	0.2
	Date	19/10/2017	

CO1 Assessment Tools:

CPL701.1: **Direct Methods (80%): Test 1 / Labs1-3 / UniExam_Oral**

CO1dm = 0.2*T1 + 0.4*Lab (1-3) + 0.4*UOral

Indirect Methods (20%): Course exit survey

CO1idm =Course_Exit_Survey

CPL701.1 = 0.8*CO1dm + 0.2* CO1idm

CO2 Assessment Plan

CPL701.2	CPL701.2: Demonstrate various network and distributed system attacks by exploiting common vulnerabilities **[B3: Application]**		
	Delivery Methods	PRACTICALS	
	Target	**2.7**	
Sr.no	**CO Assessment Tools**	**Target (Tool wise)**	**Weightage**
1.	MCQ'S Quiz on Moodle Test 1	60% of students will score minimum 80%	0.2
	Date	10/9/18 to 14/9/18	
2.	Lab Experiments	70% students will score minimum 80% marks	0.4
	Experiment nos:	03, 04 & 05	
3.	Semester End Exams (orals)	70% of students will minimum score 70% marks	0.4
	Date	To be announced	
4.	Course Exit Survey	60% students strongly agree and agree	0.2
	Date	19/10/2017	

CO2 Assessment Tools:

CPL701.2: **Direct Methods (80%): Test 2 / Labs4-6 / UniExam_Oral**

CO1dm = 0.2*T2 + 0.4*Lab (4-6) + 0.4*UOral

Indirect Methods (20%): Course exit survey

CO2idm =Course_Exit_Survey

CPL701.2 = 0.8*CO2dm + 0.2* CO2idm

CO3 Assessment Plan

CPL701.3	CPL701.3: Apply and validate solutions to computer network security challenges using common network security tools and formal methods. **[B3: Application]**		
	Delivery Methods	PRACTICALS	
	Target	**2.5**	
Sr.no	**CO Assessment Tools**	**Target (Tool wise)**	**Weightage**
1.	MCQ'S Quiz on Moodle Test 1	60% of students will score minimum 80%	0.2
	Date	9/10/18 to 13/10/18	
2.	Lab Experiments	70% students will score minimum 80% marks	0.2
	Experiment nos:	07, 08 & 09	
3.	Mini Project	60% of students will minimum score 70% marks	0.4
4.	Semester End Exams (orals)	70% of students will minimum score 70% marks	0.2
	Date	To be announced	
5.	Course Exit Survey	60% students strongly agree and agree	0.2
	Date	19/10/2017	

CO3 Assessment Tools:

CPL701.3: **Direct Methods (80%): Test 3 / Labs7-9 / Mini_Project / UniExam_Oral**

CO1dm = 0.2*T3 + 0.2*Lab (7-9) + 0.4*Mini_Project + 0.2*UOral

Indirect Methods (20%): Course exit survey

CO3idm =Course_Exit_Survey

CPL701.3 = 0.8*CO3dm + 0.2* CO3idm

Course Outcomes Target:

Upon completion of this course students will be able to:

CPL701.1: Analyze Network infrastructure by using different reconnaissance and port scanning tools. **[B2: Analysis]**

Target level: 2.7

CPL701.2: Demonstrate various network and distributed system attacks by exploiting common vulnerabilities **[B3: Application]**

Target level: 2.7

CPL701.3: Apply and validate solutions to computer network security challenges using common network security tools and formal methods. **[B3: Application]**

Target level: 2.5

Content Beyond Syllabus:

1. **DevOps Security Practices covered in Experiment no 07 with the help of Tripwire tool.**

Curriculum Gap:

No Curriculum Gap Identified

Rubrics for the Lab Experiments:

FR. Conceicao Rodrigues College Of Engineering

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

Department of Computer Engineering

B.E. (Computer) (semester VII)

(2018-2019)

Class : BE Computer

Subject Name: NTAL

Subject Code: CPL701

Experiment No:	**1 TO 9**
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)	

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]

Rubrics for assessment of Mini Project:

FR. Conceicao Rodrigues College Of Engineering

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

Department of Computer Engineering

B.E. (Computer) (semester VII)

(2018-2019)

Class : BE Computer

Subject Name: NTAL

Subject Code: CPL701

Experiment No:	**10 MINI-PROJECT**
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	Completeness(03)	
3	Features (04)	
4	Solutions validity(2)	

Signature of the Teacher:

Explanation of Rubrics: MINI-PROJECT

Indicator	Very Poor	Poor	Average	Good	Excellent
On time Submission & Completion (1) Maintains project deadline	Project not done (00)	More than two session late (0)	Two sessions late (00)	One of the progress report on time (0.5)	Both progress report on time (01)
Completeness(03) Complete all parts of project	N/A	40-60% complete (01)	60-80% complete (02)	80-90% complete(2.5)	90-100% complete(03)
Project specific Technical Features(04) 1. Open source tool 2. Installation 3. Configuration 4. Test bed 5. Attack vector	N/A	One feature (01)	Two features (02)	Three features(03)	4-5 features (04)
Solutions validity(2) 1. Detection of attack 2. Preventing attacks	N/A	N/A	Detection possible but unable to prevent attacks (01)	Only detection and partial prevention (1.5)	Detection and prevention both possible (02)

FR. Conceicao Rodrigues College of Engineering
Department Of Computer Engineering

NTAL: List of Experiments (2018-2019)

Exp No.	Concept	CO Mapping	Title/aim
01	Information Gathering	CO1	Study the use of network reconnaissance tools like ping, Nslookup and Whois to gather information about networks and domain registrars.
02	Packet Sniffing		Study of packet sniffer tools like Wireshark and its capture filters.
03	Active Reconnaissance		Port scanning and OS fingerprinting using NMAP
04	Attack Vector	CO2	Metasploit Framework Part 1 : Using various Exploits to hack into a windows XP system
05	Attack Vector		Metasploit Framework Part 2 – msfconsole & Exploiting Vulnerable Linux System
06	Web Application Attacks		Burpsuite – Use Burp Intruder to Brute force Forms
07	Security Solution, IDS	CO3	Installation of Tripwire to Detect Server Intrusions on an Ubuntu machine
08	Firewalls		Use of Iptables in Linux to create firewalls.
09	Log Analysis		GoAccess (A Real-Time Apache and Nginx) Web Server Log Analyzer
10	Security Solutions		Mini Projects

FR. Conceicao Rodrigues College Of Engineering

Department Of Computer Engineering

NTAL: List of Experiments (2018-2019)

Practical Plan

Exp No.	Date Planned				Concept	Title/aim
	A	B	C	D		
01	16/7/18to 20/7/18	16/7/18to 20/7/18	16/7/18to 20/7/18	16/7/18to 20/7/18	Information Gathering	Study the use of network reconnaissance tools like ping, Nslookup and Whois to gather information about networks and domain registrars.
02	23/7/18to 27/7/18	23/7/18to 27/7/18	23/7/18to 27/7/18	23/7/18to 27/7/18	Packet Sniffing	Study of packet sniffer tools like Wireshark and its capture filters.
03	30/7/18to 03/8/18	30/7/18to 03/8/18	30/7/18to 03/8/18	30/7/18to 03/8/18	Active Reconnaissance	Port scanning and OS fingerprinting using NMAP
04	6/8/18 to 10/8/18	6/8/18 to 10/8/18	6/8/18 to 10/8/18	6/8/18 to 10/8/18	Attack Vector	Metasploit Framework Part 1: Using various Exploits to hack into a windows XP system
05	20/8/18 to 24/8/18	20/8/18 to 24/8/18	20/8/18 to 24/8/18	20/8/18 to 24/8/18	Attack Vector	Metasploit Framework Part 2 – msfconsole & Exploiting Vulnerable Linux System
06	3/9/18 to 7/9/18	3/9/18 to 7/9/18	3/9/18 to 7/9/18	3/9/18 to 7/9/18	Web Application Attacks	Burpsuite – Use Burp Intruder to Brute force Forms
07	12/9/18 to 14/9/18	12/9/18 to 14/9/18	12/9/18 to 14/9/18	12/9/18 to 14/9/18	Security Solution, IDS	Installation of Tripwire to Detect Server Intrusions on an Ubuntu machine
08	17/9/18 to 21/9/18	17/9/18 to 21/9/18	17/9/18 to 21/9/18	17/9/18 to 21/9/18	Firewalls	Use of Iptables in Linux to create firewalls.
09	24/9/18 to 28/9/18	24/9/18 to 28/9/18	24/9/18 to 28/9/18	24/9/18 to 28/9/18	Log Analysis	GoAccess (A Real-Time Apache and Nginx) Web Server Log Analyzer
10	1/10/18 to 05/10/18	1/10/18 to 05/10/18	1/10/18 to 05/10/18	1/10/18 to 05/10/18	Security Solutions	Mini Projects

FR. Conceicao Rodrigues College Of Engineering

Department Of Computer Engineering
NTAL-LAB (CPL701)
(2018-2019)

Project progress report

Title of the Project:

Date:

Class BE-COMPUTERS **SEM: VII**

Subject In charge: Prof. Mahendra Mehra

Members name	Planned efforts	Actual efforts		Remarks
		Knowledge gained	Practical implementation	

FR. Conceicao Rodrigues College Of Engineering

Department Of Computer Engineering
NTAL-LAB (CPL701)
(2018-2019)

Mini-Project Plan

[CPL701.3-- Apply and validate solutions to computer network security challenges using common network security tools and formal methods]

Date	Activity
18/07/2017	Project Group formation, Topic Submission through Google Form
14/08/2017	1st Project Progress Report
28/08/2017	Project Demonstration + Corrections and Improvements
18/09/2017	2nd Project Progress Report
9/10/18 to 13/10/18	Project Report and Presentation

Project Report Template: Minimum 5 Pages

Report index:

1. Title page (fill the template, last page of this document)

2. Introduction: (HEADING2)

Give general introduction about the topic (12pt,TNR)

3. Problem statement: (HEADING2)

State reason for choosing this topic (12pt,TNR)

4. Proposed solution: (HEADING2)

With diagrams and theory. (12pt,TNR)

Attach screenshots wherever applicable label each figure (fig 01: figure name 10pt,TNR)

5. Survey: (HEADING2)

Content (12pt,TNR)

6. Technology used: (HEADING2)

Content (12pt,TNR)

7. Conclusion

Content (12pt,TNR)

8. References (HEADING2)

Content (12pt,TNR)

TITLE OF PROJECT REPORT

A PROJECT REPORT

Submitted by

NAME OF THE CANDIDATE(S)

In partial fulfillment for the completion of mini project

In the Subject of **Network Threats and attack Laboratory**

FOURTH YEAR
COMPUTER ENGINEERING

Fr. Conceicao Rodrigues College of Engineering, Bandra (w)

JUL-NOV 2017

FR. Conceicao Rodrigues College Of Engineering

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

Computer Engineering Department

Course Exit Form

(2017- 2018)

(1) I am able to gather information about the networks by using both active and passive reconnaissance and port scanning tools [CO1]

- Not selected
- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

(2) I am able to demonstrate various network and distributed system attacks by exploiting common vulnerabilities [CO2]

- Not selected
- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

(3) I am able to Implement and validate solutions to computer network security challenges using common network security tools and formal methods. [CO3]

- Not selected
- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

List of Attendance Defaulters till Unit Test1 (Specify the criteria of attendance for defaulting)

Criteria of attendance for defaulting attendance less than 50%

Sr. No.	Roll Number	Name of the student	Attendance in %	Reason for defaulting	Comment/Remark

Action Taken for Defaulters

List of Attendance Defaulters till Unit Test2 (Specify the criteria of attendance for defaulting)

Criteria of attendance for defaulting attendance less than 50%

Sr. No.	Roll Number	Name of the student	Attendance in %	Reason for defaulting	Comment/Remark

Action Taken for Defaulters-test2

Identification of Strong and Weak Students using Test

		No of Students					
Test No.	**Test Date**	**Total Students**	**Full Marks**	**>80%**	**79%>marks>60%**	**less than 60%**	**Failed**
TEST1							
TEST2							

Classification: Tool (Test)	**Category**	**ROLLNO.**	**NAME OF STUDENTS**
Strong students	TEST1>=90% AND TEST2>=90%		
Weak Students	<50%		

Identification of Strong and Weak Students using Assignment

		No of Students					
Assig. No.	**Assig. (Given Date)**	**Assig. (Submission Date)**	**Full Marks**	**>80%**	**79%>marks>60%**	**less than 60%**	**Failed**
1							
2							
3							

Classification: Tool (Assignment)	**Category**	**Name of student**
Strong students	All students above 9	
Weak Students	All students below 6	

Identification of Strong and Weak Students using Lab Performance

		No of Students					
		Total Students	**Full Marks**	**>80%**	**79%>marks>60%**	**less than 60%**	**Failed**

Classification: Tool (Lab Performance)	**Category**	**Name of students**
Strong students	All students above 9	
Weak Students	All students below 6	

Strong/ Weak Students Identified and Action taken:

Sr. No	Date	Roll No	Action Planned	Report Taken (YES/NO)
1				
2				
3				

Report Template: Action taken for strong and weak students (in hard copy)

Efforts taken for those who failed in the tests

Remedial Classes:

Steps:

1. Put up notice
2. Take attendance
3. Take Feedback

COURSE ID:	COURSE NAME:
SEM	DATE:
Topic covered	--
Feedback (Any 5 students on random)	
Roll No	Feedback