University of Mumbai

No. AAMS_UGS/ICC/2024-25/146

CIRCULAR:-

Attention of all the Principals of the Affiliated Colleges, Directors of the Recognized Institutions and the Heads, University Departments is invited to this office Circular No. AAMS_UGS/ICC/2024-25/169 dated 30th September, 2024 relating to the syllabus of **B.Voc (Cyber Security and Digital Forensics) (Sem – I to II) (CBCS).**

They are hereby informed that the recommendations made by the **Board of Studies in Information Technology** at its meeting held on 22nd August, 2024 and subsequently passed by the Board of Deans at its meeting held on 3rd September, 2024 **vide** item No. 6.21 (N) have been accepted by the Hon'ble Vice Chancellor as per the power confirmed upon him under section 12(7) of the Maharashtra Public Universities Act, 2016 and that in accordance therewith **to introduce B.Voc (Cyber Security and Digital Forensics) Sem – III & IV** with effect from the academic year 2024-25.

(The Circular is available on the University's website www.mu.ac.in).

(Dr. Prasad Karande)
REGISTRAR

MUMBAI – 400 032
30th September, 2024

To

All the Principals of the Affiliated Colleges, Directors of the Recognized Institutions and the Head, University Departments.

BOD 6.21(N) 03/09/2024

Copy forwarded with Compliments for information to:-

1) The Chairman, Board of Deans,
2) The Dean, Faculty of Technology,
3) The Chairman, **Faculty of Information Technology**
4) The Director, Board of Examinations and Evaluation,
5) The Director, Department of Students Development,
6) The Director, Department of Information & Communication Technology,
7) The Director, Centre for Distance and Online Education (CDOE) Vidyanagari,
8) The Deputy Registrar, Admission, Enrolment, Eligibility & Migration Department (AEM),

Copy forwarded for information and necessary action to :-	
1	The Deputy Registrar, (Admissions, Enrolment, Eligibility and Migration Dept)(AEM), dr@eligi.mu.ac.in
2	The Deputy Registrar, Result unit, Vidyanagari drresults@exam.mu.ac.in
3	The Deputy Registrar, Marks and Certificate Unit,. Vidyanagari dr.verification@mu.ac.in
4	The Deputy Registrar, Appointment Unit, Vidyanagari dr.appointment@exam.mu.ac.in
5	The Deputy Registrar, CAP Unit, Vidyanagari cap.exam@mu.ac.in
6	The Deputy Registrar, College Affiliations & Development Department (CAD), deputyregistrar.uni@gmail.com
7	The Deputy Registrar, PRO, Fort, (Publication Section), Pro@mu.ac.in
8	The Deputy Registrar, Executive Authorities Section (EA) eau120@fort.mu.ac.in He is requested to treat this as action taken report on the concerned resolution adopted by the Academic Council referred to the above circular.
9	The Deputy Registrar, Research Administration & Promotion Cell (RAPC), rapc@mu.ac.in
10	The Deputy Registrar, Academic Appointments & Quality Assurance (AAQA) dy.registrar.tau.fort.mu.ac.in ar.tau@fort.mu.ac.in
11	The Deputy Registrar, College Teachers Approval Unit (CTA), concolsection@gmail.com
12	The Deputy Registrars, Finance & Accounts Section, fort draccounts@fort.mu.ac.in
13	The Deputy Registrar, Election Section, Fort drelection@election.mu.ac.in
14	The Assistant Registrar, Administrative Sub-Campus Thane, thanesubcampus@mu.ac.in
15	The Assistant Registrar, School of Engg. & Applied Sciences, Kalyan, ar.seask@mu.ac.in
16	The Assistant Registrar, Ratnagiri Sub-centre, Ratnagiri, ratnagirisubcentar@gmail.com
17	The Director, Centre for Distance and Online Education (CDOE), Vidyanagari, director@idol.mu.ac.in
18	Director, Innovation, Incubation and Linkages, Dr. Sachin Laddha pinkumanno@gmail.com
19	Director, Department of Lifelong Learning and Extension (DLLE), dlleuniversityofmumbai@gmail.com

Copy for information :-	
1	P.A to Hon'ble Vice-Chancellor, vice-chancellor@mu.ac.in
2	P.A to Pro-Vice-Chancellor pvc@fort.mu.ac.in
3	P.A to Registrar, registrar@fort.mu.ac.in
4	P.A to all Deans of all Faculties
5	P.A to Finance & Account Officers, (F & A.O), camu@accounts.mu.ac.in

To,

1	The Chairman, Board of Deans pvc@fort.mu.ac.in
2	**Faculty of Humanities,** **Dean** 1. Prof.Anil Singh Dranilsingh129@gmail.com **Associate Dean** 2. Dr.Suchitra Naik Naiksuchitra27@gmail.com 3.Prof.Manisha Karne mkarne@economics.mu.ac.in
	Faculty of Commerce & Management, **Dean** 1. Dr.Kavita Laghate kavitalaghate@jbims.mu.ac.in **Associate Dean** 2. Dr.Ravikant Balkrishna Sangurde Ravikant.s.@somaiya.edu 3. Prin.Kishori Bhagat kishoribhagat@rediffmail.com

	Faculty of Science & Technology **Dean** 1. Prof. Shivram Garje ssgarje@chem.mu.ac.in **Associate Dean** 2. Dr. Madhav R. Rajwade Madhavr64@gmail.com 3. Prin. Deven Shah sir.deven@gmail.com
	Faculty of Inter-Disciplinary Studies, **Dean** 1.Dr. Anil K. Singh aksingh@trcl.org.in **Associate Dean** 2.Prin.Chadrashekhar Ashok Chakradeo cachakradeo@gmail.com
3	Chairman, Board of Studies,
4	The Director, Board of Examinations and Evaluation, dboee@exam.mu.ac.in
5	The Director, Board of Students Development, dsd@mu.ac.in DSW direcotr@dsw.mu.ac.in
6	The Director, Department of Information & Communication Technology, director.dict@mu.ac.in

BOD – 3/9/2024
12 (7) of M.P.U.A. 2016
Item No. — 6.21 (N)

UNIVERSITY OF MUMBAI

Title of the U.G. Program

B. Voc. (Cyber Security and Digital Forensics)

Syllabus for

Semester III & IV

(As per AICTE guidelines with effect from the academic year 2024–2025)

UNIVERSITY OF MUMBAI

Syllabus for Approval

Sr. No.	Heading	Particulars
1	Title of the Course	**B.Voc. (Cyber Security and Digital Forensics)**
2	Eligibility for Admission	**After Passing First Year Engineering as per the Ordinance 0.6242**
3	Passing Marks	**40%**
4	No. of Years / Semesters	**3 years/6 semesters**
5	Level	~~P.G.~~ / **U.G.**/ ~~Diploma / Certificate~~ (Strike out which is not applicable)
6	Pattern	~~Yearly~~ / **Semester** (Strike out which is not applicable)
7	Status	**New** / ~~Revised~~ (Strike out which is not applicable)
8	To be implemented from Academic Year	**With effect from Academic Year: 2023-2024**

Offg. Associate Dean
Dr. Deven Shah
Faculty of Science and Technology
Technology University of Mumbai

Offg. Dean
Prof. Shivram S. Garje
Faculty of Science and
University of Mumbai

Preamble

To meet the challenge of ensuring excellence in engineering education, the issue of quality needs to be addressed, debated and taken forward in a systematic manner. Accreditation is the principal means of quality assurance in higher education. The major emphasis of the accreditation process is to measure the outcomes of the program that is being accredited. In line with this, the Faculty of Science and Technology (in particular Engineering) of University of Mumbai has taken a lead in incorporating philosophy of outcome based education in the process of curriculum development.

Faculty resolved that course objectives and course outcomes are to be clearly defined for each course, so that all faculty members in affiliated institutes understand the depth and approach of course to be taught, which will enhance the learner's learning process. Choice based Credit and grading systems enables a much-required shift in focus from teacher-centered to learner-centric education since the workload estimated is based on the investment of time in learning and not in teaching. It also focuses on continuous evaluation which will enhance the quality of education. Credit assignment for courses is based on 15 weeks teaching learning process, however content of courses is to be taught in 13 weeks and remaining 2 weeks to be utilized for revision, guest lectures, coverage of content beyond syllabus etc.

There was a concern that the earlier revised curriculum was more focused on providing information and knowledge across various domains of the said program, which led to heavy loading of students in terms of direct contact hours. In this regard, the faculty of science and technology resolved that to minimize the burden of contact hours, total credits of the entire program will be of 170, wherein focus is not only on providing knowledge but also on building skills, attitude and self-learning. Therefore in the present curriculum skill based laboratories and mini projects are made mandatory across all disciplines of engineering in the second and third year of programs, which will definitely facilitate self-learning of students. The overall credits and approach of curriculum proposed in the present revision is in line with AICTE model curriculum.

The present curriculum will be implemented for the First of B.Voc Cyber Security and Digital Forensics from the academic year 2023-24. Subsequently this will be carried forward for Second Year and Final Year Engineering in the academic years 2024-25, 2025-26, respectively.

Preface by Board of Studies in _____

Dear Students and Teachers, we, the members of Board of Studies _____, are very happy to present the Second-year syllabus effective from the Academic Year 2024-25. We are sure you will find this syllabus interesting and challenging.

_____ is one of the most sought-after courses amongst engineering students hence there is a continuous requirement of revision of syllabus. The syllabus focuses on providing a sound theoretical background as well as good practical exposure to students in the relevant areas. It is intended to provide a modern, industry-oriented education in Computer Engineering. It aims at producing trained professionals who can successfully become acquainted with the demands of the industry worldwide. They obtain skills and experience in up-to-date knowledge to analysis, design, implementation, validation, and documentation of computer software and systems.

The revised syllabus falls in line with the objectives of affiliating University, AICTE, UGC, and various accreditation agencies by keeping an eye on the technological developments, innovations, and industry requirements.

The salient features of the revised syllabus are:

1. Reduction in credits to 60(30+30) is implemented to ensure that students have more time for extracurricular activities, innovations, and research and On Job Training (OJT).
2. Introduction of Skill Based Lab and Mini Project to showcase their talent by doing innovative projects that strengthen their profile and increase the chance of employability.
3. Students are encouraged to take up part of course through MOOCs platform SWAYAM

We would like to place on record our gratitude to the faculty, students, industry experts and stakeholders for having helped us in the formulation of this syllabus.

Board of Studies in _____

: Chairman

: Member

: Member

: Member

: Member

: Member

: Member

: Member

: Member

:Member

Program Structure for First Year B. Voc Cyber Security and Digital Forensics
UNIVERSITY OF MUMBAI (With Effect from 2023-2024)

Semester I

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
General Education Component								
BVCDFG101	Professional Skill-I (Soft Skill Development)	3	-	1*	3	--	1	4
BVCDFG102	Applied Mathematics	3	-	1*	3	--	1	4
BVCDFG103	Programming principles with C	3	2	-	3	1	--	4
	Total	9	2	2	9	1	2	12
Skill Component								
BVCDFS101	Computer Networks	3	2	-	3	1	--	4
BVCDFS102	Cybersecurity Fundamentals	3	2	-	3	1	--	4
BVCDFS103	Operating System and Network Security	3	2	-	3	1	--	4
BVCDFS104	On Job Training/ Skill based Internship	-	12	-	--	6#	--	6
	Total	**9**	**18**	**--**	**9**	**9**	**--**	**18**
Grand Total		**18**	**20**	**2**	**18**	**10**	**2**	**30**

Course Code	Course Name	Examination Scheme							
		Theory					Term Work	Pract. &oral	Total
		Internal Assessment			End Sem. Exam	Exam. Duration (in Hrs)			
		Test 1	Test2	Avg					
General Education Component									
BVCDFG101	Professional Skill-I (Soft Skill Development)	10	10	10	40	2			50
BVCDFG102	Applied Mathematics	20	20	20	80	3	25	--	125
BVCDFG103	Programming principles with C	20	20	20	80	3	25	25	150
Skill Component									
BVCDFS101	Computer Networks	20	20	20	80	3	25	25	150
BVCDFS102	Cybersecurity	20	20	20	80	3	25	25	150

	Fundamentals								
BVCDFS103	Operating System and Network Security	20	20	20	80	3	25	25	150
BVCDFS104	On Job Training/ Skill based Internship	--	--	--	--	--	50#	--	50
Total		**--**	**--**	**110**	**440**	**--**	**175**	**100**	**825**

- *Should be conducted batch wise.
- # Indicates Practical and Oral Marks includes report and presentation.

Program Structure for First Year B. Voc Cyber Security and Digital Forensics
UNIVERSITY OF MUMBAI (With Effect from 2023-2024)

Semester II

Course Code	Course Name	Teaching Scheme (Contact hours)			Credits Assigned			
		Theory	**Pract.**	**Tut.**	**Theory**	**Pract.**	**Tut.**	**Total**
General Education Component								
BVCDFG201	Professional Skill-II (Business communication Ethics)	3	-	1*	3	--	1	4
BVCDFG202	Statistics for Data Science	3	-	1*	3	--	1	4
BVCDFG203	Digital Logic & Computer Architecture	3	2	-	3	1	--	4
	Total	9	2	2	9	1	2	12
Skill Component								
BVCDFS201	Python Programming	3	2	-	3	1	--	4
BVCDFS202	Web Application Security	3	2	-	3	1	--	4
BVCDFS203	Database Management and Security	3	2	-	3	1	--	4
BVCDFS204	On Job Training/ Skill based Internship	-	12	-	--	6#	--	6
	Total	**9**	**18**	**--**	**9**	**9**	**--**	**18**
Grand Total		**18**	**20**	**2**	**18**	**10**	**2**	**30**

Course Code	Course Name	Examination Scheme							
		Theory					**Term Work**	**Pract. &oral**	**Total**
		Internal Assessment			**End Sem. Exam**	**Exam. Duration (in Hrs)**			
		Test 1	**Test2**	**Avg**					
General Education Component									
BVCDFG201	Professional Skill-II	10	10	10	40	2			50

	(Business Communication Ethics)								
BVCDFG202	Statistics for Data Science	20	20	20	80	3	25	--	125
BVCDFG 203	Digital Logic & Computer Architecture	20	20	20	80	3	25	25	150
Skill Component									
BVCDFS201	Python Programming	20	20	20	80	3	25	25	150
BVCDFS202	Web Application Security	20	20	20	80	3	25	25	150
BVCDFS203	Database Management and Security	20	20	20	80	--	25	25	150
BVCDFS204	On Job Training/ Skill based Internship	--	--	--	--	--	50#	--	50
Total		**--**	**--**	**110**	**440**	**--**	**175**	**100**	**825**

- *Should be conducted batch wise.
- # Indicates Practical and Oral Marks includes report and presentation.

Program Structure for First Year B. Voc Cyber Security and Digital Forensics
UNIVERSITY OF MUMBAI (With Effect from 2023-2024)

Semester III

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
General Education Component								
BVCDFG 301	Professional Skill-III (Entrepreneurship)	3	-	1*	3	--	1	4
BVCDFG 302	Ethical Hacking	3	-	1*	3	--	1	4
BVCDFG 303	Machine Learning I	3	2	-	3	1	--	4
	Total	**9**	**2**	**2**	**9**	**1**	**2**	**12**
Skill Component								
BVCDFS 301	Cybersecurity Risk Management and Auditing	3	2		3	1	--	4
BVCDFS 302	Malware Analysis and Reverse Engineering	3	2	_	3	1	--	4
BVCDFS 303	Cyber Threat Intelligence	3	2	-	3	1	--	4
BVCDFS 304	On Job Training/ Skill based Internship	-	12	-	--	6#	--	6
	Total	**9**	**18**	**--**	**9**	**9**	**--**	**18**
Grand Total		**18**	**20**	**2**	**18**	**10**	**2**	**30**

Course Code	Course Name	Examination Scheme							
		Theory					Term Work	Pract. &oral	Total
		Internal Assessment			End Sem. Exam	Exam. Duration (in Hrs)			
		Test 1	Test2	Avg					
General Education Component									
BVCDFG 301	Professional Skill-III (Entrepreneurship)	10	10	10	40	2			50
BVCDFG 302	Ethical Hacking	20	20	20	80	3	25	--	125
BVCDFG 303	Machine Learning I	20	20	20	80	3	25	25	150
Skill Component									
BVCDFS 301	Cybersecurity Risk Management and Auditing	20	20	20	80	3	25	25	150
BVCDFS 302	Malware Analysis and Reverse Engineering	20	20	20	80	3	25	25	150
BVCDFS 303	Cyber Threat Intelligence	20	20	20	80	--	25	25	150
BVCDFS 304	On Job Training/ Skill	--	--	--	--	--	50#	--	50

	based Internship								
Total		**--**	**--**	**110**	**440**	**--**	**175**	**100**	**825**

- *Should be conducted batch wise.
- # Indicates Practical and Oral Marks includes report and presentation.

Program Structure for First Year B. Voc Cyber Security and Digital Forensics
UNIVERSITY OF MUMBAI (With Effect from 2023-2024)

Semester IV

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	**Pract.**	**Tut.**	**Theory**	**Pract.**	**Tut.**	**Total**
General Education Component								
BVCDFG 401	Professional Skill-IV (Aptitude and Logic Building)	3	-	1*	3	--	1	4
BVCDFG 402	Security Architecture and Engineering	3	-	1*	3	--	1	4
BVCDFG 403	Digital Forensics	3	2	-	3	1	--	4
	Total	**9**	**2**	**2**	**12**	**1**	**2**	**12**
Skill Component								
BVCDFS 401	Penetration Testing and Vulnerability Assessment	3	2		3	1	--	4
BVCDFS 402	Cybercrime Investigation Techniques	3	2	–	3	1	--	4
BVCDFS 403	Network Forensics	3	2	-	3	1	--	4
BVCDFS 404	On Job Training/ Skill based Internship	-	12	-	--	6#	--	6
	Total	**9**	**18**	**--**	**9**	**9**	**--**	**18**
Grand Total		**18**	**20**	**2**	**21**	**10**	**2**	**30**

Course Code	Course Name	Examination Scheme							
		Theory					**Term Work**	**Pract. &oral**	**Total**
		Internal Assessment			**End Sem. Exam**	**Exam. Duration (in Hrs)**			
		Test 1	**Test2**	**Avg**					
General Education Component									
BVCDFG 401	Professional Skill-IV (Aptitude and Logic Building)	10	10	10	40	2			50
BVCDFG 402	Security Architecture and Engineering	20	20	20	80	3	25	--	125
BVCDFG 403	Digital Forensics	20	20	20	80	3	25	25	150
Skill Component									
BVCDFS 401	Penetration Testing and	20	20	20	80	3	25	25	150

	Vulnerability Assessment								
BVCDFS 402	Cybercrime Investigation Techniques	20	20	20	80	3	25	25	150
BVCDFS 403	Network Forensics	20	20	20	80	--	25	25	150
BVCDFS 404	On Job Training/ Skill based Internship	--	--	--	--	--	50#	--	50
Total		**--**	**--**	**110**	**440**	**--**	**175**	**100**	**825**

- *Should be conducted batch wise.
- # Indicates Practical and Oral Marks includes report and presentation.

Program Structure for First Year B. Voc Cyber Security and Digital Forensics
UNIVERSITY OF MUMBAI (With Effect from 2023-2024)

Semester V

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
General Education Component								
BVCDFG 501	Professional Skill-IV (Cloud Forensics)	3	-	1*	3	--	1	4
BVCDFG 502	Environmental Management	3	-	1*	3	--	1	4
BVCDFG 503	Cyber Security Laws	3	2	-	3	1	--	4
	Total	**9**	**2**	**2**	**12**	**1**	**2**	**12**
Skill Component								
BVCDFS 501	Blockchain Forensics and Crypto-currency Investigation	3	2		3	1	--	4
BVCDFS 502	Ransomware Investigation	3	2	_	3	1	--	4
BVCDFS 503	Mobile Security and Forensics	3	2	-	3	1	--	4
BVCDFS 504	Major Project I	-	12	-	--	6#	--	6
	Total	**9**	**18**	**--**	**9**	**9**	**--**	**18**
Grand Total		**18**	**20**	**2**	**21**	**10**	**2**	**30**

Course Code	Course Name	Examination Scheme							
		Theory					Term Work	Pract. &oral	Total
		Internal Assessment			End Sem. Exam	Exam. Duration (in Hrs)			
		Test 1	Test2	Avg					
General Education Component									
BVCDFG 501	Professional Skill-IV (Cloud Forensics)	10	10	10	40	2			50
BVCDFG 502	Environmental Management	20	20	20	80	3	25	--	125
BVCDFG 503	Cyber Security Laws	20	20	20	80	3	25	25	150
Skill Component									
BVCDFS 501	Blockchain Forensics and Crypto-currency Investigation	20	20	20	80	3	25	25	150
BVCDFS 502	Ransomware Investigation	20	20	20	80	3	25	25	150
BVCDFS 503	Mobile Security and Forensics	20	20	20	80	--	25	25	150

BVCDFS 504	Major Project I	--	--	--	--	--	50#	--	50
Total		**--**	**--**	**110**	**440**	**--**	**175**	**100**	**825**

- *Should be conducted batch wise.
- # Indicates Practical and Oral Marks includes report and presentation.

Program Structure for First Year B. Voc Cyber Security and Digital Forensics
UNIVERSITY OF MUMBAI (With Effect from 2023-2024)

Semester VI

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
General Education Component								
BVCDFG 601	Professional Skill-IV (API Pentesting)	3	-	1*	3	--	1	4
BVCDFG 602	Information Retrieval System	3	-	1*	3	--	1	4
BVCDFG 603	Distributed Computing	3	2	-	3	1	--	4
	Total	**9**	**2**	**2**	**12**	**1**	**2**	**12**
Skill Component								
BVCDFS 601	Cloud Computing Security	3	2		3	1	--	4
BVCDFS 602	Machine Learning II	3	2	_	3	1	--	4
BVCDFS 603	Security information and Event Management.	3	2	-	3	1	--	4
BVCDFS 604	Major Project II	-	12	-	--	6#	--	6
	Total	**9**	**18**	**--**	**9**	**9**	**--**	**18**
Grand Total		**18**	**20**	**2**	**21**	**10**	**2**	**30**

Course Code	Course Name	Examination Scheme							
		Theory					Term Work	Pract. &oral	Total
		Internal Assessment			End Sem. Exam	Exam. Duration (in Hrs)			
		Test 1	Test2	Avg					
General Education Component									
BVCDFG 601	Professional Skill-IV (API Pentesting)	10	10	10	40	2			50
BVCDFG 602	Information Retrieval System	20	20	20	80	3	25	--	125
BVCDFG 603	Distributed Computing	20	20	20	80	3	25	25	150
Skill Component									
BVCDFS 601	Cloud Computing Security	20	20	20	80	3	25	25	150
BVCDFS 602	Machine Learning II	20	20	20	80	3	25	25	150
BVCDFS 603	Security Information and Event Management.	20	20	20	80	--	25	25	150

BVCDFS 604	Major Project II	--	--	--	--	--	50#	--	50
Total		**--**	**--**	**110**	**440**	**--**	**175**	**100**	**825**

- *Should be conducted batch wise.
- # Indicates Practical and Oral Marks includes report and presentation.

Program Structure for First Year B. Voc Cyber Security and Digital Forensics
UNIVERSITY OF MUMBAI (With Effect from 2024-2025)
Semester III

Course Code:	Course Title	Credit
BVCDFG 301	Professional Skill-III (Entrepreneurship)	4

Prerequisite: Business Communication Ethics	
Course Objectives:	
1	To provide a detailed overview of entrepreneurship as the foundation of business growth
2	To teach to adopt entrepreneurship as value creation in the national economy.
3	It provides multiple constructs for entrepreneurs to be successful.
4	It provides multiple pathways for their companies to achieve sustainable growth.
Course Outcomes:	
1	To understand key concepts underpinning entrepreneurship
2	To apply knowledge in the recognition and exploitation of product/ service/ process opportunities
3	To demonstrate key concepts underpinning innovation and the issues associated with developing and sustaining innovation within organizations
4	To understand, how to design creative strategies for pursuing, exploiting and further developing new opportunities
5	To understand Issues associated with securing and managing financial resources in new and established organizations.

Module		Content	Hrs
1		**Introduction to Entrepreneurial Journey**	**8**
	1.1	Entrepreneurial Journey	
	1.2	Entrepreneurial Discovery	
2		**Ideation and Prototyping**	**8**
	2.1	Ideation and Prototyping.	
	2.2	Testing, Validation and Commercialization, Disruption as a Success Driver	
3		**Technological Innovation and Entrepreneurship**	**8**
	3.1	Technological Innovation and Entrepreneurship – 1	

	3.2	Technological Innovation and Entrepreneurship – 2 ,Raising Financial Resources	
4		**Education and Entrepreneurship**	**7**
	4.1	Education and Entrepreneurship.	
	4.2	Beyond Founders and Founder-Families, India as a Start-up Nation	
5		**National Entrepreneurial Culture**	**7**
	5.1	National Entrepreneurial Culture.	
	5.2	Entrepreneurial Thermodynamics, Entrepreneurship and Employment.	
6		**Start-up Case Studies.**	**7**
	6.1	Discuss at least five case studies.	
Total			**45**

Textbooks:	
1	Peter Thiel "Zero to One: Notes on Startups, or How to Build the Future", Crown, 16 Sept 2014 - Business & Economics - 224 pages.
2	Eric Ries "The Lean Startup: How Today's Entrepreneurs Use Continuous Innovation to Create Radically Successful Businesses" published January 1, 2011, Board Book

Referecebooks:	
1	C B Rao "India as Global Start-up Hub: Mission with Passion" Notion Press, 2018,
2	Ashlee Vance ,"Elon Musk: Tesla, SpaceX, and the Quest for a Fantastic Future", Ecco Press, Publish Year: 2015
3	Walter Isaacson "Steve Jobs", October 1, 2011

Assessment:	
Internal Assessment:	
Assessment consists of two class tests of 10 marks each. The first class test is to be conducted when approx. 40% syllabus is completed and second class test when additional 40% syllabus is completed. Duration of each test shall be one hour.	
End Semester Theory Examination:	
1	Question paper will comprise of total six questions.
2	All question carries equal marks
3	Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3)
4	Only Four question need to be solved.

5	In question paper weightage of each module will be proportional to number of respective lecture hours as mention in the syllabus.

Useful Links	
1	https://onlinecourses.nptel.ac.in/noc20_mg35/preview.
2	https://www.business-school.ed.ac.uk/msc/entrepreneurship-innovation/overview/learning-outcomes

List of Tutorial:

Tutorial Number	**Tutorial Topic**
1	Field study of Industries offices in vicinity.
2	Visit to Atal incubation Center.
3	Create Business Model on any project.

Course Code:	Course Title	Credit
BVCDFG 302	**Ethical Hacking**	**4**

Prerequisite:	
Course Objectives:	
1	To describe Ethical hacking and fundamentals of computer Network.
2	To understand about Network security threats, vulnerabilities assessment and social engineering.
3	To discuss cryptography and its applications.
4	To implement the methodologies and techniques of Sniffing techniques, tools, and ethical issues.
5	To implement the methodologies and techniques of hardware security.
6	To demonstrate systems using various case studies.
Course Outcomes:	
1	Articulate the fundamentals of Computer Networks, IP Routing and core concepts of ethical hacking in real world scenarios.
2	Apply the knowledge of information gathering to perform penetration testing and social engineering attacks
3	Demonstrate the core concepts of Cryptography, Cryptographic checksums and evaluate the various biometric authentication mechanisms.
4	Apply the knowledge of network reconnaissance to perform Network and web application-based attacks.
5	Apply the concepts of hardware elements and endpoint security to provide security to physical devices.
6	Simulate various attack scenarios and evaluate the results.

I	**Introduction to Ethical Hacking**	Fundamentals of Computer Networks/IP protocol stack, IP addressing and routing, Routing protocol, Protocol vulnerabilities, Steps of ethical hacking, Demonstration of Routing Protocols using Cisco Packet Tracer **Self-learning Topics**:TCP/IP model, OSI model	**8**

II	**Introduction to Cryptography**	Private-key encryption, public key-encryption, key Exchange Protocols, Cryptographic Hash Functions & applications, steganography, biometric authentication, lightweight cryptographic algorithms.Demonstration of various cryptographic tools and hashing algorithms **Self-learning Topics**: Quantum cryptography, Elliptic curvecryptography	**8**
III	**Introduction to network security**	Information gathering, reconnaissance, scanning, vulnerability assessment, Open VAS, Nessus, System hacking: Password cracking, penetration testing, Social engineering attacks, Malware threats, hacking wireless networks (WEP, WPA, WPA- 2), Proxy network, VPN security, Study of various tools for Network Security such as Wireshark, John the Ripper, Metasploit, etc. **Self-learning Topics**: Ransomware(Wannacry), Botnets, Rootkits, Mobile device security	**12**
IV	**Introduction to web security and Attacks**	OWASP, Web Security Considerations, User Authentication, Cookies, SSL, HTTPS, Privacy on Web, Account Harvesting, Web Bugs, Sniffing, ARP poisoning, Denial of service attacks, Hacking Web Applications, Clickjacking, Cross-Site scripting and Request Forgery, Session Hijacking and Management, Phishing and Pharming Techniques, SSO, Vulnerability assessments, SQL injection, Web Service Security, OAuth 2.0, Demonstration of hacking tools on Kali Linux such as SQLMap, HTTrack, hping, burpsuite,Wireshark etc. **Self-learning Topics**: Format string attacks	**10**
V	**Elements of Hardware Security**	Side channel attacks, physical unclonable functions, Firewalls,Backdoors and trapdoors, Demonstration of Side Channel Attacks on RSA, IDS and Honeypots. **Self-learning Topics**: IoT security	**4**
VI	**Case Studies**	Various attacks scenarios and their remedies. Demonstration ofattacks using DVWA. **Self-learning Topics**: Session hijacking and man-in-middleattacks	**3**
Total			**45**

Textbooks:	
1	Computer Security Principles and Practice --William Stallings, Seventh Edition, Pearson Education, 2017
2	Security in Computing -- Charles P. Pfleeger, Fifth Edition, Pearson Education, 2015
3	Network Security and Cryptography -- Bernard Menezes, Cengage Learning, 2014
4	Network Security Bible -- Eric Cole, Second Edition, Wiley, 2011
5	Mark Stamp's Information Security: Principles and Practice --Deven Shah, Wiley, 2009
References:	
1	UNIX Network Programming –Richard Steven,Addison Wesley, 2003
2	Cryptography and Network Security -- Atul Kahate, 3rd edition, Tata Mc Graw Hill, 2013 3.TCP/IP Protocol Suite -- B. A. Forouzan, 4th Edition, Tata Mc Graw Hill, 2017
3	Applied Cryptography, Protocols Algorithms and Source Code in C -- Bruce Schneier, 2nd Edition / 20th Anniversary Edition, Wiley, 2015
4	UNIX Network Programming –Richard Steven,Addison Wesley, 2003
5	Cryptography and Network Security -- Atul Kahate, 3rd edition, Tata Mc Graw Hill, 2013 3.TCP/IP Protocol Suite -- B. A. Forouzan, 4th Edition, Tata Mc Graw Hill, 2017
Assessment:	
Internal Assessment:	
Assessment consists of two class tests of 20 marks each. The first class test is to be conducted when approximately 40% syllabus is completed and the second class test when an additional 40% syllabus is completed. Duration of each test shall be one hour.	
End Semester Theory Examination:	
1	Question paper will comprise a total of six questions.

2	All question carries equal marks
3	Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3then part (b) will be from any module other than module 3)
4	Only Four questions need to be solved.
5	In question paper weightage of each module will be proportional to number of respectivelecture hours as mentioned in the syllabus.

Useful Digital Links	
1	https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
2	https://dvwa.co.uk/
3	http://testphp.vulnweb.com/

Suggested List of Tutorials	
Sr. No.	**Title of Tutorials**
1	To implement Break a Caesar Cipher code.
2	Develop a network analyzer to monitor incoming and outgoing data packets on a specific network.
3	To explore **H4cker software**
4	Create a tool that records and stores every keystroke.
5	Set up your own lab environment with vulnerable web apps (e.g., DVWA, Mutillidae, or OWASP Juice Shop).
6	Explore platforms like Metasploit, Immunity Debugger, and IDA Pro.
7	Study smart contracts and blockchain vulnerabilities.
8	Learn about WPA/WPA2 cracking, rogue access points, and deauthentication attacks.

Course Code:	Course Title	Credit
BVCDFG 303	**Machine Learning I**	**4**

Prerequisite: Engineering Mathematics, Data Structures, Algorithms	
Course Objectives:	
1	To introduce the basic concepts and techniques of Machine Learning.
2	To acquire in depth understanding of various supervised and unsupervised algorithms
3	To be able to apply various ensemble techniques for combining ML models.
4	To demonstrate dimensionality reduction techniques.
Course Outcomes:	
1	To acquire fundamental knowledge of developing machine learning models.
2	To select, apply and evaluate an appropriate machine learning model for the given
3	To demonstrate ensemble techniques to combine predictions from different models.
4	To demonstrate the dimensionality reduction techniques.

Module		Content	Hrs
1		Introduction to Machine Learning	5
	1.1	Machine Learning, Types of Machine Learning, Issues in Machine Learning, Application of Machine Learning, Steps in developing a Machine Learning Application.	
	1.2	Training Error, Generalization error, Overfitting, Underfitting, Bias-Variance trade-off.	
2		Learning with Regression and Trees	10
	2.1	Learning with Regression: Linear Regression, Multivariate Linear Regression, Logistic Regression.	

	2.2	Learning with Trees: Decision Trees, Constructing Decision Trees using Gini Index (Regression), Classification and Regression Trees (CART)	
	2.3	Performance Metrics: Confusion Matrix, [Kappa Statistics], Sensitivity, Specificity, Precision, Recall, F-measure, ROC curve	
3		Ensemble Learning	7
	3.1	Understanding Ensembles, K-fold cross validation, Boosting, Stumping, XGBoost	
	3.2	Bagging, Subagging, Random Forest, Comparison with Boosting, Different ways to combine classifiers	
4		Learning with Classification	8
	4.1	Support Vector Machine Constrained Optimization, Optimal decision boundary, Margins and support vectors, SVM as constrained optimization problem, Quadratic Programming, SVM for linear and nonlinear classification, Basics of	
		Kernel trick.	
	4.2	Support Vector Regression, Multiclass Classification	
5		Learning with Clustering	8
	5.1	Introduction to clustering with overview of distance metrics and major clustering approaches.	
	5.2	Graph Based Clustering: Clustering with minimal spanning tree Model based Clustering: Expectation Maximization Algorithm, Density Based Clustering: DBSCAN	
6		Dimensionality Reduction	7
	6.1	Dimensionality Reduction Techniques, Principal Component Analysis, Linear Discriminant Analysis, Singular Valued Decomposition.	
Total			**45**

Textbooks:	
1	Peter Harrington, ―Machine Learning n Action‖, DreamTech Press
2	Ethem Alpaydın, ―Introduction to Machine Learning‖, MIT Press
3	Tom M. Mitchell, ―Machine Learning‖ McGraw Hill
4	Stephen Marsland, ―Machine Learning An Algorithmic Perspective‖, CRC Press
References:	

1	Han Kamber, ―Data Mining Concepts and Techniques‖, Morgan Kaufmann Publishers
2	Margaret. H. Dunham, ―Data Mining Introductory and Advanced Topics, Pearson Education
3	Kevin P. Murphy , Machine Learning ― A Probabilistic Perspective‖
4	Samir Roy and Chakraborty, ―Introduction to soft computing‖, Pearson Edition.
5	Richard Duda, Peter Hart, David G. Stork, –Pattern Classification‖, Second Edition, Wiley Publications.
Assessment:	
Internal Assessment:	
Assessment consists of two class tests of 20 marks each. The first class test is to be conducted when approximately 40% syllabus is completed and the second class test when an additional 40% syllabus is completed. Duration of each test shall be one hour.	
End Semester Theory Examination:	
1	Question paper will comprise a total of six questions.
2	All question carries equal marks
3	Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3then part (b) will be from any module other than module 3)
4	Only Four questions need to be solved.
5	In question paper weightage of each module will be proportional to number of respectivelecture hours as mentioned in the syllabus.

Useful Digital Links	
1	Data sets for Machine Learning algorithms: https://www.kaggle.com/datasets
2	Machine Learning repository- https://archive.ics.uci.edu/ml/index.php
3	Machine Learning from Coursera
4	https://towardsdatascience.com/machine-learning/home
5	https://onlinecourses.nptel.ac.in/noc21_cs85/preview

Suggested List of Experiments	
Sr. No.	**Title of Experiment**
1	To implement Linear Regression.
2	To implement Logistic Regression.
3	To implement Ensemble learning (bagging/boosting)
4	To implement multivariate Linear Regression.
5	To implement SVM
6	To implement PCA/SVD/LDA
7	To implement Graph Based Clustering
8	To implement DB Scan
9	To implement CART
10	To implement LDA

Course Code:	Course Title	Credit
BVCDFS 301	Cyber Security Risk Management and Auditing	4

Prerequisite: No Prerequisite	
Course Objectives:	
1	Gain a solid understanding of essential cyber security principles and their importance in protecting organizational assets.
2	Learn the risk management lifecycle and effectively apply risk assessment methodologies, both qualitative and quantitative.
3	Recognize various types of cyber threats and common attack vectors, and analyze vulnerabilities through real-world case studies.
4	Create and enforce comprehensive cyber security policies and procedures, ensuring compliance and regular updates.
5	Develop a robust incident response plan, manage incidents effectively, and perform post-incident activities to enhance organizational resilience.
Course Outcomes: On Successful completion of course, learner will be able to	
1	Demonstrate a strong grasp of essential cyber security concepts and their role in protecting organizational assets.
2	Perform risk assessments using qualitative and quantitative methods, applying frameworks like NIST and ISO/IEC 27005.
3	Recognize various cyber threats and attack vectors, and analyze vulnerabilities through real-world case studies.
4	Create, implement, and enforce comprehensive cyber security policies and procedures, ensuring compliance and regular updates.
5	Develop a robust incident response plan, manage incidents from detection to recovery, and conduct post-incident reviews to enhance resilience.

Module		Content	Hrs
1		**Introduction to Cyber Security and Risk Management**	**8**
	1.1	Introduction to Cyber Security, Understanding Cyber Security, Importance of Risk Management.	
	1.2	Key Concepts and Terminology, The Risk Management Lifecycle, Practical Exercise: Risk Management Scenario Analysis.	
	1.3	Types of Cyber Threats, Common Attack Vectors.	
2		**Identifying Threats and Vulnerabilities**	**8**
	2.1	Understanding Vulnerabilities, Case Studies of Major Cyber Incidents	
	2.2	Practical Exercise: Identifying Threats and Vulnerabilities	
	2.3	Introduction to Risk Assessment, Qualitative vs. Quantitative Risk Assessment	
3		**Risk Assessment Methodologies**	**8**
	3.1	Risk Assessment Frameworks:- NIST, ISO/IEC 27005,etc	
	3.2	Practical Exercise: Understanding Different Frameworks	
	3.3	Conducting Risk Assessments	
4		**Identifying, Analyzing, and Mitigating Risks**	**6**
	4.1	Identifying and Analyzing Risks, Practical Exercise: Performing a Risk Assessment	
	4.2	Risk Mitigation Strategies, Risk Avoidance, Risk Reduction	
	4.3	More on Risk Mitigation, Risk Sharing and Transfer, Risk Acceptance	
5		**Implementing Security Controls and Policies**	**7**
	5.1	Implementing Security Controls, Practical Exercise: Developing a Risk Mitigation Plan	
	5.2	Developing Cyber Security Policies, Implementing Cyber Security Procedures	
	5.3	Policy Enforcement and Compliance, Regular Review and Updates, Practical Exercise: Drafting Cyber Security Policies	
6		**Cyber Security Frameworks and Incident Response**	**8**
	6.1	Overview of Key Cyber Security Frameworks, NIST Cybersecurity Framework	
	6.2	More on Frameworks and Standards, ISO/IEC 27001 and 27002, CIS Controls, Industry-Specific Standards, Practical Exercise: Mapping Organizational Controls to Frameworks	

	6.3	Incident Response Planning, Incident Detection and Analysis, Containment, Eradication, and Recovery, Post-Incident Activities. Developing an Incident Response Team, Practical Exercise: Simulating an Incident Response	
Total			**45**

Textbooks:	
1	**Information Security Risk Assessment Toolkit:** Practical Assessments through Data Collection and Data Analysis by Mark Talabis, Jason Martin, 1st Edition
References:	
1	**Risk Management Framework:** A Lab-Based Approach to Securing Information Systems by James Broad, Kelly Stewart, 1st Edition
Useful Link for E-Resources:	
1	Cyber Security Risk Management | Udemy
2	Introduction to Cybersecurity & Risk Management Specialization [3 courses] (UC Davis) | Coursera
3	Cybersecurity Audit Certificate | ISACA
4	https://onlinecourses.nptel.ac.in/noc23_cs127/preview
5	https://onlinecourses.nptel.ac.in/noc24_cs85/preview

Assessment:	
Internal Assessment:	
Assessment consists of two class tests of 20 marks each. The first-class test is to be conducted when approx. 40% syllabus is completed and the second-class test when an additional 40% syllabus is completed. Duration of each test shall be one hour.	
End Theory Examination:	
1	Question paper will comprise a total of six questions.
2	All question carries equal marks
3	Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3)
4	Only four questions need to be solved.
5	In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus.

Suggested List of Experiments

Sr. No.	**Title of Experiment**
1	Case Studies to be done on each Module for at least five Organizations/Company/Corporate.

Course Code:	Course Title	Credit
BVCDFS 302	Malware Analysis and Reverse Engineering	4

Prerequisite: No Prerequisite	
Course Objectives:	
1	Provide a comprehensive understanding of the various types of malware and their impact on computer systems.
2	Equip students with essential skills in static and dynamic malware analysis techniques.
3	Develop proficiency in reverse engineering and understanding malicious code through hands-on exercises.
4	Introduce advanced methods for detecting, analyzing, and mitigating sophisticated malware threats.
5	Enhance the ability to effectively communicate findings and collaborate with cybersecurity teams.
Course Outcomes: On Successful completion of course, learner will be able to	
1	Demonstrate a thorough understanding of malware types, behaviors, and the threats they pose.
2	Apply static and dynamic analysis techniques to dissect and understand malware samples.
3	Utilize reverse engineering tools to deconstruct and analyze executable files.
4	Identify and bypass obfuscation and anti-analysis techniques used by advanced malware.
5	Produce comprehensive analysis reports and effectively communicate technical findings to various stakeholders.

Module		Content	Hrs
1		**Introduction to Malware Analysis**	**8**
	1.1	Definition and Types of Malware, Historical Perspective and Evolution of Malware, Impact and Consequences of Malware Attacks	
	1.2	Goals and Objectives of Malware Analysis, Ethical and Legal Considerations, Malware Analysis Methodologies (Static vs. Dynamic Analysis)	
	1.3	Creating Isolated Sandboxes, Tools for Malware Analysis (Virtual Machines, Snapshots), Network Simulation and Monitoring Tools	
2		**Static Malware Analysis**	**8**
	2.1	Understanding File Formats (PE, ELF, Mach-O), Hashing and File Fingerprinting, Identifying Packing and Obfuscation Techniques	
	2.2	Extracting Metadata with Tools (e.g., PEiD, Exeinfo PE), Strings Analysis and Indicators of Compromise (IoCs), File Signature Analysis	
	2.3	Disassembly with IDA Pro and Ghidra, Code Analysis and Reverse Engineering, Recognizing and Understanding Common Code Constructs	
3		**Dynamic Malware Analysis**	**8**
	3.1	Behavioral Analysis:- Setting Up Dynamic Analysis Tools (e.g., Cuckoo Sandbox), Monitoring File System, Registry, and Network Activity, Identifying Behavioral Indicators	
	3.2	Memory Analysis: - Introduction to Volatility Framework, Capturing and Analyzing Memory Dumps, Extracting Artifacts from Memory	
	3.3	Advanced Dynamic Analysis: - Debugging Malware with OllyDbg and x64dbg, API Call Monitoring and Analysis, Identifying Anti-Analysis Techniques and Countermeasures	
4		**Reverse Engineering Fundamentals**	**6**
	4.1	Introduction, Objectives and Use Cases of Reverse Engineering, Legal and Ethical Considerations, Overview of Reverse Engineering Tool	
	4.2	Assembly Language Basics: - Understanding CPU Architectures (x86, x64), Assembly Language Syntax and Instructions, Converting High-Level Code to Assembly	
	4.3	Analyzing Executables, Examining Executable Headers, Function Identification and Analysis, Control Flow Graphs and Call Graphs	
5		**Advanced Reverse Engineering Techniques**	**7**

	5.1	Code Obfuscation and Anti-Reversing Techniques, Common Obfuscation Methods (e.g., Packing, Encryption), Identifying and Bypassing Anti-Debugging Mechanisms, Techniques for Deobfuscating Code	
	5.2	Reversing Network Protocols, Capturing and Analyzing Network Traffic, Understanding Custom Protocols, Reconstructing Protocol Specifications	
	5.3	Reversing Malicious Code, Case Studies of Reversing Real-World Malware, Techniques for Extracting Decryption Keys, Analyzing Polymorphic and Metamorphic Malware	
6		**Practical Malware Analysis and Reporting**	**8**
	6.1	Comprehensive Malware Analysis, End-to-End Analysis of Malware Samples, Documenting Findings and IoCs, Developing Mitigation and Response Strategies	
	6.2	Reporting and Communication, Writing Detailed Malware Analysis Reports, Communicating Technical Findings to Non-Technical Audiences, Collaboration with Incident Response Teams	
	6.3	Capstone Project: Real-World Malware Analysis, Practical Exercise: Analyzing a Complex Malware Sample, Presentation of Findings and Defense Strategies, Peer Review and Feedback Session	
Total			**45**

Textbooks:	
1	**Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software**, Michael Sikorski and Andrew Honig, 1st Edition.
References:	
1	**Malware Analyst's Cookbook and DVD:** Tools and Techniques for Fighting Malicious Code, Michael Ligh, Steven Adair, Blake Hartstein, and Matthew Richard, 1st Edition
Useful Link for E-Resources:	
1	Reverse Engineering & Malware Analysis in 21 Hours | REMAC+ | Udemy
2	FREE Intro to Malware Analysis & Reverse Engineering Online Training Course | Cybrary
3	MARE- Malware Analysis and Reverse Engineering Certification Course (hackerassociate.com)
4	https://blog.securitybreak.io/my-top-books-to-learn-malware-analysis-and-reverse-engineering-2ae1c6e209b9
5	https://medium.com/@ivancmoliveira/reverse-engineering-and-analyzing-malware-wannacry-3ce8b3f6406a

Assessment:

Internal Assessment:	
Assessment consists of two class tests of 20 marks each. The first-class test is to be conducted when approx. 40% syllabus is completed and the second-class test when an additional 40% syllabus is completed. Duration of each test shall be one hour.	
End Theory Examination:	
1	Question paper will comprise a total of six questions.
2	All question carries equal marks
3	Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3)
4	Only four questions need to be solved.
5	In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus.

Suggested List of Experiments	
Sr. No.	**Title of Experiment**
1	Packet sniffing with Wire shark
2	Capturing intruders through packet inspection
3	Analysis of various Malware types and behavior
4	Basic Static Analysis
5	Basic Dynamic Analysis
6	Analyzing windows programs
7	Android malware analysis
8	Data encoding and malware countermeasures
9	Comparative study of various malware analysis tools
10	Tools available in Antivirus Application.

Course Code:	Course Title	Credit
BVCDFS 303	Cyber Threat Intelligence	4

Prerequisite: No Prerequisite	
Course Objectives:	
1	Provide a comprehensive understanding of the cyber threat landscape and the importance of threat intelligence.
2	Equip students with essential skills in gathering, analyzing, and interpreting threat data.
3	Develop proficiency in utilizing threat intelligence tools and frameworks through hands-on exercises.
4	Introduce advanced methods for predicting and mitigating cyber threats.
5	Enhance the ability to effectively communicate threat intelligence findings and collaborate with cybersecurity teams.
Course Outcomes: On Successful completion of course, learner will be able to	
1	Demonstrate a thorough understanding of cyber threats, threat actors, and their tactics, techniques, and procedures (TTPs).
2	Apply various methodologies to gather and analyze cyber threat intelligence data.
3	Utilize threat intelligence platforms and tools to identify and assess threats.
4	Develop strategies to predict and mitigate potential cyber threats based on intelligence data.
5	Produce comprehensive threat intelligence reports and effectively communicate findings to various stakeholders.

Module		Content	Hrs
1		**Introduction to Cyber Threat Intelligence**	**8**
	1.1	Definition and Importance of CTI, History and Evolution of Cyber Threat Intelligence, Types of Threat Intelligence (Strategic, Operational, Tactical, Technical)	
	1.2	Understanding Key CTI Concepts and Terminology, The Intelligence Lifecycle, Practical Exercise: CTI Scenario Analysis	
	1.3	Types of Cyber Threats, Common Attack Vectors, Threat Actors and Their Motivations	
2		**Threat Data Collection and Sources**	**8**
	2.1	Threat Data Collection Techniques:- Passive and Active Data Collection Methods, Open Source Intelligence (OSINT), Human Intelligence (HUMINT)	
	2.2	Practical Exercise: Collecting Threat Data, Hands-on Exercise in Collecting Data from Various Sources, Ensuring Data Quality and Relevance	
	2.3	Overview of Popular TIPs, Integrating Data Sources with TIPs, Practical Exercise: Setting Up a TIP	
3		**Analyzing Cyber Threat Intelligence**	**8**
	3.1	Threat Analysis Techniques:- Qualitative and Quantitative Analysis Methods, Indicators of Compromise (IoCs), Analyzing Tactics, Techniques, and Procedures (TTPs)	
	3.2	Practical Exercise: Threat Analysis, Hands-on Analysis of Collected Threat Data, Using Analytical Tools and Techniques	
	3.3	Advanced Threat Analysis:- Pattern Recognition and Trend Analysis, Attribution and Profiling Threat Actors, Case Studies of Major Cyber Incidents	
4		**Threat Intelligence Frameworks and Models**	**6**
	4.1	Introduction to Popular CTI Frameworks	
	4.2	(MITRE ATT&CK, Diamond Model), Understanding the Kill Chain Model	
	4.3	Conducting Threat Intelligence Operations, Planning and Executing CTI Operations, Threat Hunting and Incident Response Integration, Case Studies of Successful CTI Operations	
5		**Communicating Threat Intelligence**	**7**

	5.1	Reporting and Disseminating Intelligence:- Writing Effective Threat Intelligence Reports, Visualizing Data for Better Understanding, Communicating Findings to Different Audiences	
	5.2	Practical Exercise: Reporting Threat Intelligence:- Creating and Presenting Threat Intelligence Reports, Peer Review and Feedback	
	5.3	Collaboration and Sharing Intelligence:- Information Sharing and Analysis Centers (ISACs), Legal and Ethical Considerations in Sharing Intelligence, Best Practices for Collaboration	
6		**Advanced Threat Intelligence Techniques**	**8**
	6.1	Predictive Intelligence and Threat Forecasting:- Predictive Analytics in CTI, Tools and Techniques for Threat Forecasting, Practical Exercise: Predicting Future Threats	
	6.2	Cyber Threat Intelligence Automation:- Leveraging AI and Machine Learning in CTI, Automating Data Collection and Analysis, Practical Exercise: Implementing Automation in CTI	
	6.3	Capstone Project: Real-World CTI Analysis, Comprehensive Threat Intelligence Analysis Project, Presentation of Findings and Recommendations, Whole Review and Doubts Session	
Total			**45**

Textbooks:	
1	**Cyber Threat Intelligence: From Strategy to Implementation by Henry Dalziel, 1st Edition**
References:	
1	**The Threat Intelligence Handbook:** A Practical Guide for Security Teams to Unlocking the Power of Intelligence by Chris Poulin, et al., 1st Edition
Useful Link for E-Resources:	
1	Certified Cyber Threat Intelligence Analyst | Udemy
2	Cyber Threat Intelligence Course by IBM | Coursera
3	Threat Intelligence Training | CTIA Certification | EC-Council (eccouncil.org)
4	https://medium.com/@ivancmoliveira/reverse-engineering-and-analyzing-malware-wannacry-3ce8b3f6406a
5	https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Assessment:	
Internal Assessment:	
Assessment consists of two class tests of 20 marks each. The first-class test is to be conducted when approx. 40% syllabus is completed and the second-class test when an additional 40% syllabus is completed. Duration of each test shall be one hour.	
End Theory Examination:	
1	Question paper will comprise a total of six questions.
2	All question carries equal marks
3	Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3)
4	Only four questions need to be solved.
5	In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus.

Suggested List of Experiments	
Sr. No.	**Title of Experiment**
1	Study on threat modeling for an Organisaton.
2	Study on the threat intelligence lifecycle,
3	Study on frameworks like MITRE ATT&CK and STRIDE.
4	Study about log aggregation tools,
5	vulnerability scanners,
6	how to evaluate cyber risk using frameworks like CVSS.
7	Study on threat modeling for an Organisaton.
8	Study on the threat intelligence lifecycle,
9	Study on frameworks like MITRE ATT&CK and STRIDE.

Program Structure for First Year B. Voc Cyber Security and Digital Forensics
UNIVERSITY OF MUMBAI (With Effect from 2024-2025)
Semester IV

Course Code:	Course Title	Credit
BVCDFG 401	**Professional Skill-IV (Aptitude and Logic Building)**	**4**

Prerequisite:	
Course Objectives:	
1	This course aims to provide an exposure in creating and delivering effective multimedia presentations that convey the key points.
2	Analyzing data in spreadsheet
3	How to write technical report
Course Outcomes:	
1	Understand Programs and Computers
2	Learn how programs and codes operate by using code and scratch.
3	To develop your critical thinking and reasoning skills.
4	The capacity to comprehend searching and sorting
5	Capacity to use formal mathematics to define computer programs (such as recursive functions)
6	Determine the truth value of unquantified phrases by using logical principles to define sets using the list or set builder notation and connecting symbolic laws of logic.

I	**Introduction to Computers**	Computer Systems, Computer Languages, Software Development, Operating System, Number Systems and their conversion, Crypt arithmetic Problems, Pseudocode and Flowchart	**10**

II	**Introduction to Code and Scratch**	Introduction to code (Sequence, if..else and Loops) Design a small code in scratch(animation)	**8**
III	**Critical thinking and logical reasoning**	Critical Thinking: What does it mean to think critically? An overview of definition, Computer programming and logical thinking	**8**
IV	**Searching and Sorting Techniques**	Searching Techniques: Linear Search, Binary Search Sorting Techniques: Selection, Insertion,	**6**
V	**Quantitative Abilities**	Problems on Ages Problems on Profit and Loss Problems on Simple and Compound Interest Problems on Time and Distance	**7**
VI	**Logical Reasoning & Verbal Reasoning**	Number Series Alpha Numerical, Letter & Symbol Series Numerical and Alphabet Puzzles Seating Arrangement Para – Jumble, Text Completion	**6**
Total			**45**

Textbooks:	
1	Computational Thinking, Karl Beecher BCS, The Chartered Institute for IT, 1th Edition,2017
2	Introduction to Algorithm ,Thomas Corman,PHI,3th Edition,2010
References:	
1	Think Smarter: Critical Thinking to Improve Problem-Solving and Decision-Making Skills Michael Kallet, Wiley, 2nd Edition, 2014
Assessment:	
Internal Assessment:	
Assessment consists of two class tests of 10 marks each. The first class test is to be conducted when approximately 40% syllabus is completed and the second class test when an additional 40% syllabus is completed. Duration of each test shall be one hour.	
End Semester Theory Examination:	

1	Question paper will comprise a total of six questions.
2	All question carries equal marks
3	Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3then part (b) will be from any module other than module 3)
4	Only Four questions need to be solved.
5	In question paper weightage of each module will be proportional to number of respectivelecture hours as mentioned in the syllabus.

Useful Digital Links	
1	https://www.tutorialspoint.com/basics_of_computers/basics_of_ computers_introduction.htm
2	https://plato.stanford.edu/entries/critical-thinking/
3	https://studio.code.org/s/courseb-2020
4	https://scratch.mit.edu/projects/editor/?tutorial=getStarted
5	https://www.careerride.com/mcq/logical-reasoning-quantitative- aptitude-mcq-questions-319.aspx

Course Code:	Course Title	Credit
BVCDFG 402	**Security Architecture and Engineering**	**4**

Prerequisite:	
Course Objectives:	
1	The course introduces to security engineering process and design.
2	The students should get exposer to older and modern Security Models.
3	They shall learn to Information Security, assess and mitigate the vulnerabilities.
Course Outcomes:	
1	Implement and manage engineering processes using secure design principles
2	Understand the fundamental concepts of security models.
3	Select controls based upon systems security requirements.
4	Understand the security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)
5	Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements.
6	Understand Modern Security Model and their use.

I	**Secure System Design Principles**	Secure System Design Principles, Integrated Systems, Journey Towards Zero Trust Security Models: Security Models, Biba Integrity Model Bell LaPadula model, TCSEC, Common criteria.	**8**
II	**Select System Security Controls**	The security controls, seven different types: preventative(preventing unauthorized action on an information system), corrective(correcting an information system after an unauthorized action), detective(detecting unauthorized action), compensating(compensate an information system for a risk or vulnerability) , deterrent(controls that are used to deter would-be attackers), directive(controls that guide the subjects to comply with a	**8**

		security policy) and recovery(controls that are needed to recover from a disaster)	
III	**Assessment of Traditional Security Architectures**	Assessment of Traditional Security Architectures, Distributed Systems, Assessment of Non-traditional Security Architectures Securing Embedded Devices, High Performance Systems	**8**
IV	**Security of Information System**	Access control mechanisms, secure memory management, layering and virtualization which can be used to protect systems without disrupting the system.	**6**
V	**Assess and mitigate the vulnerabilities**	Client security issues: 'Applets', server security issues: Vulnerabilty mitigaton, database Security: Data breach, 'inference', 'aggregation' are other database risks, Cryptographic systems: DES, 3DES, AES, Blowfish, RSA, cloud-based systems, IoT and distributed systems of security architecture and knows how to mitigate them.	**7**
VI	**Moderm Security Models**	Time Based Security, Cyber Kill Chain, TBS + Kill Chain + MITRE ATT&CK, Architecting for Visibility & Detection, Architecting for Incident Response, Zero Trust Model	**8**
		Total	**45**

Textbooks:	
1	Securing Systems: Applied Security Architecture and Threat Models by Brook S E Schoenfield, CRC Press.
2	Security Architecture How & Why by Author: Tom Madsen, Accenture, Denmark, River Publishers Series in Digital Security and Forensics
References:	
1	Information Security Architecture: An Integrated Approach to Security in the Organization, Second Edition by Jan Killmeyer.
2	Practical Cybersecurity Architecture: A guide to creating and implementing robust designs for cybersecurity architects by Ed Moyle (Author), Diana Kelley (Author)

Assessment:	
Internal Assessment:	
Assessment consists of two class tests of 20 marks each. The first class test is to be conducted when approximately 40% syllabus is completed and the second class test when an additional 40% syllabus is completed. Duration of each test shall be one hour.	
End Semester Theory Examination:	
1	Question paper will comprise a total of six questions.
2	All question carries equal marks
3	Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3then part (b) will be from any module other than module 3)
4	Only Four questions need to be solved.
5	In question paper weightage of each module will be proportional to number of respectivelecture hours as mentioned in the syllabus.

Useful Digital Links	
1	https://www.educba.com/security-architecture/
2	https://www.pluralsight.com/courses/security-architecture-engineering-design-principles-cissp
3	https://www.infosecinstitute.com/skills/learning-paths/security-architecture/
4	http://www.ndl.iitkgp.ac.in/he_document/nptel/courses_106_106_106106141_video_lec7

Suggested List of Tutorials	
Sr. No.	**Title of Tutorials**
1	Study on Security Architecture: Types, Benefits https://www.geeksforgeeks.org/security-architecture-types-elements-framework-and-benefits/
2	Study on Elements of Security Architecture
3	Examples of Security Architecture Framework
4	Zero Trust Architecture in Security, https://www.geeksforgeeks.org/zero-trust-architecture-in-security/
5	Zero Security Model, https://www.geeksforgeeks.org/zero-security-model/
6	How to Use Docker Content Trust to Verify Docker Container Images, https://www.geeksforgeeks.org/how-to-use-docker-content-trust-to-verify-docker-container-images/

Course Code:	Course Title	Credit
BVCDFG 403	**Digital Forensics**	**4**

Prerequisite:	
Course Objectives:	
1	To understand the various computer and cyber-crimes in the digital world.
2	To understand a significance of digital forensics life cycle, underlying forensics principles and investigation process.
3	To understand the importance of File system management with respect to computer forensics.
4	To be able to identify the live data in case of any incident handling and application of appropriate tools and practices for the same.
5	To Develop the skills in application of various tools and investigation report writing with suitable evidences.
6	To be able to identify the network and mobile related threats and recommendation of suitable forensics procedures for the same.
Course Outcomes:	
1	Identify and define the class for various computer and cyber-crimes in the digital world.
2	Understand the need of digital forensic and the role of digital evidence.
3	Understand and analyze the role of File systems in computer forensics.
4	Demonstrate the incident response methodology with the best practices for incidence response with the application of forensics tools.
5	Generate/Write the report on application of appropriate computer forensic tools for investigation of any computer security incident .
6	Identify and investigate threats in network and mobile.

I	**Prerequisite**	Computer Hardware: Motherboard, CPU, Memory: RAM, Hard Disk Drive (HDD), Solid State Drive (SSD), Optical drive Computer Networks: Introduction CN Terminology: Router, Gateway, OSI and TCP/IP Layers Operating Systems: Role of OS in file management, Memory	**8**

		management utilities, Fundamentals of file systems used in Windows and Linux.	
II	**Introduction to Cybercrime and Computer-crime**	Definition and classification of cybercrimes: Definition, Hacking, DoS Attacks, Trojan Attacks, Credit Card Frauds, Cyber Terrorism, Cyber Stalking. Definition and classification of computer crimes: Computer Viruses, Computer Worms. Prevention of Cybercrime: Steps that can be followed to prevent cybercrime, Hackers, Crackers, Phreakers.	**8**
III	**Introduction to Digital Forensics and Digital Evidences**	Introduction to Digital Forensics: Introduction to Digital Forensics and lifecycle, Principles of Digital Forensic. Introduction to Digital Evidences: Challenging Aspects of Digital Evidence, Scientific Evidence, Presenting Digital Evidence. Digital Investigation Process Models: Physical Model, Staircase Model, Evidence Flow Model.	**8**
IV	**Computer Forensics**	OS File Systems Review: Windows Systems- FAT32 and NTFS, UNIX File Systems, MAC File Systems Windows OS Artifacts: Registry, Event Logs Memory Forensics : RAM Forensic Analysis, Creating a RAM Memory Image, Volatility framework, Extracting Information Computer Forensic Tools: Need of Computer Forensic Tools, Types of Computer Forensic Tools, Tasks performed by Computer Forensic Tools	**8**
V	**Incident Response Management, Live Data Collection and Forensic Duplication**	Incidence Response Methodology: Goals of Incident Response, Finding and Hiring IR Talent IR Process: Initial Response, Investigation, Remediation, Tracking of Significant Investigative Information. Live Data Collection: Live Data Collection on Microsoft Windows, Forensic Duplication: Forensic Duplicates as Admissible Evidence, Forensic Duplication Tools: Creating a Forensic evidence, Duplicate/Qualified Forensic Duplicate of a Hard Drive.	**7**

VI	**Forensic Tools and Report Writing**	Forensic Image Acquisition in Linux: Acquire an Image with dd Tools, Acquire an Image with Forensic Formats, Preserve Digital Evidence with Cryptography, Image Acquisition over a Network, Acquire Removable Media Forensic Investigation Report Writing: Reporting Standards, Report Style and Formatting, Report Content and Organization.	**6**
Total			**45**

Textbooks:	
1	Digital Forensics by Dr. Dhananjay R. Kalbande Dr. Nilakshi Jain, Wiley Publications, First Edition, 2019.
2	Digital Evidence and Computer Crime by Eoghan Casey, Elsevier Academic Press, Third Edition, 2011.
3	Incident Response & Computer Forensics by Jason T. Luttgens, Matthew Pepe and Kevin Mandia, McGraw-Hill Education, Third Edition (2014).
4	Network Forensics : Tracking Hackers through Cyberspace by Sherri Davidoff and Jonathan Ham, Pearson Edu,2012
5	Practical Mobile Forensic by Satish Bommisetty, Rohit Tamma, Heather Mahalik, PACKT publication, Open source publication, 2014 ISBN 978-1-78328-831-1 6. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory by Michael Hale Ligh (Author), Andrew Case (Author), Jamie Levy (Author), AAron Walters (Author), Publisher : Wiley; 1st edition (3 October 2014),
References:	
1	Scene of the Cybercrime: Computer Forensics by Debra Littlejohn Shinder, Syngress Publication, First Edition, 2002.
2	Digital Forensics with Open Source Tools by Cory Altheide and Harlan Carvey, Syngress Publication, First Edition, 2011.
3	Practical Forensic Imaging Securing Digital Evidence with Linux Tools by Bruce Nikkel, NoStarch Press, San Francisco,(2016)
4	Android Forensics : Investigation, Analysis, and Mobile Security for Google Android by Andrew Hogg, Elsevier Publication,2011
5	Scene of the Cybercrime: Computer Forensics by Debra Littlejohn Shinder, Syngress Publication, First Edition, 2002.

Assessment:	
Internal Assessment:	
Assessment consists of two class tests of 20 marks each. The first class test is to be conducted when approximately 40% syllabus is completed and the second class test when an additional 40% syllabus is completed. Duration of each test shall be one hour.	
End Semester Theory Examination:	
1	Question paper will comprise a total of six questions.
2	All question carries equal marks
3	Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3then part (b) will be from any module other than module 3)
4	Only Four questions need to be solved.
5	In question paper weightage of each module will be proportional to number of respectivelecture hours as mentioned in the syllabus.

Useful Digital Links	
1	https://www.pearsonitcertification.com/articles/article.aspx?p=462199&seqNum=2
2	https://flylib.com/books/en/3.394.1.51/1/
3	https://www.sleuthkit.org/autopsy/
4	http://md5deep.sourceforge.net/md5deep.html
5	https://tools.kali.org/
6	https://kalilinuxtutorials.com/
7	https://accessdata.com/product-download/ftk-imager-version-4-3-0
8	https://www.amazon.in/Art-Memory-Forensics-Detecting-Malware/dp/1118825098

Suggested List of Experiments	
Sr. No.	**Title of Experiment**
1	Case Studies
2	Research Papers study
3	Learn white papers fromComputer Forensics Resource Center: NIST Draft Special Publication 800-101 :
4	Make a bootable pen drive.
5	forensic duplication or mirroring :Drive to File Copy

Course Code:	Course Title	Credit
BVCDFS 401	Penetration Testing and Vulnerability Assessment	4

Prerequisite: No Prerequisite	
Course Objectives:	
1	Equip learners with essential skills in penetration testing, starting with Information Gathering to understand targeted systems.
2	Instruct learners on how to leverage vulnerabilities to gain unauthorized system access.
3	Offer knowledge on maintaining access, extracting data, and covering tracks after gaining unauthorized access.
4	Focus on common vulnerabilities in web applications and effective strategies to mitigate them.
5	Provide a comprehensive understanding of the entire cyberattack process, from initial information gathering to exploitation and post-exploitation techniques.
Course Outcomes: On Successful completion of course, learner will be able to	
1	Demonstrate ability to gather information and detect open ports and services effectively.
2	Successfully exploit system vulnerabilities to gain unauthorized access and execute payloads.
3	Master post-exploitation tactics, including maintaining access, data extraction, and employing social engineering.
4	Identify and mitigate common web application vulnerabilities, ensuring secure data transactions and user authentication.

5	Gain a thorough understanding of cybersecurity, from initial penetration testing phases to practical exploitation and post-exploitation strategies.

Module		Content	Hrs
1		**Information Gathering**	**6**
	1.1	Introduction to Penetration Testing Skills, Overview of Penetration Testing, Key Skills and Tools for Penetration Testers	
	1.2	Information Gathering: Whois and Dmitry, Google and GHDB, Shodan CLI, DNS Reconnaissance, Online Databases	
2		**Scanning and Enumeration**	**8**
	2.1	Scanning Techniques, Introduction to Scanning, Nmap Scanning, NSE Scripting (Nmap Scripting Engine)	
	2.2	Enumeration and Vulnerability Detection, Enumeration Concepts, Common Services and Ports, Msfconsole (Metasploit Framework), Enumeration Tools, Vulnerability Detection Methods, Nessus (Vulnerability Scanner)	
3		**Exploitation**	**9**
	3.1	Introduction to Exploitation Techniques	
	3.2	Exploitation Methods: Brute Force Tools, Exploits Database, Msfconsole, Exploiting Manually	
	3.3	Payloads: Msfvenom Payloads, Payloads Automation, Meterpreter	
4		**Post Exploitation**	**6**
	4.1	Introduction to Post Exploitation Tactics	
	4.2	Post Exploitation Techniques: Local vs. Remote Exploits, Privilege Escalation, Persistence, Disabling Security	
	4.3	Social Engineering, Online Services, BeEF, Phishing Frameworks, Advanced Techniques	
5		**Web Application Security Fundamentals**	**9**
	5.1	Introduction to Web Application Security, Overview of Web Application Security, Importance and Impact of Web Security	

	5.2	Web Application Vulnerabilities and Mitigation, Understanding Common Web Vulnerabilities, HTML Basics, Introduction to OWASP (Open Web Application Security Project), Cross-Site Scripting (XSS), Local File Inclusion (LFI) / Remote File Inclusion (RFI), Brute Force Attacks	
6		**Advanced Web Security Techniques**	**7**
	6.1	Web Application Vulnerabilities and Mitigation (Continued), SQL Injection, Web Payloads, Reverse Shell	
	6.2	Burp Suite, Introduction to Burp Suite, Proxy, Repeater, Intruder, Encoder	
		Total	**45**

Textbooks:	
1	**The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws by** Dafydd Stuttard, Marcus Pinto**, 2nd Edition**
References:	
1	**Advanced Penetration Testing: Hacking the World's Most Secure Networks:** by Wil Allsopp, 1st Edition
Useful Link for E-Resources:	
1	Cybersecurity course | Vulnerability Assessment | VAPT | Udemy
2	Vulnerability Assessment and Penetration Testing Certification - IIT Kanpur (simplilearn.com)
3	Vulnerability Assessment and Penetration Testing (VAPT) Courses | Koenig Solutions (koenig-solutions.com)

Assessment:	
Internal Assessment:	
Assessment consists of two class tests of 20 marks each. The first-class test is to be conducted when approx. 40% syllabus is completed and the second-class test when an additional 40% syllabus is completed. Duration of each test shall be one hour.	
End Theory Examination:	
1	Question paper will comprise a total of six questions.
2	All question carries equal marks
3	Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3)
4	Only four questions need to be solved.
5	In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus.

Suggested List of Experiments	
Sr. No.	**Title of Experiment**
1	Learn and Understanding the Attack Surface:
2	Learn to Adapting to Evolving Threats:
3	Learn to Reducing Attack Vectors:
4	Learn to Enhancing Security Measures
5	Case Study on Risk Management

Course Code:	Course Title	Credit
BVCDFS 402	**Cybercrime Investigation Techniques**	**4**

Prerequisite: No Prerequisite	
Course Objectives:	
1	Provide an in-depth understanding of the techniques and tools used in cybercrime investigations.
2	Equip students with practical skills in digital forensics and evidence collection.
3	Develop proficiency in analysing and interpreting digital evidence.
4	Introduce methodologies for tracking and identifying cybercriminals.
5	Enhance the ability to prepare and present comprehensive cybercrime investigation reports.
Course Outcomes: On Successful completion of course, learner will be able to	
1	Demonstrate knowledge of cybercrime investigation techniques and digital forensics

	principles.
2	Apply digital forensics tools to collect and analyze electronic evidence.
3	Conduct thorough investigations of cyber incidents and identify perpetrators.
4	Develop and document a step-by-step investigative process for cybercrime cases.
5	Produce detailed and accurate reports on cybercrime investigations and present findings effectively.

Module		Content	Hrs
1		**Digital Data Handling**	**9**
	1.1	Introduction to Digital Data Handling, File and Disk Handling, Viewing File Contents, Examining Disk Structures, Hexadecimal Editor, Manipulating Offsets	
	1.2	Encoding and Numeric Systems: Data Encoding Techniques, Numeric Representations, Digital Storage Capacities, Features of Solid State Drives (SSDs)	
	1.3	Automated Extraction and Metadata Examination: Automated Data Extraction, Techniques for Extracting Data, Automated Data Carving Methods, Analysis of Windows System Files	
	1.4	Metadata Examination, Metadata Inspection, Modified, Accessed, Created (MAC) Timestamps, Editing Metadata Information	
2		**Advanced File Forensics**	**7**
	2.1	Introduction to File Forensics Techniques, Techniques: Methods of Concealing Information, Identifying Concealed Files, Extracting Concealed Files, Generating Hidden Files	
	2.2	Hard Drive Analysis: Examination of Hard Disk Drives, Analysis of System Files, Master File Table (MFT) Review	
	2.3	Utilizing Forensic Toolkit (FTK): Application of Forensic Toolkit (FTK)	

3		**Evidence Collection Techniques**	**8**
	3.1	Introduction to Analysis of Digital Artifacts: Overview of Digital Artifacts, Directories Containing Artifacts, Examination of Browser Artifacts, Investigating Shadow Copies	
	3.2	Registry Data Analysis: Scrutiny of Registry Data, Retrieving Information, NTUSER.DAT File Analysis, Conducting General Searches, Employing Registry Viewing Tools	
4		**Comprehensive Analysis**	**7**
	4.1	Memory Examination: In-Depth Memory Analysis, Creation of Memory Images, Utilizing Volatility for Analysis, Data Carving from RAM	
	4.2	Event Analysis: Analysis of System Events, Utilizing Event Viewing Tools, Establishing Audit Policies, Customized Search Techniques	
	4.3	Network Analysis: Analysis of Network Traffic, Examination of Service Protocols, Identification of Darknet Connections	
	4.4	Malware Investigation: Investigation of Malicious Software, Basic Static Analysis, Fundamental Dynamic Analysis	
5		**Incident Response**	**7**
	5.1	Introduction to Incident Response and Reporting, Developing Incident Response Plans, Roles and Responsibilities, Incident Handling Procedures	
	5.2	Live Response Techniques: Conducting Live Forensics, Capturing System State, Preserving Evidence	
6		**Forensic Reporting and Analysis**	**7**
	6.1	Forensic Reporting, Documenting Findings, Writing Forensic Reports, Legal Considerations in Reporting	
	6.2	Case Studies and Practical Exercises, Analyzing Case Studies, Practical Forensic Exercises	
		Total	**45**

Textbooks:	
1	**Investigating the Cyber Breach: The Digital Forensics Guide for the Network Engineer:** by Joseph Muniz, Aamir Lakhani, **1st Edition**
References:	
1	**Incident Response & Computer Forensics:** by Jason T. Luttgens, Matthew Pepe, Kevin Mandia, 3rd Edition
2	**Cyber Crime and Digital Evidence: Materials and Cases:** by Thomas K. Clancy, Susan W. Brenner, **1st Edition**
Useful Link for E-Resources:	
1	Cybersecurity course | Vulnerability Assessment | VAPT | Udemy

2	Vulnerability Assessment and Penetration Testing Certification - IIT Kanpur (simplilearn.com)
3	Vulnerability Assessment and Penetration Testing (VAPT) Courses | Koenig Solutions (koenig-solutions.com)

Assessment:	
Internal Assessment:	
Assessment consists of two class tests of 20 marks each. The first-class test is to be conducted when approx. 40% syllabus is completed and the second-class test when an additional 40% syllabus is completed. Duration of each test shall be one hour.	
End Theory Examination:	
1	Question paper will comprise a total of six questions.
2	All question carries equal marks
3	Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3)
4	Only four questions need to be solved.
5	In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus.

Suggested List of Experiments	
Sr. No.	**Title of Experiment**
1	Learn Understanding Physical Evidence
2	Learn Documentation and Photography
3	Learn Bloodstain Pattern Analysis
4	Learn Special Scene Considerations
5	Learn Emerging Technology

Course Code:	Course Title	Credit
BVCDFS 403	Network Forensics	4

Prerequisite: No Prerequisite	
Course Objectives:	
1	Equip learners with a deep understanding of network protocols, packet structures, and advanced networking tools.
2	Teach methodologies for detecting intrusions using tools like Wireshark, TShark, and Scapy.
3	Provide insights into network analysis using frameworks like Zeek, focusing on log monitoring and packet replay for investigations.
4	Instruct learners on network investigations, anomaly detection, and the use of tools like Network Miner and file carvers.
5	Focus on configuring and operating IPS/IDS systems, Sysmon, and Snort for effective network security.
Course Outcomes: On Successful completion of course, learner will be able to	
1	Learners will demonstrate proficiency in analyzing network protocols and detecting intrusions using advanced tools.
2	Learners will gain the ability to automate processes, monitor data logs, and use Zeek for detailed network analysis.
3	Learners will acquire skills in conducting thorough network investigations, identifying anomalies, and analyzing wireless traffic.

4	Learners will develop competence in configuring and using Sysmon, Snort, and other IPS/IDS systems for network security.
5	Learners will achieve a thorough understanding of network security mitigation strategies, including the operation and configuration of IDS/IPS systems.

Module		Content	Hrs
1		**Intrusion Detection**	**8**
	1.1	Networking: Overview of Network Protocols, Understanding Packet Structure, Utilizing Netstat and ProcMon, Exploring SysInternal Tools	
	1.2	Intrusion Detection Methods: Advanced Wireshark for Network Attacks, TShark Analysis Techniques, Integrating GeoIP for Enhanced Detection, Applying the Scapy Module	
	1.3	Crafting and Analyzing Packets: Techniques for Crafting Packets, Analyzing Packet Data, Working with IPv6 Protocols	
2		**Network Analysis**	**7**
	2.1	Introduction to Zeek: Understanding Zeek and Its Capabilities, Managing Output Logs, Automating Processes with Zeek	
	2.2	Monitoring and Parsing: Monitoring Data into Logs with Zeek, Zeek-Cut Parsing Techniques	
	2.3	Investigative Techniques: Replaying Packets for Investigation, Creating Detailed Timelines from Data	
3		**Case Investigation**	**9**
	3.1	Investigation Process: Understanding the Investigation Process, Identifying and Mitigating MiTM Attacks, Finding Network Anomalies	
	3.2	Flow Analysis and Network File Carving: Conducting Flow Analysis, Techniques for Network File Carving, Using NetworkMiner, Employing File Carvers	

	3.3	Wireless Traffic and Access: Capturing and Analyzing Wireless Traffic, Gaining Access Through Wi-Fi Networks, Investigating HTTPS Traffic	
4		**Mitigation**	**6**
	4.1	IPS and IDS Systems: Introduction to IPS and IDS Systems, Understanding IDS/IPS Operation Processes, Configuring IDS/IPS for Optimal Performance	
	4.2	Sysmon: Installing and Configuring Sysmon, Capturing and Analyzing Network Events	
	4.3	Tools for Intrusion Detection: Using Snort for Intrusion Detection	
5		**Introduction to Incident Response (IR)**	**8**
	5.1	Overview of Incident Response Frameworks, Incident Response Lifecycle, Preparation, Detection, Containment, Eradication Recovery, Role of Incident Response Teams (IRTs) and Responsibilities	
	5.2	Incident Detection and Analysis, Techniques for Detecting Security Incidents, Incident Triage and Initial Assessment, Log Analysis and Correlation	
	5.3	Incident Containment and Eradication: Strategies for Containing Incidents, Steps for Eradicating Threats, Post-Incident Recovery and Lessons Learned	
6		**Threat Hunting**	**7**
	6.1	Threat Hunting Fundamentals, Introduction to Threat Hunting, Proactive vs. Reactive Threat Hunting Approaches, Using Threat Intelligence for Hunting	
	6.2	Advanced Threat Hunting Techniques (New Section), Hypothesis-Driven Threat Hunting, Indicators of Compromise (IoCs), Threat Hunting Tools and Techniques	
	6.3	Integration of Threat Hunting with Incident Response (New Section), How Threat Hunting Supports Incident Response, Developing a Threat Hunting Program, Case Studies and Best Practices	
		Total	**45**

Textbooks:	
1	**Network Forensics: Tracking Hackers through Cyberspace** by Sherri Davidoff and Jonathan Ham, 2nd Edition
References:	
1	**Zeek (formerly known as Bro):** A Powerful Network Analysis Framework **by** James R. Burgess
Useful Link for E-Resources:	
1	Certified Network Forensics Examiner : CNFE (Part1 of Part2) | Udemy
2	Network Forensics Examiner | Free Online Course | Alison
3	Getting Started with Network Forensics | EC-Council Learning (eccouncil.org)

Assessment:	
Internal Assessment:	
Assessment consists of two class tests of 20 marks each. The first-class test is to be conducted when approx. 40% syllabus is completed and the second-class test when an additional 40% syllabus is completed. Duration of each test shall be one hour.	
End Theory Examination:	
1	Question paper will comprise a total of six questions.
2	All question carries equal marks
3	Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3)
4	Only four questions need to be solved.
5	In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus.

Suggested List of Experiments	
Sr. No.	**Title of Experiment**
1	Learn EMailTrackerPro:
2	Learn Web Historian:
3	Learn Wireshark for Network Forensics

Offg. Associate Dean
Dr. Deven Shah
Faculty of Science and Technology
University of Mumbai

Offg. Dean
Prof. Shivram S. Garje
Faculty of Science and Technology
University of Mumbai