CURRICULUM FRAMEWORK AND SYLLABUS

IN

DIPLOMA IN CYBER SECURITY (DCS)

Two Year Diploma Program

One Year Certificate Program

FOR THE STUDENTS ADMITTED FROM THE

ACADEMIC YEAR 2022-2023 ONWARDS

FACULTY OF COMPUTATIONAL SCIENCES

GNA UNIVERSITY
SRI HARGOBINDGARH, PHAGWARA – HOSHIARPUR ROAD,
PHAGWARA-144401, PUNJAB
INDIA

ORDINANCE

FOR

DIPLOMA IN CYBER SECURITY (DCS)

(THIS ORDINANCE HAS BEEN APPROVED IN THE MEETING OF BOARD OF MANAGEMENT HELD ON DATED 15-JUNE-2022)

APPLICABLE W.E.F. ACADEMIC SESSION 2022-2023

SRI HARGOBINDGARH, PHAGWARA – HOSHIARPUR ROAD, PHAGWARA 144401

PUNJAB

ORDINANCE FOR

DIPLOMA IN CYBER SECURITY (DCS)

SHORT TITLE AND COMMENCEMENT

I. This ordinance shall be called the ordinance for the Diploma in Cyber Security (DCS) of GNA University, Phagwara.

II. This ordinance shall come into force with effect from academic session 2022-23.

1. **Name of Program: Diploma in Cyber Security (DCS).**
2. **Name of Faculty: Faculty of Computational Science.**
3. **Vision of the department:** To develop the skilled computer and IT professionals meeting global requirements of IT industry.
4. **Mission of the department:**

   M1: To provide state of art infrastructure and conducive environment for budding IT professionals.

   M2: To establish strong industry academia relationship to enhance the technical skills of the students and make them readily employable.

   M3: To provide exposure to the emerging and establish tools and technology in the field of computer applications.

   M4: To develop curriculum in accordance with the industry requirements.

5. **Program Educational Outcomes (PEO):**

   PEO1: To prepare students with the technical knowledge and skills needed to protect and defend computer systems and networks.

   PEO2: To develop students that can plan, implement, and monitor Cyber Security mechanisms to help ensure the protection of information technology assets.

   PEO 2: To develop students that can identify, analyze, and remediate computer security breaches

6. **Program Outcomes (PO):**

   PO1: Analyse and evaluate the cyber security needs of an organization.

   PO2: Determine and analyse software vulnerabilities and security solutions to reduce the risk of exploitation.

   PO3: Implement Cyber Security solutions and the use of Cyber Security, information assurance, and cyber/computer forensics software/tools.

   PO4: Design and develop a security architecture for an organization.

   PO5: To understand fundamentals and advanced issues of various threats faced by today's cyber infrastructure.

7. **Program Specific Outcomes (PSO):**

   PSO1: Ability to expertise in Cyber Security strategy, and design.

   PSO2: Ability to explore technical knowledge in diverse areas of Cyber Security and experience an environment conducive in cultivating skills for a successful career.

8. **General Regulations for Faculty of Computational Science:**

   8.1 The University may introduce programs under the Faculty of Computational Science which are specified under the UGC Act 1956. The Governing Body may approve the introduction, suspending or phasing out a program on the recommendation of the Academic Council either on its own or on the initiative of faculty.

   8.2 The admissions to a Faculty of Computational Science programs shall be generally governed by the rules of the UGC or any other competent authority of the MHRD or as approved by Governing Body of University and shall be as notified in the admission notification of the respective academic year.

   8.3 The minimum entry qualification for admission to the students of Faculty of Computational Science may be laid

down in the regulations or specified by the Governing Body like Minimum qualification for admission to the first-year program of Faculty of Computational Science shall be the 10 +2 in any stream. While deciding the admission procedure, the University may lay down compulsory subjects in the qualifying examination for admission for various programs in the admission policy.

8.4 A student shall be required to earn a minimum number of credits through various academic components of a curriculum, as provided for in the regulations.

8.5 A student shall be required to complete all the requirements for the award of the diploma within such period as may be specified in the regulations.

8.6 A student may be granted such scholarship as may be specified per the directions of the Governing Body from time to time or regulations laid down for the same.

8.7 A student admitted to the programs shall be governed by the rules, regulations and procedures framed and implemented by the University from time to time.

8.8 The students shall abide by the regulations mentioned in student handbook issued by the University. These standing regulations shall deal with the discipline of the students in the Hostels, Faculty, and University premises or outside. The standing orders may also deal with such other matters as are considered necessary for the general conduct of the students' co-curricular and extra-curricular activities.

8.9 In exceptional circumstances the chairman of Academic Council may, on behalf of the Council, approve amendments, modifications, Insertions or deletions of an Ordinance(s) which in his/her opinion is necessary or expedient for the smooth running of the program: provided all such changes are reported approved to the Council in its next meeting.

9. General Regulations for the DCS Program:

9.1 **Short Title and Commencement:** These regulations shall be called regulations for the Diploma program in Faculty of Computational Science of the University and shall come into force on such date as the Academic Council may approve.

9.2 **Duration:** The duration of the Certificate program leading to Certificate in Cyber Security shall be minimum one year and a year will comprise of two semesters. The duration of the Diploma programs leading to Diploma in Cyber Security shall be minimum two years and two years will comprise of four semesters. However, the duration may be extended up-to of certificate in cyber security program two years from the registered batch. The duration may be extended up-to of diploma in cyber security program four years from the registered batch. The maximum duration of the programs excludes the period of withdrawal, due to medical reasons. However, it shall include the period of suspension or any other reason of discipline /academics e.g., detention, willful absence by the student, not getting a promotion to the next class due to poor academic performance etc. Under detention, the student shall attend the University for an additional semester or more time, as equated to a period of absence/suspension.

9.3 **Starting or Phasing out of Program:** The University offers Diploma program in Computational Science leading to award a diploma in Diploma in Cyber Security, as per nomenclature laid by the UGC National Skills Qualification Framework (NSQF) / National Education Policy (NEP2020) regulations on the subject. A program may be phased out on recommendations of the Academic Council and approval of the Governing Body, on account of continuous low registration in the program or any other justifiable reason like becoming obsolete etc. Similarly, the Academic Council may approve starting of a new program or modifying the existing one on the recommendations of the Academic Council.

9.4 **Admissions:** Admission to DCS program shall be made as per procedure approved by the Governing Body and may be reviewed periodically as required. Fee structure, refund policy, the total number of seats, reservation policy, and special category seats, e.g., sponsored seats.

9.5 **Eligibility for Admission:** 10+2 in any stream or equivalent with 50% (45 % for SC/ST/OBC) marks in aggregate from any recognized board.

9.6 **Semester System:** The DCS academic programs in the University shall be based on Semester System; namely, even (Jan to June) and Odd (July to Dec) Semesters, in an academic year. The courses whether offered in a regular semester shall be evaluated as per the policy and procedure laid down.

9.7 **Semester Duration:** A semester will be of approximately 18-20 weeks duration. Of these, 90 days will be available for actual instructions including Mid Semester Exam.

10. Admission Process: The centralized admission cell shall select for admission to the program. The selection of the candidate shall be strictly on merit basis, subject to fulfilment of eligibility criteria. Candidates are required to fill the prescribed application form and submit the same to the admission cell. The admission cell after verifying the eligibility will forward the form to the Office of Registrar for further processing. If the candidate is selected, he/she is required to deposit the prescribed fee along with the application form and the required documents to the Office of Registrar.

11. Curriculum: The one year's curriculum has been divided into two semesters and shall include lectures/ tutorials/ laboratory work/project work/ viva/ seminars/ presentations/assignments etc. The curriculum will also include other curricular, co-curricular and extra-curricular activities as may be prescribed by the university from time to time.

12. Courses:

(a) Skill Component Courses: The skill component courses will refresh and strengthen a student's understanding and basic knowledge required for the successful completion of the program. Skill component courses for this program will include courses like Basics of Cyber Security, Ethical hacking.

(b) General Education Courses: General Education Courses include the course(s) which are supportive of core trade in addition to soft skills, IT skills, and language proficiency and literature.

(c) Minor/ Major Projects: Students are required to build & submit a detailed cyber security-based project.

(a) Professional Training: Each student would work with an industry or reputed academic institutions, for a period of a minimum of 6 weeks at the end of the second semester. The objective of the training is to help students to develop skills and competencies.

13. Medium of Instructions:

13.1. The medium of instructions and examination will be English.

13.2. Practical work/Project Work/ Project Report / Training Report etc., if any, should be presented in English.

14. Mode: The program is offered in 'Full Time' mode of study only.

15. Attendance Requirement to be Eligible to Appear in End Semester Examination:

15.1 Every student is required to attend at least 75% of the lectures delivered squaring tutorials, practical and other prescribed curricular and co-curricular activities.

15.2 Dean of Faculty may give a further relaxation of attendance up to 10% to a student provided that he/she has been absent with prior permission of the Dean of the Faculty for the reasons acceptable to him/her.

15.3 Further, relaxation up to 5% may be given by the Vice-Chancellor to make a student eligible under special circumstances only.

15.4 No student will be allowed to appear in the end semester examination if he/she does not satisfy the attendance requirements. Further, the attendance shall be counted from the date of admission in the University or commencing of academic session whichever is later.

15.5 Attendance of N.C.C/N.S.S. Camps or Inter-Collegiate or Inter-University or Inter-State or International matches or debates or Educational Excursion or such other Inter-University activities as approved by the authorities involving journeys outside the city in which the college is situated will not be counted as an absence. However, such absence shall not exceed four weeks per semester of the total period of instructions. Such type of facility should not be availed twice during the study.

16. Credit: Each course, except a few special audit courses, has a certain number of credits assigned to it depending upon its lecture, tutorial and/or laboratory contact hours in a week. A letter grade, corresponding to a specified number of grade points, is awarded in each course for which a student is registered. On obtaining a passing grade, the student accumulates the course credits as earned credits. A student's performance is measured by the number of credits that he/she has earned and by the weighted grade point average. A minimum number of credits should be acquired to qualify for the programs. The absolute grading system has been followed for awarding grades for the course.

Earned Credits (EC): The credits assigned to a course in which a student has obtained 'D' (a minimum passing grade) or a higher grade will be counted as credits earned by him/her. Any course in which a student has obtained F, or W or "I" grade will not be counted towards his/her earned credits.

A unit by which the course is measured. It determines the number of hours of instruction required per week.

Contact Hours per Week	Credit Assigned
1 Hr. Lecture (L) per week	1 credit
1 Hr. Tutorial (T) per week	1 credit
2 Hours Practical (Lab) per week	1 credit

16.1 Acceptance of MOOC courses

Faculty of Faculty of Computational Science accepts the MOOC course available on SWAYAM platform for credit transfer. 40% of the courses can be taken from the available list of MOOCs on SWAYAM.

Instructions for MOOC courses

(a) MOOC courses taken for credit transfer must be approved and recommended by Dean Academics and Dean of the Faculty before the start of the semester.

(b) The copy of the list of courses taken by the students for any course has to be submitted to the Controller of the Examination.

(c) MOOC course should be done from SWAYAM platform as per the guidelines of UGC.

(d) To obtain the credit the student needs to complete the assessment of the course and provide the certificate of the course issued by the SWAYAM/NPTEL. After completing the certificate, the student must submit the certificate within a week to the department.

(e) The fees (if any) for the registration and / or assessment of the MOOC course must be borne by the student only.

(f) The student can opt for a particular online MOOC course if and only if the credit of that course is equivalently mapped with the program structure.

(g) If the student obtains the same course credit which mapped with the course, then credit shall be considered for this course and the grade/marks provided by the accessing authority shall be transfer to the student. The result of the MOOC shall be taken on record by the university examination cell and a result declared for these papers.

(h) For any particular semester, all results for the MOOC course must be submitted along with the marks of other papers of the same semester by the course coordinator.

(i) MOOC course coordinators shall be appointed for each of the course taken by the student.

17. Program Structure:

Program Structure: DCS

As Per GNA UNIVERSITY

Detail course structure of DCS

Course Category	**Papers**	**Credits**	**Total Credits**
General Education Core	4	4	16
General Education Core-Lab	1	2	2
General Education Core	3	3	9
General Education Core-Lab	6	1	6
General Education Core	1	2	2
Skill Component	12	4	48
Skill Component-Lab	6	1	6
Skill Component	2	3	6
Skill Component Capstone Project-I & II	2	4	8
Industrial Training	1	4	4
Total	**38**	**28**	**107**

18. Professional / Industrial Training:

- Professional training is a Skill Component course. A student should undergo training for 6 weeks, starting after the Second semester, preferably in an industry or an academic institution is of repute permitted. Professional Training will be evaluated during the 3rd semester.
- It is the responsibility of the Corporate Relations Department (CRD) to arrange training for all the students. At the beginning of each academic session, Corporate Relations Department will prepare a program wise list of potential training organizations. These organizations will be approached by the Corporate Relations Department with a request to provide training seats. Consolidated lists of training offers will be made available to the eligible students at the beginning of even semester of the session. If a student is interested in making his/her own arrangement for the training seat, he/she will need to have the training organization approved by routing the application to the Dean/HOD of Faculty of Computational Science for approval.
- Students will be required to get their training activity and results reviewed by an organization in which they have attended the training. The department will nominate a training coordinator from amongst the faculty members. The faculty members will scrutinize the training report and the certificate issued by the corporate and will award a grade. The student will have to undergo fresh professional training in part or full duration as decided by the Dean/HOD of Faculty of Computational Science. The professional training, submission of training report and obtaining satisfactory

grade is a mandatory requirement for award of the Diploma in DCS.

19. Examination/Evaluation System: The evaluation system of the University shall be oriented to encourage academic qualities. The University follows two components to evaluate student's performance:

19.1 Internal Assessment: It includes components such as Attendance, Mid-Semester Examination, Assignments, continuous assessment tests carrying a weightage of 40%. This is applicable to all theory courses.

19.2 Laboratory Courses: The examination/evaluation criteria of the practical courses shall be decided by the respective faculty member and wherever required on the availability of the external experts/visiting faculty. Faculty may set/design the practical exercises out of any marks but the overall weightage shall be in pre-defined percentage, which the concerned faculty/course coordinator shall announce in the first class of the semester and upload on the GU-MS. Methodology for evaluation of Lab component may include day to day work, lab records, quantity/quality of work and Viva-voce/Seminar/Practical as may be decided.

19.3 Laboratory Internal Assessment: It includes components Lab Evaluation, Internal viva-voce, Attendance, Lab Practical File/Report Submission carrying a weightage of 60%. The internal marks of special courses like Minor/Major project, professional Training has been predefined.

19.4 External Assessment:

a) **End Semester Examination:** These examinations shall be conducted by Controller of Examination. The examination dates and schedule shall be released by the University.

b) End Semester Examination, carrying a weightage of 60%.

c) The external marks of special courses Minor/Major Project, Industry Training has been predefined.

d) External Lab Assessment which includes components (External Lab Viva-Voce) carrying a weightage of 40 %.

e) Every student must score at least 25% marks each in Continuous Assessment and End Semester Examination. The minimum pass percentage is 40% in aggregate. In case a student scores more than 25% each in Continuous Assessment and End Semester Examination, but the overall percentage in the concerned subject remains less than 40%, then a student must repeat End Semester Examination in that subject.

19.5 Failing to meet Attendance Requirement:

a) A student is required to attend all the classes.

b) If the attendance profile of a student is unsatisfactory, he/she will be debarred. Any student, who has been debarred due to attendance shortage, shall not be allowed to take the supplementary examination. The student shall have to register for the course in the regular semester when offered.

19.6 Makeup Examinations for Mid Semester Examination: A student may apply for a makeup examination where he/she is not able to attend the examination schedule due to reasons of personal medical condition or compassionate reason like the death of a very close relative. No other contingencies are acceptable. Except in case of a medical emergency, a student needs to seek advance approval from appropriate authority before missing the Examination.

Theory Courses:

- A student missing Mid Term Examination only shall be required to take a make-up examination.
- The students must put-up the request for make-up examination along with the medical documents to prove the genuineness of the case (for having missed the Examination) within 5 days of the last date of Examination.
- The genuineness shall be reviewed and approved by the Vice-Chancellor, whose decision shall be final.
- In case a student misses the make-up Examination also, then no further chance will be provided.
- The duration of Examination shall be as decided by the Faculty member.

- Genuine approved cases shall be notified by the Controller of Examination based on the requests received and only
- such students shall be allowed to take make-up Examination in the subjects where approval has been granted.
- The date sheet need not be taken out as the makeup examination shall be conducted under arrangement concerned faculty, who after evaluation and sharing the evaluated answer sheet with the student shall submit marks to the Controller of Examination.

19.7 Makeup of End Semester Examination: It is mandatory to appear the end semester major examination to obtain any grade for a course. A student who misses the end semester major examination shall follow a similar procedure as outlined above, to obtain approval of the Vice-Chancellor to prove the genuineness of the case. The student whose case is approved as genuine shall be awarded "I" Grade in the semester results in the given subject. The student shall be allowed to appear in the supplementary examination of the said subject. However, the grades shall be worked out by computing the marks obtained by students in Mid Term Exams, TA, Lab and supplementary examination (equated to the weightage of end semester examination). The total marks shall be compared with the marks of the class as in the regular semester for the award of grade.

19.8 Makeup of End Semester Viva of Projects: It is mandatory to appear in the final Viva examination to obtain any grade for a project course. In case of student missing the same for genuine reasons; similar method as given for written examination of theory courses shall be followed.

19.9 Procedure to be adopted by students in case of missing any of the specified Examination(s): Following procedure shall be adopted for establishing the genuineness of the case.

a. Action by the student (Medical Cases)

I. They should report an absence from the Examination(s) by the fastest possible means to the Controller of Examination. It could be email or written communication by speed post or sent by hand through any means. In the case of Hosteller's, if a student falls sick while residing in the hostel, he/she should seek the advice of the available qualified doctor.

II. The said report should preferably be sent before the Examination, but no later than 5 days after the last date of the said Examination.

III. The student should on re-joining:

a. Report to the Controller of Examination with complete medical documents to include referral/Prescription slip of the doctor specifically indicating the disease and medicine prescribed, investigation/Lab reports and discharge slip in case of admission should be provided.

b. Submit the Documents to the Controller of Examination, not later than 5 days after the last date of Examination.

IV. In case delay beyond 5 days is anticipated the student should arrange for the medical documents to be sent to the University Medical Officer by hand through a friend / relative etc. and get the said genuineness deposit with the Controller of Examination.

V. No request later than 5 days after the last date of Examination shall be accepted for reasons of ignorance or any other reasons.

b. **Action by students (any other reason)**

In case the student must miss Examination due to genuine reason other than medical, prior written sanction of Vice-Chancellor and in his absence, Dean is mandatory. No post facto requests shall be accepted in any case. The approval should be deposited with the Controller of Examination before the examination.

20. Supplementary Examination:

20.1 The supplementary examinations shall be held for each commiserating semester in December for Odd semester and May/June for Even semester respectively. For the final semester students, there is privilege to appear in the supplementary exams of all previous semester.

20.2 Eligibility: Student with 'F' grade is eligible to appear in the Supplementary Examination.

20.3 Supplementary for Projects: There shall be no supplementary examinations for the projects, except make up examination for missing the final viva as per rules outlined above.

21. Grading System: University follows eight-letter grading system (A+, A, B+, B, C+, C, D, and F) that have grade points with values distributed on a 10-point scale for evaluating the performance of the student. The letter grades and the corresponding grade points on the 10-point scale are as given in the table below.

Academic Performance	**Range of Marks**	**Grades**	**Grade Points**
Outstanding	≥90	A+	10
Excellent	≥80 & < 90	A	9
Very Good	≥70 & < 80	B+	8
Good	≥60 & < 70	B	7
Fair	≥50 & < 60	C+	6
Average	>40 & < 50	C	5
Minimally Acceptable	40	D	4
Fail	< 40	F	0
Incomplete		I	-
Withdrawal		W	-
Grade Awaited		GA	-
S-Satisfactory, US-Unsatisfactory Minor Project		S/US	-

21.1. Description of Grades:

A. **D Grade**: The D grade stands for marginal performance, i.e. it is the minimum passing grade in any course. D grade shall not be awarded below 30% marks, though each teacher may set higher marks for the same.

B. **F Grade**: The 'F' grade denotes a very poor performance, i.e. failing a course. A student has to repeat all courses in which she/he obtains 'F' grade until a passing grade is obtained. In the case of 'F', no Grade points are awarded. However, the credits of such courses shall be used as the denominator for calculation of GPA or CGPA.

C. **W Grade:** The 'W' grade is awarded to a student if he/she is allowed to withdraw for an entire Semester from the University on medical grounds for a period exceeding five weeks.

D. **'I" Grade:** The 'I' grade is awarded when the student is allowed additional opportunity like makeup Examination etc. based on which the grade is to be decided along with other components of the evaluation during the semester 24 An incomplete grade of 'I' may be given when an unforeseen emergency prevents a student from completing the work in a course. The 'I' must be converted to a performance grade (A to F) within 90 days after the first day of classes in the subsequent regular semester.

E. **X Grade**: It is equivalent to Fail grade but awarded due to a student falling below the laid down attendance requirement. Students having X grade shall be required to re-register for the course, when offered next.

22.2 **Cumulative Grade Point Average (CGPA):** it is a measure of the overall cumulative performance of a student for all semesters. The CGPA is the ratio of total credit points secured by a student in various courses in all Semesters and the sum of the total credits of all courses in all the semesters. It is expressed up to two decimals places.

NB: The CGPA can be converted to percentage by using the given formula:

CGPA x 10 = %

e.g. 7.8 x 10 = 78%

21.2 Based on the grades earned, a grade certificate shall be issued to all the registered students after every semester. The grade certificate will display the course details (Course title, number of credits, grade secured) along with SGPA of that semester and CGPA earned till that semester.

23 **General Rules: Examinations**:

a) Showing the Answer Scripts: The answer scripts of all written Examinations i.e. Mid Term or end semester examination or any other written work conducted by a teacher shall be shown to the students. Students desirous of seeing the marked answer scripts of End Semester Examination has to ensure their presence before results are declared, as per dates notified by the Controller of Examination.

b) Marks/Answer Sheets of all other tests shall also be shared with the students and thus, there shall be no scrutiny of grades. However, before the grades are forwarded to Registrar/Controller of Examination, they should be displayed on GU-MS and time are given to students, to discuss the same with respective faculty.

c) No appeal shall be accepted for scrutiny of grades.

d) Examination Fee for Supplementary. A prescribed fee will be charged as per course or as decided by the Management from time to time for taking supplementary exams.

24 **Improvement of overall Score:** A candidate having CGPA < 5.5 and wishes to improve his/her overall score may do so within two academic years immediately after passing the degree program by reappearing into maximum four course(s)/subject(s). The improvement would be considered if and only if the CGPA becomes > 5.5.

25 **Program qualifying criteria:**

For qualifying the Program every student is required to earn prescribed Credits as follows:

a) Certificate in Cyber Security (**49 credits)**

b) Diploma in Cyber Security (**107 credits)**

If any student fails to earn prescribed credits for the program, then he/she will get a chance to complete his/her Program in two more years than the actual duration of the degree.

26 **Revision of Regulations, Curriculum and Syllabi:** The University may revise, amend, change or update the Regulations, Curriculum, Syllabus and Scheme of examinations through the Board of Studies and the

27 **Conditions for Award of a Diploma:**

a) Earning a minimum credit as specified in the curriculum of respective program.

b) Should complete the requirements of the Diploma in maximum duration specified for the program. Semester withdrawals due to medical reasons are not counted in two years. However, forced withdrawal of students e.g. suspension or expulsion or nonattendance by student due to any other reasons, shall count in the maximum period of two years and minimum period of one years.

c) Successfully completing the Internship studies.

d) Should have cleared all the Skill component and general education courses of the programs.

Note: Exit option with certificate (49 credits) and certificate will be issued after the first year.

Certificate in Cyber Security Semester I

Sr. No.	Category	Code	Subject	Teaching Scheme					Examination Scheme		Total
				L	T	P			Internal	External	
1.	General Education Core Courses-1	DCS108	Computer fundamentals	3	1	0	4	4	40	60	100
2.	General Education Core Courses-1	DCS128	Computer fundamentals Lab	0	0	4	2	4	30	20	50
3.	General Education Core Courses-2	DCS102	Computer Network	4	0	0	4	4	40	60	100
4.	General Education Core Courses-2	DCS122	Computer Network Lab	0	0	2	1	2	30	20	50
5.	General Education Core Courses-3	DCS106	Operating System with Linux	4	0	0	4	4	40	60	100
6.	General Education Core Courses-3	DCS126	Operating System with Linux Lab	0	0	2	1	2	30	20	50
7.	Skill Component Core Courses-1	DCS107	Cyber Security	4	0	0	4	4	40	60	100
8.	Skill Component Core Courses-1	DCS127	Cyber Security Lab	0	0	2	1	2	30	20	50
9.	General Education Core Courses-4	COM101	English Communication	2	0	0	2	2	40	60	100
10.	General Education Core Courses-4	COM121	English Communication Lab	0	0	2	1	2	20	30	50
		Total		**17**	**1**	**12**	**24**	**30**	**340**	**410**	**750**

Certificate in Cyber Security Semester II

Sr. No.	Category	Code	Subject	Teaching Scheme					Examination Scheme		Total
				L	T	P			Internal	External	
1.	General Education Core Courses-5	DCS207	Python Programming	3	1	0	4	4	40	60	100
2.	General Education Core Courses-5	DCS227	Python Programming Lab	0	0	2	1	2	30	20	50
3.	Skill Component Core Courses--2	DCS202	Malware Taxonomy and Analysis	4	0	0	4	4	40	60	100
4.	General Education Core Courses-6	DCS208	Cryptography and Network Security	3	0	0	3	3	40	60	100
5.	General Education Core Courses-6	DCS228	Cryptography and Network Security Lab	0	0	2	1	2	30	20	50
6.	Skill Component Core Courses-3	DCS204	Cyber Forensic	4	0	0	4	4	40	60	100
8.	Skill Component Core Courses-4	DCS209	Kali Linux with Penetration Testing	4	0	0	4	4	40	60	100
9.	Skill Component Core Courses-4	DCS229	Kali Linux with Penetration Testing Lab	0	0	2	1	2	30	20	50
10.	Skill Component Core Courses-5	DCS206	Mobile Device Security	3	0	0	3	3	40	60	100
			Total	**18**	**1**	**6**	**25**	**28**	**330**	**420**	**750**

Students will undergo 6 weeks of Industry/Internship Training* after the 2nd semester. Training/Internship will be evaluated in the 3rd Semester.

Diploma in Cyber Security Semester III

Sr. No.	Category	Code	Subject	Teaching Scheme					Examination Scheme		Total
				L	T	P			Internal	External	
1.	Skill Component Core Courses -6	DCS301	Cyber Crime Investigation and Digital Forensics	3	1	0	4	4	40	60	100
2.	Skill Component Core Courses -6	DCS321	Cyber Crime Investigation and Digital Forensics Lab	0	0	2	1	2	30	20	50
3.	Skill Component Core Courses-7	DCS302	Firewall and Internet Security	4	0	0	4	4	40	60	100
4.	General Education Core Courses-7	DCS304	Web Technologies	3	0	0	3	3	40	60	100
5.	General Education Core Courses-7	DCS324	Web Technologies Lab	0	0	2	1	2	30	20	50
6.	Skill Component Core Courses-8	DCS305	Mobile Forensics	4	0	0	4	4	40	60	100
7.	Skill Component Core Courses-9	DCS306	Ethical Hacking	4	0	0	4	4	40	60	100
8.	Skill Component Core Courses-9	DCS326	Ethical Hacking Lab	0	0	2	1	2	30	20	50
9.	Skill Component Core Courses-10	DCS350	Capstone Project -I	0	0	4	4	4	60	40	100
10.	Skill Component Core Courses-11	DCS360	Industrial Training	0	0	0	4	0	60	40	100
			Total	**18**	**1**	**10**	**30**	**29**	**410**	**440**	**850**

Diploma in Cyber Security Semester IV

Sr. No.	Category	Code	Subject	Teaching Scheme					Examination Scheme		Total
				L	T	P			Internal	External	
1.	Skill Component Core Courses - 12	DCS401	Python for Cyber Security	3	1	0	4	4	40	60	100
2.	Skill Component Core Courses-12	DCS421	Python for Cyber Security Lab	0	0	2	1	2	30	20	50
3.	Skill Component Core Courses-13	DCS402	Web Application Security	4	0	0	4	4	40	60	100
4.	General Education Core Courses-8	DCS403	Blockchain Technologies and Crypto currency	3	0	0	3	3	40	60	100
6.	Skill Component Core Courses-14	DCS404	Windows and Linux Forensic Analysis	4	0	0	4	4	40	60	100
7.	Skill Component Core Courses-14	DCS424	Windows and Linux Forensic Analysis Lab	0	0	2	1	2	40	60	100
8.	Skill Component Core Courses-15	DCS405	Cyber Laws and IPR	4	0	0	4	4	40	60	100
9.	Skill Component Core Courses-16	DCS406	Cyber Security Threats	3	0	0	3	3	30	20	50
10.	Skill Component Core Courses-17	DCS450	Capstone Project -II	0	0	4	4	4	60	40	100

			Total	**21**	**1**	**8**	**28**	**30**	**360**	**440**	**800**

This evaluation pattern is followed to evaluate each course except communication skills.

Course Evaluation Pattern:

Criteria	Description	Maximum Marks
Internal Assessment (Summative)	Mid Semester Exam (MSE)	20 Marks
	Assignment	5 Marks
	Continuous Assessment Test	10 Marks
	Attendance	5 Marks
End Term Exam (Summative)	End Term Examination (ESE)	60 Marks
Total		100 Marks
Attendance (Formative)	A minimum of 75% Attendance is required to be maintained by a student to be qualified for taking up the End Semester examination. The allowance of 25% includes all types of leaves including medical leaves.	

Lab Course Evaluation Pattern:

Criteria	Description	Maximum Marks
Internal Assessment (Summative)	**Lab Evaluation (Five times a semester):** Based on following criteria: Problem solving (Based on difficulty level, one or more questions may be given) Flowchart / Algorithm / Structured description of problem to explain how the problem can be solved / Interface Design	15 Marks
	Internal viva	5 Marks
	Attendance	5 Marks
	Practical File	5 marks
External Assessment (Summative)	External Viva	20 Marks

Total	**50 Marks**
Attendance (Formative)	**A minimum of 75% Attendance is required to be maintained by a student to be qualified for taking up the End Semester examination. The allowance of 25% includes all types of leaves including medical leaves.**

SYLLABUS

DIPLOMA IN CYBER SECURITY (DCS)

(National Education Policy (NEP2020))
(Applicable for 2022-2023 onwards)

FACULTY OF COMPUTATIONAL SCIENCES
GNA UNIVERSITY
SRI HARGOBINDGARH, PHAGWARA – HOSHIARPUR ROAD,
PHAGWARA-144401, PUNJAB
INDIA

DCS108: Computer fundamentals

Credits: 4

LTP: 310

Course Description: The course aims to equip the students with various Office Automation Tools like Word processor, Spreadsheet program & Presentation program. The course includes Crafting professional word documents; excel spread sheets, power point presentations using the Microsoft suite of office tools.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Use various Office Automation Tools like Word processor, Spreadsheet software & Presentation software.

CO2: Describe the fundamental of processing unit and operating system.

CO3: Describe various peripheral devices like Input and Output devices of Computer systems, online storage devices.

CO4: Perform documentation, accounting operations, presentation skills.

Course Content

UNIT-I

Introduction to Computers: Introduction, Characteristics of Computers, Block diagram of computer. Types of computers (Analog, Digital, Hybrid, Minicomputers, Micro Computers, Mainframe Computers, Super Computers). Types of Programming Languages (Machine Languages, Assembly Languages, High Level Languages). Data Organization, Drives, Files, Directories.

Types of Memory: -Primary and Secondary (RAM, ROM, PROM, EPROM, EEPROM), Secondary Storage Devices (FD, CD, HD, Pen drive), I/O Devices (Scanners, Plotters, LCD, Plasma Display)

Number Systems: Introduction to Binary, Octal, Hexadecimal system Conversion, Simple Addition, Subtraction, Multiplication.

UNIT-II

Algorithm: Definition, Characteristics, Advantages and disadvantages, Examples.

Flowchart: Definition, Define symbols of flowchart, Advantages and disadvantages, Examples. Operating System and Services in O.S., Types of O.S.

DOS: History, Files and Directories, Internal and External Commands, Batch Files.

UNIT-III

Word Processing: Typing, Editing, Proofing & Reviewing, Formatting Text & Paragraphs, Automatic Formatting and Styles, Working with Tables, Graphics and Frames, Mail Merge, Automating Your Work & printing Documents.

Excel Spreadsheet: Working & Editing in Workbooks, Creating Formats & Links, formatting a Worksheet& creating graphic objects, Creating Charts (Graphs), formatting and analyzing data, Organizing Data in a List (Data Management), Sharing & Importing Data, Printing.

UNIT-IV

PowerPoint Presentations: Getting started in PowerPoint, creating a presentation, Creating & editing slides, previewing a slide show, Adding picture & graph, adding sound & video, adding auto shape, Animating objects.

Database packages: Purpose, usage, command, MS-Excel, Creation of files in MS-Access, Switching between applications.

Electronic Payment System: Secure Electronic Transaction, Types of Payment System: Digital Cash, Electronic Cheque, Smart Card, Credit/Debit Card E-Money, Bit Coins and Crypto currency, Electronic Fund Transfer (EFT), Unified Payment Interface (UPI), Immediate Payment System (IMPS), Digital Signature and Certification Authority.

Recommended Books / Suggested Readings:

1. Michael Miller, Absolute Beginners Guide to Computer Basics, Fourth Edition, Pearson Education (2007).
2. Deborah Morley, Charles S. Parker, Understanding Computers today and tomorrow, 11th Edition, Thomson (2007).
3. "Computers Today", D. H. Sanders, Fourth Edition, McGraw Hill, 1988.
4. Fundamental of Computers – By V. Rajaraman B.P.B. Publications.
5. "Fundamental of Computers – By P.K. Sinha.
6. MS-Office 2000(For Windows) – By Steve Sagman.

7. "Information Technology Inside and Outside", David Cyganski, John A. Orr, Paperback Edition, Pearson Education 2002.
8. IT Tools, R.K. Jain, Khanna Publishing House

DCS128: Computer fundamentals Lab

Credits: 2

LTP: 004

Course Description:

The course aims to equip the students with the knowledge of computer fundamentals. In this course includes Microsoft Office applications Word, Excel, Access and PowerPoint.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Describe basic architecture of computer.

CO2: Describe the fundamental Computer components that make up a computer's hardware and the role of each of these components.

CO3: Recognize when to use each of the Microsoft Office programs to create professional business documents.

CO4: Attain skills in Microsoft office such as: MS Word, MS Excel and MS PowerPoint.

List of Experiments

1. Identify computer hardware and software (in the lab).
2. Draw and explain the block diagram of computer system.
3. Demonstrate various peripherals and their applications.
4. Demonstrate the usage of various storage devices.
5. Illustrate the booting procedure (using windows).
6. Demonstrate installation of application software (in windows).
7. Introduction to DOS Commands.
8. Introduction to Windows.
9. Introduction to Microsoft Office.
10. Introduction to MS-Word.
11. Define page size and margins for a document.
12. Insert graphics (a picture for example) in a document.
13. Prepare a document with at least three fonts and four different font sizes. Include superscript and subscript.
14. Prepare your biodata in one A-4 size page.
15. Prepare a document with at least three fonts and four different font sizes. Include superscript and subscript.
16. Explain the use of spell check.
17. Introduction to MS-Excel.
18. Open a work sheet, name it and save it.
19. Change the width of a column/ range of columns.

DCS102: Computer Networks

Credits: 4

LTP:400

Course Description:

The course aims to equip the students with hand on use of the devices and techniques of computer network. The course includes OSI and TCP/IP model, Network Model, Network Topologies and Multiplexing and Routing.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Define, use and implement Computer Networks and the basic components of a Network system.

CO2: Explain the layers of OSI and TCP model, get knowledge about protocols.

CO3: Compare the various types of network topologies and applying them to meet the changing and challenging networking needs of organizations.

CO4: Apply various types of multiplexing techniques and apply pieces of hardware and software to make networks more efficient, faster, more secure, easier to use by Routing Algorithms.

Course Content

UNIT-1

Introduction: Introduction to Computer Networks, Components, Local Area Network (LAN), Metropolitan Area Network (MAN), Wide Area Networks (WAN), Guided Transmission Media, Twisted Pair, Coaxial cable, Optical fiber, wireless transmission, Radio waves, microwaves, infrared wave.

UNIT-II

Network Model: Satellite Communication Protocols (TCP/IP, SMTP, FTP, PPP, POP), Services, Network architecture, design issues, OSI Reference model, TCP/IP Reference model, Comparison of OSI and TCP/IP Models, Internet, Connection-Oriented and Connection oriented Protocols. Networks Frame Relay.

UNIT-III

Network Topologies: Network Topologies, Data Link Layer, Framing, Error control, Flow Control, Error Detection and correction, Circuit Switching, Packet switching, Message switching.

UNIT-IV

Multiplexing and Routing: Multiplexing (Frequency Division Multiplexing, Time Division Multiplexing, Synchronous and Asynchronous TDM), Routing Algorithms, Optimality principle, Shortest path routing, Flooding, Distance Vector Routing, Link State Routing, Hierarchical Routing, Broadcast and Multi Cast Routing.

Recommended Books / Suggested Readings:

1. Data Communications and Networking. Behrouz A. Forouzan
2. Data Communications and Networking (McGraw-Hill Forouzan Networking
3. Peterson and Davie. Computer Networks (2nd Edition). San Francisco, CA: Morgan Kaufmann Publishers, 1999.
4. Walrand and Varaiya. High Performance Communication Networks. San Francisco, CA: Morgan Kaufmann Publishers, 1996. ISBN: 1558603417.
5. Tanenbaum, A. S. Computer Networks. 4th ed. Upper Saddle River, NJ: Prentice Hall, 2003. ISBN: 0130661023.

DCS122: Computer Networks Lab

Credits: 1

LTP 002

Course Description:

The course aims to equip the students with understanding of the processes and techniques of computer network. This course includes computer networking basics.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Demonstrate the installation and configuration of network simulator.

CO2: Discuss the key elements of a computer network.

CO3: Demonstrate and measure different network scenarios and their performance behavior

CO4: Design and setup an organization network using packet tracer.

List of Experiments:

1. Study of different types of network cables
2. IP Addressing
3. Introduction to Packet Tracer 5.3 & Simple 5 PC's network
4. Cross-wired and straight cable using clamping tools.
5. Connect with other computers in LAN.
6. Building a LAN with HUPs and Switches
7. Network Commands
8. Configure network Topology using packet tracer software.
9. Distance Vector routing protocol.
10. Router Configuration Using Packet Tracer

DCS106: Operating System with Linux

Credits:4

LTP:400

Course Description:

The course aims to equip the students to understand the services provided by and the design of an operating system. This course includes Operating System, Process Management, Linux Operating System and Linux Operating System.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Describe the design issues associated with operating systems.

CO2: Discuss about Virtual memory, paging, and memory allocation.

CO3: Describe the Linux operating system.

CO4: Describe shared memory segments, message queues.

Course Content:

UNIT - I

Operating System: Concept, Components of Operating System, Operating System Operations, Protection and Security. Computing Environment, Single-Processor Systems, Multiprocessor Systems. Types of Operating Systems: Batch Operating System, Multi-Programmed Operating System, Time-Shared Operating System, Real Time Operating System, Distributed Operating Systems.

Process Management: Process Concept, Operation on Processes, Cooperating Processes, Inter-Process Communication, Threads**.**

Linux Operating System: Introduction to Linux OS, Basic Commands of Linux OS.

UNIT - II

Process Synchronization: Introduction, The Critical-Section Problem with solution, Bakery Algorithm, Synchronization hardware, Semaphores, Semaphores Implementation, Classical Problems of Synchronization with algorithms, Critical Regions, Monitors.

CPU Scheduling: Basic Concepts, Scheduling Criteria, Scheduling algorithms, Multilevel Queue Scheduling, Multilevel Feedback Queue Scheduling.

UNIT - III

Deadlock: System Models, Deadlock Characterization, Resource Allocation Graph, Deadlock Prevention, Avoidance, Detection and Recovery, Banker's algorithm.

Memory Management: Main Memory: Contiguous Memory Allocation, Fragmentation, Paging, and Segmentation. Virtual Memory: Demand Paging, Page Replacement, Page replacement algorithm, Allocation of frames, Thrashing.

Linux Operating System: Memory Management Commands and System Calls.

UNIT - IV

File, Devices and Secondary Storage Management: File-System Interface: Concepts, Access Methods, Directory and Disk Structure. File-System Structure, File-System Implementation, Directory Implementation, Allocation Methods, Free-Space Management**.**

Devices: Types of devices, Channels and Control Unit, Multiple Paths, Block Multiplexing**.** Secondary Storage: Mass-Storage Structure, Disk Structure, Disk Scheduling Algorithms, Disk Management, RAID structure of disk.

Recommended Books / Suggested Readings:

1. Silberschatz, Galvin, Greg, "Operating System Concepts", Wiley and Sons, 9th Edition, 2015.
2. Sumitabha Das, "Unix concept and Programming", McGraw Hill education, 4th Edition, 2015.
3. Godbole, Achyut, "Operating System", McGraw-Hill Education, 2nd Edition, 2005.
4. William Stallings, "Operating System: Internals and Design Principles", Person, 9th Edition, 2018.
5. A. S. Tanenbaum, "Modern Operating Systems ", Pearson, 3rd Edition, 2007.
6. Kenneth H. Rosenet al, "UNIX: The Complete Reference", McGraw-Hill/Osborne, 6th Edition, 2017.
7. Dhanjay M. Dhamdhere, "Operating System A concept based approach", Tata McGraw-Hill, 2nd Edition, 2006.
8. RB6. Madnick E. and Donovan J., "Operating Systems", Tata McGraw Hill, 2001.

DCS126: Operating System with Linux Lab

Credits: 1

LTP 002

Course Description:

The course aims to equip the students with a comprehensive study of the Linux and Shell Programming. The course includes shell scripts, Linux systems.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Discuss various basic commands, redirection and input/output of Linux based operating systems.

CO2: Describe the fundamental concepts of programming like loops, conditions, operators etc. specific to Shell Programming.

CO3: Develop shell scripts for various built-in commands of Linux.

CO4: Master the basics of Linux administration.

List of Experiments:

1. Linux Installation: Install your choice of Linux distribution e.g. Ubuntu, Fedora, Debian.
2. Installing and Removing Software: Install gcc package. Verify that it runs, and then remove it.
3. Command line operations:
   a. Install any new package on your system.
   b. Remove the package installed.
   c. Find the passwd file in / using find command.
   d. Create a symbolic link to the file you found in last step.
   e. Create an empty file example.txt and move it in /tmp directory using relative pathname.
4. File Operations:
   a. Explore mounted filesystems on your system.
   b. What are different ways of exploring mounted filesystems on Linux.
   c. Archive and backup your home directory or work directory using tar, gzip commands.
   d. Use dd command to create files and explore different options to dd.
   e. Use diff command to create diff of two files.
   f. Use patch command to patch a file. And analyze the patch using diff command again.
5. Linux Editors:
   a. vim/emacsa. Create, modify, search, and navigate a file in editor.
   b. Learn all essential commands.
6. Linux Security:
   a. Use of pseudo to change user privileges to root.
   b. Identify all operations that require pseudo privileges.
   c. Create a new user and add it to pseudo configuration file.
   d. Set password for new user.
   e. Modify the expiration date for new user using password ageing.
   f. Delete newly added user.
7. Programs based on shell scripting.

DCS107: Cyber Security

Credits:4

LTP:400

Course Description:

The course aims to equip the students to learn about Cyber security. This course includes Threats, Data Identity theft & fraud, cyber crimes and cyber laws and ethical hacking related contents.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Describe the major concepts of Cyber Security.

CO2: Describe appreciate, employ, design, and implement appropriate security technologies and policies to protect computers and digital information.

CO3: Discuss technical and legal aspects of computer crime investigations

CO4: Demonstrate the use of standards and cyber laws to enhance information security in the development process and infrastructure protection and learn the procedures of recovering computer evidence.

Course Content:

UNIT-I

Essential Terminologies: CIA, Risks, Breaches, Threats, Attacks, Exploits. Information Gathering (Social Engineering, Foot Printing & Scanning). Open Source Tools: Nmap, Zen map, Port Scanners, Network scanners.

UNIT-II

Identity theft and identity fraud: Typologies of internet theft, virtual identity, credit identity. Prevalence and victimology, physical methods, of identity theft, phishing, spyware, trojans, Zombies, Ransomwares, insurance and loan fraud, immigration fraud.

UNIT-III

Cybercrimes and Cyber Laws: The Legal Perspectives Introduction, Why Do We Need Cyber claws: The Indian Context, Information Technology Act, 2000, Challenges to Indian Law and Cybercrime Scenario in India, Amendments to the Indian IT Act.

capabilities, Searching and seizing computer related evidence, Processing of evidence and report preparation.

UNIT-IV

Ethical Hacking: System Hacking and Hacking Wireless Networks: Aspect of remote password guessing, Role of eavesdropping, Various methods of password cracking, Keystroke Loggers, Understanding Sniffers, Comprehending Active and Passive Sniffing,

Recommended Books / Suggested Readings:

1. Nina Godbole, Sunita Belapur, “Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives”, Wiley India Publications, April 2011.
2. James Graham, Richard Howard, Ryan Olson, “Cyber Security Essentials”, CRC Press, Tailor and Francis Group, 2011
3. Robert Jones, “Internet Forensics: Using Digital Evidence to Solve Computer Crime”, O’Reilly Media, October 2005
4. Computer Forensics and Cyber Crime by M.T.Britz, Pearson Education, First Impression,2012.
5. Chad Steel, “Windows Forensics: The field guide for conducting corporate computer investigations”, Wiley India Publications, December 2006.
6. Bothra Harsh, “Hacking”, Khanna Publishing House, Delhi.
7. The basic of Hacking and Penetration testing, second edition on ethical hacking and penetration by Patrick Engebretson.
8. Gupta Sarika, “Information and Cyber Security”, Khanna Publishing House, Delhi.
9. Ankit Fadia; An Unofficial Guide to Ethical Hacking 2nd Edition; Macmillan India,2006.
10. Nina Godbole, “Information System Security”, Wiley.
11. Justice Yatindra Singh, Cyber Laws, Universal Law Publishing Co, New Delhi, (2012).

12. Verma S, K, Mittal Raman, Legal Dimensions of Cyber Space, Indian Law Institute, New Delhi, (2004).

DCS127: Cyber Security Lab

Credit: 1

LTP: 002

Course Description:

The course aims to equip the students with a comprehensive study of cyber world security by identifying, analyzing and remediate computer security breaches by learning and implementing real-world problems. In this course includes different cyber security tools/techniques.

Course Outcomes (CLO):

Upon successful completion of the course, the students should be able to:

CO1: Identify and analyze the risks in various medias and reduce the exploitations.

CO2: Analyze various attacks and how to be safe from your system from it.

CO3: Design and develop a security architecture for an organization.

CO4: Design operational and strategic cyber security strategies and policies.

List of Experiments:

1. Implement the following Substitution & Transposition Techniques concepts: a) Caesar Cipherb) Rail fence row & Column Transformation.
2. Implement the Diffie-Hellman Key Exchange mechanism using HTML and JavaScript. Consider the end user as one of the parties (Alice) and the JavaScript application as other party (bob).
3. Implement the following Attack: a) Dictionary Attack b) Brute Force Attack.
4. Installation of Wire shark, tcpdump, etc and observe data transferred in client server communication using UDP/TCP and identify the UDP/TCP datagram.
5. Installation of rootkits and study about the variety of options.
6. Perform an Experiment to Sniff Traffic using ARP Poisoning.
7. Demonstrate intrusion detection system using any tool (snort or any other s/w). Demonstrate how to provide secure data storage, secure data transmission and for creating digital signatures.

COM101: **English Communication**

Credits: 2

Course Description:

1. To make students capable of using English language in context.
2. To enhance effective reading and writing skills.

This course comprises of Reading skills, writing skills, English grammar as well as vocabulary

Course Outcomes:

1. The students will develop a minute practical knowledge about English grammar and its usage
2. The students will develop an understanding of the importance of free expression.

Contents:

UNIT I

Reading Skills: Comprehension of Unseen Passage [Reading articles] (Intermediate) Summary Paraphrasing, Translation and Precis Writing.

UNIT II

English Grammar and Usage: Parts of speech, common errors in writing (based on Parts of Speech) Tenses, Change of Voice, Transformation of Sentences.

UNIT III

Basic Writing Skills and Writing Practices: Paragraph/essay writing, short life story writing, Notice (General like trip, change of name, function) making notes and Letter writing.

UNIT IV

Vocabulary Enhancement: Synonym, Antonym, Idioms and Phrasal verbs

Recommended Books / Suggested Readings:

1. *Practical English Usage.* Michael Swan OUP. 1995
2. *On Writing Well. William* Zinsser. Harper Resource Book. 2001
3. *Communication Skills*. Sanjay Kumar and Pushp Lata.Oxford University Press. 2006
4. *Exercises in Spoken English.* CIEFL, Hyderabad. Oxford University Press

Internet Links:

1. https://www.englishgrammar101.com/
2. http://learnenglish.britishcouncil.org/en/english-grammar
3. http://www.englishgrammarsecrets.com/
4. http://www.myenglishpages.com/
5. http://www.english-for-students.com/Homonyms-B.html

COM121: English Communication Lab
Credits: 1
LTP 002

Course Description: The course aims to equip the students with focus on the production and practice of sounds of language and familiarizes the students with the use of English in everyday situations both in formal and informal contexts. The course includes description of sights seen in everyday life, pronunciation of different words and its correct usage.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Develop better understanding of nuances of English language through audio- visual experience and group activities
CO2: Hone speaking skills with clarity and confidence
CO3: Have better comprehension of accent of people of different backgrounds and regions
CO4: Use English grammar accurately

Course Content

UNIT I

Daily Discourse: Common Everyday Situations: Conversations and Dialogues (Unit 1-6), Monologue (2D/4D/5D/6D), and Communication at workplace

UNIT II

Listening Skills: Listening skills on Social Interactions (Unit 1), work and study (Unit 2), daily life (Unit 3), food (Unit 4), Places (Unit 5) and Family (Unit 6)

UNIT III

Phonetic Skills: Pronunciation, Intonation, Stress (Unit 1-6) and Rhythm

UNIT IV

Speaking Skills: Group Discussion / Debate, Role Plays

SEMESTER II

DCS207: **Python Programming**

Credits: 4

LTP: 310

Course Description:

The course aims to equip the students with programming paradigms brought in by Python with a focus on File Handling. The course includes basic programming constructs in python.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Describe basic programming constructs in python.

CO2: Learn the use of control structures and numerous native data types with their methods.

CO3: Design user defined functions, modules, and packages.

CO4: Identify and handle the exceptions in programs through appropriate exceptions handling methods.

Course Content

UNIT I

Introduction: History of Python, Need of Python Programming, Applications Basics of Python Programming Using the REPL(Shell), Running Python Scripts, Variables, Assignment, Multiple Assignment, Keywords, Identifiers, Python Statement, Input-Output functions, Indentation, Documentation, Data Types.

UNIT II

Operators and Expressions: Arithmetic Operators, Assignment Operators, relational and Logical Operators, Bitwise Operators, Ternary operator, Increment or Decrement operator, Membership Operators, Identity Operators, Expressions and order of evaluations.

UNIT III

Control Structures: Decision making statements, Python loops, Python control statements.

Array: Array, array representation, basic operations performed on array.

Structures & Functions: Numbers, Strings, Lists, Tuples, Dictionary, Date & Time, Defining Functions, Exit function, default arguments.

Modules: Module, creating modules, import statement, Path Searching of a Module, Module Reloading, Standard Modules.

UNIT IV

Python packages: Introduction to PIP, Installing Packages via PIP, Using Python Packages.

Error and Exceptions: Difference between an error and Exception, Handling Exception, try except block, Raising Exceptions, User Defined Exceptions.

Object Oriented Programming OOP in Python: Classes, 'self-variable', Methods, Constructor Method, Inheritance, Overriding Methods, Data Hiding.

Recommended Books / Suggested Readings:

1. Python Programming: A Modern Approach, Vamsi Kurama, Pearson
2. Learning Python, Mark Lutz, Orielly.
3. Python, The complete Reference, Martin C. Brown, Mc Graw Hill Education.
4. Core Python Programming, R. Nageswara Rao, 2nd Ediiton, Dreamtech.

DCS227: Python Programming Lab

Credits: 1

LTP: 002

Course Description:

The course aims to equip the students to familiarize with basics of Python programming. The course includes fundamentals of programming.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Describe the Numbers, Math functions, Strings, List, Tuples and Dictionaries in Python.

CO2: Develop logic of various programming problems using numerous data types and control structures of Python.

CO3: Interpret Object oriented programming in Python.

CO4: Implement modules and functions using Python.

List of Experiments:

1. Write a program to compute GCD of two numbers.
2. Write a program to find factorial of number.
3. Write a program to find the given year is leap or not.
4. Write a program to display current date and time.
5. Write a program which accepts the radius of circle from the user and calculate the area.
6. Write a program to swap two variables.
7. Write a program to check prime number.
8. Write a program to check whether string is palindrome.
9. Write a program to generate Fibonacci series.
10. Write a program to find the quadratics equation.
11. Programs based on decision making statements.
12. Programs based on looping statements.
13. Programs based on array.
14. Write a program to find the duplicate elements in List.
15. Write a program to sorting the List.
16. Write a program to find the differences between two lists.
17. Write a program to find the most frequent words in a text read from a file.
18. Write a program to find the longest words.
19. Write a program to illustrate of use of arg and kwargs.
20. Programs based on functions.
21. Write a program to create a module of factorial in Python.
22. Write a Python class named Rectangle constructed by a length and width and a method which will compute the area of a rectangle.
23. Write a Python class named Circle constructed by a radius and two methods which will compute the area and the perimeter of a circle
24. Any other programs related to it.

DCS202: Malware Taxonomy and Analysis

Credits: 4

LTP: 400

Course Description:

The course aims to equip the students with a specialist understanding of the nature of malware, its capabilities, and how it is combated through detection and classification. This course includes static and dynamic analysis techniques, windows internals and api, and analysis techniques.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Define what the underlying scientific and logical limitations on society's ability are to combat malware.

CO2: Apply the tools and methodologies used to perform static on unknown executables.

CO3: Describe the executable formats, Windows internals and API, and analysis techniques.\

CO4: Apply techniques and concepts to unpack, extract, decrypt, or bypass new ant analysis techniques in future malware samples.

Course Content

UNIT-I

Introduction: Introduction to malware, OS security concepts, malware threats, evolution of malware, malware types viruses, worms, rootkits, Trojans, bots, spyware, adware, logic bombs, malware analysis, static malware analysis, dynamic malware analysis

UNIT-II

Static Analysis:X86 Architecture- Main Memory, Instructions, Opcodes and Endianness, Operands, Registers, Simple Instructions, The Stack, Conditionals, Branching, Rep Instructions, C Main Method and Offsets. Antivirus Scanning, Fingerprint for Malware, Portable Executable File Format, The PE File Headers and Sections, The Structure of a Virtual Machine, Reverse Engineering- x86 Architecture, recognizing c code constructs in assembly, c++ analysis, Analyzing Windows programs, Anti-static analysis techniques obfuscation, packing, metamorphism, polymorphism.

UNIT-III

Dynamic Analysis: Live malware analysis, dead malware analysis, analyzing traces of malware- system-calls, api-calls, registries, network activities. Anti-dynamic analysis technique-santi-vm, runtime-evasion techniques, Malware Sandbox, Monitoring with Process Monitor, Packet Sniffing with Wireshark, Kernel vs. User-Mode Debugging, OllyDbg, Breakpoints, Tracing, Exception Handling, Patching

UNIT-IV

Malware Functionality: Downloader, Backdoors, Credential Stealers, Persistence Mechanisms, Privilege Escalation, Covert malware launching- Launchers, Process Injection, Process Replacement, Hook Injection, Detours, APC injection.

Malware Detection Techniques: Signature-based techniques: malware signatures, packed malware signature, metamorphic and polymorphic malware signature Non-signature-based techniques: similarity-based techniques, machine-learning methods, invariant inferences.

Recommended Books / Suggested Readings:

1. Practical malware analysis The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig ISBN-10: 159327-290-1, ISBN-13: 978-1-59327-290-6, 2012 2
2. Computer viruses: from theory to applications by Filiol, Eric Springer Science & Business Media, 2006
3. Android Malware by Xuxian Jiang and Yajin Zhou, Springer ISBN 978-1-4614-7393-0, 2005
4. Hacking exposed™ malware & rootkits: malware & rootkits security secrets & Solutions by Michael Davis, Sean Bodmer, Aaron Lemasters, McGraw-Hill, ISBN: 978-0-07-159119-5, 2010 • Windows Malware Analysis Essentials by Victor Marak, Packt Publishing, 2015

DCS208: Cryptography and Network Security

Credits: 3

LTP: 300

Course Description:

The course aims to equip the students to provides the basic understanding of cryptography, how it has evolved, and some key encryption techniques used today. The course includes basics of Cryptography and Network Security.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Provide security of the data over the network.

CO2: Describe the emerging areas of cryptography and network security.

CO3: Discuss any network from the threats in the world.

CO4: Describe the concept of digital signatures, e-mail security, and web security.

Course Content

UNIT I

Introduction to the Concepts of Security: The need for security, Security Approaches, Principles of Security, Types of Attacks. Cryptographic Techniques: Plain Text and Cipher Text, Substitution Techniques, Transposition Techniques, Encryption and Decryption, Symmetric and Asymmetric Key Cryptography, Steganography, Key Range and Key Size, Possible Types of Attacks.

UNIT II

Understanding Network Security: Defining Network Security, Security Services, Security Standards, Elements of Security, Security Threats to Computer Networks, Sources of Security Threats, Security Threat Motives, Security Threat Management.

UNIT III

Symmetric Key Cryptography: DES, International Data Encryption Algorithm (IDEA), RC5, Blowfish, AES.

Asymmetric key cryptography: RSA algorithm, Digital Signatures, Message Authentication.

Cryptographic Hash Functions: Hash functions, Uses of hashing, MD5, SHA.

UNIT IV

Network Security Practice: Authentication Applications, IP Security, System Security-Intruders, Malicious Software, Firewalls.

E-mail security: Pretty Good Privacy, working of PGP, S/MIME, MIME.

Web Security: Secure Socket layer, SSL session and connection, secure electronic transaction (SET).

Recommended Books / Suggested Readings:

1. Brijendra Singh, Cryptography & Network Security, PHI.
2. Pachghare, V.K., Cryptography and Information Security, PHI.
3. William Stallings, “Cryptography and Network Security –Principles and Practices”, Prentice Hall of India, Third Edition, 2003.
4. Behrouz A. Forouzan and Debdeep Mukhopadhyay, "Cryptography and Network Security", 2nd Edition, McGrawHill Education, 2014.

DCS:228 Cryptography and Network Security Lab

Credits: 1

LTP: 002

Course Description:

The course aims to understand the concepts of various security Algorithms. The course includes algorithms DES, RSA, MD5, SHA-1

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Implement the cipher techniques.

CO2: Develop the various security algorithms.

CO3: Use different open source tools for network security and analysis.

CO4: Describe various tools related to Network Security.

List of Experiments:

1. write a program to implement the simple substitution technique named Caesar cipher.
2. write a program to implement the Playfair Substitution technique.
3. write a program to implement the hill cipher substitution techniques.
4. write a program to implement the rail fence transposition technique.
5. Write a program to implement the DES algorithm logic.
6. Write a program to implement the Blowfish algorithm logic.
7. Write a program to implement RSA Algorithm.
8. write a program to implement the MD5 hashing technique.
9. write a program to implement the SHA-I hashing technique.
10. To write a program to implement the signature scheme named digital signature standard.
11. To study various tools related to Network Security.
12. Installation of rootkits and study about the variety of options.
13. Demonstrate intrusion detection system (ids) using any tool (snort or any other s/w).

DCS204: Cyber Forensic

Credits: 4

LTP: 400

Course Description:

The course aims to equip the students with cyber forensics concept such as acquisition and analysis. The course includes IP, Firewall, Computer forensics and Data hiding. This course includes forensics, legal issues related to electronic evidence.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Describe the security issues of network layer and transport layer.

CO2: Apply security principles in the application layer.

CO3: Analyze and validate forensics data.

CO4: Demonstrate forensics tools.

Course Content

UNIT-I

Network Layer Security &Transport Layer Security: IPSec Protocol - IP Authentication Header - IP ESP - Key Management Protocol for IPSec. Transport layer Security: SSL protocol, Cryptographic Computations – TLS Protocol.

UNIT-II

E-Mail Security & Firewalls: PGP - S/MIME - Internet Firewalls for Trusted System: Roles of Firewalls – Firewall related terminology- Types of Firewalls - Firewall designs - SET for E-Commerce Transactions.

UNIT-III

Introduction to Computer Forensic: Introduction to Traditional Computer Crime, Traditional problems associated with Computer Crime. Introduction to Identity Theft & Identity Fraud. Types of CF techniques - Incident and incident response methodology - Forensic duplication and investigation. Preparation for IR: Creating response tool kit and IR team. - Forensics Technology and Systems - Understanding Computer Investigation – Data Acquisition.

UNIT-IV

Evidence Collection and Forensics Tools: Processing Crime and Incident Scenes – Working with Windows and DOS Systems. Current Computer Forensics Tools: Software/ Hardware Tools.

Analysis and Validation: Validating Forensics Data – Data Hiding Techniques – Performing Remote Acquisition – Network Forensics – Email Investigations – Cell Phone and Mobile Devices Forensics

Recommended Books / Suggested Readings:

1. Man Young Rhee, “Internet Security: Cryptographic Principles”, “Algorithms and Protocols”, Wiley Publications, 2003.
2. Nelson, Phillips, Enfinger, Steuart, “Computer Forensics and Investigations”, Cengage Learning, India Edition, 2008.
3. John R.Vacca, “Computer Forensics”, Cengage Learning, 2005
4. Richard E.Smith, “Internet Cryptography”, 3rd Edition Pearson Education, 2008.
5. Marjie T.Britz, “Computer Forensics and Cyber Crime”: An Introduction”, 3rd Edition, Prentice Hall, 2013.

DCS209: Kali Linux with penetration testing

Credits: 4

LTP: 400

Course Description:

The course aims to equip the students with basic knowledge of Kali Linux, penetration testing and IT security techniques that lies under the cyber security. This course includes the tools that Kali Linux offers to perform network penetration testing, network scanning

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Discuss the penetration testing standards.

CO2: Identify Vulnerability Assessment Tools for System.

CO3: Classify the basic structure of Exploits and Client-Side Attack and privileges escalation.

CO4: Apply a mature understanding of various types of penetration testing.

Course Content

UNIT-I

Introduction: Installing kali Linux, Configure Network Connection, Update kali Linux. Penetration testing: standard, Open Web Application Security Project (OWASP), Licensee Penetration Testing (LPT), Classification, White Box and Black Box, Penetration Testing Vs Vulnerability Assessment,

Advance Penetration Methodology: Target Framework and Scope, Gathering client requirements, Test plan checklist, Profiling test boundaries, Advance penetration testing with Kali Linux.

UNIT-II

Information Discovery: Google hacking, DNS Information Gathering, Whois Information Gathering, Route and Network information Gathering, All-in-one information gathering, Enumeration, Firewall bypassing, Route Bypassing, Network Scanning, Route Tracing.

Scanning Target: Advance Network Scanning, Port Scanning, Stealth Port scanning techniques, Udp port Scanning, Packet crafting using Hping, Nmap Scanning and Plug-ins, Active and Passive Banners.

Vulnerability Assessment Tools: Nessus, Open Vas, enumerating users, groups and shares, Enumerating DNS resource records, Enumerating Network devices.

UNIT-III

Target Exploitation: Setting up metaslpoit, Exploitation with Metasploit working with Meterpreter Session, VNC Exploitation, stealing password Hash, Adding custom Modules to Metasploit.

Privileges Escalation: Breaking Password hashes, Cracking telnet and ssh password, Cracking FTP password. Protocol tunneling, Proxy, Installing persistent Backdoor.

UNIT-IV

Advance Sniffing: ARP Poisoning, DHCP Starvation, Mac flooding, DNS Poisoning: redirecting user to fake website, Sniffing credentials from secured websites, Syn Attack, Application request Flood Attack, Service request Flood, Permanent DoS (denial of service) attack.

Testing: Wireless Penetration Testing, Exploits and client-Side attack, Social Engineering Toolkit, Firewall Testing.

Recommended Books / Suggested Readings:

1. Kali Linux Wireless Penetration Testing: Beginner's Guide: Learn to penetrate Wi-Fi and wireless networks to secure your system from vulnerabilities Kindle Edition by Vivek Ramachandran, Cameron Buchanan.
2. Basic Security Testing with Kali Linux 2 Paperback, 24 March 2016 by Daniel W. Dieterle .
3. Kali Linux Network Scanning Cookbook Paperback, 21 August 2014 by Justin Hutchens.

DCS229: Kali Linux with penetration testing Lab

Credits: 1

LTP: 002

Course Description:

The course aims that the Students will gain practical experience with designing and implementing concepts of Kali Linux. This course includes Kali Linux, Enumeration, Firewall bypassing, Route Bypassing, Network Scanning, Route Tracing.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Interpret of the penetration testing standards.

CO2: Build Vulnerability Assessment Tools for System.

CO3: Discuss the basic structure of Exploits and Client-Side Attack and privileges escalation.

CO4: Apply a mature understanding of various types of penetration testing.

List of Experiments

1. Download and Configure Kali Linux
2. Enumeration, Firewall bypassing, Route Bypassing, Network Scanning, Route Tracing.
3. Kioptrix Level 1 — Enumeration and Exploitation
4. Kioptrix Level 2 — Enumeration and Exploitation
5. Kioptrix Level 3 — Enumeration and Exploitation
6. Windows and Linux (Service and Password Hacking – Bruteforce and other techniques) Penetration Testing.

DCS206: Mobile Device Security

Credits: 3

LTP: 300

Course Description:

The course aims to equip the students with the ways how the cell phone revolution has hit both the enterprise and the consumer market in a massive way. This course includes mobile networks, managements concepts, testing scenario.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Describe the overview of Mobile device security.

CO2: Define how to protect the entire mobility ecosystem

CO3: Identify various attacks which can be possible at each stage needs to be carefully

CO4: Apply testing on various types of cellular platforms.

Course Content

UNIT-I

Introduction: Mobile Security Model, Enterprise Mobile Environment, Mobile Crypto Algorithm. Mobile Devices - features and security concerns, Platforms, Applications - development, testing and delivery

UNIT-II

Mobile Eco-System Networks: Cellular Network - baseband processor and SIM card, GSM encryption and authentication and other attacks, WIFI Networks - public hotspots and enterprise WLANs, SSL/TLS, Web Technologies - server-side and client-side web applications.

UNIT-III

Management: Enterprise Mobility Program, Transactions Security, File Synchronization and Sharing, Vulnerability Assessments, BYOD Device Backup, Data Disposal/Sanitization, NAC for BYOD, Container Technologies, Exchange ActiveSync (EAS), Mobile Authentication, Mobile Management Tools

UNIT-IV

Scenario Testing: Cellular Attacks, Attacking Web Interface, Wireless Attacks, SSL attacks, Android, iOS.

Recommended Books / Suggested Readings:

1. Fried, S. (2010). Mobile device security: A comprehensive guide to securing your information in a moving world. Boca Raton, FL: Auerbach Publications.
2. Stuttard, D. & Pinto, M. (2011). The web application hacker's handbook: Discovering and exploiting security flaws (2nd ed.). Indianapolis, IN: Wiley, John & Sons.
3. Dwivedi, H., Clark, C., & Thiel, D. (2010). Mobile application security. New York: McGraw-Hill Companies.

SEMESTER III

DCS301: Cyber Crime Investigation and Digital Forensics

Credits: 4

LTP: 310

Course Description:

The course aims to equip the students with best practices and develop the skills to concepts of digital security and forensic. This course includes of digital security, cryptography for secure channels, cyber issues and digital forensics.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Identify computer and network system security risks and take preventive steps.

CO2: Describe the working of techniques and tools available for secure communication.

CO3: Classify cybercrime issues and investigation tools for evidences collection.

CO4: Apply forensic tools and software.

Course Content

UNIT-I

Digital Securities: Introduction, Types of Attacks, Digital Privacy, Online Tracking, Privacy Laws, Types of Computer Security risks (Malware, Hacking, Pharming, Phishing, Ransomware, Adware and Spyware, Trojan, Virus, Worms, WIFI Eavesdropping, Scareware, Distributed Denial-Of-Service Attack, Rootkits, Juice Jacking), Antivirus and Other Security solution, Password, Secure online browsing, Email Security, Social Engineering, Secure WIFI settings, Track yourself online, Cloud storage security, IOT security, Physical Security Threads

Online Anonymity: Anonymous Networks, Tor Network, I2P Network, Freenet, Darknet, Anonymous OS – Tails, Secure File Sharing, VPN, Proxy Server, Connection Leak Testing, Secure Search Engine, Web Browser Privacy Configuration, Anonymous Payment

UNIT-II

Cryptography and Secure Communication: The Difference Between Encryption and Cryptography, Cryptographic Functions, Cryptographic Types, Digital Signature, The Difference Between Digital Signatures and Electronic Signatures, Cryptographic Systems Trust Models, Create a Cryptographic Key Pair Using Gpg4win/gpg4usb, Disk Encryption Using Windows BitLocker, Disk Encryption Using Open Source Tools, Multitask Encryption Tools, Attacking Cryptographic Systems, Countermeasures Against Cryptography Attacks, Securing Data in Transit, Cloud Storage Encryption, Encrypt DNS Traffic and Email communication, Secure IM and video calls

UNIT-III

Cyber Crime Issues and Investigation: Unauthorized Access, Computer Intrusions, White collar Crimes, Viruses and Malicious Code, Internet Hacking and Cracking, Virus Attacks, Pornography, Software Piracy, Intellectual Property, Mail Bombs, Exploitation, Stalking and Obscenity in Internet, Digital laws and legislation, Law Enforcement Roles and Responses, Investigation Tools, eDiscovery, EDRM Model, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Search and Seizure of Computers, Recovering Deleted Evidences, Password Cracking.

UNIT-IV

Digital Forensics: Introduction to Digital Forensics, Forensic Software and Hardware, Analysis and Advanced Tools, Forensic Technology and Practices, Forensic Ballistics and Photography, Face, Iris and Fingerprint Recognition, Audio Video Analysis, Windows System Forensics, Linux System Forensics, WIFI Security (War-driving), Network Forensics, Mobile Forensics, Cloud Forensics.

Recommended Books / Suggested Readings:

1. Digital Privacy and Security Using Windows: A Practical Guide By Nihad Hassan, Rami Hijazi, Apress
2. Digital Forensics, DSCI - Nasscom, 2012.
3. Cyber Crime Investigation, DSCI - Nasscom, 2013.

DCS321: Cyber Crime Investigation and Digital Forensics Lab

Credits: 1

LTP: 002

Course Description:

The course aims that the Students will gain practical experience with designing and implementing concepts of Digital Security and Forensic. In this course includes cyber/computer forensics software/tools.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Identify computer and network system security risks and take preventive steps.

CO2: Define the working of techniques and tools available for secure communication.

CO3: Illustrate cybercrime issues and investigation tools for evidences collection.

CO3: Apply forensic tools and software.

List of Experiments:

1. Software Tools: CyberCheck 4.0 - Academic Version CyberCheckSuite MobileCheck Network Session Analyser Win-LiFT TrueImager TrueTraveller PhotoExaminer Ver 1.1, CDRAnalyzer, Keylogger.
2. Disk Forensics:
   - 2.1. Identify digital evidences
   - 2.2. Acquire the evidence
   - 2.3. Authenticate the evidence
   - 2.4. Preserve the evidence
   - 2.5. Analyze the evidence 6. Report the findings
3. Network Forensics:
   - 3.1.1. Intrusion detection
   - 3.1.2. Logging (the best way to track down a hacker is to keep vast records of activity on a network with the help of an intrusion detection system)
   - 3.1.3. Correlating intrusion detection and logging Device Forensics
     - 3.1.3.1. Mobile phone
     - 3.1.3.2. Digital Music
     - 3.1.3.3. Printer Forensics
     - 3.1.3.4. Scanner

DCS302: Firewall and Internet Security

Credits: 4

LTP: 004

Course Description:

The course aims to demonstrate how to plan and implement a firewall based on a security policy and provide the key component to a secure system. The course includes study of internet security, protocol and its classes, threats firewalls and VPNs.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Describe the terminology and fundamentals concepts related to firewalls and network perimeter defense.

CO2: Analyze the security concerns related to common protocols associated with different layers.

CO3: Explain various techniques commonly used to bypass firewalls, along with appropriate countermeasures.

CO4: Design appropriate firewall rule-set in accordance with the requirements and network security policy of organization.

Course Content

UNIT-1

Introduction to internet security: Internet security, picking a security policy, host-based security, perimeter security, strategies for a secure network, ethics of computer security.

Security Review protocols of lower layer: Basic protocols, managing addresses and names, IP version 4/6, network address translators, wireless security.

Upper layer security review protocols: messaging, internet telephony, RPC based protocol, FTP, Remote login, SNMP, proprietary protocol, peer-to-peer networking, X11 window system

UNIT-2

Threats: web protocol, risk to the client and server, classes of attacks: stealing passwords, bugs and back doors, authentication failure, protocol failure, information leakage, DoS attack, Exponential attack (Viruses and worms), Botnets, Active attacks

Hacker workbench: Hacking goals, Scanning a network, breaking into the host, battle for the host, covering tracks, hacking tools, tiger teams, safety tools services: Authentication (remembering passwords, OTP, OTP challenges/response, Lamport's OTP algorithm, smartcard, biometrics, H2H authentication, *Inetd*-network services, Ssh-terminal and file access, Syslog)

UNIT-3

Firewall and VPNs: definition, services, advantages and disadvantages, types of firewalls (packet filters, application-level filtering, circuit level gateways, dynamic packet filter, distributed firewall), filtering services, digging for warms.

Firewall Rulesets, Tunneling and VPNs: firewall rulesets, proxies, building firewall from scratch, firewall problems, testing firewalls. Tunnels, VPN, VPN in software & hardware

UNIT-4

Protecting and Organization: Intranet explorations, intranet routing tricks, Safe host in a hostile environment, properties of secure hosts, hardware configuration, administering a secure host, skinny-dipping: life without firewall, intrusion detection, where to detect intrusion, types of IDs, Administrating IDs and IDS tools

Recommended Books / Suggested Readings:

1. Firewalls and Internet Security - Repelling the Wily Hacker, 2nd Edition, by W. R. Cheswick, S. M. Bellovin, A. D. Rubin; Addison-Wesley
2. Introduction to Computer Security, by Matt Bishop; Prentice Hall

DCS304: Web Technologies

Credits: 3

LTP: 300

Course Description:

The course aims to equip the students with a comprehensive study of the Web Technologies. The course includes HTML, CSS, JavaScript, and Ajax.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Analyze, and apply the role of languages like HTML, DHTML, CSS, XML, JavaScript, VBScript, PHP and protocols in the workings of the web and web applications.

CO2: Create web pages using HTML, DHTML and Cascading Styles sheets.

CO3: Build interactive web applications.

CO4: Create XML documents and XML Schema.

Course Content

UNIT I

Introduction: History of the web, Growth of the Web, Protocols governing the web, Web project, Web Team, Team dynamics.

World Wide Web, Web browsers, Markup Languages, Style Sheet technologies, client side, server side, HTML Headings, Links, images, Lists, Tables, Forms, Frames.

UNIT II

HTML: Formatting Tags, Links, List, Tables, Frames, forms, Comments in HTML, DHTML.

Java Script: Introduction, Documents, Documents, forms, statements, functions, objects in Java Script, Events and Event Handling,

Arrays, FORMS, Buttons, Checkboxes, Text fields and Text areas.

UNIT III

Introduction to Web Development: Website Webpage, Static Website, Dynamic Website.

XML: Introduction, Display and XML Documents, Data Interchange with an XML document, Document types definitions, Parsers using XML, Client-side usage, Server-Side usage.

UNIT IV

Introduction to Cascading Style Sheets: Concept of CSS, Creating Style Sheet, Properties, CSS Styling(Background, Text Format, Controlling Fonts), Working with block elements and objects, Working with Lists and Tables ,CSS Id and Class, Box Model(Introduction, Border properties, Padding Properties, Margin properties), CSS Advanced(Grouping, Dimension, Display, Positioning, Floating, Align, Pseudo class, Navigation Bar, Image Sprites, Attribute sector), CSS Color, Creating page Layout and Site Designs.

Recommended Books / Suggested Readings:

1. Deitel, Deitel and Neito, INTERNET and WORLD WIDE WEB –How to program, Pearson Education Asia, 5thEdition , 2011.HTML & CSS: The Complete Reference, Thomas Powell, Fifth Edition.
2. Achyut S Godbole and Atul Kahate, “Web Technologies”, Second Edition, Tata McGraw Hill, 2012.
3. Thomas A Powell, Fritz Schneider, “JavaScript: The Complete Reference”, Third Edition, TataMcGraw Hill, 2013.
4. HTML A Beginner's Guide Wendy L. Willard, Fourth Edition
5. HTML, XHTML and CSS All-In-One for Dummies Andy Harris, Second Edition
6. JavaScript, A Beginner's Guide John Pollock, Third Edition
7. Professional JavaScript for Web Developers (Wrox Programmer) Nicholas C. Zakas, Second Edition

Websites:

1. www.w3schools.com
2. www.html.net
3. www.thesitewizard.com
4. www.learndreamweavertutorials.com

DCS324: Web Technologies Lab

Credits: 1

LTP: 002

Course Description:

The course aims to equip the students with a comprehensive study of the Web Technologies. The course includes HTML, CSS, JavaScript, Ajax.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Apply the role of languages like HTML, CSS.

CO2: Analyze a web page and identify its elements and attributes.

CO3: Create web pages using HTML, and Cascading Styles sheets.

CO4: Create dynamic web pages.

List of Experiments:

1. Preparation of Biodata using Forms in HTML.
2. Simple Calculation a) Inventory Calculation.
3. Input Validation a) Payroll maintenance.
4. Event Handling a) Changing the Background Color of the Window.
5. Develop a Dynamic Web page Using CSS properties and elements for a university website.
6. To generate the random numbers and display in a table format.
7. Generation of Fibonacci series.
8. Different Pascal triangle generation.
9. Function to determine the pair of integers whether the second integer is multiple of the first.
10. Quiz program.
11. Create a guessing number game.
12. HTML form validation.
13. Program to implement the concept of operator, arrays and functions.

Websites:

1. www.w3schools.com
2. www.html.net
3. www.thesitewizard.com
4. www.learndreamweavertutorials.com

DCS305: Mobile Forensics

Credits: 4

LTP: 400

Course Description:

The course aims to equip the students with cyber forensics concept such as acquisition and analysis. The course includes IP, Firewall, Computer forensics and Data hiding. This course includes the common legal issues related to electronic evidence.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Understand the security issues of network layer and transport layer.

CO2: Apply security principles in the application layer.

CO3: Analyze and validate forensics data.

CO4: Demonstrate forensics tools.

Course Content

UNIT-I

Layer Security &Transport Layer Security: IPSec Protocol - IP Authentication Header - IP ESP - Key Management Protocol for IPSec. Transport layer Security: SSL protocol, Cryptographic Computations – TLS Protocol.

UNIT-II

E-Mail Security & Firewalls: PGP - S/MIME - Internet Firewalls for Trusted System: Roles of Firewalls – Firewall related terminology- Types of Firewalls - Firewall designs - SET for E-Commerce Transactions.

UNIT-III

Introduction to Computer Forensic: Introduction to Traditional Computer Crime, Traditional problems associated with Computer Crime. Introduction to Identity Theft & Identity Fraud. Types of CF techniques - Incident and incident response methodology - Forensic duplication and investigation. Preparation for IR: Creating response tool kit and IR team. - Forensics Technology and Systems - Understanding Computer Investigation – Data Acquisition.

UNIT-IV

Evidence Collection and Forensics Tools: Processing Crime and Incident Scenes – Working with Windows and DOS Systems. Current Computer Forensics Tools: Software/ Hardware Tools.

Analysis and Validation: Validating Forensics Data – Data Hiding Techniques – Performing Remote Acquisition – Network Forensics – Email Investigations – Cell Phone and Mobile Devices Forensics

Recommended Books / Suggested Readings:

1. Man, Young Rhee, “Internet Security: Cryptographic Principles”, “Algorithms and Protocols”, Wiley Publications, 2003.
2. Nelson, Phillips, Enfinger, Steuart, “Computer Forensics and Investigations”, Cengage Learning, India Edition, 2008.
3. John R.Vacca, “Computer Forensics”, Cengage Learning, 2005
4. Richard E.Smith, “Internet Cryptography”, 3rd Edition Pearson Education, 2008.
5. Marjie T.Britz, “Computer Forensics and Cyber Crime”: An Introduction”, 3rd Edition, Prentice Hall, 2013.

DCS306: Ethical Hacking

Credits: 4

LTP: 400

Course Description:

The course aims to covers the theory and practices of finding the vulnerabilities through forming the different attacks and then defining the appropriate security policy including the action to detect or prevent the attacks and thus reduce the damages. This course includes concepts of ethical hacking, scanning & mapping networks, viruses & its types and web/mobile attacks.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Describe and understand the basics of the ethical hacking.

CO2: Determine the signature of different attacks and prevent them

CO3: Recognize the malware and their attacks and detect and prevent them

CO4: Identify and prevent the security attacks in different environments

Course Content

UNIT-I

An Introduction to Ethical Hacking: Security Fundamental, Security testing, Hacker and Cracker, Descriptions, Test Plans-keeping It legal, Ethical and Legality**,** The Attacker's Process, The Ethical Hacker's Process, Security and the Stack

UNIT-II

Footprinting and Scanning: Information Gathering, Determining the Network Range, Identifying Active Machines, Finding Open Ports and Access Points, OS Fingerprinting Services, Mapping the Network Attack Surface**.** Enumeration, System Hacking.

UNIT-III

Malware Threats: Viruses and Worms, Trojans, Covert Communication, Keystroke Logging and Spyware, Malware Counter measures. Sniffers, Session Hijacking, Denial of Service and Distributed Denial of Service.

Web Server Hacking, Web Applications and Database Attacks: Web Server Hacking, Web Application Hacking, Database Hacking

UNIT-IV

Wireless Technologies, Mobile Security and Attacks: Wireless Technologies, Mobile Device Operation and Security, Wireless LANs. Intrusion Detection Systems, Firewalls, Honeypots, Physical Security, Social Engineering, Cloud Computing, Botnets.

Recommended Books / Suggested Readings:

1. Certified Ethical Hacker, Version 9, Second Edition, Michael Gregg, Pearson IT Certification
2. Hacking the Hacker, Roger Grimes, Wiley
3. The Unofficial Guide to Ethical Hacking, Ankit Fadia, Premier Press

DCS326: Ethical Hacking Lab

Credits: 1

LTP:002

Course Description:

The course aims that the students practices of finding the vulnerabilities through forming the different attacks and then defining the appropriate security policy including the action to detect or prevent the attacks and thus reduce the damages. This course includes foundation of cracking and ethical hacking

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Develop the foot printing and scanning

CO2: Demonstrate the techniques for system hacking

CO3: Determine the signature of different attacks and prevent them

CO4: Identify and prevent the security attacks in different environments.

List of Experiments:

1. List the tools for Ethical Hacking.
2. Implement Foot printing and Reconnaissance using tools 3d Traceroute, Alchemy Eye, DNS Tools and Network Solution Whois.
3. Implement Network Scanning using tools Advanced Port Scanner, Colasoft Ping Tool, Hide Your IP Address, Nessus and Nmap.
4. Implement Enumeration using tools Default Password List, Default Password List, OpUtil Network Monitoring Tool and OpUtil Network Monitoring Tool.
5. Implement system hacking using tools Actual spy, Alchemy Remote Executor, Armor Tool and FSecure BlackLight.
6. Implement Trojan and Backdoors using tools Absolute Startup Manager, Absolute Startup Manager, Netwirx Services Monitor and StartEd Lite.
7. Implement Viruses and Worms using tools Anubis Analyzing Unknown Binaries, Filterbit, Sunbelt CWSandbox and ThreatExpert.
8. Implement sniffers using tools Colasoft Capsa Network Analyzer, EffeTech HTTP Sniffer, Packet Sniffer and PRTG Network Monitor.
9. Write a research paper in which Ethical Hacking tools are used to address any problem definition in cyber security.

DCS350: Capstone Project-1

Credits: 4

LTP:004

Course Description:

The course aims to equip the students with practical application of IT principles for designing, fabrication and testing of working models. The course includes SDLC, Project Management.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Describe the team working and team management.

CO2: Develop components & systems in isolation which meets a common goal.

CO3: Describe practical application of engineering principles for designing, fabrication and testing of working models.

CO4: Design a system, model, component or a process to meet desired/industrial/R&D needs.

Guidelines for Project

The project is considered as a steppingstone in implementing Major projects. Hence students should plan and organize their projects meticulously and necessary discussions and planning should be done so as to achieve this objective. The following guidelines should be adhered to:

1. Team size should preferably be two with a maximum limit of 3 members.
2. Individual projects may be permitted.
3. Projects should be purely internal in nature.
4. No restriction on tools/platform/language chosen should be made.
5. Students must ensure that they have to submit their synopsis of Project within 30 days from the start of the project.
6. Two interim reports (one after analysis and another after design) should be submitted to internal guides.
7. The number of records to be submitted is limited to team size + one (Departmental copy). Hard binding of reports is mandatory.
8. The report format guidelines used to document Projects should be followed for making the final report and evaluation will be made on the same grounds.

Evaluation of Project:

External Evaluation:

Criteria for external evaluation of Project, External evaluation is done by one external examiner appointed by the HOD/DEAN of the department. The following components are to be assessed for the End Semester external Evaluation of the Project:

Quality of documentation	20 marks.
Presentation of work	20 marks
Viva	20 marks
Total	**60 marks**

Internal Evaluation:

Criteria for internal evaluation of Project, Internal evaluation is be done by conducting a Viva by a team of evaluators comprising of the concerned guides and/or Head of the Department. The following are the components for internal evaluation of the Project:

Presentation of the work/Internal Viva	15 marks
Individual involvement & teamwork	10 marks
Attendance	5marks
Timely submission and assessment of 2 interim reports	10 marks
Total	**40 marks**

DCS360: Industrial Training

Credits: 4

Course Description:

The course aims to equip the students with a professional environment and/or style typical of a global IT industry.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Understand the team working and team management.

CO2: Learn how to develop components & systems in isolation which meets a common goal.

Course Contents:

Summer Professional Training is an important part of DCS course curriculum. It provides an opportunity to DCS students to write a winter training report on latest trends/technology related to cyber Security. Following are guidelines for winter training report writing and assessment:

General Instructions:

1. Winter training report should not be less than 25 pages.
2. Proper dress code is mandatory for presenting and attending summer training PPT presentations.
3. Attendance is compulsory for all students.
4. If a student is absent for his presentation as per schedule, he/she must assess later on with reduced weightage in the presentation assessment.
5. Always prepare a draft report first and print it out.
6. Read it yourself first and correct any typographical or grammatical errors.
7. One copy of final summer training report must be submitted as a spiraled report to the coordinator.

Main Components of a Report:

1. Cover page.
2. Abstract
3. Acknowledgement and declaration.
4. Certificate.
5. Table of contents/Index page.
6. Conclusions.
7. References.

Typing Instructions for Summer Training Report:

- Specification for Fonts:
- Font Face: Times new Romano.
- Font Size: As per following preview:
  - Headings (Size 16 Bold).
  - Sub-Heading (Size 14 Bold and Italic).
  - Contents (Size 12Normal)
  - Line spacing: 1.5.
  - Text Alignment: Both left and right justified.
- Page Dimensions: Standard A4 size (297mm x 210mm).
- Margins:
  - Top margin: 0.75”
  - Bottom margin: 0.75”
  - Left margin: 1”
  - Right margin: 0.75”
- Footer: Page number should be bottom centered.
- Sections should be numbered as for example,1. Introduction.

- Subsections should be numbered as for example,3.1 Simulation Toltec.
- Paragraphs and sentences should be short.
- Start of a paragraph should not be intended, rather, give one-line space between two paragraphs.
- A sub heading at the bottom of a page must have at least two full lines below it or else it should be carried over to the next page.
- The last word of any page should not be split using a hyphen.
- References:
    - Book titles must be in capitals.
    - Reference numbers should be marked liberally inside the text of the report-e.g., ...as given in [3].
    - References should either be in chronological order or in the order in which they appear in the text.

Evaluation of Professional Training

Evaluation:

Criteria for external evaluation of Professional Training, External evaluation is done by one external examiner from the department is appointed by the HOD/DEAN of the department. The following components are to be assessed for the End Semester external Evaluation of the Professional Training:

Training Report	40 marks.
PPT Content	30 marks
Viva	30 marks
Communication skills	25 marks
Query Handling	25 marks
Total	**100 marks**

SEMESTER IV

DCS401: Python with Cyber Security

Credits: 4

LTP:310

Course Description:

The course aims that the students can help to automate tasks across the cyberattack life cycle for both cyber attackers and defenders. This learning path demonstrates some of these applications and how Python can be used to make cybersecurity professionals more efficient and effective. This include the basic concept of python, data types file handling, socket programming.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Analyze systems for vulnerabilities and security flaws.

CO2: Use Python to build tools for security analysis.

CO3: Detect and analyze security threats to an application.

CO4: Generate the secure communication channels between client and servers.

UNIT-I

Introduction to Python: Introduction to code programming, Python installation, PyCharm IDE installation, Creating Project & Python Env configuration, Basic Syntax, String Formation & code Execution.

Loops: For Loops, over Lists, While Loops, Break & Continue Uses, Strings Manipulation, Combining Loops & Conditions.

UNIT-II

Data Types & Conditions: Variables with Different Data Types, User's Input, Operators, Comparative & Arithmetic, Type Casting, Condition's, logic and syntax, Dictionary, Tuple & lists, Nested Lists.

File System & Error handling: Try & Except, Exceptions Types, Error Handling, full Methodology, File Permissions - Create, Append, read & Write, OS System Module Functions.

UNIT-III

Function & code handling: Functions Structure & uses, Return Different Data Types, Parameters in Functions, Recursion Function and its uses, Scope & Global Keyword.

Web Fetching & Parsing: Web Communication library, Requests GET functions, Requests Sessions, Requests with Parameters, Requests Via Post, Beautiful Soup library, Filter & search with bs4, Extracting Data from Web

UNIT- IV

Network Communication: Introduction to SOCKET library, Creating Client Socket, Creating Server Socket, Sanding & Receiving Data, Set Echo Communication, Client Vs Server, Retrieving Data using OS Module.

Recommended Books / Suggested Readings:

1. Python: The complete reference, Martin C. Brown, McGraw Hill Education
2. Python Programming: An Introduction to Computer Science third edition by John M Zelle

DCS421: Python with Cyber Security LAB

Credits: 1

LTP: 002

Course Description:

The course aims to equip the students to familiarize with Python programming and learn how to use it to enhance the security policies and minimize the risk of exploitations. The course includes various cyber-attacks and security fundamentals.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Analyze the secure cyber network.

CO2: Identify and implement security policies for data exchange.

CO3: Implements various attacks to secure network.

List of experiments:

1. Implement the following Substitution & Transposition Techniques concepts:
    a) Caesar Cipher
    b) Rail fence row & Column Transformation
2. Implementation of Diffie Hellman key Exchange Algorithm
3. Implement the following Attack: a) Dictionary Attack b) Brute Force Attack
4. Installation of Wire shark, tcpdump, etc and observe data transferred in client server communication using UDP/TCP and identify the UDP/TCP datagram.
5. Installation of rootkits and study about the variety of options.
6. Perform an Experiment to Sniff Traffic using ARP Poisoning.
7. Demonstrate how to provide secure data storage, secure data transmission and for creating digital signatures.

DCS402: Web Application Security

Credit: 4

LTP: 400

Course Description:

The course aims to equip the students to familiarize with Web Application Security**.** This course includes web application security fundamentals.

Course Outcome (CO):

CO1: Identify the vulnerabilities in the web applications.

CO2: Identify the various types of threats and mitigation measures of web applications.

CO3: Apply the security principles in developing a reliable web application.

CO4: Use industry standard tools for web application security.

CO5: Apply penetration testing to improve the security of web applications.

UNIT-I

Overview of Web Applications: Introduction history of web applications interface ad structure benefits and drawbacks of web applications, Web application Vs Cloud application.

Web Application Security Fundamentals: Security Fundamentals, Input Validation - Attack Surface Reduction Rules of Thumb-Classi-fying and Prioritizing Threads.

UNIT-II

Browser Security Principles: Origin Policy - Exceptions to the Same-Origin Policy - Cross-Site Scripting and Cross-Site Request, Forgery - Reflected XSS - HTML Injection.

UNIT-III

Web Application Vulnerabilities: understanding vulnerabilities in traditional client server application and web applications, client state manipulation, cookie-based attacks, SQL injection, cross domain attack (XSS/XSRF/XSSI) http header injection. SSL vulnerabilities and testing - Proper encryption use in web application.

Web Application Mitigations: Http request, http response, rendering and events, html image tags, image tag security, issue, java script on error , Javascript timing , port scanning , remote scripting , running remotecode, frame and iframe , browser sandbox.

UNIT-IV

Secure website design : Architecture and Design Issues for Web Applications, Deployment Considerations Input Validation, Authentication, Authorization, Configuration Management ,Sensitive Data, Session Management, Cryptography, Parameter Manipulation, Exception Management, Auditing and Logging, Design Guidelines, Forms and validity, Technical implementation

Recommended Books / Suggested Readings:

1. Sullivan, Bryan, and Vincent Liu. Web Application Security, A Beginner's Guide. McGraw Hill Professional,2011.

2. Stuttard, Dafydd, and Marcus Pinto. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. John Wiley Sons, 2011

DCS403: Blockchain Technologies and Cryptocurrency

Credit: 3

LTP: 300

Course Objectives:

The course aims to equip the students will understand the methodology of blockchain and its application across industries. This course includes cryptography , blockchain and cryptocurrency concepts.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Outline and examine Cryptographic concept, Blockchain Technique and Distributed system.

CO2: Understand what Bitcoin is and how it works.

CO3: Create, develop, and implement applications based on Blockchain Technology.

CO4: Perform a transaction in bitcoin.

UNIT-I

Basics: Distributed Database, Two General Problem, Byzantine General problem and Fault Tolerance, Hadoop Distributed File System, Distributed Hash Table, ASIC resistance, Turing Complete.

Cryptography: Hash function, Digital Signature - ECDSA, Memory Hard Algorithm, Zero Knowledge Proof.

UNIT-II

Blockchain: Introduction, Advantage over conventional distributed database, Blockchain Network, Mining Mechanism, Distributed Consensus, Merkle Patricia Tree, Gas Limit, Transactions and Fee, Anonymity, Reward, Chain Policy, Life of Blockchain application, Soft & Hard Fork, Private and Public blockchain.

UNIT-III

Distributed Consensus: Nakamoto consensus, Proof of Work, Proof of Stake, Proof of Burn, Difficulty Level, Sybil Attack, Energy utilization and alternate.

Cryptocurrency: History, Distributed Ledger, Bitcoin protocols - Mining strategy and rewards, Ethereum-Construction, DAO, Smart Contract, GHOST, Vulnerability, Attacks, Sidechain, Namecoin.

UNIT-IV

Cryptocurrency Regulation: Stakeholders, Roots of Bit coin, Legal Aspects-Crypto currency Exchange, Black Market and Global Economy. Applications: Internet of Things, Medical Record Management System, Domain Name Service and future of Blockchain.

Recommended Books / Suggested Readings:

1. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder,
2. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press (July 19, 2016).
3. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies
4. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System
5. DR. Gavin Wood, “ETHEREUM: A Secure Decentralized Transaction Ledger,”Yellow paper.2014.
6. Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli, A survey of attacks on Ethereum smart contracts.

DCS404: Windows and Linux Forensic Analysis

Credits: 4

LTP: 400

Course Description:

The course aims to equip the students will understand both the operating systems, their file system, directories and so on. This course comprises of acquisition techniques, window registries, email forensic and Linux forensic

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Identify and analyze the different operating systems and their file system.

CO2: Identify evidence locations, including application execution, file access, data theft, external device usage.

CO3: Examine the individuals that how a system being used, who they communicated with, and files that were downloaded, modified, and deleted.

CO4: Analyze Windows/Linux event logs to answer critical questions.

UNIT-1

Introduction: Windows operating system components, key differences in modern windows operating systems, windows core forensic principles, Analysis focus, determining your scope, Creating and investigative plan for windows forensic,

Live response and triage-based acquisition techniques: Ram acquisition and following the order of volatility, Encryption detection, Registry and locked file extraction, Windows image mounting and examination, Ntfs, file system overview, Document and file metadata

UNIT-2

Registry analysis, application execution: - registry forensics in-depth, Registry core, Hives, keys, and values, Registry last write time, Mru lists, deleted registry key recovery, identify dirty registry hives and recover missing data, Rapidly search and timeline multiple registry hives

UNIT-3

Email forensics: Evidence of user communication, how email works, Email header examination, Email authenticity, Determining a sender, geographic location, Extended mapi headers. Host-based email forensics, Exchange recoverable items, Exchange and m365 evidence acquisition and mail export, Exchange and m365 compliance search and discovery, recovering data from google workspace users, Webmail acquisition, Email searching and examination

UNIT-IV

Linux: What is Linux, Overview of flavours (distributions), Key differences between Linux and Windows forensics, Linux concepts, privileges and permissions, Linux disk layouts and key directories, Navigating a Linux system and commonly used command line utilities, Understanding devices and disk mounting, Data collection from and using Linux systems, Capturing volatile data including RAM, Built-in forensic applications i.e dd for imaging and disk wiping, Overview of file system compatibility, ext2, 3 and 4, Ext file systems How disks are mapped and data stored, Problems associated with recovering data from ext file systems, System information from a forensic image, Log files, where to find them and nature of content, Devices connected and disks mounted & demounted, User accounts – identification, passwords and permissions, Introduction to memory analysis, User system navigation, execution and printing, Linux in Business - FTP servers, databases, mail, web-servers, Capturing and process for log file examination using Linux.

Recommended Books / Suggested Readings:

1. Digital Forensics with Kali Linux (Second Edition) by Shiva V.N. Parasram.
2. Linux Forensics by Philip Polstra.
3. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory by Michael Hale Ligh, Jamie Levy and Aaron Walters

DCS424: Windows and Linux Forensic Analysis Lab

Credits: 1

LTP: 002

Course Description:

The course aims to familiarize the students with various forensic techniques and they are able to analyze the various applications, cloud storage and memory of the system.

It includes various forencics like Email, Cloud Storage, Internet browsers

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Analyze the data images and system memories for searching any sort of data

CO2: Identify and analysis email policies and hardware of system.

CO3: Analysis various internet browsers.

List of Experiments:

1. Mounting Disk Images
2. Memory Carving with AXIOM
3. User Account and System Profiling
4. Application Execution Analysis
5. Cloud Storage Forensics – Onedrive, Google
6. LNK Shell Item Analysis
7. Jumplist and Shellbags Shell Item Analysis
8. USB Analysis
9. Email Forensics
10. Windows Timeline and Recycle Bin Analysis
11. Event Log Analysis
12. Automating Artifact Processing with KAPE
13. Chrome, Edge, Internet Explorer and Firefox Forensics
14. FOR500 Forensic Challenge

DCS405: Cyber Laws and IPR

Credits: 4

LTP: 400

Course Description:

The course aims to equip the students with understanding the definition and categories of the Cyber Laws and Indian IT Act. This course include computer ethics, IPR and its issues and IT acts (Indian).

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Discuss the law against cyber offense.

CO2: Define the issues related to computer ethics**,** investigate cybercrime and collect evidences.

CO3: Describe the fundamentals of intellectual property rights issues.

CO4: Identify about Indian IT act and International law**.**

Course Content

UNIT-I

Introduction: Basics of Law, Understanding Cyber Space, Defining Cyber Laws, Scope and Jurisprudence, Concept of Jurisdiction, Cyber Jurisdiction, Overview of Indian Legal System, Introduction to IT Act 2000, Amendments in IT Act, Cyber Laws of EU – USA – Australia - Britain, other specific Cyber laws.

UNIT-II

Computer Ethics, Privacy and Legislation: Computer ethics, moral and legal issues, descriptive and normative claims, Professional Ethics, code of ethics and professional conduct. Privacy, Computers and privacy issue, Digital Evidence Controls, Evidence Handling Procedures, Basics of Indian Evidence ACT, Legal Policies, legislative background.

UNIT-III

Intellectual Property Rights Issues: Copyrights, Jurisdiction Issues and Copyright Infringement, Multimedia and Copyright issues, WIPO, Intellectual Property Rights, Understanding Patents, Understanding Trademarks, Trademarks in Internet, Domain name registration, Software Piracy, Legal Issues in Cyber Contracts, Authorship, Document Forgery.

UNIT-IV

Indian IT Act and Standards: Indian IT ACT, Adjudication under Indian IT ACT, IT Service Management Concept, IT Audit standards, ISO/IEC 27000 Series, COBIT, HIPPA, SOX, System audit, Information security audit, ISMS, SoA (Statement of Applicability), BCP (Business Continuity Plan), DR (Disaster Recovery), RA (Risk Analysis/Assessment)

International Laws governing Cyber Space: Introduction to International Cyber Law, UNCITRAL, Cyber Laws: Legal Issues and Challenges in India, Net neutrality, Role of INTERPOL.

Recommended Books / Suggested Readings:

1. Deborah G Johnson, “Computer Ethics”
2. Cyber Law Simplified by Sood
3. Cyber frauds, cybercrimes & law in India by Pavan Duggal
4. The Internet Law of India: Indian Law Series by Shubham Sinha
5. Michael E. Whitman, Herbert J. Mattord, “Principles of Information Security”, Cengage Learning Pub., 2012.

DCS406: Cyber Security Threats

Credits: 3

LTP 300

Course Description:

The course aims to equip the students to provides the basic knowledge and skills in the fundamental theories and practices of Cyber Security. The course introduces concepts of Ethical Hacking, Cyber Laws and security threats.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Understand the broad set of technical, social & political aspects of Cyber Security.

CO2: Appreciate the vulnerabilities and threats posed by criminals, terrorist.

CO3: Understand ethics behind hacking and vulnerability disclosure.

CO4: Demonstrate a critical understanding of the Cyber law with respect to country like India.

Course Content

UNIT I

Introduction: cyber security, history of cyber security, cyber security goals, cyber security principles, cyber security technologies, Cyber Security standards, Cyber Security Tools, Cyber Security Challenges, Cyber Security Risk Analysis.

UNIT II

Hacking concepts: Hacking, Types of Hacking/Hackers, types of attacker, what is Cybercrime, Types of cybercrime, Classifications of Security attacks (Passive Attacks and Active Attacks) Essential Terminology (Threat, Vulnerability, Target of Evaluation, Attack, Exploit). Concept of ethical hacking, Phase of Ethical Hacking, Hacktivism, Sniffing tools.

UNIT III

Cyber Law: Cyber terrorism, Cyber laws, need of cyber laws, What offences are covered under these laws (Hacking, Data theft, Identity theft (including Password Theft), Email spoofing, Sending offensive messages, Voyeurism, Cyber terrorism), cyber laws of India, Punishment for cybercrime in India.

Password: About Password, Different types of password (Biometric, Pattern based Graphical password, Strong Password technique, Types of Password attacks.

Web Application Based Threats: Cross-site scripting, SQL injection, Command injection, Buffer overload, Directory traversal, Phishing scams, Zombies, Drive by downloads.

UNIT IV

Security Threats: Viruses, Worms, Trojan Horse, Bombs, Trapdoors, Spoofs, E-mail viruses, Macro viruses, Malicious Software, Network and Denial of Services Attack, Security Threats to E-Commerce-Electronic Payment System, e- Cash, Credit/Debit Card.

Stay Secure in digital World: How to stay secure in digital World, have strong password, encrypt your data, security suit software, firewall setup, update OS.

Recommended Books / Suggested Readings:

1. Certified Ethical Hacker Certification Exam by William Manning.
2. Fundamentals of Cyber Security by Mayank Bhushan, BPB Publications.
3. Pankaj Sharma. Information Security and Cyber Laws, Kataria, S. K., & Sons.
4. Charles P. Pfleeger, Shari Lawerance Pfleeger, “Analysing Computer Security”, Pearson Education India.
5. Dr. Surya Prakash Tripathi, Ritendra Goyal, Praveen Kumar Shukla,” Introduction to Information Security and Cyber Law” Willey Dreamtech Press.
6. Chander, Harish,” Cyber Laws and It Protection”, PHI Learning Private Limited, Delhi, India.

DCS450: Capstone Project-II

Credits: 4

LTP: 004

Course Description:

The course aims to equip the students to provide an opportunity to apply the knowledge gained through various courses in **Cyber Security**.

Course Outcomes (CO):

Upon successful completion of the course, the students should be able to:

CO1: Discuss the team working and team management.

CO2: Learn how to develop components & systems in isolation which meets a common goal.

Guidelines for Project

Hence students should plan and organize their projects meticulously and necessary discussions and planning should be done so as to achieve this objective. The following guidelines should be adhered to:

1. Group Size: Maximum 4, most preferably: 3.
2. Certificate should include the names of all members.
3. The report format guidelines used to document Major Projects should be followed for making the final report and evaluation will be made on the same grounds.

Typing Instructions for Project Report:

- Specification for Fonts:
- Font Face: Times new Romano.
- Font Size: As per following preview:
    - Headings (Size 16 Bold).
    - Sub-Heading (Size 14 Bold and Italic).
    - Contents (Size 12Normal)
    - Line spacing: 1.5.
    - Text Alignment: Both left and right justified.
- Page Dimensions: Standard A4 size (297mm x 210mm).
- Margins:
    - Top margin: 0.75”
    - Bottom margin: 0.75”
    - Left margin: 1”
    - Right margin: 0.75”
- Footer: Page number should be bottom centered.
- Sections should be numbered as for example,1. Introduction.
- Subsections should be numbered as for example,3.1 Simulation Toltec.
- Paragraphs and sentences should be short.
- Start of a paragraph should not be intended, rather, give one-line space between two paragraphs.
- A sub heading at the bottom of a page must have at least two full lines below it or else it should be carried over to the next page.
- The last word of any page should not be split using a hyphen.
- References:
    - Book titles must be in capitals.
    - Reference numbers should be marked liberally inside the text of the report-e.g., ...as given in [3].
    - References should either be in chronological order or in the order in which they appear in the text.

Evaluation of Project:

External Evaluation:

Criteria for external evaluation of Project, External evaluation is done by an external examiner appointed by the HOD/DEAN of the department. The following components are to be assessed for the End Semester External Evaluation of the Project:

Quality of documentation	20 marks.
Presentation of work	20 marks
Viva	20 marks
Total	**60 marks**

Internal Evaluation:

Criteria for internal evaluation of Project, Internal evaluation is be done by conducting a Viva by a team of evaluators comprising of the concerned guides and/or Head of the Department. The following are the components for internal evaluation of the Project:

Presentation of the work/Internal Viva	15 marks
Individual involvement & teamwork	20 marks
Attendance	5marks
Total	**40 marks**