Professional Diploma in Cyber Investigations and Laws

Regulations, Curriculum and Syllabus

(Applicable to the students admitted from Jan 2020 onwards)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SCHOOL OF COMPUTING SCIENCES

HINDUSTAN INSTITUTE OF TECHNOLOGY AND SCIENCE

Rajiv Gandhi Salai (OMR), Padur, Chennai – 603 103

1.1 Motto, Vision, Mission and Value Statement Objectives

MOTTO

"TO MAKE EVERY MAN A SUCCESS AND NO MAN A FAILURE"

VISION

To be an International Institute of Excellence, providing a conducive environment for education with a strong emphasis on innovation, quality, research and strategic partnership blended with values and commitment to society.

MISSION OF THE INSTITUTION:

- To create an ecosystem for learning and world class research.
- To instill highest ethical standards and values with a sense of professionalism.
- To take up activities for the development of society.
- To develop national and international collaboration and strategic partnership with industry and institutes of excellence.
- To enable graduates to become future leaders and innovators.

VALUE STATEMENT

Integrity, Innovation, Internationalization

1.2 Further the Institute always strives

- to train our students with the latest and the best in the rapidly changing fields of Engineering, Technology, Management, Science & Humanities.
- to develop the students with a global outlook possessing, state of the art skills, capable of taking up challenging responsibilities in the respective fields.
- to mould our students as citizens with moral, ethical and social values so as to fulfill their obligations to the nation and the society.
- to promote research in the field of Science, Humanities, Engineering, Technology and allied branches.

1.3 Aims and Objectives of the Institute are focused on

- Providing world class education in engineering, technology, applied sciences and management.
- Keeping pace with the ever changing technological scenario to help the students to gain proper direction to emerge as competent professionals fully aware of their commitment to the society and nation.
- To inculcate a flair for research, development and entrepreneurship.

2. Admission

2.1. The admission policy and procedure shall be decided from time to time by Academic Council, the Board of Management (BOM) of the Institute, following guidelines issued by Ministry of Human Resource Development (MHRD), UGC and AICTE.

2.2 Eligibility

Aspirants with Graduation from any stream with knowledge of computers.

OR

Aspirants with higher secondary and two years exposure in computer related work.

OR

Aspirants with higher secondary followed by a diploma and two years exposure in computer related work.

The term related is used in the context of network security, computer security, security administrator, network administrator, system administrator, Desktop administrator, web administrator, domain administrator, cyber investigator, police investigator etc.,

2.3. Enrollment Process

The filled applications shall be scrutinized by the admission committee. All applicable eligibility credentials are validated (Graduation, proof of employment, proof of experience as defined in eligibility criteria). A personal interview by a Panel of professionals will be carried out to evaluate the candidate, his knowledge of computers and understand the submitted credentials to complete the enrollment.

2.4. If at any time after admission, it is found that a candidate has not fulfilled any of the requirements stipulated by the Institute, the Institute may revoke the admission of the candidate with information to the Academic Council.

3. Structure of the programme

3.1. The structure of the programme shall have theory courses, practical course(s) and professional practices including project.

3.2. Duration

The duration of the professional diploma programme will be a minimum of 6 months. However a student may be permitted to complete the programme with additional 24 months as a maximum duration.

3.3 The academic programmes of the Institute follow the credit system.

- One credit for each lecture hour per week per semester;
- One credit for each tutorial hour per week per semester;
- One credit for each laboratory practical of two/three hours per week per semester.
- One credit for 4 weeks of industrial training and
- One credit for 4 hours of project per week per semester

3.4. Award of Professional Diploma

A student has to earn minimum credits specified in the curriculum of the relevant programme of study to award of Professional Diploma.

3.5. Medium of Study

The medium of instruction, examination and the language of the project reports will be English.

3.6 Faculty Advisor

To help the students in planning their courses of study and for getting general advice on the academic programme, the Department will assign a certain number of students to a faculty member who will be called their Faculty Advisor.

4. Discipline

4.1. Every student is required to observe discipline and decorous behaviour both in-side and outside the campus and not to indulge in any activity which will tend to bring down the prestige of the University.

4.2. Any act of indiscipline of a student reported to the Dean (E&T) will be referred to a Discipline Committee so constituted. The Committee will enquire into the charges and decide on a suitable punishment if the charges are substantiated. The committee will also authorize the Dean (E&T) to recommend to the Vice Chancellor the implementation of the decision. The student concerned may appeal to the Vice Chancellor whose decision will be final. The Dean (E&T) will report the action taken at the next meeting of the Council.

5. Attendance

5.1. A student whose attendance is less than 75% is not eligible to appear for the end – semester examinations for that semester. The details of all students who have less than 75% attendance in a course will be announced by the teacher in the class.

5.2. Those who have less than 75% attendance will be considered for condonation of shortage of attendance. However, a condonation of 10% in attendance will be given on medical reasons.

5.3 Application for condonation recommended by the Faculty Advisor, HOD, Dean is to be submitted to the attendance grievance committee, the committee, depending on the merits of the case, may permit the student to appear for the end semester examinations. Application for medical leave, supported by medical certificate with endorsement by a Registered Medical Officer, should reach the HOD within seven days after returning from leave or, on or before the last instructional day of the semester, whichever is earlier.

6. Assessment Procedure

6.1. The assessment for the theory course shall be assessed through the continuous basis as follows:

Test / Exam	Weightage	Duration of Test / Exam
First Periodical Test	10%	2 hours
Second Periodical Test	10%	2 hours
Third Periodical Test/ Model	20%	3 hours
Seminar/ Assignments/ Quiz	10%	
Attendance	10%	
End – semester Exam	50%	3 hours

6.2 The assessment for the practical courses shall be
(i) Weekly assignment/Observation note book / lab records – weightage 60%.
(ii) End semester examination of 3 hours duration including viva – weightage 40%.

6.3 Project Evaluation

The periodic review shall be conducted to assess the students' performance on the project work.

The Internal Continuous Assessment = 50%

End Semester Assessment = 50%

The end – semester examination will be conducted by a panel of examiners constituted by the Controller of Examination.

7. Declaration of results

7.1 A candidate who secures not less than 50% of total marks prescribed for a course with a minimum of 50% of the marks prescribed for the end semester examination and 50% marks in the continuous internal assessment shall be declared to have passed the course and earned the specified credits for the course.

7.2 If a candidate fails to secure a pass in a course due to not satisfying the minimum requirement in the end semester examination, he/she shall register and re-appear for the end semester examination during the following semester. However, the continuous internal marks secured by the candidate will be retained for all such attempts.

7.3 A candidate can apply for the revaluation of his/her end semester examination answer paper in a theory course within stipulated time from the declaration of the results, on payment of a prescribed fee through proper application to the Registrar/Controller of Examinations through the Head of the Department. The Registrar/ Controller of Examination will arrange for the revaluation and the results will be intimated to the candidate concerned through the Head of the Department. Revaluation is not permitted for practical courses and for project work.

8. Grading

8.1 A Grading system as below will be adhered to.

Range of Marks	Letter Grade	GP
100-95	S	10
85 - 94	A	09
75- 84	B	08
65-74	C	07
55-64	D	06
50-54	E	05
< 50	U	00

8.2 Grade Point Average

GPA is the ratio of the sum of the product of the number of credits C_i of course "i " and the grade points P_i earned for that course taken over all courses "i" registered by the student to the sum of C_i for all "i ". That is,

$$GPA = \frac{\sum_i C_i P_i}{\sum_i C_i}$$

8.3 Class/ Division

8.3.1 The Classification is based on CGPA and is as follows:

CGPA $\geq$ 8.0 : **First Class with distinction**

6.5 $\leq$ CGPA < 8.0: **First Class**

5.0 $\leq$ CGPA < 6.5 : **Second Class.**

8.3.2 Further, the award of 'First class with distinction' is subject to the candidate becoming eligible for the award of the degree having passed the examination in all the courses in his/her first appearance within the minimum duration of the programme.

9 Eligibility for the award of Professional Diploma

9.1 A student will be declared to be eligible for the award of the **Professional Diploma** if he/she has

i) registered and successfully acquired the credits for the courses;

ii) successfully acquired the credits in the different categories as specified in the curriculum corresponding to the discipline (branch) of his/her study within the stipulated time;

iii) has no dues to all sections of the Institute including Hostels, and

iv) has no disciplinary action pending against him/her.

The award of the degree must be recommended by the Academic Council and approved by the Board of Management of the University.

10. Power to modify

Notwithstanding all that has been stated above, the Academic Council shall modify any of the above regulations from time to time subject to approval by the Board of Management.

PROGRAMME EDUCATIONAL OBJECTIVES

1. To develop highly competent Professionals in Cyber Investigation and Laws and Engineering who are able to spearhead related ICT industries.
2. To encourage the Graduates to go for higher studies leading to excellent research contributions to the Society.
3. To train the Graduates to practice lifelong learning for continuing professional development.

PROGRAMME OUTCOME

1. Ability to acquire and apply fundamental principles of Cyber Security and Laws
2. Capability to communicate effectively.
3. Acquisition of technical competence in specialised areas of computing discipline.
4. Ability to identify, formulate and model problems and find engineering solutions based on a systematic approach.
5. Ability to conduct investigation and research on engineering problems in a chosen field of specialisation.

HINDUSTAN INSTITUTE OF TECHNOLOGY AND SCIENCE

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Professional Diploma in Cyber Investigations & Laws

CURRICULUM

Sl. No	Course Code	Course Title	L	T	P	C	TCH
SEMESTER I							
Theory							
1.	CSP201	Cyber Risk Management	3	0	0	3	3
2.	CSP202	Cyber Investigation Management	3	0	0	3	3
3	CSP203	Cyber Forensics	3	0	0	3	3
4.	CSP204	Cyber Laws	3	0	0	3	3
5.	CSP205	SIEM & Log trails	3	0	0	3	3
Practical							
6.	CSP231	Forensics and VA lab	0	0	2	2	2
7.	CSP232	Project	0	0	6	3	6
		Total Credits	**20 Credits**				

CSP201	Cyber RISK Management	L T P C 3 0 0 3
Goal	To introduce the principles of Cyber Risk management and expose the various techniques of Risk evaluation	

Objective:	Outcome :
• Understand the components of IT Systems • Understand the IT assets and Asset evaluation techniques • Understand the Threat modeling methods • Understand the elements of Risk assessment • Understand Business Continuity	• Differentiate the IT components • Apply Asset evaluation methods • Apply threat modelling methods • Apply the elements of Risk Assessment techniques • Apply business continuity components

Unit 1: IT Systems: Information Systems - System components - network components - Risk management - What is Risk - profile - identification -assessment -Analysis -Response - Tolerance - Risk types - inherent risk - control risk - audit risk. -Security risk analysis - Advantages

Unit 2: IT Assets: Assets management - Identify Assets - Asset classification - Asset valuation - Binary Asset Valuation -Rank-Based Asset Valuation - Consensus Asset Valuation - Classification-Based Asset Valuation - others

Unit 3: Cyber Threat: Threat management - Identifying Threats -Threat model - Threat attributes - Attack tree - STRIDE - DREAD - OCTAVE - CAPEC- Threat Statements- Technical Threats and Safeguards - Physical Threats and Safeguard - Human Threats to Physical Security - The RIIOT Method: Physical Data Gathering - Test Physical Security Safeguard.

Unit 4: Risk Assessment: Security Risk Assessment - Quantitative vs. Qualitative Analysis - Determining Risk - Creating Risk Statement - Security Risk Mitigation - Selecting Safeguard - Security Risk Assessment Reports - Report Structure.

Unit 5: Business Continuity: Principles of Business continuity - Business Interruption Events – Business impact assessment – fire exposure analysis – functional analysis –compliance issues – Pre-Planning - Initial Response - Recovery - Identification of Recovery environment - Identification of Recovery Point - site and structures – Equipment and technology – documents and records electronic equipment and process equipment - Business continuity plans – crisis management plans –function restoration plans – disaster recovery plans – Incident Response Plan

Text Book

1. Thomas L Norman., Risk analysis and Security counter measure selection , CRC press, 2010
2. Ariel Evans, Managing Cyber Risk, Routledge, 2019
3. Lee T Ostrom, Risk Assessment: Tools, Techniques, and Their Applications, Wiley 2019
4. Christopher Hodson,, Cyber Risk Management: Prioritize Threats, Identify Vulnerabilities and Apply Controls, Kogan, 2019
5. Richard.E Cascarino., Auditors guide to information system auditing, John Wiley and Sons, 2007.

CSP202	Cyber Investigation Management	L T P C 3 0 0 3
Goal	Introduce the concept of Cyber investigation and prepare the individual for cyber investigation profiles	

Objective:	Outcome :
• Understand the basics of Cyber Investigation • Understand the concepts of Profiling • Understand the concepts of Crime Scene Management • Understand the evidence types and management needs • Define the Case management needs	• Differentiate between Investigation and cyber investigation • List the profiling traits • Working knowledge on Intrusion investigation • Manage evidences • Manage Case and address the requirements

Unit 1: Investigation: Concepts of Investigation - types of investigation - Digital Investigation – Intrusion investigation – Criminal investigation – forensic investigation – Network investigation - Observation skills - the investigate process – Investigation Unit - Role of investigator – Electronic Discovery – Hypothesis creation - Legal Context - Professional Ethics: Characteristics - system of professions - code of ethics and professional conduct.

Unit 2: Cyber Investigation : Warrant – Types of warrant - Search warrant - concept of search – home search – computer search - cyber investigation - Network Investigation - Investigating audit logs - Investigating Web attacks - Investigating Computer Intrusions - Profiling - criminal profiling - deviant behaviour - Motive - stylometric

Unit 3: Cyber Crime Scene: Elements of a cyber-case – Scene of cyber-crime - Surveying and preserving digital crime scene – Crime Scene Photography - Chain of custody –challenges – Admissibility.

Unit 4: Evidence Management: Evidence – Digital Evidence - Types of evidence – physical evidence – real evidence – circumstantial evidence – network evidence- digital evidence– Evidence collection – Evidence Analysis - Contextual Information – Timing - Evidence Management –- Investigative Reconstruction with Digital Evidence. - The Process of Elimination - Tools

Unit 5 Case Management : case life cycle - Identification of a cyber-crime –code of criminal procedure - Jurisdiction –types of jurisdiction – Handling a Digital Crime Scene - Cyber Crime Case filing procedures – Lodging a complaint – Registering case - Filing F.I.R. – Contents of F.I.R - Tracking of FIR - correlation & corroboration - Cyber Crime in Court - Role of court appointed experts.

Text Book

1. Rory J McMahon, Practical handbook for Private investigators, CRC, 2nd Ed 2007
2. Christopher, L.T. Brown, Computer Evidence Collection and Preservation, Cengage, 2010
3. Tom Bazley, Investigating White collar crime, Pearson 2008
4. H.K.Saharay, Law of Evidence, Eastern Law House, 2008

Reference

1. Bruce Middleton, Cyber Crime Investigators Field Guide, Auerbach,2002
2. Thomas A Johnson, Forensic Computer Crime Investigation, CRC, 2005
3. Barry A.J. Fisher, Techniques of Crime Scene Investigation, CRC, 2004
4. Peter Stephenson, Investigating Computer Related Crime A handbook for Corporate Investigators, CRC 2000
5. Gerald R McMenamin, Forensic Linguistics Advances in Forensic stylistics, CRC,2002

CSP203	Cyber Forensics	L T P C 3 0 0 3
Goal	To introduce concepts of cybercrime and Cyber Forensics with a focus on disk forensics network forensics and software forensics	

Objective:	Outcome :
• Understand the types of Cyber Crime • Understand the Disk Forensics • Understand the Software Forensics • Understand the Network Forensics	• Differentiate the types of Cyber Crimes • Apply the Disk Forensics • Apply the Software Forensics • Apply the Network Forensics

Unit I: Cyber Crime: Cyber world - Data - Information – cyber threat - cybercrime – White collar crimes – economic offense – cyber stalking - cyber extortion – insider threat - Hacker - types– cyber terrorism - cyber espionage - cyber warfare -weapons - Professional Ethics: Characteristics - system of professions - computing profession - professional relationships - code of ethics and professional conduct - Ethical dilemmas – Ethical decision making - Cyber Forensic Evidence Management

Unit II : Types of Cyber Crime: Data frauds - data diddling - scavenging - data theft - data leakage – data hiding - Information theft – cybersquatting - Id theft - Password theft – key logger - Child Pornography - obscene messages - Job Racketing - Marketing and Advertisement Rackets - Nigerian frauds- pay per click scams – web defacement - Accounting Frauds - Fraud Schemes - ATM frauds - credit, debit card crimes - Card Cloning - salami techniques - IP spoofing - email & ip address – Telecommunication Fraud - Software piracy

Unit 3: Disk Forensics : Digital data – digital device – Hard disk – Types – Disk characteristics – SSD - File systems - NTFS – MFT Structure - fragmentation -MFT fragmentation – Files and attributes - File hashing - Slack space – Disk Forensics tools - Win Hex – Disk imaging – write blockers – types of blockers - Data Carving – techniques - Scalpel - Registry Forensics - Registry – registry data types –RegEdit -concept of timeline – Anti forensics.

Unit 4: Software Forensics : Volatile Live Vs Offline Forensics - Artefacts - System Information - Linux ~ Windows – System commands - Network information – Network commands - proc file system - Software Program - source code - types of software - Source code repository - software license - commercial piracy - soft lifting - structures & versions - Analysis Tools - Objects of analysis - Obfuscation – code Obfuscation - Stylometric - author characteristics - Software Forensic challenges – Principles of Steganography

Unit 5: Network Forensics: Network components - Port scans – SYN flood -Key Loggers - Email Forensics - email spoofing – Phishing – mail header analysis - Network protocols – Protocols Susceptible to Sniffing - Active and Passive Sniffing - Wireshark – Capture and Display Filters - pcap analysis – Problems - Trojans and Backdoors, Overt and Covert Channels, Types of Trojans - Botnets - types of botnet- Structure of bots – Crime bots - Spamming bots - DoS – DDoS Attacks – types - Honey Pots - Forensic evidences.

Text Books

1. Dejey, Cyber forensics, Oxford, 2018
2. Gerard Johanses, Digital forensics and incident response, 2017
3. Harlon Carvey, Windows Registry forensics, Syngress, 2011
4. Sherri Davidoff et al, Network forensics, Prentice Hall, 2012
5. Albert J Marcella, et al, Cyber forensics, 2nd edition, Auerbach, 2008
6. George Mohay et al, Computer and intrusion forensics, Artech house, 2003
7. Mani , legal Framework on Cyber Crimes Lawmann's, Kamal Publishers, New Delhi, 2011
8. Tommie Singleton, Fraud Auditing and Forensic Accounting, John Wiley, 3rd Ed, 2006

CSP204	Cyber Laws	L T P C 3 0 0 3
Goal	To enable a prospective student to understand the various types of cybercrime, tools and associated legal implications.	

Objective:	**Outcome :**
• Understand the concept of cyber crime • Understand & differentiate types of cyber crime • Understand network crime and techniques • Understand IT ACT and role • Correlate IT ACT with related acts	• Differentiate the various types of cyber crime • Differentiate the various types of virus and BOTS and their crime ware capabilities • Differentiate the various elements of IT act and related amendments • IT acts influence on Related acts

Unit 1 CrPC: Constitution of criminal courts - power of courts - arrest of persons - process to compel appearance - summons - warrant of arrest - summons to product - search warrants - general provisions relating to search - maintenance of public order - jurisdictions of criminal courts - conditions requisite for initiating of proceedings - complaints to magistrates - charge - trial -evidence in inquiries and trials - transfer of cases - provisions of bails and bonds

Unit 2 IT Act-Digital Signature: Information Technology Act 2000 – Digital signature - Electronic Governance - Secure electronic records - Regulation of certifying authorities - Electronic signature certificates - Penalties compensation –

Unit-3: IT Act- Offences: Adjudication - Offenses - Examiner of electronic evidence - Amended IT Act - Provisions of other Acts amended by I.T. Act

Unit 4 Intellectual Property: Intellectual Property - Types of IP - Copyright Act – Ownership – Duration Registration - Originality of Material - Fixation of Material - Exclusions from Copyright Protection - Compilations – Collections - Derivative Works. Patents: Patents Act - Patentability - Design Patents - Double Patenting - Direct Infringement - Inducement to Infringe - Contributory Infringement.

Unit 5 Trade Mark act: Trademark classes - What can be trademarked - Trademark Registration Process - Post-registration Procedures- Legal rights - obligations - infringement of trade mark - trade marking cyber world - trade mark and website registration - case studies

Text book

1. V.K.Ahuja, Law relating to Intellectual Property rights. LexisNexis, 2017
2. V.K.Ahuja, Intellectual Property rights in India. Vol 1 and Vol 2 LexisNexis, 2009

Reference

3. N.R.Subbaram, Demystifying Intellectual Property Rights, LexisNexis, 2009
4. Deepak Gogia, Intellectual Property Law, Ashoka Law House, 2010

CSP205	SIEM AND LOG TRAILS	L T P C 3 0 0 3
Goal	To expose the learner on the relevance of various types of Logs generated from different systems and expose the concept of SIEM which is used for Log correlation and alerts	

Objective:	**Outcome :**
• Understand the relevance of MIB and RMON • Understand the Concept of Log formats and log correlation • Understand the relevance and working of Syslog server • Understand the relevance and working of SNORT	• Differentiate the MIBs, OIDs and RMON capabilities • Differentiate the Log formats • Understand the configurations of Syslog server • Understand SNORT configuration and SNORT rules.

Unit 1: Introduction: Concepts of Log, What Should the Logs Log? Everything - The 5 Ws (Who, What, When, Where, and Why) - Unix Logs – Windows Logs - Events and Event Lifecycle - Linux Logs - Types of logs - Security logs - Application logs – System Logs – WMI – WMI Architecture

Unit 2: SNMP: Simple Network Management Protocol – Structure – Basic commands – get get next,…Management Information Base (MIB) – V1, V2 and V3, RMON - OID notation - OID Trees - SNMP Tools, Case Studies

Unit 3: Log Formats And Log Collection: Log files – Log formats – application specific Log Formats -Apache Logs - Mail logs - Firewall Logs – vendor Specific Logs - Event Correlation - Event Normalization, Correlation Rules Log Collection - Push Log Collection - Pull Log Collection - Prebuilt Log Collection - Custom Log - Parsing/Normalization of Logs - Rule Engine/Correlation Engine - Correlation Engine, Case Studies

Unit 4: Managing Log Files: Log tools – SYSLOG – Open source Log analyzers - Log File Conversion -Standardizing Log Formats - Using XML for Reporting -Correlating Log File Data -Log Rotation and Archival -Determining an Archiving Methodology -Separating Logs, Case Studies

Unit 5: Investigating Intrusions: Intrusion detection system - NIDS, HIDS - Locating Intrusions - Monitoring Logons - Monitoring IIS - Reconstructing Intrusions – concepts of SNORT - Rules - Rule headers - Rule options - Pre- processors - Stream4 - Frag2 - Frag3 - HTTP inspect - plugins - Alerts Detail Report, Case Studies.

TEXT BOOKS

1. David Miller, Security Information and Event Management (SIEM) Implementation, McGraw-Hill, 2010
2. Client P Garrison, Digital forensics for network internet and cloud computing, , Elsevier, 2010
3. Jacob Babbin et al, Security Log Management-Identifying patterns in chaos, Syngress, 2006
4. Vivek Chopra, et al, Professional Apache Tomcat, Wrox, 2004

5. Gabriele Giuseppini, et al, Microsoft Log Parser Toolkit, Syngress, 2004
6. Toby Kohlenberg, Snort IDS and IPS toolkit, Syngress, 2007
7. Al-Sakib Khan Pathan, The State of the Art in Intrusion Prevention and Detection, CRC 2014
8. John R.Vacca, Scott Ellis, Firewalls Jumpstart for Network and Systems Administrators, Elsevier,2005.

CSP231	FORENSICS and VA LAB	L T P C 0 0 2 2
Goal	To understand the use of tools to manage forensics and system and application level vulnerability	

Objective:	Outcome :
1. Understand the technique of collecting live forensic information 2. Understand the use of disk forensic tools 3. Understand the use of mobile forensic tools 4. Understand the use of Network forensic tools	1.Exhibit live forensic data collection 2.Exhibit the use of disk forensic tool to collect and manage evidence 3.Exhibit SIM data collection techniques 4. Use network tools to collect VA and exploits data

1. Use NMAP as your tool and try out the various scan types with different flag combinations. With a single IP address and multiple IP address combinations.

2. Load a single IP address in Nessus and carry out a light scan, and intensive scan of the IP address. Generate the reports for both types of SCAN. Compare the scan and generate a report on the observed changes. Extend the exercise for a range of addresses in Nessus and repeat the light scan, and intensive scan of the identified machines. Generate the reports for both types of SCAN. Compare the scan and generate a report on the observed changes. Also list out the block range of Filters available for SCAN as a part of your report

3. Load a single IP address in OPENVAS and carry out a light scan, and intensive scan of the IP address. Generate the reports for both types of SCAN. Compare the scan and generate a report on the observed changes. Extend the exercise for a range of IP addresses in OPENVAS and repeat the light scan, and intensive scan of the IP address. Generate the reports for both types of SCAN. Compare the scan and generate a report on the observed changes. Also list out the block range of Filters available for SCAN as a part of your report.

4. Use the password cracker tool (**SALT** or equivalent) and with a given encrypted / or shadowed password file, try to identify the username and the respective passwords.

5. Using Wireshark as a tool capture the network traffic and reconstruct the data flowing through the network for an Identified HTTP traffic.

6. Using Wireshark as a tool, load an captured pcap file and analyse the same with respect to given problem. Isolate the evidences from the captured traffic file, construct a forensic report describing the incidents in a time line view.

7. Live Forensics: Identify the following details from the target machine using live analysis tool. List loaded programs, List current network connections, List running processes, List open share files, list of routing table entries, list of ARP entries.

8. Using Nikto as a web application analysis tool, scan a given website for web vulnerabilities at the web server level and the application level

9. Using Wapiti as a web application analysis tool scan a given website for web vulnerabilities at the web server level and the application level

10. For a given email header, carry out the header analysis, identify the domains, and reconstruct the mail traffic flow from the sender to the receiver. Differentiate between internal and external IP addresses if available in the header and try to reconstruct the network.

11. In a given machine Identifiy the list of visited websites with respect to Internet explorer and Firefox. Generate the output as a timeline entry. Mark observed deviations in browsing based on the timeline and describe the person's activity at that point in time.

12. Take a USB stick which has a few jpeg images. Delete a few JPEG images. and create an disk image of USB. Mount the disk image and using Scalpel tool retrieve the deleted images.

13. With a sample apache attack log, analyse the shared log and try to identify the attacker along with the steps in identifying the method of entry.

14. For the given Asset inventory, identify the threat and risk matrix and hence calculate the exposure risk for the shared assets. Propose a risk mitigation plan.

15. With the given windows system, use a suitable disk explorer tool and identify the directory structure and windows specific hidden file locations especially, the event and security log entry locations and system32 locations with file size entries,

16. With the given windows system, identify the various registry entries and generate a report on the current configuration and current user permissions. With the given configuration and the permissions, try to reconstruct the users, and their privileges.

17. **Demonstration only**: Load a SIM card and analyze the various folders available as a part of the SIM.

<table>
<tr><td>CSP232</td><td>Project</td><td rowspan="2">L T P C
0 0 6 3</td></tr>
<tr><td>Goal</td><td colspan="2">Develop the mini project by using Cyber Forensics Techniques</td></tr>
<tr><td colspan="2">Objective:
• Develop a mini project using Cyber Forensics Techniques and Cyber Laws</td><td>Outcome :
• Ability to Design a mini project using Cyber Forensics techniques and Cyber Laws</td></tr>
</table>