Source book for
Certificate Course in Ethical Hacking and Information Security

1. **Course Objective:** This course is aimed to provide skills on security programming which will help the students who want to make carrier in security domain.

2. **Eligibility Criteria:** Any Engineering /Science graduate with mathematics up to 10+2 level

3. **Prerequisite:** Candidate should have knowledge of computer & networking fundamentals and Basic Computer Programming with OOPs concepts

4. **Teaching Schema: (Tabular format)**

Sl. No.	Modules	Hours
1	Java Programming with Crypto API	80
2	Application Security	70
3	Ethical Hacking	70
4	Management Development Program	60
5	Project	40
	Total	**320**

5. **Suggested Schedule**

Suggested Schedule for Certificate in Ethical Hacking and Information Security		
Week	**Session 1**	**Session 2**
1	**Java Programming with Crypto API(80 Hrs)**	
2	Java Programming with Crypto API	
3	Java Programming with Crypto API	**Application Security (70Hrs)**
4	Application Security	
5	Application Security	**Ethical Hacking (70 Hrs)**
6	Application Security	Ethical Hacking
7	Ethical Hacking	
8	Ethical Hacking	**Management Development Program(60hrs)**
9	Management Development Program	
10	Management Development Program	**Project(40 Hrs)**
11	**Exam Break & Course End Exam**	
12	**Project**	**Project Evaluation &Course End Re-Exam**

Note: 30 hrs of training will be considered in one week

6. **Session wise Breakup:**

Note: Each single session is of two hours duration for all subjects mentioned below and consider T as Theory and L as lab.

Java Programming with Crypto API(40 T + 40 L hrs)

Session 1:

- Java Language and its features
- The Java Language –
- Data types, Variables, Constants, operators, Control Statements (if, for, while, switch etc.)
- Classes in java
- Constructors, finalize, instance data and methods, the new operator
- Methods, overloading, parameter passing, objects as parameters
- Memory management, garbage collection
- The this facility, static data and methods, block, scope, lifetime
- JDK and its usage (Java Compiler, Java Runtime, Java Debugger, Java doc)
- Difference between applications and applets
- The first Java Program

Session 2:

- Inner classes, Abstract Classes & wrapper classes.
- Interfaces
- Packages
- Access Control Rules

Session 3:

- Exception Handling
- Exceptions as objects,
- Exception hierarchy
- Try, catch and finally
- Different exception classes

Session 4:

- The java. Lang package, Object, Number, Math, System
- The String class
- The java.util Package
- Arrays, Vectors, Stack, Hash table, Dictionary, Property

Session 5:

- The Java Collection Framework
- Multithreaded programming in Java
- Multithreading: advantages and issues
- The Thread class, thread groups

- The Run able interface
- Thread synchronization
- Inter-Thread communication

Session 6:

- The java.io Package
- Files
- Byte Streams and Unicode Character Streams
- Persistence of objects
- Object Serialization Methods

Session 7:

- Introduction to Java Network Programming
- URL
- Inet Address
- Socket, and ServerSocket
- DatagramPocket
- DatagramSocket

Session 8:

- Remote Method Invocation
- The java.rmi package
- The Remote interface
- The UnicastRemoteObject and Naming classes
- Stub, rmic, rmiregistry

Session 9 & 10:

- Servlets : Dynamic Content Generation
- Advantages of Servlets over CGI
- The Servlet interface
- The HttpServlet, HttpServletRequest, HttpServletResponse classes
- Exception Handling

Session 11:

- Session
- Session Management
- Session Tracking with
- Cookies
- HttpSession
- Request Dispatcher

Session 12 & 13:

- JSP: Separating UI from Content generation code
- MVC architecture
- Life cycle of a JSP page
- Directives, Implicit and Explicit Objects, Scriptlets, Expressions, Expression Language

Session 14:

- Scope
- JSP Error Page handling
- Session Tracking
- JSP Using JavaBeans
- Custom Actions and Tag Libraries in JSP
- Java Server Pages Standard Tag Library

Session 15:

- Introduction to security and cryptography
- Java cryptography Architecture
- Security Protocols
- SSL and TLS

Session 16:

- Encryption and Decryption
- A basics of SSL client and Server
- Client side Authentication

Session 17:

- Managing SSL Session Information
- Dealing with HTTPS

Session 18:

- Handling Denial of Service
- Injection and Inclusion

Session 19:

- Buffer Overflows and Input Validation
- Access Control

Session 20:

- Jquery & Authentication Bypass

Assignments:

- Get yourself acquainted with java environment. Build a class Emp, which contains details about the employee and compile and run its instance.
- Create an inner class for a manager, which contains information about the manager. Use the appropriate interfaces. Create an anonymous inner class for Tech. Members using the Session one assignment
- Create an appropriate data structures to store your employee object and use the java.util.package properties.
- Create a user defined exception to check whether your employee exist in your data structure and using the catch and finally block. Redeem an appropriate solution.
- Using the collection framework define an appropriate interface to your above application
- Using Multi-Threading create objects in java E.g. Create a clock & synchronize your application.
- Write a multithreaded chat server and a GUI client.
- Write an RMI server that returns a Result object to your RMI client application. He GUI client sends a roll number to the server and the server looks up a database table for the

students' details (name, marks, rank etc) and passes a Result object to the client encompassing all these info.
- Implement exception handling in Servlet.
- Use Java Servlets technology in designing and implementing an Air Ticket reservation system. Incorporate Sessions in the Air Ticket reservation system.
- Separate UI code from the controller code in your Air Ticket reservation system by incorporating JSP and Servlets.

Application Security(30 T + 40 L Hrs)

Session 1:
- Introduction to MYSQL
- Installing and Configuring MYSQL

Session 2:
- Creating and Dropping Database
- Queries in MYSQL

Session 3:
- Web Application Security Risks
- Identifying the Application Security Risks

Session 4:
- Data Extraction
- Advanced Identification/Exploitation

Session 5:
- Other HTTP fields
- Injection in stored procedures

Session 6 :
- Threat Risk Modelling
- OWASP Top 10

Session 7:
- Denial of Service
- Injection and Inclusion
- Buffer Overflows and Input Validation
- Access Control

Session 8:
- Cross site scripting
- Case Study On Web Application Framework

Session 9:
- Installing Python
- Your First Python Program
- Declaring Functions
- What's an Object?
- Indenting Code
- Testing Modules
- Native Data types

Session 10:
- Introducing Dictionaries

- Defining Dictionaries
- Modifying Dictionaries
- Deleting Items From Dictionaries
- Files
- Introducing Lists
- Defining Lists
- Adding Elements to Lists
- Searching Lists
- Deleting List Elements
- Using List Operators

Session 11:

- Introducing Tuples
- Declaring variables
- Referencing Variables
- Assigning Multiple Values at Once
- Formatting Strings
- Mapping Lists
- Joining Lists and Splitting Strings
- Historical Note on String Methods

Session 12:

- Using Optional and Named Arguments
- Using type, str, dir, and Other Built-In Functions
- Object References
- Socket with Python

Session 13:

- Regular Expressions Using python
- Functions and Functional Programming
- Object Oriented Linux Environment
- Classes, Objects and OOPS concepts

Session 14:

- File Handling
- Directory Access Permissions
- Controls Socket
- Libraries and Functionality Programming
- Servers and Clients Arch
- Web Servers and Client scripting
- Introduction to Python web development framework

Session 15:

- Libraries and Functionality Programming
- Servers and Clients Arch
- Web Servers and Client scripting
- Exploit Development techniques
- Writing plugins in Python
- Exploit analysis Automation Process
- Debugging basics

Assignments:

1. Write a function *translate()* that will translate a text into "*rövarspråket*" (Swedish for "robber's language"). That is, double every consonant and place an occurrence of "o" in between. For example, translate("this is fun") should return the string "tothohisos isos fofunon".

2. Define a function *overlapping()* that takes two lists and returns True if they have at least one member in common, False otherwise.

3. Define a procedure *histogram()* that takes a list of integers and prints a histogram to the screen. For example, histogram([4, 9, 7]) should print the following:

```
****
*********
*******
```

4. Write a function *find_longest_word()* that takes a list of words and returns the length of the longest one.

5. Write a function *filter_long_words()* that takes a list of words and an integer *n* and returns the list of words that are longer than *n*

6. Write a version of a palindrome recognizer that also accepts phrase palindromes such as "*Go hang a salami I'm a lasagna hog.*", "*Was it a rat I saw?*", "*Step on no pets*", "*Sit on a potato pan, Otis*", "*Lisa Bonet ate no basil*", "*Satan, oscillate my metallic sonatas*", "*I roamed under it as a tired nude Maori*", "*Rise to vote sir*", or the exclamation "*Dammit, I'm mad!*". Note that punctuation, capitalization, and spacing are usually ignored.

7. A pangram is a sentence that contains all the letters of the English alphabet at least once, for example: *The quick brown fox jumps over the lazy dog*. Your task here is to write a function to check a sentence to see if it is a pangram or not.

8. In cryptography, a Caesar cipher is a very simple encryption techniques in which each letter in the plain text is replaced by a letter some fixed number of positions down the alphabet. For example, with a shift of 3, A would be replaced by D, B would become E, and so on. The method is named after Julius Caesar, who used it to communicate with his generals. ROT-13 ("rotate by 13 places") is a widely used example of a Caesar cipher where the shift is 13. In Python, the key for ROT-13 may be represented by means of the following dictionary:

```
key = {'a':'n', 'b':'o', 'c':'p', 'd':'q', 'e':'r', 'f':'s', 'g':'t', 'h':'u', 'i':'v', 'j':'w', 'k':'x', 'l':'y', 'm':'z', 'n':'a',
                    'o':'b', 'p':'c', 'q':'d', 'r':'e', 's':'f', 't':'g', 'u':'h', 'v':'i', 'w':'j', 'x':'k', 'y':'l', 'z':'m', 'A':'N',
                    'B':'O', 'C':'P', 'D':'Q', 'E':'R', 'F':'S', 'G':'T', 'H':'U', 'I':'V', 'J':'W', 'K':'X', 'L':'Y',
                    'M':'Z', 'N':'A',          'O':'B', 'P':'C', 'Q':'D', 'R':'E', 'S':'F', 'T':'G', 'U':'H', 'V':'I',
                    'W':'J', 'X':'K', 'Y':'L', 'Z':'M'}
```

Your task in this exercise is to implement an encoder/decoder of ROT-13. Once you're done, you will be able to read the following secret message:

Pnrfne pvcure? V zhpu cersre Pnrfne fnynq!

Note that since English has 26 characters, your ROT-13 program will be able to both encode and decode texts written in English.

9. Define a simple "spelling correction" function ***correct()*** that takes a string and sees to it that
   1) two or more occurrences of the space character is compressed into one, and
   2) inserts an extra space after a period if the period is directly followed by a letter.
   E.g. correct("*This is very funny and cool.Indeed!")* should return "*This is very funny and cool. Indeed!*"
10. In English, the present participle is formed by adding the suffix -ing to the infinite form: go -> going. A simple set of heuristic rules can be given as follows:

    - If the verb ends in ***e***, drop the ***e*** and add ***ing*** (if not exception: be, see, flee, knee, etc.)
    - If the verb ends in ***ie***, change ***ie*** to ***y*** and add ***ing***
    - For words consisting of consonant-vowel-consonant, double the final letter before adding ***ing***
    - By default just add ***ing***

    Your task in this exercise is to define a function ***make_ing_form()*** which given a verb in infinitive form returns its present participle form. Test your function with words such as lie, see, move and hug. However, you must not expect such simple rules to work for all cases.

Ethical Hacking(32 T + 38L Hrs)

Session 1:

- Security Management Concepts & Principles
- Human side of Information Security's
- Threats of Information System
- Threats and attacks
- Classification of Threads and attacks

Session 2:

- Protecting Information System Security
- Security in Mobile and Wireless Computing
- Credit card frauds in mobile and wireless Computing
- Information Security Management
- Fundamentals of Information Security

Session 3:

- Introduction to Ethical Hacking
- Understanding Ethical Hacking Terminology
- Identifying Different Types of Hacking Technologies
- Understanding the Different Phase Involved in Ethical Hacking

Session 4:

- Types of Hacker Classes
- Ethical Hackers and Crackers
- Goals of Attackers
- Security, Functionality And Ease of Use Triangle
- Defining the Skills Required to become an Ethical Hacker

Session 5:

- How to Conduct Ethical Hacking
- Creating a Security Evaluation Plan
- Types of Ethical Hacks
- Foot-printing and Social Engineering
- Understand How Traceroute Is Used in Foot-printing
- Define the Terms Port Scanning, Network Scanning and Vulnerability Scanning
- Understand various Scanning Methodologies
- SYN, Stealth, XMAS, NULL, IDLE and FIN Scans

Session 6:

- TCP Communication Flag Types
- Banner Grabbing and OS Fingerprinting Techniques
- How Proxy servers are used in launching an Attack?
- Http tunneling Techniques
- IP Spoofing Techniques
- Enumeration
- Password-cracking Techniques
- Cracking Windows Passwords
- Redirecting the SMB Logon to the attackers
- SMB Redirection, SMB Relay MITM Attacks and Countermeasures
- NetBIOS DOS Attacks
- DDos Attack

Session 7:

- Password-Cracking Countermeasures
- Active/Passive online Attacks
- Offline Attacks
- Keyloggers and other Spyware Technologies
- Trojans and Backdoors
- Overt and Covert Channels
- Types of Trojans
- Reverse-connecting Trojans
- Netcat Trojan
- Indications of a Trojan Attacks

Session 8:

- Wrapping
- Trojan Construction Kit and Trojan Makers
- The countermeasure Techniques in Preventing Trojans
- Trojan-Evading techniques
- System File Verification

Session 9:

- Difference between a Virus and a Worm
- Types of Viruses
- Antivirus Evasion Techniques
- Virus Detection Methods

Session 10:

- Protocols Susceptible to Sniffing
- Active and Passive Sniffing
- ARP Poisoning
- Ethereal Capture and Display Filters
- MAC Flooding
- DNS Spoofing Techniques
- Describe Sniffing Countermeasures

Session 11:

- Types of DOS Attacks
- How DDos Attacks Work
- How BOTs/BOTNETs work
- Smurf Attacks
- SYN Flooding
- Spoofing vs Hijacking
- Types of Session Hijacking
- Steps to perform session Hijacking
- Prevention of session Hijacking

Session 12:

- Hacking Web Servers
- Web Application Vulnerabilities
- Web-Based Password Cracking Techniques
- Wireless Hacking
- WEP, WPA Authentication Mechanisms and Cracking Techniques
- Wireless Sniffers and Locating SSIDS, MAC spoofing
- Wireless hacking Techniques
- Methods used to secure Wireless Networks

Session 13:

- Mobile Device Communication Technology
- Android Structure
- Vulnerable Apps
- Issue With RF Technology

Session 14:

- Backdoor Devices
- Distributed Dos attacks
- Linux Hacking
- Linux Backdoors
- IDSs, Honeypots and Firewalls

Session 15:

- Physical Security
- Overview of Physical Security
- Need of Physical Security
- Factors Affecting Physical Security
- Penetration Testing Methodologies

Session 16: Malware Reverse Engineering

- Types of Malware
- Malicious code Families
- Latest Trends in Malware
- Analysis Of Malware

Assignments:

1. Create a Trozan using metasploit.
2. Work around Samspade tool and carry out *who-is* on existing domains.
3. Using Google Dorks/Hacks carry out the information gathering exercise.
4. Find out shared hosting details for a domain using Kali/BT and bing search.
5. Using Netcraft find out Web server/ server associated with the domains.
6. Carry out information gathering of domain using FOCA.
7. Carry out VA/PT of domain using Nessus, find out the vulnerable hosts, exploit their vulnerabilities and create a penetration testing report.
8. Using Wireshark create a filter and analyse and find the versions of services running for:
    a. FTP Traffic only.
    b. Https Traffic only
    c. ECHO request/reply
9. Set up a Virtual lab environment with Windows XP (SP1), Metasploitable OS, and BRICKS/DVWA web server and an Attacker machine (KALI/BT) in virtual machines (network in NAT mode).
   Now carry out Vulnerability assessment in environment
    a. Network VA/PT
        i. Find the open ports in domain
        ii. Find out the hosts in domains
        iii. Find out the services running on domains and their versions
        iv. Banner Grabbing of server
        v. Find out default vulnerabilities in Services
        vi. Exploit the vulnerabilities
        vii. Deploy and maintain the backdoor
        viii. Perform SNMPWalk and SNMP Enumeration in domain.
    b. Web VA/PT
        i. Find the domain information
        ii. Find the details of server and its default vulnerabilities
        iii. Perform manual testing for OWASP top 10
        iv. Perform automated testing using BurpSuite or ZAP proxies.
    c. Tools: nmap, netcat, netcraft, nslookup, whois, dig, ping, Nessus, Metasploit, FOCA

Management Development Program (30 T + 30 L hrs)

Session 1:

- Introduction to communication,
- Barriers to communication, Kind of communication,
- Confidence building Non-verbal Communication

Session 2:

- Fluency and vocabulary
- Synonyms

- Antonyms
- Grammar, Noun Pronoun,
- Verb, Adjective, Preposition, Conjunction

Session 3:

- Words of Idioms & phrases
- Sentence Construction Pronunciation,

Session 4:

- Greeting,
- Conversation practice,
- Polite Conversation,

Session 5:

- Resume Writing,
- Covering letter,
- Email,

Session 6:

- Presentation Skill,
- What is group discussion?
- Interview skills, Mock interview

Session 7:

- Analogy, Series Completion (Number, Alphabet, Letter Series)
- Coding-Decoding for Number
- Alphabet and Letter
- Blood Relations

Session 8:

- Puzzle Test: Classification Type questions
- Compression Type questions
- Sequential order questions
- Section based on given conditions
- Questions involving family members

Session 9:

- Alphabet test
- Order of words
- Letter words problems
- Rule detection
- Alphabetical quibble
- Word formation
- Number
- Ranking
- Time Sequence Test
- Mathematical operations
- Logical sequence of words

Session 10:

- Arithmetic reasoning
- Logical reasoning
- Statement-Arguments
- Statement-Assumptions
- Statement-courses of Action

- Statement-Conclusions
- Deriving conclusion from passages

Session 11:

- General Aptitude
- Addition
- Multiplication
- Divisibility
- Squaring
- Cube
- HCF and LCM
- Fraction

Session 12:

- Number system
- Permutation & combination
- Probability
- Ratio & Preparation

Session 13:

- Partnership
- Percentage
- Average
- Problem on Ages
- Profit and loss

Session 14:

- Simple Interest
- Compound Interest
- Time and work
- Work and Wages

Session 15:

- Trains
- Streams Pronoun
- Alligation
- Clock
- Pipes and cisterns

Lab Practice:

1. Faculty needs to conduct GD, presentation for speaking, conducting mock interviews etc.
2. Faculty needs to conduct tests, Surprise tests, assignments etc.

7. List of Text/Reference Books

Name of the Module	Title of the Book	Author/Publication	Edition	ISBN
Java Programming with Crypto API	Java 6 and J2EE 1.5	Kogent/ Dreamtech	latest	9789350040096
	Java The Complete Reference	McGraw Hill Education (India) Private Limited	8th	9781259002465
Application Security	Web Application Security A Beginner Guid	McGraw Hill Education (India) Private Limited	1st	9781259005466
	Python for Unix and Linux System Administration	Noah Gift, Jeremy Jones/ Bill O\'reilly	latest	9788184045833
Ethical Hacking	Gray Hat Hacking: The Ethical Hackers Handbook	Shon Harris/TMH	3rd	978-0071077316
	Malware, Rootkits & Botnets A Beginner	McGraw Hill Education (India) Private Limited		9781259029387
Management Development Program	High School English Grammar & Composition Revised Edition	Wren, Martin / S. Chand Publisher	2011 Edition	9788121900096
	Communication Skills Publication Year 2011	Sanjay Kumar, Pushp Lata / Oxford University Press	2011 Edition	9780198069324
	Professional Communication Skills	Praveen S R Bhatia / S.Chand Publishing	2011 Edition	9788121920926
	Quantitative Aptitude For Competitive Examinations	R. S. Aggarwal / S. Chand Publishing	17th Edition	9788121924986
	A Modern Approach To Verbal & Non-Verbal Reasoning	R. S. Aggarwal / S.Chand Publishing	Year 2012 Edition	9788121905510
	How to Prepare for GD and Interview (With CD) 3rd Edition	Hari Mohan Prasad, Rajnish Mohan/TMH	2010	0070706344

8. Evaluation Guidelines

8.1. Evaluation

Evaluation is a necessary and essential part of conducting the C-DAC Certificate Course in Ethical Hacking & Information Security, as it provides important feedback and inputs to both the institute as well as the student. The institute gets an idea about the relative performance of each student, which also serves as feedback about the design and conduct of the programme. The student gets a clear picture of his academic standing, individually and in comparison to his fellow students.

In order to ensure timely and efficient evaluation and certification of all students, the following guidelines are being issued and should be followed religiously.

8.2. Evaluation Methodology

8.2.1 Each centre should have a Designated Responsible Member (DRM) for Evaluation.

8.2.2 The DRM Evaluation would be responsible for coordinating all activities relating to evaluation at the training centre and for communicating with CDAC ACTS, Pune.

8.2.3 Evaluation is a compulsory part of the process of obtaining C-DAC Certified Ethical Hacking & Information Security certificate. All students are required to pass in each subject of the course in order to be eligible to receive the C-DAC Certificate.

8.2.4 The faculty of every subject should outline the objectives of the evaluation to be conducted for that particular subject, so as to enable the student to prepare himself/ herself properly.

8.2.5 The performance of students is constantly evaluated through surprise quizzes, hourly examinations, assignments throughout the term, submission of term reports, presentations and final examinations at the end of the course.

8.2.6 Mode of exams will be in online / offline, but prior information will be given by C-DAC, ACTS about the mode of the exam and it will be final.

8.3. EVALUATION METHODS

8.3.1 Course End Evaluation

After completion of the all subjects, a written examination CEE (Course End Examination) will be held, which will test the knowledge of the students of each subject and it is a compulsory part of the evaluation. Conducting CEE involves performing duty with responsibility. A small mistake in the process may hamper the whole system. Everyone has to play their role in an effective manner. It is a joint effort work which has to be carried out in a combined way. Right from receiving question paper from ACTS, C-DAC to sending the OMR answer sheet (in case of offline exam) and the response file (in case of online exam) for evaluation dealt with lot of responsibility.

ACTS, C-DAC in its pursuit of excellence, believes in providing a congenial atmosphere to the students during all exams in order to get them to perform at their optimum level. However, there are certain norms which the students are expected to be aware of and observe both in letter and spirit. These norms are:

8.3.1.1 Impersonation may lead to permanent expulsion from the Institute.

8.3.1.2 Cell phones are strictly prohibited in the exam hall/room.

8.3.1.3 Valid ID card is mandatory for entry to the exam room / hall.

8.3.1.4 Punctuality is most important at all times. Students are expected to check their exam location and be seated at least 10 minutes prior to the exam time.

8.3.1.5 In case of offline exam, as per ACTS, C-DAC policy all question papers are to be returned along with the answer script.

8.3.1.6 Students are required to bring their own stationary as no lending or borrowing is permitted during examination.

8.3.1.7 Programmable calculators or any other kind of electronic devices are strictly prohibited inside the exam area.

8.3.1.8 Indiscipline in the exam hall/ room will not be tolerated.

8.3.1.9 Possession of any written material related to the subject or communication with their fellow students, will result in disciplinary actions.

8.3.1.10 A student must score a minimum of 40 percent marks, in order to successfully clear the course.

8.3.1.11 It is recommended that the students should ensure 100% attendance for each course. 10% absences are permissible, only in case of illness, or emergencies. These have to be approved by the Centre Head. Approval is contingent upon the evidence provided.

8.3.1.12 There will be 150 questions to answer in 3 hours duration in CEE as per the following distribution mentioned in Table – 1.

Table – 1

Sl. No.	Modules	Hours	No. of Questions
1	Java Programming with Crypto API	80	40
2	Application Security	70	40
3	Ethical Hacking	70	40
4	Management Development Program	60	30
5	Project	40	-
	Total	**320**	**150**

8.3.2 GENERAL GUIDELINES FOR AWARD OF GRADES:

The marks of obtained in the CCEE shall be calculated to get total marks out of 100. The rounding off shall be done on the higher side. The grades shall be awarded on the basis of cut off in the absolute marks, as mentioned in Table – 2.

Table 2

Lower range of marks	Grade	Upper range of marks
91	≤ A+ <	100
81	≤ A <	90
71	≤ B+ <	80
61	≤ B <	70
51	≤ C+ <	60
41	≤ C <	50
0	≤ F <	40

8.3.3 Guidelines of CEE:

CEE will be conducted normally before the commencement of Project work of the course. The written examination should be of 180 minutes duration. It should consist of objective questions. A typical objective type exam paper should contain the following types of questions: –

- Multiple choice
- Yes or No
- True or False

Objective questions are useful in testing the recognition and recall abilities of students. They also help in keeping the exam short and easier to evaluate.

For the pure objective type question papers, there will be 150 objective type questions with 4 maximum answer options having only one correct option. The value of each objective type question is of one mark only. There will not be any negative marks for the wrong answers given by the students.

8.3.4 Guidelines for setting Question Papers:

While setting the question papers for theory Exam the following weightages should be assigned as per the difficulty level of the questions.

Levels	Requirements	Weightage
Level A – Easy	Requires elementary knowledge which may be obtained by attending all lectures and completion of mandatory lab assignments	25%
Level B – Intermediate	Requires thorough study of all course material, attendance at all lectures and completion of mandatory assignments	50%
Level C – Difficult	Requires study and lab work beyond the prescribed course material and mandatory assignments	25%

8.4. Guidelines for generating questions:

8.4.1 Question paper setter has to use sample paper format provided by C-DAC, ACTS Pune

8.4.2 Mention the subject name without fail.

8.4.3 Language of the question should be easy to understand.

8.4.4 The answers must have relevant objective type choices and “only one” correct answer.

8.4.5 The questions must be prepared by referring appropriate books, reference books, reference material, and course material having good information.

8.4.6 The question must be created by the domain expert afresh and should not be copied directly from any book, website, existing previous question papers etc.

8.4.7 The question should be unique and should have not been published anywhere.

8.4.8 Please mention the source of the question wherever possible, as it may help us in referring the same for detailing if required.

8.4.9 The caliber of the question should suffice the growing need of competition.

8.4.10 The question paper should have questions covering the entire syllabus.

8.4.11 The questions have to be typed in MS Word with “Arial” having letter size 12 point. Do not bold any letter, word or sentence in any part of the question paper.

8.4.12 It is essential to give password to the word document and send/tell the password separately.

8.4.13 It is essential that utmost care is taken at your end to maintain the secrecy of the soft copy at all time.

8.4.14 An expert team will review all questions. The questions will be filtered as per following:

- If the question is incomplete
- If the answer of the question is wrong
- If the question is not there in the syllabus
- If the question appears more than once
- If the question is too lengthy
- If the question is irrelevant
- If the options to the questions are irrelevant

8.5. Template for generation of Questions

Date:
Question generated by: Mr. /Ms.
Subject Name:
Q. No.
Question: <Text of the question>

Answer Choices
A:
B:
C:
D:

Difficulty Level: Easy / Intermediate / Difficult
Reference: (Name of books)
(If question taken from book) (Mention name of the book, author, ISBN)
Total Number of Questions Generated: _____

8.6. Template for Answer Key:

Module name:			
Question No.	**Answer Keys**	**Question No.**	**Answer Keys**
1		|	
2		|	
3		141	
4		142	
5		143	
6		144	
7		145	
8		146	
9		147	
10		148	
|		149	
|		150	

8.7. **Evaluation of answer papers:**

For Offline mode: Use of OMR sheets will be useful for processing the result of multiple choice exams. OMR is an effective way to collect data, process for the result and also it takes less time with greater accuracy in less effort. Centres need to follow the best way for scanning the OMR sheets, process the result and publish the result. Centres which are not using OMR can user OCR to conduct the exams and evaluate the students. Centre which are not using OMR or OCR can evaluate the students manually and process the result.

For Online mode: Course end exam will be through online s/w. Evaluation will be through that Exam s/w.

If a student requests for re-evaluation then the student has to pay `150 /- and it should be routed through training centre. The Re-evaluation fee should be paid to respective C-DAC training Centres, in case of Authorized Training Centres associated to C-DAC, Pune, payment to be made in favour of "C-DAC, ACTS" and payable at Pune. (This is applicable only for theory exam)

8.8. **Moderation:**

8.8.1 Grace marks would be awarded as per the methodology below:
Maximum of 4% of total term end theory exam marks can be awarded to a candidate.

8.8.2 Maximum of 8% of individual course end module test marks (maximum marks) can be awarded per module.

S No.	Name of the course	Total Marks	Maximum grace marks for the course
1	Certificate Course in Ethical Hacking and Information Security	150	6

On completion of the moderation exercise the revised marks should be updated in the marks database.

8.9. **Re-examinations:**

The following conditions will be applicable for the course end re-exam:

8.9.1. Students who do not appear for an exam on the scheduled date will not have an automatic right to re-examination. Only those students who, in the opinion of the centre/course coordinator have a genuine reason for being absent may be allowed to appear for a re-exam.

8.9.2. Students who have failed an exam may be allowed to appear for a re-exam.

8.9.3. The re-exam should be conducted following the same process as the regular examination.

8.9.4. Students, who failed/remained absent in the Course End Examination conducted by C-DAC, shall be allowed to appear in the re-examination only once.

8.9.5. Students who remain absent or fail in the re-examination will not get any further chance for appearing for a third attempt or further. In such case the candidate can receive the Performance Statement and the certificate of participation without any grade.

8.9.6. On evaluation of their answer sheets 20% of the marks obtained by the students will be deducted (towards de-rating for re-examination) for arriving at the final score, i.e. in order to clear the module test the student has to score a minimum of 50% marks instead of 40%.

8.10. **Project Module:**

8.10.1. Project work should be start as soon as possible.

8.10.2. After that students should be ready with all mandatory documents with database design and then completion of all teaching modules they can do the project.

8.10.3. Performance in the Project module will be awarded in grade. The Project grade will be mentioned separately on the certificate & will have no effect on the overall grade obtained by a student.

8.10.4. Students may do industry-sponsored projects, but will be required to do the project work within the centre.

8.10.5. Evaluation of the Project module will take place as following:

8.10.5.1. Internal evaluation will be take place at mid of the module

8.10.5.2. External evaluation will take place at the end of the module

Based on both evaluations, final grade will be awarded & communicated to C-DAC ACTS, Pune

8.11. **Guidelines for Project Evaluation**

Evaluation of Project work needs to be carried out as per the following guidelines:

a. Literature study.
b. Submission of abstract for their colloquium/seminar/project work along with the references.
c. Submission of the detailed work report
d. Two presentations each for 15 minutes on the work done restricted to 15 – 20 slides followed by evaluation.
e. The evaluation for 100 marks will be splited up as follows:

i.	Literature survey	– 10
ii.	Contents of the project work	– 20
iii.	Contents Flow of Presentation	– 15
iv.	Communication and Presentation Skills	– 20
v.	Depth of Knowledge in the topic	– 15
vi.	Viva Voce	– 15
vii.	Attendance	– 5

f. Soft copy of the presentation should be submitted to C-DAC.

8.12 Ensuring Security of Evaluation data/records:

8.12.1. Ensure that all data relating to evaluation of students is stored in a secure place that cannot be accessed by unauthorized personnel.

8.12.2. All question papers must be prepared and stored in a separate area specifically designated for the purpose.

8.12.3. Whenever any external faculty sets a question paper, ensures that he should follows the guidelines given by C-DAC ACTS Pune.

8.12.4. Ensure that only one copy of any question paper is prepared in physical (printed) form for review and revision.

8.12.5. When the question paper is finalized, print out one master copy and gets it signed by the paper setter, Reviewer and DRM Evaluation.

8.12.6. Prepare required number of photocopies of the question paper and store them in a safe and secure location before the exam.

8.12.7. The data relating to evaluation of students, such as soft copies of question papers and answer keys, student marks database and performance statements etc. must be kept in a separate domain/directory which is accessible only to authorized personnel. Ensure that the data is regularly backed up.

8.12.8. The question papers for the theory as well as the laboratory examinations at all the centres will be set by CDAC, ACTS Pune. The centres according to guidelines provided by C-DAC, ACTS Pune, will conduct the evaluation of the laboratory and assignments locally.

Note: The Evaluation Guidelines, Rules and Regulations issued by C-DAC, ACTS – Pune from time to time shall be binding on all the centers and all the students. C-DAC, ACTS, Pune reserves the right to add, modifies or deletes any or entire contents of this document at any point of time without giving any notice. It's the responsibility of the centre coordinator to inform such changes to the students in form of a formal notice with a duly signed copy to C-DAC, ACTS, Pune.

9. Requirements (S/W and H/W)

Certificate Course in Ethical Hacking and Information Security	
A. Servers	
1. Unix / Linux	
2. Windows server 2008 /2012	
3. Application / Dummy Servers Configured for various modules	
4. Cisco IOS Simulators	
5. Fedora Core	
6. Threat Management Gateway	
Severs Configuration (Please write specifications)	
1. Processor	latest
2. RAM	5GB
3 HDD	500GB
4. Network Card (extra 2 NIC)	
5. 1.44 MB FDD	
6. AGP Card with 4/8 MB VRAM	
7. 2 Serial ports, 1 parallel port, 104 Keys Keyboard.	
8 CD / DVD Drive	
B. Clients Machines / Network Nodes	
1. Processor	latest
2. RAM	2GB/MB
3. HDD IDE / EIDE	160GB
4. AGP-64 bit Card with 8 MB / 4MB VRAM	
5. PCI Network Card 10/100 Base T, UTP Ethernet	
6. Multimedia Kit	
C. Network	

1. 10/100 Base T UTP Hub(s)
2. UTP CAT-5 Cabling with RJ-45 connectors
3. UTP Patch Cables
4. 3 switches (4 port or 8 port Switch is sufficient)
5. Juniper UTM Box
D. Communication and Internet
1 Internet Access
2. ISDN Connectivity
3. Modem 28.8/ 33 / 56 KBPS
4. Direct Internet Line
E. Printers
1. Dot Matrix Printers 132 columns
2. Laser Printer
F. Additional Lab Equipments
1. Amplified Speakers, Headphones & mikes
2. Hi-Lumen OHP
3. Video Projector (XGA / SVGA Compatible)
4. TWAIN Compliant Colour Scanner
G. Module Specific Software Environments and Operating Systems
1.Wireshark
2. JDK1.7
3. Eclipse
4. TOMCAT
5.nmap
6.GNS
8.Symantec Ghost
9.SNMP enumeration tool
10.netcat
11.putty
12.WinSCP
H. Operating System Software Common For all Course modules
1. Windows 2012 Server / Windows8
2. RedHat Linux 7
3. Kali Linux
4. Clear OS
5. Alien Vault