ETHICAL HACKING
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – I

Subject Code	**16SFC11**	IA Marks	20
Number of Lecture Hours/Week	04	Exam Marks	80
Total Number of Lecture Hours	50	Exam Hours	03

CREDITS – 04

Course objectives: This course will enable students to

- Learn aspects of security, importance of data gathering, foot printing and system hacking.
- Learn tools and techniques to carry out a penetration testing.
- How intruders escalate privileges?
- Explain Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation.
- Compare different types of hacking tools.

Module 1	**Teaching Hours**
Casing the Establishment: What is foot printing, Internet Foot printing, Scanning, Enumeration, basic banner grabbing, Enumerating Common Network services. Case study: Network Security Monitoring.	**10 Hours**
Module 2	
Securing permission: Securing file and folder permission, Using the encrypting file system, Securing registry permissions. Securing service: Managing service permission, Default services in windows 2000 and windows XP. Unix: The Quest for Root, Remote Access vs Local access, Remote access, Local access, After hacking root.	**10 Hours**
Module 3	
Dial-up, PBX, Voicemail and VPN hacking, Preparing to dial up, War-Dialing, Brute-Force Scripting PBX hacking, Voice mail hacking, VPN hacking, Network Devices: Discovery Autonomous System Lookup, Public Newsgroups, Service Detection, Network Vulnerability, Detecting Layer 2 Media.	**10 Hours**
Module 4	
Wireless Hacking: Wireless Foot printing, Wireless Scanning and Enumeration, Gaining Access, Tools that exploiting WEP Weakness, Denial of Services Attacks, Firewalls: Firewalls landscape, Firewall Identification-Scanning Through firewalls, packet Filtering, Application Proxy Vulnerabilities, Denial of Service Attacks, Motivation of Dos Attackers, Types of DoS attacks, Generic Dos Attacks, UNIX and Windows DoS.	**10 Hours**
Module 5	
Remote Control Insecurities, Discovering Remote Control Software, Connection, Weakness.VNC, Microsoft Terminal Server and Citrix ICA, Advanced Techniques Session Hijacking, Back Doors, Trojans, Cryptography, Subverting the systems Environment, Social Engineering, Web Hacking, Web server hacking web application hacking, Hacking the internet Use, Malicious Mobile code, SSL fraud, E-mail Hacking, IRC hacking, Global countermeasures to Internet User Hacking.	**10 Hours**

Course Outcomes

The students should be able to:

- Explain aspects of security, importance of data gathering, foot printing and system hacking.
- Explain aspects of security, importance of data gathering, foot printing and system hacking.
- Demonstrate how intruders escalate privileges.
- Demonstrate how intruders escalate privileges.
- Demonstrate how intruders escalate privileges.

Question paper pattern:
The question paper will have ten questions.
There will be 2 questions from each module.

Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books:

1. Stuart McClure, Joel Scambray and Goerge Kurtz, Hacking Exposed 7: Network Security Secrets & Solutions, Tata Mc Graw Hill Publishers, 2010.
2. Bensmith, and Brian Komer, Microsoft Windows Security Resource Kit, Prentice Hall of India, 2010.

Reference Books:

1. Stuart McClure, Joel Scambray and Goerge Kurtz, "Hacking Exposed Network Security Secrets & Solutions", 5th Edition, Tata Mc Graw Hill Publishers, 2010.
2. Rafay Baloch, "A Beginners Guide to Ethical Hacking".
3. Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, "Gray Hat Hacking The Ethical Hackers Handbook", 3rd Edition, McGraw-Hill Osborne Media paperback(January 27, 2011)

PRAGMATICS OF INFORMATION SECURITY
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – I

Subject Code	**16SSE12**	IA Marks	20
Number of Lecture Hours/Week	04	Exam Marks	80
Total Number of Lecture Hours	50	Exam Hours	03

CREDITS – 04

Course objectives: This course will enable students to

- Explain the fundamentals of Cryptography.
- Acquire knowledge on cryptographic tools used to provide confidentiality, integrity and authenticity.
- Differentiate the various user authentication methods, access control schemes and authentication applications.
- Acquire the knowledge on IP Security tools.
- Acquire the knowledge about malicious software.

Module 1	**Teaching Hours**
Overview: Computer Security Concepts, Requirements, Architecture, Trends, Strategy Perimeter Security: Firewalls, Intrusion Detection, Intrusion Prevention systems, Honeypots Case Study: Readings, Intrusion and intrusion detection by John McHugh.	**10 Hours**
Module 2	
User Authentication: Password, Password-based, token based, Biometric, Remote User authentication. Access Control: Principles, Access Rights, Discretionary Access Control, Unix File Access Control, Role Based Access Control Internet Authentication Applications: Kerberos, X.509, PKI, Federated Identity Management.	**10 Hours**
Module 3	
Cryptographic Tools: Confidentiality with symmetric encryption, Message Authentication & Hash Functions, Digital Signatures, Random Numbers. Symmetric Encryption and Message Confidentiality: DES, AES, Stream Ciphers, Cipher Block Modes of Operation, Key Distribution.	**10 Hours**
Module 4	
Internet Security Protocols: SSL, TLS, IPSEC, S/ MIME. Public Key Cryptography and Message Authentication: Secure Hash Functions, HMAC, RSA, Diffie Hellman Algorithms Case Study: Readings, Programming Satan's Computer Ross Anderson and Roger Needham.	**10 Hours**
Module 5	

Malicious Software: Types of Malware, Viruses & Counter Measures, Worms, Bots, Rootkits Software Security: Buffer Overflows, Stack overflows, Defense, Other overflow attacks Case Study.	**10 Hours**

Course Outcomes

The students should be able to:

- Explain the fundamentals of Cryptographic techniques.
- Identify the security issues in the network and resolve it.
- Implement security algorithms in the field of Information technology
- Identifying the type of malware attacks and implementing preventive measures.

Question paper pattern:

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books:

1. Computer Security: Principles and Practice, William Stalling & Lawrie Brown, 2008, Indian Edition 2010, Pearson.

Reference Books:

1. Readings: Smashing The Stack For Fun And Profit, Aleph One http:// www.phrack.com/ issues.html ? issue = 49&id=14#article
2. Chuck Easttom, " Computer Security Fundamentals" Pearson, 2012.

CYBER CRIME AND CYBER FORENSICS
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – I

Subject Code	**16SFC13**	IA Marks	20
Number of Lecture Hours/Week	04	Exam Marks	80
Total Number of Lecture Hours	50	Exam Hours	03

CREDITS – 04

Course objectives: This course will enable students to

- Explain the fundamentals of Cyber Crime.
- Analyze the nature and effect of cybercrime in society.
- Demonstrate Accounting Forensics.
- Explain Computer Crime and Criminals and Liturgical Procedures.

Module 1	**Teaching Hours**
Introduction and Overview of Cyber Crime, Nature and Scope of Cyber Crime, Types of Cyber Crime, Social Engineering, Categories of Cyber Crime, Property Cyber Crime.	**10 Hours**
Module 2	
Unauthorized Access to Computers, 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.	**10 Hours**
Module 3	
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, Network Forensics.	**10 Hours**

Module 4	
Introduction to Cyber Crime Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Hands on Case Studies, Encryption and Decryption Methods, Search and Seizure of Computers, Recovering Deleted Evidences, Password Cracking.	**10 Hours**
Module 5	
Laws and Ethics, Digital Evidence Controls, Evidence Handling Procedures, Basics of Indian Evidence ACT IPC and CrPC , Electronic Communication Privacy ACT, Legal Policies.	**10 Hours**

Course Outcomes

The students should be able to:

- Explain the fundamentals and types of cybercrime.
- Distinguish various types of computer crime.
- Illustrate computer forensic techniques to identify the digital forensics associated with criminal activities.
- Apply forensic analysis tools to recover important evidence for identifying computer crime.
- Discuss laws and ethics involved in cyber crime.

Question paper pattern:

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books:

1. Bernadette H Schell, Clemens Martin, "Cybercrime", ABC – CLIO Inc, California, 2004. "Understanding Forensics in IT ", NIIT Ltd, 2005.
2. Nelson Phillips and Enfinger Steuart, "Computer Forensics and Investigations", Cengage Learning, New Delhi, 2009.

Reference Books:

1. Kevin Mandia, Chris Prosise, Matt Pepe, "Incident Response and Computer Forensics ", Tata McGraw -Hill, New Delhi, 2006.
2. Robert M Slade," Software Forensics", Tata McGraw - Hill, New Delhi, 2005.

PROBABILITY STATISTICS AND QUEUING THEORY
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – I

Subject Code	16LNI14 / 16SCN14/16SCS14/ 16SSE14 / 16SIT14 /16SCE14 / **16SFC14**	IA Marks	20
Number of Lecture Hours/Week	04	Exam Marks	80
Total Number of Lecture Hours	50	Exam Hours	03

CREDITS – 04

Course objectives: This course will enable students to

- Develop analytical capability and to impart knowledge of Probability, Statistics and Queuing.
- Apply above concepts in Engineering and Technology.
- Acquire knowledge of Hypothesis testing and Queuing methods and their applications so as to enable them to apply them for solving real world problems

Module 1	**Teaching Hours**
Axioms of probability, Conditional probability, Total probability, Baye's theorem, Discrete Random variable, Probability mass function, Continuous Random variable. Probability density function, Cumulative Distribution Function, and its properties, Two-dimensional Random variables, Joint pdf / cdf and their properties	**10 Hours**
Module 2	
Probability Distributions / Discrete distributions: Binomial, Poisson Geometric and Hyper-geometric distributions and their properties. Continuous distributions: Uniform, Normal, exponential distributions and their properties.	**10 Hours**
Module 3	
Random Processes: Classification, Methods of description, Special classes, Average values of Random Processes, Analytical representation of Random Process, Autocorrelation Function, Cross-correlation function and their properties, Ergodicity, Poisson process, Markov Process, Markov chain.	**10 Hours**
Module 4	
Testing Hypothesis: Testing of Hypothesis: Formulation of Null hypothesis, critical region, level of significance, errors in testing, Tests of significance for Large and Small Samples, t-distribution, its properties and uses, F-distribution, its properties and uses, Chi-square distribution, its properties and uses, $\chi 2$ – test for goodness of fit, $\chi 2$ test for Independence	**10 Hours**
Module 5	
Symbolic Representation of a Queuing Model, Poisson Queue system, Little Law, Types of Stochastic Processes, Birth-Death Process, The M/M/1 Queuing System, The M/M/s Queuing System, The M/M/s Queuing with Finite buffers.	**10 Hours**

Course Outcomes

The students should be able to:

- Demonstrate use of probability and characterize probability models using probability mass (density) functions & cumulative distribution functions.
- Explain the techniques of developing discrete & continuous probability distributions and its applications.
- Describe a random process in terms of its mean and correlation functions.
- Outline methods of Hypothesis testing for goodness of fit.
- Define the terminology &nomenclature appropriate queuing theory and also distinguish various queuing models.

Question paper pattern:
The question paper will have ten questions.
There will be 2 questions from each module.

Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books:

1. Probability, Statistics and Queuing Theory, V. Sundarapandian, Eastern Economy Edition, PHI Learning Pvt. Ltd, 2009.

Reference Books:

1. Probability & Statistics with Reliability, Queuing and Computer Applications, 2nd Edition by Kishor. S. Trivedi , Prentice Hall of India ,2004.
2. Probability, Statistics and Random Processes, 1st Edition by P Kausalya, Pearson Education, 2013.

ACCESS CONTROLAND IDENTITY MANAGEMENT SYSTEM
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – I

Subject Code	**16SFC151/**	IA Marks	20
Number of Lecture Hours/Week	03	Exam Marks	80
Total Number of Lecture Hours	40	Exam Hours	03

CREDITS – 03

Course objectives: This course will enable students to

- Compute tasks with security contexts.
- Different classifications of identity management system.
- Various models for Trust paradigms.
- Discretionary access model and Access Matrix Model.
- Classify all the active entities of a protection system.

Module 1	**Teaching Hours**
Access control: Introduction, Attenuation of privileges, Trust and Assurance, Confinement problem, Security design principles, Identity Management models, local, Network, federal , global web identity, XNS approach for global Web identity, Centralized enterprise level Identity Management.	**8 Hours**
Module 2	
Elements of trust paradigms in computing, Third party approach to identity trust, Kerberos, Explicit third party authentication paradigm, PKI approach to trust establishment, Attribute certificates, Generalized web of trust models, Examples.	**8 Hours**
Module 3	
Mandatory access control, comparing information flow in BLP and BIBA models, Combining the BLP and BIBA models, Chinese wall problem.	**8 Hours**
Module 4	
Discretionary access control and Access matrix model, definitions, Safety problem, The take grant protection model, Schematic protection model, SPM rules and operations, Attenuating, Applications	**8 Hours**
Module 5	
Role based access control, Hierarchical Access Control, Mapping of a mandatory policy to RABC, Mapping discretionary control to RBAC, RBAC flow analysis, Separation of Duty in RBAC, RBAC consistency properties, The privileges perspective of separation of duties, Functional specification for RBAC.	**8 Hours**

Course Outcomes

The students should be able to:

- Analyze to compute tasks with security contexts.

- Categorize the identity management system into different classes.
- Measure the different elements of Trust paradigms for various models.
- Compare and contrast between Discretionary access model and Access Matrix Model.
- Categorize all the active entities of a protection system.

Question paper pattern:
The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books:
1. Messoud Benantar, "Access Control Systems: Security, Identity
2. Management and Trust Models", Springer, 2009.

Reference Books:
1. Elena Ferrari and M. Tamer A-zsu , "Access Control In Data Management
2. Systems", Morgan & Claypool Publishers, 2010.

CLOUD SECURITY
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – I

Subject Code	**16SFC152**	IA Marks	20
Number of Lecture Hours/Week	03	Exam Marks	80
Total Number of Lecture Hours	40	Exam Hours	03

CREDITS – 03

Course objectives: This course will enable students to

- Describe the fundamentals of Cloud Computing.
- Summarize the need of cloud compliance and existing cloud solutions.
- Explain the cloud security concepts.
- Demonstrate the operations of Data Centre.
- Distinguish the concepts of Identity management and virtualization.

Module 1	**Teaching Hours**
Cloud Computing Architectural Framework: Cloud Benefits, Business scenarios, Cloud Computing Evolution, cloud vocabulary, Essential Characteristics of Cloud Computing, Cloud deployment models, Cloud Service Models, Multi- Tenancy, Approaches to create a barrier between the Tenants, cloud computing vendors, Cloud Computing threats, Cloud Reference Model, The Cloud Cube Model, Security for Cloud Computing, How Security Gets Integrated.	**8 Hours**
Module 2	
Compliance and Audit: Cloud customer responsibilities, Compliance and Audit Security Recommendations. Portability and Interoperability: Changing providers reasons, Changing providers expectations, Recommendations all cloud solutions, IaaS Cloud Solutions, PaaS Cloud Solutions, SaaS Cloud Solutions.	**8 Hours**
Module 3	
Traditional Security, Business Continuity, Disaster Recovery, Risk of insider abuse, Security baseline, Customers actions, Contract, Documentation, Recovery Time Objectives (RTOs), Customers responsibility, Vendor Security Process (VSP).	**8 Hours**
Module 4	
Data Center Operations: Data Center Operations, Security challenge, Implement Five Principal Characteristics of Cloud Computing, Data center Security Recommendations. Encryption and Key Management: Encryption for Confidentiality and Integrity, Encrypting data at rest, Key Management Lifecycle, Cloud Encryption Standards,	**8 Hours**

Recommendations.	
Module 5	
Identity and Access Management: Identity and Access Management in the cloud, Identity and Access Management functions, Identity and Access Management (IAM) Model, Identity Federation, Identity Provisioning Recommendations, Authentication for SaaS and Paas customers, Authentication for IaaS customers, Introducing Identity Services, Enterprise Architecture with IDaaS , IDaaS Security Recommendations. Virtualization: Hardware Virtualization, Software Virtualization, Memory Virtualization, Storage Virtualization, Data Virtualization, Network Virtualization, Virtualization Security Recommendations.	**8 Hours**
Course Outcomes	
The students should be able to: • Demonstrate the growth of Cloud computing, architecture and different modules of implementation. • Evaluate the different types of cloud solutions among IaaS, PaaS, SaaS. • Access the security implementation flow, actions and responsibilities of stake holders. • Generalize the Data Centre operations, encryption methods and deployment details. • Provide recommendations for using and managing the customer's identity and choose the type of virtualization to be used.	
Question paper pattern: The question paper will have ten questions. There will be 2 questions from each module. Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.	
Text Books: 1. Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy, An Enterprise Perspective on Risks and Compliance", Oreilly Media 2009.	
Reference Books: 1. Vic (J.R.) Winkler, "Securing the Cloud, Cloud Computer Security Techniques and Tactics", Syngress, April 2011.	

ADVANCED CRYPTOGRAPHY
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – I

Subject Code	**16SFC153**	IA Marks	20
Number of Lecture Hours/Week	03	Exam Marks	80
Total Number of Lecture Hours	40	Exam Hours	03

CREDITS – 03

Course objectives: This course will enable students to

- The concepts of principles and practice of cryptography and network security.
- Overview of the Feistel cipher, Distribution of Public Keys, digital signatures and Authentication protocols.
- How to analyze the security of multiple encryption schemes and Triples DES.
- Structure and Building of secure authentication systems using message authentication techniques.
- The concepts of principles and practice of visual cryptography.

Module 1	**Teaching Hours**
OSI security architecture: Classical encryption techniques, Cipher principles, Data encryption standard, Block cipher design principles and modes of operation, Evaluation criteria for AES, AES cipher, Triple DES, Placement of encryption function, Traffic confidentiality.	**8 Hours**
Module 2	
Key management: Diffie Hellman key exchange, Elliptic curve architecture and cryptography, Introduction to number theory, Confidentiality using symmetric encryption, Public key cryptography and RSA.	**8 Hours**
Module 3	
Authentication requirements: Authentication functions, Message authentication codes, Hash functions, Security of hash functions and MACS, MD5 Message Digest algorithm, Secure hash algorithm, Ripend, HMAC digital signatures, Authentication protocols.	**8 Hours**
Module 4	
Quantum Cryptography and Quantum Teleportation: Heisenberg uncertainty principle, polarization states of photons, quantum cryptography using polarized photons, local vs. non local interactions, entanglements, EPR paradox, Bell's theorem, Bell basis, teleportation of a single qubit theory and experiments.	**8 Hours**
Module 5	
Future trends: Review of recent experimental achievements, studyon technological feasibility of a quantum computer candidate physical systems and limitations imposed by noise.	**8 Hours**

Course Outcomes

The students should be able to:

- Explain the concepts of principles and practice of cryptography and network security.
- Present an overview of the Feistel cipher, Distribution of Public Keys, digital signatures and Authentication protocols.
- Analyze the security of multiple encryption schemes and Triples DES.
- Build secure authentication systems by use of message authentication techniques.
- Explain the concepts of principles and practice of visual cryptography.

Question paper pattern:

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books:

1. William Stallings, "Cryptography and Network Security -Principles and Practices", 3rd Edition, Prentice Hall of India, 2003.
2. Atul Kahate, "Cryptography and Network Security", Tata McGraw -Hill, 2003.
3. William Stallings, "Network Security Essentials: Applications and Standards", Pearson Education Asia, 2000.

Reference Books:

1. R. P. Feynman, "Feynman lectures on computation", Penguin Books, 1996.
2. Gennady P. Berman, Gary D. Doolen, Ronnie Mainiri & Valdmis Itri Frinovich, "Introduction to quantum computers", World Scientific, Singapore, 1998.
3. Jonathan Katz, Yehuda Lindell, "Introduction to Modern Cryptography" Principles And Protocols",CRC Press.

APPLICATION AND WEB SECURITY
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – I

Subject Code	**16SFC154**	IA Marks	20
Number of Lecture Hours/Week	03	Exam Marks	80
Total Number of Lecture Hours	40	Exam Hours	03

CREDITS – 03

Course objectives: This course will enable students to

- Web application's vulnerability and malicious attacks.
- Basic web technologies used for web application development.
- Basic concepts of Mapping the application
- Illustrate different attacking illustrations.
- Basic concepts of Attacking Data Stores.

Module 1	**Teaching Hours**
Web Application (In) security: The Evolution of Web Applications, Common Web Application Functions, Benefits of Web Applications , Web Application Security. Core Defense Mechanisms: Handling User Access Authentication, Session Management, Access Control, Handling User Input, Varieties of Input Approaches to Input Handling, Boundary Validation. Multistep Validation and Canonicalization: Handling Attackers, Handling Errors, Maintaining Audit Logs, Alerting Administrators, Reacting to Attacks.	**8 Hours**
Module 2	
Web Application Technologies: The HTTP Protocol, HTTP Requests, HTTP Responses, HTTP Methods, URLs, REST, HTTP Headers, Cookies, Status Codes, HTTPS, HTTP Proxies, HTTP Authentication, Web Functionality, Server-Side Functionality, Client-Side Functionality, State and Sessions, Encoding Schemes, URL Encoding, Unicode Encoding, HTML Encoding, Base64 Encoding, Hex Encoding, Remoting and Serialization Frameworks.	**8 Hours**
Module 3	
Mapping the Application: Enumerating Content and Functionality, Web Spidering, User-Directed Spidering, Discovering Hidden Content, Application Pages Versus Functional Paths, Discovering Hidden Parameters, Analyzing the Application, Identifying Entry Points for User Input, Identifying Server-Side Technologies, Identifying Server-Side Functionality, Mapping the Attack Surface.	**8 Hours**
Module 4	
Attacking Authentication: Authentication Technologies, Design Flaws in Authentication Mechanisms, Bad Passwords, Brute-Forcible Login, Verbose Failure Messages,	**8 Hours**

Vulnerable Transmission of Credentials, Password Change, Functionality, Forgotten Password Functionality, "Remember Me" Functionality, User Impersonation, Functionality Incomplete, Validation of Credentials, Nonunique Usernames, Predictable Usernames, Predictable Initial Passwords, Insecure Distribution of Credentials. Attacking Access Controls: Common Vulnerabilities, Completely Unprotected, Functionality Identifier-Based Functions, Multistage Functions, Static Files, Platform Misconfiguration, Insecure Access Control Methods.	
Module 5	
Attacking Data Stores: Injecting into Interpreted Contexts, Bypassing a Login, Injecting into SQL, Exploiting a Basic Vulnerability Injecting into Different Statement Types, Finding SQL Injection Bugs, Fingerprinting the Database, The UNION Operator, Extracting Useful Data, Extracting Data with UNION, Bypassing Filters, Second-Order SQL Injection, Advanced Exploitation Beyond SQL Injection: Escalating the Database Attack, Using SQL Exploitation Tools, SQL Syntax and Error Reference, Preventing SQL Injection.	**8 Hours**

Course Outcomes

The students should be able to:

- Achieve Knowledge of web application's vulnerability and malicious attacks.
- Understand the basic web technologies used for web application development
- Understands the basic concepts of Mapping the application.
- Able to illustrate different attacking illustrations
- Basic concepts of Attacking Data Stores.

Question paper pattern:

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books:

1. The Web Application Hacker's Handbook: Finding And Exploiting Security
2. Defydd Stuttard, Marcus Pinto Wiley Publishing, Second Edition.

Reference Books:

1. Professional Pen Testing for Web application, Andres Andreu, Wrox Press.
2. Carlos Serrao, Vicente Aguilera, Fabio Cerullo, "Web Application Security" Springer; 1st Edition
3. Joel Scambray, Vincent Liu, Caleb Sima ,"Hacking exposed", McGraw-Hill; 3rd Edition, (October, 2010).
4. OReilly Web Security Privacy and Commerce 2nd Edition 2011.
5. Software Security Theory Programming and Practice, Richard sinn, Cengage Learning.
6. Database Security and Auditing, Hassan, Cengage Learning.

ETHICAL HACKING LABORATORY
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – I

Subject Code	**16SFC16**	IA Marks	20
Number of Lecture Hours/Week	01+03	Exam Marks	80
Total Number of Lecture Hours	50	Exam Hours	03

CREDITS – 02

Course objectives: This course will enable students to

- Evaluate modern tools
- Analyze packet capturing in network
- Define forensic analysis
- Security in various web applications

1. Wireshark: Experiment to monitor live network capturing packets and analyzing over the live network.
2. LOIC: DoS attack using LOIC.
3. FTK: Bit level forensic analysis of evidential image and reporting the same.
4. Darkcomet : Develop a malware using Remote Access Tool Darkcomet to take a remote access over network. 4.
5. HTTrack: Website mirroring using Httrack and hosting on a local network.
6. XSS: Inject a client side script to a web application.
7. Emailtrackerpro: Email analysis involving header check, tracing the route. Also perform a check on a spam mail and non-spam mail.

Course Outcomes

The students should be able to:

- Evaluate modern tools
- Analyze packet capturing in network
- Define forensic analysis
- Security in various web applications

Conduction of Practical Examination:

1. All laboratory experiments (nos) are to be included for practical examination.
2. Students are allowed to pick one experiment from **each part and execute both**
3. Strictly follow the instructions as printed on the cover page of answer script for breakup of marks
4. **Change of experiment is allowed only once and marks allotted to the procedure part to be made zero.**

SEMINAR
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – I

Subject Code	16SCE17 / 16SCN17 / 16LNI17 / 16SIT17 / 16SSE17 / 16SCS17 / **16SFC17**	IA Marks	100
Number of Lecture Hours/Week	----	Exam Marks	-
Total Number of Lecture Hours	----	Exam Hours	-

CREDITS – 01

Course objectives: This course will enable students to

- Motivate the students to read technical article
- Discover recent technology developments

Descriptions

The students should read a recent technical article (try to narrow down the topic as much as possible) from any of the leading reputed and refereed journals like:

1. IEEE Transactions, journals, magazines, etc.
2. ACM Transactions, journals, magazines, SIG series, etc.
3. Springer
4. Elsevier publications etc

In the area of (to name few and not limited to)

- Web Technology
- Cloud Computing
- Artificial Intelligent
- Networking
- Security
- Data mining

Course Outcomes

The students should be able to:

- Conduct survey on recent technologies
- Infer and interpret the information from the survey conducted
- Motivated towards research

Conduction:

The students have to present at least ONE technical seminar on the selected topic and submit a report for internal evaluation.

Marks Distribution: Literature Survey + Presentation (PPT) + Report + Question & Answer + Paper: 20 + 30 + 30 + 20 (100).