SOMAIYA VIDYAVIHAR UNIVERSITY
K J Somaiya College of Engineering

Syllabus

Honours Programme in

Cyber Security and Forensics

(Offered by Department of Computer Engineering)

From

Academic Year 2024-25

Revision 2

(Approved in Academic Council meeting dated_ _ _)

K J Somaiya College of Engineering, Mumbai-77

(A Constituent College of Somaiya Vidyavihar University)

Honours' Degree Programme in Cyber Security and Forensics

Offered by Department of Computer Engineering

Introduction:

Security is a critical issue in all the computing systems due to increasing number of security related breaches and incidents. The need of security professionals is ever increasing due to most of the services being made available online.

With the information sharing and processing going from centralized to distributed to the entire internet and due to inherent vulnerabilities and weaknesses of hardware, software and protocols there are constant risks and threats on compromising of data and information. This led to the need of Security in the form of controls, algorithms, procedures, policies and laws for securing information in the cyber space.

This programme will focus on basics of security starting security goals, vulnerabilities, threats & controls to advanced topics like cyber forensics and cyber laws etc. There will be topics on applied cryptography, cyber security, forensics, secure coding and vulnerability assessment & penetrative testing.

Objectives: The offered programme aims to give the understanding of:

(1) Security goals, vulnerabilities, threats & controls.

(2) Implementation of various control mechanisms related to various security services.

(3) Understand cybercrime, its prevention and cyber laws.

(4) Carrying out the various information security-related tasks such as Penetration Testing and Vulnerability Analysis.

(5) Understand Digital forensics and Advanced Offensive Security techniques.

Learning Outcomes of the Honours' Degree Programme:

At the successful completion of this programme, an Engineering Graduate will be able to:

- Design and develop secure applications and systems.
- Classify the types of cybercrimes their prevention and applicability of various cyber laws.
- Implement penetration testing, vulnerability analysis and offensive security techniques for applications and systems.
- Apply and use various digital forensic tools for cybercrime investigation.

Assessment Methods: Evaluation is done by a variety of tools including Open book tests, MCQs (multiple choice questions), Study of research papers, Internal Assessment tools and End Semester Examinations etc. Mini-Projects are offered in courses also to encourage project based learning among students.

Acronyms used in syllabus document	
Acronym	**Definition**
CA	Continuous Assessment
ESE	End Semester Exam
IA	Internal Assessment
O	Oral
P	Practical
P&O	Practical and Oral
TH	Theory
TUT	Tutorial
TW	Term work
ISE	In-semester Examination
CO	Course Outcome

Acronyms used in Course code e.g. 116hxxC301

Position of Digit	Acronym	Definition
1	**2**	SUV 2023 Second Revision
2	**16**	KJSCE
3	**H**	**Honour Degree Program**
4	**02 (xx)**	**Cyber Security and Forensics**
5	**C**	Core Course
	L	Laboratory Course
	T	Tutorial
	P	Project Based Course
6	**1/2/3/4**	Semester Number
7	**01/02/03--**	Course Number

Proposed Credit Scheme

Course Code	Course Name	Teaching Scheme (Hrs.) TH – P – TUT	Total (Hrs.)	Credits Assigned TH – P – TUT	Total Credits	Suggested semester of Honours' degree
216H02C401	Applied Cryptography	3 – 0 – 0	03	3 – 0 – 0	03	IV
216H02L401	Applied Cryptography Laboratory	0 – 2 – 0	02	0 – 1 – 0	01	IV
216H02C501	Cyber Forensics and Laws	3 – 0 – 0	03	3 – 0 – 0	03	V
216H02T502	Cyber Security & Forensics - Case-Studies and Tools	0 – 0 - 2	02	0 – 0 - 2	02	V
216H02C601	Secure Coding	3 – 0 – 0	03	3 – 0 – 0	03	VI
216H02L601	Secure Coding Laboratory	0 – 2 – 0	02	0 – 1 – 0	01	VI
216H02C701	Vulnerability Assessment and Penetration Testing	3 – 0 – 0	03	3 – 0 – 0	03	VII
216H02T701	Vulnerability Assessment and Penetration Testing Lab	0 – 0 – 2	02	0 – 0 – 2	02	VII
	Total	**12 – 04 – 4**	**20**	**12 – 2 – 4**	**18**	

Proposed Examination Scheme

Course Code	Course Name	Examination Scheme				
		Marks				
		CA		ESE[$]	Lab/ Tut CA	Total
		ISE	IA			
216H02C401	Applied Cryptography	30	20	50	-	100
216H02L401	Applied Cryptography Laboratory	-	-	-	50	50
216H02C501	Cyber Forensics and Laws	30	20	50	–	100
216H02T502	Cyber Security & Forensics - Case-Studies and Tools	-	-	-	50	50
216H02C601	Secure Coding	30	20	50	-	100
216H02L601	Secure Coding Laboratory	-	-	-	50	50
216H02C701	Vulnerability Assessment and Penetration Testing	30	20	50	-	100
216H02T701	Vulnerability Assessment and Penetration Testing Lab	-	-	-	50	50
Total		**120**	**80**	**200**	**200**	**600**

Course Code	Name of the Course			
216H02C401	Applied Cryptography			
Teaching Scheme (Hrs./Week)	TH	P	TUT	Total
	03	--	--	03
Credits Assigned	03	--	--	03

Evaluation Scheme	Marks				
	LAB/TUT CA	CA (TH)		ESE	Total
		ISE	IA		
	--	30	20	50	100

Course prerequisites (if any):

Some mathematical maturity, in terms of understanding and working with mathematical definitions, concepts, and proofs, and elementary notions of logic, set theory, number theory, probability and statistics

Course Objectives

In the era of Digital Computers and internet ensuring confidentiality, authentication, integrity of data during communication is very critical. This course impart students the knowledge of cryptographic algorithms and techniques to achieve same. It also introduces students to the advances in the area of cryptography.

Course Outcomes

At the end of successful completion of the course the student will be able to

CO1	Discuss fundamentals of Information Security and cryptography
CO2	Demonstrate and implement various Cryptographic Algorithms for securing systems
CO3	Comprehend cryptographic hash functions, Message Authentication Codes and Digital Certificates and their uses for Authentication
CO4	Realize advances in the field of cryptography

Module No.	Unit No.	Details	Hrs.	CO
1	**Introduction to Information Security & Cryptography**		07	CO 1
	1.1	Information Security and its goals, Vulnerability Threats and Attacks, Security services and security mechanisms		
	1.2	Encryption and Decryption, Symmetric and Asymmetric Key Cryptography, Types of keys, Cryptanalysis methods		
	1.3	Classical Cryptography: Substitution and Transposition encryption Techniques		
	#Self Learning: Cryptanalysis of substitution ciphers, The Adventure of the Dancing Men - Short story by Sir Arthur Conan Doyle			
2	**Cryptographic Arithmetic and Key management**		08	CO2
	2.1	Cryptographic Arithmetic: Modular arithmetic, additive and multiplicative inverse, set of residues, Extended Euclidean Algorithm		
	2.2	Mathematics for Asymmetric key cryptography: Prime generation, primality testing, prime factorization, Euler Totient function		
	2.3	**Key management:** Generating Keys, Nonlinear Keyspaces, Transferring Keys, Verifying Keys, Using Keys, Updating Keys, Storing Keys, Backup Keys, Compromised Keys, Lifetime of Keys, Destroying Keys, Public-Key Key Management		
	2.4	**Key exchange algorithm**: Diffie Hellman Key exchange, Man-in Middle attack		
	#Self Learning : IBM Secret-Key Management Protocol, Key Exchange Algorithms: Shamir's Three-Pass Protocol, Conference Key Distribution and Secret Broadcasting			
3	**Symmetric Key Cryptography**		07	CO2
	3.1	Building blocks of modern and classical Block Ciphers: P box, S Box, EX-OR operations, circular shifts, swaps, split and combine, Rounds, Initialization vectors, Confusion, Diffusion, Fiestel Ciphers, Non-Fiestel ciphers		
	3.2	**DES**: DES Structure, DES Analysis: Properties, Design Criteria, DES Strength and Weaknesses, DES Security, Multiple DES, 3DES		
	3.3	**AES**: AES Structure, Transformations, Key Expansion Analysis of AES: Security, Implementation, Simplicity and Cost		
	#Self Learning –RC5, Classical Block Cipher Modes			
4	**Asymmetric Key Cryptography**		07	CO2
	4.1	**Public key cryptography:** Principles of public key cryptosystems, The RSA algorithm, attacks on RSA,		

	4.2	Introduction to Elliptic Curve Cryptosystems as improvement over RSA, ECC as discrete logarithmic problem		
	#Self Learning : Rabin Cryptosystem			
5	**Message Authentication and Digital Signatures**		**09**	**CO3**
	5.1	Overview of Authentication mechanisms: Biometrics, challenge response systems, one time pads, passwords, multi-factor authentication, token based authentication, single sign-on, Kerberos, PKI, etc Using Symmetric and Asymmetric Encryption for : Authentication, confidentiality, non-repudiation		
	5.2	Hash : Cryptographic Hash Function, Hash Function Requirements, Hash function attacks, Birthday Paradox SHA-512, HMAC Message Authentication Code (MAC), Digital Authentication Algorithm (DAA)		
	5.3	PKI: Roles - responsibilities of Certification Authority and Registration Authority, Applications of PKI, Digital certificates. Using Public Key for Authentication, Digital Signatures, Properties of Digital Signatures beyond Message Authentication, DSS, Authentication Applications: X.509 Authentication Service, Kerberos		
	#Self Learning : RSA and Schnorr Digital Signature MD5 for non cryptographic applications, Challenge Handshake Authentication Protocol (CHAP), Extensible Authentication Protocol (EAP)			
6	**Introduction to Advances in Cryptography**		**07**	**CO4**
	6.1	Quantum Cryptography, Quantum key distribution-QKD		
	6.2	Homomorphic Encryption		
	6.3	Secure Multi-Party Computation (MPC), Zero-Knowledge Proofs		
	5.4	Cryptographic Obfuscation		
		Total	**45**	

Students should prepare all Self Learning topics on their own. Self-learning topics will enable students to gain extended knowledge of the topic. Assessment of these topics may be included in IA and Laboratory Experiments.

Recommended Books:

Sr. No.	Name/s of Author/s	Title of Book	Name of Publisher with country	Edition and Year of Publication
1.	Behrouz A. Forouzan	Cryptography and Network Security	Mc Graw Hill	3rd Edition, 2017
2.	William Stallings	Computer Security Principles and Practice	Pearson Education	2016. 5th Edition
3.	Bruce Schneier	Applied Cryptography	Wiley	2015, Second Edition
4.	Mark stamp	Information Security Principal and Practice	Wiley	2008, 3rd Edition
5.	Jaydip Sen	Theory and practice of cryptography and network security protocols and technologies	Intech Publishers, Croatia, Europe	2013. First Edition
6.	Oded Goldreich	Foundations of Cryptography – A Primer	Foundations and Trends® in Theoretical Computer Science: Vol. 1: No. 1, pp 1-116	2005

Course Code	Name of the Course			
216H02L401	Applied Cryptography Laboratory			
Teaching Scheme (Hrs./Week)	TH	P	TUT	Total
	--	02	--	02
Credits Assigned	--	01	--	01
Evaluation Scheme	Marks			
	LAB/TUT CA	CA (TH)		ESE / Total
		ISE	CA	
	50	--	--	-- / 50

Laboratory Suggestions:

Since this is an introductory course in CSF, the experiments should be a blend of programming, tools, libraries and virtual labs. Experiments relevant with course concepts needing programming skills appropriate for sem III or some applications those could use some libraries related to cryptographic concepts

Laboratory will consist of experiments covering entire syllabus of the course "Applied Cryptography". Students will be graded based on continuous assessment of laboratory work.

Course Code	Course Title			
216H02C501	Cyber Forensics & Laws			
	TH	P	TUT	Total
Teaching Scheme(Hrs.)	03	--	--	03
Credits Assigned	03	--	--	03

Examination Scheme	Marks				
	LAB/TUT CA	CA (TH)		ESE	Total
		IA	ISE		
	--	20	30	50	100

Course prerequisites: Fundamentals of Cryptography, Computer Organization & Architecture.

Course Objectives:

The objective of the course is to enable students to understand the basic principles of cyber security, computer crimes and methods of defense. The course introduces the process of digital forensic investigation, extraction of evidences using appropriate tools. It covers the techniques of data hiding, recovery, disk analysis, volatile data extraction. Further, it explores different network based attacks, tools to monitor/mitigate such attacks. Tools such as metasploit, interfaces to dark web and deep web explore the conducive environment for attackers. Cyber laws, IT Acts enable the student to understand the legal aspects of various cyber-crimes.

Course Outcomes

At the end of successful completion of the course the student will be able to

CO 1: Understand the fundamentals of security framework.

CO 2: Apply security principles & tools for computer and mobiles to protect their devices.

CO 3: Understand the fundamentals of digital forensics & investigation process.

CO 4: Apply forensic tools to extract and investigate the evidences from network.

CO 5: Relate the corresponding computer security laws and acts in the digital space.

Module No.	Unit No.	Details	Hrs.	CO
1	**Introduction to Cyber Security Framework.**		06	CO 1
	1.1	Introduction to security architecture, goals, attack vectors, methods of defense.		
	1.2	Cybercrime, types of cybercrimes, Regulation of cyberspace, cyberspace framework, Issues and challenges of cyber security.		
	1.3	Cybercrime on Social Media - Security and Privacy management, ATM based frauds & other digital frauds.		
2	**Digital Device Security.**		09	CO 2
	2.1	End Point device and Mobile phone security, Password policy, Security patch management, electronic evidence and handling, electronic media, collection, searching and storage of electronic media.		
	2.2	Data backup, Downloading and management of third party software, Device security policy.		
	2.3	Cyber Security best practices, Significance of host firewall and Ant-virus, Management of host firewall and Anti-virus, Wi-Fi security, Configuration of basic security policy and permissions, Data privacy.		
	#Self Learning - GDPR Compliance.			
3	**Digital Forensics Fundamentals**		10	CO 3
	3.1	Introduction, six A's of digital forensics, digital evidence, digital investigations, incident response, incident response methodology.		
	3.2	Classification of digital evidence - volatile and non-volatile, rules and guidelines for extraction of digital evidence, forensic duplicates, establishing chain of custody, admissibility of evidence in the court of law.		
	3.3	Information retrieval and recovery, cloning techniques, password cracking, data recovery from file systems and mobile devices, forensics audit, tools for forensic investigation - Encase, Helix, FTK, Autopsy, Sleuth kit Forensic Browser, FIRE, Found stone Forensic ToolKit, Win Hex, Linux dd and other open source tools, anti-forensics.		
	#Self Learning – CERT and its role in digital investigation.			
4	**Network Forensics**		14	CO 4
	4.1	Network based attacks – MITM, OWASP, ARP spoofing, IP and MAC spoofing, DNS attacks, SYN flooding attacks, port scanning, DOS, DDOS etc.		
	4.2	Network traffic log analysis, Network Monitors, Network Forensics – acquisition of real time evidence, process and guidelines for evidence handling on networks.		
	4.3	E-mail in Investigations, roles of the Client and Server in E-mail, Investigating E-mail based Crimes and Violations, Examination of E-mail Messages, E-mail Headers, and Additional E-mail Files, Tracing an E-mail Message, Network E-mail Logs, E-mail Forgery and Tracking.		

	4.4	Network Forensic Tools & Applications – Browser forensics, Nmap, Nessus, Wireshark, Metasploit, Kali-Linux, Deep-Web, Dark-Web.		
	#Self Learning : Network forensic cases studies.			
5	**Cyber Laws & Acts.**		**06**	**CO 5**
	5.1	Introduction to cyber ethics, Software Piracy, Intellectual Property, IP Theft, Copyright, Trademark, Privacy and Censorship.		
	5.2	Indian laws – Information Technology (IT) Act 2000, IT Amendment Act 2008, National Cyber Security Strategy 2020, The Digital Personal Data Protection Act of 2023 (DPDP).		
	#Self Learning : Network forensic cases studies.			
		Total	**45**	

- Instructor needs to provide additional resources to students for in-depth understanding and practical applicability of the indicated topic/topics.

Recommended Books:

Sr. No.	Name/s of Author/s	Title of Book	Name of Publisher with country	Edition and Year of Publication
1.	Marie-Helen Maras	*Computer Forensics: Cybercriminals, Laws and Evidences*	Jones and Bartlett Learning	2nd Edition, 2014
2.	Bill Nelson Amelia Phillips Christopher Steuart.	*Guide to Computer Forensics and Investigations*	Course Technology, Cengage Learning, USA	4th Edition, 2010
3.	Jason T. Luttgens, Mathew Pepe, Kevin Mandia	*Incident Response and Computer Forensics.*	Tata McGraw Hill Education	3rd Edition, 2014.
4.	Nina Godbole, Sunit Belapure,	*Cyber Security- Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*	Wiley- India	2011
5.	Davidoff Ham	Network Forensics Tracking Hackers through Cyberspace	Pearson, India	1st Edition, 2013.
6.	Cory Altheide, Harlan Carvey	*Digital Forensics with Open Source Tools*	Syngress, Elsevier, USA	2011

Course Code	Course Title			
216H02T502	Cyber Security & Forensics - Case-Studies and Tools			
	TH	P	TUT	Total
Teaching Scheme(Hrs.)	--	--	02	02
Credits Assigned	--	--	02	02

Examination Scheme	Marks				
	LAB/TUT CA	CA (TH)		ESE	Total
		IA	ISE		
	50	--	--	--	50

Course prerequisites: Basic fundamentals of Computer Systems, Operating Systems, Networks & Cryptography.

Course Objectives: The objective of this course is to provide the student with hands-on knowledge of different tools and techniques used for investigations of cyber forensic incidents. The course covers different experimentation in the domain of Digital Forensics & Investigations, Data hiding and carving techniques, Network Forensics using different tools & techniques.

Course Outcomes:

At the end of successful completion of the course the student will be able to :

CO 1: Determine & analyze software vulnerabilities, security solutions to reduce the risk of exploitation.

CO 2: Understand the process of identifying digital evidence and its analysis.

CO 3: Identify & apply appropriate forensic tools & techniques for investigation of the incidents.

CO 4: Apply different fingerprint techniques on digital assets.

CO 5: Explore advanced forensic and anti-forensic techniques.

Module No.	Unit No.	Details	Hrs.	CO
1	**Cybersecurity and Forensics**		**04**	**CO 1**
		Introduction to Forensic Tools and Techniques, Case Study Analysis: Historical Cybersecurity Breaches Hands-on Lab: Setting Up Forensic Environment		
		Case studies		
2	**Digital Evidence and Analysis**		**08**	**CO 2**
		Tools and Techniques for Evidence Collection Data Recovery and Repair Forensic Imaging and Hashing Hands-on Lab: Evidence Collection Practice Practical Exercise: Creating Forensic Images of Storage Devices		
		Case studies		
3	**Forensics#**		**08**	**CO 3**
		Network Forensics Memory Forensics and Volatile Data Analysis Case Study: Memory Analysis in Incident Response Steganography Detection Email forensics Social media forensics Incident response forensics Live Forensics Tools		
		Case studies		
4	**Digital fingerprinting**		**06**	**CO 4**
		Digital fingerprinting Device Fingerprinting Browser Fingerprinting Network Fingerprinting Operating System Fingerprinting User Fingerprinting		
		Case studies		
5	**Advanced concepts in forensics**		**04**	**CO 5**
		Anti-Forensics tools and Techniques Counter-Forensics and Mitigation Strategies		
		Case studies		
		Total	**30**	

#students should explore some forensics on their own while some can be conducted during laboratory session

Course Code	Name of the Course			
216H02C601	Secure Coding			
Teaching Scheme (Hrs./Week)	TH	P	TUT	Total
	03	--	--	03
Credits Assigned	03	--	---	03
Evaluation Scheme	Marks			
	LAB/TUT CA	CA (TH)		ESE	Total
		IA	ISE		
	--	20	30	50	100

Course pre-requisites:
Knowledge of programming languages, cryptography, web development

Course Objectives:
By the end of this course, students should have a comprehensive understanding of secure programming principles, architecture, design, coding practices, and testing methodologies. They should be able to apply this knowledge to develop secure software and mitigate vulnerabilities effectively.

Course Outcomes (CO):
1. Understand secure coding best practices, procedures, policies and software vulnerabilities
2. Design software applications using secure architecture concepts
3. Development of secure software application
4. Understand and incorporate various secure software development frameworks and maturity models.

Module No.	Unit No.	Contents	No of Hrs.	CO
1	**Introduction**		07	CO1
	1.1	The Philosophy of Secure Programming, Defining Secure Programming, Robust vs. Secure Programming, Security Policies and Procedures, Secure Programming General Philosophy, Where to Look for Vulnerabilities, Secure Programming best practices,		
	1.2	Vulnerabilities in various programming languages, Vulnerabilities in various domains: Web Application, Mobile Applications and Database Applications Dangers of Vulnerable Components/Programs		
	1.3	Understanding secure SDLC model, Methodologies for developing secure code: Risk analysis, threat modelling, and guidelines for secure coding practice.		
2	**Secure architecture and Principles of secure designing**		06	CO2
	2.1	What is security architecture?		
	2.2	Principles of security architecture, principles of secure software development, case study: Java sandbox		
	2.3	Secure design steps, Secure deployment and maintenance, Security Auditing		
3	**Secure Design and Implementation**		10	CO2
	3.1	Security requirements in application software, Security Technical reference model (TRM)		
	3.2	Secure Design steps, Special design issues, Software design considerations for security and resilience; Good and bad practises in secure design, case studies		
	3.3	Security requirements, security framework, Good and bad Practises in implementation, case studies		
4	**Software development and security test cases**		12	CO3
	4.1	Vulnerabilities and controls : mobile application development, web based application development, cross domain application developement.		
	4.2	Secure coding practices, Cryptographic libraries and tools for secure coding		
	4.3	Standardized testing policy, security requirements, security testing, Secure testing approach,		
	4.4	Security test cases for : identification requirements, authentication requirements, authorization requirements, confidentiality requirements, integrity requirements, availability requirements, non-repudiation requirements, system maintenance security requirements		
	4.5	Manual source code review, Automated source code analysis Manual and automated tools for code review and analysis		

5	**Secure Coding Maturity Models and framework**		10	CO4
	5.1	Secure Software Development Framework (SSDF), OWASP's application security verification standard, Open Software Assurance Maturity Model (OpenSAMM), Building Security In Maturity Model (BSIMM)		
	5.2	Case studies		
		Total	45	--

Reference Books :

Sr. No	Name/s of Author/s	Title of Book	Publisher	Edition/Year
1	Mark G. Graaff, Kenneth R. van Wyk	Secure Coding: Principles and Practices	O'Reilly	2003, First Edition
2	Mark Merkow, Lakshmikanth Raghvan	Secure and Resilient software: Requirements, test cases and testing methods	CRC Press	2012
3	Michael Howard, David LeBlanc	Writing secure code	Microsoft Press	Second Edition
4	Neil Daswani, Christoph Kern, and Anita Kesavan.	Foundations of Security	Apress	2007,First Edition
5				
1.	Best Practises for secure coding, https://safecomputing.umich.edu/protect-the-u/protect-your-unit/secure-coding/best-practices, last retrieved on Dec 13,2023			
0.	OWASP Top 10 Mobile Vulnerabilities Developers Need to Understand, https://www.cypressdatadefense.com/blog/owasp-mobile-top-10-vulnerabilities/, last retrieved on Dec 13,2023			
0.	41 Common Web Application Vulnerabilities Explained, "https://securityscorecard.com/blog/common-web-application-vulnerabilities-explained", last retrieved on Dec 13,2023			
0.	OWASP Top Ten, "https://owasp.org/www-project-top-ten/", last retrieved on Dec 13,2023			

Course Code	Name of the Course
216H02L601	Secure Coding Laboratory

Teaching Scheme (Hrs./Week)	TH	P	TUT	Total
	--	02	--	02
Credits Assigned	--	01	--	01

Evaluation Scheme	Marks				
	LAB/TUT CA*	CA (TH)		ESE	Total
		IA	ISE		
	50	--	--	--	50

LAB/TUT CA:

***LAB/TUT CA is an evaluation carried out during the said laboratory/tutorial throughout the semester on a continuous basis. In case of Laboratory, it can be a combination of laboratory experiments performed (at least 8-10), written record of experiments (Journal), Viva/On-screen test and/or Quiz, programming assignments (wherever applicable) and practical examination (if any) conducted during the semester. In case of tutorial, it can be a combination of graded assignments, group/individual activities such as presentations, group discussion, report writing etc. (as applicable).**

Please note:

- The total marks assigned for Continuous Assessment (LAB/TUT) as per scheme can be distributed in a number of components as given above.
- Course coordinator should decide the rubrics/distribution of marks for different components in consultation with all other faculty teaching the same course.
- The rubrics/distribution should be uniform for all batches.
- The rubrics/distribution should be communicated to all students at the beginning of the semester.

Course Code	Name of the Course			
216H02C701	Vulnerability Analysis and Penetration Testing			
Teaching Scheme (Hrs./Week)	TH	P	TUT	Total
	03	--	--	03
Credits Assigned	03	--	--	03

Evaluation Scheme	Marks				
	LAB/TUT CA	CA (TH)		ESE	Total
		IA	ISE		
	--	20	30	50	100

Course pre-requisites:
Knowledge of Networking and System Programming

Course Objectives:
The objective of this course is to impart knowledge about the principles and techniques associated with the information and cybersecurity practice known as penetration testing or ethical hacking. The topics covered in the course are the entire penetration testing process including planning, reconnaissance, scanning, exploitation, post exploitation, and result reporting.

Course Outcomes (CO):
1. Understand penetration testing with scope of its ethical implications, documentation, and reporting.
2. Perform Penetration testing and vulnerability assessment on various systems.
3. Comprehend post exploitation phase of penetration testing.
4. Apply unique techniques to gather exploitation intelligence, identify risk and demonstrate impact with Red Team and Blue Team strategies

Module No.	Unit No.	Contents	No of Hrs.	CO
1	**Introduction to Penetration Testing**		4	C01
	1.1	Introduction to Penetration testing, Ethics, Laws.		
	1.2	Types of Penetration Testing, Phases of Penetration Testing.		
	1.3	Setting up a Penetration Lab		
	Self Study: Kali Linux, Parrot OS			
2	**Information Gathering/ Footprinting**		9	CO2
	2.1	Reconnaissance: Passive Information gathering with Foot printing, Active Information Gathering, Open Service Information Gathering		
	2.2	Network Scan: Passive and active Network Scan, Port Scanning, ARP Spoofing, Network Traffic Scanning.		
	2.3	OS Fingerprinting		
	Self Study: Maltego, Recon-ng, NMAP			
3	**Identification of Vulnerability and Exploits**		14	CO3
	3.1	Understanding Vulnerabilities		
	3.2	Buffer Overflow Exploitation		
	3.3	Fuzzing		
	3.4	Searching for Exploits		
	3.5	System Hacking		
	3.6	Post Exploitation and Covering tracks		
	3.7	Privilege Escalation Exploits (Windows and Linux)		
	3.8	Port Redirection and Tunnelling		
4	**Exploitation and Professional Reporting**		10	CO3
	4.1	ARP Spoofing, MITM and Session Hijacking		
	4.2	Shell Script Exploitation		
	4.3	Password Cracking: Exploring Hydra and John the Ripper		
	4.4	Metasploit Framework: Metasploit User Interfaces, Setting up Metasploit Framework, Exploring the Metasploit Framework		
	4.5	Preparing Report and Presenting Findings		
5	**Security Landscape, Red Team, and Blue Team**		8	CO4
	5.1	Incident Response Process		
	5.2	Red Team and Blue Team		
	5.3	Red Team Operations		
	5.4	Blue Team Défense		
		Total	45	--

Reference Books :

Sr. No	Name/s of Author/s	Title of Book	Publisher	Edition/Year
1	Georgia Weidman	Penetration Testing: A Hands-On Introduction to Hacking	No Starch Press	1st Edition, 2014
2	George Kurtz, Joel Scambray, and Stuart McClure	Hacking Exposed 7: Network Security Secrets and Solutions	McGraw Hill	2012
3	Rafay Baloch	Ethical Hacking and Penetration Testing Guide	CRC Press	2015
4	Peter Kim	The Hacker Playbook 2	Secure Planet LLC	2015
5	Micah Zenko	Red Team How to Succeed by Thinking Like the Enemy	Basic Books	2015
6	Don Murdoch GSE	Blue Team Handbook: A Condensed Field Guide for the Cyber Security Incident Responder	Createspace Independent Publishing Platform	2014

*In addition to printed books, faculty can suggest (authentic) URL's or e-books, e-contents etc.

Course Code	Name of the Course
216H02C701	Vulnerability Analysis and Penetration Testing Tutorial

Teaching Scheme (Hrs./Week)	TH	P	TUT	Total
	--	--	02	02
Credits Assigned	--	--	02	02

Evaluation Scheme	Marks				
	LAB/TUT CA*	CA (TH)		ESE	Total
		IA	ISE		
	50	--	--	--	50

LAB/TUT CA:

***LAB/TUT CA is an evaluation carried out during the said laboratory/tutorial throughout the semester on a continuous basis. In case of Laboratory, it can be a combination of laboratory experiments performed (at least 8-10), written record of experiments (Journal), Viva/On-screen test and/or Quiz, programming assignments (wherever applicable) and practical examination (if any) conducted during the semester. In case of tutorial, it can be a combination of graded assignments, group/individual activities such as presentations, group discussion, report writing etc. (as applicable).**

Please note:

- The total marks assigned for Continuous Assessment (LAB/TUT) as per scheme can be distributed in a number of components as given above.
- Course coordinator should decide the rubrics/distribution of marks for different components in consultation with all other faculty teaching the same course.
- The rubrics/distribution should be uniform for all batches.
- The rubrics/distribution should be communicated to all students at the beginning of the semester.