UNIVERSITY OF MUMBAI

Syllabus

Honours/ Minor Degree Program

in

Cyber Security

FACULTY OF SCIENCE & TECHNOLOGY

(As per AICTE guidelines with effect from the academic year 2022-2023)

University of Mumbai Cyber Security (With effect from 2022-23)										
Year & Sem	Course Code and Course Title	Teaching Scheme Hours / Week			Examination Scheme and Marks					Credit Scheme
		Theory	Seminar/ Tutorial	Pract	Internal Assessment	End Sem Exam	Term Work	Oral/ Pract	Total	Credits
TE Sem V	**HCSC501: Ethical Hacking**	04	--	--	20	80	--	--	100	04
	Total	**04**	**-**	**--**	**100**		**-**	**-**	**100**	**04**
										Total Credits = 04
TE Sem. VI	**HCSC601: Digital Forensic**	04	--	--	20	80	--	--	100	04
	Total	**04**	**-**	**-**	**100**		**-**	**-**	**100**	**04**
										Total Credits = 04
BE Sem. VII	**HCSC701: Security Information Management**	04	--	--	20	80	--	--	100	04
	HCSSBL601: Vulnerability Assessment Penetration Testing (VAPT) Lab (SBL)	--	--	04	--	--	50	50	100	02
	Total	**04**	**-**	**04**	**100**		**50**	**50**	**200**	**06**
										Total Credits = 06
BE Sem. VIII	**HCSC801: Application Security**	04	-	--	20	80	--	--	100	04
	Total	**04**	**-**	**-**	**100**		**-**	**-**	**100**	**04**
										Total Credits = 04
Total Credits for Semesters V,VI, VII &VIII = 04+04+06+04=18										

Cyber Security: Sem V								
Course Code	**Course Title**	**Theory**	**Practical**	**Tutorial**	**Theory**	**Practical/Oral**	**Tutorial**	**Total**
HCSC501	**Ethical Hacking**	**04**	**--**	**--**	**04**	**--**	**--**	**04**

Course Code	**Course Title**	**Examination Scheme**							
		Theory Marks				**Term Work**	**Practical**	**Oral**	**Total**
		Internal assessment			**End Sem. Exam**				
		Test1	**Test 2**	**Avg.**					
HCSC501	**Ethical Hacking**	**20**	**20**	**20**	**80**	**--**	**--**	**--**	**100**

Course Objectives:

Sr. No.	**Course Objectives**
The course aims:	
1	To describe Ethical hacking and fundamentals of computer Network.
2	To understand about Network security threats, vulnerabilities assessment and social engineering.
3	To discuss cryptography and its applications.
4	To implement the methodologies and techniques of Sniffing techniques, tools, and ethical issues.
5	To implement the methodologies and techniques of hardware security.
6	To demonstrate systems using various case studies.

Course Outcomes:

Sr. No.	**Course Outcomes**	**Cognitive levels of attainment as per Bloom's Taxonomy**
On successful completion, of course, learner/student will be able to:		
1	Articulate the fundamentals of Computer Networks, IP Routing and core concepts of ethical hacking in real world scenarios.	L1,L2
2	Apply the knowledge of information gathering to perform penetration testing and social engineering attacks.	L3
3	Demonstrate the core concepts of Cryptography, Cryptographic checksums and evaluate the various biometric authentication mechanisms.	L1,L2
4	Apply the knowledge of network reconnaissance to perform Network and web application-based attacks.	L3
5	Apply the concepts of hardware elements and endpoint security to provide security to physical devices.	L3
6	Simulate various attack scenarios and evaluate the results.	L4,L5

DETAILED SYLLABUS:

Sr. No.	**Module**	**Detailed Content**	**Hours**	**CO Mapping**
0	**Prerequisite**	Computer Networks, Databases, system security	**2**	-

I	**Introduction to Ethical Hacking**	Fundamentals of Computer Networks/IP protocol stack, IP addressing and routing, Routing protocol, Protocol vulnerabilities, Steps of ethical hacking, Demonstration of Routing Protocols using Cisco Packet Tracer **Self-learning Topics**:TCP/IP model, OSI model	**10**	CO1
II	**Introduction to Cryptography**	Private-key encryption, public key-encryption, key Exchange Protocols, Cryptographic Hash Functions & applications, steganography, biometric authentication, lightweight cryptographic algorithms.Demonstration of various cryptographic tools and hashing algorithms **Self-learning Topics**: Quantum cryptography, Elliptic curve cryptography	**08**	CO3
III	**Introduction to network security**	Information gathering, reconnaissance, scanning, vulnerability assessment, Open VAS, Nessus, System hacking: Password cracking, penetration testing, Social engineering attacks, Malware threats, hacking wireless networks (WEP, WPA, WPA-2), Proxy network, VPN security, Study of various tools for Network Security such as Wireshark, John the Ripper, Metasploit, etc. **Self-learning Topics**: Ransomware(Wannacry), Botnets, Rootkits, Mobile device security	**12**	CO2
IV	**Introduction to web security and Attacks**	OWASP, Web Security Considerations, User Authentication, Cookies, SSL, HTTPS, Privacy on Web, Account Harvesting, Web Bugs, Sniffing, ARP poisoning, Denial of service attacks, Hacking Web Applications, Clickjacking, Cross-Site scripting and Request Forgery, Session Hijacking and Management, Phishing and Pharming Techniques, SSO, Vulnerability assessments, SQL injection, Web Service Security, OAuth 2.0, Demonstration of hacking tools on Kali Linux such as SQLMap, HTTrack, hping, burp suite,Wireshark etc. **Self-learning Topics**: Format string attacks	**10**	CO4
V	**Elements of Hardware Security**	Side channel attacks, physical unclonable functions, Firewalls,Backdoors and trapdoors, Demonstration of Side Channel Attacks on RSA, IDS and Honeypots. **Self-learning Topics**: IoT security	**6**	CO5
VI	**Case Studies**	Various attacks scenarios and their remedies. Demonstration of attacks using DVWA. **Self-learning Topics**: Session hijacking and man-in-middle attacks	**4**	CO6

Text Books:

1. Computer Security Principles and Practice --William Stallings, Seventh Edition, Pearson Education, 2017

2. Security in Computing -- Charles P. Pfleeger, Fifth Edition, Pearson Education, 2015
3. Network Security and Cryptography -- Bernard Menezes, Cengage Learning, 2014
4. Network Security Bible -- Eric Cole, Second Edition, Wiley, 2011
5. Mark Stamp's Information Security: Principles and Practice --Deven Shah, Wiley, 2009

References:

1.UNIX Network Programming –Richard Steven,Addison Wesley, 2003
2. Cryptography and Network Security -- Atul Kahate, 3rd edition, Tata Mc Graw Hill, 2013
3.TCP/IP Protocol Suite -- B. A. Forouzan, 4th Edition, Tata Mc Graw Hill, 2017
4. Applied Cryptography, Protocols Algorithms and Source Code in C -- Bruce Schneier, 2nd Edition / 20th Anniversary Edition, Wiley, 2015

Online Resources:

Sr. No.	Website Name
1.	https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
2.	https://dvwa.co.uk/
3.	http://testphp.vulnweb.com/

Assessment:

Internal Assessment (IA) for 20 marks:

- IA will consist of Two Compulsory Internal Assessment Tests. Approximately 40% to 50% of syllabus content must be covered in First IA Test and remaining 40% to 50% of syllabus content must be covered in Second IA Test

➢ **Question paper format**

- Question Paper will comprise of a total of **six questions each carrying 20 marks Q.1** will be **compulsory** and should **cover maximum contents of the syllabus**
- **Remaining questions** will be **mixed in nature** (part (a) and part (b) of each question must be from different modules. For example, if Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)
- A total of **four questions** need to be answered