Lesson Plan Cyber Security (HONORS): Ethical Hacking

Subject: Ethical Hacking

Subject code: HCSC501

Teacher-in-charge: Dr. B. S. Daga

Academic Term: July – October 2023

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

Course Objectives:

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:		
HCSC501.1	Demonstrate comprehension of foundational concepts in Computer Networks, IP Routing, and ethical hacking in real-world scenarios. (Understanding)	L1,L2
HCSC501.2	Apply acquired knowledge of information gathering techniques to execute penetration testing and social engineering attacks. (Applying)	L3
HCSC501.3	Evaluate core principles of Cryptography, cryptographic checksums, and diverse biometric authentication mechanisms. (Evaluating)	L1,L2
HCSC501.4	Utilize network reconnaissance expertise to perform attacks on networks and web applications. (Applying)	L3
HCSC501.5	Implement hardware elements and endpoint security concepts to ensure the protection of physical devices. (Applying)	L3
HCSC501.6	Analyze and assess outcomes from simulated attack scenarios. (Evaluating)	L4

CO-PO-PSO Mapping:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
HCSC501.1	1	1												1
HCSC501.2	1	2												2
HCSC501.3	2	1												1
HCSC501.4	1	1												2
HCSC501.5	1	1												2
HCSC501.6	2	1			2									2

Justification of PO to CO mapping:

Course Outcome	Competency	Performance Indicator
HCSC501.1	1.3 Demonstrate competence in engineering fundamentals	1.3.1 Apply engineering fundamentals
HCSC501.2	1.3 Demonstrate competence in engineering fundamentals	1.3.1 Apply engineering fundamentals
	2.1 Demonstrate an ability to identify and formulate complex engineering problem	2.1.2 Identify processes/modules of a computer-based system and parameters to solve a problem
	2.2 Demonstrate an ability to formulate a solution plan and methodology for an engineering problem	2.2.3 Identify existing solution/methods to solve the problem, including forming justified approximations and assumptions.
HCSC501.3	1.3 Demonstrate competence in engineering fundamentals	1.3.1 Apply engineering fundamentals
	1.4 Demonstrate competence in specialized engineering knowledge to the program	1.4.1 Apply theory and principles of Computer Science and engineering to solve
HCSC501.4	1.3 Demonstrate competence in engineering fundamentals	1.3.1 Apply engineering fundamentals
HCSC501.5	1.3 Demonstrate competence in engineering fundamentals	1.3.1 Apply engineering fundamentals
HCSC501.6	1.3 Demonstrate competence in engineering fundamentals	1.3.1 Apply engineering fundamentals
	1.4 Demonstrate competence in specialized engineering knowledge to the program	1.4.1 Apply theory and principles of Computer Science and engineering to solve an engineering problem
	4.2 Demonstrate an ability to design experiments to solve open-ended problems	4.2.1 Design and develop appropriate procedures/methodologies based on the study objectives
	5.2 Demonstrate an ability to select and apply discipline-specific tools, techniques and resources	5.2.2 Demonstrate proficiency in using discipline-specific tools

Justification of CO to PSO mapping:

Course Outcome	Competency	Performance Indicator
HCSC501.1		
HCSC501.2	2.2 Demonstrate an ability to identify potential threats and attacks to the information technology assets.	2.2.2 Identify the flow and methodology of the attacks. 2.2.3 Choose appropriate tools to identify different types of threats and cyber-attacks.
HCSC501.3	2.2 Demonstrate an ability to identify potential threats and attacks to the information technology assets.	2.2.1 Analyse the static and web vulnerabilities.
HCSC501.4	2.2 Demonstrate an ability to identify potential threats and attacks to the information technology assets.	2.2.1 Analyse the static and web vulnerabilities.
	2.3 Demonstrate an ability to identify tools and measures to protect the assets from cyber-attacks.	2.3.1 Identify the defense methodologies and the measures to prevent the attacks and protect assets.
HCSC501.5	2.3 Demonstrate an ability to identify tools and measures to protect the assets from cyber-attacks.	2.3.2 Identify the techniques to detect attacks.
	2.4 Demonstrate an ability to apply the security mechanisms to real-world problems.	2.4.2 Apply measures and tools for protecting the assets.
HCSC501.6	2.2 Demonstrate an ability to identify potential threats and attacks to the information technology assets.	2.2.2 Identify the flow and methodology of the attacks.
	2.3 Demonstrate an ability to identify tools and measures to protect the assets from cyber-attacks.	2.3.2 Identify the techniques to detect attacks.
	2.4 Demonstrate an ability to apply the security mechanisms to real-world problems.	2.4.1 Simulate the solution on a virtual system.

CO Assessment Tools:

Course Outcomes	*Indirect Method (20%)*			
	Unit Test		End Sem Exam	Course Exit Survey
	I	II		
HCSC501.1	40%	--	60%	100%
HCSC501.2	--	40%	60%	100%
HCSC501.3	20%	20%	60%	100%
HCSC501.4	40%	--	60%	100%
HCSC501.5	--	40%	60%	100%
HCSC501.6	--	40%	60%	100%

CO calculation= (0.8 *Direct method + 0.2*Indirect method)

Curriculum Gap identified: (with action plan): Nil

Content beyond syllabus: Nil

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:

1. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
2. https://dvwa.co.uk/
3. http://testphp.vulnweb.com/

Submitted By:	**Approved By**	
Prof. Dr. B. S. Daga	Dr. Sujata Deshmukh	Sign:
Sign:		Sign:
Date of Submission:	**Date of Approval**	