Lesson Plan Cyber Security (HONORS): Ethical Hacking

Subject: Ethical Hacking

Subject code: HCSC501

Teacher-in-charge: Prof. Unik Lokhande

Academic Term: July – October 2022

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	Articulate the fundamentals of Computer Networks, IP Routing and core concepts of ethical hacking in real world scenarios.	L1,L2
HCSC501.2	Apply the knowledge of information gathering to perform penetration testing and social engineering attacks.	L3
HCSC501.3	Demonstrate the core concepts of Cryptography, Cryptographic checksums and evaluate the various biometric authentication mechanisms.	L1,L2
HCSC501.4	Apply the knowledge of network reconnaissance to perform Network and web application-based attacks.	L3
HCSC501.5	Apply the concepts of hardware elements and endpoint security to provide security to physical devices.	L3
HCSC501.6	Simulate various attack scenarios and evaluate the results.	L4,L5

CO-PO-PSO Mapping:

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

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

Lesson Plan

Class	TE Cyber Security (Honors), Sem V		
Academic Term	July- October 2022		
Subject	Ethical Hacking (HCSC501)		
Periods (Hours) Per Week	Lecture	4	
	Practical	N/A	
	Tutorial	N/A	
Evaluation System		**Hours**	**Marks**
	Theory examination	4	80
	Internal Assessment	--	20
	Practical Examination	--	--
	Oral Examination	--	--
	Term work	--	--
	Total	4	100

Time Table	**Day**	**Time**
	Tuesday	8.45AM -9.45AM
	Wednesday	8.45AM -9.45AM
	Thursday	8.45AM -9.45AM
	Friday	8.45AM -9.45AM

Course Content and Lesson plan

Week No.	**Lecture No.**	**Planned Dates**	**Actual Dates**	**Topics to be covered**	**Content Delivery Method/Learning Activities/ Remarks**
1	1	02-08-2022	02-08-2022	Fundamentals of Computer Networks/IP protocol stack,	Black Board, PPT
	2	03-08 -2022	03-08 -2022	Proxy network, VPN security	Black Board, PPT
	3	04-08 -2022	04-08 -2022	IP addressing and routing, Routingprotocol	Black Board, PPT
	4	05-08 -2022	05-08 -2022	Wireshark Demo, John the Ripper Demo	Black Board, PPT, Demonstration
2	5	10-08 -2022	10-08 -2022	Metasploit Demo	Black Board, PPT
	6	11-08 -2022	11-08 -2022	Protocol vulnerabilities	Black Board, PPT
	7	12-08 -2022	12-08 -2022	OWASP, Web Security Considerations,	Black Board, PPT
3	8	17-08 -2022	17-08 -2022	User Authentication	Black Board, PPT
	9	18-08 -2022	18-08 -2022	Steps of ethical hacking, Demonstration of Routing Protocols using Cisco Packet Tracer	Black Board, PPT
	10	19 -08 -2022	24-08 -2022	Cookies, SSL	Black Board, PPT

4	11	23 -08 -2022	23 -08 -2022	Private-key encryption, public key encryption	Black Board, PPT
	12	24 -08 -2022	26-08 -2022	HTTPS, Privacy on Web,	Black Board, PPT
	13	25 -08 -2022	25 -08 -2022	key Exchange Protocols,	Black Board, PPT
	14	26 -08 -2022	07 -09 -2022	Account Harvesting, Web Bugs, Sniffing, ARP poisoning	Black Board, PPT
5	15	30 -08 -2022	30 -08 -2022	Cryptographic Hash Functions & applications	Black Board, PPT
	16	01-09 -2022	08 –09-2022	Steganography, biometric authentication	Black Board, PPT
	17	02 -09 -2022	09 -09 -2022	Denial of service attacks, Hacking Web Applications, Clickjacking	Black Board, PPT
6	18	08 -09 -2022	08 –09-2022	Lightweight cryptographic algorithms	Black Board, PPT
	19	09 -09 -2022	09 -09 -2022	Cross-Site scripting and Request Forgery	Black Board, PPT
7	20	13 -09 -2022	13 –09-2022	Demonstration of various cryptographic tools	Black Board, PPT
	21	14 -09 -2022	21-09 -2022	Session Hijacking and Management, Phishing and Pharming Techniques,	Black Board, PPT
	22	15 -09 -2022	15 -09 -2022	Hashing algorithms	Black Board, PPT
	23	16 -09 -2022	23-09 -2022	SSO, OAuth 2.0	Black Board, PPT
8	24	20 -09 -2022	20 -09 -2022	Hashing algorithms	Black Board, PPT
	25	21 -09 -2022	28-09 -2022	SQL injection, Demonstration of SQL Map.	Black Board, PPT, Demonstration
	26	22 -09 -2022	22 -09 -2022	Information gathering, Reconnaissance	Black Board, PPT
	27	23 -09 -2022	30 -09 -2022	Vulnerability assessments, Web Service Security	Black Board, PPT
9	28	27 -09 -2022	27 -09 -2022	Information gathering, Reconnaissance	Black Board, PPT
	29	28 -09 -2022	07 -10 -2022	Demonstration of hacking tools on Kali Linux (HTTrack, hping, burp suite)	Demonstration
	30	29 -09 -2022	29 -09 -2022	Scanning tools	Black Board, PPT
	31	30 -09 -2022	12 -10 -2022	Side channel attacks, physical unclonable functions	Black Board, PPT
10	32	04-10 -2022	04-10 -2022	UT1 Remedial	Black Board, PPT
	33	06 -10 -2022	06 -10 -2022	Open VAS,	Demonstration, Black Board, PPT
	34	07 -10 -2022	14 -10 -2022	Firewalls-I	Black Board, PPT
11	35	11 -10 -2022	11 -10 -2022	Vulnerability assessment	Black Board, PPT
	36	12 -10 -2022	14 -10 -2022	Firewalls-II	Black Board, PPT

	37	13 -10 -2022	13 -10 -2022	System hacking: Password cracking	Demonstration, Black Board, PPT
	38	14 -10 -2022	21 -10 -2022 Online Mode	Backdoors and trapdoors, Attacks on RSA	Google meet, PPT
12	39	20 -10 -2022	20 -10 -2022	Nessus	Black Board, PPT
	40	21 -10 -2022	21 -10 –2022 Online Mode	IDS and Honeypots.	Google meet, PPT
13	41	25 -10 -2022	25 -10 -2022	Social engineering attacks	Black Board, PPT
	42	27 -10 -2022	30-10 -2022 Online Mode	Various attacks scenarios and their remedies. (Buffer Overflow and DOS)	Google meet, PPT
	43	28 -10 -2022	28 -10 -2022	Social engineering attacks	Black Board, PPT
14	44	1-11 -2022	1-11 -2022	UT2 remedial	Black Board, PPT
	45	2-11 -2022	30-10-2022 Online Mode	Demonstration of attacks using DVWA. (Buffer Overflow, Slowloris and Social Engineering Toolkit)	Demonstration, Google meet, PPT
	Total:45				

Submitted By:	**Approved By**	
Prof. Unik Lokhande Sign:	Dr. Sujata Deshmukh	Sign:
	Dr. B. S. Daga	Sign:
	Prof. Merly Thomas	Sign:
	Prof Monica Khanore	Sign:
	Prof. Roshni Padate	Sign:
	Prof. Kalpana Deorukhkar	Sign:
Date of Submission:	**Date of Approval**	