THIRD-YEAR OF BACHELOR OF COMPUTER SCIENCE REVISED SYLLABUS ACCORDING TO CBCS

COURSE TITLE: ETHICAL HACKING

SEMESTER-V, W.E.F. 2021-2022

Recommended by the Board of Studies in Computer Science
And
Approved by the Academic Council

Devrukh Shikshan Prasarak Mandal's
Nya. Tatyasaheb Athalye Arts, Ved. S. R. Sapre Commerce, and Vid. Dadasaheb Pitre Science College (Autonomous), Devrukh.
Tal. Sangameshwar, Dist. Ratnagiri-415804, Maharashtra, India

Academic Council Item No: _____

Name of the Implementing Institute	:	Nya. Tatyasaheb Athalye Arts, Ved. S. R. Sapre Commerce, and Vid. Dadasaheb Pitre Science College (Autonomous), Devrukh. Tal. Sangameshwar, Dist. Ratnagiri-415804,
Name of the Parent University	:	University of Mumbai
Name of the Programme	:	Bachelor of Science
Name of the Department	:	Computer Science
Name of the Class	:	Third Year
Semester	:	Six
No. of Credits	:	03
Title of the Course	:	Ethical Hacking
Course Code	:	USCST67
Name of the Vertical	:	Skill Enhancement
Eligibility for Admission	:	Any 12th Pass seeking Admission to Degree Programme in adherence to Rules and Regulations of the University of Mumbai and Government of Maharashtra
Passing Marks	:	40%
Mode of Assessment	:	Formative and Summative
Level	:	UG
Pattern of Marks Distribution for TE and CIA	:	70:30
Status	:	CBCS
To be implemented from Academic Year	:	2021-2022
Ordinances /Regulations (if any)		

Syllabus for Third Year of Bachelor of Science in Computer Science

(With effect from the academic year 2021-2022)

SEMESTER-VI **Paper No.– 7**

Course Title: Ethical Hacking **No. of Credits - 03**

Type of Vertical: Skill Enhancement **COURSE CODE: USCST67**

Learning Outcomes Based on BLOOM's Taxonomy:

After completing the course, the learner will be able to…		
Course Learning Outcome No.	Blooms Taxonomy	Course Learning Outcome
CO-01	Understand	Learner will know to identify security vulnerabilities and weaknesses in the target applications.
CO-02	Remember	They will also know to test and exploit systems using various tools and understand the impact of hacking in real time machines.

Syllabus for Third Year of Bachelor of Science in Computer Science

(With effect from the academic year 2021-2022)

SEMESTER-VI **Paper No.–7**

Course Title: Ethical Hacking **No. of Credits - 03**

Type of Vertical: Skill Enhancement **COURSE CODE: USCST67**

COURSE CONTENT			
Unit No.	**Content**	**Credits**	**No. of Lectures**
I	Information Security : Attacks and Vulnerabilities Introduction to information security : Asset, Access Control, CIA, Authentication, Authorization, Risk, Threat, Vulnerability, Attack, Attack Surface, Malware, Security-Functionality-Ease of Use Triangle Types of malware :Worms, viruses, Trojans, Spyware, Rootkits Types of vulnerabilities : OWASP Top 10 : cross-site scripting (XSS), cross site request forgery (CSRF/XSRF), SQL injection, input parameter manipulation, broken authentication, sensitive information disclosure, XML External Entities, Broken access control, Security Misconfiguration, Using components with known vulnerabilities, Insufficient Logging and monitoring, OWASP Mobile Top 10, CVE Database Types of attacks and their common prevention mechanisms : Keystroke Logging, Denial of Service (DoS /DDoS), Waterhole attack, brute force, phishing and fake WAP, Eavesdropping,	**01**	**15**

	Man-in-the-middle, Session Hijacking, Clickjacking, Cookie Theft, URL Obfuscation, buffer overflow, DNS poisoning, ARP poisoning, Identity Theft, IoT Attacks, BOTs and BOTNETs Case-studies : Recent attacks – Yahoo, Adult Friend Finder, eBay, Equifax, WannaCry, Target Stores, Uber, JP Morgan Chase, Bad Rabbit		
II	Ethical Hacking – I (Introduction and pre-attack) Introduction: Black Hat vs. Gray Hat vs. White Hat (Ethical) hacking, Why is Ethical hacking needed?, How is Ethical hacking different from security auditing and digital forensics?, Signing NDA, Compliance and Regulatory concerns, Black box vs. White box vs. Black box, Vulnerability assessment and Penetration Testing. Approach : Planning - Threat Modeling, set up security verification standards, Set up security testing plan – When, which systems/apps, understanding functionality, black/gray/white, authenticated vs. unauthenticated, internal vs. external PT, Information gathering, Perform Manual and automated (Tools: WebInspect/Qualys, Nessus, Proxies, Metasploit) VA and PT, How WebInspect/Qualys tools work: Crawling/Spidering, requests forging, pattern matching to known vulnerability database and Analyzing results, Preparing report, Fixing security gaps following the report Enterprise strategy : Repeated PT, approval by security testing team, Continuous Application Security Testing, Phases: Reconnaissance/foot-printing/Enumeration, Phases: Scanning, Sniffing	**01**	**15**
III	Ethical Hacking :Enterprise Security Phases : Gaining and Maintaining Access : Systems hacking – Windows and Linux – Metasploit and Kali Linux, Keylogging, Buffer Overflows, Privilege Escalation, Network hacking - ARP Poisoning, Password Cracking, WEP Vulnerabilities, MAC Spoofing, MAC Flooding, IPSpoofing, SYN Flooding, Smurf attack, Applications hacking : SMTP/Email-based attacks, VOIP	**01**	**15**

	vulnerabilities, Directory traversal, Input Manipulation, Brute force attack, Unsecured login mechanisms, SQL injection, XSS, Mobile apps security, Malware analysis : Netcat Trojan, wrapping definition, reverse engineering Phases : Covering your tracks : Steganography, Event Logs alteration Additional Security Mechanisms : IDS/IPS, Honeypots and evasion techniques, Secure Code Reviews (Fortify tool, OWASP Secure Coding Guidelines) hyperplanes, k-NN Unsupervised Learning: Principal Components Analysis (PCA), k-means clustering, Hierarchical clustering, Ensemble methods		
	Total	03	45

Required Previous Knowledge

Students should know basic concepts related to computer and computer handling

Access to the Course

The course is available for all the students admitted for Bachelor of Science (Computer Science).

Forms of Assessment

The assessment of the course will be of Diagnostic, Formative and Summative type. At the beginning of the course diagnostic assessment will be carried out. The formative assessment will be used for the Continuous Internal Evaluation whereas the summative assessment will be conducted at the end of the term. The weightage for formative and summative assessment will be 60:40. The detailed pattern is as given below.

Semester End Evaluation (70 Marks)
Question Paper Pattern
Time: 2:30 hours

Question No.	Unit/s	Question Pattern	Marks
Q.1	I ,II &III	MCQ/Fill in the blanks/One line sentence	10
Q.2	I	Descriptive Questions	20
Q.3	II	Descriptive Questions	20
Q4.	III	Descriptive Questions	20
	Total		**70**

Internal evaluation (30 Marks)

Sr. No.	Description	Marks
1	Classroom Tests	10
2	Project/ Viva/ Presentations/ Assignments	10
3	Attendance	10
	Total	**30**

Grading Scale

10 points grading scale will be used. The grading scale used is O to F. Grade O is the highest passing grade on the grading scale, and grade F is a fail. The Board of Examinations of the college reserves the right to change the grading scale.

Reference book:

- Certified Ethical Hacker Study Guide v9, Sean-Philip Oriyano, Sybex; Study Guide Edition,2016
- CEH official Certified Ethical Hacking Review Guide, Wiley India Edition, 2007

Text book:

- Techmax publication book

Additional References:

1) Certified Ethical Hacker: Michael Gregg, Pearson Education,1st Edition, 2013
2) Certified Ethical Hacker: Matt Walker, TMH,2011
3) http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines
4) https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project
5) https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10
6) https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
7) https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_ Guide
8) https://cve.mitre.org/
9) https://access.redhat.com/blogs/766093/posts/2914051
10) http://resources.infosecinstitute.com/applications-threat-modeling/#gref
11) http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html

Course: USCSP69	Practical of USCST67 (Credits : 1, Lectures/Week: 3)
USCSP69	1. Use Google and Whois for Reconnaissance 2. a) Use CrypTool to encrypt and decrypt passwords using RC4 algorithm b) Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords 3. a) Run and analyze the output of following commands in Linux – ifconfig, ping, netstat, traceroute b) Perform ARP Poisoning in Windows 4. Use NMap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS 5. a) Use Wireshark (Sniffer) to capture network traffic and analyze b) Use Nemesy to launch DoS attack 6. Simulate persistent cross-site scripting attack 7. Session impersonation using Firefox and Tamper Data add-on 8. Perform SQL injection attack 9. Create a simple keylogger using python 10. Using Metasploit to exploit (Kali Linux)