COURSE TITLE	**ETHICAL HACKING**
COURSE CODE	**01CC0403**
COURSE CREDITS	**4**

Objective:

1 The objective of this course is to equip students with comprehensive knowledge and practical skills in Ethical Hacking by enabling them to understand various security vulnerabilities and their associated domains, explore different attacking methods, and apply effective defensive and mitigation strategies. It also aims to develop their understanding of database security concepts along with standard models, and introduce them to a wide range of security tools and testing techniques used in the industry. Through this, students will be prepared to assess, analyze, and enhance the security posture of information systems in an ethical and responsible manner.

Course Outcomes: After completion of this course, student will be able to:

1 Apply ethical hacking methodologies to identify vulnerabilities and assess risks

2 Analyze different phases of hacking including reconnaissance, scanning, and exploitation

3 Implement cryptographic practices for secure network communication and data protection.

4 Evaluate penetration testing techniques using industry-standard tools for network security.

5 Analyze real-world cyber threats and apply defensive strategies to mitigate risks.

Pre-requisite of course:1. Basic Knowledge of Coding 2. Basic Knowledge of Database Management 3. Basic Knowledge of Networking 4. Basic Knowledge if OS

Teaching and Examination Scheme

Theory Hours	Tutorial Hours	Practical Hours	ESE	IA	CSE	Viva	Term Work
3	0	2	50	30	20	25	25

Contents : Unit	Topics	Contact Hours
1	**Introduction of Ethical Hacking (EH)** Overview of Hacking, Types of Hacking, Types of Hackers, How to be Ethical, Legal Issues in Hacking, Ethical Hacking importance in Cyber Security, How Ethical hacking relates with strengthening the security, Red Team & Blue Team Fundamentals in EH	9

Contents : Unit	Topics	Contact Hours
2	**Ethical Hacking Fundamentals** 5 Phases of Ethical Hacking (In depth study of each phase), CIA Triad importance in Ethical Hacking, Difference between Information security & Cyber security, How Ethical hacking covers IS & CS, Use case of EH in information security, Use case of EH in Cyber security, What is Vulnerability, Types of Vulnerability, What is Threat, Types of Threat, Threat vector, Threat model & Threat Assessment, Threat Hunting & Threat Intelligence, What is Risk, Types of Risk, Risk Mitigation Strategies, Risk Matrix, Qualitative & Quantitative risk analysis, Risk Management Life cycle, Types of Testing in EH, Black box testing fundamentals with tools association, Grey box testing fundamentals with tools association, White box testing fundamentals with tools association, Difference of each testing, Scenario where EH can perform which types of Testing with example	9
3	**Ethical Hacking Association with other Domains** What is Operating System? ? Types of OS ? Windows CLI & PowerShell overview ? Windows OS basic commands ? Windows OS Advance commands ? Windows OS Important commands ? Linux Terminal overview ? Linux OS basic commands ? Linux OS Advance commands ? Linux OS Important commands, What is DBMS ? What is DATA & Information, difference ? Types of Data Base ? What is SQL & NOSQL, Importance & difference ? RAID level Architecture in DBMS ? ER model in DBMS ? SQL queries in DBMS (Practical Approach, What is Data Structure ? Importance of DS in cyber security ? File Paging ? What is Algorithms and importance in DS ? How pointer works in DS ? File System in DS, Networking Fundamentals ? What is Internet & network ? Types of Network ? OSI Model & TCP/IP Model ? Important Protocols in networking ? Important Protocols used in communication ? What is Port & famous Port numbers ? How Protocol & Ports associated with each other ? Topologies and it’s types ? Firewall & it’s types	8

Contents : Unit	Topics	Contact Hours
4	**Ethical Hacking Practical Approach Part-1** OWASP, What is OWASP?, Different models of OWASP, Cyber Security perspective in OWASP, Important models (Mobile, Web, Cloud), Information Gathering, What is Information, Types of Information & it's importance in EH, Difference between Recon, Foot printing & Social Engineering, Importance of Social Engineering in Cyber Security, How Hackers use Social engineering skills (Practical approach), Tools associated with Information Gathering (Practical approach), Active & Passive Information gathering concept, Active & Passive Information gathering tools (Mostly Github), Active & Passive Information gathering tools (Mostly Github), OSINT, What is OSINT?, Overview of OSINT (Practical Approach), How OSINT helpful in gathering publically available information (Practical Approach), Different areas in OSINT, Search Parameters in OSINT, Active & Passive information gathering of target using OSINT (Practical approach), Scanning, What is Scanning in EH, Tools associated with scanning, Scanning importance in hacking, How hackers gather information in scanning phase, Metasploit Framework, What is Metasploit framework, Metasploit framework association with Hacking, Payload creation with Metasploit, Hacking with Metasploit	5
5	**Ethical Hacking Practical Approach Part-2** Gaining Access, What is Access Gain?, What is Authentication & Authorisation, Privilege Escalation, Password cracking using Kali Linux tools (JTR & Hydra), How to gain access, How to bypass user account, Revers Shell & Backdoor concept in Hacking, Malware concept in Cyber security, Types of malware, Widely used malware for hackers, Popular platforms for Malware, How Malware plays vital role in maintaining the access, Nmap tool (How hackers used Nmap/ Zenmap tool for network scanning), How Whois, Mitaka, Fierce, Pagodo, Nslookup, Dig tool used for domain enumeration, Wayback machine, Recon-ng, Red-Hawk, sublist3r tool study, How hackers used Wireshark tool for hacking, OpenVAS Kali Linux tool, Website Enumeration tools in Kali & OSINT, Firewall Identification commands and tools, VPN use and how to stay safe in EH, Burpsuite tool for injection in EH	5
Total Hours		**36**

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
1	**Practical 1** Exploring CVEs: Simulating Known Vulnerabilities in Web Applications	2
2	**Practical 2** Real-Time Threat Intelligence Gathering and Correlation	2

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
3	**Practical 3** Active and Passive Reconnaissance Using Open-Source Intelligence (OSINT)	2
4	**Practical 4** Identifying and Exploiting Client-Side Vulnerabilities: DOM XSS & CORS Misconfigurations	2
5	**Practical 5** Advanced Server-Side Injection Techniques: SSRF and XXE in Real- World Apps	2
6	**Practical 6** Evaluating Remote File Inclusion and Template Injection in Custom Web Applications	2
7	**Practical 7** Secure Coding Practices: Implementing Input Validation and Output Encoding	2
8	**Practical 8** Case Study Analysis: Dissecting Major Web Application Breaches	2
9	**Practical 9** Simulating a Web Application Security Incident and Executing a Response Plan	2
10	**Practical 10** Automated Web App Scanning and Reporting Using Sqlmap and Nmap	2
11	**Practical 11** Simulating Session Hijacking and Cookie Theft Attacks	2
12	**Practical 12** Performing Access Control Testing and Role-Based Authorization Checks	2
13	**Practical 13** Identifying and Preventing Security Misconfigurations in Web Servers	2
14	**Practical 14** Exploiting Deserialization Vulnerabilities in Web Applications	2
15	**Practical 15** Implementing Logging and Monitoring for Web Application Threat Detection	2
Total Hours		**30**

Textbook :

1 Cybersecurity Essentials, Charles J. Brooks, Christopher Grow, Philip Craig,Donald Short, John Wiley & Sons, Inc., 2018

References:

1 Network Security Essentials: Applications and Standards , Network Security Essentials: Applications and Standards , William Stallings, Pearson, 2017

2 “The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws”, “The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws”, Dafydd Stuttard, Marcus Pinto, John Wiley & Sons , 2011

Suggested Theory Distribution:

The suggested theory distribution as per Bloom’s taxonomy is as follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

Distribution of Theory for course delivery and evaluation

Remember / Knowledge	**Understand**	**Apply**	**Analyze**	**Evaluate**	**Higher order Thinking / Creative**
10.00	10.00	50.00	20.00	10.00	0.00

Instructional Method:

1 The course delivery method will depend upon the requirement of content and the needs of students. The teacher, in addition to conventional teaching methods by black board, may also use any tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.

2 The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory and class-room

3 Practical examination will be conducted at the end of semester for evaluation of performance of students in the laboratory.

4 Students will use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory.

Supplementary Resources:

1 TryHackMe” – https://tryhackme.com.

2 “Hack The Box (HTB Academy) “– https://academy.hackthebox.com

3 “Cybrary “– https://www.cybrary.it

4 “OWASP Top 10” – https://owasp.org/www-project-top-ten/