VALUE ADDED COURSE

Swarrnim School of Computing & IT

Year: 2019-2020

Subject: Ethical Hacking **Subject Code: VACEH**

Program:	BCA/B.SC.-IT	**Branch:**	All

Hours:- 30 hrs.

Objective:-

- To provide an understanding of the basic concepts of ethical hacking and the significance of cybersecurity.
- To develop practical skills in identifying and addressing security vulnerabilities in computer systems and networks.
- To educate students on various hacking techniques, tools, and countermeasures.
- To equip students with knowledge on the ethical and legal aspects of hacking and cybersecurity.

Swarrnim Startup & Innovation University * Swarrnim School of Computing & IT * Gandhinagar

Detailed Syllabus:

Sr. No.	Module & Content	Total Hrs
1	**Module-1: Introduction to Ethical Hacking** - Overview of Ethical Hacking: Definition, Importance, and Ethics. - Types of Hackers: Black Hat, White Hat, Grey Hat. - Phases of Ethical Hacking: Reconnaissance, Scanning, Gaining Access, Maintaining Access, and Covering Tracks. - Understanding Information Security and Cyber Laws. - Basics of Penetration Testing and Vulnerability Assessment.	**06**
2	**Module-2: Footprinting and Reconnaissance** - Understanding Footprinting: Purpose and Techniques. - Tools for Footprinting: Whois, Nslookup, Shodan, Google Dorking. - Gathering Information: DNS Enumeration, IP Mapping, Social Engineering. - Hands-on Lab: Using Reconnaissance Tools for Information Gathering.	**06**
3	**Module-3: Scanning Networks and Vulnerabilities** - Network Scanning Techniques: Port Scanning, Ping Sweeps, and Banner Grabbing. - Tools for Scanning: Nmap, Netcat, Angry IP Scanner. - Vulnerability Scanning: Identifying and Assessing Vulnerabilities in Systems and Applications. - Hands-on Lab: Performing Network and Vulnerability Scanning.	**06**
4	**Module-4: System Hacking and Exploitation Techniques** - Understanding Password Cracking Techniques: Brute Force, Dictionary Attack, Rainbow Tables. - System Hacking Phases: Gaining Access, Escalating Privileges, Executing Applications. - Keyloggers, Spyware, and Trojans: Techniques and Tools. - Hands-on Lab: Cracking Passwords and Understanding Exploitation Techniques.	**06**
5	**Module-5: Web Application Security and Countermeasures** - Introduction to Web Application Security: OWASP Top 10 Vulnerabilities. - Common Web Attacks: SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF). - Securing Web Applications: Secure Coding Practices, Web Application Firewalls (WAFs). - Introduction to Secure Sockets Layer (SSL) and Secure Hypertext Transfer	**06**

Swarrnim Startup & Innovation University
Swarrnim School of Computing & IT
Gandhinagar

	Protocol (HTTPS). - Hands-on Lab: Simulating Web Attacks and Learning Mitigation Techniques.	

Reference Books

1. Engebretson, Patrick. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy, 2nd Edition, Syngress, 2013.

2. Kim, David, and Solomon, Michael. Fundamentals of Information Systems Security, 3rd Edition, Jones & Bartlett Learning, 2016.

3. Raj, K., and Lal, B.K. Cyber Security: Understanding Cyber Crimes, Computer Forensics, and Legal Perspectives, Wiley India, 2018.

Swarnim Startup & Innovation University * Gandhinagar * Swarnim School of Computing & IT

Vikas Sharma

HoD-SSCIT