DISCIPLINE SPECIFIC ELECTIVE COURSE – DSE 2B Ethical Hacking

Course title & Code	Credits	Credit distribution of the course			Eligibility criteria	Pre-requisite of the course (if any)
		Lecture	Tutorial	Practical/ Practice		
Ethical Hacking	4	3	0	1	Class XII Pass	NA

Learning Objectives

This course introduces the concepts of Ethical Hacking and gives the learner the opportunity to learn about different tools and techniques in Ethical hacking and security, to identify and analyze the stages an ethical hacker requires to take in order to compromise a target system as well as will apply preventive, corrective and protective measures to safeguard the system.

Learning Outcomes

On successful completion of the course, students will be able to:

1. Identify the tools and techniques required to carry out penetration testing
2. Identify, evaluate, treat, and report the security vulnerabilities of various security techniques used to protect system and user data.
3. Implement robust security measures and strengthen the overall security of the network.
4. Demonstrate the concepts of security at the level of policy and strategy in a computer system.

SYLLABUS OF DSE-2B

Unit 1 Introduction (6 hours)

Ethical Hacking Overview - Role of Security and Penetration Testers - Penetration-Testing Methodologies- Laws of the Land - Overview of TCP/IP- The Application Layer - The Transport Layer - The Internet Layer - IP Addressing - Network and Computer Attacks - Malware - Protecting Against Malware Attacks.- Intruder Attacks - Addressing Physical Security

Unit 2 Foot Printing, Reconnaissance and Scanning Networks (9 hours)

Footprinting Concepts - Footprinting through Search Engines, Web Services, Social Networking Sites, Website, Email - Competitive Intelligence - Footprinting through Social Engineering - Footprinting Tools - Network Scanning Concepts - Port-Scanning Tools - Scanning Techniques - Scanning Beyond IDS and Firewall

Unit 3 Enumeration and vulnerability analysis (9 hours)

Enumeration Concepts - NetBIOS Enumeration – SNMP, LDAP, NTP, SMTP and DNS Enumeration - Vulnerability Assessment Concepts - Desktop and Server OS Vulnerabilities - Windows OS Vulnerabilities

Unit 4 System hacking (12 hours)

Hacking Web Servers - Web Application Components- Vulnerabilities - Tools for Web Attackers and Security Testers Hacking Wireless Networks - Components of a Wireless Network – Wardriving- Wireless Hacking

Unit 5 Network protection systems (9 hours)

Access Control Lists. - Cisco Adaptive Security Appliance Firewall - Configuration and Risk Analysis Tools for Firewalls and Routers - Intrusion Detection and Prevention Systems – Network-Based and Host-Based IDSs and IPSs - Web Filtering - Security Incident Response Teams – Honeypots.

Practical component

Practical exercises based on the syllabus.

Essential Readings

1. Michael T. Simpson, Kent Backman, James E. Corley, Hands-On Ethical Hacking and Network Defense, Course Technology, Delmar Cengage Learning, 2010.
2. Patrick Engebretson, The Basics of Hacking and Penetration Testing, 2nd Edition, Syngress, Elsevier, 2013.
3. Dafydd Stuttard, Marcus Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition, Wiley, 2011.

Suggested Readings

1. Justin Seitz, Black Hat Python: Python Programming for Hackers and Pentesters, 2014.