SILVER OAK UNIVERSITY

College of Technology

Bachelor of Technology
Information Technology
Course Name: Cyber Security
Course Code:1010043362
Semester:5th

Prerequisite:

Basic fundamental knowledge of computers and Internet

Course Objectives:

1. This course mainly focuses on technical, legal, and social issues related to cybercrime and cyber security needed for the same. These crimes are such in which a computer may be used as a target, a tool or both.
2. Various types of cybercrimes, cyber-criminals, methods involved in cyber-attacks etc. will be focused in this course that creates the basic understanding of the need of cyber security.

Teaching Scheme:

Teaching Scheme				
L	T	P	Contact Hours	Credit
3	0	2	5	4

Contents:

Unit	Topics	Teaching Hours	Weightage %
1	**Introduction to Cyber Crime:** Definition and Origin of the Word, Cyber Crime and Information Security, Cyberspace, Cyber Security: Definition, Who are Cyber Criminals, Classification of Cyber crimes, Basic Terminologies: Vulnerability, Threat, Exploit, Attack, Active Attacks, Passive Attacks, Types of hackers, How Criminal Plans the Attack, What is hacking , Phases of Hacking.	7	10
2	**Basics of Cyber Attacks:** What is malware, Types of malwares: Virus, Worms Trojan, backdoors, Keyloggers and Spyware, Proxy server and Anonymizers, Buffer Overflow, Cyber Defamation, Software Piracy, Computer Sabotage.	12	30
3	**Various Cyber Attacks:** E-mail Spoofing, Salami Attack, Data Diddling, Forgery, Online Frauds, Email Bombing, Computer Network Intrusion, Password Sniffing, Credit Card Frauds, Identity Theft, Social Engineering and its types, Botnet, Botnet Architecture, Phishing: How does phishing work, Dos and Ddos Attacks, SQL Injection	12	15
4	**Understanding Digital Forensics and Cyber Law:** Introduction to Incident Response, Digital Forensics, Need for Computer	8	15

	Forensic, Digital Evidence and rules of Evidence, Digital Forensic Life Cycle, Cyber Laws, why do we need cyber laws: The Indian IT ACT 2000, Admissibility of Electronic records, Amendments made in Indian ITA 2000		
5	**Introduction to Network Defense:** Firewall Basics, Packet Filter Vs Firewall, How a Firewall Protects a Network, Stateless Vs Stateful Firewalls, IDS, IPS, IDS vs IPS, Network Address Translation (NAT), Open Port,Port Forwarding, the basic of Virtual Private Networks, Linux Firewall, Windows Firewall, Snort: Intrusion Detection System	8	15
6	**Vulnerability Scanning:** Overview of vulnerability scanning, Open Port/Service Identification, Banner/Version Check, Traffic-Probe, Vulnerability Probe, Vulnerability Examples, Network Reconnaissance – Nmap, Networks Vulnerability Scanning - Netcat, Network Sniffers and Injection tools – Tcpdump and Wireshark,	8	10
7	**Web Application Scanning tools** Web Application vulnerabilities scanning tools: Vega Scanner, Nikto, W3af, Application Inspection tools: Zed Attack Proxy, Sqlmap, DVWA, Password Cracking and Brute-Force Tools: John the Ripper, L0phtcrack, Pwdump	5	5

Course Outcomes:

Sr. No.	CO Statement	Unit
CO-1	Identify and distinguish between the different types of Cybercrimes.	1
CO-2	Identify the method of performing various cyber attacks using different malwares	2
CO-3	Classify different types of digital forensic methods and IT laws 4 by the use of case studies	3
CO-4	To assess and evaluate the computer networks and ports using network scanning tools	5
CO-5	To analyze different system vulnerabilities and web application vulnerabilities using vulnerability scanning tools for TCP and UDP systems	4

Teaching & Learning Methodology:

The various methods or tools to teach the above subject:

1. PPT
2. Video Lectures etc

List of Experiments: Total Hours: 28

Sr. No.	Practical Name
1	To study about different types of Cybercrimes
2	To study about phases of hacking
3	To study basic concepts of malwares

4	Perform TCP/UDP scanning using Nmap
5	Create Connectivity using NETCAT.
6	Perform Web Application scanning using Vega.
7	Perform SQL Injection using DVWA.
8	Perform Penetration Testing using DVWA
9	Analyze the Network Traffic using Wireshark
10	Case Study on Indian IT ACT 2000.

Major Equipment:

1. Latest configured Computer systems
2. Vulnerability scanning tools
3. Network scanning tools
4. DVWA

Books Recommended:

1. Nina Godbole and Sunit Belpure,"Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives" by Publication Wiley.
2. Mike Shema,"Anti-Hacker Tool Kit (Indian Edition)" by Publication McGraw Hill.

List of Open-Source Software/learning website:

1. http://silveroakuni.ac.in/video-lecture
2. http://www.coursera.org/

CO-PO-PSO Matrix:

Co. No.	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO-1		1		1		2		3	2			1	1	1
CO-2		1		1	2	1	1	2	2			2	1	1
CO-3		1		1		1	1	2	2	1		2	1	2
CO-4	1		2		3		3		3			2	1	1
CO-5	1	2	2		3		3		3			2	1	2