Charotar University of Science and Technology

Devang Patel Institute of Advance Technology and Research

Department of Computer Science & Engineering

Subject Name: Cyber Security and Cyber Laws **Semester**: 7th
Subject Code: CS472 **Academic year**: 2022-2023

Course Outcomes (Cos):
At the end of the course, the students will be able to

CO1	After learning the course, students should be able to learn about cyber-attack, type of cybercrimes
CO2	Learn cyber security vulnerabilities and security safeguard.
CO3	Learn hand-on on how to prevent the web using different web application tools.
CO4	Learn about how to protect the network using different network tools and Intrusion detection and prevention techniques,
CO5	Learn basis of Cryptography and network security
CO6	Understand about cyber laws
CO7	Learn about cyber-Forensics and investigation of information hiding.
CO8	Learn about how to protect them self and ultimately society from cyber-attacks.

Sr. No.	Name of Practical	Hrs	CO's
1.	**Perform 5 different types of (port) scanning using nmap on a single port and capture the packets using wireshark and analyze the output.**	2	1
2.	**Perform a Vulnerability Scan on a system within the Local Area Network and Submit the report**	2	2
3.	**Implementation to identify web vulnerabilities, using OWASP project**	2	2,3,4
4.	**Implementation of Windows/Linux security using firewall** **A. Block ICMP ping using OUTPUT chain and echo- reply.** **B. Setup SPI Firewall that** **a. Allow all outgoing connection.** **b. Block all unwanted incoming connection.**	4	1,2
5.	**Configure a windows FTP server for user-based access. Capture packets while you connect to FTP server and Login. Find the packet that shows username and password. Capture packets and observe the results?**	4	3,4
6.	**Implementation to gather information from any PC's connected to the LAN using whois, port scanners, network scanning, IP**	2	1,2,5

	scanners etc.		
7.	**Set up a Virtual lab environment with Windows XP (SP1), Metasploitable OS, and BRICKS/DVWA web server and an Attacker machine (KALI/BT) in virtual machines (network in NAT mode).** **Now carry out Vulnerability assessment in environment** **a. Network VA/PT** **i. Find the open ports in domain.** **ii. Find out the hosts in domains.** **iii. Find out the services running on domains and their versions.** **iv. Banner Grabbing of server.** **v. Find out default vulnerabilities in Services.** **vi. Exploit the vulnerabilities.** **vii. Deploy and maintain the backdoor.** **b. Web VA/PT** **i. Find the domain information.** **ii. Find the details of server and its default vulnerabilities.** **iii. Perform automated testing using BurpSuite or ZAP proxies.** **Tools: nmap, netcat, netcraft, nslookup, whois, dig, ping, Nessus, Metasploit, FOCA.**	**4**	**3,4,5**
8.	**Gather information of any domain/website/IP address using following Information Gathering Tools.** **1. Samspade** **2. Nslookup** **3. Whois** **4. Tracert**	**2**	**3,4,5,8**
9	**Create a remote connection using open SSH.**	**2**	**5**
10	**Perform Live / Memory Analysis on a Linux OS and prepare a detailed report.**	**2**	**4,5**