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**: 6th
Subject Code: CS383 **Academic year**: 2022-23

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

CO1	Classify various security goals, mechanisms and attacks
CO2	Evaluate various intrusion detection and prevention techniques
CO3	Evaluate the security attacks on given environment by vulnerability assessment and penetration testing and identify various cyber-attacks and get awareness about the relatable cyber laws.
CO4	Design the technique or model to provide security for given scenario

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.**	**4**	**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**	**3**
4.	**Perform log analysis of machine data using Splunk software in windows/linux. This machine data can come from web applications, sensors, devices or any data created by user.**	**4**	**3**
5.	**Monitor the traffic in real time and issue alerts to users when it discovers potentially malicious packets or threats on Internet Protocol (IP) networks using SNORT.**	**4**	**2**
6.	**Implementation to gather information from any PC's connected to the LAN using whois, port scanners, network scanning, IP scanners etc.**	**2**	**3,4**
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**	**4**	**3,4**

	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.		
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
9	Identify any 5 online web portals for information gathering. Scan an IP address/URL for gathering information. Prepare a report.	2	2,3
10	Perform Live / Memory Analysis on a Linux OS and prepare a detailed report.	4	2,3