B.E / B.Tech. PRACTICAL END SEMESTER EXAMINATIONS, NOVEMBER/DECEMBER 2023

Fifth Semester

CCS340 - CYBER SECURITY

(Regulations 2021)

Time : 3 Hours   Answer any one Question   Max. Marks 100

Aim//Procedure	Program	Results	Viva-Voce	Record	Total
20	30	30	10	10	100

1.	Install Kali Linux on Virtual box and display all open ports in the host system.
2.	Install metasploitable2 on the virtual box and search for unpatched vulnerabilities
3.	Install Linus server on the virtual box and install ssh
4.	Launch brute-force attacks on the Linux server using Hydra
5.	Perform real-time network traffic analysis and data pocket logging using Snort
6.	Use Fail2ban to scan log files and ban IPs that show the malicious signs
7.	Demonstrate the nmap command d and scan a target using nmap and list vulnerabilities.
8.	Perform open source intelligence gathering using Whois Lookups and DNS Reconnaissance
9.	Use Metasploit to exploit an unpatched vulnerability
10.	Install Kali Linux and use bash scripting to list all open ports in a given IP.
11.	Discover remote operating system using nmap Also, detect IP spoofing and port scanning using nmap
12.	Implement a dictionary attack using Hydra
13.	Demonstrate intrusion detection system using snort
14.	Perform open source intelligence gathering using Maltego
15.	Installation of rootkits and study about the variety of options.

16.	Search for unauthorized servers or network service on your network using nmap and remove computers which do not meet the organization guidelines.
17.	Perform open source intelligence gathering using Harvester
18.	Download and install nmap. Use it with different options to scan open ports,perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan,
19.	Demonstrate host based intrusion detection system using any tool.
20.	Install Kali Linux and use its tool to find vulnerable system in a network.