

BCA-5-01P: Introduction to Cyber Security Lab

Total Marks: 50

External Marks: 35

Internal Marks: 15

Credits: 2

Pass Percentage: 40%

| | |
|--|---|
| Course Name: Introduction to Cyber Security Lab | |
| Course Code: BCA-5-01P | |
| Course Outcomes (COs) | |
| After the completion of this course, the students will be able to: | |
| CO 1 | Identify and analyze common cyber threats, including malware, phishing attacks, and network vulnerabilities. |
| CO 2 | Apply techniques to detect, mitigate, and respond to various types of cyber threats. |
| CO 3 | Implement security configurations for operating systems, network devices, and applications. |
| CO 4 | Apply ethical hacking techniques to identify and exploit vulnerabilities in controlled environments, emphasizing responsible and legal practices. |
| CO5 | Implement cryptographic techniques for security purpose |

Detailed Contents:

| S. No. | Name of Experiments |
|---------------|--|
| 1 | How to identify open ports, services, and potential vulnerabilities on target systems. |
| 2 | How to scan and enumerate devices on a network using Nmap tool. |
| 3 | How to analyse the malware in a controlled environment. |
| 4 | Conduct an experiment for phishing simulation to demonstrate common phishing tactics. |
| 5 | How to configure a firewall to control incoming and outgoing network traffic. |
| 6 | Design and implement the rules to permit or deny specific types of traffic. |
| 7 | Design and implement the secure communication using tools like OpenSSL or GPG. |
| 8 | Simulate various common password cracking techniques. |
| 9 | Study of Computer Forensics and different tools used for forensic investigation |

| | |
|----|---|
| 10 | How to encrypt and decrypt messages using the chosen algorithm and analyze the security properties. |
|----|---|