## DCS-2-02P: Cyber Attacks and Counter Measures Lab

Total Marks: 50
External Marks: 35
Internal Marks: 15
Credits: 2
Pass Percentage: 40%

| | |
|---|---|
| **Course Name: Cyber Attacks and Counter Measures**<br>**Course Code: DCS-2-02P** | |
| **Course Outcomes (COs)**<br>After the completion of this course, the students will be able to: | |
| **CO 1** | Develop skills in configuring security settings for operating systems, networks, and applications. |
| **CO 2** | Analyse network traffic using tools like Wireshark. |
| **CO 3** | Conduct vulnerability assessments to identify potential weaknesses and recommend appropriate countermeasures. |
| **CO 4** | Apply tools to analyze network traffic and system logs in real-time. |
| **CO 5** | Understand and apply secure coding practices to develop resilient software. |

## Detailed Contents:

| S. No. | Name of Experiment |
|---|---|
| 1 | How to create signatures to detect and block the malware using antivirus or intrusion detection systems. |
| 2 | How to capture and analyse network traffic using tools like Wireshark. |
| 3 | How to configure and test an intrusion detection system to identify and respond to malicious activities. |
| 4 | Implement the firewall rules by simulating different attack scenarios and assessing the effectiveness of the configured rules. |
| 5 | Conduct a phishing simulation to test user awareness and susceptibility. |
| 6 | Evaluate the effectiveness of implemented countermeasures and educate users on recognizing phishing attempts. |
| 7 | Develop and implement a patch management plan to address identified vulnerabilities. |
| 8 | Simulate a cybersecurity incident and implement an incident response plan. |
| 9 | Perform security testing on a web application to identify and remediate common vulnerabilities. |

| | |
|---|---|
| 10 | How to implement countermeasures to mitigate the impact of the attack and ensure service availability. |