Guru Nanak Dev Engineering College, Ludhiana
Department of Computer Science and Engineering

No.CSE/07/3236 Dated 14/01/2025

Department of Computer Science and Engineering is going to start a Value Added Course on "**Digital Security - Concepts and Practical Aspects**" for session Jan-June 2025 (**online mode**)

Expert : Er. Parminder Singh Sandhu
Information Security Manager, Apple, USA.

Interested students are required to register by 15.01.2025 (12:30 PM) link for registration is as follows:-
https://forms.gle/Wdvb6ADbqJfQJ73G7

HOD (CSE)

Tentative Contents for the Course is as follows:

Section 1: **Foundations of Cybersecurity (4 hours)**

Introduction to Cybersecurity
Definition, importance, and key concepts.
Overview of common threats (malware, phishing, ransomware).
Cybersecurity Principles
Confidentiality, Integrity, and Availability (CIA Triad).
Cybersecurity Landscape
Current trends and challenges.
Case studies of notable cyberattacks.

Section 2: Basics and Setup (4 hours)

Introduction and Environment Setup
Install and configure virtual machines (Kali Linux, Windows).
Basic Linux and Windows commands.
Hands-On Networking Basics
Build a small network using a virtual lab.
Analyze traffic using Wireshark.
Practical: Identifying Network Protocols

Section 3: Network Security (4 hours)

Scanning and Enumeration
Perform network scans using Nmap and Zenmap.
Discover open ports and services.
Packet Analysis
Use Wireshark to capture and analyze packets.
Detect anomalies in network traffic.
Practical: Simulate a DDoS Attack

Section 4: System Security (4 hours)_

Securing Operating Systems
Apply security patches and harden configurations.
Configure firewalls and antivirus software.
Privilege Escalation Techniques
Test user privileges in Windows and Linux.
Mitigate privilege escalation risks.
Practical: Exploiting and Securing a Vulnerable VM

Section 5: Web Application Security (4 hours)
Web Vulnerability Scanning
Use tools like Burp Suite and OWASP ZAP.
Identify SQL Injection and XSS vulnerabilities.
Exploiting Web Applications
Perform SQL Injection and XSS attacks on test sites.
Demonstrate secure coding practices to fix issues.
Practical: Exploit a Test Website

Section 6: Ethical Hacking and Penetration Testing (4 hours)
Introduction to Penetration Testing
Hands-on with Metasploit framework.
Conduct vulnerability assessments.
Exploitation and Reporting
Exploit identified vulnerabilities.
Generate detailed penetration test reports.
Practical: Complete a Pen Test Lab

Section 7: Incident Response and Malware Analysis (4 hours)
Live Incident Simulation)
Detect and respond to simulated ransomware attacks.
Use forensic tools to trace attack origins.
Malware Analysis
Analyze malware behavior in a sandbox.
Identify mitigation techniques.
Practical: Investigate and Contain an Incident

Section 8: Governance, Risk, and Compliance (4 hours)
Security Policies and Best Practices
Apply real-world security standards (ISO 27001, NIST).
Risk Assessment Hands-On
Conduct a practical risk assessment for a given scenario.
Practical: Draft a Cybersecurity Policy

Section 9: Project and Assessment (4 hours)
Project: Simulated Attack and Defense
Set up and defend against simulated attacks.
Present a comprehensive report with recommendations.
Review and Practical Assessment

Real-world problem-solving based on course content.