

Title of the Course	Ethical Hacking and Cyber Security
Operational Plan No	CSE-3
Dates and Venue	Contact Mode
Course Objectives	<ul style="list-style-type: none"> ➤ To understand Ethical hacking principles, methodologies, and best practices ➤ To practice hands-on penetration testing and vulnerability assessment using standard tools ➤ To analyze and mitigate web application and network security risks (e.g., SQL Injection, XSS) ➤ To secure cyberspace: networks, systems, and web applications using appropriate defense strategies ➤ To implement security mechanisms such as a firewall, IDS/IPS, and Virtual Private Networks ➤ To understand malware, phishing, and social engineering attacks and their prevention techniques ➤ To apply cryptographic techniques for ensuring information security ➤ To utilize digital forensic tools for cybercrime investigation and analysis ➤ To understand the legal and ethical aspects of cybersecurity
Course Contents	<ul style="list-style-type: none"> ➤ Role of Cryptography in securing Cyber space ➤ Symmetric & Asymmetric Cryptography techniques ➤ Fundamentals of Ethical Hacking: Principles, methodologies, and best practices ➤ Cyber Threats and Attack Vectors: Social Engineering, Malware, Phishing, Social Engineering, DoS/DDoS ➤ Web Application Security: SQL Injection, XSS, CSRF (Demonstration & Prevention) ➤ Hands-on: Vulnerability Assessment and Penetration Testing Techniques & Tools ➤ Network Security: Network Scanning & assessment, Firewalls, IDS/IPS, and Defence Strategies ➤ Wireless Security: Wi-Fi Vulnerabilities and Protection Mechanisms ➤ Digital Forensics: Tools and Techniques for Cyber Crime Investigation (Case Studies)
Course Coordinators	Dr. C. Rama Krishna : rkc@nitttrchd.ac.in Er. Amrendra Sharan : amrendra@nitttrchd.ac.in