COURSE OUTLINE

PROGRAMME TITLE	Introduction to Ethical Hacking using Kali Linux
OVERVIEW (brief introduction of the topic)	This 1 day course provides a hands-on course introduces ethical hacking for cybersecurity professionals, covering Kali Linux tools, penetration testing, and legal considerations.
LEARNING OUTCOME	After completing the course, participants will be able to: a. Fundamentals: Scope, laws, and rules of ethical hacking. b. Kali Linux: Essential tools for reconnaissance, scanning, and exploitation. c. Practical Attacks: Simulated breaches using Nmap, Nikto, and Metasploit. d. Defensive Insights: How to protect systems from similar exploits. e. Legal & Ethical Compliance: Responsible disclosure and industry best practices.
DURATION (days)	One (1) Day – Face to Face (Lab Session)
TARGET PARTICIPANTS (sector/position/level)	IT and Professionals, IT security teams, system administrators, and professionals securing OT/IT environments
COURSE CONTENT (with subModuls)	Module 1: What is Ethical Hacking? Scope, Rules of Engagement, and Laws Subtopics: • Definition of ethical hacking vs. malicious hacking • Roles of ethical hackers (penetration testers, red teams, security auditors) • Legal frameworks (Computer Misuse Act, GDPR, PCI DSS, local cyber laws) • Rules of Engagement (RoE) – Contracts, permissions, and scope limitations Module 2: Kali Linux Overview: Tools and Interface Subtopics: • Introduction to Kali Linux (purpose-built for penetration testing) • Key tools categorization: • Information Gathering (Nmap, Maltego, theHarvester)

	• Vulnerability Analysis (Nikto, OpenVAS) • Exploitation (Metasploit, SQLmap) • Post-exploitation (Meterpreter, C2 frameworks) • Basic Linux commands for ethical hackers • Customizing Kali (persistence, VPN setup, tool updates) Module 3: Hands-on Demo: Information Gathering with Nmap & Nikto Subtopics: • Nmap (Network Scanning) • Host discovery • Port scanning techniques • Service/OS detection • Scripting engine Module 4: Case Study: Simulated Penetration Test on an Isolated Server Subtopics: • Scenario: A petroleum retail company's unsecured server Steps taken: • Reconnaissance (WHOIS, subdomain enumeration) • Scanning (Nmap for open ports) • Exploitation (Weak SSH credentials, outdated Apache) • Post-exploitation (Data exfiltration, privilege escalation) • Lessons learned: How such breaches impact fuel automation & payment systems Module 5: Exploiting Vulnerable Systems using Metasploit Subtopics: • Metasploit Framework Overview (Modules, payloads, sessions) Exploitation Steps: • Searching for exploits • Configuring payloads • Executing the exploit

	Post-exploitation: • Dumping passwords • Keylogging (keyscan_start) • Pivoting to internal networks • Defensive measures: How to detect & prevent such attacks Module 6: Debrief, Legal Considerations, Ethical Use of Hacking Skills Subtopics: • Recap of key learnings • Legal risks (unauthorized testing, data breaches) • Bug bounty programs (HackerOne, Bugcrowd) • Ethical responsibilities (responsible disclosure, protecting client data) • Q&A and next steps (advanced training, certifications)
LEARNING METHODOLOGIES	Interactive Lectures, Hands-On Labs & Demos, Group Activities & Collaboration, Real-World Scenarios & Use Cases, Capstone Project