COURSE OUTLINE

PROGRAMME TITLE	Host Vulnerability Assessment Using Nessus
OVERVIEW (brief introduction of the topic)	This 1 day course provides a hands-on training provides IT security professionals, system administrators, and penetration testers with the skills to conduct effective vulnerability assessments using Nessus.
LEARNING OUTCOME	After completing the course, participants will be able to: a. Install & configure Nessus (Scanners, user roles, policies) b. Perform credentialed & non-credentialed scans (Windows, Linux, network devices) c. Analyze scan results (Prioritizing CVEs, false positives) d. Generate actionable reports (Technical & executive summaries) e. Integrate Nessus with SIEM & ticketing systems
DURATION (days)	One (1) Day – Face to Face (Lab Session)
TARGET PARTICIPANTS (sector/position/level)	IT and Professionals, Security analysts, network admins, compliance auditors, and SOC teams.
COURSE CONTENT (with subModuls)	Module 1: Introduction to Vulnerability Assessment & Nessus • Vulnerability Management Lifecycle (Discovery, Prioritization, Remediation) • Nessus Architecture (Tenable.sc vs. Nessus Professional, Scanner Types) • Installation & Initial Setup (Licensing, User Roles, Plugin Updates) • Hands-on Lab: Deploying Nessus & Basic Configuration Module 2: Scan Configuration & Execution (10:45 – 12:30) • Scan Policies & Templates (Discovery, Compliance, Malware Checks) • Credentialed vs. Non-Credentialed Scans (Windows, Linux, Network Devices) • Advanced Settings (Safe Checks, Performance Optimization) • Hands-on Lab: Running a Network Vulnerability Scan Module 3: Analyzing & Validating Results (13:30 – 15:00) • Interpreting Scan Results (CVSS Scores, Exploitability, Risk Ratings)

	• False Positive/Negative Identification (Manual Verification) • Prioritizing Remediation (Patch Management, Workarounds) • Hands-on Lab: Analyzing a Scan Report & Filtering Critical Vulnerabilities Module 4: Reporting & Automation • Generating Reports (Executive Summary, Technical Details, Compliance) • Integrating with SIEM & Ticketing Systems (Wazuh/Splunk/ Jira/ ServiceNow) • Automating Scans (Scheduled Scans, API Integration) • Q&A / Final Challenge Lab
LEARNING METHODOLOGIES	Interactive Lectures, Hands-On Labs & Demos, Group Activities & Collaboration, Real-World Scenarios & Use Cases, Capstone Project