Enterprise Vulnerability Management & Threat Assessment (EVMTA)

24-Hour Hourwise Training Curriculum (6 Days × 4 Hours/Day)

Duration: 6 Days (24 Hours) **Schedule:** 4 Hours/Day **Level:** Beginner to Intermediate

COURSE OVERVIEW & PROGRAM DETAILS

Delivery:	Instructor-Led & Practical Sandbox Labs	**Target Audience:**	Security Analysts, System Admins, IT Engineers, Vulnerability Managers
Tools Covered:	Nmap, OpenVAS (Greenbone), Burp Suite Community, Nikto, Lynis, Microsoft Defender		

DAY 1 Foundations & Asset Discovery (4 Hours)

Hour	Theory Topics	Practical / Lab Work
1	Introduction to VM, Threat vs Vulnerability vs Risk, Lifecycle, Roles	—
2	Types of Vulnerabilities, Zero-day vs N-day	—
3	CVE, CWE, CVSS, CPE, Advisories, Prioritization	Explore NVD, MITRE CVE/CWE, CISA KEV
4	Asset Discovery Concepts	Nmap Asset Discovery & Enumeration

DAY 2 Assessment Fundamentals & Infrastructure Scanning (4 Hours)

Hour	Theory Topics	Practical / Lab Work
1	Assessment Methodology, Scope, Auth vs Non-auth	—
2	Scanning Fundamentals, Policies, Scheduling	Configure OpenVAS Scan Policies
3	Network & Host Assessment	Nmap Infrastructure Assessment
4	Scanner Architecture & Reporting	OpenVAS Infrastructure Assessment

DAY 3 Web Application Vulnerability Assessment (4 Hours)

Hour	Theory Topics	Practical / Lab Work
1	HTTP/HTTPS, Sessions, OWASP Top 10	—
2	Burp Suite Essentials	Configure Proxy & Capture Requests
3	SQLi, XSS, IDOR, Headers, Cookies	Burp Testing on DVWA
4	Reporting & Validation	Document Findings

DAY 4 Analysis, Remediation & Patch Verification (4 Hours)

Hour	Theory Topics	Practical / Lab Work
1	Scan Analysis, CVSS Scoring	Analyze Scan Reports
2	False Positives / False Negatives	Validate Findings
3	Patch Management & System Hardening	Patch & Verify Systems
4	Rescanning & Documentation	Verification Exercise

DAY 5 Enterprise Vulnerability Management & Compliance (4 Hours)

Hour	Theory Topics	Practical / Lab Work
1	Risk-Based Vulnerability Management (RBVM)	—
2	Continuous Vulnerability Management	Configure Scheduled Scans
3	Compliance Frameworks: NIST, CIS, ISO 27001, PCI DSS	Lynis Secure Config Review
4	Enterprise Reporting & Dashboards	Generate Executive & Technical Reports

DAY 6 Practical Implementation & Enterprise Case Study (4 Hours)

Hour	Theory Topics	Practical / Lab Work
1	End-to-End Vulnerability Management Workflow	Assessment Planning
2	Enterprise Case Study Analysis	Assessment Setup
3	VM Industry Best Practices	Enterprise Assessment using Nmap, OpenVAS & Burp Suite
4	Course Review, Final Assessment & Q&A	Review Findings, Remediation Discussion & Report Presentation

Tools Covered & Lab Environment: Nmap, OpenVAS (Greenbone Enterprise / CE), Burp Suite Community Edition, Nikto Web Scanner, Lynis System Auditing, Microsoft Defender for Endpoint.