Vulnerability Assessment with Nessus and OpenVAS Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Vulnerability Assessment with Nessus and OpenVAS Training Course is engineered to equip participants with in-demand skills in Vulnerability Management using the industry-leading proprietary scanner, Nessus, and the powerful open-source alternative, OpenVAS. Mastering these tools is crucial for any organization looking to reduce its Attack Surface and achieve stringent Regulatory Compliance. Graduates will be prepared to identify, prioritize, and report system weaknesses, moving beyond simple scanning to implementing a complete, continuous Vulnerability Lifecycle. This is an essential step for careers in Penetration Testing, Security Auditing, and Security Operations

The program delivers real-world expertise through a lab-intensive methodology, bridging the gap between theoretical knowledge and practical application. We will deep-dive into Credentialed Scanning for high-accuracy results, Web Application Scanning techniques, and the critical skill of False Positive Remediation. By comparing and contrasting the capabilities of both Nessus and OpenVAS, participants will gain a strategic perspective on selecting the right tool for diverse enterprise and small-to-medium business (SMB) environments, ensuring they can immediately contribute to enhancing their organization's Cyber Resilience and Risk Posture.

Programme Curriculum

Vulnerability Assessment with Nessus and OpenVAS Training Course

Introduction

Vulnerability Assessment with Nessus and OpenVAS Training Course is engineered to equip participants with in-demand skills in Vulnerability Management using the industry-leading proprietary scanner, Nessus, and the powerful open-source alternative, OpenVAS. Mastering these tools is crucial for any organization looking to reduce its Attack Surface and achieve stringent Regulatory Compliance. Graduates will be prepared to identify,

prioritize, and report system weaknesses, moving beyond simple scanning to implementing a complete, continuous Vulnerability Lifecycle. This is an essential step for careers in Penetration Testing, Security Auditing, and Security Operations

The program delivers real-world expertise through a lab-intensive methodology, bridging the gap between theoretical knowledge and practical application. We will deep-dive into Credentialed Scanning for high-accuracy results, Web Application Scanning techniques, and the critical skill of False Positive Remediation. By comparing and contrasting the capabilities of both Nessus and OpenVAS, participants will gain a strategic perspective on selecting the right tool for diverse enterprise and small-to-medium business (SMB) environments, ensuring they can immediately contribute to enhancing their organization's Cyber Resilience and Risk Posture.

Course Duration

5 days

Course Objectives

1. Master Vulnerability Lifecycle Management
2. Conduct High-Accuracy Credentialed Scans
3. Analyze and Prioritize Findings using CVSS v3.1
4. Differentiate and Apply Nessus and OpenVAS for Enterprise Scanning
5. Develop Robust Vulnerability Assessment Report Templates
6. Automate Scans for Continuous Security Monitoring
7. Identify and Remediate False Positives and False Negatives
8. Integrate Scanners with SIEM and Ticketing Systems
9. Perform Web Application and Compliance Audits
10. Implement Post-Scan Configuration Hardening
11. Understand Legal and Ethical Hacking Frameworks
12. Calculate and Communicate Business Risk from Technical Vulnerabilities
13. Apply Threat Intelligence to Prioritize Remediation

Target Audience

1. Security Analysts
2. Penetration Testers and Ethical Hackers
3. System and Network Administrators
4. IT Auditors and Compliance Officers
5. Cybersecurity Consultants
6. DevSecOps Engineers
7. Risk Management Professionals
8. Security Engineers

Course Modules

Module 1: Foundational Concepts & Assessment Planning

- Define Vulnerability Assessment and Penetration Testing.
- Introduction to Common Vulnerability Scoring System and risk-based prioritization.
- Understanding the Vulnerability Management Lifecycle.
- Legal and ethical considerations
- Passive and active information gathering techniques

- Case Study: Analyzing a Ransomware Incident where an unpatched CVE identified in a prior VA report was the initial entry vector.

Module 2: OpenVAS Installation & Configuration

- Installing and setting up Greenbone Security Manager Community Edition.
- Understanding and updating the Greenbone Enterprise Feed
- Configuring Scan Targets, Credentials, and Scan Configs
- Executing the first basic, unauthenticated internal network scan.
- Interpreting initial OpenVAS results and dashboard overview.
- Case Study: Using OpenVAS for a cost-effective VA for a Small Business with a limited IT security budget.

Module 3: Nessus Deployment & Essential Scanning

- Installation and activation of Nessus Professional/Essentials on Windows/Linux.
- Navigating the Nessus User Interface and understanding Plugins.
- Configuring Policy Templates for basic, advanced, and Web Application Scans.
- Performing Credentialed Scanning for deeper visibility.
- Troubleshooting common scan issues
- Case Study: Simulating an Enterprise VA using Nessus Agents for scanning remote and ephemeral endpoints in a large corporate network.

Module 4: Advanced Scanning Techniques

- Customizing scan policies to prevent network disruption or Denial of Service.
- Compliance Auditing with Nessus and OpenVAS
- Scanning Web Applications for common vulnerabilities
- Advanced target enumeration using Nessus's host discovery and Nmap integration.
- Scanning virtual/cloud environments and mobile devices
- Case Study: Conducting a PCI DSS Compliance Audit scan on a payment server using a Nessus compliance template to generate a required report.

Module 5: Result Analysis and Prioritization

- Analyzing raw scan data to identify critical vulnerabilities.
- Applying the CVSS base score and factoring in environmental/temporal metrics.
- False Positive Remediation and verification techniques.
- Prioritizing remediation efforts using Vulnerability Prioritization Technology concepts.
- Mapping vulnerabilities to the MITRE ATT&CK Framework.
- Case Study: Analyzing a high-volume OpenVAS report and using a risk matrix to prioritize the top 5 vulnerabilities for immediate patching.

Module 6: Professional Reporting and Communication

- Best practices for creating clear, actionable Vulnerability Assessment Reports.
- Structuring the report for both Executive and Technical Audiences.
- Exporting and customizing reports in various formats
- Developing and presenting a remediation plan with clear timelines and owners.
- Metrics for tracking Risk Reduction and assessment program effectiveness.

- Case Study: Reviewing an executive summary and technical appendix from a Nessus scan, focusing on effective communication of Zero-Day risk.

Module 7: Post-Assessment & Integration

- Establishing a Continuous Vulnerability Monitoring strategy.
- Integrating Nessus/OpenVAS output with SIEM tools.
- Using output for Patch Management systems and ticketing
- Performing Verification Scans to confirm successful remediation.
- Advanced automation concepts using APIs/scripting
- Case Study: Implementing a workflow where a critical vulnerability found by Nessus triggers an automated ticket in a helpdesk system and a notification in a SIEM dashboard.

Module 8: Open-Source vs. Commercial Strategy & Future Trends

- Nessus and OpenVAS
- When to choose an open-source tool and when to justify a commercial license.
- Cloud Vulnerability Scanning and DevSecOps Integration.
- Understanding the role of vulnerability scanning in Threat Hunting.
- Preparation for relevant Cybersecurity Certifications
- Case Study: A corporate merger scenario where one company used Nessus and the other OpenVAS; developing a unified vulnerability management strategy.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com