KOENIG
step forward

Nessus Essentials Vulnerability Scanner

Duration: 3 days (24 hrs)

Module 1: Introduction to Nessus Essentials

1. Overview of Nessus Essentials
   - Licensing limitations and capabilities of the free version.
   - Comparison with Nessus Professional.
2. Setting up Nessus Essentials
   - Installation and initial configuration.
   - Activation and registration process.
   - Interface walkthrough.

Module 2: Core Vulnerability Assessment Concepts

1. Understanding Vulnerability Assessment
   - Difference between vulnerability scanning, penetration testing, and compliance audits.
   - Common vulnerabilities and threats.
2. Role of Nessus in Security Assessments
   - Use cases for small-scale environments.
   - Limitations due to tool restrictions.

Module 3: Nessus Policy and Scan Configuration

1. Creating and Managing Scan Policies
   - Policy templates overview.
   - Customizing scan policies for specific environments.
2. Target Selection and Asset Scoping
   - IP range selection and exclusions.
   - Best practices for asset categorization.

Module 4: Performing Vulnerability Scans

1. Types of Scans in Nessus Essentials
   - Basic network scans.
   - Web application scanning (within limits of Essentials).
2. Configuring and Running Scans
   - Optimizing scan settings for speed and accuracy.

- Handling large subnets with scan limitations.

Module 5: Interpreting Scan Results

1. Reviewing Scan Outputs
   - Understanding the Nessus dashboard.
   - Navigating the findings and severity levels.
2. Vulnerability Prioritization
   - Analyzing CVSS scores and impact metrics.
   - Mapping vulnerabilities to critical assets.

Module 6: Reporting and Communication

1. Exporting Scan Results
   - Available formats in Nessus Essentials (e.g., .csv, .html).
   - Creating custom reports for stakeholders.
2. Communicating Vulnerabilities
   - Building concise and actionable reports.
   - Recommended remediations based on findings.

Module 7: Advanced Configuration Techniques

1. Credentialed Scanning
   - Understanding the limitations in Nessus Essentials.
   - Simulating credentialed scans for practice (theory-based).
2. Fine-Tuning Scans
   - Adjusting scan performance settings.
   - Managing plugins and exclusions.

Module 8: Best Practices for Nessus Essentials

1. Ensuring Scanning Accuracy
   - Avoiding common configuration mistakes.
   - Maintaining up-to-date plugins and policies.
2. Leveraging Nessus as Part of a Broader Security Strategy
   - Integrating Nessus outputs with other free tools.
   - Planning the transition to Nessus Professional for scaling.

Please Note: Tools Used: Nessus Essentials (Free Version)