Introduction
https://academy.hackthebox.com/achievement/949661/108

This report provides a comprehensive overview of vulnerability assessment, focusing on the OpenVAS tool. It covers various aspects, from initial setup and configuration to conducting scans, analyzing results, and reporting. This document aims to offer insights into effective vulnerability management and the critical role of structured reporting in information security.
Key Points from Pages 1 to 17

1. **Getting Started with OpenVAS (Page 1-3)**
    - **Installation and Initial Configuration**: Guidance on installing and configuring OpenVAS.
    - **Access and Login Procedures**: Instructions on accessing the OpenVAS web interface.
2. **Scanning Configuration (Page 4-6)**
    - **Setting up Scans**: Steps to create and configure scans in OpenVAS.
    - **Target Specification**: How to define targets for vulnerability scanning.
    - **Scheduling Scans**: Options for scheduling and automating scans.
3. **Scan Execution (Page 7-9)**
    - **Running Scans**: Process of initiating and monitoring scans.
    - **Interpreting Scan Statuses**: Understanding various scan states and progress indicators.
4. **Result Analysis (Page 10-12)**
    - **Understanding Scan Outputs**: Analyzing the results generated by scans.
    - **Vulnerability Severity Levels**: Breakdown of vulnerabilities based on severity.
    - **False Positive Management**: Identifying and handling false positives.
    - **Questions and answers**:

        Q: What is the name of one of the accessible SMB shares from the authenticated Windows scan? (One word)
        **A: wsus**
        Q: What was the target for the authenticated scan?
        **A: 172.16.16.100**
        Q: What is the plugin ID of the highest criticality vulnerability for the Windows authenticated scan?
        **A: 156032**
        Q: What is the name of the vulnerability with plugin ID 26925 from the Windows authenticated scan? (Case sensitive)
        **A: VNC Server Unauthenticated Access**
        Q: What port is the VNC server running on in the authenticated Windows scan?
        **A: 5900**
5. **Exporting Results (Page 13-15)**
    - **Accessing and Viewing Reports**: Instructions on retrieving scan results.
    - **Export Formats**: Various formats available for exporting reports, including XML, CSV, PDF, ITG, and TXT.
    - **Using the openvasreporting tool**: Steps to export results into an Excel document using the openvasreporting tool.
6. **OpenVAS Skills Assessment (Page 16)**
    - **Case Study**: Vulnerability assessment for Inlanefreight's Linux server.
    - **Required Actions**: Detailed instructions for setting up and executing the scan.
    - **Questions and Answers**:
        - Operating System: Ubuntu.
        - FTP Vulnerability: Anonymous FTP Login Reporting.
        - Target IP: 172.16.16.160.
        - HTTP Server Vulnerability: Cleartext Transmission of Sensitive Information via HTTP.
7. **Reporting (Page 17)**

- **Importance of Reporting**: Emphasizing the significance of clear and comprehensive reporting in information security.
- **Structure of a Strong Report**: Guidelines for creating an effective vulnerability assessment report, including sections like Executive Summary, Overview of Assessment, Scope and Duration, and Vulnerabilities and Recommendations.

**Conclusion**

This report outlines the critical steps and considerations in conducting a vulnerability assessment using OpenVAS. From installation to detailed reporting, it underscores the importance of each stage in the process. Proper setup, execution, and analysis of scans are fundamental to identifying potential vulnerabilities. However, the most crucial aspect lies in the effective communication of these findings. Clear, comprehensive reporting not only aids in understanding the current security posture but also guides actionable steps towards enhancing it. As security threats evolve, such assessments and reports become indispensable tools in maintaining robust cybersecurity defenses.