Software Requirements Specification (SRS) for Nmap Security Audit

1. Introduction

1.1 **Purpose** The purpose of this document is to outline the requirements for conducting a security audit using Nmap, a network scanning tool, to assess the security posture of target systems.

1.2 **Scope** This SRS applies to the use of Nmap for security auditing in various network environments, detailing the expected functionalities, user interfaces, and performance metrics.

1.3 **Definitions, Acronyms, and Abbreviations**

- **Nmap**: Network Mapper, a tool for network discovery and security auditing.
- **TCP**: Transmission Control Protocol.
- **UDP**: User Datagram Protocol.
- **SSL**: Secure Sockets Layer.
- **HTTPS**: HyperText Transfer Protocol Secure.

2. Overall Description

2.1 **Product Perspective** Nmap operates independently and can be integrated into larger security audit frameworks. It is a command-line tool but also provides a GUI (Zenmap).

2.2 **Product Functions**

- Network discovery
- Port scanning (TCP/UDP)
- Service detection
- OS fingerprinting
- Vulnerability detection via scripts

2.3 **User Classes and Characteristics**

- **Security Analysts**: Users with knowledge of network security who will interpret scan results.
- **System Administrators**: Users managing networks and servers who require insights on network security.
- **Developers**: Users who need to identify potential vulnerabilities in applications.

2.4 **Operating Environment** Nmap is compatible with multiple operating systems, including:

- Linux
- Windows
- macOS

3. Specific Requirements

3.1 **Functional Requirements**

- **FR1**: The system shall initiate a network scan on a specified target IP address or range.
- **FR2**: The system shall perform TCP/UDP port scanning and identify open ports.
- **FR3**: The system shall provide service and version detection for open ports.
- **FR4**: The system shall conduct OS fingerprinting to identify the operating system running on the target.
- **FR5**: The system shall execute predefined scripts for vulnerability assessment.
- **FR6**: The system shall generate a detailed report of the scan results.

3.2 **Non-Functional Requirements**

- **NFR1**: The system shall complete a scan in a reasonable time, depending on the target size (e.g., less than 10 minutes for small networks).
- **NFR2**: The system shall handle a minimum of 100 concurrent scans without performance degradation.
- **NFR3**: The system shall ensure accurate detection of services and vulnerabilities with a minimum accuracy rate of 90%.
- **NFR4**: The system shall have a user-friendly interface for report generation.

4. System Features

4.1 **User Interface**

- Command-line interface with options for various scanning parameters.
- GUI (Zenmap) with point-and-click functionality for less technical users.

4.2 **Reporting**

- Export options for scan results (e.g., HTML, XML, plain text).
- Summary of findings including open ports, detected services, and potential vulnerabilities.

5. External Interface Requirements

5.1 **Hardware Interfaces**

- Nmap can be run on standard desktop hardware with network interface cards capable of TCP/IP networking.

5.2 **Software Interfaces**

- Integration with third-party tools for enhanced vulnerability assessment (e.g., Metasploit).

6. Performance Requirements

- The tool should be able to handle large networks efficiently, supporting configurable scan intensity levels.

7. Security Requirements

- The system should adhere to security best practices, ensuring that scan operations do not unintentionally disrupt network services.

8. Documentation

- User manuals detailing installation, configuration, and usage.
- Technical documentation for developers and system integrators.