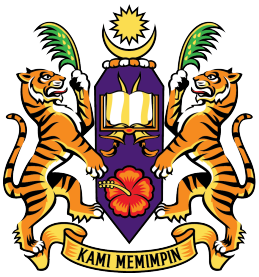

CST334 : NETWORK MONITORING AND SECURITY
CST338 : NETWORK AND COMMUNICATION SECURITY

Port Scanning Detection System
Software Design Description (SDD)

Daniel Hergast
Simon Alix

Date: 16.01.2022

Contents

1 Introduction

1.1 Purpose

The purpose of Software Design Description for the PSDS tool is to organize and plan the structure of the software in a way that is efficient, maintainable, and easy to understand. This includes creating a detailed plan for the software's architecture and functionality, outlining the various components and how they interact with one another. During the design phase, we will determine the requirements for the tool and identify potential challenges or constraints. We will use this information to create a detailed design that outlines the overall structure of the software, including the different modules and components used to build the tool.

The design will also include detailed specifications for each component, such as implementation details, interactions with other components, and the type of data they will handle. This will ensure that we have a clear understanding of the requirements and can begin the implementation phase with a clear plan. A well-designed software will ensure that the tool is efficient and easy to maintain, making it easier to understand the codebase, identify and fix bugs, and make updates to the software.

1.2 Scope

The tool that we are designing as IT developers is aimed at preventing and tracing port scanning attacks that originate from outside of a network. The software is designed to enhance the security of the network by monitoring network traffic for any signs of port scanning activity and alerting network administrators of any detected attempts. Additionally, it will provide information on the source of the attack, such as the IP address and geographical location, to aid in identifying and potentially prosecuting the attacker. The tool will also block any detected port scans from reaching their target, which can improve incident response times and prevent potential damage. The benefits of using this tool include improved network security, faster incident response times, and the ability to monitor for unusual network activity and identify potential security threats.

1.3 Overview

The SDD (Software Design Description) documents for the PSDS (Port Scanning Detection System) will provide a detailed plan of the software's architecture and functionality. It will outline the various components of the system, including the capturing system, port scan detection based on patterns, and the log and alert system. The SDD will also detail the requirements for the tool, including the specific technical requirements, such as the use of Wireshark and Python, as well as the scapy and os libraries. Additionally, the SDD will include information on the design and implementation of the different modules and components of the system, including the buffer, filter, and log file. The SDD will also include information on how these components interact with one another and how they handle different types of data. Overall, the SDD will provide a comprehensive overview of the PSDS system, including the design, functionality, and technical requirements, which will be used to guide the development and testing of the tool.

1.4 Definitions and Acronyms

Term	Definition
PSDS	Port Scanning Detection System
SDD	Software Design Description

2 Considerations for producing an SDD

2.1 Software life cycle

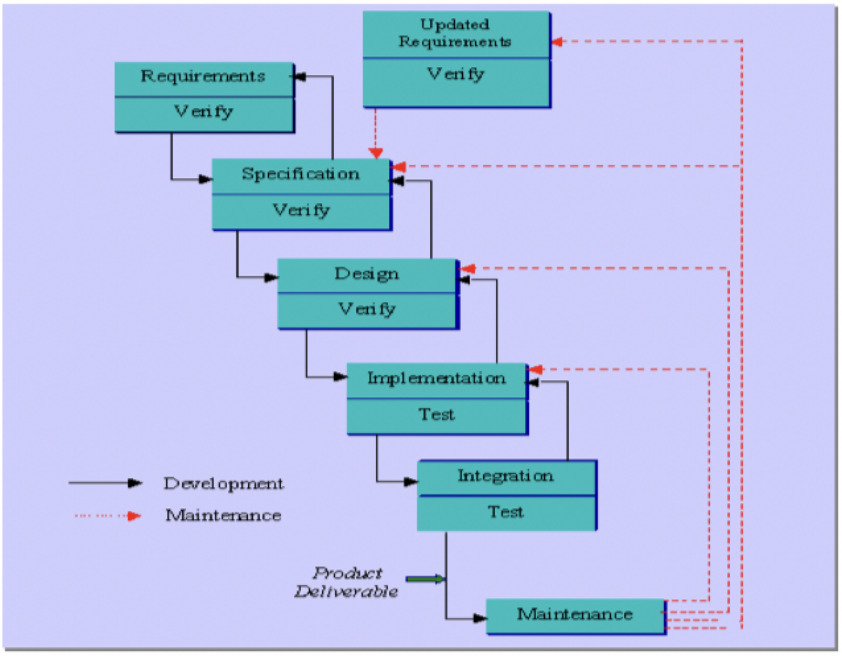

Figure 1: Software life cycle Waterfall Model view

2.2 SDD within the life cycle

During the design phase of our waterfall model life cycle, we developed the SDD for our PSDS tool. We thoroughly evaluated the requirements and specifications of the tool to ensure that it would meet the needs of the user. To ensure that the implementation of the tool would be successful, we created a detailed plan for the software's architecture and functionality, outlining the various components and how they interact with one another. This prototype of the software design was crucial as it allowed us to identify any potential challenges or constraints that may arise during the implementation phase. It also provides a clear understanding of the requirements and a plan of action for the implementation phase. Additionally, having a well-designed software ensures that the tool is efficient, easy to maintain and enables us to fix any issues that may arise during the maintenance phase.

2.3 Purpose of an SDD

The goal of this software design document is to clearly outline the various components of our system, including the different views and how they interact, as well as any constraints or requirements that may impact the overall architecture. It also includes information on how use cases will be implemented, how the system will handle concurrent processes, the different layers and subsystems, and any potential performance considerations. This document serves as a guide for the implementation phase, ensuring that the design is well thought out and can be easily maintained.

3 System Overview

We acknowledge that no network or company is completely immune to cyber attacks. While we cannot completely prevent an attack, we can strengthen our defense by implementing various security tools. Some of these tools actively block attempts while others passively detect intrusions. The PSDS belongs to the latter category, it is a passive security tool designed to detect and log port scanning attempts. Our assumption is that cyber attacks usually begin with a reconnaissance phase, which often involves port scanning. The primary goal of our PSDS tool is to accurately record the date, time, and other details of these attempts, providing a starting point for further analysis of the attack. The PSDS can significantly reduce the time and resources required for packet analysis by focusing on the specific time frame of the attack. Our tool, the PSDS, has three main components: the Network Capturing System, the Pattern-based Port Scan Detection, and the logging and alerting component.:

- The buffer component of our tool is responsible for capturing network traffic on a specific interface and temporarily storing the packets. This buffer allows us to analyze the packet flow at a later time, as we are unable to track it in real-time. The buffer size can be configured using a configuration file, which includes parameters such as buffer size, number of files, and number of packets. These specifications can be adjusted based on the specific needs and resources of the company. For example, in our use case, the operator is required to take a log every day, so the buffer size should be sufficient to store one day's worth of data.

- The second component of our tool is a filter that helps us identify potential scan attacks by analyzing IP packets, particularly TCP packets, and paying close attention to the TCP handshake. We use certain clues, such as a conversation that is only a half-handshake, or a header and windows size that is abnormally short, to identify potential scan attacks. However, this filter cannot be applied to real-time traffic, as it requires tracing back all the conversations and identifying redundant IP addresses. So far, our detection algorithm can detect two types of scan: stealth scan and TCP scan.

- The final component of our tool is the output, which is a log file that collects information about suspicious packets. This includes details such as the name of the .pcap file, the packet number, the type of scan, the IP address of the attacker and the target, and the number of scanned ports. This log file can provide a detailed starting point for further analysis of the attack.

4 Design Description Information

4.1 Introduction

This document is adopted from the Software Engineering Standards Committee of the IEEE Computer Society, "IEEE Recommended Practice for Software Design Descriptions", IEEE Std 1016-1998.

The SDD provides an architectural overview of the PSDS. This document presents to various stakeholders different types of abstraction. It aims to provide the stakeholders a clear understanding of the system.

4.2 Architectural Design

The PSDS tool is a security solution that aims to detect and respond to port scanning attempts on a network. It consists of four main components: the traffic capture module, the packet analysis module, the detection module, and the alert and logging module. The traffic capture module captures network traffic and sends it to the packet analysis module, which analyzes the packets to determine if any suspicious activity is present. If the detection module identifies a port scan, it sends an alert to the alert and logging module which records the event and notifies the administrator. This process is done in a specific sequence to ensure that all potential threats are identified and handled efficiently.

4.3 Use-case View

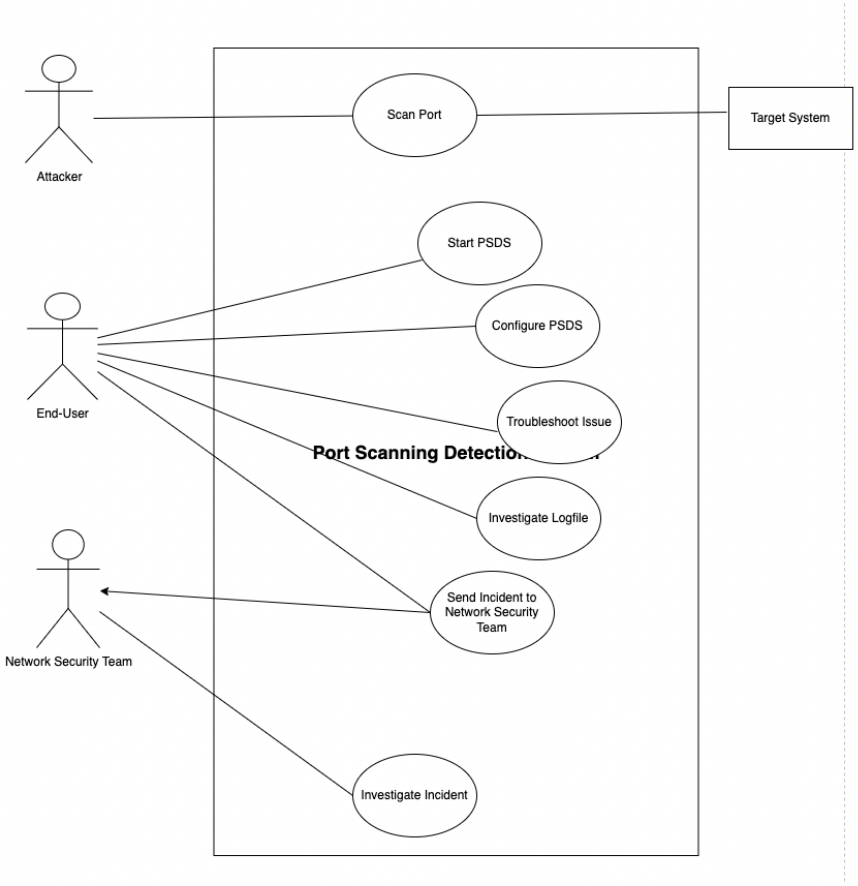

Figure 2: Use-Cases View

4.4 Logical View

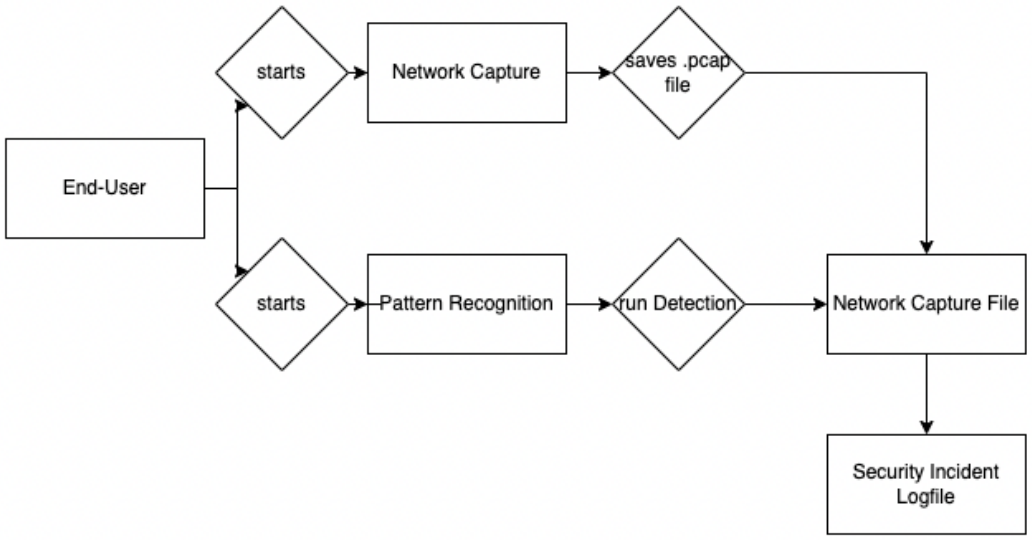

Figure 3: Logical Structure of the Security Incident Logfile

4.5 Decomposition Description

Capturing Traffic Module:

- Input: Raw network traffic packets
- Output: Pcap file

This module is responsible for gathering network traffic data. It uses standard network protocols such as TCP and UDP to capture all incoming and outgoing network traffic. The captured data is then passed to the next module for further processing.

Packet Filter Module:

- Input: Pcap file
- Output: TCP packet

This module is used to narrow down the data to only relevant packets. It uses various filtering criteria such as IP address, port number, and protocol to identify relevant traffic. This filtered data is then passed to the next module for analysis.

Analyser Module:

- Input: TCP packet
- Output: Scan detection results

This module is used to identify any potential port scanning attempts. It uses various techniques such as frequency analysis and sequence analysis to determine whether the filtered traffic data contains any signs of a port scan. If a scan is detected, the information is passed to the log and alert system module for recording and notification.

Log and Alert System Module:

- Input: Scan detection results
- Output: Alert notifications

This module is responsible for recording and notifying of any detected threats. It uses standard logging formats to record all detected scans and provides the ability to configure notifications to be sent to the user via email or SMS.

4.6 Design Rationale

In our architecture tool here are a few potential issues or weaknesses in the design of the PSDS tool:

- False positives: The PSDS tool may generate alerts for legitimate network traffic that is mistaken for a port scan. This could lead to unnecessary investigations and wasted time for the user or administrator.
- False negatives: The PSDS tool may fail to detect actual port scans if the techniques used for detection are not effective or if the scan uses a method that is not covered by the tool.
- Limited coverage: The PSDS tool may only detect port scans on the specific network it is monitoring and may not detect scans on other networks or on different types of attacks.
- Scalability: As the network traffic increases, the PSDS tool might not be able to handle the load and may result in delays or failures in detecting scans.
- Sensitivity: The tool might be too sensitive and generate too many alerts, making it difficult to distinguish between real threats and false positives.
- Complexity: The tool might be too complex to set up, configure, or troubleshoot.
- Lack of flexibility: The tool might not adapt well to new types of scans or have a low level of customization.

5 Data Design

5.1 Data Description

The information domain of the Port Scanning Detection System (PSDS) includes network traffic data, port scan detection results, and system configurations. This information is transformed into various data structures in order to facilitate storage, processing, and organization.

The network traffic data is captured by the system and stored in the form of pcap files, which is a standard format used by Wireshark for capturing network packets.

These packets are then given to the pattern recognition module, which uses various techniques to determine whether the filtered traffic data contains any signs of a port scan. If a scan is detected, the information is passed to the log and alert system module for recording and notification.

The log and alert system module stores the scan detection results in a custom-made data storage solution. This storage solution includes the information detected pcap file name, Packet Number, Type, Source IP-Adress, Target IP-Adress and Port numbe to give maximum information about the security incident and help in further investigations.

The system configurations are stored in a configuration file, which consists of certain setting possibilities for the system. This file is used to configure various parameters such as detection intervals, alerting thresholds and storage times, which are directly related to the company's needs and resources.

5.2 Data Dictionary

Data Item	**Type**	**Description**	**Comment**
File Name	Text	The name of the network capturing .pcap file	
Packet Number	Integer	The packet number of the file	
Type	Text	The type of Port Scan	Can consist of the different types of Scans such as Stealth
Source IP-Adress	Text	The IP-Address of the Attacker	
Target IP-Adress	Text	the IP-Address of the Target	
Port	Integer	The number of the scanned port	

6 Human Interface Design

The PSDS tool does not currently have a graphical user interface (GUI) available. Instead, it must be started and operated through a command line interface (CLI). While this may not be as user-friendly as a GUI, it allows for more advanced options and configurations to be easily accessed and managed. The CLI is accessible to users with basic knowledge of command line navigation and allows for customization and automation of the tool's functions. Additionally, the CLI provides a clear and concise display of the tool's status and output, making it easy for the user to understand and troubleshoot any issues that may arise.