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

Port Scanning Detection System
Software Requirements Specification (SRS)

Daniel Hergast
Simon Alix

`Date: 16.01.2022`

Contents

1 Introduction

1.1 Purpose

The purpose of this document is to present a detailed description of the Port Scanning Detection System (PSDS). It will explain the purpose and features of the system, what the system will do, the constraints under which it must operate and how the system will be implemented and used. This document is intended for both the stakeholders and the developers of the system.

1.2 Scope of Project

This software system is a port scanning detection system that any network security engineer can incorporate into an IDS. This system is designed to help automate network security by detecting potential attacks on the network before they occur by identifying an attacker's reconnaissance. To achieve its practical goals, the product will take an easy-to-use and easy-to-understand rule-based approach to simple but effective low-latency detection.

More specifically, this system will detect port scanning methods on a network using a rule-based and threshold-based pattern recognition approach with alerts informing of a potential intrusion alert. The software will detect any form of scanning, including sophisticated stealth methods such as slow or decoy scanning. In this way, an attacker can be stopped by blocking their IP before an actual attack can take place or important information can be gathered.

1.3 Glossary

Term	**Definition**
Attacker	An individual or group attempting to gain unauthorized access to a target system
Target System	The computer or network that the attacker is attempting to compromise
End-User	The individual who is using the target system and the Port Scanning Detection System for its intended purpose such as IT-Administrator
Network Security Team	A group of individuals responsible for monitoring and protecting a network from cyber threats
Software Requirements Specification	A document that outlines the specific requirements for a software system, including functional and non-functional requirements
.pcap file	A packet capture file that contains a record of network traffic and can be used for network analysis and troubleshooting.
Intrusion Detection System (IDS)	A security system that monitors network traffic and alerts network security team to suspicious activity, such as port scanning.
Port Scanning Detection System (PSDS)	A software or hardware solution used to detect and alert on port scanning activity on a network in order to identify potential security threats.

1.4 References

IEEE. IEEE Std 830-1998 IEEE Recommended Practice for Software Requirements Specifications. IEEE Computer Society, 1998.

1.5 Overview of Document

The next chapter, the Overall Description section, of this document gives an overview of the functionality of the product. It describes the informal requirements and is used to establish a context for the technical requirements specification in the next chapter. The third chapter, Requirements Specification section, of this document is written primarily for the developers and describes in technical terms the details of the functionality of the product.

Both sections of the document describe the same software product in its entirety, but are intended for different audiences and thus use different language.

2 Overall Description

2.1 System Environment

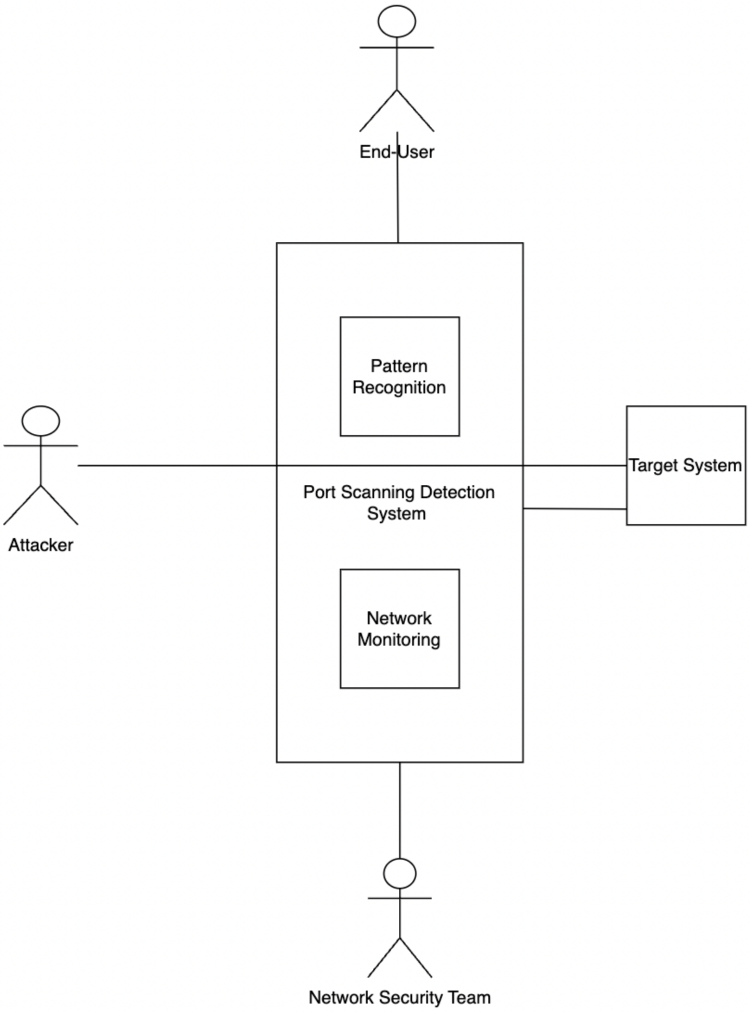


Figure 1: Port Scanning Detection System general view

The port scanning detection system (PSDS) consists of three active actors, namely the attacker, the network security team, and the end user, and one passive actor, the target system or network and a cooperating system consisting of network monitoring and pattern recognition. The attacker, also known as the scanner, initiates the process by attempting to connect to various ports on the target system or network which is connected to the PSDS. The end user's scanning detection system, which consists of Network Monitoring and Pattern Recognition, actively monitors network traffic and identifies and generates alerts for any potentially suspicious port scanning activity. These alerts are then analyzed and acted upon by the network security team, which is responsible for taking appropriate action to mitigate and respond to the detected port scanning attempts.

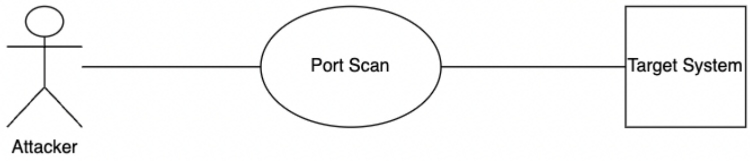
<<The division of the PSDS into two component parts, the Network Monitoring and the Pattern Recognition is an example of using domain classes to make an explanation clearer. >>

2.2 Functional Requirements Specification

This section describes the use cases for each active actor individually. The network security team has only one use case, while the end user who manages the port scanning detection system is the primary actor. The target system is a passive actor in the system whose only purpose is to illustrate the attacked system or network. The attacker shall demonstrate a possible attack that triggers the functions of the PSDS. The following defines a "use case" for the attacker, but it is not a real part of the functional section of the PSDS.

2.2.1 Attacker Use Case

Use case: Port Scan
Diagram:



Brief Description
The attacker attempts to detect open ports on the target system by using various techniques and stealth methods to perform a port scan.

Initial Step-By-Step Description
Before this use case can be initiated, the attacker has identified the IP address of the target system they wish to infiltrate.

1. The attacker uses a port scanner tool, such as Nmap, to send a series of connection requests to various ports on the target system.
2. The target system responds to these requests, indicating whether the ports are open, closed, or filtered.
3. The system logs the Network Activity for further analysis.

2.2.2 End-User Use Case

The End-User has the following sets of use cases:

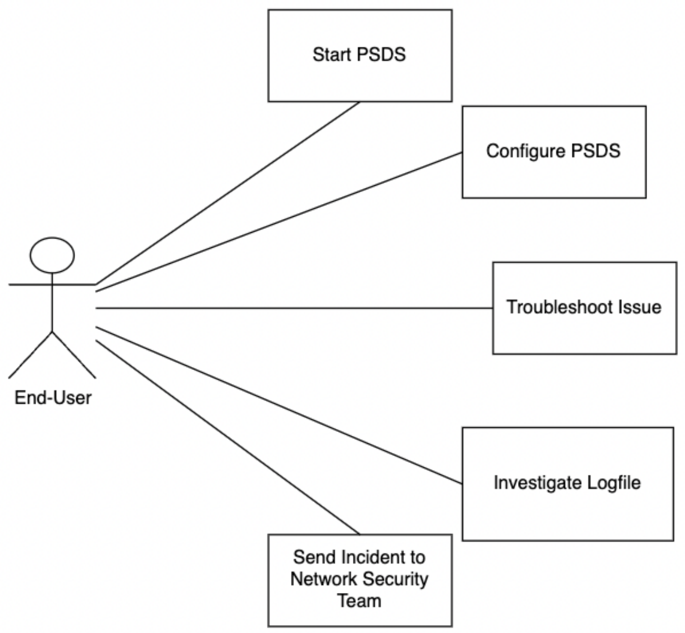
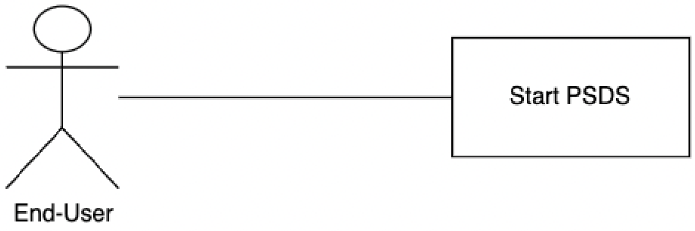


Figure 2: End-User Use Cases

Use case: Start PSDS

Diagram:



Brief Description

The End-User starts the PSDS

Initial Step-By-Step Description

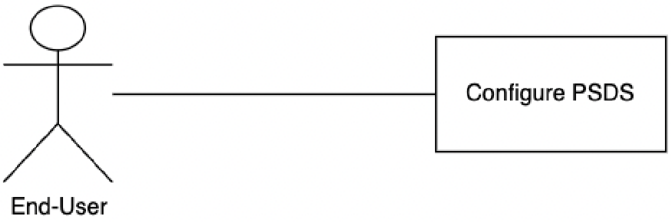
Before this use case can be initiated, the End-User has to setup the network properly, so the PSDS is connected to capture all the network traffic.

1. The End-User types in the proper command to start the PSDS.

2.The PSDS then automatically captures network traffic and analyzes it for specific port scanning patterns.

Use case: Configure PSDS

Diagram:



Brief Description

The End-User opens the configuration file to edit the settings, such as traffic detection intervals, alert thresholds, and storage times.

Initial Step-By-Step Description

Before this use case can be initiated, the End-User has connected to the PSDS.

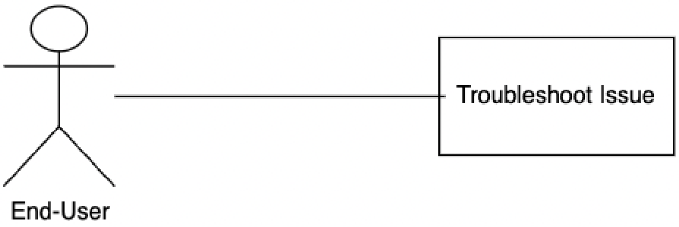
1. The End-User opens the configuration file PSDS.conf.

2. The End-User edits certain settings in the configuration file.

3.The End-User saves the file and restarts the PSDS.

Use case: Troubleshoot Issues

Diagram:



Brief Description

The End-User troubleshoots possible problems.

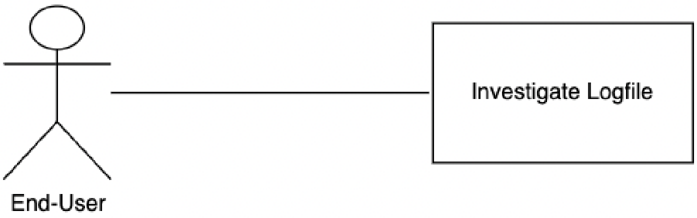
Initial Step-By-Step Description Before this use case can be initiated, the End-User has connected to the PSDS

1. The End-User detects a problem with network detection or pattern recognition.

2.The End-User takes appropriate action to correct the problem, such as restarting the PSDS or changing the configuration.

Use case: Investigate logfile

Diagram:



Brief Description

The End-User receives an email with an alert and examines the associated logfile for further analysis

Initial Step-By-Step Description

Before this use case can be initiated, the End-User has started the PSDS and the PSDS has generated a logfile with security incidents.

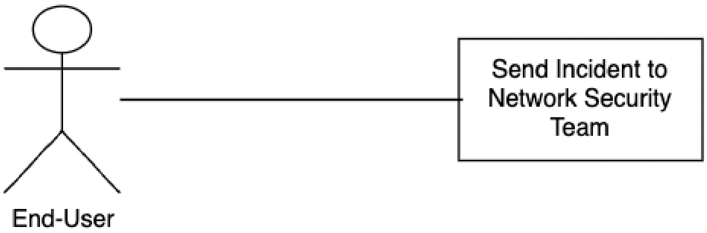
1. The PSDS generates a log file and automatically sends an alert message to the End-User via email.

2.The End-User connects to the PSDS and views the captured security incidents in the repository.

3.The End-User Decides if it is legitimate, and then forwards it to the Network Security Team or not, and then edits the configuration

Use case: Send Incident to Network Security Team

Diagram:



Brief Description

The End-User discovers a legitimate network incident in the log file and notifies the Network Security Team for further analysis.

Initial Step-By-Step Description

Before this use case can be initiated, the End-User has started the PSDS and a logfile with a Security Incident has been constructed.

1. The End-User accepts the logfile as a serious security incident.

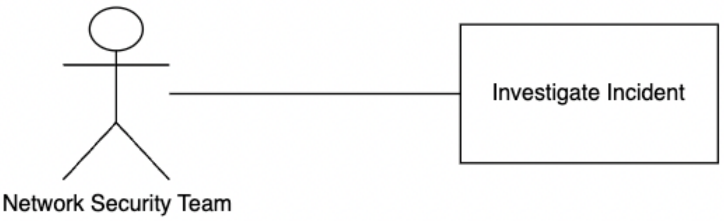
2. The End-User Informs the network security team via any means of communication to analyze the incident and take appropriate action.

2.2.3 Network Security Team Use Case

The responsibility for Network Security can be assigned to a group of individuals or a single person, who could be a member of the IT Administration Team or a seperate Network Security Team.

Use case: Investigate Incident

Diagram:



Brief Description

The Network Security Team opens log files provided by the IT administrator and recorded network traffic to investigate security incidents..

Initial Step-By-Step Description

Before this use case can be initiated, the End-User has received authentic security issues in a log file sent to the Network Security Team.

1. The Network Security Team connects to the PSDS

2. The Network Security Team opens the network traffic file belonging to the log file and the log file itself of the security incident for further analysis.

3.The Network Security Team takes appropriate action to address detected security incidents such as IP blocking

2.3 User Characteristics

The attacker would typically be an individual a group or an organisation attempting to gain unauthorized access to a computer or network. They may use automated tools with different approaches to scan for open ports on the target system in order to identify vulnerabilities that can be exploited.

The target system would be the computer or network that the attacker is attempting to gain access to. This could include servers, desktop computers, or other devices connected to a network.

The network security team would be responsible for monitoring and protecting the target system from unauthorized access. They would use specific reports and alerts from the port scanning detection system to identify potential threats and take appropriate action to protect the network. They are expected to be professionals in the field of IT-Security.

The end-user of a port scanning detection system would typically be a system administrator or other IT professional responsible for maintaining the target system. They would use and manage the port scanning detection system to monitor for threats and generate reports and alerts to be sent to the security team.

2.4 Non-Functional Requirements

The port scanning detection system will be part of an intrusion detection system (IDS) and will be installed at the edge of a network to monitor all traffic within that network. The system should comply with industry standards and regulations and have low latency and high throughput. It must be scalable to handle increasing network size. The system must also be robust in its reliability and easily updated and maintained with an attacker's evolving techniques.

3 Requirements Specification

3.1 External Interface Requirements

The port scanning detection system must be able to detect all network traffic from different network types such as Ethernet, WiFi and cellular networks (if any). It must be able to support all required communication protocols such as TCP, UDP, and ICMP so that it can detect and analyze port scans. In addition, it is important that the system can generate reports and alerts for the network security team based on network monitoring and pattern recognition rules. A management and remote interface is also required to update and maintain the system. Finally, it might also be necessary to include an API to integrate the system with an existing IDS (optional).

3.2 Functional Requirements

3.2.1 Scan Port

An attacker's port scan is the scenario that triggers the PSDS. It is not a real use case of the system, but is shown to illustrate the usage pattern of the system and can occur at any stage. (see Section 2.2.1

3.2.2 Start PSDS

Use Case Name	Start PSDS
XRef	Section 2.2.2, Start PSDS
Trigger	The End-User initiates the Network Capturing System by inputting the appropriate commands in the Command Line Interface (CLI)
Precondition	The PSDS is properly connected at the edge of the network, ready to detect and alert on any port scanning activity
Basic Path	1. The End-User initiates the Network Capturing System by entering the correct commands in the Command Line Interface (CLI). 2. The user activates the Pattern Recognition Engine by inputting the necessary commands in the CLI.
Alternative Paths	The End-User has the capability to independently start and restart both the Network Capturing System and the Pattern Recognition Engine using the appropriate commands in the Command Line Interface (CLI)
Postcondition	Once the Network Capturing System and the Pattern Recognition Engine are activated, the system will continuously run in the background, capturing network data and analyzing it for any signs of security incidents. The captured network data is automatically saved into a file for further analysis. The Pattern Recognition Engine also runs in the background, constantly scanning for any signs of security incidents and if detected, the incident will be recorded in a log file for future reference
Exception Paths	The End-User has the capability to stop both the Network Capturing System and the Pattern Recognition Engine independently at any time, by inputting the appropriate commands in the Command Line Interface (CLI). This allows the user to control the operation of the PSDS, and turn off the engines whenever it's necessary
Other	None

3.2.3 Configure PSDS

Use Case Name	Configure PSDS
XRef	Section 2.2.2, Configure PSDS
Trigger	The End-User opens the Configuration file in the PSDS Directory
Precondition	The PSDS has been installed
Basic Path	1. The End-User sees a Configuration file with the Variables ”CapturingInterval”, ”DeletionTime”, different Threshhold values and ”Emailaddress”. 2. The End-User can modify these settings as necessary to optimize the performance of the PSDS and to suit their specific needs. 3. The End-User saves the file. 4. The End-User restarts the engines.
Alternative Paths	None
Postcondition	The Configuration of the PSDS has been changed.
Exception Paths	The End-User can restore the file to its original settings or discard the changes.
Other	None

3.2.4 Troubleshoot Issues

Use Case Name	Troubleshoot Issues
XRef	Section 2.2.2, Troubleshoot Issues
Trigger	The End-User encounters any issues while using the PSDS.
Precondition	The End-User has started the PSDS.
Basic Path	1. Check the log files in the PSDS directory for any error messages or warnings that can provide insight into the problem. 2. Review the Configuration file to ensure that the settings are correctly configured. 3.Verify that the PSDS is properly connected to the network and that all necessary components are functioning correctly. 4. Check the online documentation or contact the vendor’s support for additional help. 5. If the issue persists, The End-User can also seek help from an IT professional or network administrator who is familiar with the PSDS.
Alternative Paths	The End-User can encounter Issues at any time.
Postcondition	The End-User has fixed the issue or has contacted the vendor for support.
Exception Paths	None
Other	None

3.2.5 Investigate Logfile

Use Case Name	Investigate Logfile
XRef	Section 2.2.2, Investigate Logfile
Trigger	The End-User has been notified withan alert via email that a new logfile is available for review
Precondition	The End-User configured the PSDS properly.
Basic Path	1. The End-User checks the alert email in their inbox and sees that there is a new log file with a timestamp available. 2. The End-User accesses the log file by navigating to the PSDS directory where the file is stored and reviews the contents of the file. 3.The End-User evaluates the severity of the incident by analyzing the information in the log file, such as the type of attack, the source and destination IP addresses, and the date and time it occurred. 4.Based on the seriousness of the incident, the End-User takes appropriate action, such as forwarding the incident to the Network Security Team for further investigation or modifying the Configuration file to prevent future occurrences. They can also decide to escalate the incident to upper management for a more comprehensive solution.
Alternative Paths	None
Postcondition	The End-User has forwarded the Incident to the Network Security Team or configured the PSDS differently
Exception Paths	None
Other	None

3.2.6 Send Incidents to the Network Security Team

Use Case Name	Send Incidents to the Network Security Team
XRef	Section 2.2.2, Send Incidents to the Network Security Team
Trigger	The End-User has recieved an alert with a logfile of a security incident
Precondition	The PSDS has decided that the security incident is serious.
Basic Path	1. The End-User forwards the alert via email to the Network Security Team.
Alternative Paths	The End-User has the ability to review the log file containing information about the security incident at any time and make a decision regarding the incident.
Postcondition	The Security Incident Alert is being investigated by the Network Security Team.
Exception Paths	None
Other	None

3.2.7 Investigate Incidents

Use Case Name	Investigate Incidents
XRef	Section 2.2.3, Investigate Incidents
Trigger	The Network Security Team has received an email with an alert about a possible security incident.
Precondition	A logfile indicating a security incident has been generated and the End-User has determined it to be of significant concern.
Basic Path	1. The Network Security Team accesses the PSDS Directory. 2. The team examines the logfile associated with the received security incident alert. 3. The Network Traffic is analyzed at the timestamp of the security incident in the logfile to further investigate the incident. 4.The Network Security Team takes necessary actions to protect the network, such as blocking the IP that was used for scanning, or implementing other appropriate measures.
Alternative Paths	The Network Security Team can initiate their investigation at any point.
Postcondition	The Network Security Team has implemented the necessary measures to defend the network and has also saved a copy of the logfile as a backup..
Exception Paths	The Network Security Team decides that the logfile does not contain a security incident.
Other	None

3.3 Detailed Non-Functional Requirements

3.3.1 Logical Structure of the Logfile Data

The logical structure of the data to be stored as a logfile of a security incident is given below.

The logical structure of the security incident logfile data is as follow:

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	

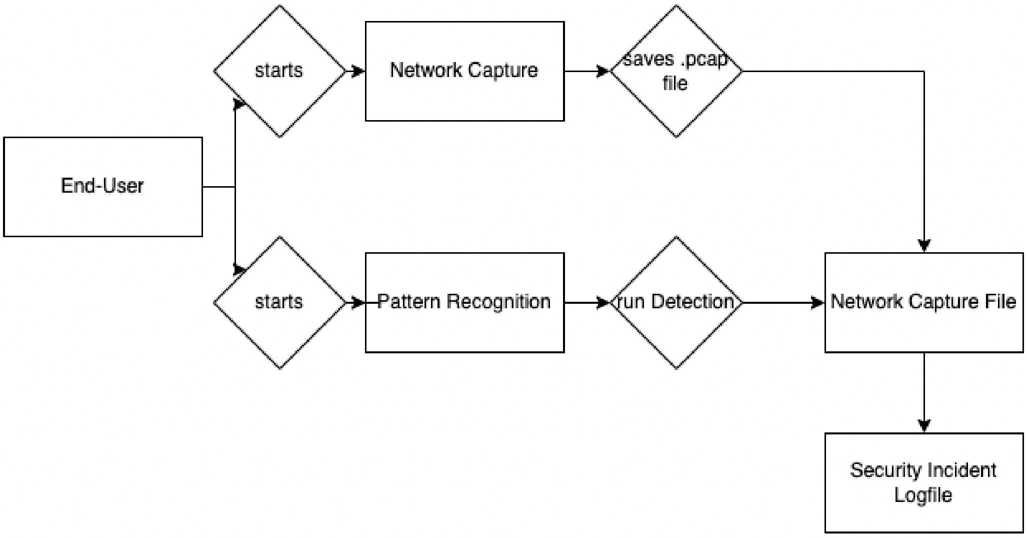


Figure 3: Logical Structure of the Security Incident Logfile

3.3.2 Scalability and Reliability

The system should have a distributed architecture to meet both of these demands since it enables horizontal expansion and redundancy, allowing it to handle heavy traffic and guarantee high availability. The system should also have a strong and trustworthy detection algorithm that can recognise port scans with accuracy and minimise false positives.