TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Hendrik Jaanimägi 192846IADB

Cyber Defence System Management System for Autonomous Vehicles

"Building Distributed Systems" coursework

Supervisor: Andres Käver
[Academic degree]

Tallinn 2023

Tallinn 2023

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Hendrik Jaanimägi

17.02.2023

Abstract

[Text]

This thesis is written in English and is [number of pages in main document] pages long, including [number] chapters, [number] figures and [number] tables.

Annotatsioon

Sõiduki ohuhaldussüsteem

[Tekst]

Antud tees on kirjutatud inglise keeles ning sisaldab teksti [lehekülgede arv] leheküljel, [peatükkide arv] peatükki, [jooniste arv] joonist, [tabelite arv] tabelit.

List of abbreviations and terms

CDSMS	Cyber Defence System Management System

Table of contents

List of Figures

…

List of tables

...

1 Introduction

While there is a lot of research into cyber-attack detection on autonomous vehicular platforms, currently, no commercial product is available to address threats on such targets. Most relevant research focuses on one-dimensional attack vectors or does not consider the broadest scope of potential cyber threats. None of the previous studies has considered the idea of implementing an automated response to the detection of attacks. The Cyber Defence System Management System (CDSMS) strives to fill these gaps, acting as an intrusion detection platform capable of monitoring for evidence of a compromise or an attack from cyber, physical exploitation, and electromagnetic threat vectors. In the event of a potential attack, the system will provide an appropriate mitigating response to secure or contain the threat autonomously, ensuring the resiliency of a vehicular platform while in an operational environment.

The role of the CDSMS is to help ensure that a vehicular platform is “cyber secure”. To fulfil the latter, the CDSMS needs to be capable of detecting malicious activity, including cyber and electronic warfare domains, and apply proportional threat responses rather than ensure an unbreachable system. The latter is achieved by detecting threats, analysing them, and providing relevant platform components with either a recommendation or a response action that would attempt a graceful degradation of the overall system. The outcome of the CDSMS is to provide a complete cybers defence system that vendors can integrate into any autonomous vehicular platform.

This project aims to develop a threat management system on top of a vehicular platform’s existing data bus and various logging layers by creating a unified backend service and a frontend client for managing a platform’s threat management needs.

2 System Requirements

The CDSMS needs to fulfil the following system requirements:

- The CDSMS shall provide the platform with interfaces for receiving mirrored network traffic, telemetry, and other log data.
- The CDSMS shall provide an interface for publishing response recommendations and actions to relevant platform components.
- The CDSMS shall provide the platform's operator with a blueprint editor for configuring various system events as threats or otherwise informational threats.
- The CDSMS shall provide the platform with means for vulnerability management.
- The CDSMS shall provide the platform with means for asset management.
- The CDSMS shall detect and respond to threats within the vehicular platform and from connected external systems.
- The CDSMS shall provide recommendations for mitigating threats in a manner that allows for graceful degradation of the platform's components where possible.
- The CDSMS shall provide recommendations for actions to disconnect the platform's components from networks and reset or power off components to implement a decided threat response.
- The CDSMS shall provide a human interface for managing a platform's threat detection and response configuration.

2.1 Assumptions

The CDSMS design takes into consideration the following assumptions about the vehicular platform:

- The platform’s C2 has the final call after a CDSMS-initiated response recommendation unless specified as an automated response.
- …

3 System Architecture

…

3.1 Entity-Relationship Diagram

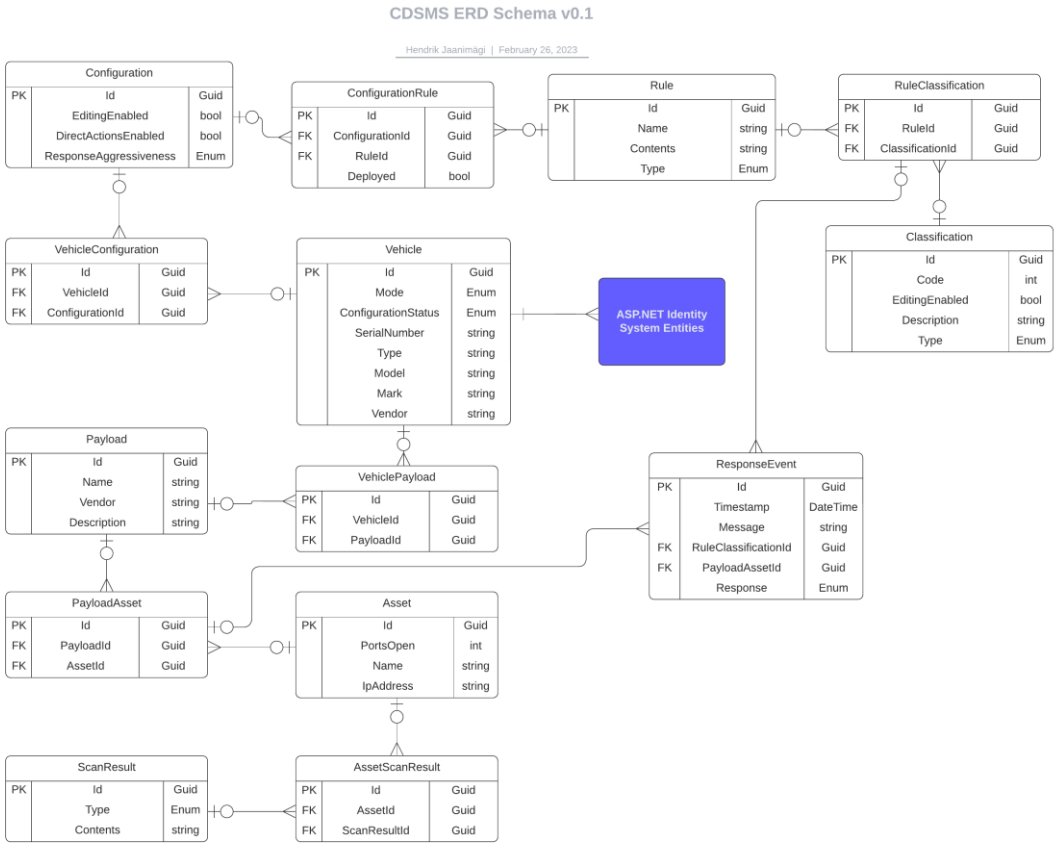

Figure 1. CDSMS ERD Schema.

Figure 1 represents the complete ERD schema of the CDSMS with relationships and entity attributes defined.

3.2 Third-Party Dependencies

…

4 Interfaces

4.1 REST API Endpoints

…

4.2 Web Application

The following figures represent CDSMS views available in its web interface.

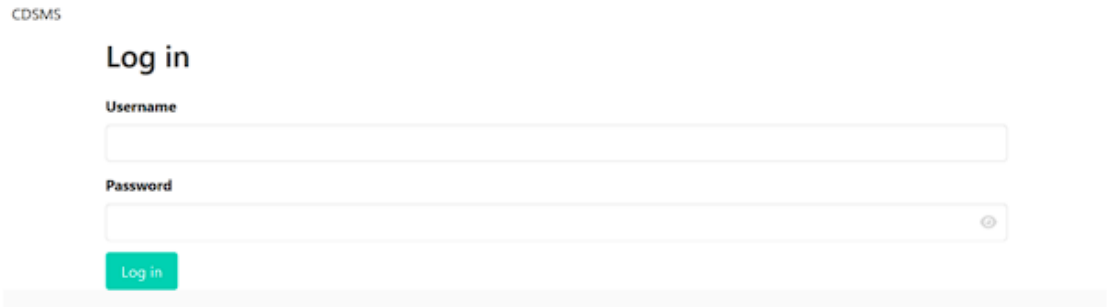

Figure 2. CDSMS User Login View.

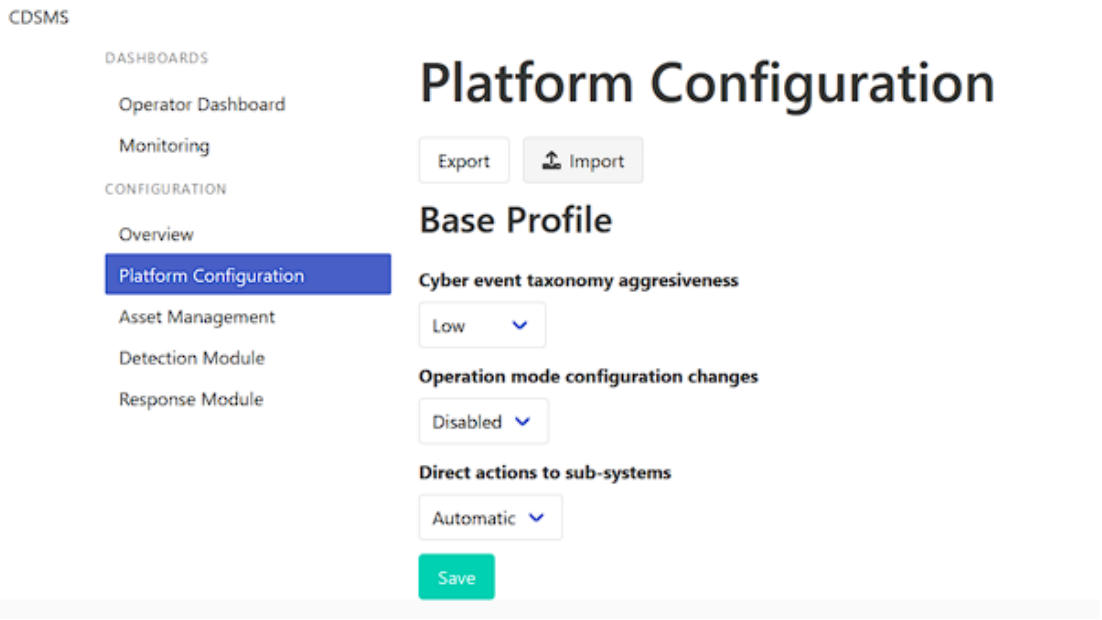

Figure 3. CDSMS Platform Configuration View.

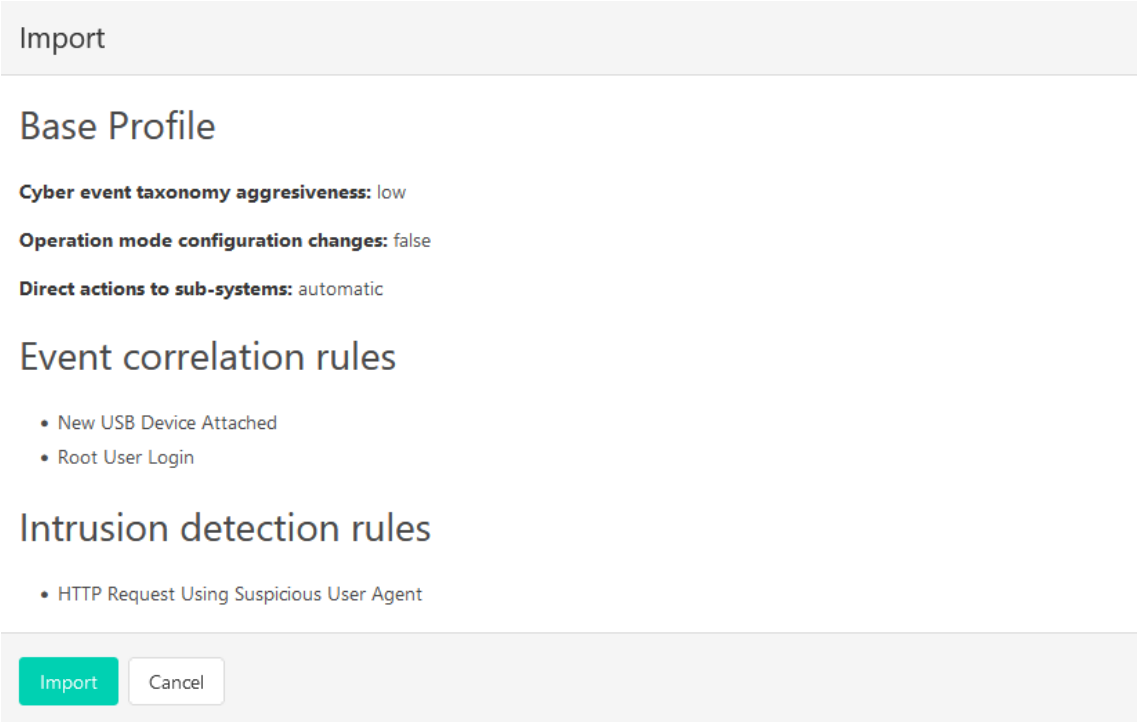

Figure 4. CDSMS Configuration Import View.

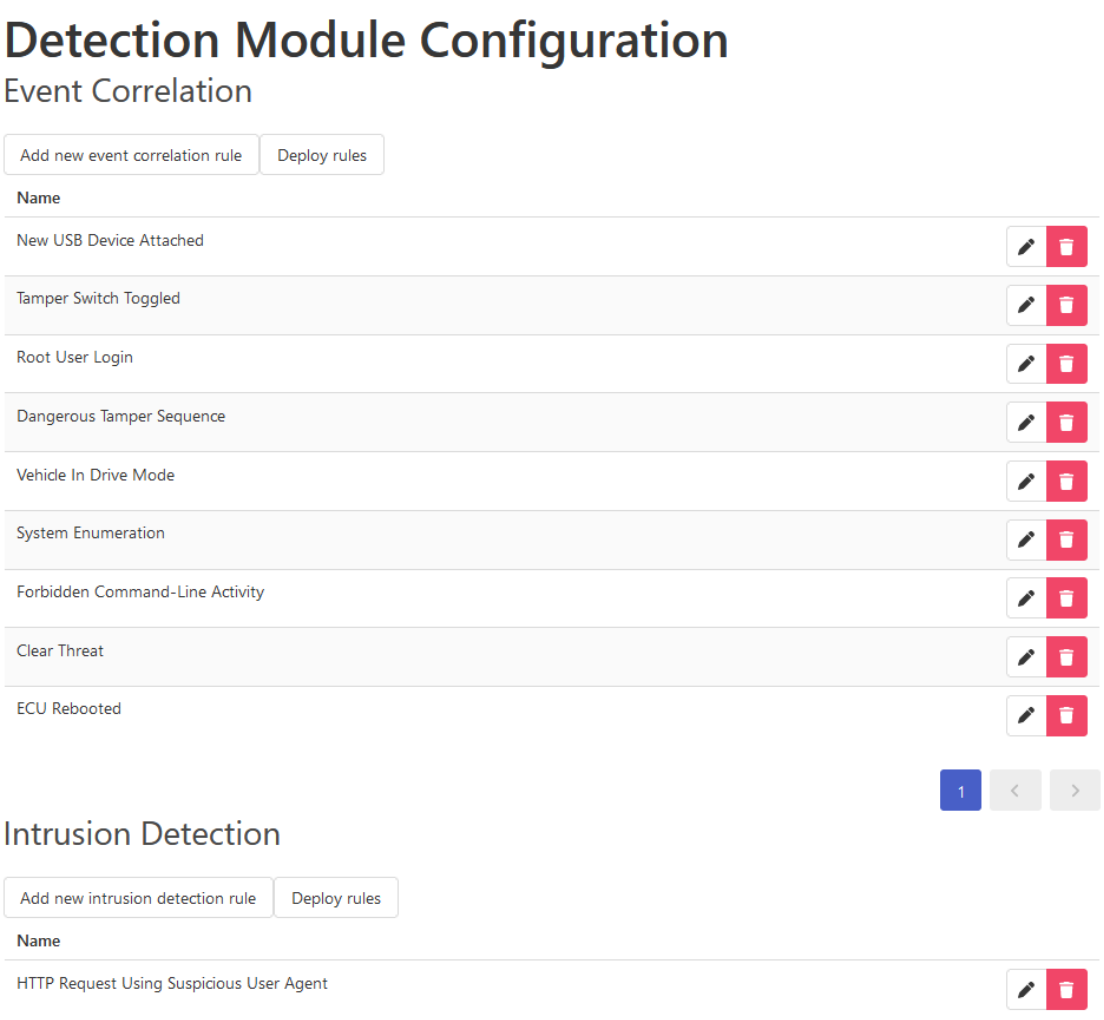

Figure 5. CDSMS Detection Module Configuration View.

Figure 6. CDSMS Event Correlation Rule Creation View.

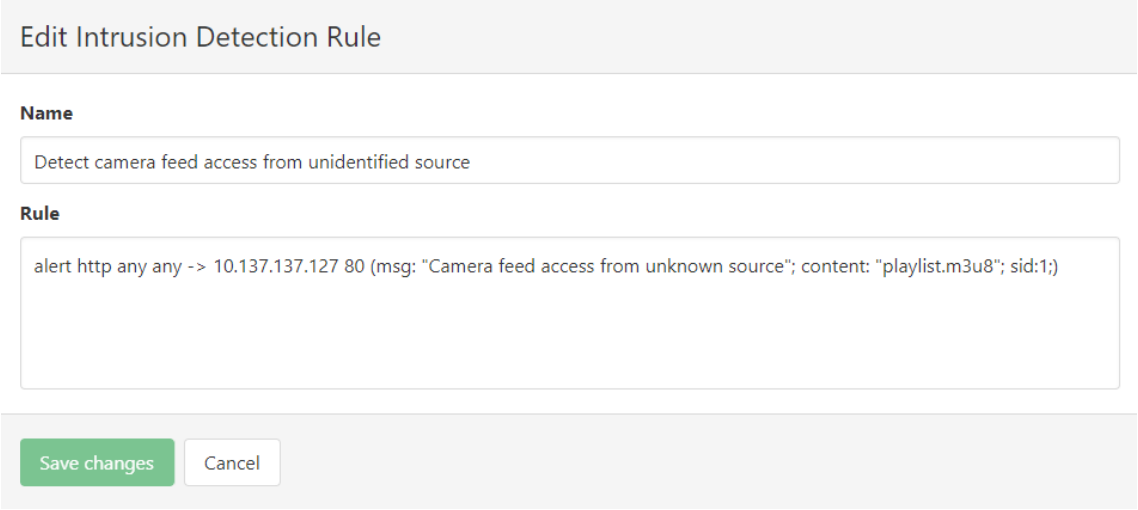

Figure 7. CDSMS Intrusion Detection Signature Creation View.

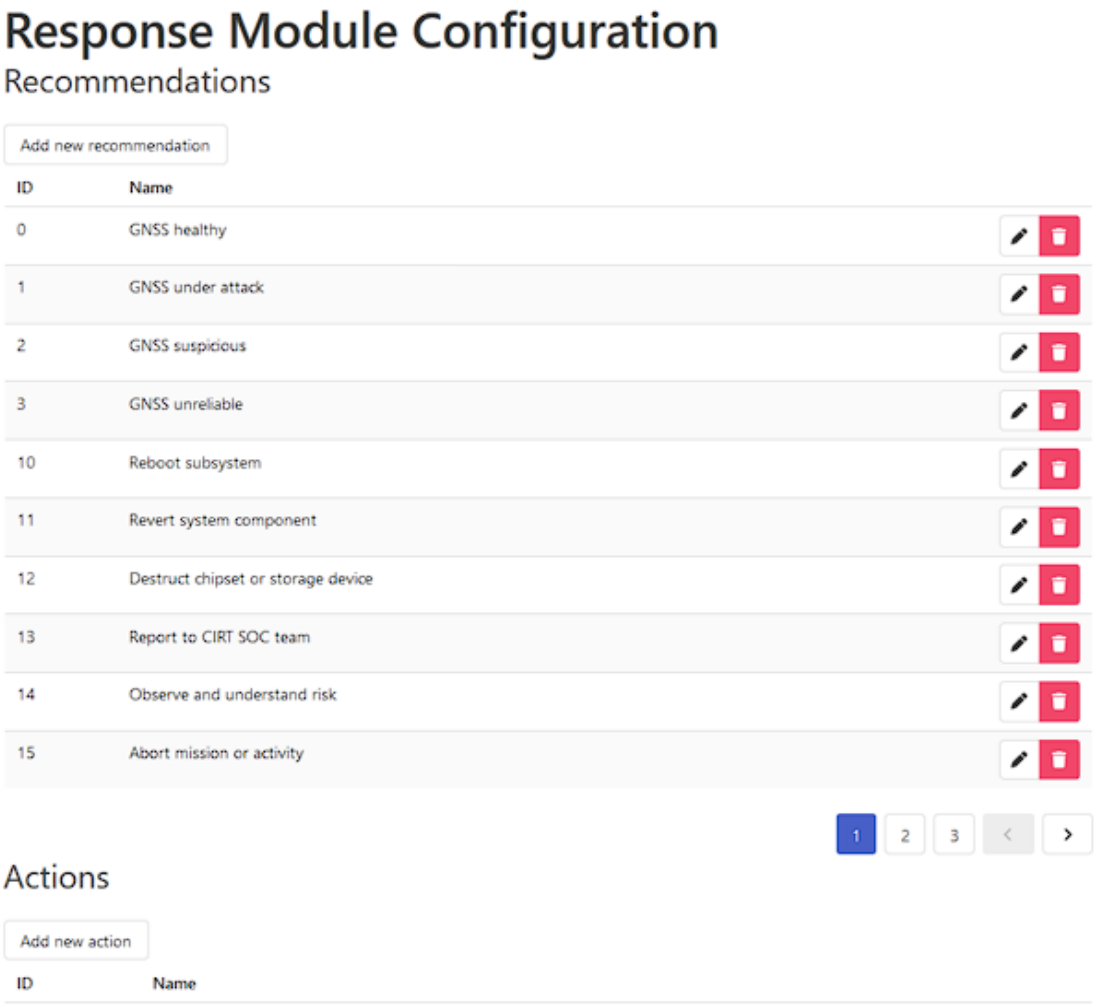

Figure 8. CDSMS Decision Matrix Configuration View.

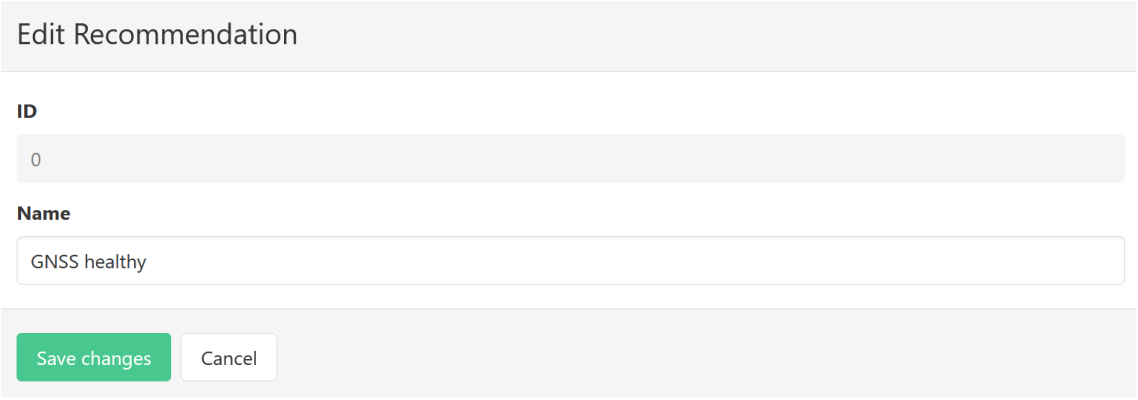

Figure 9. CDSMS Decision Matrix Response Recommendation Modal View.

Monitoring

Timestamp	Source	Message
11/11/2022, 4:02:16 PM	Correlation	Closed an SSH session for the root user (ECU)
11/11/2022, 9:13:52 AM	Correlation	Opened an SSH session for the root user (ECU)
11/8/2022, 11:48:42 AM	Correlation	Potential system compromise detected. Forbidden command-line activity during operational mode.
11/8/2022, 11:47:35 AM	Correlation	Suspicious command "lsblk" execution during drive mode
11/8/2022, 11:47:20 AM	Correlation	Suspicious command "uname -a" execution during drive mode
11/8/2022, 11:46:39 AM	Correlation	Vehicle in drive mode
11/8/2022, 11:22:25 AM	Correlation	Dangerous tamper sequence detected
11/8/2022, 11:20:14 AM	Correlation	New USB device attached to ECU

Figure 10. CDSMS Event Monitoring View.

Asset Management

Scan for assets | Enumerate assets

Name	IP address	Ports	Vulnerabilities
	10.128.7.4	1	
dhcp	10.128.7.208	2	1
cds	10.128.7.209	4	
gstreamer	10.128.7.210	2	
ecu	10.128.7.211	5	
	10.128.7.212	8	1
attack	10.128.7.213	1	
	10.128.7.214	5	
	10.128.7.217	27	12 52 12 5
	10.128.7.218	2	1 4
	10.128.7.220	2	

Figure 11. CDSMS Asset Management View.

Figure 12. CDSMS Asset Management Modal View.

10.128.7.217

Ports

Port	Name	Report
21/tcp	ftp	Port 21/tcp was found to be open
22/tcp	ssh	Port 22/tcp was found to be open
25/tcp	smtp	Port 25/tcp was found to be open
68/udp		Port 68/udp was found to be open
80/tcp	www	Port 80/tcp was found to be open
123/udp	ntp	Port 123/udp was found to be open
137/udp	netbios-ns	Port 137/udp was found to be open
138/udp		Port 138/udp was found to be open
139/tcp	smb	Port 139/tcp was found to be open
161/udp	snmp	Port 161/udp was found to be open
443/tcp	www	Port 443/tcp was found to be open
445/tcp	cifs	Port 445/tcp was found to be open

Figure 13. CDSMS Asset Management Enumeration Modal View – Discovered Ports.

Vulnerabilities

Category	Name	Severity ↓
Misc.	Samba 'AndX' Request Heap-Based Buffer Overflow	critical
Service detection	SSL Version 2 and 3 Protocol Detection	critical
SNMP	SNMP Agent Default Community Name (public)	high
General	Samba Badlock Vulnerability	high
Service detection	rlogin Service Detection	high
Misc.	OpenSSL Heartbeat Information Disclosure (Heartbleed)	high
Misc.	Network Time Protocol Daemon (ntpd) monlist Command Enabled DoS	high
General	SSL Certificate Signed Using Weak Hashing Algorithm	high
General	SSL Medium Strength Cipher Suites Supported (SWEET32)	high
Service detection	TLS Version 1.1 Protocol Deprecated	medium
Service detection	SSL Anonymous Cipher Suites Supported	medium
Misc.	SSH Weak Algorithms Supported	medium
SNMP	SNMP 'GETBULK' Reflection DDoS	medium
SMTP problems	SMTP Service STARTTLS Plaintext Command Injection	medium

Figure 14. CDSMS Asset Management Enumeration Modal View - Vulnerabilities.

5 Further Development

…

6 Summary

This coursework aimed to create a cyber defence system that would effectively detect cyber-attack against autonomous vehicular platforms and apply proportional mitigation tactics to such attacks rather than ensure an unbreachable system. To achieve the goal, the author used the following:

- …

The outcome of the work is a working implementation of a cyber defence system that can be integrated into autonomous vehicles and increase their cyber defence capabilities.

References

There are no sources in the current document.

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I [First name Middle name Last name]

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "[Thesis title]" , supervised by [Supervisor's name]
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

[dd.mm.yyyy]

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.