AMMAN ARAB UNIVERSITY

جامعة عمان العربيـــــة

College of Computer Sciences and Informatics

كلية العلوم الحاسوبية والمعلوماتية

TRIPLE O DETECTION AND ANALYSIS TOOL

: Students

Name: Oday Raed Qammoh ID: 202010070

Name: Omar Riziq Mabsot ID: 202110708

Name: Omar Thaer Awad ID: 202110262

Supervisor

Dr. Dyala Ibrahim

A project report submitted in partial fulfillment of the requirements

for B.Sc. degree in ***Cybersecurity***

Amman – Jordan

Acknowledgements

We would like to express our profound gratitude to all these individuals for supporting us in completing this project.

A special thanks is due to the dean of the college Dr.hussam Al-hammad for his part in improving the faculty of computer science and informatics and supporting it’s students as well as providing us with many opportunities regarding our major.

We would also like to express our sincere gratitude to our supervisor Dr.Dyala Ibrahim for being with us in this project since the start and walking us through it step by step as well as encouraging and motivating us to aim for higher results and achievements.

Lastly, we thank the entire education faculty for providing us with advice and suggestions. Additionally, we are eternally grateful to our families and friends for their continued support.

Omar Awad
Omar Mabsot
Oday Qammoh

Abstract

The documentation for the graduation project titled "Triple O Detection and analysis tool" presents a comprehensive overview of a sophisticated system designed to detect and analyze threats within a network environment. This project aims to enhance network security by implementing advanced algorithms and techniques for threat detection, classification, and response.

The system utilizes a combination of signature-based detection and anomaly detection algorithms to identify potential threats such as malware, intrusions, and suspicious activities. Through real-time monitoring and analysis of network traffic, the system can promptly detect security incidents, thereby minimizing the risk of data breaches and unauthorized access.

Key features of the project include a user-friendly interface for monitoring network activity and detailed threat reports. This documentation provides an introduction, defines objectives, establishes a scope, introduces upcoming issues and challenges, sets requirements and evaluation metrics to demonstrate the effectiveness and reliability of the proposed solution.

Overall, this graduation project contributes to the field of cybersecurity by offering a robust and reactive approach to network threat detection and analysis, empowering organizations to safeguard their networks against evolving cyber threats effectively.

List of Tables

List of Figures

List of abbreviations

TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual private network
API	Application Programming Interface
CPU	Central Processing Unit
DNS	Domain Name System
PKI	Public Key Infrastructure
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
JSON	JavaScript Object Notation
LAN	Local Area Network
MAC	Media Access Control

NIDS	Network-Based Intrusion Detection System
NIPS	Network-Based Intrusion Prevention System
OS	Operating System
PCAP	Packet Capture
RDP	Remote Desktop Protocol
SMTP	Simple Mail Transfer Protocol

CHAPTER 1

INTRODUCTION

1.1 Overview

The project aims to develop a tool for analyzing and detecting viruses and malware in networks and routers. This tool will enhance network security by identifying and suggesting solutions for threats to data integrity and system functionality.

1.2 Problem Statement

Networks and routers are vulnerable to various forms of malware, viruses, and numerous technical issues that can compromise data security and disrupt network operations. The lack of effective tools to detect and analyze these threats poses a significant risk to organizations and individuals.

1.3 Project Objectives

- Develop a comprehensive tool capable of analyzing network traffic for viruses and malware.
- Implement robust detection algorithms to identify and classify different types of threats.
- Enhance the tool's capabilities to detect malware in routers.
- Provide real-time alerts and notifications for immediate response to security breaches.
- Ensure compatibility with a wide range of network configurations and router models.

1.4 Research Strategy (Framework)

The research strategy will involve a combination of literature review, data collection, algorithm development, and testing. Key steps include:

1. Reviewing existing literature on malware detection techniques in networks.
2. Collecting data on common malware signatures and network vulnerabilities.
3. Developing detection algorithms based on anomaly and signature recognition.
4. Testing the tool in simulated and real-world network environments to evaluate its effectiveness.

1.5 Scope

The project will focus on developing a software tool for analyzing and detecting viruses and malware in network traffic and routers. The tool will not address physical security measures or hardware vulnerabilities in routers, nor will it mitigate threats or vulnerabilities on it's own (needs human help). The tool will provide a detailed report for the user about issues in the network so that they are aware and can then resolve them.

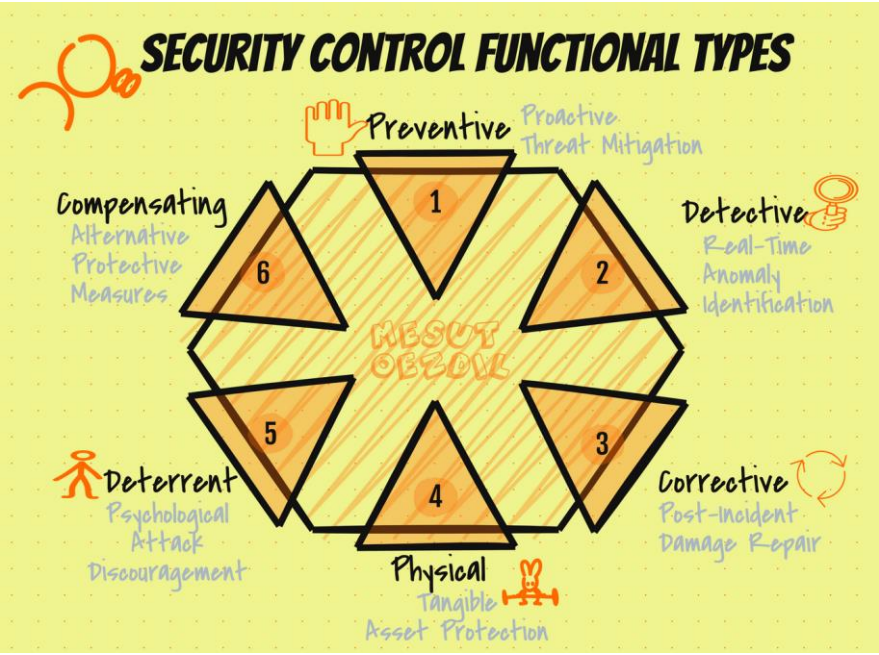

Figure (1.1)

1.6 Gantt Chart

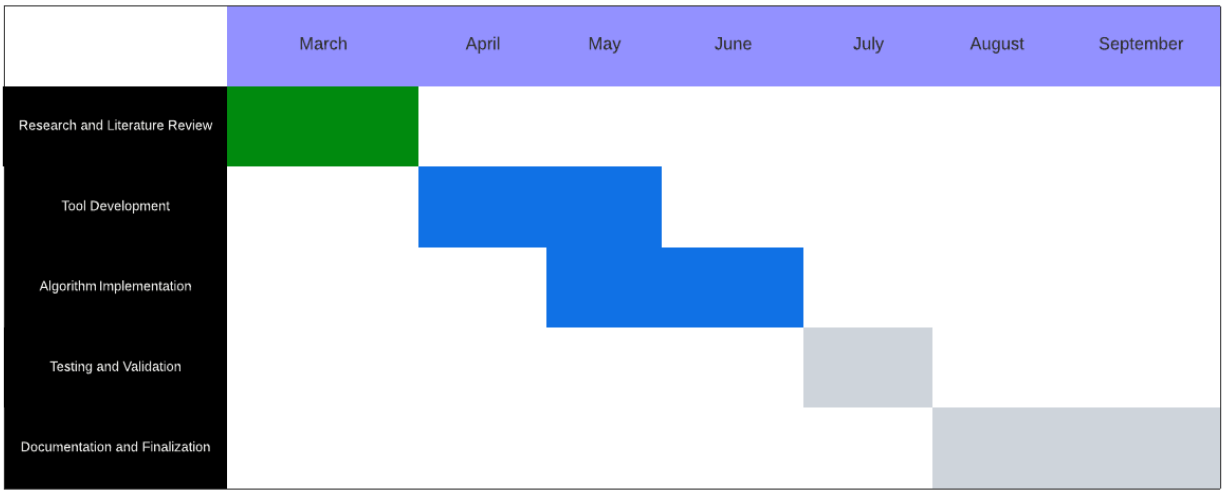

Figure (1.2)

The Gantt chart outlines the project timeline and key milestones:

- Research and Literature Review: 1 month
- Tool Development: 2 months
- Algorithm Implementation: 2 months
- Testing and Validation: 1 month
- Documentation and Finalization: 2 months

1.7 Project Outline

1. Introduction: Overview of the project and its significance.
2. Literature Review: Review of existing research on malware detection in networks.
3. Methodology: Description of the research strategy and framework.
4. Design Models: Details on the design and implementation of the malware detection tool.
5. Experiments and results: Evaluation of the tool's performance in detecting viruses and malware.
6. Conclusion and future works: Analysis of the findings and implications for network security. Summary of the project outcomes and future recommendations.

CHAPTER 2

LITERATURE REVIEW

Overview 2.1

The literature review delves into the realm of network and router security, focusing on the detection and analysis of threats to ensure the integrity and security of network systems. Various studies have explored techniques and methodologies to enhance the detection and analysis of security threats in network environments.

Related Work 2.2

Many studies have contributed to the literature on network security, particularly in malware detection and analysis. Research has explored the use of machine learning, deep learning, and static analysis techniques to detect and analyze malware in network traffic, emphasizing the importance of early detection and prediction mechanisms.

Discussions 2.2.1

The literature highlights the significance of monitoring and analyzing network traffic to detect and mitigate security threats effectively. Studies have emphasized the need for advanced detection mechanisms that can adapt to the evolving threat landscape, including the use of machine learning models and behavioral analysis to enhance the accuracy and efficiency of threat detection.

Figure (2.1)

Issues and Challenges 2.2.2

One of the primary challenges faced in network and router security is the detection of advanced persistent threats (APTs) and malware that evade traditional security measures. Researchers have identified the need for improved detection mechanisms that can effectively identify and mitigate sophisticated threats in network environments. Additionally, the rapid evolution of attack patterns poses a challenge in developing robust detection strategies to combat emerging threats.

Summary 2.3

The literature review underscores the critical importance of robust detection and analysis techniques in safeguarding network and router security. Researchers have explored various approaches, including machine learning, static analysis, and behavioral analysis, to enhance the detection of malware and security threats in network traffic. Despite the challenges posed by advanced threats and evolving attack patterns, ongoing research aims to develop innovative solutions to strengthen network security and mitigate potential risks effectively.

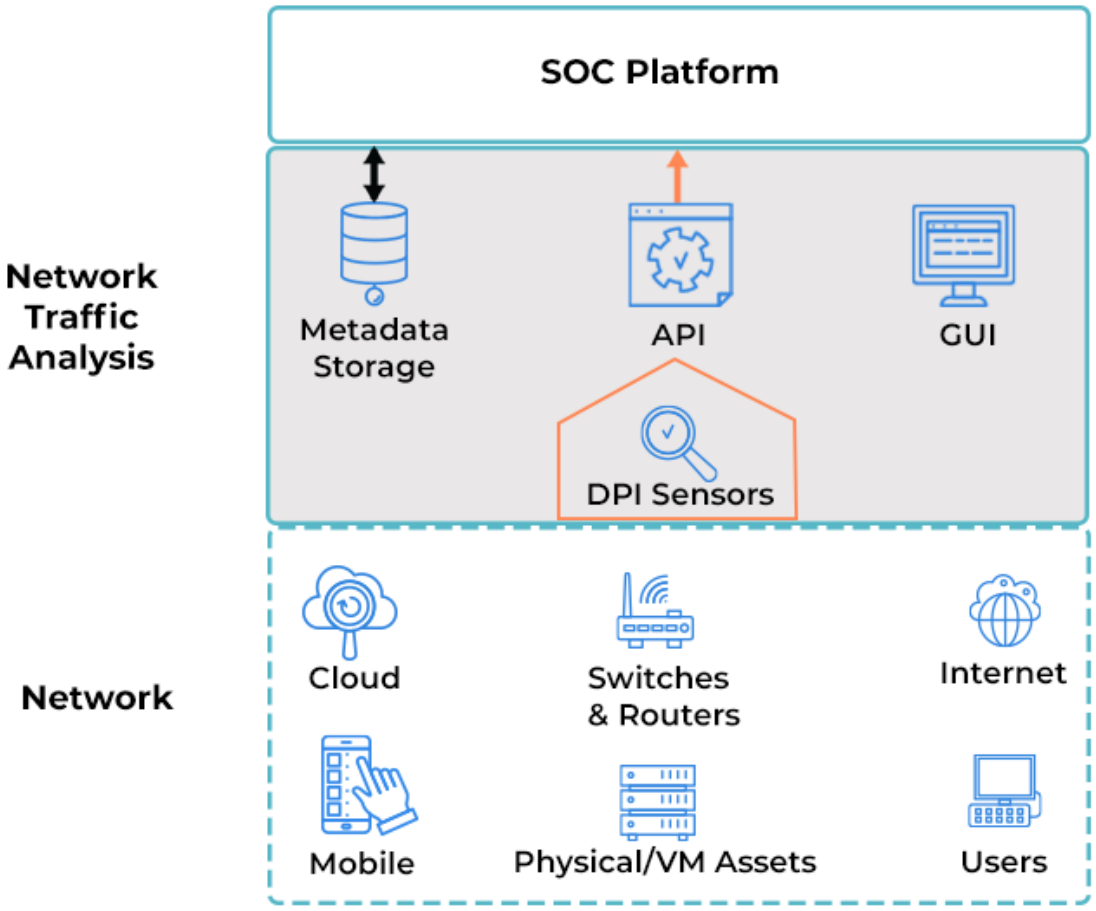
SOC Platform
Network Traffic Analysis
Metadata Storage
API
GUI
DPI Sensors
Network
Cloud
Switches & Routers
Internet
Mobile
Physical/VM Assets
Users

Figure (2.2)

CHAPTER 3

METHODOLOGY

3.1 Overview

This documentation project's objective is to develop a comprehensive guide for a network detection and analysis tool. This guide will provide detailed information on the tool's features, functionality, and usage, ensuring that users can effectively utilize the tool for network monitoring and security.

3.2 Feasibility Study

A feasibility study was conducted to determine the viability of this documentation project. Key factors considered included:

- The tool's current usage and adoption rate
- The level of user support required
- The availability of existing documentation and resources
- The potential impact on the network security and performance

Network scanning tools are widely used by both network administrators and malicious actors. There is a growing need for more advanced network scanning detection and analysis capabilities to protect against sophisticated attacks.

Level of User Support Required:

Implementing an effective network scanning detection and analysis tool would require significant user support and training. Network administrators would need to be educated in how to properly configure and use the tool and interpret the results. Ongoing technical support would also be necessary to address any issues that arise.

Potential Impact on Network Security and Performance:

A well-designed network scanning detection and analysis tool could significantly improve an organization's overall network security posture. By quickly identifying and alerting people to suspicious scanning activity, the tool could help prevent or mitigate potential attacks. However, the tool's implementation and operation would need to be carefully managed to ensure it does not negatively impact network performance or introduce additional vulnerabilities. In conclusion, the development of a network scanning detection and analysis tool appears to be viable and valuable.

3.3 Risk Analysis

Inaccurate Vulnerability Detection	The tool must be able to reliably identify a comprehensive set of known vulnerabilities across a wide range of software, operating systems and devices. Inaccurate or incomplete detection can leave critical weaknesses unidentified.
Lack of Automated Scanning and Remediation	The tool should automate network discovery, vulnerability scanning, risk prioritization and provide remediation guidance to minimize manual effort and ensure timely issue resolution.
Inability to Scan Diverse Network Environments	The tool must be able to intelligently scan and analyze a wide variety of network environments.
Insufficient Reporting and Workflow Integration	The tool should provide detailed technical and executive reporting to demonstrate security posture and enable stakeholders to prioritize remediation.
Outdated Vulnerability Database	The tool's vulnerability database must be regularly updated to detect the latest known vulnerabilities, including zero-day threats. Relying on an outdated database leaves the network exposed to emerging risks.
Lack of Authenticated Scanning Capabilities	The tool should support authenticated scans that leverage credentials to perform in-depth analysis of system configurations and vulnerabilities beyond what unauthenticated scans can detect.
High False Positive Rates	The tool should minimize false positive results to avoid wasting time investigating non-issues and enable focusing on real vulnerabilities that require remediation.

Critical risk (3.1)

3.4 Methodology Process

The methodology process for this documentation project will follow the Agile approach. This approach allows for flexibility and adaptability throughout the project, ensuring that the documentation meets the evolving needs of users.

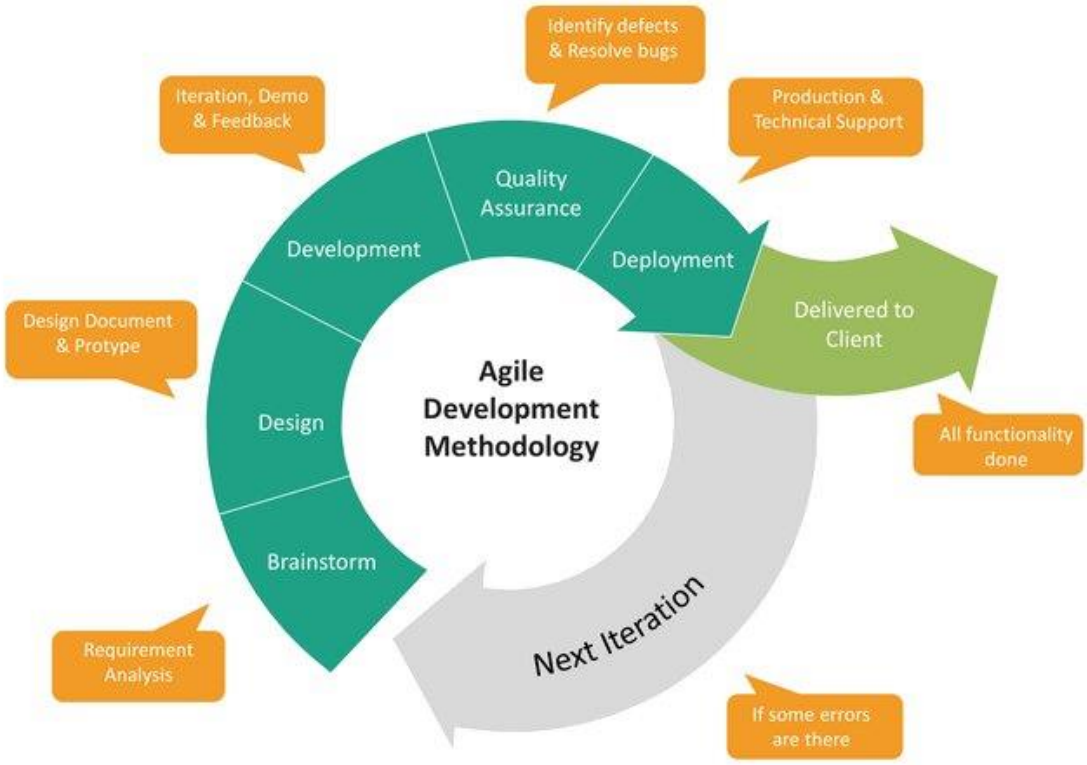

Figure (3.1)

3.4.1 Requirements

The requirements for this documentation project were collected through research into similar projects and analysis of tools in use.
The types of requirements included are:

- Functional
- Non-Functional

Network Discovery	Automatically discover and map all devices connected to the network, including servers, workstations, routers, switches, firewalls, etc.

Port Scanning	Scan for open ports on network devices to identify potential attack vectors
Vulnerability Detection	Identify known vulnerabilities in operating systems and applications based on comprehensive vulnerability databases
Configuration Checks	Check network device configurations for misconfigurations that could lead to security issues
Anomaly Detection	Detect anomalous network behavior that could indicate malicious activity or attacks in progress
Reporting	Generate detailed reports on discovered vulnerabilities, misconfigurations, and anomalies with clear remediation guidance
Alerting	Provide real-time alerts when critical vulnerabilities are detected, or anomalous activity is observed
Remediation Tracking	Track remediation efforts and provide visibility into which vulnerabilities have been addressed

Functional requirements (3.2)

Performance	- The tool should be able to scan and analyze large networks with thousands of devices in a timely manner - The tool should be able to process and analyze network traffic data in real-time with minimal latency
Scalability	- The tool should be able to handle increasing amounts of network traffic and devices as the organization grows, without significant performance degradation - The tool should be able to scale up or down based on changing network size and traffic patterns
Reliability	- The tool should have high uptime and availability - The tool should be able to recover gracefully from failures and continue operation ideally without data loss

Security	- The tool should have robust security measures to protect the collected network data and analysis results - The tool should support role-based access control and multi-factor authentication to restrict access to authorized personnel only
Usability	- The tool should have an intuitive and user-friendly interface that allows network administrators to easily configure, operate and interpret the results - The tool should provide clear and actionable insights, alerts and recommendations to help administrators quickly identify and resolve network issues
Compliance	- The tool should comply with relevant industry standards and regulations for network security and data privacy (e.g. NIST, HIPAA, PCI-DSS)
Extensibility	- The tool should have a modular and extensible architecture that allows easy integration with other security and network management tools - The tool should support custom plugins and scripts to extend its functionality as per evolving organizational needs
Maintainability	- The tool should have clear and comprehensive documentation to facilitate easy installation, configuration and troubleshooting - The tool should have automated update and patch management capabilities to ensure it remains up to date with the latest security fixes and feature enhancements

Non-functional Requirements (3.3)

CHAPTER 4

DESIGN MODELS

CHAPTER 5

EXPERIMENTS AND RESULTS

CHAPTER 6

CONCLUSION AND FUTURE WORKS

6.1 Overview
6.2 Summary about the project
6.3 Achieved objectives
6.4 Main contributions of the work
6.5 Limitation
6.6 Future Work

REFERENCES

1- Article:

Author(s), “Article title”, Journal title, vol., no., Page number(s), month-Year.

Ex:

[1] H. S. A. &. A. E. Al-Shourbaji, "Boosting Ant Colony Optimization with Reptile Search Algorithm for Churn Prediction," *Mathematics,* vol. 10, no. 7, p. 1031, 2022.

2- Conference:

Author(s), “Article title”, Conference title, Country, City, Page number(s), month-Year.

Ex:

[1] M. R. a. C. A. C. C. Sierra, "Improving PSO-based multi-objective optimization using crowding, mutation and∈-dominance," in *International conference on evolutionary multi-criterion optimization*, Berlin, Heidelberg, 2015.

3- Book:

Author(s), “Book title”, Publisher, Year

Ex:

[1] S. J. a. H. E. Stein, The EQ edge: Emotional intelligence and your success, Florida: John Wiley & Sons, 2011.

4- Website:

Author(s), "*Page title."* **Website title. Web Address (accessed date retrieved).**

Ex:

[1] D. Holland, "Finding the Building Blocks of Wood." unimelb.edu.au. https://pursuit.unimelb.edu.au/articles/finding-the-building-blocks-of wood?utm_source=linkedin.com&utm_medium=social&utm_content=story (accessed June 13, 2021).

Appendices [if any]