

Thesis topic: 'Design and implementation of an intrusion detection system (IDS) based on Snort and Suricata in a corporate network'

Prepared by

ALI MMADI, PhD student-Midocean University



Literary Criticism (2)

Task 1

INTRODUCTION

I am Ali Mmadi, a PhD student in Information Technology, specializing in Cybersecurity. As part of the "Critical Studies 2" module, I am presenting today the first task, which consists of critiquing the format of a master's thesis.

I chose to analyze a dissertation entitled:

"Design and Implementation of an Intrusion Detection System (IDS) Based on Snort and Suricata in a Corporate Network."

The objective of this review is to evaluate the formal aspects, the coherence of the presentation, and the scientific rigor of the writing, in accordance with the guidelines of the university guide.



1. Analysis of the presentation and format

First, regarding the general format, the dissertation complies with the standards set by the university: The Times New Roman font is used throughout the document. The 12-point size for the text and 14-point size for main headings is properly observed. Margins and spacing are consistent, providing a pleasant reading experience.



However, I noticed a small inconsistency in the subtitles of Chapter II, where the font size varies slightly. Moreover, the figure captions do not always follow the same style: some are italicized, others are bold, which affects visual uniformity. Concerning printing and physical presentation, the document is clean, well-bound, and free of notable printing errors. Page numbers are properly placed and the pagination matches the table of contents.

2. Structural coherence and logical presentation

The thesis is structured in a logical manner:

- a **general introduction**,
- a **literature review**,
- a **methodology section**,
- a **practical part**,
- and finally a **general conclusion** with future perspectives.

Each chapter begins with a brief introduction and ends with a partial conclusion, which demonstrates good adherence to the scientific writing technical details.

However, in the methodology section, the description of the experimental environment would have benefited from being presented before the technical configuration of **Snort** and **Suricata**. This would have allowed the reader to better understand the context before delving into the method.

3. Quality of writing and language

From a linguistic standpoint, the dissertation is written in clear and precise technical French, suitable for the field of cybersecurity. There are a few minor agreement and punctuation mistakes, but nothing that hinders comprehension. The language is simple and fluent, and complex concepts, such as network anomaly detection or packet analysis, are well explained.

The thesis includes a summary in Arabic, French, and English, but the English version could be slightly improved to adopt terminology more specific to the field, for example replacing "**security attacks**" with "**network intrusions**".

The author also made good use of citations and references. However, some direct quotes from articles on **Suricata** could have been rephrased to strengthen the originality of the text.

4. Presentation of appendices and visual elements

The **appendices section** is well-organized: it contains **Snort** and **Suricata** configurations, the Bash scripts used for automation, as well as screenshots of simulated attack tests. Each appendix is numbered and referenced in the main text, which makes navigation easier.

However, some appendices sometimes lack **a brief introductory description** to explain their content or purpose, which would have helped the reader understand their connection to the previous chapters.

CONCLUSION

In conclusion, the thesis "Design and Implementation of an Intrusion Detection System Based on Snort and Suricata" is **formally well-structured**, clear, and compliant with academic standards. **The strong points lie in the neat presentation, linguistic clarity, and overall coherence of the document.** The aspects to improve mainly concern the **uniformity of the subtitles, the harmonization of the figures, and the contextualization of the appendices.**

This exercise allowed me to **develop a critical perspective on the form and visual rigor of a scientific thesis**, an essential skill in the doctoral journey in cybersecurity.

Key references:

This thesis draws on several key references, including the pioneering work of Roesch (1999) on Snort, the NIST SP 800-94 guide on IDS/IPS, as well as recent studies comparing Snort and Suricata, such as those by Kaur and Kaur (2022). These sources strengthen the scientific credibility of the work and ensure its compliance with international cybersecurity research standards.

Roesch, M. (1999). Snort - Lightweight Intrusion Detection for Networks. In Proceedings of the 13th USENIX Conference on System Administration (LISA '99).

► Historical and foundational reference for the Snort IDS system, which describes its architecture and detection mechanisms. Open Information Security Foundation (OISF).

(2023). Suricata User Guide – Official Documentation. Available at: <https://suricata.io>

► Official document describing the configuration, signatures, and multi-threading capabilities of Suricata. Scarfone, K., & Mell, P.

(2007). Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94, National Institute of Standards and Technology.

► International normative reference on the classification, architecture, and management of IDS/IPS. Zhang, Y., & Lee, W. (2000). Intrusion Detection in Wireless Ad-Hoc Networks. In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You for your attention

