Intrusion Detection Tools

Kim André Næss, Dale Bada, Muhammad Javed Iqbal
Cyber Security
Noroff University College
Kristiansand, Oslo, Norway
kim.naess@stud.noroff.no, dale.bada@stud.noroff.no, muhammad.iqbal@stud.noroff.no

***Abstract*—In this state-of-art review paper, we will examine the latest Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) applicable for Small and Midsize Busnisess (SMB), where SMB are as defined by Gartner [1].**

This review has 3 key objectives. Firstly, we will define and identify what kind of network security threats are most prevalent and most urgent for SMBs' to address. Secondly, we will identify what open source software are available for SMBs' to manage and mitigate identified threats. Then in the third final part, we will review a select number of these open source software and assess how well each system protects SMBs' from the identified network threats.

Each tools' features, capabilities, advantages and limitations will be compared. How each system fare with regards to manageability, cost effectiveness and return of investment also will be taken into consideration before we conclude which system will be crowned with a recommendation as IDS/IPS for SMBs'.

***Index Terms*—**
Question - Question for Ian???
What are expected to be in the index of terms?

- **Keyword and their elaborations?**
- **Abbreviation index?**
- **Terminology glossary?**

Lorem ipsum dolor sit amet mollit sunt duis velit non aliquip in labore minim.

I. Introduction

A. A brief background and history

IDS and IPS are a category of network tools or systems to detect and prevent malicious network activities. One of the earliest network based security defenses was firewall. Firewalls were later complimented with IDS' as network administrators and security personnel came to acknowledge that firewalls may allow malicious communications, both in and out bound, via valid sessions. Thus were IDS' introduced, which had the capability to inspect and validate individual packet and validate signatures of different indictors of compromise (IOC). Which are able to alert the administrators of positively identified malicious communication.

B. Evolving Threat Landscape and Countermeasures

IDS' were initially installed on a host server (HIDS), then specific network IDS devices (NIDS) excelarated its market penetration by providing IDS functionality an a more conveniently deployable and manageble unit.

Follow-up - to-do!!!

- Expand on IPS, with some historical information.
- Describe current threats
- Elaborate on IPS evolving to, or its relation with, next-gen firewalls.
- Establish a segway to SIM, EM then SIEM and its further evolution to XDRs.

C. Detection and Prevention for SMBs'

SIEMs' are typically deployed in larger Enterprise IT environments. SIEMs takes center the stage in a companies Security Operations Center (SOC). These are often complex systems due to business process integration, or systems integration with IT Service Management tools like SolarWinds, ServiceNow og Jira, to name a few. All of the above drives cost of ownership up. Some may opt to subscribe to SOC as services to reduce cost. SMBs may aso choose to omit certain features and functionalities SIEMs offer, and choose a solution based on open source software with comparable functionality. As such, the scope of this state-of-art review are open source IDS systems. Though occasionally, we will look at how an IDS relates to a larger tool chain, systems or technologies. This is inevitable as security relies on a layered approach, and reliance on a single tool, method or policy is bad practice. It is also relevant to assess an IDS as part of a companies infrastructure roadmap as the company scales up.

D. Addressing SMBs' most prevalent network threat with IDS/IPS

IDS and IPS has a significant drawback against the primary network threat SMBs are facing today; namely malware and Ransomware, as identified in the Norsis [2] threat report for 2021. IDS and IPS main function is to detect, alert and prevent threats that are traversing the network. Malware and ransomware on the other hand are resident on a host. Malware and ransomware are also designed to be as stealthy as possible while at rest on the host and when initiating communication on the network. They apply various techniques to obfuscate their existance on the host. And they can piggy-back on trusted network sessions. While the binary signatures detection tools use to identify them on delivery are rendered unusable with a simple recompilation or more advanced polymophic coding techniques. Therefore it is crucial that IDS and IPS are deployed together with other security tools and systems to be able to maximize its utilization. Larger network may also benefit from properly segmented and architecturally designed

with security in mind. As always, a layered secuirty approach must be applied.

Follow-up - to-do!!!

- Find appropriate reference material describing modern/advance malware and ransomeware.

II. Main topic - change to your topic name

Notes - work in progress:

Section content being assessed.

A. Subtopic1

Notes - work in progress:

Section content being assessed.

B. Subtopic2

Notes - work in progress:

Section content being assessed.

C. Subtopic3

Notes - work in progress:

Section content being assessed.

III. Ethical Issues

Notes - work in progress:

Section content being assessed.

IV. Summary

Notes - work in progress:

Section content being assessed.

V. Conclusion

Security best-practice rely on a holistic and layered approach...

Follow-up - to-do!!!

- Provide evidence for security best-practices to further elaborate and support the statement.
- Provide concrete examples where IDS and IPS are ineffective againts malware and ransomware.

With all the limitations inherent to IDS and IPS taken into cosideration. The most effective, cost effective and managable systems is...

Follow-up - to-do!!!

- Insert name of IDS/IPS here when all the review has been conduted.

Appendix A: Citation Examples

References

[1] Gartner, "Definition of small and midsize business - it glossary — gartner." [Online]. Available: https://www.gartner.com/en/information-technology/glossary/smbs-small-and-midsize-businesses

[2] Norsis, "Norsis trusler trender 2021 digital," 2021. [Online]. Available: https://norsis.no//wp-content/uploads/2021/03/NorSIS_Trusler_Trender_2021_Digital.pdf