Intrusion Detection Tools

Kim André Næss, Dale Peregrino 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*—This state-of-art review paper will examine the latest Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) applicable for Small and Midsize Businesess (SMB), where SMB are as defined by Gartner [1].**

This review has 3 key objectives. Firstly, it 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 how ~~a select number of~~ these open source software ~~and assess how well each system~~ addresses ~~SMBs' from~~ the identified network threats.

Question - Restructure Topic/Subtopic???
Shall we separate section "D" from the introduction into its own topic? To match with the "3 objectives" mentioned above...

Each tools' features, capabilities, advantages and limitations will be compared. How each system fare with regards to manageability, cost effectiveness and return of investment, will also be taken into consideration. With all above parameters being equal, should be able to determine which IDS/IPS are most suitable for SMBs'.

***Index Terms*—Intrusion Detection Tools, Small Business, Machine Learning, IDS,**

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 indicators of compromise (IOC). Which are able to alert the administrators of positively identified malicious communication. Later, the integration of detection and prevention (IDS and IPS) in a single systems or devices like next-generation firewalls, further enhancing the security postures of organizations where these systems are deployed.

B. Evolving Threat Landscape and Countermeasures

IDS' were initially installed on a host server (HIDS), then specific network IDS devices (NIDS) gained even more popularity by providing IDS functionality in a more conveniently deployable and manageable 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 also 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 existence 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 polymorphic 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 security approach must be applied.

Follow-up - to-do!!!

- Find appropriate reference material describing modern/advance malware and ransomware.
- Ref. US/UK?

II. Reviewing IDS Systems for Small and Midsized Businesses

A. Merits vs Operational Constraints of Intrusion Detection Systems

1) OSSEC: OSSEC capabilities is supported with the most used operating systems for businesses, which run on Linux, Windows or Mac OS. The system is free to use and this makes it ideal for small businesses, that might have a tight budget to finance their investments. The features that OSSEC home page (ossec.net/about) is claiming to have is Log based Intrusion Detecion(LIDs), Rootkit and Malware Detection, Active Response, Compliance Auditing, File Integrity Monitoring (FIM) and System Inventory.

According to (Reznik) Suricata is the second most popular IDS tools used, only bypassed by SNORT in popularity. Containing features like hardware acceleration and multithreading to perform spesific functions more effectivley.

Suricata has according to the (techfunnel article) all of the mentioned capabilites of OSSEC and is claimed to be fast and could also detect advanced threats. This capabilities are also supported by a literature review paper on IDS (A Comprehensive Systematic Literature Review on Intrusion Detection Systems) where the advantages of Suricata are mentioned along with additional benefits like filtered events and alarms, automatic protocol detection, application layer data collection to name a few. The downsides however are something that a small business should take into consideration as the CPU usage is high, and it has a smaller supported community compared to SNORT. The installation process is also mentioned as complex, and the need for special competance in this area for a small business may be needed.

2) SNORT: **Notes - Individual subtopic - SNORT:**

Work on-going:

- Gathering information about implementation and deployment examples that can be applied to SMBs.
- Gathering concret implementation example where SNORT is used in conjucntion with ML and DL to address polymorphic and metamorphic malware.

Intrusion detection is experimental (A novel approach to intrusion detection using SVM ensemble with feature augmentation, Jie Gu et al, 2019) and (Hands-On Artifical Intelligence for CyberSecurity, Parisi A, 2019, p 22)

Malware Analysis objectives:

- Distinguish malicious binary files from legitimate files. - Automate the preparatory phase of malware analysis; triage. - The analyst must understand the logic by which the Machine Learning, and Deep Learning tools apply; for finetuning, knowing what method or algorithm to address relevant to the task at hand. Properly assess the results and how to adapt.

What characterizes an efficient Malware detection software:

- A quick and successful preliminary screening of possible malicious binary. - An analyst that can quickly verify and alert about the malicious binary. - Adaptive to new threats and their contextual changes

What can be malicious files:

- All files, even non-executable files such as a .PDF, .TXT, .JPG etc. (Hands-On Artifical Intelligence for CyberSecurity, Parisi A, 2019, p 112)

Modes of malware analysis:

- Static analysis - Dynamic analysis

What are malwares:

- Trojans - Botnets - Downloaders - Rootkits - Ransomware - APT - Zero Days

3) Zeek: According to [1] Zeek (previously known as Bro) is an intrusion detection system that differs from others in that it focuses on network analysis. Unlike rules-based engines, which are meant to identify exceptions, Zeek searches for dangers and generates warnings. Zeek is an open-source, passive network traffic analyser. Zeek is widely used by operators as a network security monitor (NSM) [2] to aid in the investigation of suspicious or malicious behaviour. Zeek also provides support for a broad variety of traffic analysis activities outside of the security area, such as performance assessment and troubleshooting. Extracting data from HTTP sessions, detecting malware by interacting with external registries, reporting vulnerable versions of software visible on the network, recognising popular online apps, detecting SSH brute-forcing, checking SSL certificate chains, and much more are all included into Zeek.

Pros:

- Zeek is a traffic analysis tool that is completely flexible and expandable. To express any analytic job, Zeek offers a domain-specific, Turing-complete scripting language.
- A low-cost alternative to pricey proprietary technologies, Zeek operates on commodity hardware. Zeek is a network monitoring tool that goes well beyond the capabilities of most other tools, which are often confined to a narrow collection of pre-programmed analytic activities.
- As a platform for gathering and analysing network data, Zeek is best suited to the task at hand.
- The transaction data provided by Zeek is the company's biggest selling point. This means that if a network interface is being monitored, Zeek will create a collection of high-fidelity, highly annotated transaction logs by default. In a judgment-free, policy-neutral way, these logs explain the protocols and activities on the network.

Cons:

- ZeeK/Bro's deep packet inspection consumes a lot of resources, which is a drawback if you're looking for flexibility. In terms of threat intelligence, Snort and Suricata are the two most popular options. The community is continuously attempting to make Bro more user-friendly because of this.

4) IBM QRADAR: IBM has developed QRadar, a tool for handling security issues [3]. Additionally, it can analyse data from a wide range of sources (router/firewall/application/folder) and store and manage data, as well as uncover vulnerabilities and information about risks to data security. Additionally, QRadar has a variety of monitoring functions that look for changes in user or network activity that might suggest an attack or a policy violation. QRadar may send notifications to the appropriate recipient, for example by e-mail, informing them of the occurrence of a violation or attack.

Pros:

- Streamlines the identification and prioritization of threats in the IT infrastructure.
- Simplifies alert processing so that security analysts may concentrate their investigations on a smaller number of high-probability threats.
- Improves threat management by generating comprehensive data access and user activity reports for each user.
- The ability to work in both on-premises and in the cloud
- Complies with regulations by generating thorough reports on data access and user activities.
- Security intelligence solutions may be provided cost-effectively by managed service providers using multi-tenancy and a master console.

Cons:

Based of user reviews the cons of IBM Qradar Siem are mentioned below.

- The product is quite sluggish since it was designed using outdated technologies. Windows log collection is very time-consuming and antiquated."
- To have a system that correctly warns you when an attack is taking place, you can't just click a couple buttons."vBecause to this, IBM QRadar couldn't be used for correlation.

B. Deploying Intrusion Detection Systems

Notes - work in progress:

- ~~Which is the best suited IDS system for SMB companies~~
  - ~~How easy are the IDS systems to by-pass?~~
  - What are the minimum HW required for deployment? How hard or easy are the IDS to install, run and manage?
  - ~~How effective are the IDS to detect/safeguard against ransomware/malware?~~

Section content being assessed.

Notes - :

Kim's input for section B goes here

Notes - :

Dale's input for section B goes here

Notes - :

Muhammad's input for section B goes here

C. The Efficacy of Intrusion Detection Systems Against Malware and Ransomware

Notes - work in progress:

- ~~Which is the best suited IDS system for SMB companies~~
  - ~~How easy are the IDS systems to by-pass?~~
  - ~~What are the minimum HW required for deployment?~~
  - How effective are the IDS to detect/safeguard against ransomware/malware?

Section content being assessed.

Notes - :

Kim's input for section C goes here

Notes - :

Dale's input for section B goes here

Notes - :

Muhammad's input for section C goes here

III. Ethical Issues

Notes - work in progress:

- Anonymise
- Reputation
- Data confidentiality
- GDPR

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 against malware and ransomware.

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

Follow-up - to-do!!!

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

APPENDIX A: 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

APPENDIX B: ILLUSTRATIONS

Notes - Placeholder for images and illustrations:

Images insert here...