MULTI-STAGE IDS USING SNORT TOOL

[1]Gokul Nanju, [2]Sheron Roshith S, [3]Dhilipan Kumar P

Student
Cyber Forensics and Information Security
Dr. M.G.R Educational and Research Institute
Chennai, India.

***Abstract*- The proposed multistage IDS using snort tool basically consists of two parts. The first phase uses Snort as a fingerprint-based intrusion detection system. Snort uses pre-defined signatures to identify known attack methods and suspected fraud. It acts as a first line of protection via quick detecting recognized threats and recognized attacks. The second part focuses on anomaly detection, supporting Snort's signature-based approach. Anomaly detection is to build a basic pattern of normal network behavior. Deviations from this baseline are considered potential anomalies, meaning possible intrusions or other attack patterns that may be missed by signature-based systems. Machine learning algorithms such as clustering or classification techniques are used to model and identify these anomalies in real-time network traffic.**

INTRODUCTION

Traditional intruder detection methods—signature-based and anomaly-based—each have strengths but also inherent limitations. Signature-based systems excel at identifying existing attack patterns however conflict inside the face of new threats. On the other hand, anomaly-based schemes that rely on the interpretation of normal behavior tend to yield false positive results. Multi-Stage IDS protects the network from cyber threats in the ever-evolving digital environment. This multi-channel IDS platform leverages the versatility capabilities of Snort and seamlessly combines the power of signature-based and anomaly-based detection If it powers Snort types together, the system overcomes the limitations of single detection methods to skillfully recognize known attack signatures and unusual activities. This new platform not only addresses gaps in existing IDS systems, but also enhances network security by providing flexible and comprehensive protection against the various cyber threats.

OBJECTIVES

1.Threats Detection: Monitoring network traffic within snort to identify potential security threats or unauthorized actions.
2.Risk Assessment: Analyzing the severity and potential impact of detected threats based on snort's configured rules and signatures.
3.Incident Response: Leveraging the detected alerts and information provided by the system to promptly and effectively address security incidents.
4.Reporting: The analysis and presentation of data related to detected security incidents.

DESIGN AND IMPLEMENTATION

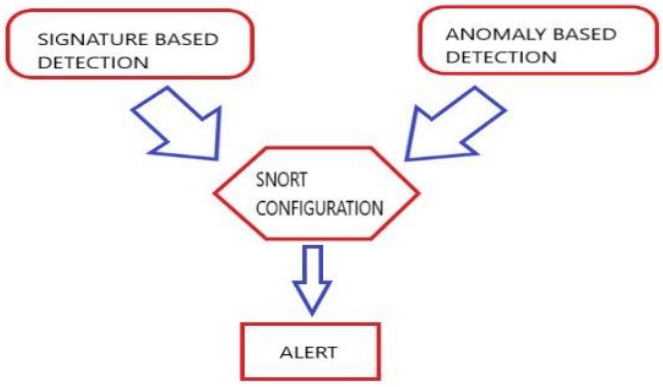

Figure:1 Represents the design of multi-stage ids using snort tool.

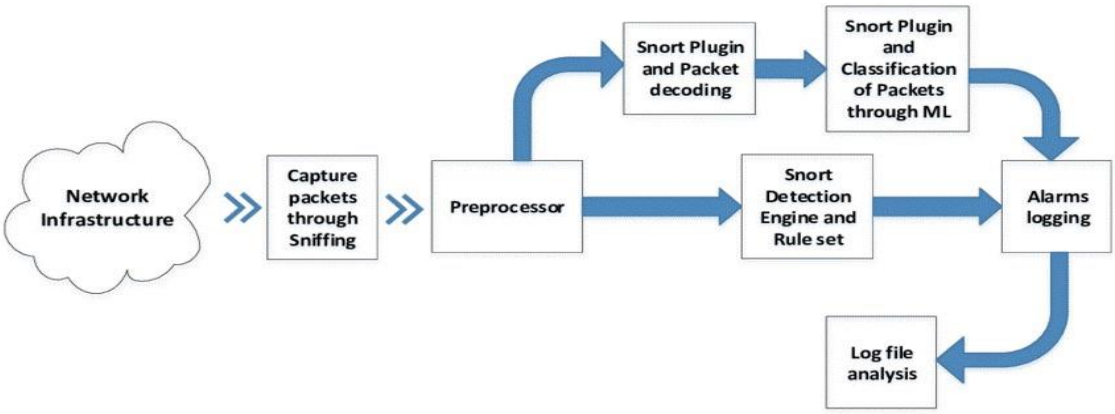

Figure:2 Represents the architecture of snort.

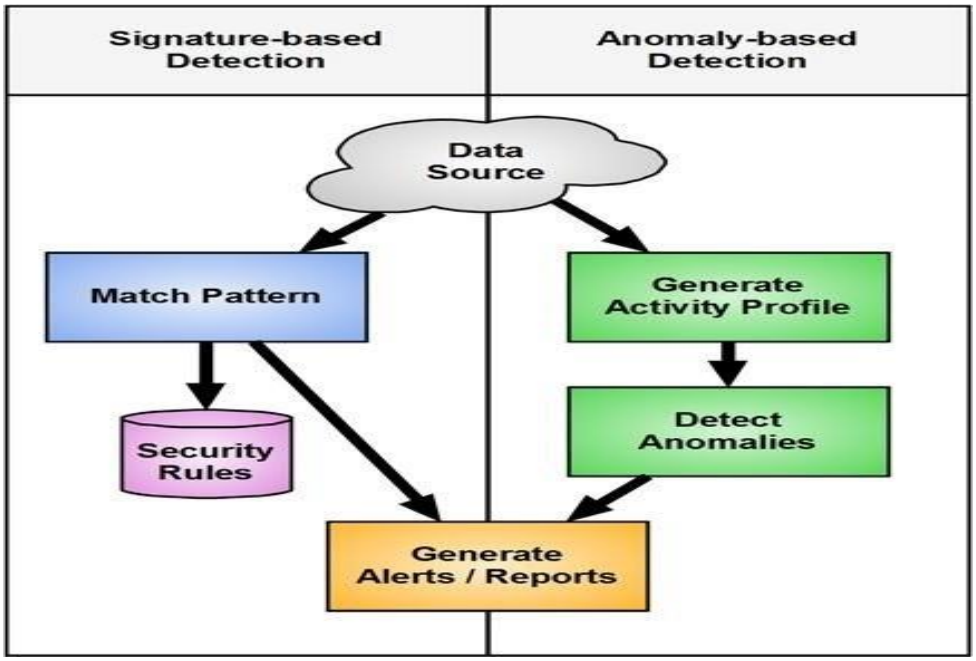

Figure:3 Represents the working of multi-stage IDS

METHODOLOGY

1.Signature-based Detection: Identifying cyber threats by comparing them to a database of known attack patterns or signatures.
2.Anomaly-based Detection: Identifying cyber threats by flagging unusual or abnormal behavior in the systems.
3.Alert: Notification generated when the system detects suspicious or potentially malicious activity
4.Reporting Module: Presentation of information about security events and incidents in a structured and comprehensible format.

CONCLUSION

Multi-Stage Intrusion Detection System (IDS) using Snort, shows its effectiveness in combating different network threats. A well-designed multi-layered architecture, which includes preemption, detection, and response measures, includes an effective and flexible security system that is essential for meeting the challenges of risk is changing. IDS leverages Snort's real-time packet inspection and custom compliance detection, identifies signatures and known errors, and enables robust social traffic analysis Its successful application across online environments builds and resilience emphasizing the edge, increasing protection against developing threats. However the device shows great promise, future research strategies can be informed by improving research protocols and exploring the latest technologies, with proper device integration and risk about increased information about this of Snort in the IDS system The integration represents an important step towards strengthening the network, promising simpler and faster input identification systems for consumption complex modern computing environments

REFERENCES:

1. "Intrusion detection prevention system using SNORT" - Aaliya Tasneem, Abhishek Kumar, Shabnam Sharma – 2018.
2. " Advanced intrusion detection system with prevention capabilities" - AB Pawar, DN Kyatanavar, MA Jawale – 2014.
3. "A review on intrusion detection system" - Rafat Rana SH Rizvi, Ranjit R Keole – 2015.
4. "Intrusion detection with Snort" - Jack Koziol – 2003.
5. "Signature based intrusion detection system using SNORT" - Vinod Kumar, Om Prakash Sangwan – 2012.
6. "Analysis of host-based and network-based intrusion detection system" - Amrit Pal Singh, Manik Deep Singh – 2014.
7. "Intrusion detection systems with Snort: advanced IDS techniques using Snort, Apache, MySQL, PHP, and ACID" - Rafeeq Ur Rehman – 2003.
8. "Managing Security with Snort & IDS Tools: Intrusion Detection with OpenSource Tools" - Kerry J Cox, Christopher Gerg – 2004.
9. "Snort intrusion detection and prevention toolkit" - Brian Caswell, Jay Beale, Andrew Baker – 2007.
10. "A realistic experimental comparison of the Suricata and Snort intrusion detection systems" - Eugene Albin, Neil C Rowe – 2012.
11. "Snort: Lightweight intrusion detection for networks"- Martin Roesch-1999.
12. " A performance analysis of snort and suricata network intrusion detection and prevention engines" - David Day, Benjamin Burns – 2011.
13. " Deployment of Snort Intrusion Detection System on Usmanu Danfodiyo University Network" - Muazu Dalhatu Sifawa, Bello Alhaji Buhari, Lawal Sulaiman – 2022.
14. "Performance evaluation of advanced intrusion detection system" - Kiran Bala1, Narendra Kumar2, Ashok Kumar Singh3 – 2018.
15. "Computer network security ids tools and techniques (snort/suricata)" - O Eldow, P Chauhan, P Lalwani, M Potdar – 2016.