Intrusion Detection Prevention System using SNORT

Aaliya Tasneem
Ajeenkya D Y Patil University, Pune

Abhishek Kumar
Ajeenkya D Y Patil University, Pune

Shabnam Sharma
iNurture Education Solutions, Bangalore

ABSTRACT
Living in the age of information, each and every action result in some form of data creation. According to statistics, over 300 thousand tweets and over 4 million Facebook posts are being generated per minute. Knowing the fact that more users and more data require more security. In the modern era, security and reliability have become the major concerns for an individual or an organization. In this paper, various terminologies, techniques and methodologies related to Intrusion Detection and Prevention System (IDPS) have been discussed. This paper provides different approaches on implementation of IDPS that is based on in-depth study of various research endeavors. It majorly deals with the concept of Intrusion Detection System using Snort which is a popular tool for network security. It is widely accepted by corporate sectors in order to secure their organization's network. The paper gives a fair knowledge of Snort, about its purpose, the modes it associated with, its implementations and the applications. Review has been made on the basis of the studies and research done in the literature section.

Keywords
Intrusion Detection System; Intrusion Prevention System; Snort

1. INTRODUCTION
Since the digital age is taken over, our lives have been encoded into digital clouds and stored on hard drives. Protecting this data has become the number one priority in ensuring privacy and security. IDPS is just another tool that when used properly will ensure that attacks are mitigated quickly. In fact, a network with a firewall and no IDPS is just as high security prison with no guards on Patrol. The major significance of IDPS are because of these two reasons, i.e. data protection & data privacy.

2. IDS/IPS
In general term, an intrusion can be said as an unauthorized access to someone's property or area, but when it comes to computer science, it is an act to compromise the basic computer network security goals viz. confidentiality, integrity, and privacy. Intrusion Detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents of threats and violations of computer security practices, acceptable use policies or standard security policies.

Intrusion Detection System (IDS) detects the presence of intrusion in the network. It is designed to monitor the events occurring in a computer system or network and responds to events with signs of possible incidents of violations of security policies. On the other hand, Intrusion Prevention System (IPS), is the network security system or technology that is capable of not only detecting the intrusion activities but also take required counter measures to prevent them.

3. TYPES OF TECHNOLOGIES
There are many types of IDPS technologies. For the purposes of this document, they are divided into the following four groups based on the type of events that they monitor and the ways in which they are deployed.

3.1 Network based IDPS
A network-based intrusion detection system monitors and examines the network traffic for any suspicious activity or threats in the network. It reads the packets flowing in the network and searches for any malicious activity by identifying suspicious pattern in the packets. If any threat is discovered, then based upon the threat the system will take actions such as notifying administrators about it.

3.2 Wireless based IDPS
Wireless based Intrusion Detection Prevention System analyzes the traffic of wireless network by analyzing wireless protocol activities and take appropriate actions. It detects unauthorized wireless local area network in use. It cannot identify suspicious activity in the application layer, transport layer and protocol activities. It is deployed in a particular range where the organization can monitor the wireless network.

3.3 Network Behavior Analysis
NBA examines network traffic to identify threats which generate unusual traffic flows such as DDoS (Distributed Denial of Service) attack, malwares (e.g. worms, backdoors), and policy violations. These systems are deployed for monitoring the flow on an organization's internal network, sometimes it is used to monitor organization's networks and external network.

3.4 Host based IDPS
HIDPS monitors characteristics of a single host and identifies intrusions within that host by monitoring host's file system, file access, system calls or network events. It can prevent system level attacks and can detect attacks which NIDPS cannot. The hosts load can be distributed over the network. It can even analyze activities that are transferred in end-to-end encrypted communications.

4. METHODOLOGIES OF IDPS
To detect and prevent any intrusion, there are a lot of methodologies which IDPS uses. These methodologies are used as per the requirement of the system.

4.1 Anomaly based Methodology
These types of attack are used for detecting the unknown attacks i.e. it detects behavior that is not known before. No rules are needed to be written for this methodology. It detects malicious traffic based on normal network traffic pattern. The disadvantage of such method is that it generates high false alarm rate.

4.2 Signature based Methodology
This methodology is used to detect unknown attacks which are already predefined in the form of signature and are saved. When a data is sent to the network, it first goes to the server where the server scans it for malicious content. It compares the network packet from the database of signature which is

already stored in the network and if any packet matches, then it discards the packet or if no match is there then it sends the packet to the network. It is good for organization that are concerned with known attack.

4.3 Stateful Protocol Analysis

It compares established profiles of how protocols should behave against the observed behavior. It uses information about connections between the hosts and compares it with the entries present in the state table. The state table keeps a record of connections between computers that include; source IP address and port, destination IP address and port and the protocol that is used. Its main advantage is that system can detect attacks from inside a network.

4.4 Hybrid based

It is the integration of two different intrusion detection system – anomaly and signature-based detectors or may be the hybridization of any two methodologies. It collects the output of both anomaly and signature-based detector and then calculates the attack probability. This method updates anomaly detector's normal network model and also signature-based detectors rule set. It calculates the final decision on the probability of an attack by using the collected outputs of the anomaly and signature-based detectors.

5. SNORT

Snort is a free open source intrusion detection system. It's very popular and powerful multi packet tool run by a lot of different people and companies. It is one of the Signature based Intrusion Detection and Prevention System. The beauty of this tool lies with the formation of rules. Rules can be created/designed to block traffic or to merely send alerts, alerts can be logged to a log file, can be sent to the console or displayed on the screen. They can be configured to send an email to someone or they can be logged to database. Various options can be used for the formation of rules. Snort basically works on the three modes: Sniffer mode, Packet logger mode and NIDS mode. It can be run as a packet sniffer mode from command line which is simply looking at header information and printing the details on the screen. It can be used as a packet logger mode, which takes each packet and log it into the log files which resides in the root directory. The file can be viewed later on using Snort or tcpdump. This mode is for the later use as if someone wants to view the captured packets later on. The third and the last mode is Network Intrusion Detection System mode (NIDS mode) which is the most important mode among all, considering the intrusion detection point of view. Snort as NIDS mode, uses its rules to find out if there are any intrusion activities going on the network. Snort use NICs running in promiscuous mode to analyze and capture raw packet data in real time in NIDS mode. Snort can perform real-time packet logging, content searching/matching and protocol analysis and also can detect a variety of attacks with known loopholes. It not only monitors or detects the intrusions but also can prevent it by taking various actions like_ reject, drop and block. The difference between NIDS and the first two modes of Snort is that the snort in NIDS mode is actually applying different actions to the packet content that are flowing across the network against the ruleset that's indicated it is being used by the snort.

6. LITERATURE REVIEW

The paper [1] first analyzed the architecture of Snort and its working principle. They designed a system using the PF_RING data packet capture module in IDS based on Snort Intrusion behavior can be detected by this system. This system works well and has been successfully tested. As per the authors, this system may provide a good model for the realization of the intrusion detection system.This paper [2] tells about the structure of snort and NTOP, and proposes a new design idea of combining Snort with NTOP, which is validated by the experiment. The results of experiment prove that intrusion behavior can be detected by this system. This system works well and has been successfully tested. As per the authors, this system may provide a good model for the realization of the intrusion detection system.In paper [3], the authors have explained how to implement the intrusion detection process using Snort, which includes building the compiling environment and analyzing the work-flow and rule tree. This paper proposes the process of Snort in Linux and shows how to debug the Snort in VC++. The working process of fpEvalHeaderSW and the building process of intelligent matching rule also been explored in the paper.

In paper [4], the authors have developed a system considering the Software Engineering Framework which gives a solution to combine logging, and network-based intrusion detection and prevention system. They configured the snort in inline mode for Intrusion prevention. Splunk Technology has been used for logging of dropped packets. Future prospects of this paper would be, to write signatures for other protocols and viruses.

In paper [5] the authors analyses various approaches proposed by security researchers specifically using Snort as their IDS tool. To overcome various challenges in Intrusion detection process, this paper proposes a level-based architecture that can detect and prevent both known and unknown attacks. The efficiency of the proposed architecture can be proved by

integrating it with Snort Tool using Code Refactoring. Also, it [5] proposed an environment setup to evaluate the modified Snort Tool performance in future.

This paper [6] provides an effective solution to network security threats by designing the distributed intrusion detection system framework in networks based on Snort. It [6] expounds the ideas and methodology of Snort-based framework in networks, by using centralized network intrusion detection system based on Snort. The main idea of this research paper is to unify distributed detection and centralized management by the hierarchical distribute structure and hence to solve the security threats more effectively that the campus network is facing.

In the paper [7], the authors provide a critical review of the IDS technology, the issues that occurs during its implementation and the challenges and limitation in the Intrusion Detection System. It [7] proposed future work while exploring all the topics of IDS, the in-depth discussion and the contribution of each research in the respective field. It [7] provides effective solutions for the challenges faced in Intrusion detection through various techniques like_ machine learning, AI, data mining, alert processing technique etc. Through this review they outlined many upcoming researches instead LINPAC. They showed the design structure and work process of the packet capture technology used in Snort system, and given the respective test results.

Paper [8], provides detailed information about the current techniques and their approaches to deal with intrusions. It describes the general architecture of IDS and its limitations and challenges that current IDS's face. Authors [8] have made a survey on the overall progress of intrusion detection systems

based on the knowledge of existing types, techniques and architectures in the literature and have highlighted the present research challenges and loopholes in IDS in the paper.

In paper [9], the authors have provided a review on how AI based technique plays an important part in the IDS. They discussed about the advantages and limitations of AI based techniques. The paper helps in better understanding of the concepts and ideas towards different directions of research done in the field of IDS. This [9] paper provide useful insights about the applications of AI based techniques to IDS and related fields. The summary of review of literature is mentioned in Table 1.

Table 1: Survey of various IDPS techniques

Sr. No.	Author	Methodology	Application Area	Future Scope
	Ashara Banu Mohamed et al, 2012	Review paper	Richer Processed Alert	Alert Processing Technique
	Gulshan Kumar et al, 2010	AI based Technique	Machine learning, Data Mining	AI based technique in ID.
	Mohd Nazri Ismail et al, 2009	VPN Technology Implementation	Open Source Analyzer for Snort (OSAS)	Developing a prototype model to filter, delete and quarantine the malware attack in real time network.
	Poonam Sinai Kenkre et al, 2015	Software Engg. Framework, SNORT (inline mode), Splunk technology	Real time IDPS development	Writing Signatures for other protocols and viruses. Separate tool to generate graphs and report of SNORT rules.
	RaviTeja Gaddam et al, 2017	Integrating Snort Tool using Code Refactoring	Deploying modified snort tool in Kali Linux to evaluate the performance of modified snort	Integrate proposed design into snort tool and evaluate it to achieve better detection rate with less false alarm
	YingHui Peng	Combining SNORT with NTOP		Model for realization of perfect intrusion detection system
	YU-XIN DING et al, 2009	Combining misuse-based detection with anomaly detection	HIDS under Debian GNU/Linux	Improve real-time detection performance of HIDS and decrease time cost in ADS module

7. CONCLUSION

So, in future IDPS lands us with the increased level of automation in attack tools driving the expertise required to breach security into nothing. The proportionality increases the complexity of the security which is tough on security professionals. These systems still have a hard time detecting other non-instant or zero-day attacks like the Stuxnet attack. The major offerings of this paper are technologies and methodologies associated with IDPS and how SNORT can be useful in the whole process. The performance of IDPs depends on the detection rate and false positive rates. Nonetheless, IDPs looks as an ever evolving to continue to protect against the newest and modern security threats available.

8. REFERENCES

[1] Chi, R. (2014, January). Intrusion detection system based on snort. In Proceedings of the 9th International Symposium on Linear Drives for Industry Applications, Volume 3 (pp. 657-664). Springer Berlin Heidelberg.

[2] Peng, Y. (2012, May). Research of network intrusion detection system based on snort and NTOP. In Fuzzy Systems and Knowledge Discovery (FSKD), 2012 9th International Conference on (pp. 2764-2768). IEEE.

[3] Zhou, Z., Zhongwen, C., Tiecheng, Z., & Xiaohui, G. (2010, May). The study on network intrusion detection system of Snort. In Networking and Digital Society (ICNDS), 2010 2nd International Conference on (Vol. 2, pp. 194-196). IEEE.

[4] Kenkre, P. S., Pai, A., & Colaco, L. (2015). Real time intrusion detection and prevention system. In Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014 (pp. 405-411). Springer, Cham.

[5] Gaddam, R., & Nandhini, M. (2017, March). An analysis of various snort based techniques to detect and prevent intrusions in networks proposal with code refactoring snort tool in Kali Linux environment. In Inventive Communication and Computational Technologies (ICICCT), 2017 International Conference on (pp. 10-15). IEEE.

[6] Kai, Z. (2012, March). Research and design of the distributed intrusion detection system based on Snort.

In 2012 International Conference on Computer Science and Electronics Engineering (pp. 525-527). IEEE.

[7] Mohamed, A. B., Idris, N. B., & Shanmugum, B. (2012). A brief introduction to intrusion detection system. In Trends in Intelligent Robotics, Automation, and Manufacturing (pp. 263-271). Springer, Berlin, Heidelberg.

[8] Bashir, U., & Chachoo, M. (2014, March). Intrusion detection and prevention system: Challenges & opportunities. In Computing for Sustainable Global Development (INDIACom), 2014 International Conference on (pp. 806-809). IEEE.

[9] Kumar, G., Kumar, K., & Sachdeva, M. (2010). The use of artificial intelligence based techniques for intrusion detection: a review. Artificial Intelligence Review, 34(4), 369-387.

[10] Khamphakdee, N., Benjamas, N., & Saiyod, S. (2014, May). Improving intrusion detection system based on snort rules for network probe attack detection. In Information and Communication Technology (ICoICT), 2014 2nd International Conference on (pp. 69-74). IEEE.

[11] Zhai, J., & Xie, Y. (2011, August). Researh on Network Intrusion Prevention System Based on Snort. In Strategic Technology (IFOST), 2011 6th International Forum on (Vol. 2, pp. 1133-1136). IEEE

[12] Boughrara, A., & Mammar, S. (2012, March). Implementation of a SNORT's output Plug-In in reaction to ARP Spoofing's attack. In Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), 2012 6th International Conference on (pp. 643-647). IEEE

[13] Garg, A., & Maheshwari, P. (2016, January). Performance Analysis of Snort-based Intrusion Detection System. In Advanced Computing and Communication Systems (ICACCS), 2016 3rd International Conference on (Vol. 1, pp. 1-5). IEEE.

[14] Upadhyay, U., & Khilari, G. (2016, May). SQL injection avoidance for protected database with ASCII using SNORT and HONEYPOT. In Advanced Communication Control and Computing Technologies (ICACCCT), 2016 International Conference on (pp. 596-599). IEEE

[15] Patel, S. K., & Sonker, A. (2016, December). Internet Protocol Identification Number Based Ideal Stealth Port Scan Detection Using Snort. In Computational Intelligence and Communication Networks (CICN), 2016 8th International Conference on (pp. 422-427). IEEE