International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Network Intrusion Detection System Using Snort

Dr C K Gomathy[1], Dr V Geetha[2], M. Yajhna Shree[3], R.Sri Pravallika[4]

[1, 2] Assistant Professor, [3, 4] UG Scholars
Department of CSE, SriChandrasekharendra Saraswathi Viswa MahaVidyalaya- (SCSVMV Deemed to be University), India.

ABSTRACT:

An hacker is an attacker who always tries to get unlocked to remove security,intrusion detection system occurs when an unauthorized person try to interrupt the normal flow of operations . Even when such attacks are rising, as in the case of virus and malware, they are always initiated by an alone individual whose purpose is to leak or cause harm to organizational or personal data. IDS consists procedures for detection of unusual activities happening on the network.In security IDS works like a alarm alerts in that it detects attacks happening to the network or the database. An intrusion detection not only used for alerting the devices but also identifies the strengthening and weakening of the systems firewall.Recently Snort has been a widely used tool for identifying Network based Attacks. A Snort is tool which can give alert to the authentic user or Network Administrator by giving alert for illegal network activities.

Key Words: Hacker,alarm ,NetworkAdministrator, attacks, Snort, intrusion detection, illegal.

1. Introduction:

We all know that today we all are dependent on computer technology in any form. As the use of technology is increases, risk associated with technology is also increases. Network security is the big challenge among the researchers. People are working in the field of network security from 1987 when Dorothy Denning published an intrusion detection model [2]. But till now we did not get any perfect solution. There are so many network security tools available such as antivirus, firewall, etc. But they are not able to cover all security risks in the network [11]. The main work of intrusion detection system is to identify the intrusion in the network. And for that it collects important information from the network, process it and if identify attack then alert for the possible attack. This paper focuses on analyzing the abnormal connection that has been detected by our Intrusion Detection System via Snort when we flow the DARPA Data Set over the network. Intrusion Detection System (IDS) works as a network packet sniffer, which based on comparisons of packet contents with known virus signatures encapsulated as rules, can initiate action and record events and information related to them in a log file and/or database. Snort is a popular NIDS that is used to audit network packets and compare those packets with the database of known attack signature. And Snorts attack signature database can also be updated time by time.

2. Literature Survey – NIDS using Snort

Intrusion Detection Systems (IDS) play a crucial role in safeguarding network infrastructure. Among the open-source IDS tools, **Snort** stands out due to its flexibility, signature-based detection capabilities, and

widespread community support. This literature survey presents an overview of recent research and developments in the field of NIDS using Snort.

References (IEEE Style)

[1] M. Roesch, "Snort - Lightweight Intrusion Detection for Networks," *Proceedings of the 13th USENIX Conference on System Administration*, 1999, pp. 229-238.

[2] A. V. Patel, H. R. Modi, and S. J. Patel, "Performance Analysis of Snort Based IDS on Various Attacks," *International Journal of Computer Applications*, vol. 98, no. 6, pp. 15–21, Jul. 2014.

[3] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Computers & Security*, vol. 28, no. 1-2, pp. 18–28, 2009.

[4] S. H. Shah and M. A. Qureshi, "Enhanced Intrusion Detection System using Hybrid Model with Snort," *IEEE International Conference on Emerging Technologies (ICET)*, 2018, pp. 1–6.

[5] B. A. Forouzan and M. Firdaus, "Implementation of Intrusion Detection System using Snort for Security Enhancement in Education Network," *International Journal of Scientific & Technology Research*, vol. 8, no. 11, pp. 2347–2350, 2019.

Need of Intrusion Detection System:

When working on an network our data or personally identifiable information [PII] is our responsibility to make our network more secure by network monitoring tools and making network secure and there are several other reasons to use an Intrusion Detection System. To detect the malware and virus attacks that are cannot be prevented by other security measures :

- To detect and deal with network basedattacks
- To perform the qualified service and secured network for users.
- To provide an insightful information about the malware and the user networking issues.

Network Based Intrusion Detection and Prevention System

A Network Based IDS (NIDS) present in a computer or device connected to a segment of an individual network and monitors network traffic on that network segment, looking for ongoing attacks like for XSS, SQL injection, Cross Site Request Forgery, File Inclusion .When a possible occurances that the network-based Intrusion Detection System is planned to know what's happening on a network, it responds by sending notifications to system administrators. NIDS looks for attack patterns and pattern signatures within network traffic, such as it looks for the exchange of a sequence of related packets in a certain pattern,Which scans ports and protocols on the network attack .NIDS's are installed at a specific place in the network from where it is possible to watch the traffic going into and out of a particular network segment. And or it can be installed to monitor all traffic between the systems that make up an entire network. A fundamental problem for network intrusion detection systems (NIDSs) that passively monitor a network link is the ability of a skilled hacker to destroy detection by exploiting ambiguities in the traffic.

Intrusion Detection Prevention System Methods:

- Signature Based Intrusion Detection System.
- Statistical Anomaly Based Intrusion Detection System.
- Stateful Protocol Analysis Intrusion Detection Prevention System**.**

Intrusion Detection Prevention System Response:

Intrusion prevention systems (IPS)), are network security devices that monitor network and system activities for an unusual activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about said activity, attempt to block the activities, and report to the host .Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and system activities for malicious activity. The main differences are, unlike intrusion detection systems.

The following are some of the responses that an IDS.

- alarms.
- E-mail messages.
- Log entries.
- packet information.
- Reconfigure firewall.
- Close the connection.

Snort:

Snort is an open source network intrusion detection system utilizing a users host, which combines the benefits of signature and pattern, protocol and based inspection methods. Snort is the most widely deployed intrusion detection technology worldwide and has become the in reality standard for the industry. Snort is used primarily to passively monitor network traffic and generate alerts when threats are detected.

Components of Snort:

Snort is multiple divided into different components the major components of the snort to identify the network based attacks are:

I. Packet Decoder
II. Preprocessors
III. Detection Engine
IV. Logging and Alerting System
V. Output Modules

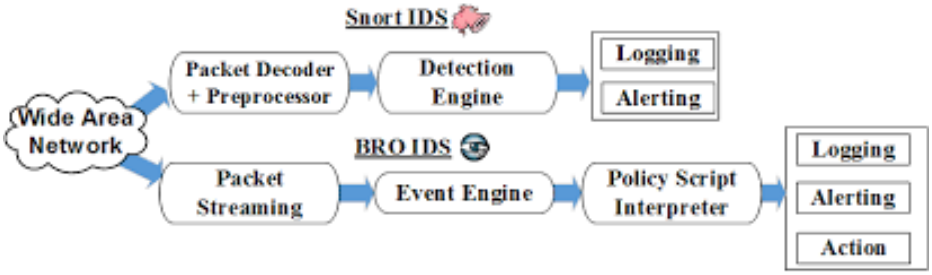

Fig.1 Working of Snort

How to Protect IDS Itself

IDS protects all the network admin attacks but how does it protect itself or identify the different attacks. If security of the IDS is compromised and firewall security might be compromised, you may start getting fake alert for the system admin. The intruder may disable IDS before actually performing any attack. There are different ways to protect your system, starting from exceptionally wideranging recommendations to some sophisticated methods. The first work that you can do is not to run any service on your IDS sensor itself. Implement a WSNNetwork servers are the most common method of destroying a system. New patches shouldreleased by vendors. This is almost a continuous and non-stop process. The platform on which you are running IDS should be patched with the latest releases.Configure the IDS machine so that it does not respond to ping (ICMP Echo-type) packets. If you are running Snort on a Linux machine, use net filter and iptable to block any unwanted data. Snort will still be able to see all of the data.

Snort with Network Interfaces:

To capture a data on the network it is must to have an uniqueidentification for the windows serveras well as the virtual machine for example if you are working on kali linuxthen its mandatory to check the internal and ecternal communications on the network. Generally for the VM's the network interfaces are based on the internal communications such as "lo" -> loopback and "eth0" ethernet communications. And where each has different adaptors and different ip address for the Network address translation there is an different adapter and for the Bridged adapter there is an other network translations. To find out the current network interfaces give the command as the "ip a" or "ifconfig" for the details of the interfaces.

Snort Alert Modes:

```
alert icmp any any -> any any (msg: "ICMP Packet detected"; sid:1000001 ; rev:1;)
```

When Snort is running in the Intrusion packet capturing mode, it generates alerts when a captured packet matches a rule. Snort can send alerts in many modes. These modes are configurable through the command line as well as through snort.luafile. Common alert modes are explained in this section. To explain the alert modes, I have used a rule that creates an alert when Snort detects an ICMP packet with TTL 100. This rule is listed below.

Working with snort rules :

Snort rules are completely based on the network and the protocol used by the user In addition to that, there are databases of known vulnerabilities that intruders want to exploit. These known attacks are also used as signatures to find out if someone is trying to exploit them. These signatures may be present in the header parts of a packet or in the payload. Snort's detection system is based on rules. These rules in turn are based on intruder signatures. Snort rules can be used to check various parts of a data packet. Snort 1.x versions can analyze layer 3 and 4 headers but are not able to analyze application layer protocols. Upcoming Snort version 2 is expected to add support of application layer headers as well. Rules are applied in an orderly fashion to all packets depending on their types. A rule may be used to generate an alert message, log a message, or, in terms of Snort, pass the data packet, i.e., drop it silently. The word pass here is not equivalent to the traditional meaning of pass as used in firewalls and routers. In firewalls and routers, pass and drop are opposite to each other. Snort rules are written in an easy to understand syntax. Most of the rules are written in a single line. However you can also extend rules to multiple lines by using a backslash character at the end of lines. Rules are generally placed in the file called **/etc/snort/rules/local.rules** and also that path is added to the snort.conf and snort .lua file for the identification of the rules.

Conclusion:

This paper proposes the implementation process of Snort in Kali Linux. This IDS System demonstrated that it can detect and analyze the intrusion in real time network traffic. Once the Snort will identify any intrusion then it will send alert to security person and security person will take required action immediately. The future work is to develop an AI based NIDS inorder to visualize it as an dashboard pie char to the users who are able to monitor and identify the network attacks easily.

References:

1. Daniel Barbara, Ningning Wu and Sushil Jajodia Detecting novel network intrusion using bayes estimators. In Proceedings of First SIAM Conference on data mining Chicago, 2001. https://scholar.google.com/scholar?as_q=Detecting+novel+network+intrusion+using+bayes+estimators&as_occt=title&hl=en&as_sdt=0%2C
2. Markus Breunig, Hans-Peter Kriegel, Raymond T. Ng, and Jörg Sander. Lof: Identifying densitybased local outliers. In Proceedings of the ACM SIGMOD Conference, Dallas, TX, 2000. https://ieeexplore.ieee.org/abstract/document/9182928/references#references.
3. Abdulrahman Alzahrani, Ali Alqazzaz, Huirong Fu and Nabil Almashf, Web Application Security Tools Analysis, IEEE, 2017. https://scholar.google.com/scholar?as_q=Web+Application+Security+Tools+Analysis&as_occt=title&hl=en&as_sdt=0%2C31
4. Sandip Sonawane, Shailendra Pardeshi and Ganesh Prasad, "A survey on intrusion detection techniques," Proceeding of National Conference on Emerging Trends in Information Technology (NCETIT), pp. 127-133, 2012. https://scholar.google.com/scholar?as_q=A+survey+on+intrusion+detection+techniques&as_occt=title&hl=en&as_sdt=0%2C31

5. H. Alnabulsi, M. R. Islam and Q. Mamun, "Detecting SQL injection attacks using SNORT IDS," Asia-Pacific World Congress on Computer Science and Engineering, Nadi, Fiji, 2014, pp. 1-7, doi: 10.1109/APWCCSE.2014.7053873.
https://ieeexplore.ieee.org/abstract/document/7053873
6. K. Gupta, R. Ranjan Singh and M. Dixit, "Cross site scripting (XSS) attack detection using intrustion detection system," 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, 2017, pp. 199-203, doi: 10.1109/ICCONS.2017.8250709.
https://ieeexplore.ieee.org/abstract/document/8250709
7. http://proquest.com/openview/885ab9a9d8f5c1b92d177780fbe81699/1?cbl=18750&diss=y&pq-origsite=gscholar