ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

A Comparative Study of Intrusion Detection System tools and Techniques

Sonali Nemade, Madhuri A. Darekar, Jyoti Bachhav, Sunanyna Shivthare

Assistant Professor, Dept. of Computer Science, Dr.D.Y.Patil A.C.S. College, Pune, India

Assistant Professor, Dept. of Computer Science, Dr.D.Y.Patil A.C.S. College, Pune, India

Assistant Professor, Dept. of Computer Science, Dr.D.Y.Patil A.C.S. College, Pune, India

Assistant Professor, Dept. of Computer Science, Dr.D.Y.Patil A.C.S. College, Pune, India

ABSTRACT: Intrusions in computing environment have become very common undesired malicious activities that have taken a start with computing resources. Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) are the standard measures to secure computing resources mostly in a network. In this paper, we have discussed the three technologies and five tools in details, their functionality, their performances and their effectiveness to stop the malicious activity over a computer network. In this paper, our purpose is to focus on how IDS is used to detect intrusion in network to provide safe and intrusion free network by using different tools and techniques. This paper helps in analysing and evaluating of various IDS tools used in high-speed networks. While IDS tools have become prevalent in today's market, they are still not completely fool proof and can fail to identify serious malicious attacks.

KEYWORDS: Intrusion Detection System, Anomaly Detection, SNORT, SURICATA, Bro IDS, SECURITY ONION.

I. INTRODUCTION

IDS is used to identify, monitor, block and report behaviour which is anomalous and use of existing data on computer networks by unauthorized users. Its function is to provide safety to distributed computing environments which are controlled and managed by a particular network. Based on the function IDS are categorised into different types. The main goal of research is to test the IDS tools, determine their efficiency as well as their ease of use which are available in today's market.

Computers and networks Security is managed by Intrusion detection (ID). This system gathers and analyses information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses *vulnerability assessment* (sometimes referred to as *scanning*), which is a technology developed to assess the security of a computer system or network.

The following is a conceptual definition for intrusion: "Any set of actions that attempt to compromise integrity, confidentiality or availability of a resource" [UCR 2008].

There are three properties which can be used to describes characteristics of IDS,

1. *Confidentiality* – Authorized users are only allowed to access the information and Unauthorized persons are not allowed
2. *Integrity* – This talks about trustworthiness of information. Integrity is also known as data consistency. Data is not allowed to be altered in unauthorized manner
3. *Availability* – Information is made available to authorized users only.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

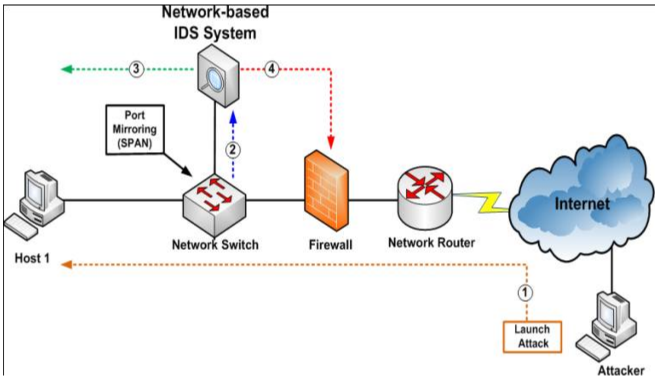
(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

II. TYPES OF IDS'S

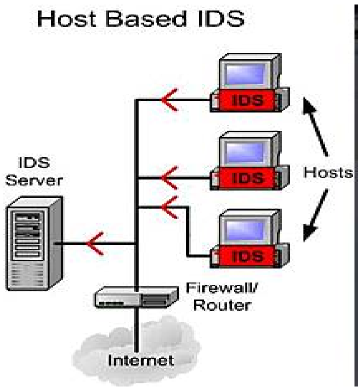
A. NETWORK-BASED:



A Network Intrusion Detection System (NIDS) is one common type of IDS that analyses network traffic at all layers of the Open Systems Interconnection (OSI) model and monitors the network traffic for malicious activity. They are easy to develop and its possible to view traffic from many systems at one glance. A term becoming more widely used by vendors is "Wireless Intrusion Prevention System" (WIPS) to describe a network device that monitors and analyses the wireless radio spectrum in a network for intrusions and performs counter measures which monitors network traffic for particular network segments or devices and analyses the network and application protocol activity to identify suspicious activity. It can identify many different types of events of interest. The NIDS are also called passive IDS since this kind of systems inform the administrator system that an attack has or had taken place, and it takes the adequate measures to assure the security of the system.

This is beneficial in situations where network topology changes or where system resources have been moved, the intrusion detection system monitors can be moved and used as needed. However, network-based solutions have their share of problems.

B. HOST-BASED SYSTEMS



The main aim of Host-based intrusion detection systems is to collect information about activity on a particular single system, or host. These host-based agents, which are sometimes referred to as sensors, would typically be installed on a machine that is deemed to be susceptible to possible attacks. The term "host" refers to an individual computer, thus a separate sensor would be needed for every machine. Sensors work by collecting data about events taking place on the system being monitored. Other sources from which a host-based sensor can obtain data, "include system logs, other logs generated by operating system processes, and contents of objects not reflected in standard operating system audit and logging mechanisms" [1].

According to the source of the data to examine, the Host Based Intrusion Detection System can be classified in two categories:

1. **The HIDS Based Application:**
   The IDS of this type receive the data in application, for example, the logs files generated by the management software of the database, the server web or the firewalls.
2. **The HIDS Based Host:**
   The IDS of this type receive the information of the activity of the supervised system. This information is sometimes in the form of audit traces of the operating system. It can also include the logs system of other logs generated by the processes of the operating system and the contents of the object system not reflected in the standard audit of the operating system and the mechanisms of logging. A HIDS must be installed on each machine and requires configuration specific to that operating system and software.

C. HYBRID INTRUSION DETECTION SYSTEM:

Hybrid intrusion detection systems facilitate management and alert notification from both network and host-based intrusion detection devices. Hybrid solutions provide logical complement to NID and HID - central intrusion detection management. Some of the most current intrusion detection system only uses one of the two detection methods, misused detection or anomaly detection both of them have their own limitations, The technique which combines misuse detection system and anomaly detection system is known as hybrid intrusion detection system .

a) Anomaly Intrusion Detection :

An Anomaly-Based Intrusion Detection System is a system for detecting computer intrusions which are classified as either normal or anomalous. The classification is done by heuristics or rules, rather than patterns or signatures, and will detect any type of misuse that different from normal system operation [8]. Anomaly-based Intrusion Detection does have some disadvantage, namely a high false positive rate and the ability to be fooled by a correctly delivered attack, but it is good technique for known attacks.

b) Misuse Intrusion Detection :

Another major technique of IDS is known as misuse detection. It is also sometimes known to as signature-based detection because alarms are generated based on specific attack signatures. These attack signatures passes specific traffic or activity that is based on known intrusive activity.

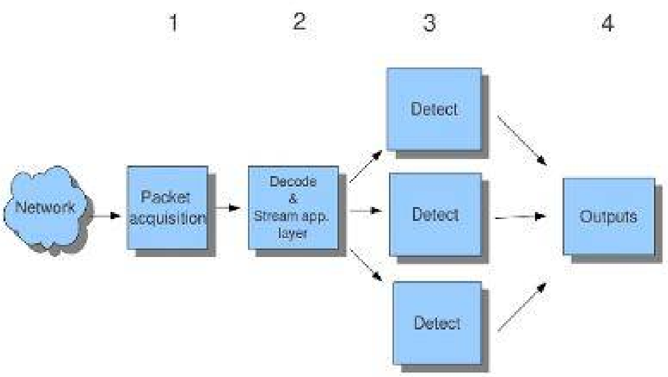
III. IDS TOOLS

There are several IDS tools are available at free of cost. The followings are the list of IDS tools with its descriptions, advantages and disadvantages.

A. SURICATA:

Suricata is one of the fast and robust network intrusion detection engine. It is capable of real time intrusion detection (IDS). Suricate is based on a signature-based methodology, rule/policy driven security, and anomaly-based approach for detecting intrusions [10]. Suricata inspects the network traffic using a powerful and extensive rules and signature language.

Suricata is an open source, fast and highly robust network intrusion detection system developed by the Open Information Security Foundation. The Suricata engine is capable of real-time intrusion detection, inline intrusion prevention and network security monitoring. Suricata consists of a few modules like Capturing, Collection, Decoding, Detection and Output. It captures traffic passing in one flow before decoding, which is highly optimal. It configures separate flows after capturing and specifying how the flow will separate between processors.



Advantages:

1. Does the network traffic processing on the seventh layer of the OSI model which, in turn, enhances its capability to detect malware activities.
2. Automatically detects and parses protocols like IP, TCP, UDP, ICMP, HTTP, TLS, FTP, SMB and FTP so that rules apply on all protocols.
3. Advanced features consist of multi-threading and GPU acceleration.

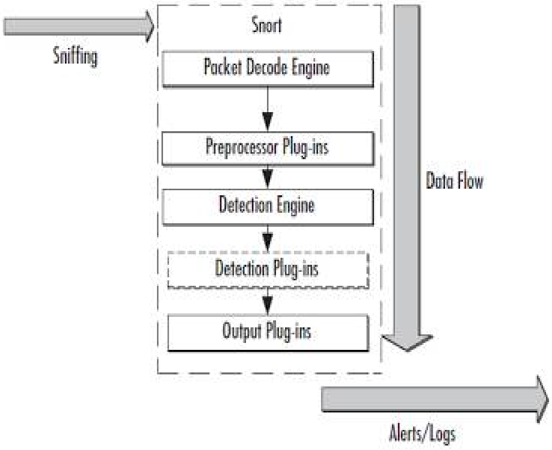
Disadvantages:

1. Less support as compared to other IDSs like Snort.
2. Complicated in operation and requires more system resources for full-fledged functioning

B. SNORT:

Snort is open source software and light weight software developed by Martin Roesch in 1998, and is an open source network intrusion detection and prevention system. Snort software act as a packet sniffer, packet logger or as a network intrusion detection and prevention system [NIDS, NIPS]. Snort will read network packets and display them on the console if it is in a sniffer mode, it will log packets to disk at the time of packet logger selection. It will monitor the network traffic and analyse the traffic against a rule set defined by the user at the time of network intrusion detection and prevention system. This comes under network IDS.

Snort Architecture consists of mainly 7 modules



1. **Packet Capture Module:** This module gathers packets from network adapter. It is based on the libpcap library for Unix like systems and for windows systems WinPacap is used.

2. Decoder: Decoder fits the captured packets into data structures and identifies link level protocols. Then, it takes the next level, decodes IP, and then TCP or UDP in order to get useful information like ports and addresses. Snort will alert if it finds malformed headers (unusual length TCP options, etc.)

3. Pre-processors: Pre-processors can be treated as filters, which identifies things such as suspicious connection attempts to some TCP/UDP ports or too many TCP SYN packets sent in a short period of time (port scan). Pre-processors function is to take packets potentially dangerous for the detection engine to try to find known patterns. Pre-processors can alert on, classify, or drop a packet before sending it to detection engine

4. Detection Engine: Detection Engine makes use of the detection plug-ins, it matches packets against rules loaded into memory during Snort initialization.

5. Rules Files: Rules are plain text files which contain a list of rules with syntax. This syntax includes protocols, addresses, output plug-ins associated and some other things.

6. Detection Plug-ins: These are modules referenced from its definition in the rules files. They are used to identify patterns whenever a rule is evaluated.

7. Output Plug-ins: These are the modules which allow formatting the notifications (alerts, logs) for the user to access them in many ways (console, extern files, databases, etc).

Advantages:

1. Free to download and is open source.
2. Easy to write rules for intrusion detection.
3. Highly flexible and dynamic in terms of live deployments.
4. Good community support for solving problems and is under rapid development.

Disadvantages:

1. No GUI interface for rule manipulation.
2. Somewhat slow in processing network packets.
3. Cannot detect a signature split over multiple TCP packets, which occurs when packets are configured in inline mode.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

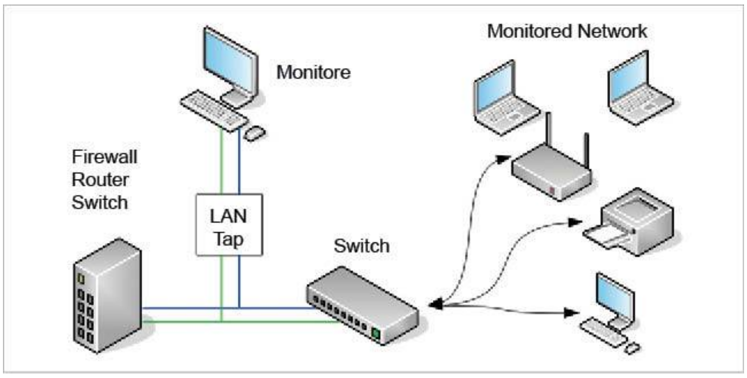
(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

C. OPEN WIPS-NG:

OpenWIPS-ng is an open source and modular Wireless IPS (Intrusion Prevention System). It captures wireless traffic and detects and identifies standard and hidden networks in order to attempt to detect intrusions. Pattern based IDS have also been designed in recent studies that concentrate on the configuring of an IDS solution that will allow the method of detection to be based on an essential part of the network such as protecting specific protocols as a basis for the method of detection. It is composed of three parts:



Sensor(s): a “Dumb” device that capture wireless traffic and sends it to the server for analysis. Also responds to attacks.

Server: Aggregates the data from all sensors, analyses it and responds to attacks. It also logs and alerts in case of an attack.

Interface: GUI manages the server and displays information about the threats on your wireless network(s). This is signature based intrusion detection. This can run in the commodity hardware. This performs scanning, detection and intrusion prevention process.

Advantages:

1. Modular and plugin based.
2. Software and hardware required can be built by DIYers.
3. Additional features are supported via use of plugin.

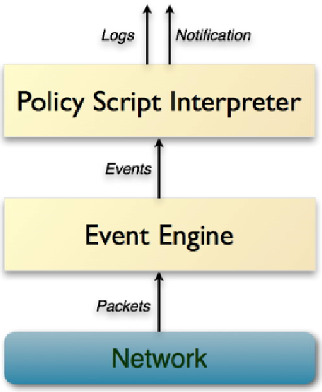
Disadvantages:

1. Only works for wireless networks.
2. Only suitable for low and medium level administration, and not fully compliant for detecting all sorts of wireless attacks.
3. No detailed documentation and community support compared to other systems.

D. BRO IDS:

Bro IDS is anomaly-based intrusion detection, and is usually employed in combination with Snort. Bro is actually a domain-specific language for networking applications in which Bro IDS is written. The technology is especially effective at nearly every signature has an arrow to the right. This means that only packets with the same direction can match.

Bro-ids Architecture consists of mainly 5 modules.



1) Packet Capture:

Bro captures traffic using libpcap. Packets filtered by Bro-IDS are based on ports and bits in IP or TCP headers. For examples, 13th bit of TCP header indicates whether it is set with SYN, FIN, RST or nothing. This information is important to keep the status of TCP connections states.

2) **Event Engine:**

This layer performs several integrity checks to assure that the packet headers are well-formed. For example, it verifies the IP header checksum is correct. At this point Bro reassembles IP fragments so that network layer analyzer can accent to complete IP datagram's. It sends events to the Policy layer.

3) **Signature Engine**:

Signature Engine inspects the packet stream, and generates an event each time a signature is matched. Those events can then be analyzed by a policy script.

4) **Policy Layer:**

The policy script interpreter executes scripts written in a specialized Bro language. These scripts specify event handlers the happenings received for the Event.

E. SECURITY ONION

It is actually an Ubuntu-based Linux distribution for IDS and network security monitoring (NSM), and consists of several of the above open source technologies working in concert with each other. For those desiring the best of the aforementioned tools in one single package, Security Onion is worth considering among all. Security Onion contains three major functionalities, such as full packet capturing process, network-based (NIDS) and host-based intrusion detection intrusion detection systems (HIDS) and powerful analysis tools, and provides log and alert data for detected events and activities. Security Onion provides multiple IDS options.

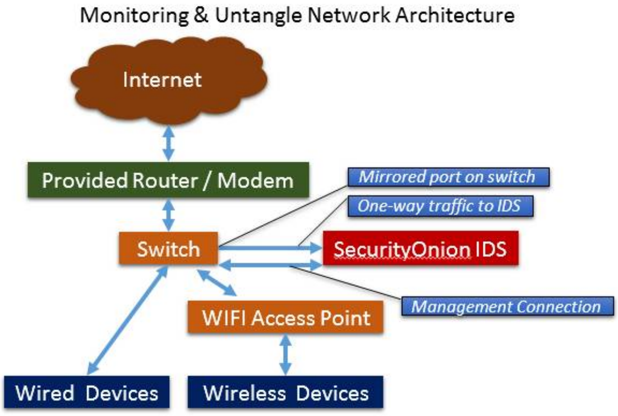
It requires proper management by the systems administrator to review alerts, monitor network activity and to regularly update the IDS based detection rules. Security Onion has three core functions:

1. **Full packet capture:**

   This is done using net sniffing, which captures all network traffic that Security Onion can see, and stores as much as your storage solution can hold. It is like a real-time camera for networks, and provides all the evidence of the threats and malicious activities happening over the network.

2. **Network-based and host-based IDS:**

   It analyses the network or host systems, and provides log and alert data for detected events and activity. Security Onion has varied IDS options like rule-driven IDS, analysis-driven IDS, HIDS, etc.



3. **Analysis tools:**

   In addition to network data capture, Security Onion comprises various tools like Sguil, Squert, ELSA, etc, for assisting administrators in analysis. Security Onion also provides diverse ways for the live deployment of regular standalone, server-sensor and hybrid monitoring tools.

IV. COMPARISON OF IDS TOOLS

Tool Name	Provider	Type	Description	Platform
SURICATA	Open information security foundation	NIDS, NIPS	Automatic Protocol Detection, File Matching Process And Compatible With SNORT	Linux, unix ,MAC,windows etc.,
SNORT	Cisco system	NIDS, NIPS	Can Detect Dos, CGI, Intrusion, Port Scans, SMB And Layer Attacks. SNORT Has The Ability To Make Concurrent Traffic Analysis And Packet Logging On Internet Protocol (IP) Networks	(Cross Platform) Linux, windows
OpenWIPS-ng	Dug Song	NIDS	This Tool Was Written In Good Faith To Aid In The Testing Of Network Intrusion Detection Systems, Firewalls, And Basic TCP/IP Stack Behaviour.	Linux
Bro IDS	Vern Paxson	NIDS, AIDS	Employed In Combination With Snort	Linux, MAC OS X, FreeBSD
Security Onion	Aircrack-NG	NIPS	Openwips-Ng Is An Open Source And Modular Wireless IPS (Intrusion Prevention System).	Linux

V. CONCLUSION

In this paper we have studied and focused about various intrusion detection techniques and tools. This study gives the overview and its advantages and disadvantages of the tools that are used to detect and prevent the intrusions. In this paper we analysed three types of IDS and five intrusion system tools, the IDS types are network based, host based intrusion detection system, hybrid IDS. From the comparison made between these tools and techniques, we summarize some points. Several tools support only little type of security threats and issues. Defining rules properly will lead the highest detection rate, so the rules should be configured properly. Several tools are still having trouble in detection of accurate intruders with minimum hardware and sensor supports. So there is a need to provide a comprehensive analysis to make a new and effective tool with high accuracy in detection and less in computational cost.

REFERENCES

1. Sandip K. "Host based intrusion detection system. International Conference on Mechanical Engineering and Technology (ICMET-London 2011). ASME Press, 2011.
2. K. Vinod and O. P. Sangwan, "Signature based intrusion detection system using snort", International Journal of Computer Applications & Information Technology, vol. 1, no. 3, **(2012)**, pp. 35-41.
3. R. R. Ur, "Intrusion detection systems with Snort: advanced IDS techniques using Snort, Apache, MySQL, PHP, and ACID", Prentice Hall Professional, **(2003)**.
4. Helman, P., Liepins, G., Richards, W.: Foundations of Intrusion Detection. In: Proceedings of the IEEE Computer Security Foundations Workshop V (1992).
5. Janne Anttila", Intrusion Detection in Critical Ebusiness Environment ", Presentation, 2004.
6. Day, David, Burns B. A performance analysis of snort and suricata network intrusion detection and prevention engines. Fifth International Conference on Digital Society, Gosier, Guadeloupe. 2011.
7. Burks, Doug. "Security Onion. nd.[Online]. Available: http://blog. securityonion. net/p/securityonion. html.[Accessed 11 May [2014] (2012).
8. Depren, Ozgur. An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks. Expert systems with Applications. 2005; 29(4): 713-722.
9. Sandip K. "Host based intrusion detection system. International Conference on Mechanical Engineering and Technology (ICMET-London 2011). ASME Press, 2011.
10. Vigna, Giovanni, Kemmerer RA. NetSTAT: A network-based intrusion detection system." Journal of computer security. 1999; 7(1): 37-71.