# COMPARISON BETWEEN HIDS AND NIDS

**Subhash**[*]

**Jyoti Yadav**[**]

**Dr. Deepak Dhull**[***]

## Abstract

**In this paper we define and discuss various types and techniques of Intrusion Detection and the intrusion detection system that are employed to detect these attacks. We also present features of various Intrusion Detection tools .A comparison of the basic types of Intrusion Detection system has been done.**

***Index Terms*—Anomaly detection; Intrusion Detection; Intrusion Detection Tools; Network security; Network Attacks; Signature detection.**

[*] M.Tech Student (Siddhivinayak College of Higher Education,Alwar(Raj.))

[**] Govt. College, Narnaul (Hr)

[***] Head, Deptt. Of Computer Science, GC, Narnaul(Hr)

**INTRODUCTION:-** Security is a big issue for all networks in today's environment. Intrusion detection is a set of techniques and methods that are used to detect suspicious activity both at the network and host level. Why worry about detecting intrusions if you've installed firewalls, spam filters, and activated passwords for authenticity? The answer is simple because intrusions still do occur!! For example generally people forget to lock a window, similarly they sometimes forget to correctly update a firewall's rule set. Computer systems are still not 100 percent safe even with the most advanced protection. In fact, most computer security experts agree that, given user-desired features such as network connectivity, we'll never achieve the goal of a completely secure system. As a result, we must develop and deploy intrusion detection techniques and tools to discover and react against computer attacks. Intrusion detection systems or IDS do exactly as the name suggests: they detect possible intrusions. The goal of IDS tools is to detect computer attacks or illegal access, and to alert the concerned people about the detection or security breach. An IDS installed on a network can be viewed as a burglar alarm system installed in a house [1].Measures to evaluate the efficiency of an intrusion detection:

- **Accuracy** – Inaccuracy occurs when an intrusion detection system flags as anomalous or intrusive a legitimate action in the environment.
- **Performance** – The performance of an intrusion detection system is the rate at which audit events are processed. If the performance of the intrusion detection is poor, then real-time detection is not possible.
- **Completeness** – Incompleteness occurs when the intrusion detection system fails to detect an attack. This measure is very difficult to evaluate because it is impossible to have a global knowledge about the attacks or abuses of privileges.
- **Fault Tolerance** – An intrusion detection system should itself be resistant to attacks, especially denial of service, and should be designed with this goal in mind. This is very important because most of the IDS run on top of commercially available operating systems or hardware, which are known to be vulnerable to attacks.
- **Timeliness** – An IDS has to perform and propagate its analysis as quickly as possible to enable security procedures. This implies more than the measure of performance, because it not only encompasses the intrinsic processing speed of the intrusion detection system, but also the time required to propagate the same and to react to it.

There are three **basic types of intrusion detection systems**: Host-based and Network-based stack-based. Each has a distinct approach to monitor and secure data, and distinct advantages and disadvantages. But in this paper we will focus mainly on HIDS and NIDS.

***Host-based intrusion detection systems (*HIDS)** are IDSs that operate on a single workstation. HIDSs evaluate information found on a single or multiple host systems, including contents of operating systems, system and application files. HIDS monitor traffic on its host machine by utilizing the resources of its host to detect attacks. [2]

***Network-based intrusion detection systems*** **(NIDS)** are IDSs that operate as stand-alone devices on a network. NIDSs evaluate information captured from

Network communications, analyzing the stream of packets which travel across the network . NIDS monitors traffic on the network to detect attacks such as denial of service attacks; port scans or even attempts to crack into computers by monitoring network traffic [2]. The TABLE 1 shows the difference between HIDS and NIDS

| **Properties** | **Network Based Intrusion Detection** | **Host based intrusion detection systems** |
|---|---|---|
| **Residence** | the computer/application connected to a part on an organization's network | a particular computer or server, known as the host. |
| **Functioning** | monitors network traffic on that segment looking for indication of ongoing or successful attacks. | monitors activity only on that system looking for any malicious program running. |
| **Types** | Snort, Cisco NIDS, and Netprowler | e Tripwire, Cisco HIDS, and Symantec ESM |
| **Working device** | NIDS uses a monitoring port, when placed next to a networking device like hub, switch. The port views all the traffic passing through the device. | Capable of monitoring system configuration data bases, such as windows registries, and stored configuration files like .ini, .cfg and .dat files. |
| **Working principle** | Works on the principle of signature matching, ie comparing attack patterns to known signatures in their data base. | . Work on the principle of configuration and change management. An alert is triggered when file attributes change, new files created or existing files deleted. |
| **Works in** | NIDS are suitable for medium to large scale organizations due to their volume of data and resources. So, many smaller companies are hesitant in deploying IDS. | Generally, most HIDS have common architec-tures, meaning that most host systems work as host agents reporting to a central console. |
| **Protection on/off LAN** | It protects you on your LAN but not off the LAN | It protects you on and off the LAN |
| **Versatility** | Less | More |
| **Price** | Expensive | HIDS are more affordable systems |
| **Training required** | More | Less than NIDS |
| **Bandwidth requirements on (LAN)** | 2(NIDS uses up LAN bandwidth) | 0(HIDS does not use LAN bandwidth) |
| **Scan area** | Neither scan possible | Local machine registry scans and personal area networks scan are |

| | | |
|---|---|---|
| | | possible |
| **Disable risk factor** | Failure rate is much higher | Less |
| **Upgrade potential** | NIDS is typically flashed onto the flash memory and has low overhead. | HIDS can be upgraded through a centralized script |

Another type of intrusion detection is *Stack-based intrusion detection system (SIDS)* :This type of system consists of an evolution to the HIDS systems. The packets are examined as they go through the TCP/IP stack and, therefore, it is not necessary for them to work with the network interface in promiscuous mode. This fact makes its implementation to be dependent on the Operating System that is being used.

**Limitations of IDS**

a)*Noise* can severely limit an Intrusion detection system's effectiveness.

b)*Bad packets* generated from software bugs, corrupt DNS data, and local packets that escaped can create a significantly high false-alarm rate.[5]

It is not uncommon for the number of real attacks to be far below the false-alarm rate. Real attacks are often so far below the false-alarm rate that they are often missed and ignored.[5]

Many attacks are geared for specific versions of software that are usually outdated.

A constantly changing library of signatures is needed to deal with such threats. Outdated signature databases can leave the IDS vulnerable to new strategies.[5]

**INTRUSION DETECTION TECHNIQUES**

In this section we explain the intrusion detection Techniques. Basically, there are 3 techniques in IDS:

Anomaly based , Signature/Misuse based, Stateful Protocol Analysis Detection.

***Misuse/Signature-Based Detection***: This method of detection utilizes signatures, which are attack patterns that are preconfigured and predetermined. Based upon a set of signatures and rules, the detection system is able to find and log suspicious activity and generate alerts. This IDS analyzes the network traffic looking for patterns that match a library of known signatures. Once a match is found the intrusion prevention system takes appropriate action.

The issue is that there will be lag between the new threat discovered and Signature being applied in IDS for detecting the threat. During this lag time your IDS will be unable to identify the threat.[3] The way this technique deals with intrusion detection resembles the way anti-virus software operates. Signatures can be exploit-based or vulnerability-based.

Exploit-based signatures analyze patterns appearing in exploits being protected against, while Vulnerability-based signatures analyze vulnerabilities in a program, its execution, and conditions needed to exploit .

Example: Some IDS that use signature based strategy are Snort , Network Flight Recorder , Network Security Monitor etc.

***Advantages:***

i. These are very effective at detecting attacks without generating an overwhelming number of false alarms.

ii.These quickly and reliably diagnose the use of a specific attack tool or technique. This can help security managers prioritize corrective measures and track security problems on their systems.

iii.These are very effective at detecting known threats.

***Disadvantages:***

i. These detectors can only detect those attacks they know about therefore they must be constantly updated with signatures of new attacks.

ii. These detectors are designed to use tightly defined signatures that prevent them from detecting variants of common attacks.

iii. largely ineffective at detecting unknown threats and many variants on known threats.

iv. . Signature-based detection cannot track and understand the state of complex communications, so it cannot detect most attacks that comprise multiple events.

***Anomaly/Statistical Detection****:* An anomaly based detection engine will search for something rare or unusual . They analyze system event streams, using statistical techniques to find patterns of activity that appear to be abnormal. This technique is based on the detection of traffic anomalies. This method of detection works by creating baseline performance of average network traffic conditions. After a baseline is created, the system intermittently samples network traffic, using statistical analysis to compare the sample to the set baseline. If the activity is outside the baseline parameters, the intrusion prevention system takes the appropriate action.

Basically a statistical anomaly-based IDS determines normal network activity like what sort of bandwidth is generally used, what protocols are used, what ports and devices generally connect to each other- and alert the administrator or user when traffic is detected which is anomalous(not normal).[3] Anomaly-based intrusion detection usually depends on packet anomalies present in protocol header parts. In some cases these methods produce better results compared to signature-based IDS. An anomaly-based IDS tries to find suspicious activity on the system. After that, the system will inform about any suspicious activity.

***Advantages:***

i. Detect unusual behavior and thus have the ability to detect symptoms of attacks without specific knowledge of details.

ii. Anomaly detectors can produce information that can in turn be used to define signatures for misuse detectors.

iii.Very effective at detecting previously unknown threats.

***Disadvantages:***

i.Usually produce a large number of false alarms due to the unpredictable behaviours of users and networks.

ii.It often require extensive "training sets" of system event records in order to characterize normal behaviour patterns.

iii. These are highly expensive

iv. These might recognize an intrusive behavior as normal behavior because of insufficient data.

v. It inadvertently includes malicious activity within a profile.

vi. It establishes profiles that are not sufficiently complex to reflect real-world computing activity.

vii. It generates many false positives.

***Stateful Protocol Analysis Detection**:* This method identifies deviations of protocol states by comparing observed events with “predetermined profiles of generally accepted definition of benign activity.”[4] It works by comparing predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations. Unlike anomaly-based detection, which uses host or network-specific profiles, stateful protocol analysis relies on vendor-developed universal profiles that specify how particular protocols should and should not be used.

***Advantage:***

It is capable of understanding and tracking the state of protocols that have a notion of state, which allows it to detect many attacks that other methods cannot.

***Disadvantages:***

i.It is often very difficult or impossible to develop completely accurate models of protocols.

ii. It is very resource-intensive.

iii. It cannot detect attacks that do not violate the characteristics of generally acceptable protocol behavior.

## TOOLS FOR IDS

A large number of intrusion detection products are available today (freely available / commercial) which address a range of organizational security goals and considerations. We have provided a list of most common IDS tools.

***SNORT*** - A free and open source network intrusion detection and prevention system, was created by Martin Roesch in 1998 and now developed by Sourcefire. [7][8]. Through protocol analysis, content searching, and various pre-processors, Snort detects thousands of worms, vulnerability exploit attempts, port scans, and other suspicious behavior .This lightweight network intrusion detection and prevention system excels at traffic analysis and packet logging on IP networks. It detects threats, such as buffer overflows, stealth port scans, CGI attacks, SMB probes and NetBIOS queries, NMAP and other port scanners and DDoS clients, and alerts the user about them. It develops a new signature to find vulnerabilities. It records packets in their human-readable form from the IP address.

***OSSEC* –** HIDS –An open source host-based intrusion detection system, performs log analysis, integrity checking, rootkit detection, time-based alerting and active response [7][8].In addition to its IDS functionality, it is commonly used as a SEM/SIM solution. Because of its powerful log analysis engine, ISPs, universities and data centers are running OSSEC HIDS to monitor and analyze their firewalls, IDSs, web servers and authentication logs. It is scalable, multi-platform, open source Host-based Intrusion Detection System (HIDS). It has a powerful correlation and analysis engine, integrating log analysis; file integrity checking; Windows registry monitoring; centralized policy enforcement; rootkit detection; real-time alerting and active response.

***OSSIM:*** The goal of Open Source Security Information Management, OSSIM is to provide a comprehensive compilation of tools which, when working together, grant network/security administrators with a detailed view over each and every aspect of networks, hosts, physical access devices, and servers [7]. OSSIM incorporates several

other tools, including Nagios and OSSEC HIDS.

***SURICATA****:* An open source-based intrusion detection system, was developed by the Open Information Security Foundation (OISF) [9].

***BRO****:* An open-source, Unix-based network intrusion detection system [9]. Bro detects intrusions by first parsing network traffic to extract its application-level semantics and then executing event-oriented analyzers that compare the activity with patterns deemed troublesome.

***BASE****:* The Basic Analysis and Security Engine, BASE is a PHP-based analysis engine to search and process a database of security events generated by various IDSs, firewalls and network monitoring tools [7].

***SGUILl****:* Sguil is built by network security analysts for network security analysts [8].Its main component is an intuitive GUI that provides real-time events from Snort/barnyard. It also includes other components which facilitate the practice of network security monitoring and event driven analysis of IDS alerts.

***FRAGROUTE*** – It is a one-way fragmenting router – IP packets get sent from the attacker to the Fragrouter, which transforms them into a fragmented data stream to forward to the victim. Fragrouter helps an attacker launch IP-based attacks while avoiding detection.

***METASPLOIT*** - It is an advanced open-source platform for developing, testing, and using exploit code. It ships with hundreds of exploits, as you can see in their online exploit building demo. This makes writing your own exploits easier, and it certainly beats scouring the darkest corners of the Internet for illicit shell code of dubious quality.

***TRIPWIRE*** – It Detects Improper Change, including additions to, deletions from and modifications of file systems and identifies the source. It Simplifies and Eases Management of Change Monitoring Policies.

## CONCLUSION

First of all we compare the intrusion detection techniques normally used i.e signature-based IDS and anomaly-based IDS . Both have advantages and disadvantages which imply that none of them can be said to be better than the other. Signature- based IDS are more reliable and provide better performance when the system receives patterns that match with the library of known signatures, but is not able to detect new attacks not available in the signature database. In contrast, the anomaly based IDS are able to detect unknown attacks with the disadvantage of increasing the number of false alarms. In either of the techniques , without neglecting the need to protect systems against reported attacks, it is very important to have systems capable of reacting against new attacks, because these new attacks are often the most dangerous due to the absence of pre-established defenses. Secondly we compare the two basic intrusion detection systems used

.HIDs examine specific host-based actions, such as what applications are being used, what files are being accessed and what information resides in the kernel logs. NIDs analyze the flow of information between computers, i.e., network traffic. They essentially "sniff" the network for suspicious behavior. Thus, NIDs can detect a hacker before he's able to make an unauthorized intrusion, whereas HIDs won't know anything is wrong until the hacker has already breached the system. Thus in a summarized way HIDs Benefits are that these may seem like a poor solution at first, but they do have several benefits. For one, they can prevent attacks from resulting in any damage. For instance, if a malicious file attempts to rewrite a file, the HID can cut off its privileges and quarantine it. HIDs can keep laptops protected when they're taken off a network and into the field. Ultimately, HIDs are a "last line of defense" tool used to ward off attacks missed by the NID. While the NIDs Benefits include its excellence to protect hundreds of computer systems from one network location. This makes a NID less expensive and easier to deploy. More important, it allow administrators to protect non-computer devices, such as firewalls, print servers, VPN concentrators and routers. Additional benefits include flexibility with multiple operating systems and devices, and protection against bandwidth floods and DoS attacks. Thus an Optimal Solution is that network should feature both a HID and a NID. The former will protect local machines , while the NID will keep the actual network safe and secure. Both are capable of providing more security than any single firewall or anti-virus suite, but each lacks certain capabilities that the other contains. Thus, combining the two is the only way to create a truly robust defensive network. Most existing intrusion detection systems suffer from at least two of the following problems [2]:

First, the information used by the intrusion detection system is obtained from audit trails or from packets on a network. Data has to traverse a longer path from its origin to the IDS and in the process can potentially be destroyed or modified by an attacker. Furthermore, the intrusion detection system has to infer the behavior of the system from the data collected, which can result in misinterpretations or missed events. This is referred as the *fidelity* problem.

Second, the intrusion detection system continuously uses additional resources in the system it is monitoring even when there are no intrusions occurring, because the components of the intrusion detection system have to be running all the time. This is the *resource usage* problem.

Third, because the components of the intrusion detection system are implemented as separate programs, they are susceptible to tampering. An intruder can potentially disable or modify the programs running on a system, rendering the intrusion detection system useless or unreliable. This is the *reliability* problem.

## REFERENCES

[1] Paul Innella and Oba McMillan, Tetrad Digital Integrity, LLC “An Introduction to Intrusion Detection Systems” December 6, 2001

[2] Micheal E. Whitman and Herbert J. Mattord, “Principles of Information Security” page 289-294

[3]Mattord, verma (2008). *Principles of Information Security*. Course Technology. pp. 290–301.

[4].Michael E. Whitman; Herbert J. Mattord (2009). *Principles of Information Security*. Cengage Learning EMEA.

[5] Anderson, Ross (2001). *Security Engineering: A Guide to Building Dependable Distributed Systems*. New York: John Wiley & Sons. pp. 387–388. ISBN 978-0-471-38922-4.

[6] Engin Kirda; Somesh Jha; Davide Balzarotti (2009). *Recent Advances in Intrusion Detection: 12th International Symposium, RAID 2009, Saint-Malo, France, September 23–25, 2009, Proceedings*. Springer. pp. 162–. ISBN 978-3-642-04341-

[7] Sectools.Org: Results; http://sectools.org/tools.html

[8] SecTools.Org: Top 125 Network Security Tools; http://sectools.org/tag/ids/

[9] Suricata (software); http://en.wikipedia.org/wiki/Suricata_(software)