Network Based Intrusion Detection and Prevention Systems: Attack Classification , Methodologies and Tools

Nareshkumar Harale, Dr. B.B.Meshram
SGBAU, Amravati, VJTI, Mumbai, Maharashtra, India

Abstract: *Complex and common security attackshave become a common issue nowadays. Success rate of detecting these attacks through existing tools seems to be decreasing due to simple rule-bases Some attacks are too complex to identify for today's firewall systems.This paper highlights various security attacks classification techniques pertaining to TCP/IP protocol stack, it also covers an existingintrusion detection techniques used for intrusion detection , and features of various open source and commercial Network Intrusion Detection and Prevention (IDPS) tools. Finally paper concludes with comparison and evaluation of an open source and commercial IDPS tools and techniques which are used to detect and prevent the security attacks.*

Keywords—*Signature Detection, Anomaly Detection, Static Anomaly, Dynamic Anomaly, Network Attacks, Intrusion Detection Methodologies, Network Security Tools, Network IDS (Intrusion Detection System), Network IPS (Intrusion Prevention System), Network IDPS (Intrusion Detection and Prevention System).*

I. INTRODUCTION

Suppose a strange man is standing in front of your house. He looks around, studying the surroundings, and then walks to the front door and tries to open it. The door is locked. Efforts in vain, he moves to a nearby window and gently tries to open it. It, too, is locked. It seems your house is secure. So why to install an alarm? This is a common question for intrusion detection advocates. Why bother detecting intrusions if you've configured WAN routers, Core Switches, installed firewalls, spam filters security controls, and activated passwords for authenticity? The newer simple: because intrusions still do occur!! Just as people sometimes forget to lock a window, for example, they sometimes forget to correctly update a firewall's rule set. Computer systems are still not 00 percent safe even with the most advanced protection. In fact, most computer security experts agree that, given user-desired features such as Networkconnectivity; we'll never achieve the goal of a completely secure system. An intrusion is a formal term escribing the act of compromising a system. And detecting either failed or successful attempts to compromise the system is called an Intrusion Detection. In a nutshell, Intrusion detection systemsor IDS do exactly as the name suggests: they detect possible intrusions. The goal of IDS software tools is to detect computer attacks or illegitimate access, and to alert the IT Administrator about the detection or security breach. An IDS installed on a Network can be viewed as a burglar alarm system installed in a house. Through their methods are different, both detect when an intruder/attacker/burglar is present, and others subsequently issue some type of warning signal or alert [1]. Monitor, detect, and respond to any unauthorized activity are the adages of Intrusion detection systems. Network attacks such as DoS attacks can be detected by monitoring the Network traffic. There are two basic types of IDS:Host based and Networkbased. Each has a distinct approach to monitoring and securing data, and each has distinct Benefits and Drawbacks. Host-based intrusion detection systems (HOST IDS) are IDSs that operate on a single workstation. HOST IDSmonitortraffic on its Host machine by utilizing the resources of its Host to detect attacks. [2] Networkintrusion detection systems (Network IDS) are IDSs that operate as stand-alone devices on a Network. Network IDS 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 local network traffic [2]. Table 1 shows the difference betweenHost IDS and Network IDS giving the Benefits and Drawbacks of each. Host IDS and Network IDS can be combined to form separate hybrid class of NetworkIDS where agents are deployed on every Host within the Network being protected. A Network IDS operates much like a hybrid per-hostNetwork IDS since a single agent usually processes the network traffic directed to the host it runs upon. The basic reason for having this type of Hybrid IDS was the need to work online with encrypted networks and their data destined to the single host since end points only can see decrypted network traffic).

The paper is organized as below. Section II emphasizes on the Network attack classification techniques. Section III covers network intrusion detection methodologies, and Section IV concludes the comparison of various Open Source and commercial IDPS tools.

II. NETWORKSECURITY: NETWORK ATTACKS CLASSIFICATION

A high level network security can be considered by defining two components, security and networks. According to dictionary, security is the freedom fromdanger or anxiety, no sense of threat. A computer Network as we know is a group of interconnected computers. Security is described through the accomplishment of basic security properties, namely Data confidentiality, Authentication, Access control, Data Integrity and Non-repudiation [3]. Security threats can be classified into external or internal threats. Threats originating outside anenterprise or an institution are external and in contrast an internal threat is one originating inside the organization. There are two types of internal threats: Intended attacks and unintended attacks.

Network based IDS	Host based IDS
Resides on the computer/application connected to a parton an organization's Network and monitors Network traffic onthat segment looking forindication of ongoing or successful attacks.	Resides on a particular host machineor server, known as the Host, andmonitors activity only on thatsystem looking for anymalicious programs running.
• Types of Network IDS include SNORT,Cisco Network IDS, Suricata and Bro etc. • Network IDS uses a monitoring port, when placed next to Networking device like hub, switch. The port views all the traffic passing through the device. • Works on the principle of signature matching, i.e. comparing attack patterns to known signatures in their database. • NetworkIDS 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.	• Types of Host IDS, includeTripwire, Cisco Host IDS, OSSEC HIDS andSymantec ESM • Capable of monitoring systemconfiguration data bases, such aswindows registries, and storedconfiguration files like .ini, .cfgand .dat files. • Work on the principle ofconfiguration and changemanagement. An alert is triggered when file attributeschange, new files created or existing files deleted. • Host IDS havecommon architectures, meaningthat most Host systems work asHost agents reporting to a centralmanagement console.
Benefits: • Large networks can be monitored by deploying a few devices with a good Network design. • Ongoing network operations won't be interrupted by deploying Network IDS, since they runsin passive mode. • NetworkIDSs are not susceptible to direct attack and may not be detectable by attackers.	**Benefits:** • Attacks local events can be detected byHost IDS. • Host IDS functions on the Hostsystem, where encrypted trafficwill be decrypted and availablefor processing. • The use of switched Networkdoes not affect a Host IDS. • Host IDS can detectinconsistencies in theapplication.
Drawbacks: • Network IDS may fail to recognize attack when Network volume becomes over-whelming. • Since many switches have limited or no monitoring port capability, some Networks are not capable of providing all the data for analysis by a Network IDS. • Network IDS cannot analyze encrypted packets, making some of thetraffic invisible to the process and reducing the effectivenessofNetwork IDS. • Attacks involving fragmented or malformed packets cannoteasily be detected.	**Drawbacks**: • More management effortsrequired to install configure andmanage Host IDS. • Both direct attacks and attacksagainst the Host operating systemresults in compromise and/orloss in functionality of Host IDS. • Host IDS is susceptible to someDoS related attacks. • Target Host OS level audit logs occupy largeamounts of disk space and diskcapacity needs to be added,which may reduce systemperformance. • Host IDS cannot scan /detectmulti-Host and non-Hostnetworkdevices

Table 1: Difference between Host based and Network based IDS

Intended attacks are malicious attacks carried out by disgruntled employees for various reasons such as, financial payment, or to cause harm to the organization. Unintended attacks such as, deleting important data files cause unwarranted performance and financial damage to the organization. In this section we discuss some of the basic Network attacks. Security threats and attacks may involve any OSIlayers, from physical to application layer.

A. Denial-of-Service (DOS) attacks

It is an attempt to prevent the authorized users from utilizing the requested service/ resource running as part of business infrastructure operation. A more advanced Distributed Denial of Service occurs when in a distributed environment the attacker sends or rather floods the hostmachine or a Destination system with numerous connection requests knocking the Destination system to the knees, leaving them no other option to restart their system. Some well known DOS attacks are:
1) **SYN Attack** where the attacker exploits the incapability of the server to handle unfinished connection requests. Server is flooded with connection requests. The server crashes waiting for the acknowledgmentsof the requests.

2) **Ping of Death** where the attacker sends a ping request which is larger than 65,536 bytes size which is the maximum allowed size for the IP, causing the Destination system to crash or restart.

There are numerous DOS attacks are happened in the past. 14 major websites including web sites of presidential Blue House, the defense ministry, New York Stock Exchange, the National Assembly, Shinhan Bank, the mass-circulation newspaper Chosen and the top Internet portal Naver.com came under DDoS attack originated from a small cable TV website in Seoul overloading and knocking them down.[8] Another most heard was he Google’s Self-Inflicted Denial-of-Service Attack. A Google employee, working on updating their malwarenotification service uploaded a simple little "/" as a malware site a few months ago (January 31, 2009), effectively declaring the entire Internet to be malware for nearly 55 minutes. Google lost a lot of money in ad revenue during those 55 minutes. In addition, Google suffered reputational losses. Google's self-conflicted denial-of-service attack is a stark reminder to all IT security professionals about what is the greatest threat and risk to operational security.

B. Eavesdropping or MITM (Man-In-The-Middle) attacks

This external type of attack where there is an unauthorized interception of network communication and disclosure of exchanged information. This can be performed in different layers – for example, in Network layer by sniffing into the exchanged packets or in physical layer by physically wiretapping the access medium.

C. Spoofing attack

The attacker mimicsa legitimate user. IP spoofing is a common example where the system is convinced that it is communicating with a trusted target machine/host and provides access to the attacker. The attacker sends a packet with an IP address of a known Host by alerting the packet at the transport layer.

D. Intrusion attacks or User to Root Attack (U2R)

An unauthorized user tries to gain access to system or boot through the Network option. Buffer overflow attack is a typical intrusion attack which occurs when a web service receives more data than it has been programmed to handle leading to data loss.

E. Logon Abuse attacks

A successful logon abuse attack would bypass the authentication and access control mechanisms and grant a user with more privileges that authorized.

F. Application layer Attacks

The attacker exploits the weakness in the application layer – for example, security weakness in the web server, or in faulty controls in the filtering of an input on the server side. Examples include malicious software attack (viruses, Trojans, etc.), web server attacks, and SQL injection.

III. INTRUSION DETECTION METHODOLOGIES

Basically, there are two techniques in IDS: Anomaly based and Signature/Misuse based intrusion detection. Amiable, one of the main factors that holdis considered while buying IDS which is whether to go for an Anomaly based or signature based detection technique. IDS vendors should be aware of the pros and cons of these techniques. We also explain the Destination Monitoring and Stealth Probe techniques later in this section.

A. Anomaly based intrusion detection

First off, anomalies also known as outliers, exceptions or peculiarities are patterns in data that don’t conform to a well-defined notion of normal conduct of a system [4]. The Figure 1 show’sabnormalities O1, O2 and O3 that differ from the normal conduct N1 and N2. A simple example showing anomalies Anomaly detection technique is designed to uncover the patterns of behavior that are from normal and abnormal which anything is that widely deviates from it gets flagged as a possible intrusion. Anomaly detection can be categorized into static and dynamic [5].

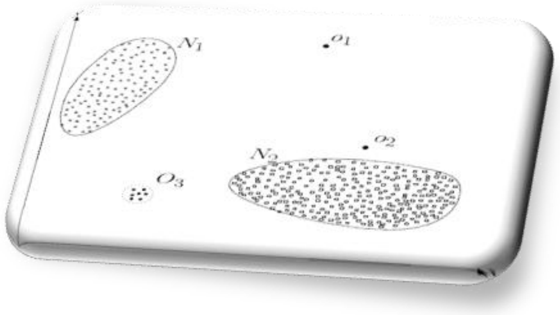


Figure 1: Anomaly detection technique -Sample Example

***In Static Anomaly Identifier*(SAI) -**It is assumed that a part of the monitored target machine remains constant or static. The static portion of a system is composed of two parts: the system code and that portion of system data that remains constant. Static portions of the system can be represented as a binary bit string or a set of such strings (such as files). If this portion ever deviates from its original form, either an error has occurred or an intruder has altered the static portion of the target machine. Static anomaly identifiers are said to check for data or file integrity.

In Dynamic Anomaly Identifier (DAI) -the definition of conduct is included. System conduct is defined as a sequence (or partially ordered sequence) of distinct events. For example, audit records produced by the operating system are used by Network IDS to define the events of interest. In this case, the conduct can be observed only when audit records recreated by OS. Events may occur in a strict sequence. More frequently, such as with distributed systems, partial ordering of events is more suitable. The system may rely on parameters that are set during initialization to reflect system conduct if it is uncertain whether conduct is anomalous or not. Initial conduct is assumed to be normal. It is measured and then used to set parameters that describe correct r nominal conduct. There is typically an unclear boundary between normal and anomalous conduct depicted in Figure 2. If uncertain conduct is not considered anomalous, then intrusion activity may not be detected. If uncertain conduct is considered anomalous, then system administrators may be alerted by false alarms/ when there is no intrusion [5].

The most common way to draw this border condition is with statistical distributions having a mean and standarddeviation. Once the distribution has been established, a condition can be drawn using some number of standard deviations. If an observation lies at a point outside of the (parameterized) number of standard deviations, it is reported as a possible intrusion. A dynamic anomaly identifier defines an “actor”, as the potential intruder. An actor is frequently defined o be a specific user, with an account. Alternatively, user or system processes are monitored. The mapping between processes, accounts, and users is only determined when an alert is to be raised. In most operatingsystems there is clear traceability from any process to the user/account for which it is acting. Likewise, an operating system maintains a mapping between a process and the physical devices in use by that process. Anomaly based intrusion detection is useful for detecting attacks like:

1) Misuse of Protocol and Service Ports

Features of the standard protocols or packet structure can sometimes be misrepresented or modified by an attacker in order tobypass through a firewall. Installation of backdoor services on well-known standard ports is another common misuse of service ports.

2)*DoS attacks on Crafted Payloads*

For many platforms different firewalls are present like for Linux IPTable firewall is in-built firewall present which has to be configured by writing customized rules. It is rule-based Intrusion Prevention System. Same way for windows Net defender, WIPFW (windows firewall) which is based on BSD firewall ipfw. By writing ipfw rules the Networkor the system can be sheltered. There are two types of IDS one is NetworkIDS and other is Host based IDS. Network Intrusion tries to identify the malicious activity by monitoring the incoming and outgoing Network traffic. The following figure 3 shows the methods to detect the types of DoS attacks. To detect the attacks or anomalous traffic on the network first step is to execute packet sniffing. There are two types of mode present to capture the packet one is normal in that the packets intended tothe system are only captured by the system and other is Promiscuous mode in which every packet which is going through the interface is captured by the system. It will be useful to monitor the network traffic the system has to be operated in promiscuous mode.In every Network IDS the overall architecture contains the following basic logical interfaced components.

1. *Packet Sniffer unit:* this unit captures the packet from the interface either in promiscuous mode or in normal mode. Promiscuous mode is explained above.
2. *Intrusion Detection or Preprocessing engine:* in this unit it uses the different methodologies to detect the attack depending on flow based analysis or protocol based analysis.
3. *Countermeasures:* in this the packets which contains the malicious code or if any abnormal flow of packets is observed the particular action is selected to avoid the intruder to enter in to the Network [10].

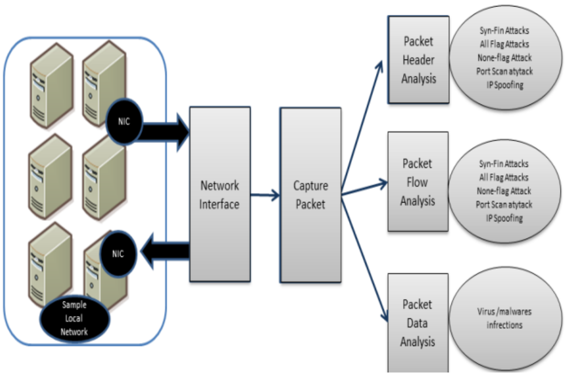


Figure2:Classification of DoS attacks

When a malicious intruder creates an attack using a constructed IP packet, the resulting Denial of Service DoS) can occur on the Network bandwidth, CPU cycles, memory resources, or application process/programs. Examples of this type of DoS include process table exhaustion, IP stack colliding, or a web application .soft spot. The impact of this DoS attack would be an anomaly in service quality.

3) DoS attack is based on Volume (DDoS)

Anomaly based intrusion detection is the only reliable means for detectionin the case of the DoS attack that floods the Network with a large volume of traffic. This is because sophisticated attack traffic may not be distinguishable from regular traffic on a per packet basis and the attack does not apparent a specific signature that can be captured by signature-based mechanisms. For example, the following traffic pattern anomalies can be observed as a result of the Distributed Denial of Service (DDoS): TCP control packet statistics for TCP SYN flood or relative volumes of TCP, UDP, and ICMP traffic for UDP or ICMP flood.

4) Buffer Overflow

The buffer overflow is the most common vulnerability exploited by attackers. Buffer overflow with hellcode execution is the most serious form of this exploit because a successful attack can result in arbitrary program execution on the victim system(s). Many exploited fields, such as user passwords for TP, are supposedly made of printable ASCII characters based on the standard Request For Comments (RFCs) by the Internet Engineering Task Force (IETF). Excessive non-printable ASCII characters are anomalies of strong suspicion. Furthermore, shellcode embedded in these fields are sure signs of malicious intent.

5) Other Natural Network Failures

Failures in routers/switches can result in changes in traffic pattern observed at certain points of the Network. This can be in the form of sudden drop in the volume of traffic due to broken connections, or in the form of traffic shift from one link to another due to traffic rerouting as a recovery action. All these changes are noteworthy and can be detected as traffic anomalies. Anomaly Detection Techniques represents a broad spectrum of detection techniques. One can define profiles in terms of simple thresholds or more complex statistical distributions; and profiles can be self-learned or manually set, adaptive, or static [11]. Three broad types of anomaly based detection techniques are discussed in the following paragraphs.

1. *Protocol Anomaly Detection* - As mentioned earlier protocol anomaly refers to all exceptions related to protocol format and conductwith respect to common practice on the Internet and standard specifications. This includes network and transport layer protocol anomalies in layers 3-4 and application layer protocol anomalies in layers 6-7. Unusual conditions are checked for in the process of IP defragmentation, TCP reassembly. When the IDS areinline, many exceptions leading to ambiguous interpretation by the end Host can be averted. When an IDS is monitoring application protocol conduct, it must be able to perform deep application protocol parsing, which is also known as decoding. The following anomalies are examples of protocol level anomalies that could be identified when application protocolsconduct is being observed:
   - Illegitimate field values and combinations
   - Illegitimate command usage

- Unusually long or short field lengths, which can designate an attacker is attempting to introduce a buffer overflow
- Uncommon number of occurrences of particular fields/commands
- Running a protocol or service for a non-standard purpose or on a non-standard port

2. *Application Payload Anomaly -Application* anomaly must be supported by detailed analysis of application protocols to define accurate conduct constraints for them. Application anomaly also requires understanding of the application semantics in order to be effective. One needs to know what type of encoding is legal for a given field, and hat other applications can be embedded within it. One good example of application level anomaly is the presence of shellcode in unexpected fields. A reliable anomaly profile allows shellcode execution attacks to be detected without knowing what particular exploit code is involved, or even the existence of exploit code.

3. *Statistical Anomaly Based Intrusion Detection-* A normal TCP network traffic follows a well-defined three-way handshake process for connection setup, data transfer phase, and then completes with the connection tear down. There is a stable balance among different types of TCP packets in the absence of attacks which is compared against short-term observations that will be affected by attack events. Statistical anomaly based IDS captures this conductand differentiates between the long term and short term observations in a given protected environment to avoid generating false alarms on normal traffic variations. Traffic profiles based on statistical measures could arise DDoS anomalies based on rare events of the difference between the long and short-term distributions or based on a rare occurrence of long bursts of high-rate traffic. A well-designed system couldallow the user to set a sensitivity level to reflect how tolerant their Network or servers are to traffic surge. he lowers the sensitivity level; the more severe the traffic profile deviation must be before the algorithm raises a DDoS alarm. The normal profiles are continuously learned while the system is in detection mode, with safeguard against statistics poisoning under attacks. This allows the anomaly profiles to adapt to typical environmental changes that occur in an organization [6]. For example, some of the events that are detected include: SYN Flood attacks, UDP Flood attacks, ICMP Flood attacks, TCP data segment flood attacks.

Benefits:

i. IDSs detect unusual conduct and thus have the ability to detect symptoms of attacks without specific knowledge of details.
ii. Anomaly identifiers can produce information that can in turn be used to define signatures for misuse identifiers.

Drawbacks:

i. Anomaly detection methodologies usually produce a large number of false alarms due to the unpredictablebehaviors of users and Networks.

ii. Anomaly detection methodologies often require extensive “training sets” of system event records in order to characterize normal conduct patterns.

B. Misuse/Signature based Intrusion Detection

The second major category of IDS is misuse detection also referred to as signature-based detection because alarms are generated based on specific attack signatures. These attack signatures encompass specific traffic or activity that is based on known intrusive activity. The following are the two techniques in misuse detection:
1) Expression Matching -The simplest form of misuse detection is expression matching, which searches in event stream (log entries, Network traffic, or the like) for occurrences of specific patterns/signatures. A simple example would be "^GET[^$]*/etc./passed$" - this checks for something that looks like an HTTP request for the Unix password file. Signatures can be very simple to construct, however especially when combined with protocol-aware field decomposition.

2) State Transition Analysis – this model attacks as a Network of states and transitions matching events. Every observed event is applied to finite state machine instances (each representing an attack scenario), possibly causing transitions. Any machine that reaches its final (acceptance) state indicates an attack as depicted in Figure 2 This approach allows complex intrusion scenarios to be modelled in a simple way, and is capable of detecting slow or distributed attacks, but may have difficulty expressing elaborate scenarios.

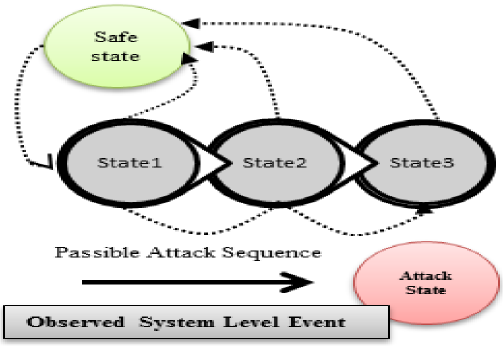


Figure 3: Schematic Structure of a State Machine

Benefits:

i. Misuse identifiers are very effective at detecting attacks without generating an overwhelming number offalse alarms.
ii. Misuse identifiers can 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.

Drawbacks:

i. Misuse identifiers can only detect those attacks they know about therefore they must be constantly updated with signatures of new attacks.
ii. These are designed to use tightly defined signatures that prevent them from detecting variants of common attacks. State-based misuse identifiers can overcome this limitation, but are not commonly used in commercial IDSs.

C. Destination Host Monitoring

Any change modifications in the Destination objects are reported by the Destination Monitoring Systems. This is usually done through cryptographic algorithm that computes a cryptochechsum for each Destination file [12]. changes such as file modification or program logon which would cause changes in the cryptochecksum reported by the IDS. This type of system is the easiest to implement, because it does not require constant monitoring by the administrator. Integrity checksum can be computed at whatever intervals you wish, and n either all files or just the mission/system critical files. Tripwire software will perform Destination monitoring sing cryptochecksum by providing instant notification of changes to configuration files and enabling automatic restoration.

D. Stealth Probes

Stealth probes collects and correlate data to try to detect attacks made over long period of time, often referred to as “low and slow” attacks [12]. Attackers, for example, will check for system vulnerabilities and pen ports over a two-month period, and wait another two months to actually launch the attacks. They ake a wide-area sampling and attempt to discover any correlating attacks.

IV. MODERN NETWORK INTRUSION DETECTION AND PREVENTION SYSTEMS

A. Open Source Network Intrusion Detection and Prevention system

There are wide array of intrusion detection products available today (freely available of commercial) addresses range of organizational security goals and considerations. We have provided a list of most common Network IDS tools [9] describing their features. Below table2gives the high level comparisons of Open Source Network IDS tools which are commonly used in the intrusion detection activity.

B. Commercial Network Intrusion Detection and Prevention system

Nowadays network security threat landscape is changing constantly , attackers are refining their attack strategies and increasing both the volume and intelligence of their attacks. Enterprises now must defend against Targeted Persistent Attacks (TPA). In the past years, servers were the main Destination for attacker, however attacks against desktop client applications are now typical and present a clear danger to organization. Exploits are analyzed based on yearly consistency, by attack vector, impact type such system exposure , service exposure and system or service fault , block rate by top vendor such Oracle ,Microsoft, Adobe, IBM, Apple etc.

Implementation of an network intrusion prevention system (IDPS) can be a complex process with multiple factors affecting the overall security effectiveness of the solution. These should be considered over the course of the useful life of the solution, and include:

Network IDS Name ---	**Snort**	**Suricata**	**Bro-NIDS**
Feature Support	**Features Decryption**		
Signature/ Anomaly Based IDS	**Signature Based**	**Signature Based**	**Signature + Statistical Anomaly**
Protocol Inspection Support	Yes	Yes - (Packet Logged with TLS/SSL,HTTP/DNS Request)	Yes , Analysis Engine +Policy Script Integration
Deployment Ease	Yes	No	No
Customized Deployment	No	No	Yes
High Performance Network Support	No	Yes	Yes
Administrative GUI Console	Yes	Few options	No
Analysis GUI Console	Snorby,BASE,Squil	Few options	No Options
OS Support	UNIX/Linux	Windows/Unix/Linux	Windows
Post Analysis Automation Support	No	No	Yes
Multithreading Support	No	Yes	No
Community Support	Yes , Extensively	Moderate	Moderate ,Now growing user base
IPv6 Support	No	No	Yes
License Distribution Support -Free	GPL License	GPL License	BSD License (More Free)
IP Reputation Support	No	No	Yes
GeoIP Support	No	No	Yes , with IPv4 and ASN lookups
Hardware Acceleration	No	Yes (Built-in GPU)	No
Rating Based Feature Supported	1	2	3
Feature Roadmap	Progressive	Progressive	Strongly Aggressive

Table 1: Network IDPS Comparison Feature Sheet

i. Attack Exploit block rate
ii. Anti-evasion capabilities (resistance to common evasion techniques)
iii. Device stability and reliability capability
iv. Overall manageability and Central Control

In order to determine the relative security effectiveness of devices on the market and facilitate accurate product comparisons, NSS LAB Labs has developed a unique metrics :

Formula for Security Effectiveness Measurement for Network IDS
Security Effectiveness=Exploits Block Rate X Anti-Evasion Rating X Stability & Reliability

By focusing on overall security effectiveness instead of the exploit block rate alone, NSS LAB is able to factor in the ease with which defenses can be bypassed, as well as the reliability of the device because enterprise users consider effective management to be a critical component of any enterprise security deployment, this also should be factored into total cost of ownership (TCO)and overall product selection. This is outside the scope of this report, however. For more information, refer to the TCO and Management CARs. For a complete view of Security Effectiveness mapped against Value, refer to the Security Value Map (SVMCAR.NSS Lab research indicates that the majority of enterprises tune their IDPS. Therefore, for NSS Lab testing of Network IDPS products, the devices are deployed with a tuned policy. Every effort is made to deploy policies that ensure the optimal combination of security effectiveness and performance, as would be the aim of a typical customer deploying device in a live network environment. This provides reference with the most useful information on key IDPS security effectiveness and performance capabilities based upon their expected usage. Evasion techniques area means of disguising and modifying attacks in order to avoid detection and blocking by security products. Resistance to evasion is a critical component in an IDPS.

If a single evasion is missed, an attacker can utilize an entire class of exploits to circumvent the IDPS, rendering it virtually useless. Many of the techniques used in this test have been widely known for years and should be considered minimum requirements for the Network IDPS product category, while others are more recent. This particular category of tests is critical in the final weighting with regard to product guidance. This chart depicts the relationship between protection and performance when tuned policies are used. Farther up indicates better security effectiveness, and farther to the right indicates higher throughput When selecting products, those along the top line of the chart (closer to 100% security effectiveness) should be prioritized. The throughput is a secondary consideration and will be dependent on enterprise-¬-specific deployment requirement.

Exploit Block Rate : Security effectiveness testing requires the deep expertise of attack engineering to generate the same types of attacks used by modern cyber criminals, utilizing multiple commercial, open source, and proprietary tools as appropriate. With over 1800 live exploits , NSS LAB's is the industry's most comprehensive test to date. Most notable,all of the live exploits and payloads in these test have been validated such that a:

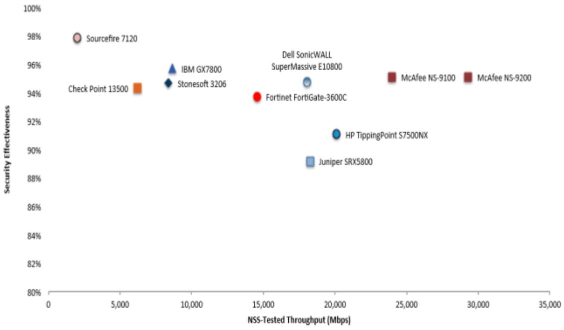


Figure 4: IDPS Tool Throughput Vs Security Effectiveness

- A reverse shell is returned
- A bind shell is opened on the Destination allowing the attacker to execute arbitrary commands
- A malicious payload is installed
- The system is rendered unresponsive.

This approach is no longer viewed as acceptable and, despite the difficulty of providing extensive coverage for client-side attacks, the IDPS industry has attempted to provide more complete client-side coverage. NSS LAB utilizes the following definitions:

- **Attacker-Initiated**: The threat/exploit is executed by the attacker remotely against a vulnerable application and/or operating system. These attacks traditionally Destination servers(which is why they are often referred to as server-side attacks).
- **Destination-Initiated**: The threat/exploit is initiated by the vulnerable Destination(which is why they are often referred to as client-side attacks). The attacker has little or control as to when the Destination user or application will execute the threat. These attack traditionally Destination desktop client applications.

Evasions: Evasion techniques are a means of disguising and modifying attacks at the point of delivery in order to avoid detection and blocking by securityproducts. Failure of a security device to handle correctly a particular type of evasion potentially will allow an attacker to use an entire class of exploits for which the device is assumed to have protection. This renders the device virtually useless. Many of the techniques used in this test have been widely known for years and should be considered minimum requirements for the IDPS product category. Providing exploit protection results without fully factoring in evasion can be misleading. The more classes of evasion that are missed—IP fragmentation TCP segmentation, RPC fragmentation, URL obfuscation, TCP split handshake and FTP evasion—the less effective the device.

For example, it is better to miss all techniques in one evasion category (say, TP evasion) than one technique in each category, which would result in a broader attack surface. Furthermore, evasions operating at the lower layers of the network stack (IP fragmentation or TCP segmentation) will have a greater impact on security effectiveness than those operating at the upper layers (HTTP or FTP obfuscation.) This is because lower-level evasions will impact potentially a wider number of exploits; therefore, missing TCP segmentation is a such more serious issue than missing FTP obfuscation. A product's effectiveness is significantly handicapped if it fails to detect exploits that employ obfuscation or evasion techniques, and the NSS LAB product guidance is adjusted to reflect this. As with exploits, evasions can be employed specifically to obfuscate attacks that are initiated either locally by the Destination (client-side), or remotely by the attacker against a server (server-side). Some evasions are equally effective when used with both server-side and client-side attacks.

Stability & Reliability : Long-term stability is particularly important for an in-line device, where failure can produce network outages. These tests verify the stability of the device under test along with its ability to maintain security effectiveness while under normal load and while passing malicious traffic. Products that are not able to sustain legitimate traffic (or that crash) while under hostile attack will not pass. The device under test is required to remain operational and stable throughout these tests, and to block 100% of previously blocked traffic, raising an alert for each attack. If any prohibited traffic passes successfully, caused by either the volume of traffic or the device under test failing open for any reason, this will result in a FAIL.

Security Effectiveness: The tools security effectiveness is determined by factoring the results of evasions testing and stability& reliability testing into the exploit block rate. Figure 5 depicts the security effectiveness of each device.

Network IDPS Tool Name	**Exploit Block Rate**	**Anti-Evasion Rating**	**Stability and Reliability**	**Security Effectiveness**
Check Point 13500	94%	100%	100%	94.4%
Dell SonicWALL SuperMassive E10800	95%	100%	100%	94.8%
Fortinet FortiGate 3600C,	94%	100%	100%	93.8%
HP TippingPoint S7500NX	91%	100%	100%	91.1%
IBM GX7800	96%	100%	100%	95.7%
Juniper SRX5800	89%	100%	100%	89.2%
McAfee NS9100	95%	100%	100%	95.1%
McAfee NS9200	95%	100%	100%	95.1%
Sourcefire 7120	98%	100%	100%	97.9%
Stonesoft 3206	95%	100%	100%	94.7%

Table 2: Network IDPS Tool Performance Comparison Sheet

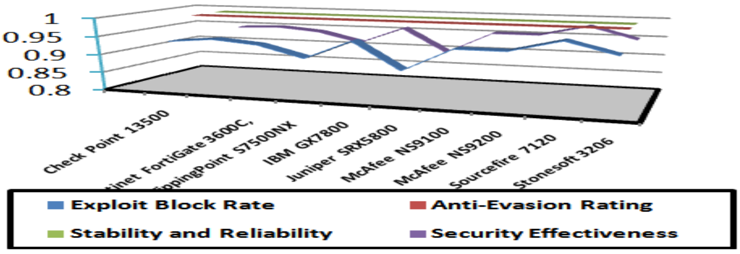


Figure5: Network IDPS Tool Capability Performance Representation

Managed Security Effectiveness

Security devices are complicated to deploy including essential systems such as centralized management console options, log aggregation, and event correlation/management systems further complicate the procurement decision. If a device cannot be managed effectively, the security effectiveness of that device is compromised. As part of this performance evaluation testing exercise, NSS Labs performed in-depth technical evaluations of the main features and capabilities of the enterprise IDPS systems offered by each vendor, covering the following key areas [14]:

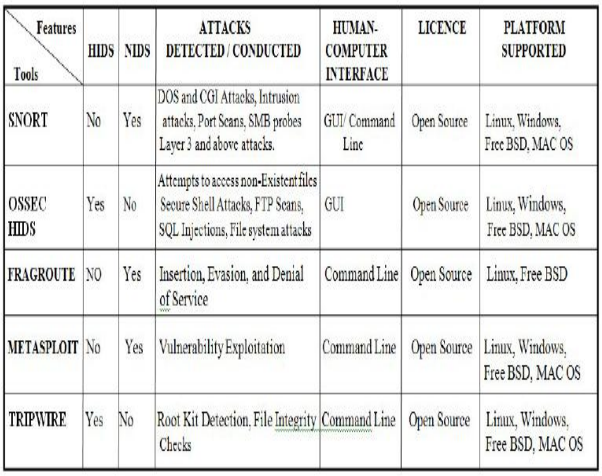
•**General Management and Configuration** –how easy is it to install and configure devices, and deploy multiple devices throughout a large enterprise network?

•**Policy Handling** –how easy is it to create, edit, and deploy complicated security policies across an enterprise?

•**Alert Handling** –how accurate and timely is the alerting, and how easy is it to drill down to locate critical information needed to remediate a security problem?

•**Reporting** –how effective is the reporting capability, and how readily can it be customized?

The results of these tests are reported, along with detailed cost models, in the Management CAR and Total Cost of Ownership(TCO) CAR.



Features / Tools	HIDS	NIDS	ATTACKS DETECTED / CONDUCTED	HUMAN-COMPUTER INTERFACE	LICENCE	PLATFORM SUPPORTED
SNORT	No	Yes	DOS and CGI Attacks, Intrusion attacks, Port Scans, SMB probes Layer 3 and above attacks.	GUI/ Command Line	Open Source	Linux, Windows, Free BSD, MAC OS
OSSEC HIDS	Yes	No	Attempts to access non-Existent files Secure Shell Attacks, FTP Scans, SQL Injections, File system attacks	GUI	Open Source	Linux, Windows, Free BSD, MAC OS
FRAGROUTE	NO	Yes	Insertion, Evasion, and Denial of Service	Command Line	Open Source	Linux, Free BSD
METASPLOIT	No	Yes	Vulnerability Exploitation	Command Line	Open Source	Linux, Windows, Free BSD, MAC OS
TRIPWIRE	Yes	No	Root Kit Detection, File Integrity Checks	Command Line	Open Source	Linux, Windows, Free BSD, MAC OS

Table 3: Open Source Host and Network IDS Tools

SNORT Network IDS - 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 P address.

OSSEC – HOST IDS – It is scalable, multi-platform, open source Host-based Intrusion Detection system (HOST IDS). 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.

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 our own exploits easier, and it certainly beats scouring the darkest corners of the Internet for illicit shell ode of dubious quality.

TRIPWIRE – It Detects Improper Change, including Safe Possible Attack ObservedEvent Attack additions to, deletions from and modifications of file systems and identifies the source. It Simplifies and eases Management of Change Monitoring Policies.

V. CONCLUSION

Various security attacks and their classification pertaining to TCP/IP protocol stack, and existingintrusion detection techniques used for intrusion detection are visited for better understanding of the intrusion detection and protection systems.

Network intrusion detection methodologies such as anomaly and signature based network intrusion detection and prevention system along with their benefits are analyzed for efficiency and effectiveness.

Finally paper concludes with comparison and evaluation of an open source and commercial IDPS tools and techniques which are used to detect and prevent the security attacks.Holistically cooperation with not only Network IDPS but also other network security components are mandatory forachieving a robust network security for better future of the organizations.

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] Christos Douligeris and Dimitrios N. Serpanos “Network Security Current Status and Future Trends”

[4] Varun Chandola, Arindam Banerjee, and Vipin Kumar“Anomaly Detection: A Survey” August 15, 2007

[5] Anita K. Jones and Robert S. Sielken, Department of Computer Science University of Virginia “Computer System Intrusion Detection: A Survey”

[6] Dr. Fengmin Gong, Chief Scientist, McAfee Network Security Technologies Group, “Deciphering Detection Techniques: Part II Anomaly-Based Intrusion Detection” March 2003

[7] Carl Endorf, Eugene Schultz, Jim Mellander “Intrusion detection & prevention” page 18

[8] Deccan Herald, “Cyber-attacks cripple websites”,http://www.deccanherald.com/content/12577/cyber-attacks-cripple-websites.html

[9] “ Top 5 Intrusion Detection Systems”, http://sectools.org/ids.html.

[10] Dr. B.B.Meshram,Suchita Patil ," Network Intrusion Detection and Prevention techniques for DoS attack ",International Journal of Scientific and Research Publications ,Volume 2, Issue 7, July 2012 ISSN 2250-3153.

[11] E. Earl Eiland, Scott C. Evans, T. Stephen Markham, Bruce Barnett, “Network Intrusion Detection: Using MDLCOMPRESS for Deep Packet Inspection”, 978-1-4244-2677-5/08/$25.00 ©20081EEE.

[12] Karen Scarfone Peter Mell ,“Guide to Intrusion Detection and Prevention Systems (IDPS)”, National Institute of Standards and Technology Special Publication 800-94 Natl. Inst. Stand. Technol. Spec. Publ. 800-94, 127 pages (February 2007).

[13] Mihui Kim, Inshil Doh and Kijoon Chae , “Defense Mechanism using Overlay against DDoS Attacks on Converged Networks”, Feb. 2-14, 2007 ICACT2007.

[14] Shikha Goel , Sudesh Kumar , “An Improved Method of Detecting Spoofed Attack in Wireless LAN”, 2009 First International Conference on Networks & Communications 2009 IEEE.

[15] Tao Xia, Guangzhi Qu, Salim Hariri , Mazin Yousif , “An Efficient Network Intrusion Detection Method Based on Information Theory and Genetic Algorithm”, 0-7803-8991-3l051-2005 IEEE.

[16] Hui Li, Dihua Liu, “Research on Intelligent Intrusion Prevention System Based on Snort”, 2010 International Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE).

[17] Thomas Skybakmoen,Jason Pappalex, “Network Intrusion Prevention System Comparative Analysis –Security”, NSS Labs 2013.