

Intrusion Detection & Intrusion Prevention Systems

IDS & IPS

Nirmalan Nagenthiran , Ramitha Jayasekara , Sudeera Jayasekara

October 2010

CONTENTS

Keywords.....	iv
Abstract.....	iv
Introduction	1
IDS/IPS Architecture.....	2
Basic assumptions	2
Components of an IDS/IPS	2
Attack Detection Methods.....	3
Signature detection (or Misuse Detection).....	3
Anomaly detection.....	3
Target Monitoring.....	4
Stealth Probes	4
Denial of Service (DoS) Detection	4
Technologies used for attack detection.....	5
State-less IDS / IPS	5
State-full IDS / IPS	5
Deep Packet Inspection.....	5
Differentiation between IDS and IPS	6
Host-based intrusion detection and prevention systems (HIDS / HIPS).....	7
File System Monitors	7
Log file analyzers.....	8
Connection analysis	9
Kernel based IDSs.....	10
Network-based intrusion detection and prevention systems (NIDS / NIPS)	11
Architecture of Network based IDS/IPS	12
Troubleshooting IDS.....	13
False Positives and False Negatives	13
False Positives or False Alarms.....	13
False Negatives	13
The Future of Intrusion Detection and Prevention.....	15
Unified Threat Management	15
UTM Features.....	15
Types of UTM	16
Benefits of UTM	16

Shortcomings of UTM	17
Appendix	i
Wireless Intrusion Detection	i
WIDS Functionality.....	i
Attacks Fundamentals.....	ii
Planning phase	ii
Reconnaissance phase	ii
Attack phase.....	ii
Post-attack phase.....	ii
Types of Attacks	iii
Denial of service (DoS)	iii
Remote exploits	iii
Trojans and Backdoor programs.....	iii
Misuse of Legitimate Access	iii
References	a

Keywords

IDS, IPS, Intrusion, Host based IDS, Network based IDS, Wireless IDS, Components of IDS, Signature Detection, Anomaly Detection, Misuse Detection , Stealth Probes, Target Monitoring, Denial of Service Monitoring, Stateless IDS ,State full IDS , Deep Packet Inspection, Attack Fundamentals.

Abstract

In modern interlinked computer based systems security is of utmost importance. The safeguarding of security is becoming increasingly difficult, because the possible technologies of attack are becoming ever more sophisticated; at the same time, less technical ability is required for the novice attacker, because proven past methods are easily accessed through the Web.

Majority of security violations in systems occur due to malicious users or malicious code being able to penetrate through a system' s security barriers, and affect the system either by changing the system behaviour, extracting the system's information or both. Such malicious actions are identified as intrusions.

Intrusion detection (ID) is a type of security management system for computers and networks.

Aim: The aim of this document is to provide insight into Intrusion detection and prevention concepts and technologies, discussing their advantages and disadvantages.

Introduction

Intrusions are “Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource (System)” [1]

An intrusion detection system collects and analyzes various data within a computer or a network to identify possible security violations, which includes both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

The concept of intrusion detection has been around for nearly twenty years, but the popularity and usage of such systems increased exponentially in the recent years.

One of the first published documents which relates to intrusion detection was published by James Anderson in 1980. The document introduced the notion that audit trails contained vital information that could be valuable in tracking misuse and understanding user behaviour. The first model for intrusion detection, the Intrusion Detection Expert System (IDES) was developed in 1985[2].

The market share of intrusion detection systems increased after 1997, and several companies which mainly focused on developing intrusion detection systems were born. The technological advancements have since continued and major developments have been achieved.

Security protocols implemented to identify intrusions can be broadly categorized into,

- Intrusion detection systems (IDS) which are hardware and/or software mechanisms that detect and logs inappropriate, incorrect, or anomalous activity and report it for further investigation [3].
- Intrusion Prevention Systems (IPS) contains IDS functionality but more sophisticated systems which are capable of taking immediate action in order to prevent or reduce the malicious behaviour [4].

Some functionality of intrusion detection systems are [5],

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Analysis of abnormal activity patterns
- Tracking user policy violations

IDS/IPS Architecture

Basic assumptions

IDS/IPS systems rely on two fundamental assumptions which are vital for their functionality. They are [7],

- System activities are observable
- Normal and intrusive activities have distinct evidence – the goal of an IDS/IPS is to detect the difference.

Components of an IDS/IPS

IDS/IPS systems typically consist of the following components [7],

- **Data pre-processor**- Collects and formats the data to be analyzed by the detection algorithm.
- **Detection algorithm**- Based on the detection model detects the difference between “normal” and intrusive audit records.
- **Alert filter**-Based on the decision criteria and the detected intrusive activities, estimates their severity and alerts the operator/manages responsive activities (usually blocking for IPS).

Figure 1 shows how these components interact with each other in IDS [7]

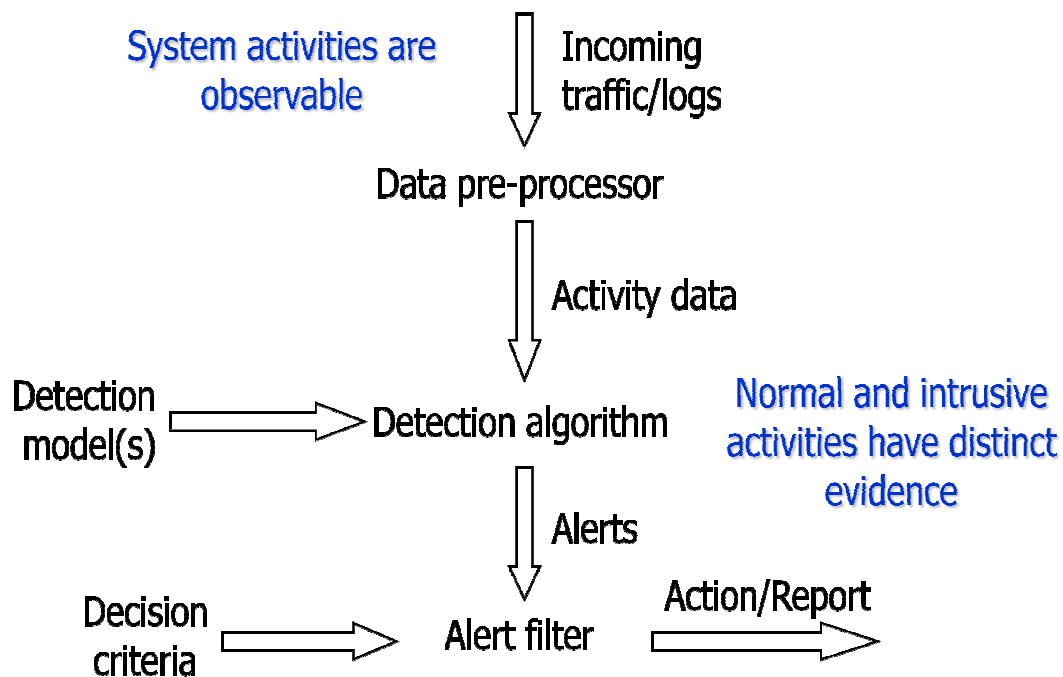


Figure 1 : Components of an IDS/IPS

Attack Detection Methods

Attack detection can be performed using different methodologies. The following are some generic vulnerability assessment methodologies,

Signature detection (or Misuse Detection)

Signature detection involves matching intrusive behaviour of malicious users/code or searching network traffic for a series of bytes or packet sequences known to be malicious.

A key advantage of this detection method is that signatures are easy to develop and understand. Signature detection relies on pattern matching which can be performed very quickly on modern systems so the amount of power needed to perform these checks is minimal for a confined rule set.

Signature engines also have their disadvantages. While signatures work well against attacks with a fixed behavioural pattern, they do not work well against the multitude of attack patterns created by a human or a worm with self-modifying behavioural characteristics. Because they only detect known attacks, a signature must be created for every attack, and novel attacks cannot be detected.

Since a new signature must be created for each new intrusion, and as the rule set grows, the engine performance inevitably slows down. This is the very reason that most intrusion-detection appliances reside hardware that runs from two to as many as eight processors with multiple Gigabit network cards.

Detection is further complicated by advancing exploit technology that permits malicious users to conceal their attacks behind payload encoders and encrypted data channels.

Signature engines are also prone to false positives since they are commonly based on regular expressions and string matching. [10]

Anomaly detection

Anomaly detection operates by building a model of “normal” system behaviour. Normal system behaviour is determined by observing the standard operation of the system or network. Anomaly detection then takes the normal observation model and uses statistical variance, or data mining techniques with artificial intelligence, to determine if the system or network environment behaviour is running normally or abnormally.

The assumption in anomaly detection is that an intrusion can be detected by observing a deviation from the normal or expected behaviour of the system or network [11].

A drawback of anomaly detection is that malicious activity that falls within normal usage patterns is not detected. An activity such as directory traversal on a targeted vulnerable server, which complies with network protocol, easily goes unnoticed since it does not trigger any out-of-protocol, payload or bandwidth limitation flags.

However, anomaly detection has an advantage over signature-based engines in that a new attack for which a signature does not exist can be detected if it falls out of the normal traffic patterns. [10]

Target Monitoring

These systems do not actively search for anomalies or signatures, but instead look for the modification of specified files. This is more of a corrective control, designed to uncover an unauthorized action after it occurs in order to reverse it. One way to check for the hidden editing of files is by computing a cryptographic hash beforehand and comparing this to new hashes of the file at regular intervals. This type of system is the easiest to implement, because it does not require constant monitoring by the administrator. Integrity checksum hashes can be computed at whatever intervals you wish, and on either all files or just the mission/system critical files [8].

Stealth Probes

This technique attempts to detect any attackers that choose to carry out their mission over prolonged periods of time. Attackers, for example, will check for system vulnerabilities and open ports over a two-month period, and wait another two months to actually launch the attacks. Stealth probes collect a wide-variety of data throughout the system, checking for any methodical attacks over a long period of time. They take a wide-area sampling and attempt to discover any correlating attacks. In effect, this method combines anomaly detection and misuse detection in an attempt to uncover suspicious activity [8].

Denial of Service (DoS) Detection

DoS detection compares current traffic behaviour with acceptable normal behaviour to detect DoS attacks, where normal traffic is characterized by a set of pre-programmed thresholds. This can lead to false alarms or attacks being missed because the attack traffic is below the configured threshold [17].



Figure 2 : Different types of attacks & detection methods

Technologies used for attack detection

The following is a list of key technologies used for attack detection, which provides a stream of data that is then analyzed by the above mentioned methods,

State-less IDS / IPS

Most of the IPS currently available are stateless. They typically utilize a network adapter configured in promiscuous mode to monitor and analyze all traffic in real-time as it travels across the network. The traffic is analyzed on a packet-by-packet basis. Each packet is compared against a database of known patterns for a match. The disadvantage of such an approach is that, it fails to detect some attack patterns which are spread across a number of packets, each of which when examined individually may be harmless [15].

State-full IDS / IPS

A State-full IDS can be defined as a packet filtering and analysis mechanism which makes decision on whether the security of a network is breached by analyzing information contained in the current packet AND information from previous packets. In addition to detecting those attacks, which a stateless IDS can detect, this system can also detect those attacks, which are launched from more than one host, and those attacks in which more than one packet is used in the attack [15].

Deep Packet Inspection

Deep Packet Inspection is a term used to describe the capabilities of a Intrusion Detection System to look within the application payload of a packet or traffic stream and make decisions on the significance of that data, based on the content of that data. The engine that drives deep packet inspection typically includes a combination of signature-matching technology along with anomaly analysis in order to determine the impact of that communication stream [14]. Figure 3 illustrates the message and the accumulation of headers for deep packet inspection.

Analysis of packet headers can be done economically since the locations of packet header fields are restricted by protocol standards. However, the payload contents are, for the most part, unconstrained. Therefore, searching through the payload for multiple string patterns within the data stream is a computationally expensive task. The requirement that these searches be performed at wire speed adds to the cost. Additionally, because the signature database is dynamic, it must be easily updateable.

Promising approaches to these problems include a software-based approach (Snort implementing the Boyer-Moore algorithm), and a hardware-based approach (FPGA's running a Bloom filter algorithm).

DPI technology can be effective against buffer overflow attacks, denial of service (DoS) attacks, sophisticated intrusions, and a small percentage of worms that fit within a single packet. However, the complexity and immaturity of these systems have resulted in a number of recent exploits [16].

Differentiation between IDS and IPS

An Intrusion Detection System (IDS) device is passive, watching packets of data traverse the network from a monitoring port, comparing the traffic to configured rules, and setting off an alarm if it detects anything suspicious.

An Intrusion Prevention System (IPS) has all the features of a good IDS, but can also stop malicious traffic from invading the enterprise. Unlike IDS, an IPS sits in line with traffic flows on a network, actively shutting down attempted attacks as they're sent over the wire. It can stop the attack by terminating the network connection or user session originating the attack, by blocking access to the target from the user account, IP address, or other attribute associated with that attacker, or by blocking all access to the targeted host, service, or application.

In addition, an IPS can respond to a detected threat in two other ways. It can reconfigure other security controls, such as a firewall or router, to block an attack. Some IPS devices can even apply patches if the host has particular vulnerabilities. In addition, some IPS can remove the malicious contents of an attack to mitigate the packets, perhaps deleting an infected attachment from an email before forwarding the email to the user.

Intrusion detection systems are typically of two types, which are, Host-based intrusion detection systems / intrusion prevention (HIDS / HIPS) and Network-based intrusion detection systems / intrusion prevention (NIDS / NIPS).

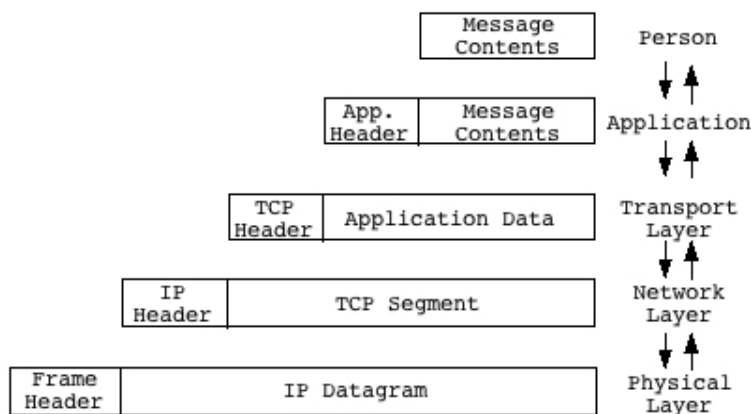


Figure 3: The Message and the Accumulation of Headers for Deep Packet Inspection

Host-based intrusion detection and prevention systems (HIDS / HIPS)

Host-based IDS are generally considered as passive components but in some cases they also include intrusion prevention methodologies. Pieter et al. recognizes four different methods of host-based intrusion detection, [6]

- File system monitors - Systems checking the integrity of files and directories.
- Log file analyzers - Systems analyzing log files for patterns indicating suspicious activity.
- Connection analyzers - Systems that monitor connection attempts to and from a host.
- Kernel based IDSs - Systems that detect malicious activity on a kernel level.

Implementations of intrusion detection systems generally use one of these four methods to detect intrusions.

File System Monitors

File system monitor HIDS help detect a break-in on a system after it has occurred. Such monitors can check files on a large number of different characteristics. The list below shows some types of variability assessment performed by this type of HIDS, which can be generally categorized into Signature detection and Target monitoring.

- **Permissions** - Changes in the permissions of a file or directory are detected.
- **Owner/group** - If the owner or group of a file or directory is changed this is detected.
- **Size** - If a file grows or shrinks in size this is reported.
- **Directory size** - Adding or deleting of files in a directory is detected.
- **Mtime, atime & ctime** - Both file system monitors check for changes in the mtime (last modification time), atime (last access time), and ctime (last time the owner, permissions, etc. where changed) of a file or directory.
- **Checksums** - The integrity of a file or directory can be checked using a cryptographic hash. This type of checking is based on the fact that it is very difficult (to near impossible) to change a file's contents without affecting the unique hash of the file. The most commonly used algorithms are md5 (the de-facto standard), and SHA-1 (NIST standard).
- **Type** - If, for example, a file is replaced with a directory or device of the same name this is detected.

File system monitor HIDS has number of disadvantages. Because file systems tend to be very dynamic in nature it is hard to create a configuration that catches all intrusions, while not producing many false positives.

Something minor as installing a new application can create a huge number of alarms on IDS of this type. Another disadvantage is that this type of IDS generally doesn't work real-time. It is therefore possible for an attacker to cover up his tracks before being detected [6].

Log file analyzers

Log files can be analyzed in order to determine if any intrusions have taken place. Log file analyzers are tools that perform,

- **Pattern matching** - Applying (extended) regular expressions to log files based on prior knowledge.
- **Pattern matching with correlation between events** – Considering a large number of events and pinpointing the few events that are really important as well as on timing information.

Since data in textual form is matched in pattern matching log file analyzers, attackers can use all kinds of encoding techniques to avoid matching the rules defined.

Pattern matching log file analyzer is useful when for matching strings in a more static context. However, maintenance increases if used to detect new exploits as they are released.

- **Anomaly detection** - After learning how the normal loglines should look like, anomaly detection systems can detect anomalous loglines and report about them. The above problem of encoding does not occur with Anomaly detection based log file analyzers, since they do not depend on prior knowledge.

The problem with log file analyzers is that they depend on events being logged on log files. If an attacker manages to prevent logging of malicious activities, then log file analyzers will not be successful [6].

Connection analysis

Connection analysis HIDS implementations detect incoming network connections only to the host they run on. Connection analysers do not perform monitoring of connections to other hosts, which is the key feature of Network based intrusion detection systems.

Connection analysers typically scan for following violations,

- **Unauthorized TCP and UDP connections** - Detect unauthorized connections on both TCP and UDP ports
- **Port scan detection** – Detect scanning of open ports on a host, by a malicious user or automated tool.

Apart from the passive detection behaviours, some Connection analyzers are also capable taking evasive action against above listed intrusions which characterizes Intrusion prevention systems behaviour (IPS).

Some other prevention measures implemented with Connection analyzers are,

- **Host blocking** - allows for active blocking of an offending host
- **Banner display** - display an informational banner to the offender, instead of blocking them

Connection analyzers have their fair share of weak points also. They are typically poor at detecting attacks which use,

- **Unsupported protocols**
- **Large pool of attacker IP's**
- **Attacker slowly scans the ports**

But these weak points depend on the connection analyzer implementation which can be fixed but complicates the analyzer implementation [6].

Kernel based IDSs

Kernel based IDS is an addition to or adaption of a kernel to have the kernel itself detects intrusions. Such IDS are capable of detecting,

- Anomaly detection based on a user's system usage.
- Logging possibly maliciously used system calls.
- Anomaly detection on the order of system calls in processes.
- Anomaly detection on the arguments of system calls in processes.
- Logging changes made to system binaries.
- Logging port scans or probes
- File and directory protection, preventing alterations even by root.
- Hiding of files and directories.
- Setting capabilities on a per process basis
- Protect processes, blocking signals from possibly unauthorized users.
- Blocking network related tampering, like changing firewall settings.
- Preventing kernel module loading or unloading.
- Preventing raw disk I/O

Detecting excessive calls from the stack or the data segment of processes will enable the IDS to detect most exploits for today's software.

Installing a new application, or update an already running one, the kernel based IDS would required to be disabled partially or totally. During that session the administrator can perform administrative duties, like installing applications or configuring kernel based IDS itself. After updating or installing an application, kernel based IDS may need to reload the configuration file to protect any newly installed files [6].

Network-based intrusion detection and prevention systems (NIDS / NIPS)

Network-based intrusion detection analyzes data packets that travel over the actual network. These packets are examined to verify their nature. This surveillance of the connections between computers makes network-based IDS great at detecting access attempts from outside the trusted network [8].

By far the most common security measure for network security is a firewall. Though they both relate to network security, NIDS / NIPS differs from a firewall in that a firewall looks outwardly for intrusions in order to stop them from happening. A NIDS also watches for attacks that originate from inside the network [9].

Network-based intrusion detection systems (NIDS) tend to be more distributed than host-based IDS. Software, or appliance hardware in some cases, resides in one or more systems connected to a network, and are used to analyze data such as network packets.

In general, network-based systems are best at detecting the following activities:

- **Unauthorized outsider access:** When an unauthorized user logs in successfully, or attempts to log in, they are best tracked with host-based IDS. However, detecting the unauthorized user before their log on attempt is best accomplished with network-based IDS.
- **Bandwidth theft/denial of service:** These attacks from outside the network single out network resources for abuse or overload. The packets that initiate/carry these attacks can be noticed with use of network-based IDS.

Network based systems rely on deploying sensors at strategic locations and inspecting network traffic for possible violations.

For NIDS/NIPS sensor placement, the target network should be analyzed and choke points identified.

A choke point would be any point in a network where traffic is limited to a small number of connections. An example is usually a company's Internet boundary, where traffic crosses only a router and a firewall. The links between the router and firewall are perfect choke points and good places to consider placing sensors. In the case of VPN networks, care must be taken to inspect the unencrypted side of the VPN tunnel [13].

Adhering to the generic vulnerability criteria identified above, network based system generally have the following detection methodologies [12],

- Pattern, expression or bytecode matching (Signature matching)
- Frequency or threshold crossing (Anomaly and Stealth probe detection)
- Correlation of lesser events (Stealth probe detection)
- Statistical anomaly detection

Architecture of Network based IDS/IPS

The following diagram depicts the architecture of Network based IDS

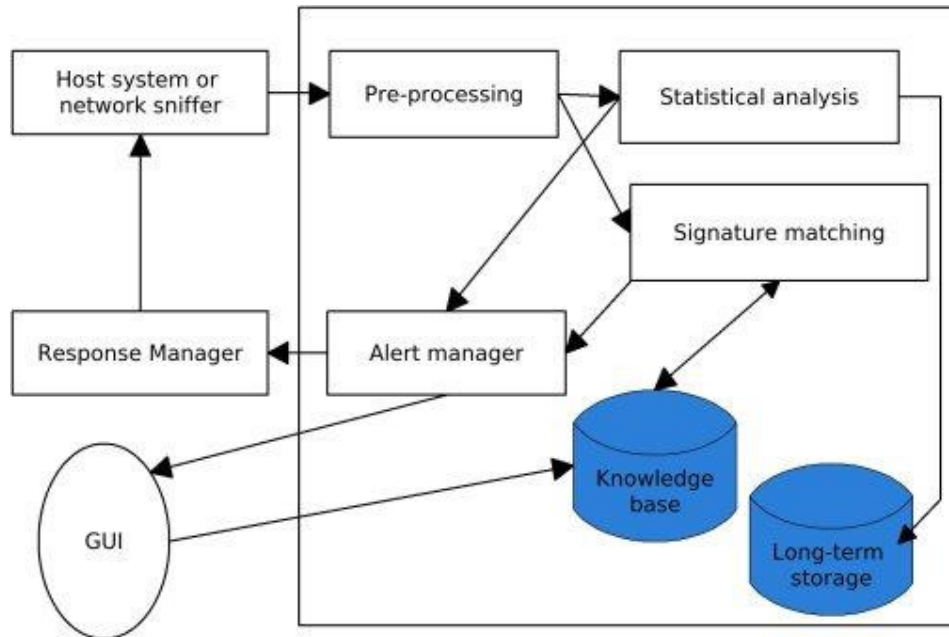


Figure 4 : Architecture of Network IDS

To guarantee a precise detection the NIDS must detect packets at a wire speed. However, with the recent trend of high-speed networks, the capability of a single NIDS cannot meet the speed's demand [18].

Currently Software based NIDS /NIPS systems are roughly capable of achieving 60 Mbps throughput. But a hardware based solution such as the McAfee IntruShield IPS appliances can achieve a rate of 2 Gbps at most [19].

Furthermore to promote the NIDS performance and efficiency, present studies on IDSs for high-speed network monitoring have begun to choose the distributed architecture as an alternative. In such a design, the incoming network traffic is disseminated to a pool of sensors, which process a fraction of the whole traffic, reducing the possibility of packet loss caused by overload [18].

Troubleshooting IDS

False Positives and False Negatives

False Positives or False Alarms

The term false positive is a broad and somewhat vague term that describes a situation in which an IDS device trigger an alarm in a when there is malicious activity or attack occurring. Other common terms used to describe this condition are "false alarms" and "benign trigger". False alarms can be subdivided into several more meaningful and specific categories. Common categories into which false alarms can be divided include [24]:

- **Reactionary Traffic alarms:** Traffic that is caused by another network event, often non malicious. An example of this would be a NIDS device triggering an ICMP flood alarm when it is really several destination unreachable packets caused by equipment failure somewhere in the Internet cloud.
- **Equipment-related alarms:** Attack alerts that are triggered by odd, unrecognized packets generated by certain network equipment. Load balancers often trigger these types of alarms.
- **Protocol Violations:** Alerts that are caused by unrecognized network traffic often caused by poorly or oddly written client software.
- **True False Positives:** Alarms that are generated by an IDS for no apparent reason. These are often caused by IDS software bugs
- **Non Malicious alarms:** Generated through some real occurrence that is non malicious in nature, possibly like our Code Red web page example above.

Depending on network traffic and the IDS design that is deployed, a normal IDS sensor without any customization may have only 10% of its alarms associated with a true security event. The remaining 90% of noise is not an acceptable percentage. While it may be debatable what can be considered an acceptable percentage of false alarms, with correct tuning (depending on the technology in use) an average real alarm rate of 60% or better is possible under normal conditions. I have seen real alarm rates above 90%, depending on the level of tuning and the type of traffic on a network.

False Negatives

False negative is the term used to describe a network intrusion device's inability to detect true security events under certain circumstances. In other words, malicious activity is not detected and alerted. Fortunately, there are actions that can be taken to reduce the chance of false negative conditions without increasing the number of false positives.

Some causes for false negatives are [24],

- **Network design issues:** Network design flaws such as improper port spanning on switches and traffic exceeding the ability of a switch or hub contribute to these problems. Other problems include multiple entry point networks where the NIDS device cannot see all incoming and outgoing traffic.
- **Encrypted traffic design flaws:** These problems arise because the IDS is unable to understand encrypted traffic. Placing the NIDS behind VPN termination points and use of SSL accelerators are good ways to ensure the NIDS is understands all traffic.
- **Lack of change control:** Many times false negative conditions are created by a lack of communication between IS departments, networking, and security staff. Most of the time this is in the form of network or server changes that are not properly communicated to security staff. As a result, security is not able to implement measures to mitigate the risk associated with changes in security posture.
- **Improperly written signatures:** Although the attack is known and the signature is developed, the signature does not properly catch the attack or mutations of the attack because it has not been written properly.
- **Unpublicized attack:** The attack is not publicly known, therefore vendors have no knowledge and no signature is developed.

- **Poor NIDS device management:** For a variety of reasons, the NIDS device may not be properly configured. Contributing factors include:
 - Exclusionary rules to reduce false alarms that are too general;
 - The device is under too much load and cannot properly process all data;
 - Alarming is not configured properly; and,
 - The system administrator has a poor understanding of the vulnerabilities and threats associated with specific attacks.
- **NIDS design flaw:** The NIDS device simply does not catch the attack due to poor design or signature implementation.

The Future of Intrusion Detection and Prevention

The futuristic trend of IDS/IPS systems is converge IDS/IPS capabilities with other security solutions. The technology has unified with each other to form unified threat management.

Unified Threat Management

The ultimate goal of UTM is integration -- to provide a comprehensive set of security features in a single product that can be deployed in a single location and managed through a single console. The simplification and consolidation offered by a unified security product can potentially improve security because policies and rules can be developed centrally, often resulting in fewer rule errors that may lead to security oversights. A single security product also reduces security management demands, easing management labour [20].

UTM Features

UTM often incorporates the following features,

- Advanced firewalls with deep packet inspection
- Gateway antivirus and antispyware Antispam
- Intrusion detection/prevention functionalities

Some UTM platforms include additional features such as,

- Web content filtering to block inappropriate or malicious websites
- Virtual private network (VPN) support for secure remote access and secure wireless access for user mobility within the enterprise.

A limited number of UTM platforms add advanced features such as WAN acceleration, rate shaping or even inter-zone security to guard against threats originating within the local network itself. Ultimately, the actual feature set depends on the particular product, so solution providers are challenged to recommend UTM systems with appropriate feature sets. It's important to note that UTM features can be enabled independently allowing clients to start with certain features like antivirus, and then add other features like VPN functionality over time [20].

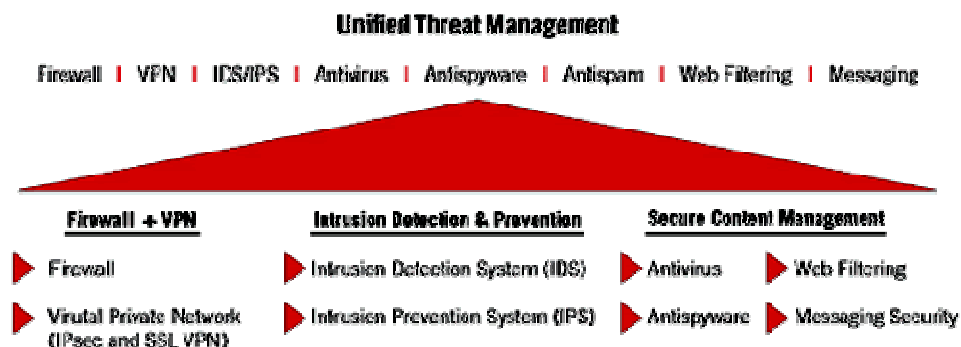


Figure 5 : Unified Threat Management Overview

Types of UTM

Hardware based UTM's: These appliances come with specialized ASIC chip-sets which are tailor made to handle the processing that is required to scan for multiple threats simultaneously. Apart from the hardware, they feature a network security operating system which is highly robust and integrates with all the individual components of the UTM. The individual components themselves are license based– the components could be selected and purchased individually.

Software based UTM's: The licensing is similar to the hardware based UTM's, but the network security operating system and the individual UTM components (like anti-spam, IPS etc) are hosted on standard computer servers with a certain minimum configuration based on the number of users and the applications that are run simultaneously.

Distributed UTM's: They do not comprise of a single appliance to combat the various network security threats, but multiple hardware boxes from the same vendor, each specialized in its own functionality (like separate boxes for IPS, Web-Filtering etc) but still having a common management interface which makes them virtually a single appliance that can be controlled on a single platform.

Benefits of UTM

Some of the benefits of UTM are [21, 22],

- The ability to obtain management leverage by combining multiple functions into a common interface there by providing simplicity in operations.
- The ability of a UTM device to consolidate all of the alerts and only notify the administrator once is time saving and cost effective.
- UTM avoids repetition of processes and hence saves time. Common processes (like scanning packets) are done once and used for all the applicable modules.
- Single management interface to create uniform policy across the enterprise and across the different modules.
- Multiple patches, multiple upgrades and hence multiple maintenance contracts for each security module can be avoided using UTM's

Shortcomings of UTM

Some of the disadvantages of UTM are [22],

- UTM introduces a single point of failure for all the network security elements, unless a high availability configuration is deployed.
- There is always a possibility of performance constraint as there are limitations in hardware processing capabilities to handle so many applications/users simultaneously.
- Some UTM devices may not have the granular features supported by stand alone technologies and hence those functionalities are either ignored or additional investments in terms of add-on's needs to be made.
- There is always challenge from cloud computing initiatives and UTM's might have to be deployed in a virtual manner (One UTM divided in to several logical units, each serving different locations etc.) in the future, which is not possible currently.

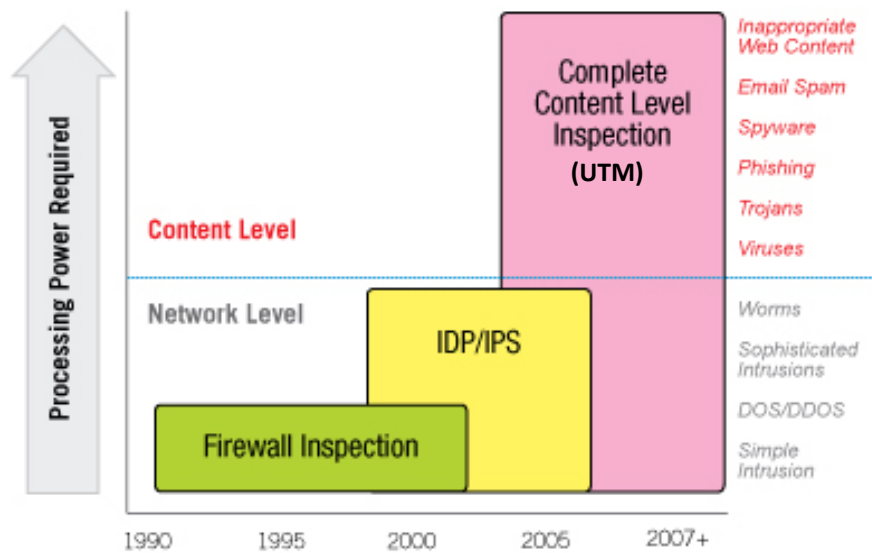


Figure 6 : Processing Power vs. Time

Appendix

Wireless Intrusion Detection

Like their wired counterparts, wireless intrusion detection systems (WIDS) are designed to monitor network traffic. Although product architectures vary, WIDS typically depend upon remote sensors, distributed throughout the monitored network. Sensors passively observe wireless activity, reporting back to a central IDS server. That server is responsible for analyzing reported activity, generating intrusion alarms and a history database. Results may be presented on the server itself, or remotely through some type of IDS client [25].

WIDS Functionality

- Prevention capabilities to temporarily or permanently inhibit a wireless attacker's ability to communicate with your WLAN or any adjacent wired network. Temporary wireless blocking can discourage an attacker, just as an alarm siren can scare away a burglar. Persistent blocking can give you time to find and eliminate a rogue, without continuing to jeopardize your network during investigation.
- Configurable device lists to differentiate between authorized ME (Mobile equipment), neighbour ME, and all others. But such lists require on-going maintenance. In densely-populated urban areas, investigating every new device is at best labour-intensive, at worst impossible. Many WLAN owners prefer to be alerted only when an unknown device has actually penetrated their network, and then take wired-side steps to neutralize that threat.
- Capable of inspecting IP payload to analyze traffic streams and behaviour over time to determine whether a station or AP is communicating with an upstream network. As in the wired world, payload encryption can make this task more difficult.
- Incorporate location detection to some degree. One method is to manually search around the sensor receiving the strongest signal from the transmitter. Another method is triangulation -- comparing the signal received by three or more sensors to better pinpoint a transmitter's probable location. A third method is RF fingerprinting -- modelling RF characteristics within a coverage area for comparison to received signal strength to predict the transmitter's location.

Some WIDS examples include AirDefense Enterprise, AirMagnet Enterprise, AirTight SpectraGuard, Bluesocket BlueSecure, Highwall Enterprise, Network Chemistry RFprotect, Newbury Networks WiFi Watchdog, Red-M Red-Detect, and VigilantMinds AirXone.

Attacks Fundamentals

There are four phases in attacks carried over systems they are,

Planning phase

The attacker often makes use of the system in its intended manner before making the attack. Public availability for legitimate access helps the attacker define the scope and goals of the attack. After the initial preparation is complete, the attacker decides on the scope of the attack. Example: the attacker may sign up for an account on an online e-commerce system or log onto a public server.

Reconnaissance phase

The attacker next gathers information or performs reconnaissance on the targeted network. The attacker carries out a variety of different inquiries with the goal of pinpointing a specific method of attack (port scanning etc.) The goal of the attacker in this phase is to narrow down the field of thousands of possible exploits to a small number of vulnerabilities that are specific to the targeted host/network. The attacker attempts to make this reconnaissance as hard to notice as possible. Even so, there are many different means of reconnaissance and some of them can be detected by an intrusion detection system.

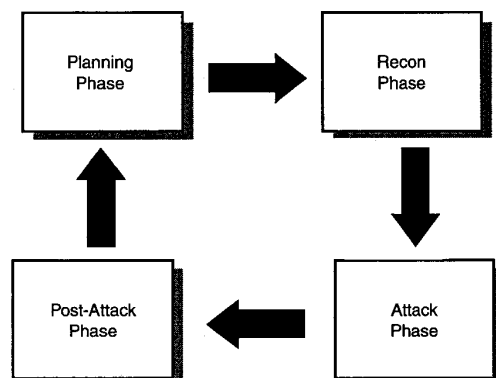
Attack phase

The intruder carries out the attack. The types of attacks will be discussed in the next section.

Post-attack phase

After an attacker has successfully penetrated into a host on the targeted network the attacker carries out his/her plan and makes use of information resources as he/she considers appropriate. Possible post-attack activities are,

- Covering tracks
- Penetrating deeper into network infrastructure
- Using the host to attack other networks
- Gathering, manipulating, or destroying data
- Handing over the host to a friend or a hacker group
- Walking or running away without doing anything



Types of Attacks

Denial of service (DoS)

DoS attack is any attack that disrupts the function of a system so that legitimate users can no longer access it. Can be specific to a service (e.g. FTP attack), or an entire machine. DoS attacks commonly utilize spoofed IP addresses because the attack is successful even if the response is misdirected. The attacker requires no response, and in cases like the Smurf attack, wants at all costs to avoid a response. This can make DoS attacks difficult to defend from, and even more difficult to detect.

- **Resource depletion DoS attack:** Functions by flooding a service with so much normal traffic that legitimate users cannot access the service. An attacker inundating a service with normal traffic can exhaust finite resources such as bandwidth, memory and processor cycles. Examples: SYN flood, Smurf, etc.
- **Malicious packet DoS attacks:** Function by sending abnormal traffic to a host to cause the service or the host itself to crash. Occur when software is not properly coded to handle abnormal or unusual traffic. Such traffic can cause software to react unexpectedly and crash. Attackers can use these attacks to bring down even IDS. Examples: Microsoft FTP DoS, SNORT ICMP DoS, etc.

Remote exploits

Attacks designed to take advantage of improperly coded software to compromise and take control of a vulnerable host and can function in the same manner as the malicious payload traffic DoS attacks. These attacks take advantage of improperly checked input or configuration errors. Examples: Buffer overflows, Unicode exploit, Cookie poisoning, SQL injection, etc.

Trojans and Backdoor programs

By installing a backdoor program or a Trojan, an attacker can bypass normal security controls and gain privileged unauthorized access to a host. A backdoor program can be deployed on a system in a variety of different ways. E.g. a malicious software engineer can add a backdoor program into legitimate software code. Backdoor programs might be added for legitimate maintenance reasons in the software development life cycle, but later forgotten. A Trojan is defined as software that is disguised as a benign application. Remote control Trojans typically listen on a port like a genuine application. Through this open port, an attacker controls them remotely. Trojans can be used to perform any number of functions on the host. Some Trojans include portscanning and DoS features. Others can take screen and Webcam captures and send them back to the attacker. Trojans and backdoor programs have traditionally listened on a TCP or UDP port, making it easy to detect them and undertake countermeasures. Because of that, Trojans have evolved so they no longer need to listen on a TCP or UDP port. Now instead, they listen for a specific sequence of events.

Misuse of Legitimate Access

Attackers often attempt to gain unauthorized use of legitimate accounts by getting authentication information. This can be performed by means of technical and/or social engineering methods. IDS, especially the anomaly detection ones, may be used to detect such activities.

References

- [1] C.N.S.S.L. Glossary - Texas State Library,
<http://www.tsl.state.tx.us/ld/pubs/compsecurity/glossary.html>
Accessed on: 29/09/2010
- [2] The Evolution of Intrusion Detection Systems | Symantec Connect,
<http://www.symantec.com/connect/articles/evolution-intrusion-detection-systems>
Accessed on: 29/09/2010
- [3] E-Banking - Appendix B: Glossary,
http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/ebanking_04_appx_b_glossary.html
Accessed on: 30/09/2010
- [4] Information Technology at Johns Hopkins-Glossary G-I,
<http://www.it.jhmi.edu/glossary/ghi.html>
Accessed on: 30/09/2010
- [5] What is intrusion detection? - Midmarket IT Security Definitions - Intrusion detection,
http://searchmidmarketsecurity.techtarget.com/sDefinition/0,,sid198_gci295031,00.html
Accessed on: 30/09/2010
- [6] Host-based Intrusion Detection Systems - Pieter de Boer & Martin Pels,
<http://staff.science.uva.nl/~delaat/snb-2004-2005/p19/report.pdf>
Accessed on: 02/10/2010
- [7] IDS/IPS Definition and Classification - Gjøvik University College,
http://www.hig.no/index.php/content/download/8588/118736/file/Topic_1.ppt
Accessed on: 02/10/2010
- [8] An Introduction to IDS - Paul Innella,
<http://www.symantec.com/connect/articles/introduction-ids>
Accessed on: 02/10/2010
- [9] What is Intrusion detection system(IDS) - Ax3soft Corporate,
<http://www.ids-sax2.com/articles/IntrusionDetectionSystem.htm>
Accessed on: 02/10/2010
- [10] IDS: Signature versus anomaly detection - James C. Foster,
http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1092691,00.html
Accessed on: 03/10/2010
- [11] Computer and Network IDS : Anomaly-Based - IDStutorial.com,
<http://idstutorial.com/anomaly-detection.php>
Accessed on: 03/10/2010
- [12] Network- vs. Host-based Intrusion Detection - Internet Security Systems,
http://documents.iss.net/whitepapers/nvh_ids.pdf
Accessed on: 03/10/2010

- [13] IDS and IPS placement for network protection - Robert Drum,
http://www.infosecwriters.com/text_resources/pdf/IDS_Placement_RDrum.pdf
Accessed on: 03/10/2010
- [14] Firewall Evolution - Deep Packet Inspection - Ido Dubrawsky,
<http://www.symantec.com/connect/articles/firewall-evolution-deep-packet-inspection>
Accessed on: 03/10/2010
- [15] Stateful Intrusion Detection System - Senthilkumar Krishnamurthy & Arunabha Sen,
www.public.asu.edu/~halla/papers/SIDS_ISC.ps
Accessed on: 03/10/2010
- [16] The Perils of Deep Packet Inspection - Dr. Thomas Porter,
<http://www.symantec.com/connect/articles/perils-deep-packet-inspection>
Accessed on: 10/10/2010
- [17] Next Generation Intrusion Detection Systems (IDS) - McAfee Network Protection Solutions,
http://www.mcafee.com/us/local_content/white_papers/wp_intruvertnextgenerationids.pdf
Accessed on: 10/10/2010
- [18] New Trend of Intrusion Detection System for High-speed Networks - Wei Wei
<http://www.apng.org/9thcamp/Papers/WeiWei.pdf>
Accessed on: 10/10/2010
- [19] Hardware Network Intrusion Detection - Chia-Tien Dan Lo
<http://www.cs.utsa.edu/~danlo/talk/2006/hNIDS.pdf>
Accessed on: 10/10/2010
- [20] Unified threat management: The next-generation network firewall - Stephen Bigelow
http://searchsecuritychannel.techtarget.com/generic/0,295582,sid97_gci1322686_tax311688,00.html
Accessed on: 12/10/2010
- [21] Managing the unified threat management device -- Is it really unified? - Mike Rothman
http://searchsecuritychannel.techtarget.com/tip/0,289483,sid97_gci1236510,00.html
Accessed on: 12/10/2010
- [22] An Introduction to Unified Threat Management in Network Security - excitingip.com
<http://www.excitingip.com/553/unified-threat-management-network-security/>
Accessed on: 12/10/2010
- [23] IDS vs. IPS Explained - focus.com
<http://www.focus.com/fyi/it-security/ids-vs-ips/>
Accessed on: 12/10/2010
- [24] Strategies to Reduce False Positives and False Negatives in NIDS - Kevin Timm
<http://www.symantec.com/connect/articles/strategies-reduce-false-positives-and-false-negatives-nids>
Accessed on: 12/10/2010
- [25] Beyond wireless intrusion detection - Lisa Phifer
http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci1035554_mem1,00.html?track=IDSLG
Accessed on: 12/10/2010