An Overview of Intrusion Detection System (IDS)

Presented by:

Monzur Morshed

TigerHATS

www.tigerhats.org
TigerHATS - Information is power

The International Research group dedicated to Theories, Simulation and Modeling, New Approaches, Applications, Experiences, Development, Evaluations, Education, Human, Cultural and Industrial Technology

Homepage: www.tigerhats.org
Twitter: www.twitter.com/tigerhats
An Overview of Intrusion Detection System

Presented by
Monzur Morshed
(TigerHATS)
Overview

- Intrusion Detection System
- Types of IDS
- IDS Mechanism
- Responsibility of IDS
- IDS Terminology
- Difference between Firewall & IDS
- Why Do I Need An IDS, I Have A Firewall?
- Several IDS diagram
- HIDS Vs. NIDS
- Passive Vs. Active IDS
- Challenges
- Top IDS
- Conclusion
What is Intrusion?

An intrusion is a deliberate unauthorized attempt, successful or not, to break into, access, manipulate, or misuse some valuable property and where the misuse may result into or render the property unreliable or unusable. The person who intrudes is an intruder.

Intrusion Detection:

Intrusion detection is a technique of detecting unauthorized access to a computer system or a computer network.
Intrusion Detection Defined

- Clear Definition:
  An Intrusion detection system pertains to the methods used to identify an attack on a computer or computer network.

- Formal Definition:
  “[Intrusion Detection] is the art of detecting inappropriate, incorrect, or anomalous activity.”

  -Dirk Lehmann, Siemens CERT
An intrusion detection system (IDS) is a system used to detect unauthorized intrusions into computer systems and networks. An IDS inspects all of the inbound and outbound network activity, and identifies suspicious patterns that indicate an attack that might compromise a system. Intrusion Detection Systems are usually configured to send an alert to a human being when they detect suspicious activity. Many types of alerts can be used, from entries in log files to e-mail or text messages sent by SMS.
Why Intrusion Detection?

- Computer Networks wage a constant struggle against intruders and attackers.
- Attacks on distributed systems grow stronger and more prevalent everyday.
- Intrusion detection methods are a key to controlling and potentially eradicating attacks on a system.
Types of IDS

There are two types of Intrusion Detection Systems:

- Host Based
- Network Based
Types of IDS

Host based IDS:
Intrusion Detection System is installed on a host in the network. HIDS collects and analyzes the traffic that is originated or is intended to that host.

Network based IDS:
Network IDSs (NIDS) are placed in key areas of network infrastructure and monitors the traffic as it flows to other host. Unlike HIDS, NIDS have the capability of monitoring the network and detecting the malicious activities intended for that network.
The following diagram shows a representation of a HIDS.

- The Orange machines represent where the HIDS is installed.
- In HIDS, the host or machine will be protected at all times.
In the NIDS diagram shows that an attempt has been made to channel the traffic through the NIDS machine or device on the network.

“If you had to isolate a single machine and take the machine away from the network when in transit that NIDS would be very flawed.” - Webopedia

The Red device represents where the NIDS has been installed.
Network Intrusion Detection System

Advantages:

- Can get information quickly without any reconfiguration of computers or need to redirect logging mechanisms
- Does not affect network or data sources
- Monitor and detects in real time networks attacks or misuses
- Does not create system overhead
Network Intrusion Detection System

Disadvantages:

- Can not scan Protocols if data is encrypted
- Can infer from network traffic what is happening on host but cannot tell the outcome
- Hard to implement on fully switched networks
- Has difficulties sustaining network with a very large bandwidth
Host-based Intrusion Detection System

Advantages:

- Specific and have more detailed signatures
- They can reduce false positive rates
- They can determine whether or not an alarm may impact that specific system
- They can be very application specific
- Operates in encrypted environments
Host-based Intrusion Detection System

Disadvantages:

- The IDS must have a process on every system you want to watch
- The IDS can have a high cost of ownership and maintenance
- The IDS uses local system resources
- The IDS, if logged locally, could be compromised or disabled
- Does not protect entire infrastructure
Intrusion Detection Mechanism

There are four (4) models of intrusion detection mechanism:

- Stack-based detection
- Signature-based detection
- Anomaly-based detection
- Hybrid-based detection
Intrusion Detection Mechanism

Stack based:

Stack based IDS is latest technology, which works by integrating closely with the TCP/IP stack, allowing packets to be watched as they traverse their way up the OSI layers.

Signature based/Pattern Matching based:

Signature-Based IDS use a rule set to identify intrusions by watching for patterns of events specific to known and documented attacks. It is typically connected to a large database which houses attack signatures. It compares the information it gathers against those attack signatures to detect a match. e.g., An e-mail with a subject of “Free Music!” and an attachment filename of “freemusic.exe”, which are characteristics of a known form of malware.
Intrusion Detection Mechanism

Anomaly based:

Anomaly-Based IDS examines ongoing traffic, activity, transactions and behavior in order to identify intrusions by detecting anomalies.

Hybrid based:

Hybrid-based intrusion detection is the combination of Stack, Signature, Anomaly-base Detection. Because of the difficulties with the anomaly-based and signature-based detections, a hybrid model is being developed. Much research is now focusing on this hybrid model.
Inside and Out

Intrusion Detection (ID) may be attempted in two ways:

1. Attacks from outside the computer environment or network.

2. “Misuse” that originates inside the network.
Responsibilities of IDS

- Prevent Intrusion with Firewall, Network Port Security, Systrace (process jail).
- Simulation software.
- Monitoring data, security logs or actions on the network
- Analyze to ascertain whether it is an attack.
- Detect the attack or intruder using some scheme.
- Report Intrusion to System Administrator
- Act on or defend computer system and possibly repel attack.

Note: Systrace is a computer security utility which limits an application's access to the system by enforcing access policies for system calls.
IDS Terminology

**Alert/Alarm** - A signal suggesting that a system has been or is being attacked.

**True Positive** - A legitimate attack which triggers an IDS to produce an alarm.

**False Positive** - An event signaling an IDS to produce an alarm when no attack has taken place.

**False Negative** - A failure of an IDS to detect an actual attack.

**True Negative** - When no attack has taken place and no alarm is raised.
IDS Terminology

**Noise** - Data or interference that can trigger a false positive

**Site policy** - Guidelines within an organization that control the rules and configurations of an IDS

**Site policy awareness** - The ability an IDS has to dynamically change its rules and configurations in response to changing environmental activity

**Confidence value** - A value an organization places on an IDS based on past performance and analysis to help determine its ability to effectively identify an attack
<table>
<thead>
<tr>
<th>Positive</th>
<th>True</th>
<th>False</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>An alarm was generated and a present condition should be alarmed</td>
<td>An alarm was generated and there is no condition present to warrant one</td>
</tr>
<tr>
<td>Negative</td>
<td>An alarm was <strong>NOT</strong> generated and there is no condition present to warrant one</td>
<td>An alarm was <strong>NOT</strong> generated and a present condition should be alarmed</td>
</tr>
</tbody>
</table>
Difference between Firewall & IDS

- **An intrusion detection system (IDS)** generally detects unwanted manipulations of computer systems, while a firewall is a dedicated application, or software running on another computer, which inspects network traffic passing through it, and denies or permits passage based on a set of rules.

- **Firewalls** are more simple and just block certain ports, stopping unauthorized access. On the other hand, **Intrusion Detection systems** are more complex and inspect packets to see what is actually inside them, if someone has actually gotten thru what did they do etc.

- **An IDS** may only detect and warn you of a violation of your privacy. Although most block major attacks, some probes or other attacks may just be noted and allowed through. A firewall will block almost all attacks unless specified otherwise or designed otherwise. The only problem is, the firewall might not warn you of the attacks and may just block them.

- It may be a good idea to have both an **IDS** and a **Firewall**, because the **IDS** will warn you and **Firewall** will block the attack.
What does a firewall do?

- **Firewall** is a program or hardware device that protects the resources of a private network from users of other networks.

- **Firewall** blocks open ports through which an intruder can gain access to your system and the valuable data you have stored in it.

- **Firewalls** limit access between networks to prevent intrusion and do not signal an attack from inside the network.

- As all information passes through firewall, user can know what is happening in the network.

- **Firewall** allows to create rules or set privileges for the type of traffic that can pass through the firewall in both directions.

- **Firewall** blocks malicious viruses from entering your system.
What does IDS do?

- An IDS monitors the activities of the system and alerts the user of any intrusion.

- An IDS evaluates a suspected intrusion once it has taken place and signals an alarm.

- An IDS adds integrity to the system and the infrastructure.

- An IDS helps the system administrator to set up policies.

- An IDS also watches for attacks that originate from within a system.
Components of IDS

- Audit Data
- Preprocessor
- Audit Records
- Activity Data
- Detection Engine
- Alarms
- Decision Table
- Decision Engine
- Action/Report

System activities are observable. Normal and intrusive activities have distinct evidence.
Where to locate IDS?

- Between network and Extranet
- In the DMZ (Demilitarized Zone) before the Firewall to identify the attacks on your servers in DMZ (e.g., Mail server, DNS, Web server)
- Between the firewall and network, to identify a threat in case of the firewall penetration
- In the Remote access environment
- If possible between servers and user community, to identify the attacks from the inside
- On the intranet, ftp, and database environment
Who needs to be involved?

- Information Security Officers
- Network Administrators
- Database Administrators
- Senior Management
- Operating System Administrators
- Data owners
Why Do I Need An IDS, I Have A Firewall?

- Not all traffic may go through a firewall. i.e., modem on a user computer

- Not all threats originates from outside. As networks uses more and more encryption, attackers will aim at the location where it is often stored unencrypted (Internal network) datas.

- Firewall does not protect appropriately against application level weaknesses and attacks.
IDS #1 – Firewall does not produce enough info to effectively detect hits.
IDS #2 – detects attacks that penetrate the FW
IDS #3 – detects attacks attempted against the FW
IDS #4 – Insider attacks will be detected
Host Based System (HIDS)

- Run on distinct hosts or devices within the network.
- Monitors the incoming and outgoing packets behavior, and reports any abnormal activity detected.
- System logs (syslog), the integrity of the file system integrity (fingerprinting), and process execution are examined, such as the TCPWrappers and the network stack.
- “In a host-based system, the [intrusion detection system] examines at the activity on each individual computer or host.” - Webopedia.com
Network-based system (NIDS)

- The individual packets flowing through a network are analyzed.
- NIDS can detect suspicious packets that are designed to be overlooked by a firewall’s “crude” filtering rules.
- The network traffic is examined for pattern matching among packets, and the flow of the network is also examined.
Passive vs. Active Intrusion Detection

- A **Passive IDS** is limited to intrusion detection.
- A Passive Intrusion Detection System may identify the suspicious traffic, and create a report that is sent to the system administrator.
- An **Active IDS** reacts upon detecting the intrusion, so that it may terminate the connection to the host in question.
- Active Intrusion detection systems may result in over-reaction of otherwise normal traffic and network activity.
Challenges

- Deployment & Myths
- Using IDS in fully switched networks
- Sustaining OC3 (Optical Carrier Transmission) speed or higher
- Interpreting all the data being presented
- Encryption, VPN, Tunnels
- Ongoing Support
- Performance
- Response team
Top Intrusion Detection Systems

- Snort
- Bro
- OSSEC HIDS
- Fragroute/Fragrouter
- BASE
- Sguil
An IDS is like a three year old kid, it’s not happy unless you are constantly watching it all the time.

Contrary to all other devices, an IDS talks back to you and demand immediate attention.

One of the most important point is how you are going to monitor your systems, what are you going to do when the alarm goes off at three in the morning?

There is about 400 different IDS on the market. Only a few of these products integrate well in large environment, are scalable, and easy to maintain.

Acquire the IDS that meets your need, not the one that the vendor think you need.
Thank you

TigerHATS

www.tigerhats.org