

# Access Control -- IDS

❖ *DigitalSherlock.com | SafeHack.com*

❖ *Date: 2005/05/27*

❖ *Document Name: access\_control\_ids.pdf*

❖ *GNU Free Documentation License*

❖ *Version 1.00, 2005-05-27*

❖ *Copyright © 2005 Adonis, MSc, Eng, CISSP, Security+, CEH, GSec, MCSE, etc.*

❖ *Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation.*

## ❖ Overview

- **IDS is a system that is used to monitor network traffic or monitor audit logs**
- **Intrusion detection is the process of monitoring the events occurring**
- **Software or hardware products that automate the monitoring and analysis process.**
- **Reasons to acquire and use IDSs**
  - **To prevent problem behaviors by increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse the system,**
  - **To detect attacks and other security violations that are not prevented by other security measures,**
  - **To detect and deal with the preambles to attacks (commonly experienced as network probes and other “doorknob rattling” activities),**
  - **To document the existing threat to an organization**
  - **To act as quality control for security design and administration, especially of large and complex enterprises**
  - **To provide useful information about intrusions that do take place, allowing improved diagnosis, recovery, and correction of causative factors.**

## ❖ Goals

- **Accountability**
  - **Accountability is the capability to link a given activity or event back to the party responsible for initiating it**
  - **Accountability is difficult in TCP/IP networks**
  - **TCP/IP Allow attackers to forge the identity of source addresses**
- **Response**
  - **Response is the capability to recognize a given activity or event as an attack and then taking action to block**

## ❖ Network-Based IDSs

- **Intro**
  - **It is Passive**
  - **Provide Real Time information**
  - **Consist of a set of single-purpose sensors or hosts placed at various points in a network**
- **Advantages**
  - **A few well-placed network-based IDSs can monitor a large network.**
  - **Deployment of network-based IDSs has little impact upon an existing network**
  - **Are usually passive devices that listen on a network wire without interfering with the normal operation of a network**

- Network-based IDSs can be made very secure against attack and even made invisible to many attackers

➤ **Disadvantages**

- May have difficulty processing all packets in a large or busy network
- May fail to recognize an attack launched during periods of high traffic

## ❖ **Host-Based IDSs**

➤ **Advantages**

- Can detect attacks that cannot be seen by network-based IDS
- Operate in an environment in which network traffic is encrypted
- Analyze activities with great reliability and precision
- Host-based IDSs are unaffected by switched networks
- Host-based IDSs operate on OS audit trails, they can help detect Trojan horse or other attacks that involve software integrity breaches
- Utilize information sources of two types, operating system audit trails, and system logs

➤ **Disadvantages**

- Host-based IDSs are harder to manage, as information must be configured and managed for every host monitored
- IDS may be attacked and disabled as part of the attack.
- Host-based IDSs are not well suited for detecting network scans
- Host-based IDSs can be disabled by certain denial-of-service attacks
- The amount of information can be immense, requiring additional local storage
- Limited by log capabilities

## ❖ **IDS Detection Methods**

➤ **Application-Based IDSs**

- **Intro**
  - Are a special subset of host-based IDSs that analyze the events transpiring within a software application
  - Detect suspicious behavior due to authorized users exceeding their authorization
- **Advantages**
  - Can monitor the interaction between user and application
  - Can often work in encrypted environments,
- **Disadvantages**
  - Vulnerable to attacks since the applications logs are not as well protected
  - Often monitor events at the user level of abstraction, they usually cannot detect Trojan horse or other such software tampering attacks
  - It is advisable to use an Application-based IDS in combination with Host-based and/or Network-based IDSs

➤ **A signature Based ID**

- Signatures or attributes of known attacks are referenced and compared against
- Use a patterns corresponding to known attacks are called signatures
- Signatures of an attack are stored and referenced
- Must have signature stored to identify
- **Advantages**
  - Very effective at detecting attacks without generating an overwhelming number of false alarms

- Can quickly and reliably diagnose the use of a specific attack tool or technique
- Can allow system managers, regardless of their level of security expertise, to track security problems on their systems
- Most common form of misuse detection used in commercial products
- **Disadvantages**
  - Can only detect those attacks they know about - therefore they must be constantly updated with signatures
  - Are designed to use tightly defined signatures that prevent them from detecting variants of common attacks
  - There are more sophisticated approaches to doing misuse detection (called “state-based” analysis techniques)

### ➤ **A statistical Anomaly Based ID**

- **An IDS acquires data and defines a "normal" usage profile for the systems**
- **Anomaly detectors identify abnormal unusual behavior (anomalies) on a host or network**
- **Profiles are constructed from historical data collected over a period of normal operation.**
- **This level can be static or heuristic**
- **Observed data defines acceptable usage patterns,**
- **IDS determines "normal" usage profile using statistical samples**
- **Detects anomaly from the normal profile**
- **In which certain attributes of user and system behavior are expressed in terms of counts, with some level established as permissible**
- **Parametric Where the distribution of the profiled attributes is assumed to fit a particular pattern**
- **Non-parametric Where the distribution of the profiled attributes is “learned” from a set of historical values, observed over time**
- **Advantages**
  - Detect unusual behavior and thus have the ability to detect symptoms of attacks without specific knowledge of details
  - Can produce information that can in turn be used to define signatures for misuse detectors
- **Disadvantages**
  - Usually produce a large number of false alarms
  - Often require extensive “training sets ” of system event records
  - Failure to recognize slow attacks

### ➤ **Type of Response**

- **Active Responses**
  - Collect additional information
    - ◆ The most innocuous, but at times most productive
  - The additional information collected can help resolve the detection of the attack.
- **Passive Responses**
  - Provide information to system users, relying on humans to take subsequent action based on that information
  - Many commercial IDSs rely solely on passive responses.
- **Change the Environment**
  - Halt an attack in progress and then block subsequent access by the attacker
  - Actions
    - ◆ Injecting TCP reset packets into the attacker’s connection to the victim system, thereby

- ♦ terminating the connection
- ♦ Re configuring routers and firewalls to block packets from the attacker's apparent location (IP address or site),
- ♦ Re configuring routers and firewalls to block the network ports, protocols, or services being used by an attacker, and
- ♦ In extreme situations, re configuring routers and firewalls to sever all connections that use certain network interfaces.
- **Take Action Against the Intruder**
  - The most aggressive form of this response involves launching attacks against
  - Attempting to actively gain information about the attacker's host or site
  - This response is not advised. Due to legal ambiguities about civil liability
- **Alarms and Notifications**
  - Alarms and notifications are generated by IDSs to inform users when attacks are detected
  - The most common form of alarm is an onscreen alert or popup window
  - Remote notification of alarms or alerts
  - Some commercial IDSs are designed to generate alarms and alerts, reporting them to a network management system
  - Some products also offer email as another notification channel
- **Types of Intrusions**
  - **Input Validation Error**
  - **Buffer Overflow**
  - **Boundary Condition**
  - **Access Validation Error**
  - **Exceptional Condition Handling error**
  - **Environmental Error**
  - **Configuration Error**
  - **Race Condition**