**Intrusion Detection**

**Intruders:**

An intruder is any person who attempts to violate security policy of a system availability, data integrity and confidentiality. Such persons usually use a “backdoor” to attack a system or a network.

**Intrusion Techniques:**

The objective of the intruder is to gain access to a system or to increase the range of privileges accessible on a system. Generally, this requires the intruder to acquire information that should have been protected. In some cases, this information is in the form of a user password. With knowledge, an intruder can log in to a system and exercise all the privileges accorded to the legitimate user.

On the basis of a survey of the literature and interviews with a number of password crackers, the following techniques are used for learning passwords:

1. Try default passwords used with standard accounts that are shipped with the system. Many administrators do not bother to change these defaults.
2. Exhaustively try all short passwords (those of one to three characters).
3. Try words in the system's online dictionary or a list of likely passwords. Examples of the latter are readily available on hacker bulletin boards.
4. Collect information about users, such as their full names, the names of their spouse and children, pictures in their office, and books in their office that are related to hobbies.
5. Try users' phone numbers, Social Security numbers, and room numbers.
6. Try all legitimate license plate numbers for this state.
7. Use a Trojan horse to bypass restrictions on access.
8. Tap the line between a remote user and the host system.

### Intrusion Detection

“Intrusion detection is a method used to detect possible suspicious activities in a network traffic or host-based system”

**Types of Intrusion Detection Technique:**

Intrusion detection systems determine if actions constitute intrusions on the basis of one or more models of intrusion. A model classifies a sequence of states or actions as “good” (no intrusions) or “bad” (intrusion).

1. Anomaly Model

**Definition:** *Anomaly detection* analyzes a set of characteristics of the system and compares their behavior with a set of expected values. It reports when the computed statistics do not match the expected measurements.

Denning identifies three different statistical models for anomaly detection

1. ***threshold metric***. A minimum of *m* and a maximum of *n* events are expected to occur. If, over aspecific period of time, less than *m* or more than *n* events occur, the behavior isdeemed anomalous.
2. ***statistical moments***. The analyzer knows the mean and standard deviation (first two moments) .If values fall outside the expected interval for that moment, the behavior that the values represent is deemed anomalous.
3. ***Markov model***. Examine a system at some particular point in time.

**EXAMPLE**: Microsoft Windows NT 4.0 allows the system to lock a user out after some number *n* of failed login attempts [479]. This is an intrusion detection system using the threshold metric with the lower limit 0 and the upper limit *n*. The attempted logins are deemed anomalous after *n* failed attempts to log in.

**Misuse Modeling**

**Definition:** *Misuse detection* determines whether a sequence of instructions being executed is known to violate the site security policy. If so, it reports a potential intrusion.

One system, IDIOT [538], monitors audit logs looking for a sequence of events that correspond to an attack.

**Specification Modeling**

**Definition:** *Specification-based detection* determines if a sequence of instructions violates a specification of how a program, or system, should execute. If so, it reports a potential intrusion.

### IDS (Intrusion Detection System)

**An intrusion detection system (IDS)** is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered.

While [anomaly detection](https://searchsecurity.techtarget.com/definition/network-behavior-anomaly-detection) and reporting is the primary function, some intrusion detection systems are capable of taking actions when malicious activity or anomalous traffic is detected, including blocking traffic sent from suspicious IP addresses.

### Different types of intrusion detection systems

Intrusion detection systems come in different flavors and detect suspicious activities using different methods, including the following:

* **A network intrusion detection system (NIDS)** is deployed at a strategic point or points within the network, where it can monitor inbound and outbound traffic to and from all the devices on the network. The agents here examine the network logs to detect any anomalous behavior.
* **Host intrusion detection systems (HIDS**) run on all computers or devices in the network with direct access to both the internet and the enterprise internal network. The agents here examine the system logs to detect any anomalous behavior.
* **Signature-based intrusion detection systems** monitor all the packets traversing the network and compare them against a database of signatures or attributes of known malicious threats, much like [antivirus software](https://searchsecurity.techtarget.com/definition/antivirus-software).

**Intrusion Detection System (IDS) Architecture:**

IDS architecture consists of three main components agent, director and notifier. **The agent** corresponds to the logger. It acquires information from a target ( from a single host, from a set of hosts or from a network).

##### **Host-Based Information Gathering**

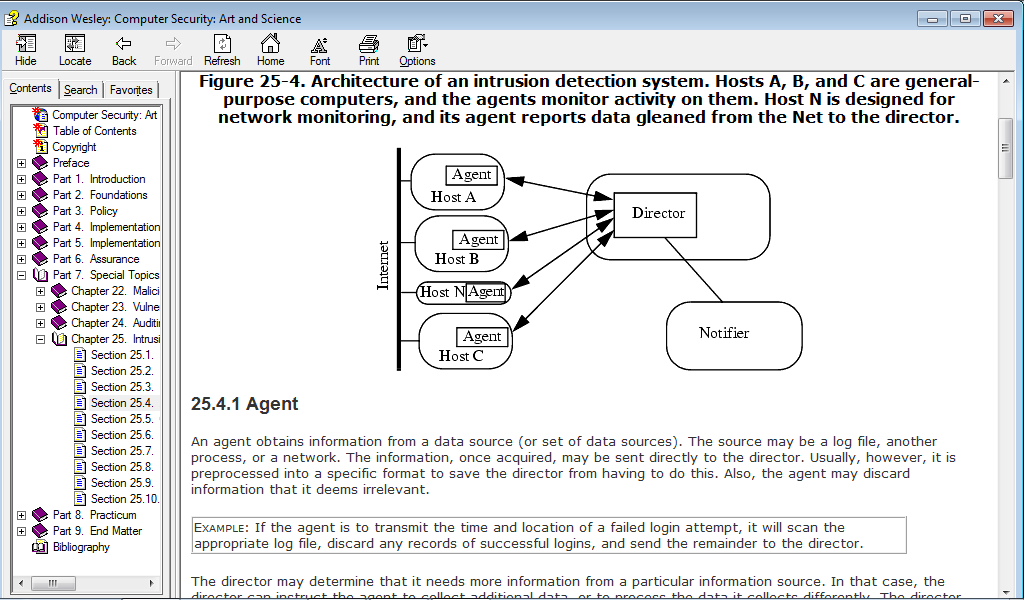
Host-based agents usually use system and application logs to obtain records of events, and analyze them to determine what to pass to the director.

##### **Network-Based Information Gathering**

Network-based agents use a variety of devices and software to monitor network traffic. It gathers information by examining the contents of the traffic itself.

**The director** corresponds to the analyzer. The director reduces the incoming log entries to eliminate unnecessary and redundant records. It then uses an analysis engine to determine if an attack is underway.

**Notifier** The notifier accepts information from the director and takes the appropriate action. In some cases, this is simply a notification to the system security officer that an attack is believed to be underway.



### Organization of Intrusion Detection Systems:

An intrusion detection system can be organized in several ways. The first system examined network traffic only. The second explored how to combine network and host sources. The third system distributed the director among multiple systems to enhance security and reliability.

### Monitoring Network Traffic for Intrusions: NSM

* The Network Security Monitor (NSM) develops a profile of expected usage of a network.
* It compares current usage with that expected profile.
* The monitor measures network utilization and log activity based on a user, a group of users, or a service. It then reports anomalous behavior if any.
* The NSM monitors the source, destination, and service of network traffic. It assigns a unique connection ID to each connection. Each element of the matrix contains the number of packets sent over that connection for a specified period of time, and the sum of the data of those packets.

**Combining Host and Network Monitoring: DIDS**

* The Distributed Intrusion Detection System (DIDS) combined the abilities of the NSM with intrusion detection monitoring of individual hosts.
* DIDS used a centralized analysis engine (the DIDS director)
* The agents are placed on each system that has to be monitored.
* The agents are also placed on a network.
* The agents scanned logs for events and reported them to the DIDS director.
* The DIDS director invoked an expert system that performed the analysis of the data.

### Autonomous Agents: AAFID

If the IDS director fails, the IDS will not function. The solution is to use autonomous agents. An autonomous agent is a process that can act independently of the system of which it is a part and can perform specific monitoring function. Each agent would have its own internal model, and when the agent detected a a violation of a specification, it would notify other agents. The agents would jointly determine whether the set of notifications were sufficient to constitute a reportable intrusion.

### Intrusion Response

Intrusion response means to handle the (attempted) attack in such a way that damage is minimized.

### 1. Incident Prevention

In the context of response, prevention requires that the attack be identified before it completes. The defenders then take measures to prevent the attack from completing.

### 2. Intrusion Handling

When an intrusion occurs, the security policy of the site has been violated. Handling the intrusion means restoring the system to comply with the site security policy and taking any actions against the attacker that the policy specifies. Intrusion handling consists of six phases.

1. **Preparation for an attack:** This step occurs before any attacks are detected. It establishes procedures and mechanisms for detecting and responding to attacks.
2. **Identification of an attack:** This triggers the remaining phases.
3. **Containment (confinement) of the attack:** This step limits the damage as much as possible.
4. **Eradication of the attack:** This step stops the attack and blocks further similar attacks.
5. **Recovery from the attack:** This step restores the system to a secure state
6. **Follow-up to the attack:** This step involves taking action against the attacker, identifying problems in the handling of the incident, and recording lessons learned (or lessons not learned that should be learned).

**Difference between IPS & IDS**

|  |  |
| --- | --- |
| **IPS** | **IDS** |
| It prevents attack from intruders | It detects intruder activities when attacked |
| It is placed in-line in the network | It can be placed anywhere in the network |
| It is basically used to record the observed intrusion events | It is used to implement security in order to report and take actions when intrusion is found |
| IPS is an application layer firewall | IDS is not a firewall |