Intrusion

Intrusion: A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without having authorization to do so.

Intrusions can come from outside your network structure or inside Some intrusions are simply meant to let you know the intruder was there, defacing your Web site with various kinds of message. Others are more malicious, seeking to extract critical information on either a one-time basis or as an ongoing parasitic relationship that will continue to siphon off data until it's discovered.

Some intruders will seek to implant carefully crafted code designed to crack passwords, record keystrokes, or mimic your site while directing unaware users to their site. Others will embed themselves into the network and quietly siphon off data on a continuing basis or to modify public-facing Web pages with various kinds of messages.

An intrusion may include any of the following:

- Malware or ransomware.
- Attempts to gain unauthorized access to a system.
- DDOS attacks.
- Cyber-enabled equipment destruction.
- Accidental employee security breaches.
- Untrustworthy users.
- Social engineering attacks.

Intrusion detection system: IDS observes network traffic for malicious transactions and sends immediate alerts when it is observed. It is software that checks a network or system for malicious activities or policy violations. Each illegal activity or violation is often recorded either centrally using a SIEM system or notified to an administration. IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access from users, including perhaps insiders.

How does an IDS work?

1. An IDS (Intrusion Detection System) monitors the traffic on a computer network to detect any suspicious activity.
2. It analyzes the data flowing through the network to look for patterns and signs of abnormal behavior.
3. The IDS compares the network activity to a set of predefined rules and patterns to identify any activity that might indicate an attack or intrusion.
4. If the IDS detects something that matches one of these rules or patterns, it sends an alert to the system administrator.
5. The system administrator can then investigate the alert and take action to prevent any damage or further intrusion.

There are 2 types of IDS and those are **Network Intrusion Detection System (NIDS)** and **Host Intrusion Detection System (HIDS).**