Chapter 7:
IDS - IPS

Intro

- An intrusion can be defined as any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource. [Heady R. 1990]
- **Intrusion detection** is a technique of detecting unauthorized access to a computer system or a computer network.
- **Intrusion prevention** is the art of preventing an unauthorized access of a system's resources.
- Intrusion detection passively detects system intrusions, intrusion prevention actively filters network traffic to prevent intrusion attempts

Intrusion Detection

- In 1980, James Anderson's paper, "Computer Security Threat Monitoring and Surveillance"
- 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

- Aurobindo Sundaram divides intrusions into six types:
  - **Attempted break-ins**. An intrusion detection system for this type is called **anomaly-based IDS**.
  - **Masquerade attacks**. These intrusions are also detected using anomaly-based IDS.
  - **Penetrations of the security control system**, which are detected by monitoring for specific patterns of activity.
  - **Leakage**, which is detected by atypical use of system resources.
  - **Denial of service**, which is detected by atypical use of system resources.
  - **Malicious use**, which is detected by atypical behavior profiles, violations ofsecurity constraints, or use of special privileges.

The System Intrusion Process

- The intrusion process into a system includes a number of stages that start with the identification of the target, followed by reconnaissance that produces as much information about the target as possible.
- After enough information is collected about the target and weak points are mapped, the next job is to gain access into the system and finally the actual use of the resources of the system

The System Intrusion Process

- Reconnaissance
- Physical Intrusion

The System Intrusion Process

Reconnaissance:

- Reconnaissance is the process of gathering information about the target system and the details of its workings and weak points.
- Hackers do the reconnaissance through system scanning for vulnerabilities.
- Vulnerabilities may include: weaknesses in operating systems, application software, and protocols, …

The System Intrusion Process

Physical Intrusion:

- Intruders can enter an organization network masquerading as legitimate users. They do this through a number of ways ranging from acquiring special administrative privileges to low-privilege user accounts on the system.

The System Intrusion Process

Denial of Service:

- Denial-of-service (DoS) attacks are where the intruder attempts to crash a service (or the machine), overload network links, overload the CPU, or fill up the disk.
- The intruder is not trying to gain information, but to simply act as a vandal to prevent you from making use of your machine.
- Common Denial-of-Service Attacks:
  - Ping-of-Death
  - SYN Flood
  - Land/Latierra
  - WinNuke

The Dangers of System Intrusions

- Loss of personal data: compared with physical data loss.
- Compromised privacy
- Legal liability

Intrusion Detection Systems (IDSs)

- An intrusion detection system (IDS) is a system used to detect unauthorized intrusions into computer systems and networks.
- Three models of intrusion detection mechanisms:
  - **anomaly-based detection** (behavior-based detection): are also considered as rule-based detection because they use rules, to be able to determine unacceptable behavior.
  - **signature-based detection** (misuse-based detection): operate in much the same way as a virus scanner, by searching for a known identity - or signature - for each specific intrusion event, can detect only previously known attacks
  - **hybrid detection**

Anomaly Detection

- An Anomaly-Based Intrusion Detection System, is a system for detecting computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous.
- The classification is based on heuristics or rules.
- In order to determine what is attack traffic, the system must be taught to recognize normal system activity. This can be accomplished in several ways, most often with artificial intelligence type techniques.

Misuse Detection

- The IDS analyzes the information it gathers and compares it to large databases of attack signatures. The IDS looks for a specific attack that has already been documented.
- Like a virus detection system, misuse detection software is only as good as the database of attack signatures that it uses to compare packets against.
- 2 problems:
  - The system cannot detect unknown attacks with unmapped and unarchived signatures.
  - The system cannot predict or detect new attacks.

Types of intrusion detection systems

- Intrusion detection systems are also classified based on their monitoring scope.
  - Network-based intrusion detection: monitor a wide area.
  - Host-based instrusion detection: monitor a small area.

Types of intrusion detection systems - NIDSs

Network-based intrusion detection systems:

- Have the whole network as the monitoring scope, monitoring the traffic on the network to detect intrusions.
- Responsible for detecting anomalous, inappropriate, or other data that may be considered unauthorized and harmful occurring on a network.
- NIDS vs Firewall?

Types of intrusion detection systems - NIDSs

Network-based intrusion detection systems:

- NIDS vs Firewall:
  - Firewalls are configured to allow or deny access to a particular service or host based on a set of rules. Only when the traffic matches an acceptable pattern is it permitted to proceed regardless of what the packet contains.
  - An NIDS also captures and inspects every packet that is destined to the network regardless of whether it is permitted or not. If the packet signature based on the contents of the packet is not among the acceptable signatures, then an alert is generated.

Types of intrusion detection systems - NIDSs

Network-based intrusion detection systems:

- Architecture of a Network-Based Intrusion Detection: several parts that must work together (sequential, parallel) to produce an alert.
  - Network Tap/Load Balancer: gathers data from the network and distributes it to all network sensors.
  - Network Sensor/Monitoring: a computer program that runs on dedicated machines or network devices on mission critical segments, receiving traffic from the balancer or live traffic from the network.
  - Analyzer: receives data from the sensors then classified as either safe or an attack

Types of intrusion detection systems - NIDSs

Network-based intrusion detection systems:

- Architecture of a Network-Based Intrusion Detection: several parts that must work together (sequential, parallel) to produce an alert.
  - Alert Notifier: contacts the security officer responsible for handling incidents whenever a threat is severe enough according to the organization's security policy
  - Command Console/Manager: central command authority for controlling the entire system
  - Response Subsystem: provides the capabilities to take action based on threats to the target systems
  - Database: the knowledge repository for all that the intrusion detection system has observed

Types of intrusion detection systems - NIDSs

Network-based intrusion detection systems:

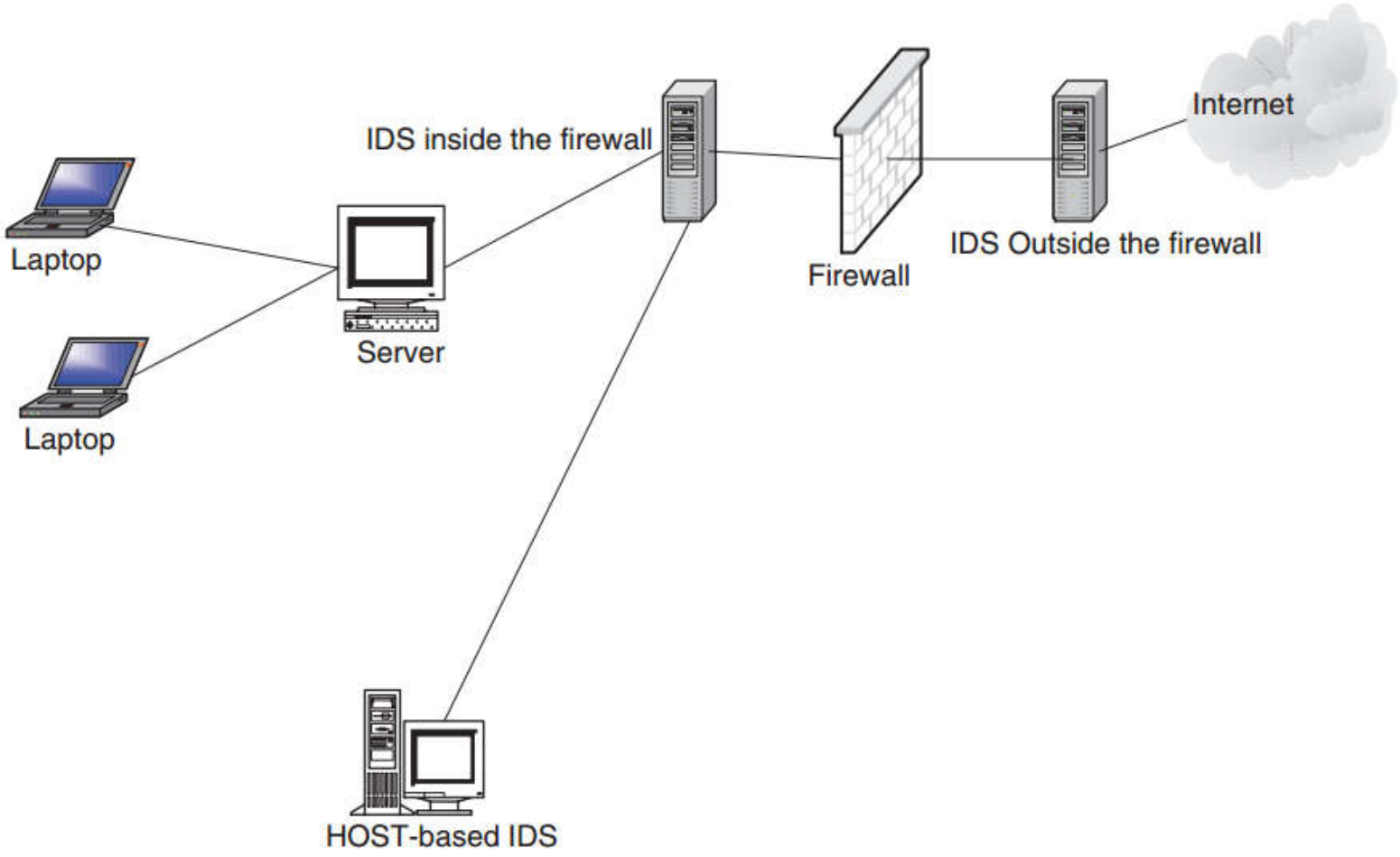

Fig. 13.1 The architecture of a network-based intrusion detection system

Types of intrusion detection systems - NIDSs

Network-based intrusion detection systems:

- Placement of IDS Sensors:the position to place a network IDS sensors actually depends on several factors. IDS sensors offen placed in the following areas:
  - Inside the DMZ
  - Between the Firewall and the Internet
  - Behind the Network Front Firewall
  - Inside the Network

Types of intrusion detection systems - NIDSs

Network-based intrusion detection systems:

- Placement of IDS Sensors:

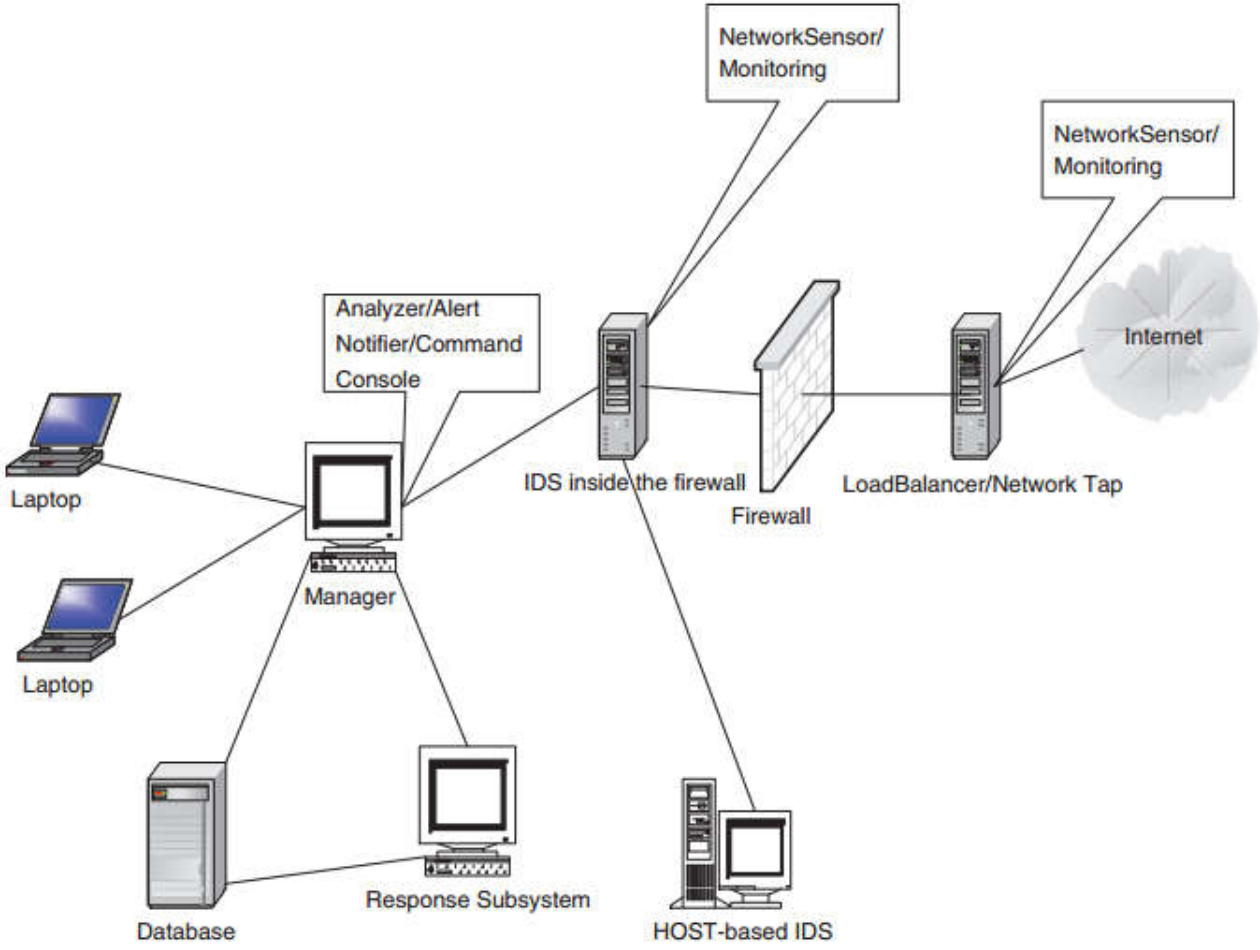

Fig. 13.2 The various places of placing the IDS sensors

Types of intrusion detection systems - NIDSs

Network-based intrusion detection systems:

- Advantages of Network-Based Intrusion Detection Systems
  - Ability to detect attacks that a host-based system would miss because NIDSs monitor network traffic at a transport layer
  - Difficulty to remove evidence (compared to HIDSs, because NIDSs are on dedicated machines that are routinely protected).
  - Real-time detection and response
  - Ability to detect unsuccessful attacks (NIDSs outsite the firewall)

Types of intrusion detection systems - NIDSs

Network-based intrusion detection systems:

- Disadvantages of Network-Based Intrusion Detection Systems
  - Blind Spots: deployed at the borders of an organization network, NIDS are blind to the whole inside network.
  - Encrypted Data: one of the major weaknesses of NIDS is on encrypted data. They have no capabilities to decrypt encrypted data. Although they can scan unencrypted parts of the packet such as headers, they are useless to the rest of the package.

Types of intrusion detection systems - HIDSs

Host-based intrusion detection systems:

- Host-based intrusion detection is the technique of detecting malicious activities on a single computer.
- It uses software that monitors operating system specific logs, including system, event, and security logs on Windows systems and syslog in Unix environments to monitor sudden changes in these logs.
- When a change is detected in any of these files, the HIDS compares the new log entry with its configured attack signatures to see if there is a match.
- If a match is detected, then this signals the presence of an illegitimate activity.

Types of intrusion detection systems - HIDSs

Host-based intrusion detection systems:

- Advantages of Host-Based Intrusion Detection Systems:
  - Ability to verify success or failure of an attack quickly
  - Low-level monitoring (able to "see" low-level local activities such as file accesses, changes to file permissions,…)
  - Near real-time detection and response (operating system can recognize the event before any IDS can)
  - Ability to deal with encrypted and switched environments.
  - Cost effectiveness (no additional hardware is needed to install HIDS)

Types of intrusion detection systems - HIDSs

Host-based intrusion detection systems:

- Disadvantages of Host-Based Intrusion Detection Systems:
  - Myopic viewpoint. Since they are deployed at a host, they have a very limited view of the network.
  - Since they are close to users, they are more susceptible to illegal tampering.

Types of intrusion detection systems -

Other types of IDS:

- Hybrid
- System integrity verifiers(SIVs) monitor critical files in a system, such as system files, to find whether an intruder has changed them.
- Log file monitors(LFMs) first create a record of log files generated by network services. Then they monitor this record, just like NIDS, looking for system trends, tendencies, and patterns in the log files that would suggest that an intruder is attacking.

Types of intrusion detection systems

Other types of IDS:

- Honeypot: is a system designed to look like something that an intruder can hack, the goal for a honeypot is to deceive intruders and learn from them without compromising the security of the network.

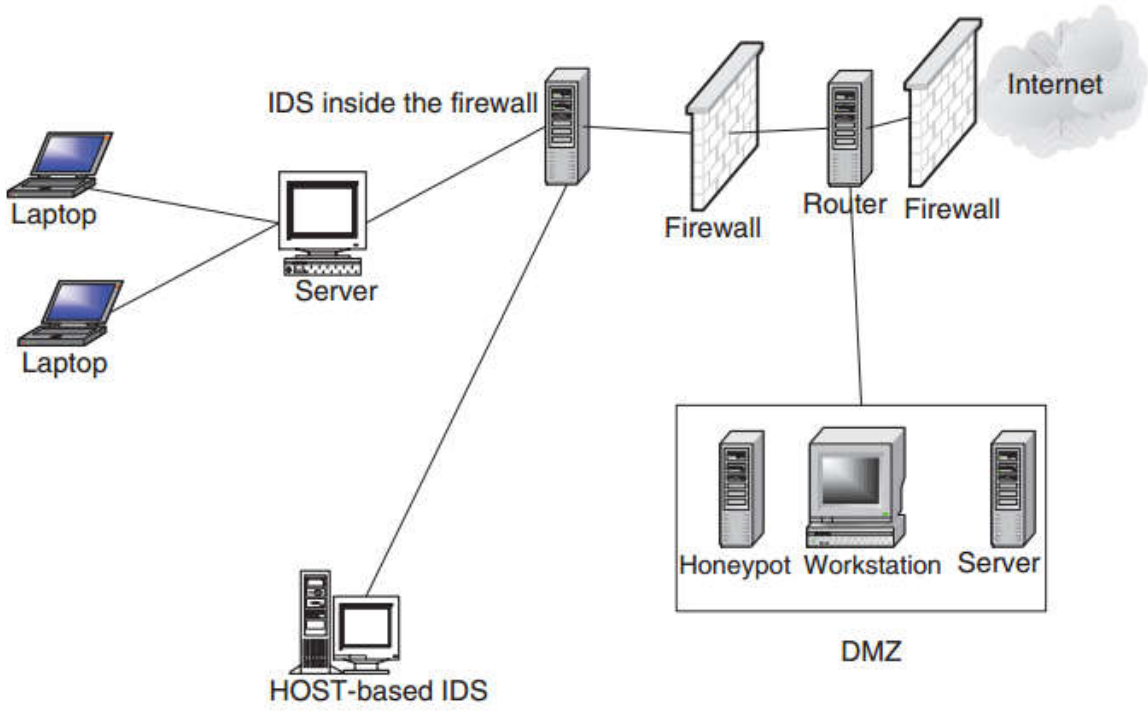

Fig. 13.3 The positioning of a honeypot

Intrusion Prevention Systems (IPSs)

- IDSs are a passive component which only detects and reports without preventing.
- The intrusion prevention system(IPS) is to prevent attacks.
- IPS fall into two categories:
  - network-based
  - host-based
- The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

Intrusion Prevention Systems (IPSs)

- Intrusion prevention systems are considered extensions of intrusion detection systems, but placed in-line and are able to actively prevent/block intrusions that are detected.
- IPS can: sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address, correct Cyclic Redundancy Check (CRC) errors, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options.

Intrusion Detection Tools

- Guide to Computer Network Security: page 295-297

Read more

- Guide to Computer Network Security, chapter 13, pg 273-295
- http://en.wikipedia.org/wiki/Intrusion_prevention_system
- http://en.wikipedia.org/wiki/Intrusion_detection_system