INTRUSION DETECTION SYSTEM

http://eforu.page.tl/
INTRODUCTION:
An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

ABSRTACT:

- INTRUSION DETECTION
determining whether or not some entity, the intruder, has attempted to gain, or worse, has gained unauthorized access to the system

- INTRUDERS ARE OF TWO TYPES
  - Internal
  - External

- OBJECTIVES OF IDS
  - Confidentiality
  - Integrity
  - Availability
  - Accountability

- INTRUSION DETECTION CAN BE USED AS
  - System detection intrusion.
  - Burglar alarm
  - Detect unauthorized access attempts.
  - First line of defense.

- WHY DO WE NEED IDS
  - To create complete secure system.
  - Recognize presence of intruders and hold them.
  - Prevent them from doing harm.
  - Make future intrusion more difficult the next time.

http://eforu.page.tl/
• FEATURE OF IDS
  - Ability to replay stored attacks for post-mortem and forensic analysis.
  - Strong reporting capabilities.
  - Stealth more sensor operation.
  - Manageable counter measures.
  - Ability to analyze encrypted traffic.
  - Easy to use GUI, and/or command line alternative if preferred

• CLASSIFICATION OF IDS
  HOST BASED: Detect intrusion by monitoring activity of a single host.

  MULTI-HOST BASED: Detect intrusion by obtaining data from multiple hosts.

  NETWORK BASED: Make decisions by monitoring the entire traffic in a network along with data from one or more hosts.

• DISADVANTAGE OF IDS
  ❖ HOST BASED
    - Continuous packets.
    - IDS goes down if host goes down.
    - More cost effective.

  ❖ MULTI-HOST BASED & NETWORK BASED
    - Data is not given immediately for its decision making.
    - The storage capacity of the centralized repository will be extremely large.
    - Adds an extra complication to the design of the intrusion detection system.

http://eforu.page.tf/