Intrusion Detection methodologies and Approaches

Intrusion Detection methodologies

- Intrusion detection methodologies are classified as three major categories:
  - Signature-based Detection (SD)
  - Anomaly-based Detection (AD)
  - Stateful Protocol Analysis (SPA)

Intrusion Detection methodologies

- Detection can be performed according to two complementary strategies:
  - defining what is the manifestation of an attack and searching for an occurrence of the attack (misuse-based or signature based)
  - defining what is the normal behaviour on the system and searching for activities that deviate from it (anomaly-based)

- The stateful in SPA indicates that IDS could know and trace the protocol states
  - SPA depends on vendor-developed generic profiles to specific protocols
  - also known as Specification based Detection

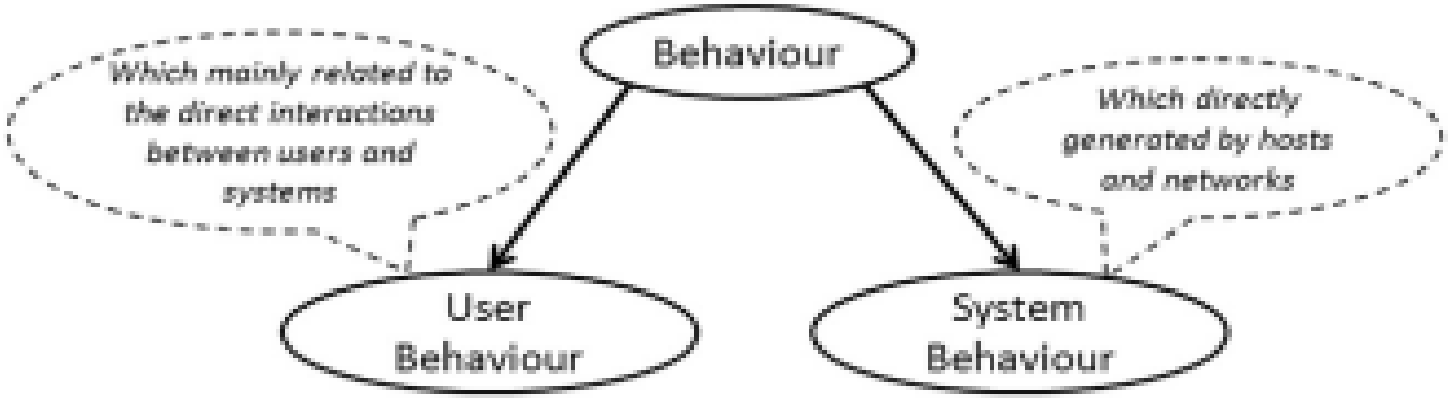
Pros and cons of intrusion detection methodologies

Signature-based (knowledge-based)	Anomaly-based (behavior-based)	Stateful protocol analysis (specification-based)
Pros		
• Simplest and effective method to detect known attacks. • Detail contextual analysis.	• Effective to detect new and unforeseen vulnerabilities. • Less dependent on OS. • Facilitate detections of privilege abuse.	• Know and trace the protocol states. • Distinguish unexpected sequences of commands.
Cons		
• Ineffective to detect unknown attacks, evasion attacks, and variants of known attacks. • Little understanding to states and protocols. • Hard to keep signatures/patterns up to date. • Time consuming to maintain the knowledge	• Weak profiles accuracy due to observed events being constantly changed. • Unavailable during rebuilding of behavior profiles. • Difficult to trigger alerts in right time.	• Resource consuming to protocol state tracing and examination. • Unable to inspect attacks looking like benign protocol behaviors. • Might incompatible to dedicated OSs or APs.

Anomaly based intrusion detection

- Anomalies also known as outliers, exceptions or peculiarities are patterns in data that do not conform to a well defined notion of normal behaviour of a system
- Behavioural intrusion detection systems focus on behaviours
- The behaviours can be divided into
  - system behaviours
  - User behaviours

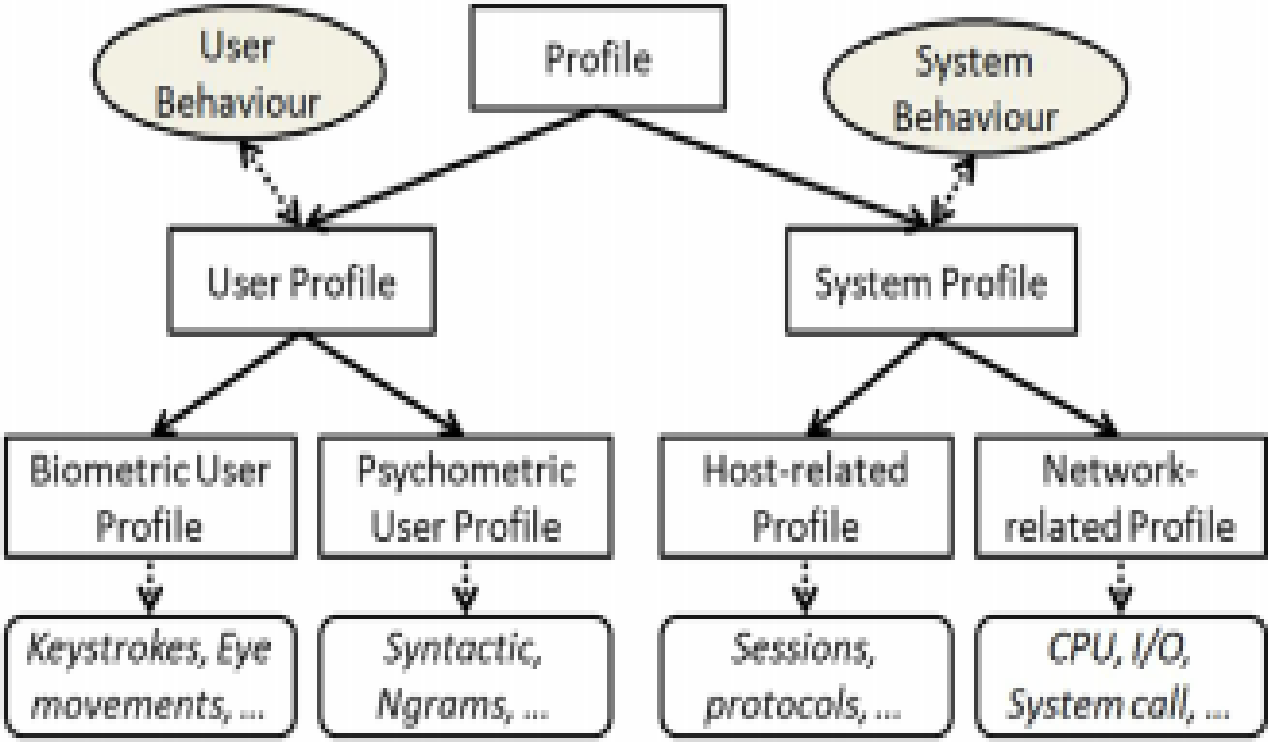
Classification of behaviours



Profiles in IDS modelling

- An anomaly-based IDS requires a user model that profiles the normal behaviour for that user so as to enable identification of anomalies in comparison to the normal behaviour of the user.

Classifications of profiles.

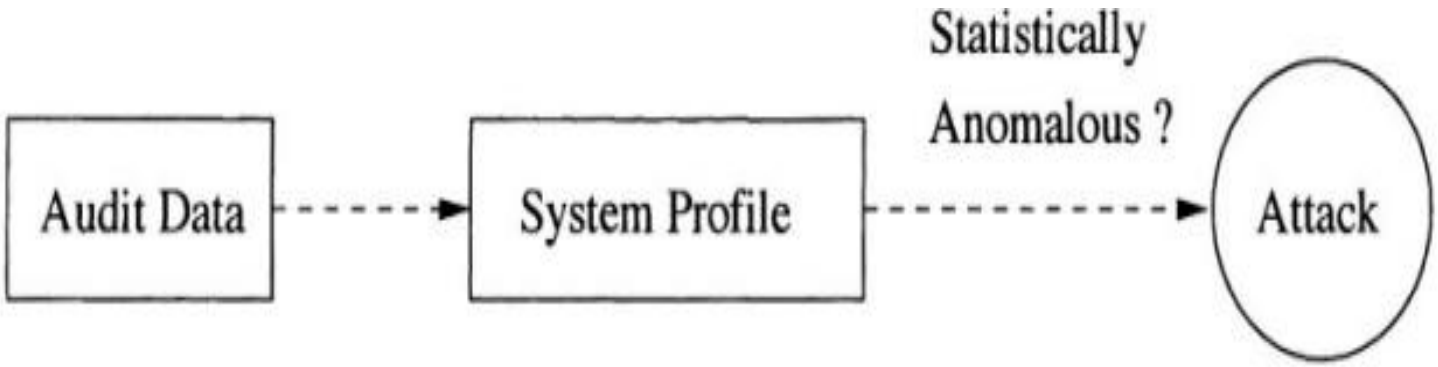


Anomaly based detection

- Anomaly Detection Techniques represents a broad spectrum of detection techniques.
- One can define profiles in terms of simple thresholds or more complex statistical distributions
- The profiles can be self-learned or manually set, adaptive, or static
- Anomaly-based systems are based on the assumption that all anomalous activities are malicious

- The normal profiles are continuously learned while the system is in detection mode
- Allows the anomaly profiles to adapt to changes that occur in an organization

Block Diagram of a Typical Anomaly Based IDS



Anomaly based detection

- *Advantages:*
  i. IDSs based on anomaly detection detect unusual behaviour and thus have the ability to detect symptoms of attacks without specific knowledge of details.

  ii. Anomaly detectors can produce information that can in turn be used to define signatures for misuse detectors.

- *Disadvantages:*
  Anomaly detection approaches usually produce a large number of false alarms due to the unpredictable behaviours of users and networks.

Anomaly based detection approaches

- Statistical Anomaly Based Intrusion Detection
- Protocol Anomaly Detection
- Application Payload Anomaly

Statistical Anomaly Based Intrusion Detection

- There is a stable balance among different types of TCP packets in the absence of attacks which is compared against short-term observations
- Statistical anomaly based IDS captures this behaviour and differentiates between the long term and short term observations

- Statistics-based approaches are mainly by means of predefined threshold, mean and standard deviation, and probabilities to identify intrusions (Marcov Process Model).

Protocol Anomaly Detection

- The protocol anomaly refers to all exceptions related to protocol format and behaviour with respect to common practice on the Internet and standard specifications
- This includes network and transport layer protocol anomalies in layers 3-4 and application layer protocol anomalies in layers 6-7.
- Unusual conditions are checked for in the process of IP defragmentation, TCP reassembly.

- Examples of protocol anomalies
  - Illegal field values and combinations
  - Illegal command usage
  - Unusually long or short field lengths, which can indicate an attacker is attempting to introduce a buffer overflow
  - Unusual number of occurrences of particular fields/commands
  - Running a protocol or service for a non-standard purpose or on a non-standard port

Application Payload Anomaly

- Application anomaly must be supported by detailed analysis of application protocols to define accurate behaviour
- Also requires understanding of the application semantics
- It is essential to know what type of encoding is legal for a given field, and what other applications can be embedded within it.

Anomaly-Based Detection

- These systems may suffer from specific problems:
  - The amount of time required to teach to the system the normal behaviour might be long.
  - The behaviour of the monitored environment might change during a period of time, requiring the system to be retrained.
  - If the training set contains attacks, the system will consider malicious behaviour normal.
  - Anomaly detection approaches often require extensive “training sets” of system event records in order to characterize normal behaviour patterns

Types of attacks detected by Anomaly based IDS

- Misuse of Protocol and Service Ports
- DoS Based on Crafted Payloads
  - When a malicious intruder creates an attack using a crafted IP packet, the resulting Denial of Service (DoS) can occur on the network bandwidth, CPU cycles, memory resources, or application process/programs.

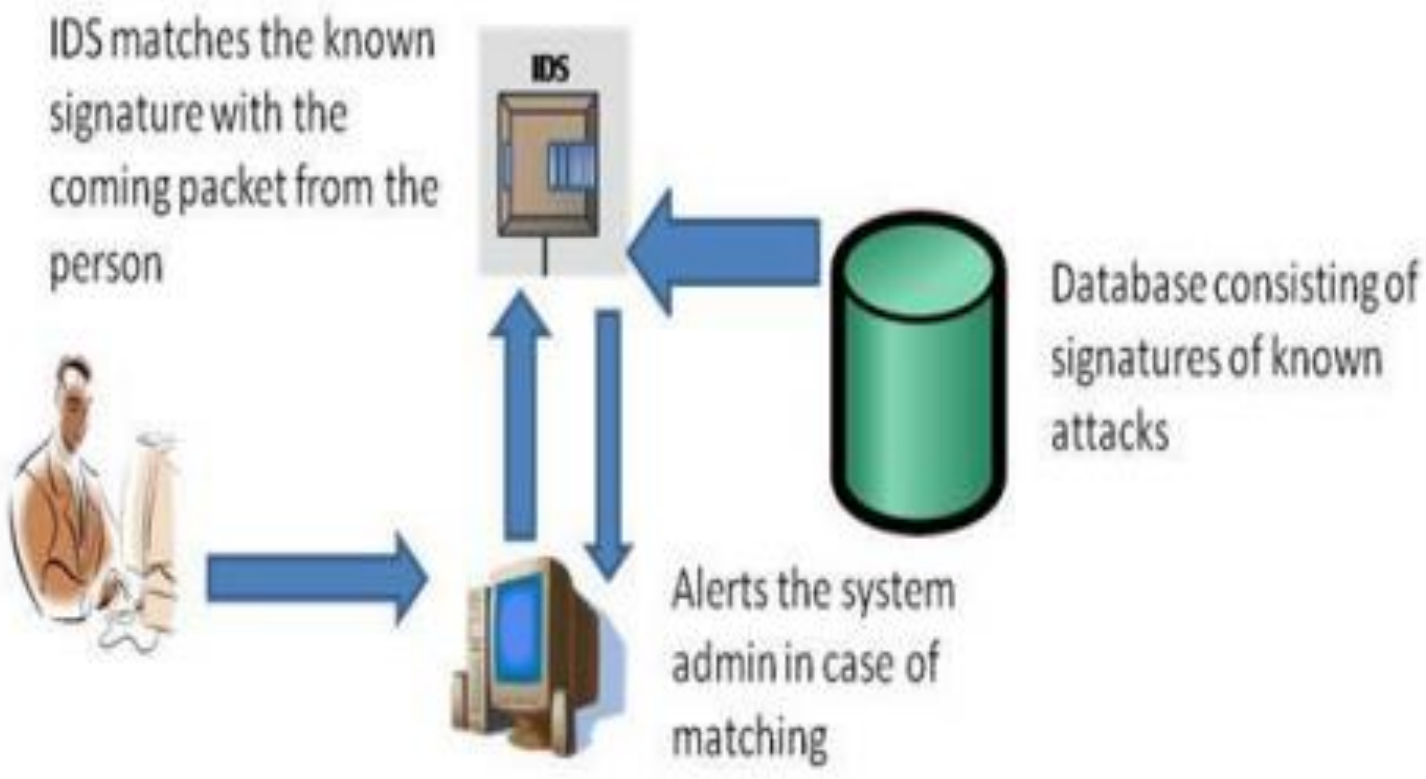
Types of attacks detected by Anomaly based IDS

- DoS Based on Volume (DDoS)
  - traffic pattern anomalies can be observed as a result of the Distributed Denial of Service (DDoS)
    - TCP control packet statistics for TCP SYN flood
    - relative volumes of TCP, UDP, and ICMP traffic for UDP or ICMP flood.

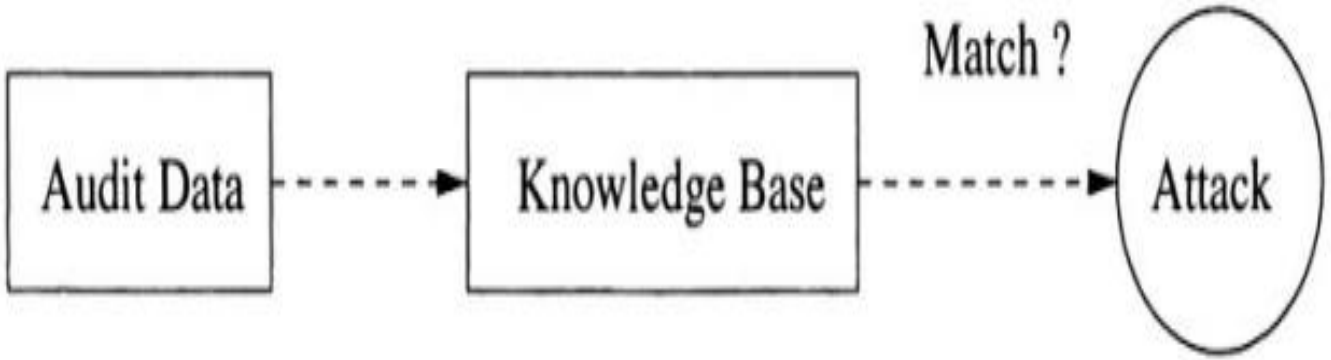
- Buffer Overflow
  - Many exploited fields, such as user passwords for FTP, are made of printable ASCII characters based on the standard Request For Comments (RFCs) by the Internet Engineering Task Force (IETF).
  - Excessive non-printable ASCII characters are anomalies of strong suspicion.
  - Shellcode embedded in these fields are sure signs of malicious intent.

Misuse-based Systems

- Misuse-based systems are equipped with a database of information (the knowledge base) that contains a number of attack models
- The audit data collected by the IDS is compared with the content of the database and, if a match is found, an alert is generated.


IDS matches the known signature with the coming packet from the person
IDS
Database consisting of signatures of known attacks
Alerts the system admin in case of matching

Block Diagram of a Typical Knowledge-Based IDS



- ***Advantages:***
  - Misuse detectors are very effective at detecting attacks without generating an overwhelming number of false alarms.
  - Misuse detectors can quickly and reliably diagnose the use of a specific attack tool or technique.

- ***Disadvantages:***
  - populating the knowledge base is a difficult, resource intensive task.
  - Misuse detectors can only detect those attacks they know about, therefore they must be constantly updated with signatures of new attacks.

Misuse based intrusion detection techniques

- Expression matching
- State transition analysis

Expression matching

- The simplest form of misuse detection is expression matching
- searches an event stream (log entries, network traffic) for occurrences of specific patterns/signatures.

- Example

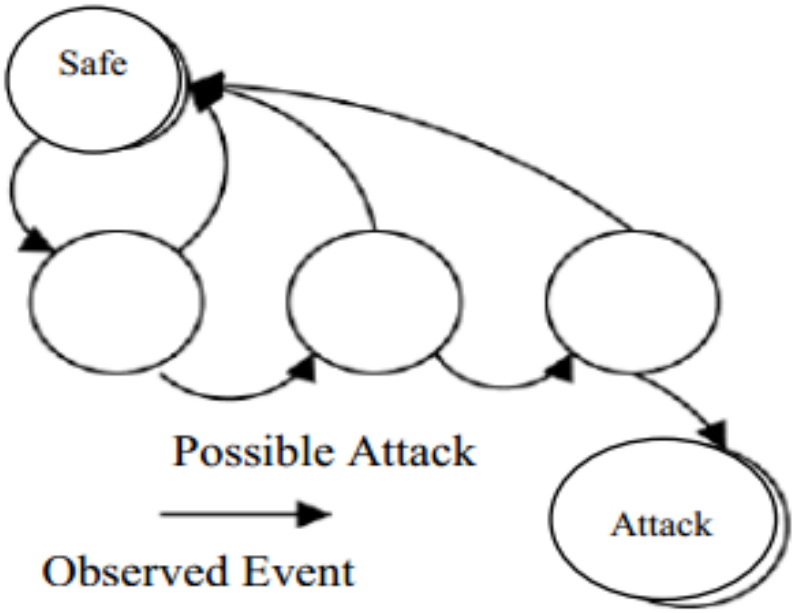
"^GET[^$]*/etc/passwd$" - this checks for something that looks like an HTTP request for the Unix password file.

An e-mail with a subject of “Free pictures!” and an attachment filename of “freepics.exe”, which are characteristics of a known form of malware

State transition analysis

- Used to describe complex attack signatures
- A *state* is a snapshot of the system representing the value of all the memory locations of the system.
- State transition analysis models an activity on the system as a series of state transitions

- Malicious activities move the state of the system from an initial safe state to a final compromised state, possibly passing through a number of intermediate states.
- Every observed event is applied to finite state machine instances
- Any machine that reaches its final (acceptance) state indicates an attack


Safe
Possible Attack
Attack
Observed Event

- This technique requires the analyst to identify those transitions that are critical in leading the system into a compromised state.

- This approach allows complex intrusion scenarios to be modelled in a simple way, and is capable of detecting slow or distributed attacks

- State transition systems are stateful tools
  - *Stateful* intrusion detection systems maintain information about past events

Advantages of State transition analysis

- State transition models are appealing because they allow high-level, even graphical, description of attacks.
- Complicated attacks can be modelled and detected.
- It also provides very detailed feedback on the generated alerts, because the entire sequence of actions that caused the alarm to be triggered can be easily provided.

- It allows to deploy a response before an attack reaches its final step.
-

Drawback of State transition analysis

- Computational requirements can be high if the system has to keep track of many concurrent attacks.

Salient Points.

- Signature-based detection is very effective at detecting known threats but largely ineffective at detecting previously unknown threats, threats disguised by the use of evasion techniques, and many variants of known threats.

- Signature-based detection is the simplest detection method because it just compares the current unit of activity, such as a packet or a log entry, to a list of signatures using string comparison operations.

Target Monitoring

- Any change or modification in the target objects are reported by the Target Monitoring Systems
- This is usually done through cryptographic algorithm that computes a crypto-chechsum for each target file
- Changes such as file modification or program logon which would cause changes in the crypto-checksum are reported by the IDS.

Stealth Probes

- Stealth probes collects and correlate data to try to detect attacks made over long period of time, often referred to as “low and slow” attacks