UNIVERSITY OF M'SILA
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE COMPUTER SCIENCE DEPARTMENT

NETWORK AND SYSTEM INTRUSION DETECTION

SAOUDI Lalia

2020-2021

Course Outline

General Principles: Introduction to IDS

- What is an IDS?
- The main types of IDS
- Intrusion Detection
- Detection Methods
- Network Intrusion Detection Systems
- System Intrusion Detection Systems
- Specific IDS: Honeypots and IPS
- Honeypots
- IPS: Intrusion Prevention Systems

What is an intrusion?

What is an Intrusion Detection System IDS?

Definition: A security tool that monitors network or system activities for malicious activities or policy violations

what is an intrusion?

It is an action aimed at compromising, on an information system : Confidentiality

Integrity

Availability

Accountability

Authentication

➢ This action can:

- Succeed
- Fail
- Be ongoing
- Be a simple preparatory phase

➢ The targeted information system can be:

- **A network**
- **A machine,**
  - an operating system
  - An application

IDS, why?

➢ Why look for signs of intrusion if we are protected?

➢ Principle of ‘key and camera’: protection AND detection

➢ Perimeter: we often opt for protection ‘at the edge’ of the system, but detection can happen at its core.

➢ e.g. firewall protecting the LAN from the Internet, and NIDS on the LAN

controlling the activity of local users.

How to detect an intrusion?

- ➢ By monitoring system activity (network, machine or application) in order to gather various events
- ➢ By analysing these events for suspicious signs
- ➢ IDS aim to automate these phases of information collection and analysis.

How to detect an intrusion?

- An IDS is essentially a sniffer paired with a engine that analyses traffic according to rules
- These rules describe traffic to be reported
- The IDS can analyse
  - Network Layer (IP, ICMP)
  - Transport Layer (TCP, UDP)
  - Application Layer (HTTP, Telnet)

And after detection?

- Understand the ongoing attack
- Gather as much information as possible:
  - Target(s)
  - Source(s)
  - Method
- Archiver, tracer: correlation with other events
- Prepare a response:
  - in the short term: blacklisting,…
  - in the long term: application of patches, legal action...

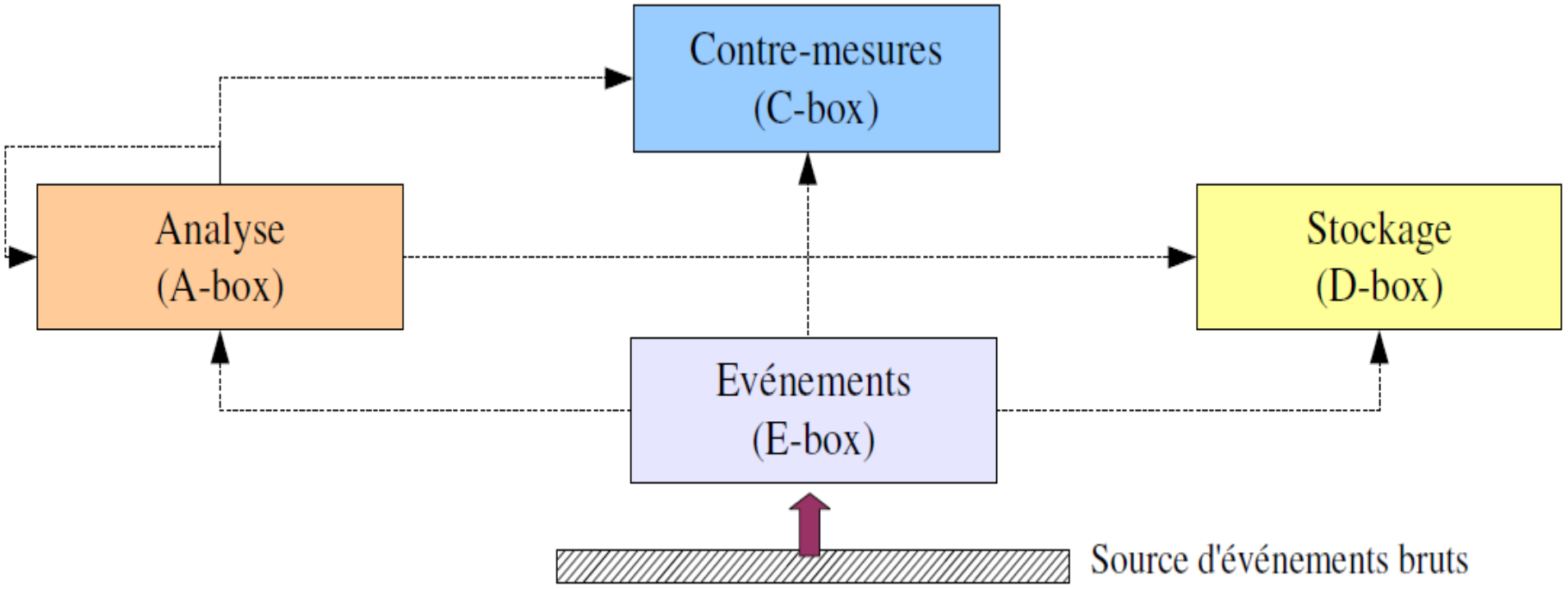
Normalisation: CIDF

➢ CIDF: Common Intrusion Detection Framework

➢ This model defines the components of an IDS:

- event generator: Ebox
- event analyser: Abox
- information storage: Dbox
- countermeasure

Normalisation: CIDF



A bit of vocabulary

- **False positive:**
  - false alert raised by the IDS
- **False negative:**
  - attack (in a broad sense) that was not detected by the IDS
- **Attack signature:**
- An attack signature is a pattern (behaviour pattern) representing all the information regarding a known attack.
- Probe: component of the IDS architecture that collects raw information

Type of monitored information system

- Network
  - NIDS: Network Intrusion Detection System
  - principle: monitor network trafic content
  - a probe can monitor multiple machines
- System
- HIDS: Host-based Intrusion Detection System
  - principle: monitor system activity
    - Logs
    - Files
    - processes
  - a machine requires its own probe
- Application

- sub-type of the HIDS

Intrusion detection method

1. Signature-based intrusion detection
2. Intrusion detection by anomaly
3. What to choose?

Signature-based intrusion detection 1/2

➢ The simplest method, based on pattern recognition

➢ if Event matches Signature then Alert

➢ Easy to implement, for any type of IDS

➢ The effectiveness of these IDS is linked to the management of the signature database

- Update
- number of rules
- sufficiently precise signatures

➢ Examples:

find the pattern /winnt/system32/cmd.exe in an HTTP request

find the pattern FAILED su for root in a system log

Signature-based intrusion detection 1/2

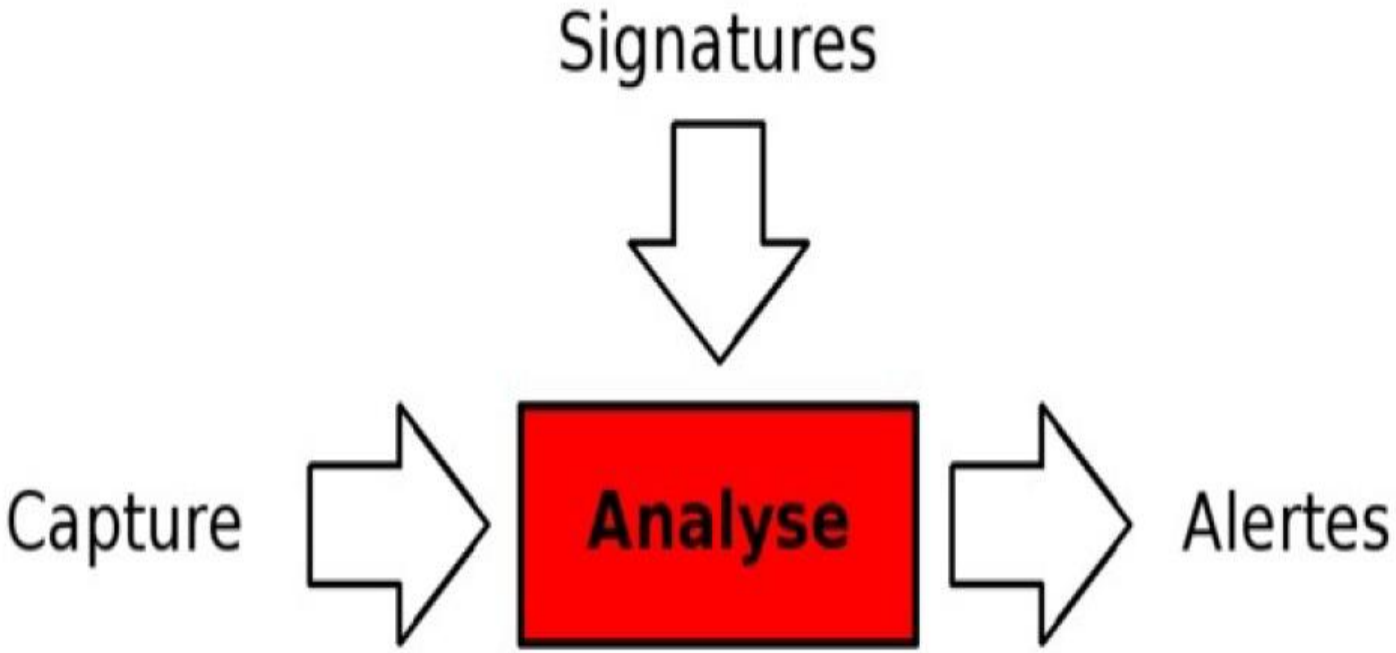


Figure 1.1: Le fonctionnement du NIDS

Capture

- Capture is used to retrieve network traffic. Generally, this is done in real time.
- Its operating mode is to copy every packet arriving at the data link layer of the operating system.
- Some packets may be ignored because under heavy load, the OS will no longer copy them.

Signatures

- Signature libraries make the analysis process similar to that of antivirus software when they rely on attack signatures.
- Thus, the NIDS is effective if it knows the attack, but ineffective otherwise.
- Signature-based tools require very regular updates.
- NIDS have the advantage of being real-time systems and have the capability to discover attacks targeting multiple machines simultaneously.

Analysis

➢ There are 2 types of network analysis

  ➢ by packet: macroscopic view, many possibilities

  ➢ by flows: global view of network activity

  ➢ For packet analysis, one can focus on different layers, each capable of providing relevant information

- ***anomalies at the header level of a packet***
- exotic combinations of TCP flags
- bad checksum
- ***anomalies in protocol behaviour***
- inconsistencies in TCP sequence and acknowledgement number
- ***malformed application layers***
- suspicious SMTP negotiation
- suspicious data

Protocol analysis

- ➢ ARP
  - null address
  - source address as ff:ff:ff:ff:ff:ff
- ➢ IP
  - bad checksum
  - incorrect packet size
  - nconsistent address
- ➢ UDP
  - bad checksum
- ➢ TCP
  - bad checksum
  - incorrect header size
  - Inconsistent flags

Data analysis

➢ Here, it is about searching for suspicious strings in the data (payload) that correspond to known attacks.

➢ Example:

- if the layer 4 protocol is TCP
- if the port for the connection is port 80
- then the application protocol is HTTP
- if furthermore, the request in the URL contains the string cmd.exe
- then it is likely an attack
- an alert will then be raised based on a request such as:

http://www.server.net/path/to/cmd.exe

Intrusion detection by signature 2/2

- ➢ Advantages
  - simplicity of implementation
  - speed of diagnosis
  - accuracy (depending on the rules)
  - identification of the attack method
    - ➢ method
    - ➢cible(s)
    - ➢source(s)
    - ➢outil ?
  - ➢ which makes it easier to respond to incidents
- ➢ Disadvantages
  - Only detects attacks known to the signature database :cannot detect zero-day attacks,
  - Database maintenance :requires regular updates
  - Evasion techniques possible once signatures are known

Intrusion detection by anomaly 1/2

- ➢ This is also referred to as behavioural intrusion detection.
- ➢ System modelling: creation of a normal profile.
- ➢ Learning phase to define this profile.
- ➢ Intrusion detection will consist of detecting a suspicious deviation between network behaviour and its profile.
- ➢ Profile examples: network traffic volume, application system calls, typical user commands, etc.
- ➢ Based on tools of varying complexity
  - Thresholds
  - Statistics
  - Probabilistic methods
  - Neural networks
  - Support vector

Intrusion detection by anomaly 1/2

➢ ***Advantages***

- Enables detection of attacks that are not known in advance.
- Facilitates the creation of rules adapted to these attacks.
- Difficult to deceive.

➢ ***Disadvantages***

- False positives are relatively numerous.
- Generating a profile is complex:
  - Length of the learning phase.
  - Healthy system activity during this phase?
- in the event of an alert, a precise diagnosis is often necessary to clearly identify the attack

What to choose ?

Choose SIGNATURE-BASED IDS when:

- Limited security expertise
- Predictable Environment
- Budget Constraints
- Need for Immediate Protection

What to choose ?

Choose ANOMALY-BASED IDS when:

- **Advanced Persistent Threats (APTs) are Concern**
  - Need to detect sophisticated, novel attacks, Targeted industry (finance, defense, critical infrastructure)

Dynamic Environment

Cloud-native, microservices architecture, Frequent infrastructure changes

- S**trong Analytics Capability**
  - Have data scientists or ML engineers, existing SIEM/log analysis infrastructure

What to choose ?

Hybrid Approach: The Best of Both Worlds

Layered Defense Strategy

Tier 1: Signature-based IDS

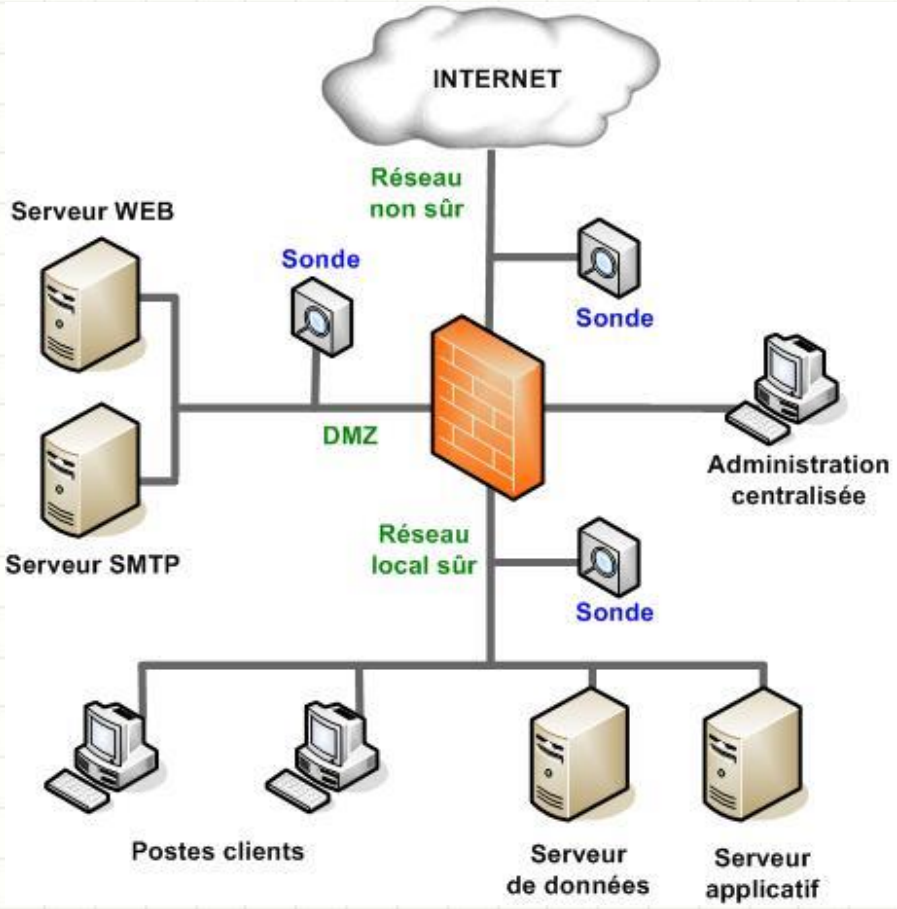
- First line of defense
- Catches known threats efficiently
- Low false positives

Tier 2: Anomaly-based IDS

- Secondary analysis
- Detects novel attack patterns

NIDS : Network Intrusion Detection Systems

IDS – Levels – Network



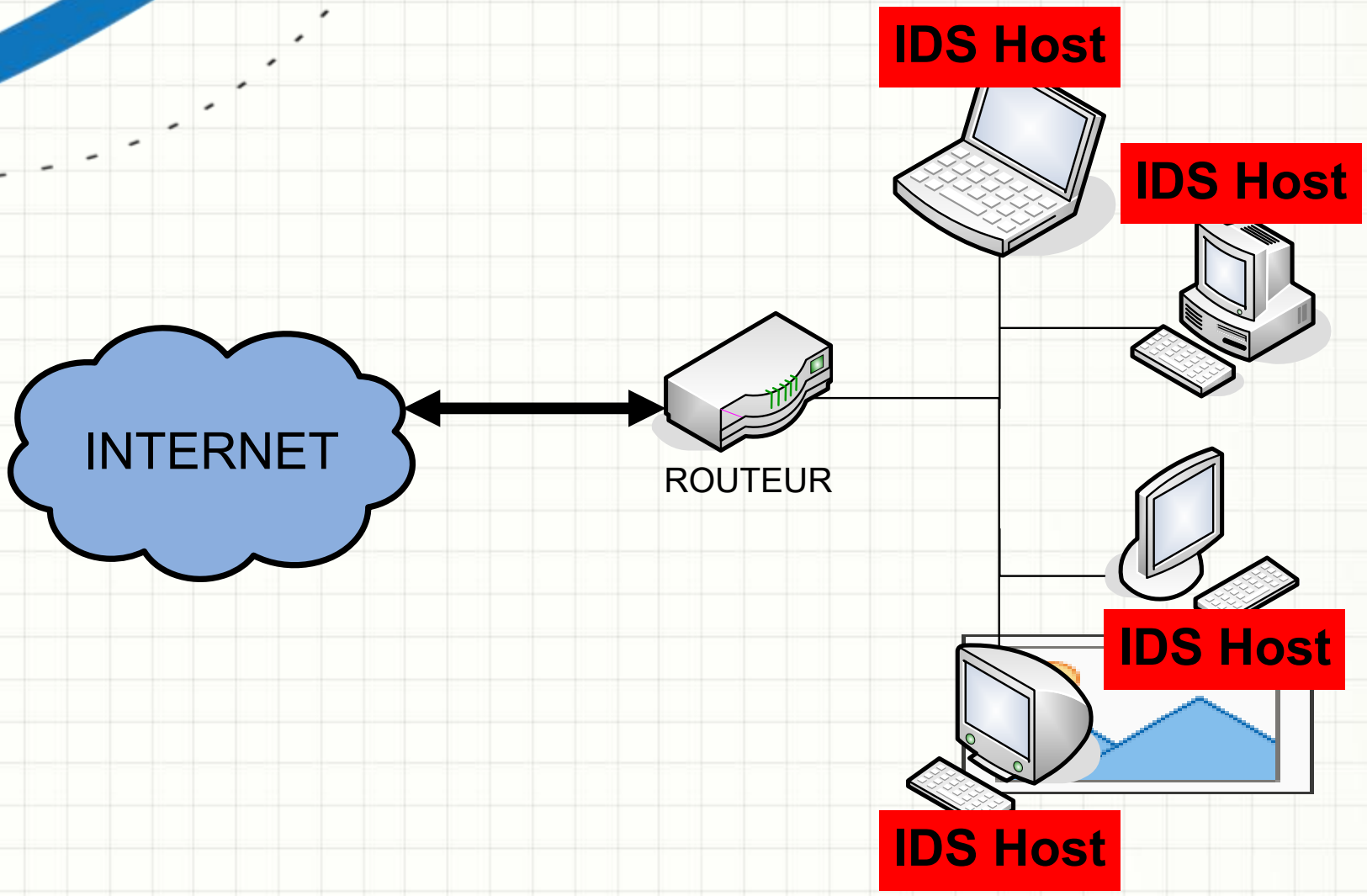
Objectives of a NIDS

- NIDS are used to monitor network activity
- of varying size
  - from a simple LAN without routing
  - to an enterprise network with thousands of machines and several hundred subnets
- at strategic points
  - on the periphery of the network
  - controlling the flows exchanged with the outside
- at the core of the network
  - monitoring the behaviour of internal users
  - looking for potential intrusions
- using various techniques
  - packet analysis
    - Stateless
    - stateful (reconstructing flows)
  - flow analysis

Some tools

- Main free NIDS
- Snort
- Bro
- Prelude IDS
- Some manufacturers integrate IDS modules into their **equipment (routers, firewalls)**
- It should be noted that many network administration tools can be used as building blocks of a NIDS architecture
- Arpwatch
- p0f
- ntop

HIDS: Host-based Intrusion Detection Systems


IDS Host
IDS Host
INTERNET
ROUTEUR
IDS Host
IDS Host

HIDS: Host based Intrusion Detection Systems

➢ An integrity check will involve verifying, by a given method, that specific files in the system have not been altered.

➢ Before proceeding with this type of check, the access to these files needs to be maximally secured:

➢ permissions on the files, parent directories

➢ data storage on physically read-only accessible devices (CDs, disks...)

➢ mounting specific partitions as read-only

➢ We can then tackle the integrity check!

HIDS: Host based Intrusion Detection Systems

➢ To detect changes on a file, we have the following methods available:

➢ **comparison with copies**

- Principle:
  - keep copies of critical files
  - periodically compare the file on the system and the copy

➢ this is the most effective method for detecting if there has been a modification, and what modification!

but it is extremely cumbersome to implement

- storage capacity for the copies
- system resources to perform the comparisons

➢ where to store the copy?

- on the system itself, in a dedicated directory
- on a removable device (read-only)
- on a hard drive that can be mounted by the system
- on the network (comparison with an NFS export for example)

➢it is crucial that the copy cannot be altered!

HIDS: Host-based Intrusion Detection Systems

➢ **comparison of file attributes**

➢principle:

➢record distinctive fields of the files to be checked

➢compare these fields to the original values

➢note any unusual modifications

➢lighter than the previous method, this process does not allow seeing what modifications were made to the files

➢can, however, detect changes other than the file's content

➢many parameters can be taken into account:

- Owner
- Permissions
- Size
- creation dates, last modification dates...

HIDS: Host-based Intrusion Detection Systems

➢ **signature comparison**

➢principle:

- a signature of each file to be protected is calculated using a cryptographic function, such as md5
- the current checksum of the file is periodically compared with the original value

➢light and easy to deploy, this method allows for the detection of modifications to a file's content, not its attributes

➢requires a sufficiently strong algorithm

➢the reference file must not be modifiable!

Intrusion Detection Systems Specific IDS: Honeypots & IPS

- **What is a honeypot?**
- ➢ A honeypot is a security resource whose value lies in being probed, attacked or compromised.
- *L. Spitzner*
- ➢ The approach is therefore to offer an information system as bait to attackers.

Objectives

- A specific IDS: any interaction with the honeypot is suspicious since it is not a system expected to converse with the world.
- Reduction of false positives
- This is not a production system but a lure: dedicated resources
- Occupy the hacker
- The honeypot can waste an attacker's time
- Discoveries of new vulnerabilities or exploits
- Assistance in generating new signatures

In practice: examples

- Setting up a low-interaction honeypot
- Tools
- The most basic: netcat on a particular port
- More comprehensive: emulation of services, machines, networks with honeyd
- Risks
- They primarily depend on the application used for emulation
- Setting up a high-interaction honeypot
- Providing a real OS to hackers
- A poorly secured machine (old OS, vulnerable services...)
- Using a virtual machine (VMWare, User Mode Linux)

IPS: Intrusion Prevention System

- The Intrusion Prevention System (IPS) is a proactive defence tool against active attacks targeting computers and networks. This network device monitors the activities of a network or system to identify malicious or undesirable behaviours and can block them.

- Course questions 9
- Q1: Why add an IDS in a network protected by a firewall?
- Q2: List the components of a CIDF standardised IDS
- Q3: What is the difference between false positives and false negatives?
- Q4: How to detect an intrusion? Q5: List the intrusion detection methods and the advantage of each in relation to false positives and false negatives.

- Q6: How to improve the effectiveness of each method
- Q7: List the HIDS intrusion detection methods
- Q8: What is a honeypot IDS?