PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
Ministry of Higher Education and Scientific ResearchAbbes
Laghrour University of Khenchela

Faculty of Science and Technology
Department: math and computer science

Master's degree in Computer Science
Option Software Engineering and
Distributed Systems

Theme

A coordinate approach in intrusion detection systems

Presented by:

- **M.** Bouchareb Abir Nihal
- **M.** Hanou Selma

Members of the jury

- **PRESIDENT:** Souidi Mohammed El Hat
- **The framer: M.** Khiar Abdelouaheb
- **EXAMINATOR:** Haouassi Hichem

2021/2022 promotion

Acknowledgements

As a preamble to this work we thank Godwho helps us and gives us patience and courage during these years of study. We would like to thank Mr. Khiar Abdelouaheb for having followed us during my work on this thesis, for his precious advice, and the competence of his supervision.

We would like to express our sincere thanks to all the professors who have taught us and who by their competence have supported us in the pursuit of ourstudies.

I dedicate this modest work to

My dear parents. My mother and my father for their patience, their support and their encouragement.

To all my family

To my sisters.

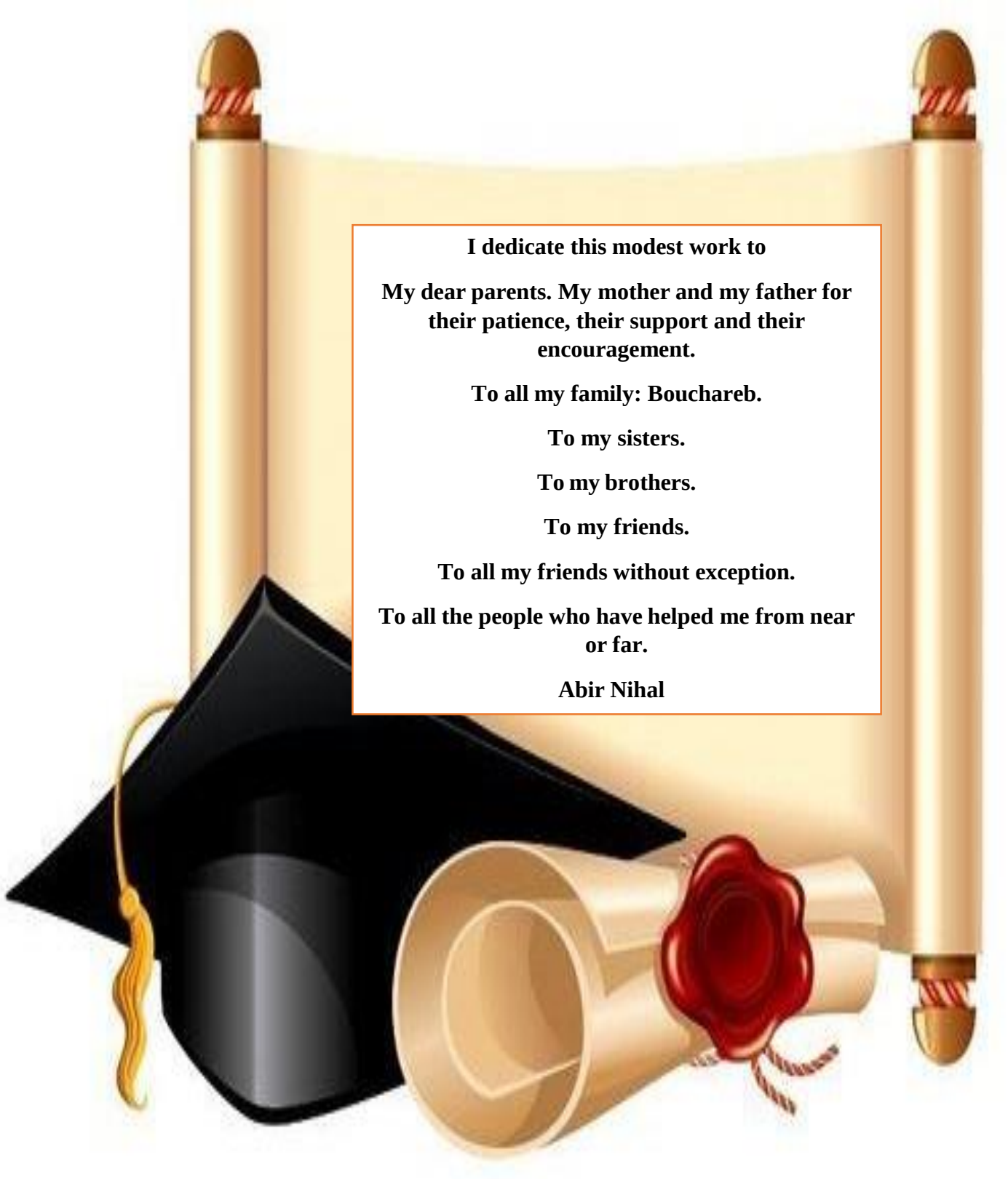
To my brothers.

To my friends.

To all my friends without exception.

To all the people who have helped me from near or far.

Salma



I dedicate this modest work to

My dear parents. My mother and my father for their patience, their support and their encouragement.

To all my family: Bouchareb.

To my sisters.

To my brothers.

To my friends.

To all my friends without exception.

To all the people who have helped me from near or far.

Abir Nihal

Table of contents

Table of contents

Table of figures

List of Abbreviations

ACID	**A**nalyze **C**onsol for **I**ntrusions **D**atabase
ARP	**A**ddress **R**esolution **P**rotocol
CD ROM	**C**ompact **D**isc **R**ead **O**nly **M**emory
CERT	**C**omputer **E**mergency **R**esponse **T**eam
CIDR	**C**lassless **I**nter-**D**omain **R**outing
CPU	**C**entral **P**rocessing **U**nit
DAQ	**D**ata **A**cquisition
DDoS	**D**istributed **D**enial **o**f **S**ervice
DMZ	**D**e **M**ilitarized **Z**one
DNS	**D**omain **N**ame **S**ervice
DVD	**D**igital **V**ersatile **D**isc
FTP	**F**ile **T**ransfer **P**rotocol
H-IDS	**H**ost **B**ased **I**ntrusions **D**etection **S**ystem
HTTP	**H**yper **T**ext **T**ransfer **P**rotocol
HTTPS	**H**yper **T**ext **T**ransfer **P**rotocol **S**ecure
ICMP	**I**nternet **C**ontrol Message **P**rotocol
IDS	**I**ntrusions **D**etection **S**ystem
IDWG	**I**ntrusions **D**etection exchange format **W**orking **G**roup
IETF	**I**nternet **E**ngineering **T**ask **F**orce
IGRP	**I**nterior **G**ateway **R**outing **P**rotocol
IP	**I**nternet **P**rotocol
IPS	**I**ntrusions **P**revention **S**ystem
IPSec	**I**nternet **P**rotocol **S**ecurity
IPX	**I**nternetwork **P**acket **E**xchange
ISS	**I**nternet **S**ecure **S**ystem
LAN	**L**ocal **A**rea **N**etwork
NFS	**N**etwork **F**ile **S**ystem

List of Abbreviations

N-IDS	**N**etwork **B**ased **I**ntrusions **D**etection **S**ystem
NMAP	**N**etwork **M**ap per
NTP	**N**etwork **T**ime **P**rotocol
OSPF	**O**pen **S**hortest **P**ath First
OSI	**O**pen **S**ystems **I**nterconnection
PHP	**H**ypertext **P**reprocessor
POP3	**P**ost **O**ffice **P**rotocol **V**ersion 3
PSSI	Information Systems Security Policy
RIP	**R**outing **I**nformation **P**rotocol
RPC	**R**emote **P**rocedure **C**all
SI	Information System
SGBD	Database Management System
SSH	**S**ecure **S**hell
SSI	Information Systems Security
SSL	**S**ecure **S**ocket **L**ayer
TCP	**T**ransmission **C**ontrol **P**rotocol
TLS	**T**ransport **L**ayer **S**ecurity
UDP	**U**ser **D**atagram **P**rotocol
URI	**U**niform **R**esource **I**dentifier
URL	**U**niform **R**esource **L**ocator
USB	**U**niversal **S**erial **B**us
VPN	**V**irtual **P**rivate **N**etwork

General Introduction

I. General Introduction

Computer networks have become much more important than they were a few years ago. Today companies from the very beginning do not hesitate to set up an IT network to facilitate the management of their infrastructure, which is why the security of these networks is a crucial issue.

Computer security is the set of technical, legal and human organizational means necessary to prevent the unauthorized use, modification or misappropriation of a system. Security involves the deployment of technical means but also, and above all, prevention, which must take into account the training and awareness of all the actors in the system, as well as the rules and good practices that must be put in place in order to avoid creating breaches and human attacks.

Two non-exclusive approaches are possible: the prevention of attacks and their detection. The firstapproach, by applying a priori control on the actions carried out within the system, ensures that users will not be able to violate the policy. This approach prevents the system from being in a corruptstate, requiring analysis and correction. As a result, preventive mechanisms are present on computersystems, often in the form of access control. However, such mechanisms have their own limitations,which may relate to theoretical aspects of underlying models or their implementation. In this context, IDSs are an alternative way of protecting the IT network.

An intrusion detection system (IDS) is a mechanism that listens to network traffic in a stealth manner in order to detect abnormal or suspicious activities and to have a preventive action on therisks of intrusion.

In this project, we will focus on network intrusion detection (IDS) tools in particular for snort, which can detect real-time network intrusions.

II. The objective of our work is:

Study the general Information on Computer N e t w o r k s and Security levels.

Study and analyze all aspects handled by an intrusion detection system (IDS)/ network intrusion prevention.

A security system and multi-agent systems (SMA).

Case study: snort.

Installing and configuring snort, linking snort with database.

We have structured our submission into five chapters:

In the first chapter, we present a general study of computer networks. We discuss computer security.

The second chapter is about devoted to the study of intrusion detection systems, its various variants and detection methods.

The third chapter is about multi-agent systems (SMA).

The fourth chapter consists of the implementation of Snort, which is an open source system for intrusion detection. We will start by giving a general presentation of SNORT, and then we will present its handling: installation, configuration and finally the features. The last chapter about our work. The IDS (Snort) uses performance in coordination system.

Chapter1: General Information on computer networks and security levels

I. Introduction

The network is a set of objects connected or maintained in connection. Previously, communications between different machines were just intended for the transport of computer data whereas today network sallow the sharing of resources that integrate other types of data such as speech and video.

In this first chapter, we describe the basic theoretical concepts about computer networks ingeneral. To do this, first, we present the types of computer networks, and then we give an overview of the different layers of the model OSI. Finally, we mention the communicationprotocols for routing data between networks, as well as the equipment used.

1. Computer networks: [1]

A computer network is a set of computers (or computer equipment) that are interconnected through standardized communication protocols. It is used for the exchange of digital data and the sharing of resources (printers, disks ...) between computer systems and applicationssuch as word processors, or browsers Web.

2. Classification of networks:

Computer networks can be divided into several types: according to their extent, their architectures and their topologies (See Figure1.1).

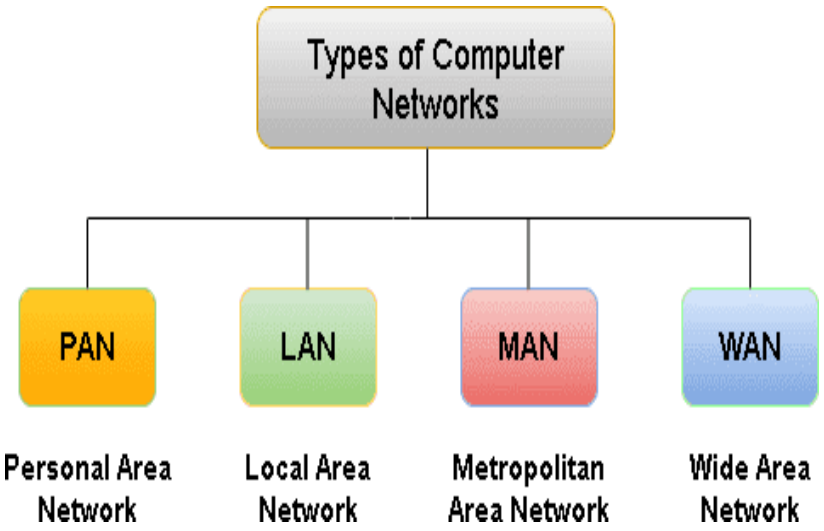


Figure 1.1: The different networks. [1]

3. The OSI model :

The OSI is a basic model standardized by the international standard organization; it was standardizedto work with a single communication model a network architecture using these different functions, which are organized in seven numbered layers. [1]
These layers are sometimes divided into two groups as the architecture table shows us below:

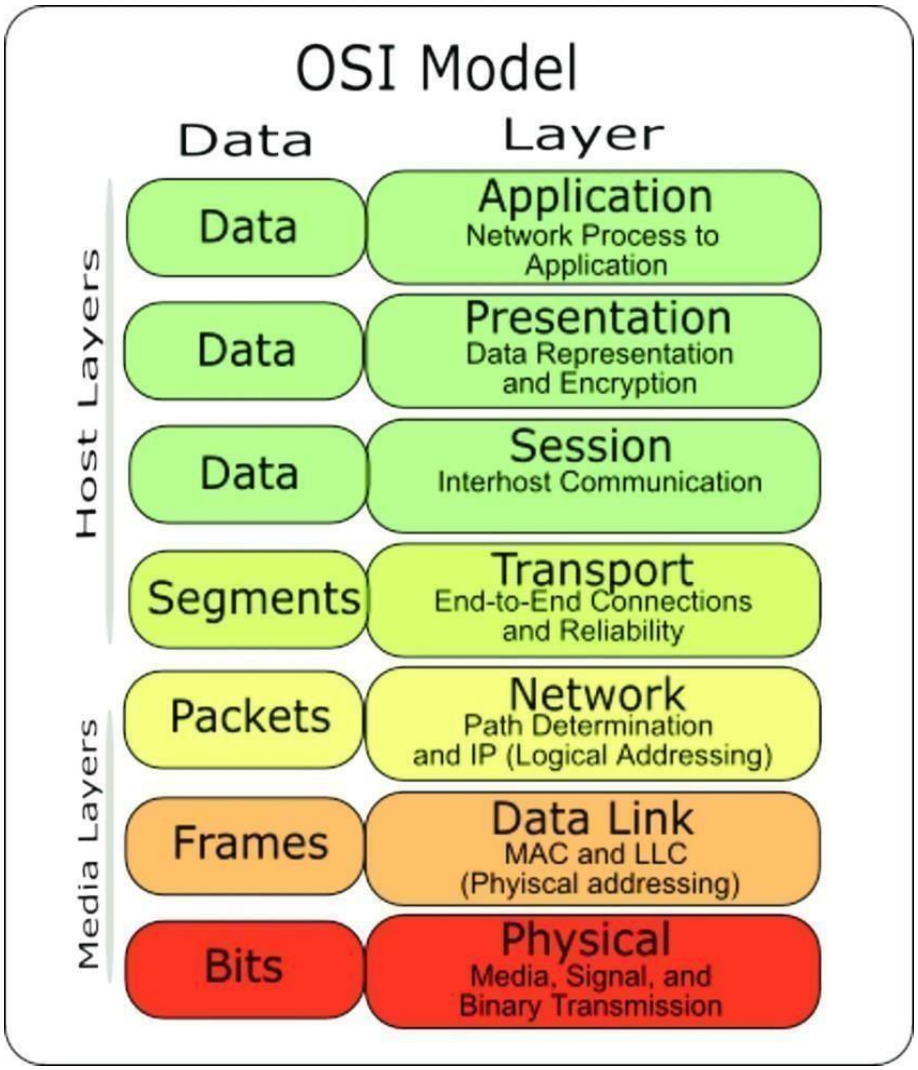


Figure 1.2: OSI model. [2]

4. TCP /IP: [3]

TCP/IP is the set of protocols used for data transfer over the internet. It is often called TCP/IP, basedon the name of its first two protocols:
TCP (Transmission Control Protocol) and IP (Internet Protocol).
The IP (Internet Protocol) layer, also known as the low layer, is mainly concerned with managing logical addressing and ensuring the routing of packets from one node to another.
The TCP (Transmission Control Protocol) layer, called the high layer, handles errors and controls the flow by setting up mechanisms for repeating packets and adjusting the reception

window (that is, the number of packages that can be received before validating/invalidating them).

The TCP/IP model has four layers: the application layer, the transport layer, the Internet layer and the network access layer (see Figure I.3). Some layers of the TCP/IP model have the same name as layers of the OSI model, but they have different functions that are mentioned below.

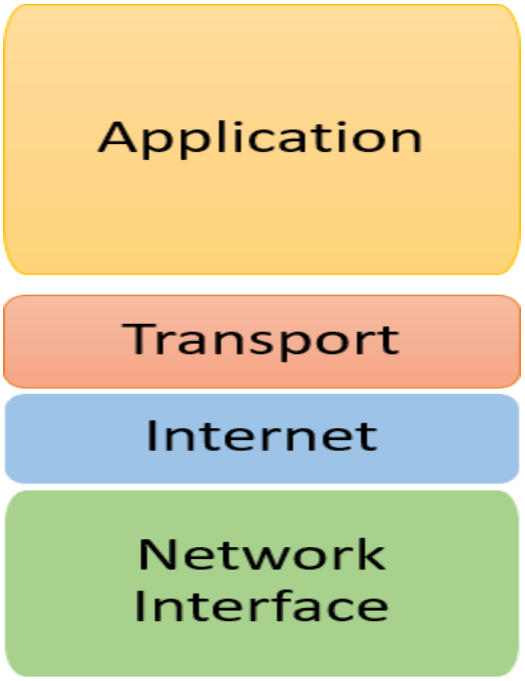


Figure 1.3: TCP Model Standard. [4]

4.1. Application Layer:

It is located at the top of the TCP/IP protocol layers. It contains network applications to communicatethrough the lower layers.

The application layer manages the high-level protocols: representation, coding and control of the dialogue. [2]

4.2. Transport layer:

The transport layer provides end-to-end communication by ignoring the intermediate machines between the sender and the receiver.[3]

The transport layer contains two protocols allowing two applications to exchange data; in the case ofTCP (Transmission Control Protocol), it regulates the flow of data and ensures reliable transport (data transmitted without error and received in the order in which it was sent) and unreliable in the case of UDP (User Datagram Protocol). It is not guaranteed that a packet (called a datagram in this case) will arrive at its destination; it is up to the application layer to ensure this.[4]

4.3. Internet layer:

The role of the Internet layer is to send source packets from any network in the inter-network and getthem to their destination, regardless of the path and networks traversed to get there.

The protocol that governs this layer is called Internet Protocol (IP). Identification of the best path and packet switching take place at this layer.[3]

4.4. Network access layer:

This is the first layer of the TCP/IP stack, and takes care of everything that an IP packet needs toestablish physical link. It supports the following concepts:

- Routing of data over the link.
- Coordination of data transmission (synchronization).
- Signal conversion (analogue to digital).
- Error checking on arrival.

5. Data encapsulation:

During a transmission, the data passes through each of the layers at the transmitting machine. At each layer, information is added to the data packet, it is a header, a set of information that guarantees the transmission. At the receiving machine, when passing through each layer, the headeris read and then removed. Thus, on reception, the message is in its original state. (See figure 1.4). [4]

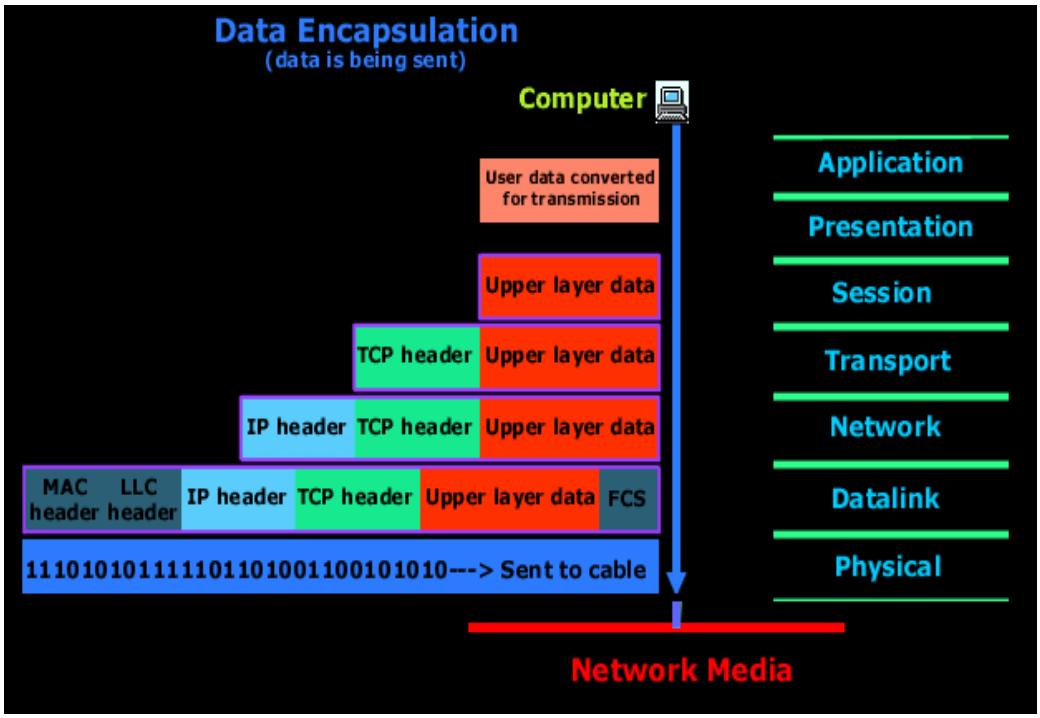


Figure 1.4: Data encapsulation. [5]

II. Network security

6. Definition

The security of a network is a set of technical, organizational, legal and human means necessary and put in place to maintain, restore and guarantee its security against accidental or intentional threats. In general, the security of a network includes the security of the computer system on whichit is based. [6]

7. Assessing network security

The security of a network can be evaluated on the basis of a number of security criteria. There aregenerally three main security criteria [6]:

Availability: It consists in guaranteeing access to a service or a resource.

Integrity: This consists of ensuring that the data has not been altered during communication (either accidentally or intentionally).

Confidentiality: This consists of making the information unintelligible to anyone other than the actors involved.
In addition to these three criteria, we can add the following criteria:

Authentication: It consists in assuring the identity of a user, i.e. to guarantee to each of the correspondents that his partner is indeed, who he thinks he is.

Non-repudiation: It consists in guaranteeing that none of the correspondents can deny the transaction.

The evaluation of the security of a computer system is a very complex process based in general on a methodology. This evaluation passes by an analysis of risks. The latter is based on a set of rules defined beforehand. [6]

8. Causes for securing networks

8.1. Vulnerabilities

All computer systems are vulnerable. It does not matter how vulnerable they are. Vulnerability is aflaw or weakness that can be exploited by a malicious person to do harm.
System vulnerabilities can be categorized into human, technological, organizational, and implementation. [6]

- Human vulnerabilities
- Technological vulnerabilities
- Organizational vulnerabilities
- Implementation vulnerabilities

8.2. Threats

A threat is an event, of accidental or deliberate origin, capable of causing damage to the Subject studied. The computer network, like any other computer network, is prey to threats of all kinds that should be identified. [6]

Threats can also be classified into two categories:

- **Passive threats:** essentially consist of copying or listening to information on the network, they harm the confidentiality of data. In this case, the person who takes a copy does not alter the information itself.
- **Active threats:** consist in altering information or the proper functioning of a service. [6]

8.3. Malicious software

This is software developed by hackers with the aim of damaging an information system.

- **Viruses:** a virus is a program segment that, when executed, reproduces itself by joining another program (of the system or of an application), and thus becomes a Trojan horse. The virus can then spread to other computers (via a network) using the legitimate program on which it has been grafted. It can also have the effect of harming by disrupting the operation of the infected computer more or less severely. [7]
- **Worms:** a worm is a self-contained program that reproduces and spreads without the users knowledge. Unlike viruses, a worm does not need a host program to replicate itself. The worm usually has a malicious purpose.
- **Trojans**: A Trojan horse is a form of malware disguised as useful software. Its purpose is tobe executed by the user, allowing him to control the computer and use it for his own purposes. Usually other malware will be installed on your computer, such as enabling fraudulent collection, falsification or destruction of data. [6]
- **Spyware:** (Spyware or spyware) is a program or sub-program, designed with the purpose ofcollecting personal data about its users and sending them to its designer, or to a third party via the Internet or any other computer network, without having obtained prior explicit and informed permission of said users.
- **Spam:** corresponds to the untimely sending of electronic mail, advertising or not, to an e-mail address. Spam is a pollution of legitimate mail by a huge mass of unsolicited junk mail. [8]

9. Intrusions

An intrusion is defined as a malicious act of internal or external origin resulting from an attack thathas successfully exploited vulnerability. It is likely to produce errors that may cause a security failure, i.e. a violation of the system's security policy. The term intrusions will be used in the case where the attack is carried out successfully and the attacker has succeeded in breaking into and/or compromising the system. [9]

10. Attacks

10.1. Definition: An attack is defined as a malicious interaction designed to violate one or more security properties. It is an external fault created with the intention to harm, including attacks launched by automatic tools: worms, viruses, etc. The notion of attack should not be confused with the notion of intrusions. [9]

10.2. Type of attacks: hackers use several attack techniques. These attacks can be grouped into three different families: [10]

- Direct attacks
- Indirect bounce attacks
- Indirect response attacks:

Category of attacks: There are four categories of attacks: [11]

- Attacks by interruption
- Attack by interception.
- Attack by modification
- Manufacturing attack

11. The means of securing a network

The security of a network is the security of the elements that compose it; there are several mechanisms and security devices, among them:

11.1. Antivirus

Antivirus software is designed to identify, neutralize and eliminate malicious software. These canbe based on the exploitation of security flaws, but they can also be programs that modify or deletefiles, whether they are documents of the user of the infected computer, or files necessary for the proper functioning of the computer.

An antivirus checks files and e-mails, boot sectors (to detect boot viruses), but also the computer's RAM, removable media (USB sticks, CDs, DVDs, etc.), data passing through any networks (including the Internet), etc.

11.2. System updates

To avoid application denial of service, you must keep all the software on your system up to date, since updates often correct software flaws that can be used by an attacker to disable the application, or worse, the server. It is therefore imperative to update your system very regularly. This is a very simple way to protect yourself from application attacks. Edit options in the configuration files that store data about each connection received by the machine such as the source IP address, the port number, the age of the connection. By analyzing this data, we can easily detect suspicious behavior and avoid certain types of attacks.

11.3. Firewalls

A firewall is a system that protects a computer or a network of computers from

from a third party network (especially the Internet). The firewall is a system that filters the data packets exchanged with the network. It is a filtering gateway with at least the following network interfaces

- an interface for the network to be protected (internal network); an interface for the external network

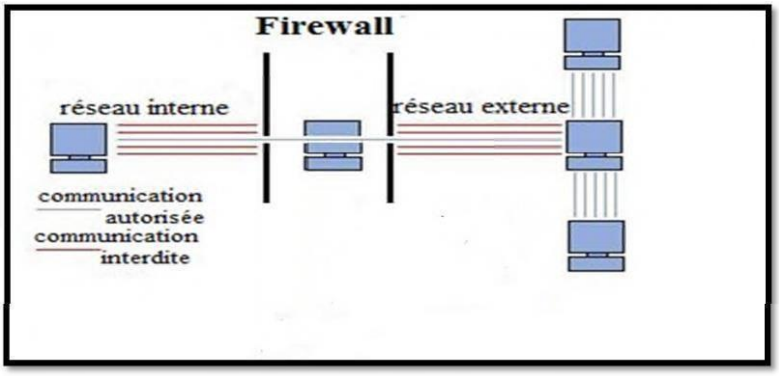


Figure 1.5: Firewall

The firewall system is a software system, sometimes based on dedicated network hard ware, which acts as an intermediary between the local network (or the local machine) and one or more external networks. It is possible to put a firewall system on any machine and with any system provided that:

- The machine is powerful enough to handle the traffic ;
- The system is secure;
- No other service than the packet filtering service is running on the server.

11.3.1. How a firewall system works

A firewall is a set of different hardware (physical) and software (logical) components that controlinternal/external traffic according to a security policy. A firewall system works most of the time thanks to filtering rules indicating the IP addresses authorized to communicate with the machineson the networks; it is thus a filtering gateway.

On the one hand, it allows blocking attacks or suspicious connections from accessing the internal network.

On the other hand, a firewall is also used in many cases to prevent uncontrolled leakage of information to the outside. It offers a real control over the network traffic of the company; it allows to analyze, to secure and to manage the network traffic.

12. DMZ architecture

A DMZ (Demilitarized Zone) is an area of a corporate network, located between the local networkand the Internet, behind the firewall. It is an intermediary network regrouping servers or services (HTTP, DHCP, mails, DNS, etc.). These servers must be accessible from the company's internal network and, for some, from external networks. The goal is to avoid any direct connection to the internal network.

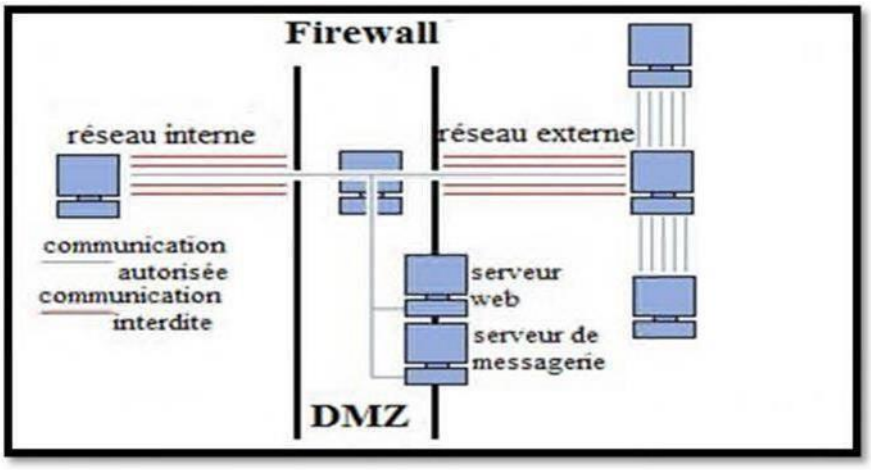


Figure 1.6: DMZ architecture

In computer networks, the Virtual Private Network (VPN) is a technique that allows remotestations to communicate securely, while using public infrastructures (Internet). [12]

12.1. VPN

A VPN relies on a protocol, called a tunneling protocol, that is, a protocol allowing data passing from one end of the VPN to the other to be secured by cryptographic algorithms. [12]

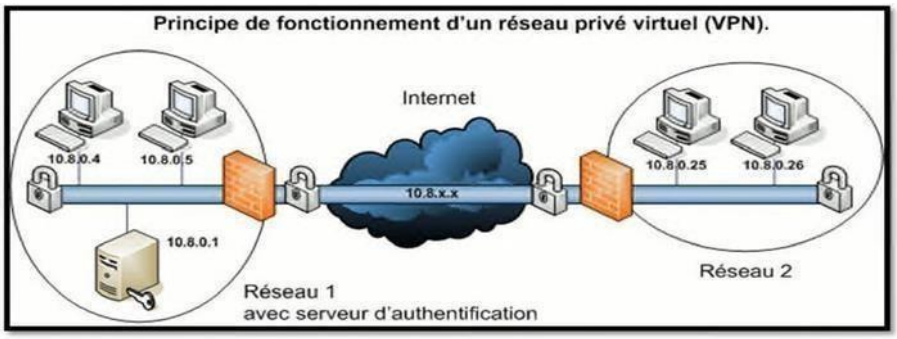


Figure 1.7: Principle of a VPN

13. IDS

Intrusion detection is defined as a mechanism that listens to network traffic in a stealthy manner, inorder to detect abnormal or suspicious activities and thus allow for a prevention strategy against therisk of attacks. There are different types of IDS, which are classified as follows:

- **Network Intrusion Detection System (NIDS):** a NIDS passively analyzes network traffic and detects intrusions in real time, in other words, a NIDS listens to all network traffic, then analyzes and generates alerts if packets appear to be dangerous.
- **Host-based Intrusion Detection System (HIDS):** A HIDS is typically placed on sensitive machines that are susceptible to attack and have sensitive corporate data.
- **Hybrid Intrusion Detection System:** A hybrid intrusion detection system is a system that is ableto combine information from both HIDS and NIDS.

Generally used in a decentralized environment, it allows gathering information from various probes placedon the network.

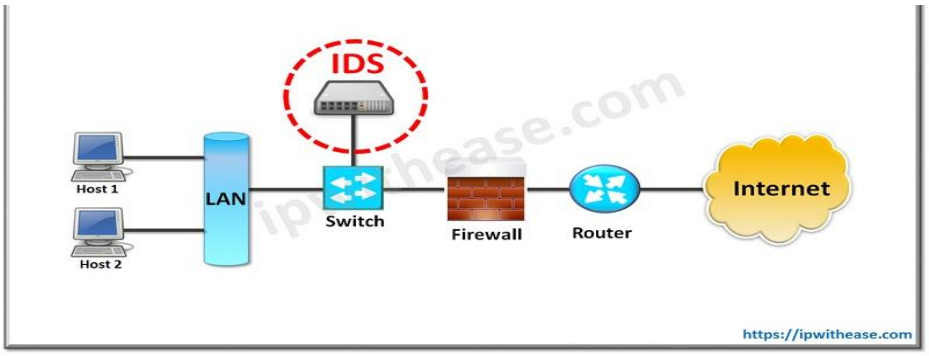


Figure 1.8: IDS

14. IPS

The IPS is an Intrusion Prevention/Protection System and not just intrusion recognition and reporting system like most IDS. The main difference between an IDS (network) and an IPS (network) is mainly due to two characteristics:

-The positioning of the IPS on the network and not only listening on the network for the IDS (traditionally positioned as a sniffer on the network).

-The possibility to immediately block intrusions regardless of the type of transport protocol used and without reconfiguring a third party equipment, which means that the IPS is natively constituted of a packet filtering technique and blocking means.

15. Security protocols

A protocol is a set of rules and procedures that must be followed to transmit and receive data on anetwork. On the Internet, the protocols used are part of a suite of TCP/IP protocols, such that mostof these protocols are not secure when transmitting data over the network. Secure protocols have been developed to encapsulate messages in encrypted data packets. These protocols include the following:

- **SSH (Secure Shell) protocol:** this is a protocol that allows TCP/IP services to access a machine through an encrypted communication called a "tunnel".
- **SSL (Secure Socket Layer) protocol:** this is a process for securing exchanges; it was designed to ensure the security of transactions carried out via the Internet.
- **HTTPS protocol:** HTTPS is nothing more than HTTP encapsulated in the TLS (Transport Layer Security) encryption layer. In general, an X509 certificate authenticates the server, the Internet user can authenticate himself through a RADIUS server, or by oneof the other processes proposed by the server software.
- **IPSec (IP Security):** IPSec (Internet Protocol Security) is designed to secure the IPv6 protocol. The slow deployment of the latter has forced IPSec to be adapted to the current IPv4protocol. A tunnel is established between two sites (see Figure 10.6), and IPsec managesall the security parameters associated with the communication. Two gateway machines, located at each end of the tunnel, negotiate the conditions for the exchange of information: which encryption algorithms, which digital signature methods and the keys used for these mechanisms. Protection is provided for all traffic and is transparent to the

various applications.

Discussion

In this chapter, we have presented the basic principles of computer networks (architectures, types, topologies...), also we have quoted the standard is models (OSI, TCP/IP) in detail; then the differentprotocols that count in a network and quote at least one protocol that belongs to each layer of the twomodels; as well as IP routing and we have presented an overview on computer security in a network.

To complete the information, we presented the network protocols that are used to transfer information. The development of the latter has posed major conflicts for users who are still confronted with an increase and growing complexity of intrusions and computer attacks in their networks

We have presented an overview of computer security in a network and the importance of implementing a security policy by outlining the needs and objectives to address the constant threats that a computer network is under. These threats are generally manifested in the form of computer attacks that we have illustrated in order to show the intensity of danger. Finally, we have proposed some existing solutions to protect and reduce the risks.

Chapter 2: Intrusion Detection System: IDS

Chapter 2: Intrusion Detection System: IDS

I. Introduction

The intrusion detection systems will fuse data from heterogeneous distributed network sensors tocreate cyberspace situational awareness.

In this chapter, we first introduce the concept of intrusion detection system (IDS) and its architecture. I also present the classification of IDS, in this framework several criteria are taken into account we start with the classification according to the method of analysis which divides the IDS into two approaches (behavioral and signature), finally we will focus on network intrusion detection.[w1]

1. Definition of an intrusion detection system

Intrusion detection is the process of monitoring events in a computer or network system and analyzing them for signs of intrusions, defined as attempts to compromise the confidentiality, integrity, availability or evasion of security mechanisms of the computer or network. Intrusion is caused by attacks accessing the system via the Internet, authorized user of the system trying to gain additional privileges for which they have not been authorized, and authorized users abusing the given privileges.
Intrusion detection system is a software or hardware that automates monitoring and analyzed processes. [13]

IDSs protect a system from attacks, misuse, and compromise. They can also monitor network activity, scan system and network configurations for vulnerabilities, analyze data integrity and more. Depending on the detection methods you choose to deploy, there are several direct and secondary benefits to using an IDS. An IDS has four main functions: analysis, logging, management and action.

- **Analysis:** Analysis of system logs to identify intent in the mass of data collected by the IDS. There are two methods of analysis: one based on attack signatures, and the other on anomaly detection.
- **Logging:** Recording of events in a log file. Examples of events: arrival of a packet, connection attempt.
- **Management:** IDSs must be managed on a permanent basis. An IDS can become pared toa security camera.
- **Action:** Alert the administrator when a dangerous attack is detected.

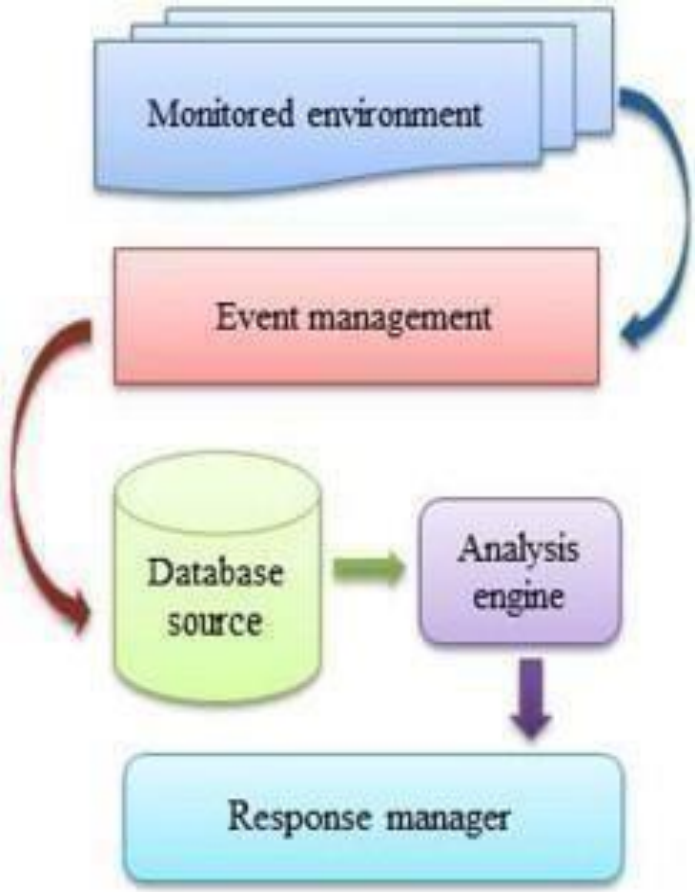


Figure 2.1: General IDS model [14]

2. IDS Detection Methods

To properly manage an intrusion detection system, it is important to understand how it works:

- How do you recognize/define an intrusion?
- How is an intrusion detected by such a system?
- What criteria differentiate a flow containing an attack from a normal flow?

These questions led us to study the internal functioning of IDSs. There are several methods for detecting an intrusion:

- The first consists of detecting signatures of known attacks in the packets circulating on the network: **The Scenario or Signature Approach.**
- The second is to detect suspicious activity in the user's behavior: **The Behavioral or Anomaly Approach. [15]**

These two techniques, as different as they are, can be combined within the same system to increase security.

2.1.Scenario or Signature Approach:

Signature based systems, which consist in searching the activity of the monitored element for signatures (fingerprints) of known attacks.
This principle of intrusion detection is reactive and poses several constraints, as it only detects the listed attacks for which it has the fingerprint. As a result, it requires frequent updates. This detection principle also implies that hackers can circumvent it by disguising their attacks, in fact, it modifies the signature known by the IDS and thus the attack becomes invisible by the IDS.

2.1.1. Scenario approach provides a clear diagnosis, so it is possible to react and counterattack, if the security policy is that way. However, they can only detect attacks contained in the knowledge base.The knowledgebase must be kept up to date at all times. It is possible to disable an IDS using thisapproach bya denial of service attack. [19]

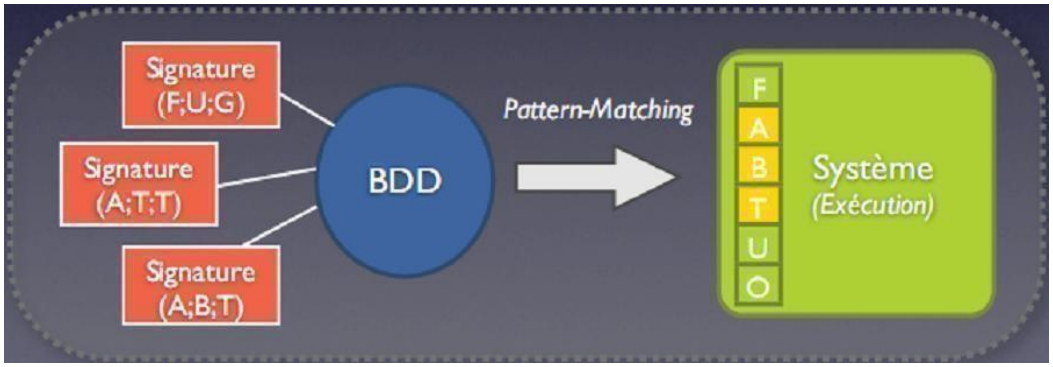


Figure 2.2: Scenario or signature approach

Three different methods to identify attacks:

- **MOTIVE ANALYSIS:** The simplest and most commonly used to detect an intrusion. A knowledgebase contains all the alphanumeric strings characteristic of an intrusion.
- **GENERIC RESEARCH:** Adapted for viruses. We look in the executable code for commands that are potentially dangerous. For example, an unreferenced DOS command is detected, email broadcasts, instructions related to known attacks.
- **INTEGRITY CHECK:** Performs a snapshot of all files on a system and generates an alert if any of the files are corrupted. MD-5 is the most frequently used but specialists now recommend SHA-256 and SHS - the hashes are signed and put in a safe and the new hashes are periodically compared to the signed hash. Today the best-known example using this approach is the SNORT IDS.

2.2.Behavioral approach (Anomaly Detection):

Behavioral approach systems consist in detecting various anomalies on the network. The administrator defines the "normal" operation of the monitored elements, so there is a learning phase to set this level. Subsequently, the IDS will be able to report to the administrator any situation that deviates from the reference level of operation. The reference operation can be elaborated by different statistical analyses of the element to be monitored. This detection system has an advantage over the previous one: it detects new types of attacks. However, sometimes adjustments will have to be made so that the baseline operation best matches the normal activity of the users and thus reduce the false alarms that would result from it.

IMMUNOLOGY (under study): Builds a model of normal service (not user) behavior. A service needs to be observed long enough under the right conditions to build a complete behavioral model.

2.2.1. The advantage of the behavioral approach is that it does not require a signature database. It therefore allows, in theory, to detect unknown attacks. What happens if there is an attack during learning? This is considered normal behavior and will never be detected. Also there is no interpretation of the attack; we don't know which attack was triggered. So we don't know how to react. It is very difficult to carry out a complete learning process.

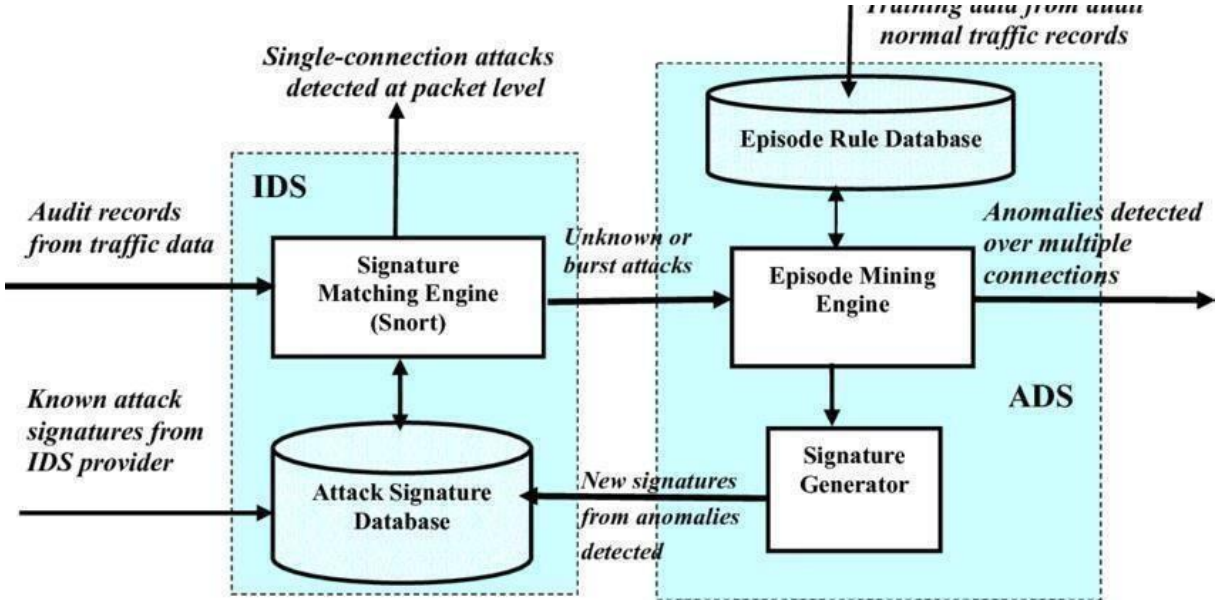


Figure 2.3: Illustration of the behavioral approach [17]

2.3.There are different techniques for identifying attacks:

2.3.1. PROBABILIST APPROACH:

One predicts what the probability of one event following another is. E.g: someone connecting to asite: high probability that the connection request will be followed by GET http://www.google.fr HTTP/1.0 and we can assume that HTTP/1.1 200 OK If this is not the case most of the time will follow it; we can have a doubt... [16]

Advantage:
- Simple and dynamic profile construction
- Reduction of false positives

Disadvantage:
- Risk of progressive deformation of the profile by repeated attacks.

2.3.2. STATISTICAL APPROACH:

Performs tests on other elements concerning the user:
- Memory occupancy rate.
- Processor usage.
- The value of the network load.
- The number of times the Internet is accessed per day. [18]

Advantage:
- Allows detection of unknown attacks.
- User habits learned automatically.

Disadvantages:
- Complexity in terms of maintenance.
- Many false positives.

3. IDS architecture

Several schemas have been proposed to describe the components of an intrusion detection system.Among them, we have chosen the one resulting from the work of the Intrusions Detection exchangeformat Working Group (IDWG) of the Internet Engineering Task Force (IETF) as a starting point,since it is the result of a broad consensus among the stakeholders in the field. [20]

The objective of the IDWG work is to define a standard for communication between certain components of an intrusion detection system. The figure illustrates this model and introduces a number of concepts:

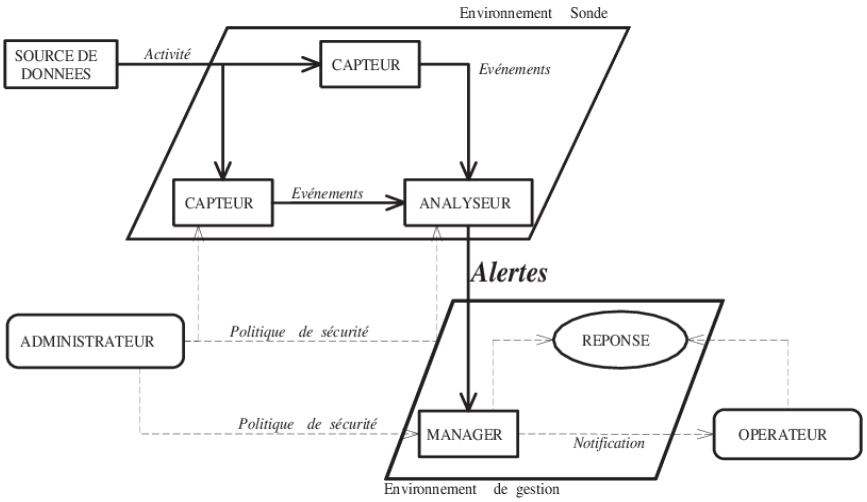


Figure 2.4: Generic model of intrusion detection proposed by the IDWG.

The IDWG architecture of an intrusion detection system contains sensors that send events to an analyzer. The sensors coupled with an analyzer form a probe, which sends alerts to a manager who notifies a human operator.

The different elements of this architecture

- **Administrator:** Person in charge of setting up the security policy, and consequently, of deploying and configuring the IDS.
- **Alert:** A formatted message issued by an analyzer if it finds intrusive activity in a data source.
- **Analyzer:** Software tool that implements the chosen approach to detection (behavioral or scenario-based), it generates alerts when it detects an intrusion.
- **Sensor:** software that generates events by filtering and formatting raw data from data source.
- **Event:** A formatted message returned by a sensor. It is the basic unit used to represent a step in a known attack scenario.
- **Manager:** A component of IDS that allows the operator to configure the various elements of a probe and to manage the alerts received and possibly the response.
- **Notification:** the method by which the IDS manager informs the operator of the occurrence of an alert.
- **Operator:** The person responsible for using the manager associated with the IDS. The operator proposes or decides on the reaction to be made in case of an alert. It is sometimes the same person as the administrator.
- **Reaction:** passive or active measures taken in response to the detection of an attack, to stop it or to correct its effects.
- **Probe:** a sensor or sensors coupled with an analyzer.
- **Data source:** a device generating information on the activities of the entities of the information system.

In this model, which represents the complete process of detection and data routing within an IDS? The administrator configures the different components (sensor(s), analyzer(s), and manager) according to a well-defined security policy. The sensors access the raw data, filter and format it to return only the events of interest to an analyzer. The analyzers use these events to decide whether an intrusion is present and if so, send an alert to the manager, who notifies the human operator, and a possible reaction can be carried out automatically by the manager or manually by the operator

An **IDS** is essentially a sniffer coupled with an engine that analyses the traffic and takes action according to the rules defined in the IDS. These rules describe the behavior of the IDS depending on the traffic **analyzed:** Alerts, logging of events in log files. An IDS can analyze the following layers:

- Network layer (IP, ICMP)
- Transport layer (TCP, UDP)

- Application Layer (HTTP, Telnet)
- Depending on the type of traffic, the IDS performs certain actions defined in the rules. Some terms are often used when talking about IDS:
- **False positive:** an alert from an IDS but which does not correspond to a real attack (False Alert).
- **False negative:** a real intrusion that was not detected by the IDS

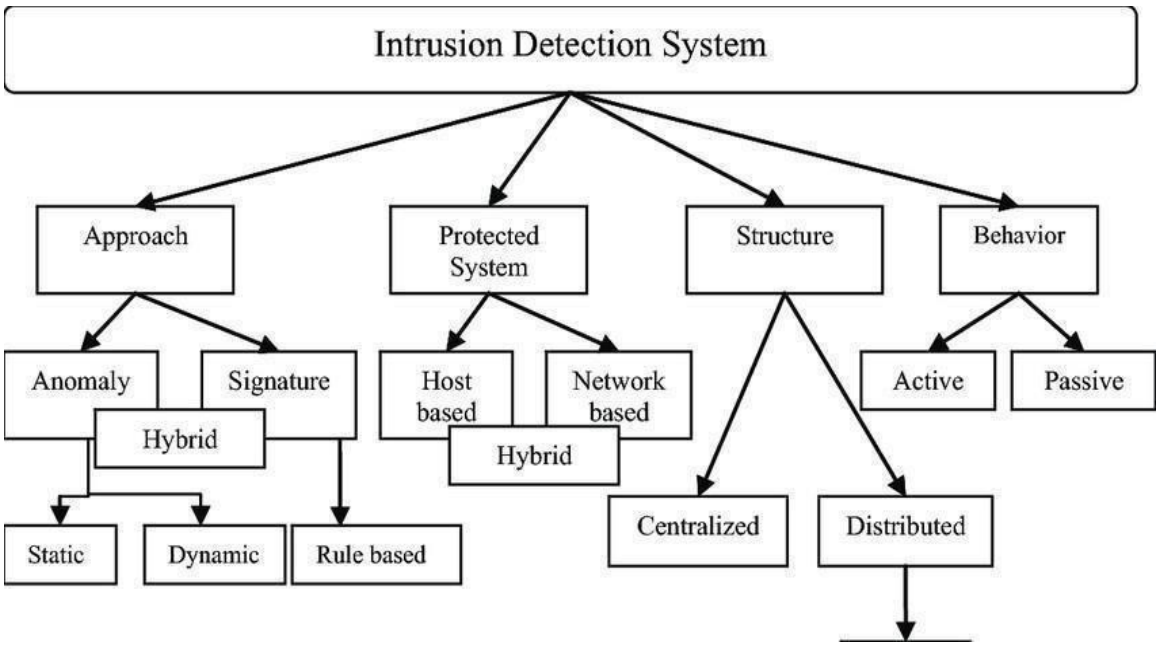


Figure 2.5: Characteristics and Operation of IDS [21]

4. Different IDS Types

There are several types of IDS, but they can be classified into two families:

- **NIDS:** Network IDS, network intrusion detection system
- **HIDS:** Host IDS, host-based intrusion detection system

Other IDS are actually derivatives of these families: Hybrid IDS, IPS (intrusion prevention systems).IDSs are available in the following formats:

- **Software:** allows any network administrator to install it on their OS. They are easy to install,configure and control. However, this OS (Windows, Linux) is a distribution whose flaws hackersmay know. It is more vulnerable if patches are not regularly installed and unused modules of the OS are kept.

4.1.NIDS

NIDS are IDS dedicated to networks. They generally include a probe (e.g. a machine) that "listens"on the network segment to be monitored, a sensor and an engine that analyses the traffic in order to detect intrusions in real time. A NIDS listens to all network traffic, then analyses it and generatesalerts if packets appear dangerous.

5. IDS Selection Criteria

Today, intrusion detection systems have really become indispensable when setting up an operational security infrastructure. They are therefore always integrated into a context and an architecture that impose constraints that can be very diverse. This is why there is no single evaluation grid for this type of tool. However, a certain number of criteria can be identified; these must necessarily be weighted according to the context of the study.

- **Reliability:** An intrusion detector must be reliable; the alerts it generates must be justified and it must not be possible for any intrusion to escape. An IDS that generates too many falsealerts will certainly be deactivated by the administrator and an IDS that detects nothing will quickly be considered useless.
- **Reactivity:** An IDS must be able to detect new types of attacks as quickly as possible; to do so, it must remain constantly updated. Automatic update capabilities are virtually indispensable.
- **Ease of implementation and adaptability:** An IDS must be easy to implement and, above all, must be able to adapt to the context in which it is to operate; there is no point in having an IDS that issues alerts in less than 10 seconds if the resources needed to react are not available to act within the same time constraints.
- **Performance:** the implementation of IDS must not affect the performance of the monitored systems. Moreover, it is always necessary to be certain that the IDS has the capacity to processall the information at its disposal (for example, a network IDS must be able to process all theflows that may occur at a given moment without ever dropping packets), otherwise it becomes trivial to mask attacks by increasing the quantity of information.
- **Multi-channel:** Good IDS must be able to use several alert channels (e-mail, pager, telephone, fax, etc.) in order to guarantee that the alerts will actually be issued. Information: The IDS must provide as much information as possible about the detected attack in order to prepare the reaction. Classification: it must be easy to rank the seriousness of the attacks detected in order to adapt the alert mode. [22]

6. Choice of IDS placement

The placement of IDSs will depend on the security policy defined in the network. However, thereare positions that can be described as standard; for example, it would be interesting to place IDSs:

- In the demilitarized zone (attacks against public systems).
- In the private network(s) (intrusions to or from the internal network).

On the outside leg of the firewall (detection of signs of attacks among all incoming and outgoing traffic, before any protection intervenes).

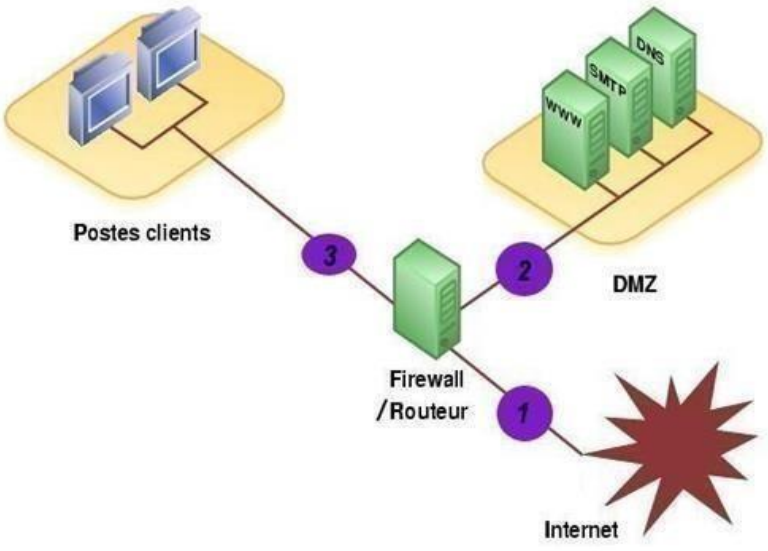


Figure 2.6: Choice of IDS Placement.

It is important to define the sensitive areas of the system (network), as well as the areas that are most vulnerable. More attractive to a hacker. It is also important to see that beyond the network architecture,the existing security organization must be taken into account:

- Are we looking fora centralized administration?
- What is the existing network monitoring organization?
- What are the internal skills and resources for managing IDS?

7. IDS limitations

Like anyIT system, IDSs have limitations. We can mention some of them:

- **Pollution/overload:** IDSs can be polluted or overloaded, for example by generating a lot of traffic (as difficult and heavy as possible to analyze). A large amount of attacks can also be sentto overload the IDS alerts. Possible consequences of this overload can be resource saturation (disk, CPU, memory), packet loss, partial or total denial of service...
- **Resource consumption:** in addition to the size of the log files (in the order of (GB), intrusion detection is excessively resource-intensive. Indeed, a NIDS system must generate logs of abnormal or suspicious activity on the network.
- **Packet loss (performance limitation):** transmission speeds are sometimes so high that they farexceed the writing speed of hard disks, or even the processing speed of processors.
- It is therefore not uncommon for packets not to be processed by the IDS, and for some of them to be received by the recipient machine.
- **Denial of service vulnerability:** An attacker may attempt to cause a denial of service in the intrusion detection system, or worse, in the operating system of the machine supporting the IDS.
- Once the IDS is disabled ("down"), the attacker can try anything he likes. [23]
-
-

8. Some tools

There are several IDS on the market, among them:

8.1.ISS Real Secure

Internet Security Systems (ISS) provides ISS Real Secure IDS, an integrated intrusion detection platform. ISS Real Secure IDS uses a standards-based approach to compare network traffic inputs and host logs of known and likely attacker methods. ISS Real Secure IDS integrates with many network andsystems management applications.

Real Secure combines three key features in a single agent:

- An intrusion detection engine.
- A personal firewall.
- An application and communication control module.

8.2.Enterasys DRAGON

Published by Enterasys Networks, it is an intrusion detection system considered one of the leaders in the market due to its performance, its ability to adapt to any type of environment and its analysis capacity. Dragon solutions consist of Network Sensor (NIDS), Host Sensor (HIDS) agents and a management system that provides the event management functions of the Dragon suite. [24]
The Network Sensor is a NIDS available in software or in a de dictated box. Since version 6, Enterasys offers three versions of appliances and software depending on the bandwidth to be analyzed. The hardware versions are backed up by their software equivalent.
The Host Sensor is a HIDS agent that detects attacks against the system on which it is installed by monitoring system and audit logs and using signature analysis mechanisms.
Dragon detects intrusions across the entire IT infrastructure wherever they occur, providing global visibility into the information system. This makes it possible to optimize the human resources needed to analyze logs from different firewalls or web servers by federating all these logs into a single Dragon console that will automatically analyze the related data.

9. Definition of Distributed Intrusion Detection System (DIDS)

The prototype Distributed Intrusion Detection System (DIDS), which generalizes the target environment in order to monitor multiple hosts, connected via a network and the network itself. The DIDS components include the DIDS Director, a single Host Monitor per host, and a single LAN Monitor for each LAN segment of the monitored network. Information is gathered and processed locally by each distributed component, with important events and information transported to, and analyzed at, a central location (viz.an Expert System, which is a sub-component of the Director).

This architecture provides the capability to aggregate information from numerous different sources.The system is designed to work with any audit trail format as long as certain pieces of criticalinformation are provided by the auditing mechanism. DIDS is designed to operate in a heterogeneous environment composed of C2 or higher rated computers. The DoD Class C2 (Controlled Access Protection) rating enforces a finely grained discretionary access control that makes users individually accountable for their actions through login procedures, auditing of security-relevant events, and resource isolation. The target environment consists of several hosts connected by a single broadcast LAN segment (presently an Ethernet, see Figure 2.8). The use of

C2-rated systems implies a consistency in the content of the system audit trails. This allows us to develop standard representations into which we can map audit data from UNIX, VMS, or any other system with C2 auditing capabilities. Some abstraction is performed on the raw audit data in order to transform the data into the standard representation. The C2 rating also provides, as part of the trusted the DIDS... [25]

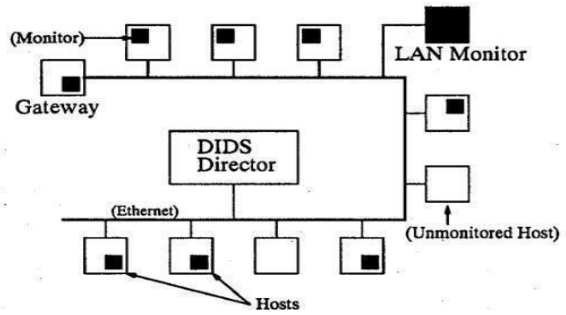


Figure 2.7: DIDS Target Environment

9.1.DIDS Architecture

The DIDS architecture combines distributed monitoring and data reduction with centralized data analysis. This approach is unique among current intrusion detection systems. The major components of DIDS are the DIDS Director, a single Host Monitor per host, and a single LAN Monitor for each broadcast LAN segment in the monitored network (Figure 2.8).

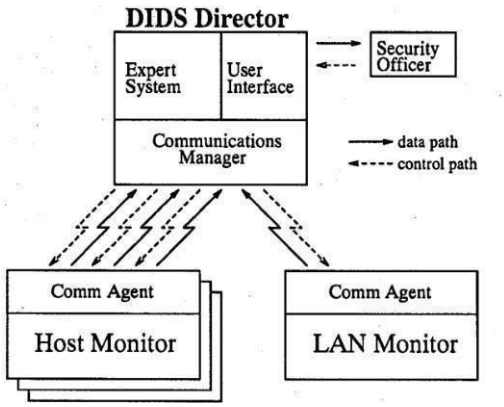


Figure 2.8: Communications Architecture

The DIDS Director's User Interface gives the Computer System Security Officer (CSSO) interactive access to the entire system. The CSSO uses the interface to watch activities on each host, observe networktraffic, and request more specific types of information from a monitor. [25]

10. SNORT [26]

SNORT is a particularly responsive IDS as it is provided as open source. It is therefore casual to obtain,and its advantage is that it has a very large database of signatures produced by the user community. It also ensures that you get quick updates to the database as soon as a new threat is reported. It was originallydesigned for the Linux system but has also been ported to Windows. There are several commercially available books dedicated to the installation and use of SNORT.

SNORT is usually used in conjunction with open source software called BASE, which is the managementand analysis console.

Conclusion

In this chapter, we have presented the generalities on IDS systems. Intrusion Detection Systems (IDS).And DIDS Intrusion detection systems are an important means of security and protection in a computer network.

Chapter 3: Multi-agent Systems

I. Introduction

Nowadays, with the immense amount of data that is circulating every second, the cyber security concerns are also growing. In recent years, cyber security-intrusion detection has become a very difficult research area in communication network and big data. Hence, traditional intrusion detection systems (IDSs) could not respond to the new security challenges. Therefore, IDSs require an effective and improved detection mechanism capable of detecting distributed intrusive activities and serious threats to network security. In this chapter, we have exposed A Multi-Agent System (MAS), which is very suitable for IDSs as it meets the features required by the networks and Big Data issues, through cooperation, autonomy, and proactivity between agents to ensure the effective detection of intrusions without the intervention of an expert.[27]

1. Definition of Multi-agent systems

(MAS), an important and relatively young branch of distributed artificial intelligence, where we will detail the concept of agent, the principle of communication between several agents and the concept of an agent, the principle of communication between several agents and the eccentricity of this approach for distributed artificial intelligence will be detailed. [28]

2. Definitions of an MAS

A multi-agent system is defined as a distributed system composed of a set of intelligent agents intelligent agents that interact, usually in cooperative, competitive or coexistent modes. Coexistence. It is a system composed of an organized set of agents, located in a certain environment and interacting according to certain relationships. Environment and interacting according to certain relationships. [28]

3. Some characteristics of an agent. [29]

We are going to see in what follows some characteristics of agents which certainly depend on thetype of the latter.
We will see in what follows some characteristics of agents which depend certainly on the type of the latter, among these characteristics we quote:

3.2. Autonomy

Denied as the own capacity of an agent to be able to reach its goal, independently of of other agents. It is, in other words, the ability of an agent to behave spontaneously, to take spontaneous behavior, to take the initiative to achieve its goals.

3.3. Flexibility

It is the possibility for an agent to modulate its behavior and morphology.

3.4. Adaptability

It is the capacity of an agent to improve its individual or collective functioning to face a perpetually evolving environment, which allows it to acquire a personality that individualizes it, and
personality that individualizes it, and differentiates it from other agents.

3.5. Rationality

A rational agent uses the resources at his disposal efficiently to select an action whose executionallows him to action whose execution allows it to reach one of its goals.
From the point of view of AI, and as indicated by Newell, the principle of rationality consists in making sure that if an agent knows that one of its actions allows it to reachits goals, then it will select this action goals, then he will select this action. Rational agents haveevaluation criteria for their actions, and select of their actions, and select according to these criteria the best actions that allow them to make the best to make the best decision. Such agents are able to justify their decisions.

3.6. Commitment

An agent is committed to perform the actions that satisfy a goal to be reached and gives himself the means to achieve it. Commitment is one of the key concepts of collective action in the case ofthis concept was introduced in AI [29], and analyzed in detail by Alan Bond. This concept was introduced in AI [29], and analyzed in detail by Alan Bond, [30]
For Jacques Ferber, commitments characterize the dependencies (duties, constraints...) which bind cognitive agents to themselves, but especially to others when they decide to perform an action, to render a service and, in a general way when they intend to do something. If agents didnot make commitments it would be impossible for them to have an adequate representation of afuture state of the world and thus to plan their own actions in anticipation of the future.

4. Interactions between agents

An interaction is a dynamic linking of two or more agents through a set of reciprocal actions [29]. The interaction between agents can be summarized into:

- Communication,
- Collaboration,
- Coordination
- Cooperation. [30]

4.1. Cooperation

Cooperation between agents consists in breaking down tasks into sub-tasks and then distributing them between the different agents, there are different types of cooperation which depend on the need of the need of the ADM: Cooperation by sharing tasks and results. [31]

4.2. Communication

An agent must be able to communicate with other agents. There are two types ofcommunication:

- **Indirect communication:** sharing information via the environment.
- **Direct communication:** Sending messages.

Agents must have the ability to manipulate a common language. [31]

There are two communication methods which are the communication by sharing information, and the communication by communication by sending messages. [31]

- **Communication by information sharing (blackboard):** This is an indirect communication wherethe agents can communicate with each other. This is an indirect communication where the agents can communicate through a common workspace (shared).It is an indirect communication where agents can communicate through a common workspace and so the concerned agent will come to getthis information.

- **Communication by message sending:** in this type of communication the agents are in direct connection, the messages are sent directly and explicitly to the recipients. There are three types of messages: questions, answers and information. At the protocol level, a message sending can be synchronous (an agent waits for its receiver's response) and asynchronous. The agents have common languages to be able to cooperate for the resolution of a problem. These languages are called languages of communication between agents (ACLs,in English Agent Communication Languages). There are different ACLs; among them, we can mention KQML (Knowledge Query and Manipulation Language), KIF (Knowledge In-Terex change Format) and ACL FIPA.

4.3. Collaboration

Collaboration is concerned with the way in which work is distributed among several agents, whether it is centralized or distributed [Ferber, 1997]. Be centralized or distributed techniques.

4.4. Coordination

Coordination analyzes how the actions of different agents should be organized in time and space inorder to achieve objectives [30]. present coordination between agents through examples such as two movers moving a heavy piece of furniture, two jugglers exchanging balls with which they jugglers exchanging balls with which they juggle, people taking turns speaking into a microphone,etc. se passer un micro, etc.[31]

5. Platform

5.1.JADE

JADE (Java Agent Development Framework) is a software framework to facilitate the development of development of FIPA-compliant agent applications for intelligent multi-agent systems interoperability. The goal of JADE is to simplify development while ensuring while ensuring standard compliance through a comprehensive set of system and agent services.

5.2.FIPA

To achieve such a goal, JADE provides the following list of features to the agent program:
Compliant Agent Platform, which includes the AMS (Agent Management System), DF (Directory Facilitator) and ACC (Agent Communication Channel). All three of these agents areautomatically activated when the agent platform starts up.
Distributed Agent Platform. The agent platform can be divided over several hosts (providedthere are no firewalls between them). A single Java application, and therefore only one JavaVirtual Machine, is executed on each host. The agents are implemented as a Java thread andJava events are used for efficient and lightweight communication between agents on the same host. An agent can still execute parallel tasks, and JADE schedules these tasks in a more way more efficient (and even simpler for the skilled programmer) than Java Virtual The machine does for threads.

6. IDS based on MAS

An adaptive intrusion detection system that can detect unknown attacks in the network traffic in real time is a major concern. Conventional adaptive systems are expensive in terms of computingresources and time, as these systems must be times, as these systems must be retrained with knownand unknown attacks. Proposes a software agent architecture combining case-based reasoning reactive behavior and learning called HyLAA (A hybrid and learning agent architecture

for network intrusion detection).

6.1.Agent-based approach

HyLAA can adapt to its environment and identify new intrusions not specified in the system design. Design of the system. This is done by learning new reactive rules by observing recurrent good solutions to the same perception from the case-based reasoning system, which will be system, which will be stored in the agent's knowledge base. The effectiveness of HyLAA to detect intrusions using case-based reasoning behavior, the accuracy of the classic actor learned by the learning component, and the performance and edacity of HyLAA to detect intrusions using the hybrid behavior with learning and without learning were evaluated, intrusions.
In the second experiment, the classic learned by the learning component showed high accuracy. The behavior of the hybrid agent with learning and without learning (third and fourth experiments, respectively) exhibited higher edacity and a balance between performance and edacity, but only the hybrid behavior exhibited better edacity and performance as long as the agent was learning

Proposed a method called real-time multi-agent system for adaptive intrusion detection system RTMAS-AIDS, based on a multi-agent system, is proposed to multi-agent system, is proposed to allow the intrusion detection system to adapt to adapt to unknown attacks. Real-time. [32]
Using the paradigms of the Artificial Immune System (AIS) paradigms as an efficient mechanism for distributed IDS. The paradigms are negative selection, clone selection, hazard theory and the immune network. Immune network. These paradigms are very successful for anomaly SDI. The proposed AIS agents are capable of learning, self-adaptation, platform mobility, autonomy and collaboration. The proposed system (MAIS-IDS) has been designed using these powerful and collaborative and collaborative agents.
This system has mobile and static agents with sensing agents as the main actors in MAIS-IDS. The lifecycles of the agents are determined using the proposed immune algorithms in specific phases. The key features of MAIS-IDS of MAIS-IDS are cloning, mutation, migration, collaboration and randomness.
MAIS-IDS was evaluated using a virtualized host network, a virtual machine hyper kernel-based virtual machine (KVM) and a management orchestra. [33].

Conclusion

In this chapter, we have presented the system multi-agents (MAS) and the interactions betweenagents, also a jade platform, multi-agent Based System for Intrusion Detection.
We talked about the basic concepts of MAS and their use in IDS (IDS based on MAS) and we mention 02 approaches MAS in IDS.
(MAS), an important and relatively young branch of distributed artificial intelligence

Chapter 4: Setting up an IDS (SNORT)

I. Introduction

Often computer networks are protected by firewalls. This protection, although necessary, doesnot allow the detection of external attacks. Indeed, a firewall is made to block unwanted network flows while letting the "useful traffic" through problem is how to analyze the potentially dangerous data inside this traffic and prevent data and prevent attacks.

Snort is one of the possible answers; it will analyze in real time, the network traffic, searching in its database of known attack profiles and log the results.

In this chapter, we will install the open source snort software under Windows describing all the describing all the installation steps and its configuration. Then, we will perform an
to make sure that the software is working properly.

1. Definition of Snort

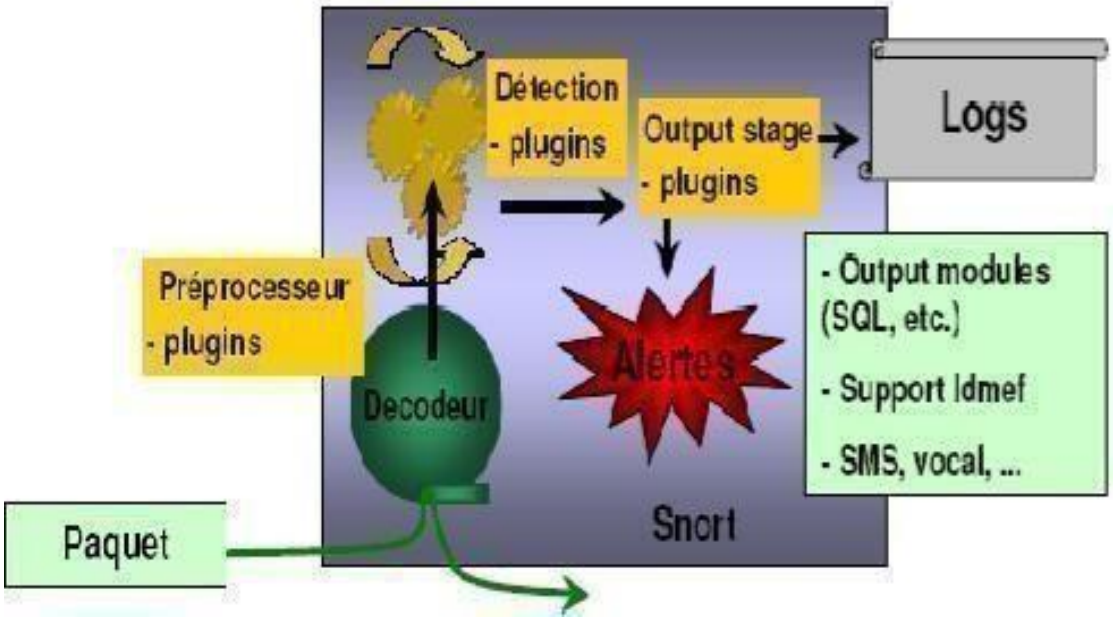
Snort is the foremost Open Source Intrusion Prevention System(IPS) in the world. Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets thatmatch against them and generates alerts for users.

Snort can be deployed in line to stop these packets, as well. Snort has three primary uses: As a packet sniffer like tcpdump, as a packet logger. Which is useful for network traffic debugging, or it can be used as a full- blown network intrusion prevention system? Snort can be downloaded and configured for personal and business use alike.

Snort is now integrated into a broad portfolio of security products from Cisco, but remains completely free to anyone who wants to use it. There are currently two versions of snort: snort2 and snort 3, which is still in beta.

2. Architecture of snort [34]

- **A basic core:** (Packet Decoder) at startup, this kernel loads a set of rules, compiles them, optimizesthem and classifies them. During runtime, the main role of the kernel is packet capture.
- **A series of pre-processors:** (Detection Engine) these enhance SNORT's ability to analyze and re-compose captured traffic. They receive the packets directly captured and decoded, rework them if necessary and then provide them to the signature search engine for comparison with the signaturedatabase.
- **A series of detection plugins:** These analyses consist mainly of comparisons between the variousfields of the protocol headers (IP, ICMP, TCP and UDP) against specific values.
- **A series of output plugins:** allows the intrusion to be processed in several ways: sending to a log file, sending an alert message to a syslog server, storing the intrusion in an SQL database. [33]



.**Figure 4.1:** Architecture of SNORT [35]

3. SNORT Operating Modes

Snort can operate in three modes: [36]

3.1.The "offline" sniffer mode, which simply reads packets flowing on the network anddisplays them continuously on the screen.

- This involves listening to the network, typing one or more lines of commands that will tellsnort what type of result to display, here are some of them:
- The verbose command displays the TCP/IP headers: snort **-v.**
- The verbose dump command, displays the IP and TCP/UDP/ICMP headers: snort **–vde**

3.2.The "packetlogger" mode which records packets on the disk. This mode is similar to the previous one, except that the logs are no longer displayed on the screen, but are written directly to a log file. The natural log directory for snort is:

- **/var/log/snort/** . The only change is that the v has been replaced by l, i.e.: **snort -de -l**
- **/var/log/snort/.** If you visit the /var/log/snort/ directory, you will see that there are several directories.

4. Alert and Log System

The alert and log system takes care of generating logs and alerts. Depending on what the detectionsystem finds inside a packet, the packet can be archived in the log file or an alert can be generated.These logs are contained in files.
The alerts in this case are stored in a database such as MySQL as an example the **ACID BASE database**.

5. **The NIDS (Network Intrusion Detection System) mode:** the most complex and the most configurable, which allows analyzing the traffic on the network following rules defined by the userand to establish actions to be executed according to the cases.

Snort uses rules to detect intrusions. There are currently

There are currently about 1500 different rules, each one adapted to a particular case. Rules can be created to observe a particular activity on the network: pings, scans, a flaw in a script, a remote takeover attempt.

Alerts can be recorded in a specific file or directly in the syslog or in a database. Each rule is added to a configuration file, which can be used to create new rules or to use existing ones. The snort configuration file is **/etc/snort/snort.conf**, the .rules files contained in the **/etc/snort/rules/** directory are files containing rules for a particular use. The name of the file is usually self-explanatory, e.g. **ftp.rules** contains rules specific to ftp and dos.rules is used for DoS (Denial of Service) attempts.[36]
This is how Snort is represented on a network diagram:

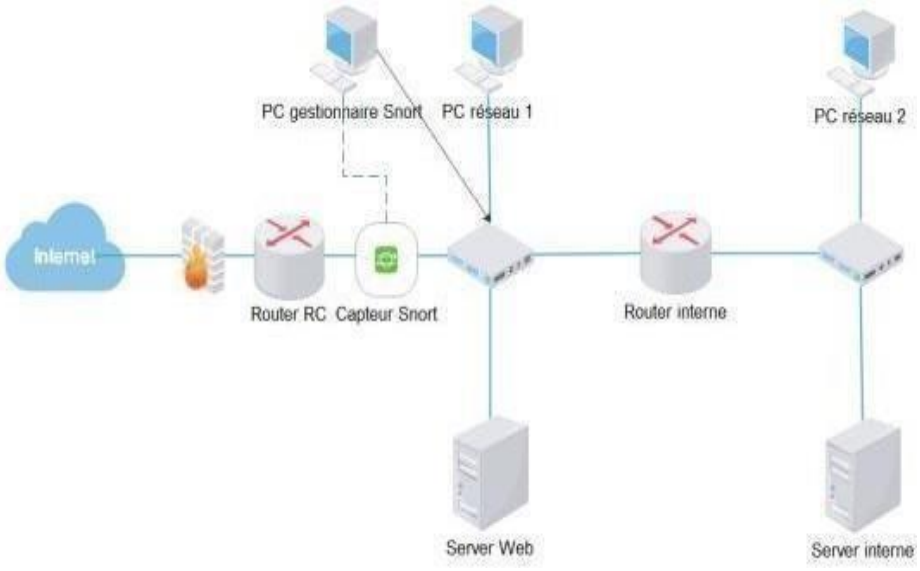


Figure 4.2: How Snort works

(Ilir Kadriu)

6. Composition of Snort

Snort is a program that consists of several folders where its resources, executable, rules and othercomponents are located. We will see in detail what Snort is composed of and what you can use, modify, add, or ignore to get the best use out of this program. Here is what Snort looks like whenyou install it:

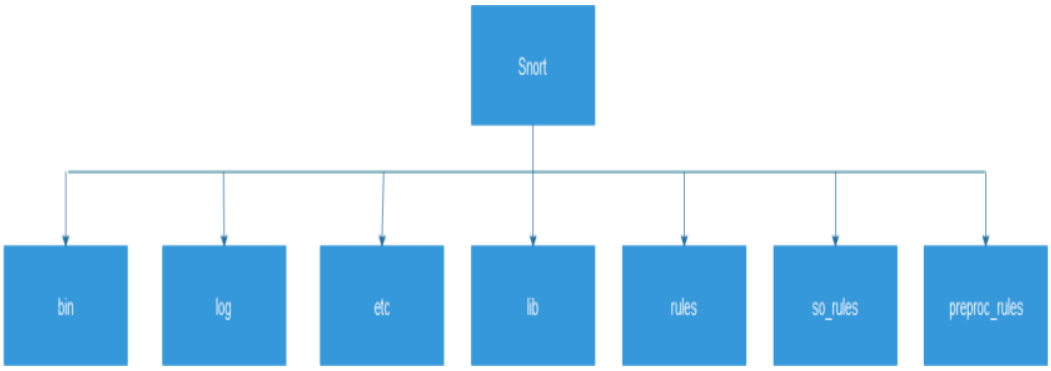


Figure 4.3: Composition of Snort

- The contents of the Snort folders in detail Firstly, there are:

- **The "bin" folder** which contains the Snort executable and its components in **".dll"** type.
- **The "doc" folder** which contains many **"ReadMe"** files from Snort users who have integrated these **"ReadMe"**, but there is also the "signatures" folder which will contain the signatures of known anomalies.
- **The "etc" folder** is very important because it contains the **"snort.conf"** fileand it is this file that will indicate the path, constants and variables to be used when Snort is launched. We will see this configuration file.
- **The " lib " folder** which will contain two folders **" snort_dynamicengine "** and **" snort_preprocessor "**. These two folders contain application plotswhen the application is launched. These parcels are of type **".dll"**. Then, wec an see that there is a **"log"** folder. This folder will contain the logs thatwere created by the events and the different alerts that were also generated by the events.
- **As for the last three folders:** **"rules"**,**"so_rules"** and **"preproc_rules"**, we will see their contents in more detail, as these folders represent the heartof Snort. [37]

7. The Snort installation and configuration steps

Obviously, we need **Snort**, we will configure Snort to record events in a **MySQL** database. Therefore, wewill need to installand configure the MySQL database management system.
Snort uses the **Libpcap** library to capture packets passing over the network, so we need to make sure it is installed. We will also need a console or graphical application that will attack the MySQL database to better view alerts and other information (statistics, graphs.).

7.1.Prerequisite installations [38]

The installation of prerequisites is often tricky. Because the prerequisites often also depend on otherpackages to be installed. That is why before installing these prerequisites we'll do a system update to make sure we have at least the basic tools to start.

Command prompt to check snorts working:

```
C:\Users\Pc>cd c:\Snort\bin

c:\Snort\bin>snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.19-WIN64 GRE (Build 85)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11


c:\Snort\bin>
```

Figure 4.4: Successfully running Snort on Windows

The available interfaces run the command: Snort –W:

```
c:\Snort\bin>snort -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.19-WIN64 GRE (Build 85)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   74:40:BB:29:51:71       0000:0000:fe80:0000:0000:0000:b892:4cc2 \Device\NPF_{C2C6CE48-5158-40E1-B6B6-3AA6B27094C
C}      Realtek RTL8723DE 802.11b/g/n PCIe Adapter
    2   76:40:BB:29:51:71       0000:0000:fe80:0000:0000:0000:0835:a388 \Device\NPF_{62619CE1-70DC-43FF-B5F4-689CDAD29DC
4}      Microsoft Wi-Fi Direct Virtual Adapter #7
    3   00:00:00:00:00:00       disabled        \Device\NPF_Loopback    Adapter for loopback traffic capture
    4   10:62:E5:DE:57:F5       0000:0000:fe80:0000:0000:0000:a9ee:9d65 \Device\NPF_{781BEBE7-E323-4D74-85E7-0908CDDDBE7
4}      Realtek PCIe GBE Family Controller #4

c:\Snort\bin>
```

Figure 4.5: list the available interfaces

7.2.Configuring Snort 2.9.19 on Windows:

- After installing Snort on Windows another important step to get started with Snort is configuringit on Windows.
- Download latest snort rule file.
- Extract three folders from the downloaded snortrules-snapshot-29170.tar folder into the Snorts corresponding folders in C drive.

Folders to be extracted are: rules , preproc_rules , etc…

- Rules folder contains the rules files and the most important local.rules file. Whichwe will use to enter all our rules.
- etc folder contains all configuration files and the most important file is snort.conffile which we will use for configuration
- Now open the snort.conf file through the notepad++ editor or any other text editorto edit configurations of snort to make it work like we want it to.
- Setup the network addresses you are protecting ipvar HOME_NET any

Note: network ip address you are using you are going to open your command promptCMD

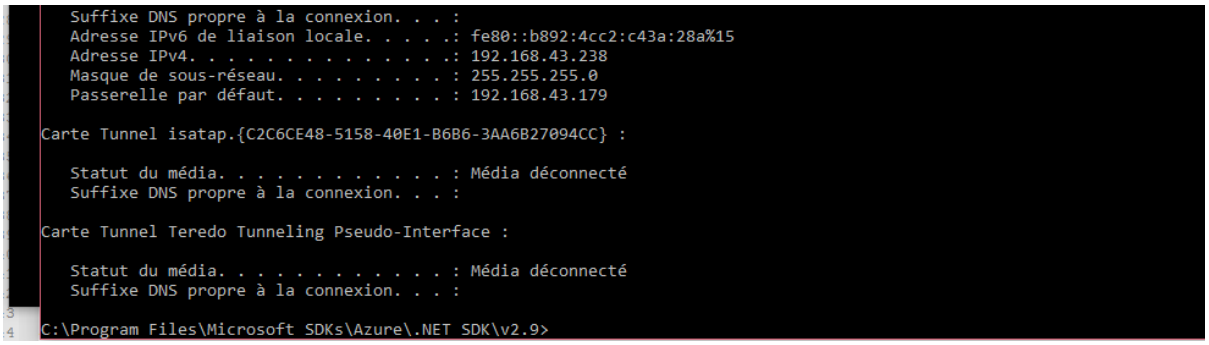


Figure 4.6: IP addresses

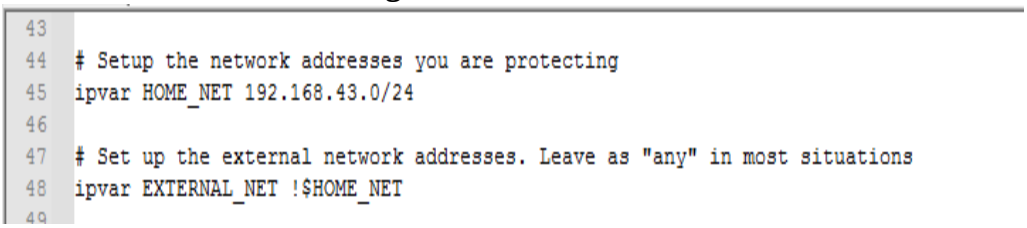


Figure 4.7: Setting up the Home Network Address in Snort

Setup the external network into anything that is not the home network. That is why! Is used in the command it denotes ‘not’.
Set up the external network addresses. Leave as “any” in most situations ipvarEXTERNAL_NET any

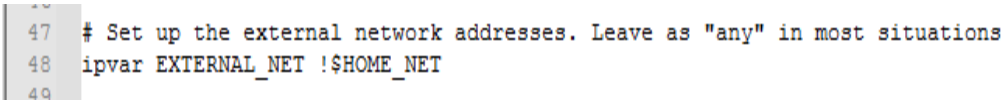


Figure 4.8: Setting up the external Network Addresses in Snort

- Now we have to define the directory for our rules and preproc rules folder:

Path to your rules files (this can be a relative path).
Note for Windows users: You are advised to make this an absolute path
such as: c:\snort\rulesvar RULE_PATH
../rulesvar SO_RULE_PATH ../so_rulesvar PREPROC_RULE_PATH
../preproc_rules

```
# Path to your rules files (this can be a relative path)
# Note for Windows users:  You are advised to make this an absolute path,
# such as:  c:\snort\rules
var RULE_PATH C:\Snort\rules
# var SO_RULE_PATH ../so_rules
var PREPROC_RULE_PATH C:\Snort\preproc_rules
```

Figure 4.9: Setting up path to our rules files and preproc rules folder in Snort.

- Now we have tosetup our white list and black list path it will be in our snorts rule folder# If you are using reputation preprocessor set these

var WHITE_LIST_PATH../rulesvar BLACK_LIST_PATH ../rules

```
# Set the absolute path appropriately
var WHITE_LIST_PATH C:\Snort\rules
var BLACK_LIST_PATH C:\Snort\rules
```

Figure 4.10: Setting up our White List and Black List files paths in Snort

Next, we have to enable to log directory, so that we store logs in our log folder.
Uncomment this line and set absolute path to log directory:
Configure default log directory for snort to log to. For more information see snort -hcommand line options(-l)## config logdir:

```
#
 config logdir: c :\snort\log
```

Figure 4.11: Setting up Log DirectoryPath in Snort

- Now we will set the path to dynamic preprocessors and dynamic engine:

path to dynamicpreprocessor libraries directory/usr/local/lib/snort_dynamicpreprocessor

```
# path to dynamic preprocessor libraries
dynamicpreprocessor directory c:\snort\lib\snort_dynamicpreprocessor

# path to base preprocessor engine
dynamicengine c:\snort\lib\snort_dynamicengine\sf_engine.dll
```

Figure 4.12: Setting up path to dynamic preprocessors and dynamic engine in Snort

-

- We will do same thing for dynamic preprocessor engine# path to base preprocessorengine dynamic engine.

/usr/local/lib/snort_dynamicengine/libsf_engine.so

```
248
249  # path to base preprocessor engine
250  dynamicengine c:\snort\lib\snort_dynamicengine\sf_engine.dll
251
252  # path to dynamic rules libraries
253  dynamicdetection directory \usr\local\lib\snort_dynamicrules
254
```

Figure 4.13: Setting up the path to dynamic preprocessor engine in Snort

- Now let's set our reputation preprocessors:

pathto dynamic rules libraries# dynamic detection directory

/usr/local/lib/snort_dynamicrules

```
251
252  # path to dynamic rules libraries
253  dynamicdetection directory \usr\local\lib\snort_dynamicrules
254
255  ##################################################
256  # Step #5: Configure preprocessors
```

Figure 4.14: Path to dynamic rules libraries in Snort

- Just comment out these lines as shown in figure 4.15 in doing so we are excludingpacket normalization of different packets.

```
263  # Inline packet normalization. For more information, see README.normalize
264  # Does nothing in IDS mode
265  # preprocessor normalize_ip4
266  # preprocessor normalize_tcp: ips ecn stream
267  # preprocessor normalize_icmp4
268  # preprocessor normalize_ip6
269  # preprocessor normalize_icmp6
270
```

Figure 4.15: Commenting out packet normalization commands in Snort

- Scroll down to the reputation preprocessors. We will just change the name of the filessince white list, blacklist are not rules they are just the list of IP addresses labelled as blackor white.

Reputation preprocessor. For more information see README.reputation preprocessor reputation: \memcap500, \prioritywhitelist, \nested_ip inner, \whitelist $WHITE_LIST_PATH/whitelist, \blacklist $BLACK_LIST_PATH\black.list

```
511    whitelist $WHITE_LIST_PATH\whitelist.rules, \
512    blacklist $BLACK_LIST_PATH\blacklist.rules
513
514  ##################################################
515  # Step #6: Configure output plugins
516  # For more information, see Snort Manual, Configuring Snort - Output Modules
```

Figure 4.16: Whitelisting and Blacklisting IPsthrough the command as shown in figure

Converted back slashes to forward slashes in lines 546–651.

```
545  # site specific rules
546  include $RULE_PATH\local.rules
547
548  include $RULE_PATH\app-detect.rules
549  include $RULE_PATH\attack-responses.rules
550  include $RULE_PATH\backdoor.rules
551  include $RULE_PATH\bad-traffic.rules
552  include $RULE_PATH\blacklist.rules
553  include $RULE_PATH\botnet-cnc.rules
554  include $RULE_PATH\browser-chrome.rules
```

Figure 4.17: Converted back slashes to forward slashes in specific lines in snort.conf file

Again just convert forward slashes to backslashes and uncomment the lines below:# decoder and preprocessor event rules# include
$PREPROC_RULE_PATH/preprocessor.rules# include
$PREPROC_RULE_PATH/decoder.rules
#include $PREPROC_RULE_PATH/sensitive-data.rules

```
656  ##################################################
657
658  # decoder and preprocessor event rules
659   include $PREPROC_RULE_PATH/preprocessor.rules
660   include $PREPROC_RULE_PATH/decoder.rules
661   include $PREPROC_RULE_PATH/sensitive-data.rules
662
```

To forward slashes in specific lines and uncommenting specific lines in snort.config file

- Now we just need to verify the presence of this command at the bottom of snort.conffile.

```
687
688  # Event thresholding or suppression commands. See threshold.conf
689  include threshold.conf
690
```

Figure 4.19: verifying presence of"include thres "hold.conf" command in snort.conf file

- Now we test snort again by running Command prompt as admin. To check if it's running fine after all the configurations.

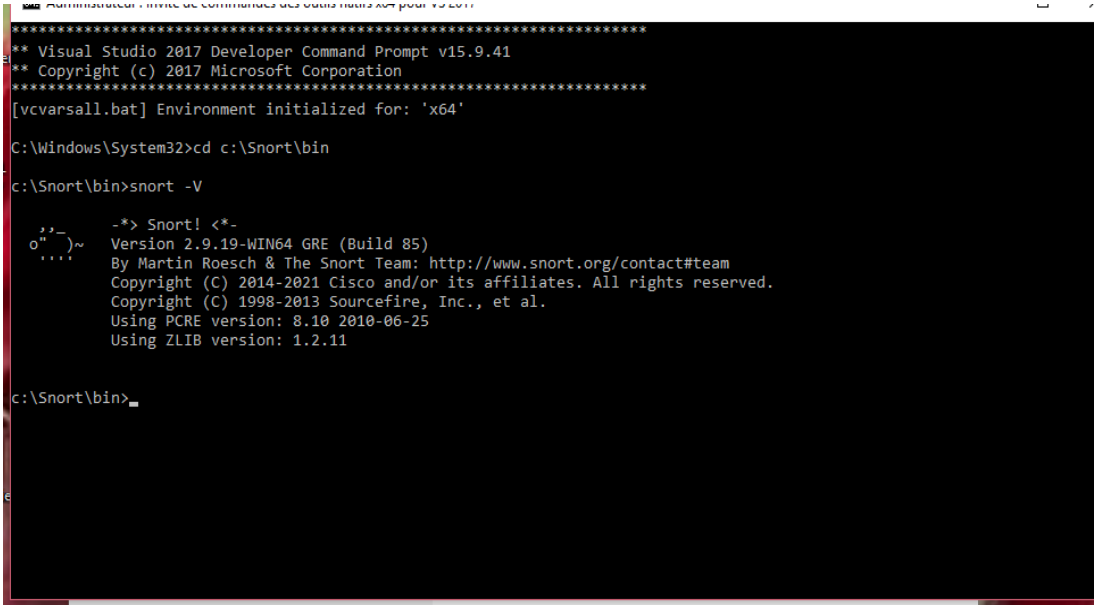


Figure 4.20: Test Running of Snort in Windows 10 after Configuration

- We can also the check the wireless interface cards from which we will be using snort by usingthe command below we can see the list of our wireless interface cards through entering this command in command prompt.

Snort — W

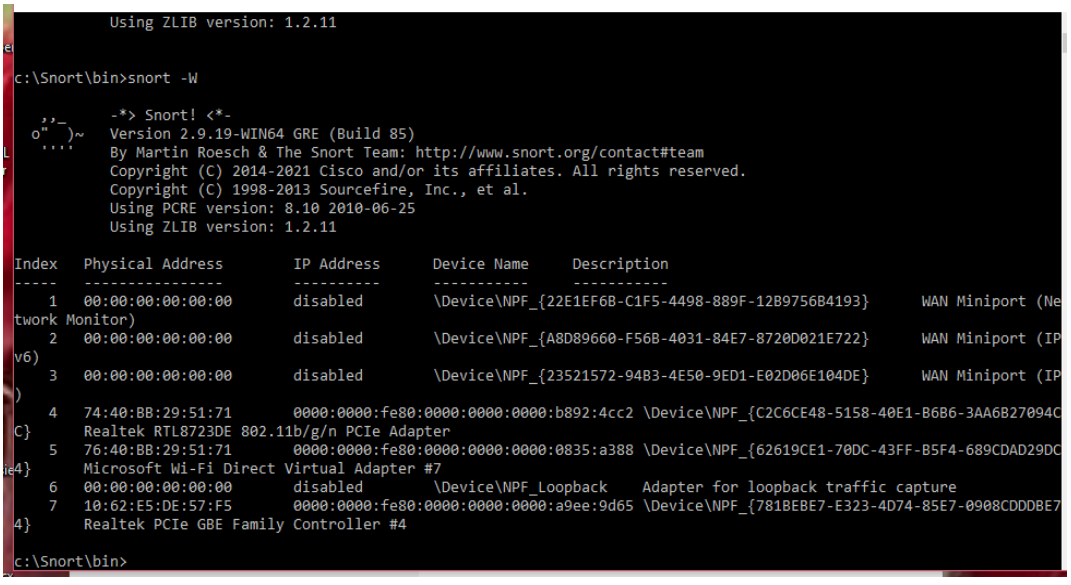


Figure 4.21: check the wireless interface cards

- Configuration validation check command:
- We will enter a command to check validation of snort's configuration.

By choosing a specific wireless interface card (1) the rest of command shows the config filepath. The command is:
snort -i1 -c C:\Snort\etc\snort.conf –T

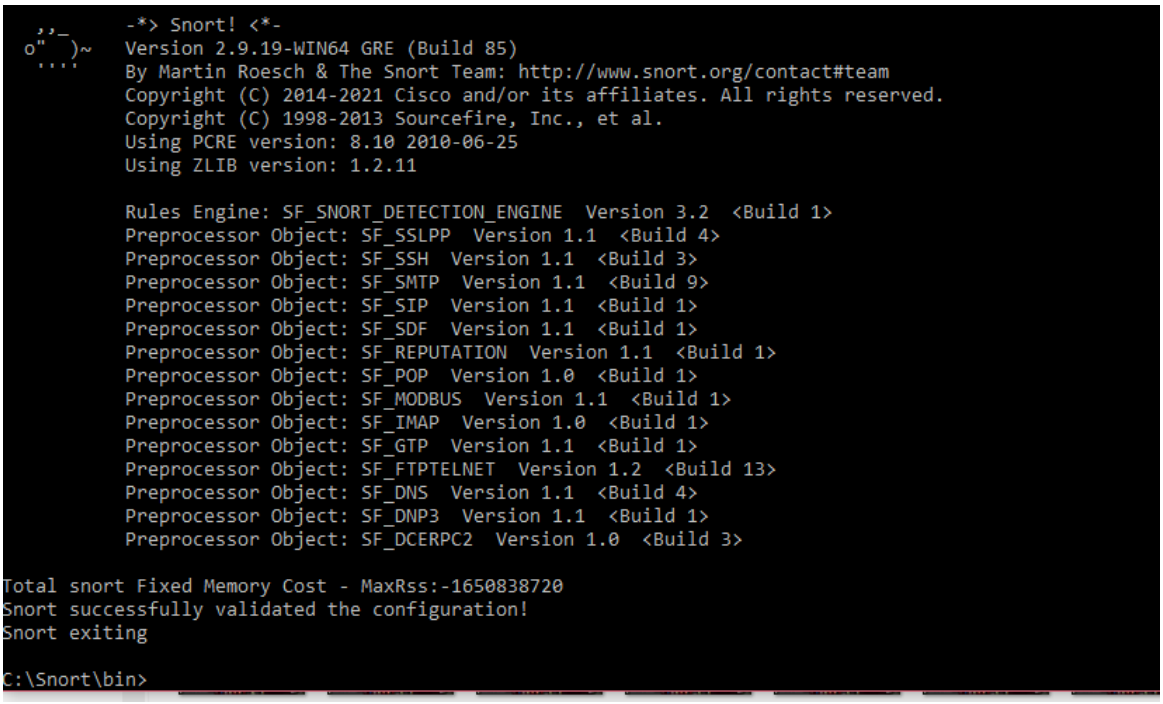


Figure 4.22: Checking Validation of Snort Configuration in Command Prompt

8. Linking SNORT with MySQL:

Edit the /snort/snort.conf file. Uncomment and edit the following line:

Output database: log, MySQL, user = snort password = snort pass dbname = snort host = local host

```
output database: log, mysql, user=snort password=snortpass dbname=snort
host=localhost
```

Figure 4.23: Linking SNORT with MySQL

The next few steps are related to setting up the MySQL database and settings. After you install MySQL, enter the MySQL commands by typing **MySQL** on the command line. This will place youin an interactive command mode. All commands must have a semicolon at the end of the line. Bydefault, the MySQL installation will not have a password set at all. You should add a default password with the following commands.

mysql
mysql > SET PASSWORD FOR root@localhost =PASSW0RD('somepassword');

After you have assigned a password to the root account, simply entering mysql will not enable you to access the interactive command mode. After a password has been assigned, use **mysql –u < username > − p**.You will then be prompted to enter the password for the user you specified (typically root).

The next step is to create the Snort database.mysql > create database snort;

You now need to give the Snort user permissions to add the needed tables to the Snort database. Use these commands:
mysql > grant INSERT,SELECT on root.* to snort@localhost;

You should now set the password for the Snort user to the same password you used in the Snort configuration file.
mysql > SET PASSWORD FOR snort@localhost = PASSWORD('snortpass');

The next step is to add some additional permissions for the Snort database using the following commands:mysql > grant ALL on snort.* to snort@localhost;
mysql > grant ALL to snort;mysql > exit

Now that the database has been created, you need to populate it with the tables Snort uses. Use the following command to create the tables:
mysql -u root -p < /etc/snort/schemas/create_mysql snort
When the command completes, it will not give any indication of its success; therefore, it will be necessary to manually verify that the tables were created.

If the package you installed did not include the /snort/schemas/ directory, you can download the source package and extract the directory fromthere. With Fedora Core 5, for some reason installing the Snort with MySQL support did *not* include the schemas directory.

Verify the MySQL tables were created in the Snort database by entering the following commands.Youshould see output similar to that shown in the following example:

```
mysql -u root -p
show databases;
+----------+
| Database |
+----------+
| mysql    |
| snort    |
| test     |
+----------+
use snort;
show tables;
```

```
+------------------+
| Tables_in_snort  |
+------------------+
| data             |
| detail           |
| encoding         |
| event            |
| icmphdr          |
| iphdr            |
| opt              |
| reference        |
| reference_system |
| schema           |
| sensor           |
| sig_class        |
| sig_reference    |
| signature        |
| tcphdr           |
| udphdr           |
+------------------+
exit
```

The list of databases is not significant, as long as the Snort database exists, of course. The tablelisting must be accurate. If any are missing, Snort will generate an error when you run it.

Conclusion

In this section, we have experimentally and manually installed Snort, with almost all its functionsand integrated security rules that are necessary for the detection of attacks.
Linking snort with database.

Chapter5: *A coordinate approach in intrusion detection systems*

I. Introduction

We overview some of the recent works that have proposed coordinate approaches, for the detection of Intrusion detection system by IDS (Snort), and this, so that we situate ourselves in relation to these works, and we show thereafter, the particularity of our work, and our own contribution to it.
We present a decentralized approach to coordinate the intrusion detection systems (IDS). This approach based on the technology of Socket.

As already mentioned, our approach for IDS based on multi-agent systems (MAS). The distributed systems have been widely used in the field of computer security, and in particular for intrusion detection.

Our goal is to consider these advantages in order to build a distributed system for collective and cooperative intrusion detection systems.

Operating principle
In our approach, the idea is to make many IDS communicate with each other, eachone representing a node of the network (machine).

II. Our approach

1. Coordination

In our work we used the multi-agents coordination because it is important forusing distributed expertise and sharing the results with others agents. [39]

1.1.The classes of agents

By classes of agents, we mean the types of agents. In addition to having different goals, beliefs and expertise, agents can also have various communication languages, ontologies, or internal architectures. It is important to take the heterogeneity of the system into consideration when choosing a coordination technique. The Blackboard strategy for example will not suffice in an environment where interacting agents have different communication languages, in our work we used socket of TCP protocol. [40]

- By the coordinate approach, we will coordinate many IDS together

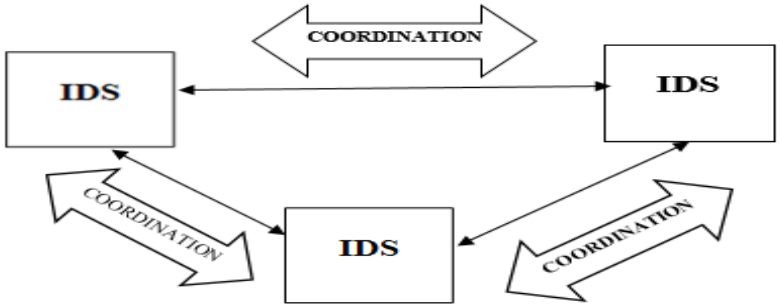


Figure5.1: Coordination of IDS.

Each IDS have an architecture (structure). In the first part, we proposed an architecture of components of an intrusion detection system.
We have chosen the one resulting from the work of the Intrusions Detection exchange format Working Group (IDWG) [20]
The objective of the IDWG work is to define a standard for communication between certain components of an intrusion detection system. The figure illustrates this model and introduces a number of concepts:

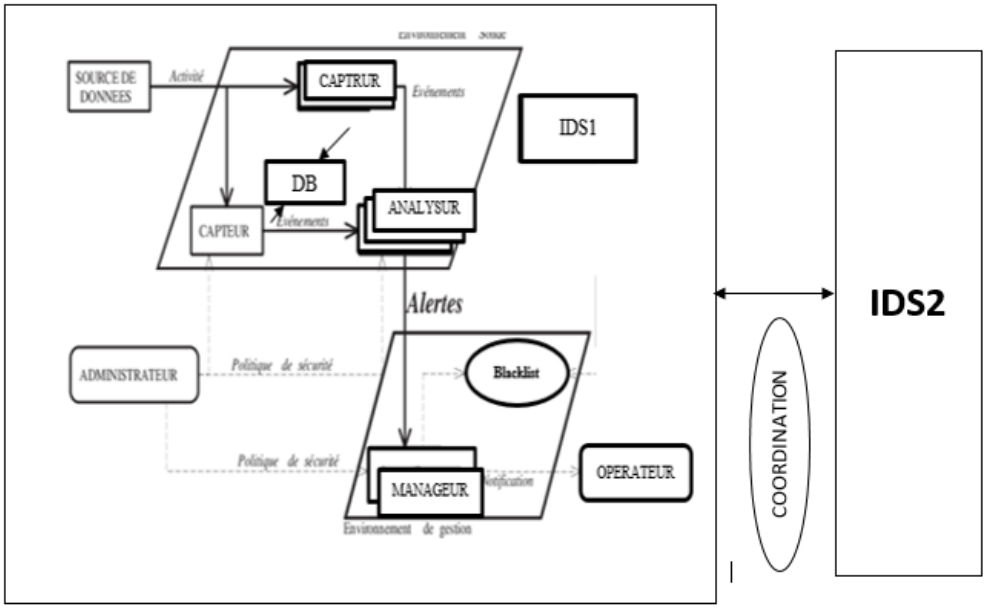


Figure5.2: Generic model of intrusion detection.

✓ We now that an agent is an entity in java (class/objet), so here the agents are classes)

1.2.Description

In this model, which represents the complete process of detection and data routing within an IDS? The administrator configures the different components (sensor(s), analyzer(s), and manager) according to a well-defined security policy. The sensors access the raw data, filter and format it toreturn only the events of interest to an analyzer. The analyzers use these events to decide whether or not an intrusion is present and if so, send an alert to the manager, who notifies the human operator, and a possible reaction can be carried out automatically by the manager or manually by the operator

- **Administrator:** Person in charge of setting up the security policy, and consequently, ofdeploying and configuring the IDS.
- **Captor:** is the Snort**.** in our work we have many captors,
- **Alert:** A formatted message issued by an analyzer if it finds intrusive activity in a data source.
- **Sensor:** software that generates events by filtering and formatting raw data from data source.
- **Event:** A formatted message returned by a sensor. It is the basic unit used to represent astep in a known attack scenario.
- **Manager:** A component of IDSthat allows the operator to configure the various elementsof a probe and to manage the alerts received and possibly the response.

- **Notification:** the method by which the IDS manager informs the operator of theoccurrence of an alert.
- **Operator:** The person responsible for using the manager associated with the IDS. The operator proposes or decides on the reaction to be made in case of an alert. It is sometimesthe same person as the administrator.
- **Reaction:** passive or active measures taken in response to the detection of an attack, to stopit or to correct its effects.
- **Probe:** a sensor or sensors coupled with an analyzer.
- **Data source:** a device generating information on the activities of the entities of the information system.
- **Analyzer:** Software tool that implements the chosen approach to detection (behavioral orscenario-based), it generates alerts when it detects an intrusion. In our work we have a many analyzer.
  WE defined some requests in our analyzer being able to associate a Java class model and a table structure in a database,the JPA specification describes a query language, called JPQL (Java Persistence Query Language). This language, which has the same functionalities as SQL, makes it possibleto query a database using the JPA entities defined in a persistence unit.

Dynamic queries

In the first way to create a JPQL query is to create a string that carries the query, andpass it to the create Query () method of the entity manager.
Example from our work:

```
public List<iphdr> getiphdrByName(String name) {

    Query query = em.createQuery("select iphdr from iphdr iphdr " +
                                 "where iphdr.nom = '" + name +  "'");

    List<iphdr> iphdr = query.getResultList() ;

     return iphdr ;
}
```

III. The implementation (our environment)

1. Definition of the windows operating system:

Windows is a desktop operating system developed by Microsoft. Forthe past three decades, Windows has been the most popular operatingsystem for personal computers.

Each version of Windows comes with a graphical user interface thatincludes a desktop with icons and a task. We work in the **windows 10 (64 bites)**

2. Eclipse IDE for Enterprise Java and Web Developers:

Eclipse is an integrated development environment (IDE) for Java andother programming languages like C, C++, PHP, and Ruby etc. Development environment provided by Eclipse includes the Eclipse Java development tools (JDT) for Java, Eclipse CDT for C/C++ andEclipse PDT for PHP, among others.

1.1. Install the Eclipse Java IDE

You can install the Eclipse Java IDE via an installer or via a packageddownload. Both approaches

are described here, using the installer is typical faster and easier.

Download and install JDK (optional if java is not installed onthe machine) install Eclipse IDE

Open the downloaded file and select 'Eclipse IDE for Enterprise Java andWeb Developers' from the pop-up.

Choose the installation folder and press the'INSTALL' button. Lastly, click on the 'LUNCH' button.

Now let us discuss these steps sequentially alongside visual aids to perceive better while installing. We choose Eclipse IDE for EnterpriseJava Developers.

3. **BASE**

- Install php-gd, which is used to generate the graphs in BASE.
- Install ADODB, which is a database abstraction library for PHP.
- It's now time to configure BASE itself. Edit the /usr/share/base- php4/base_conf.php file to ensure that the following lines are configured with paths and settings appropriate for your configuration.

```
$BASE_urlpath = '/base';
$DBlib_path = '/usr/share/ododb';
$DBtype         = 'mysql';
$alert_dbname   = 'snort';
$alert_host     = 'localhost';
$alert_port     = '';
$alert_user     = 'snort';
$alert_password = 'snortpass';
```

3.1.JDBC (Java Database Connectivity with MySQL)

To connect Java application with the MySQL database, we need to follow five following steps.Steps to connect Oracle database from Eclipse

The steps are exactly similar to what I have shown you before while connecting to Microsoft SQL Server from Eclipse IDE, the only difference is, this time, we are choosing Oracle from thelist of databases and installing Oracle JDBC driver instead of SQL Server JDBC driver.

Here are the exact steps to connect the Oracle instance from Eclipse:

- Open Eclipse IDE and Select Database Perspective (Windows >> Open Perspective
- >>Other >>Database Development).
- Create Connection Profile, Chose Oracle
- Choose JDBC Driver and specify its location
- Specify connection detail e.g. host, port, username, and password
- Test Connection

4. The technology of communication

4.1. SOCKET

We used Socket programming in Java for communication between the applications that are running on different JRE. It can be either connection-oriented or connectionless. Overall, a socket is away to establish a connection between a client (machine02) and a server (machine01).

The server forms the listener socket while the client reaches out to the server. Socket and Server Socket classes are used for connection-oriented socket programming.

4.2. Client/server paradigm

```
ServerSocket socketserveur = new ServerSocket(9999);
```

The ServerSocket class, implements a kind of socket that servers can use to listen and servers can use to listen and accept connections from clients. As for the client, it knows the name of themachine on which the server is running and the running and the port number on which it is listening. The client will request a connection to the server by identifying itself with its IP address and the port number linked to it.

```
SocketOfClient = new Socket(serverHost, 9999);
```

The Socket class implements a bidirectional connection between your Java program and another program located on the network.

One for the client and one for the server

When the server detects a new connection request, it must establish this connection (Establish a link between the two sockets).
Here is how to accept a connection from a client:

```
Socket S= SocketServer.accept();
```

Here is how to accept a connection from a client:

```
Socket S= SocketServer.accept(); s.close(); socketserver.close(); socketduserveur.close(); IOException e)
```

Used:

getInputStream() of the InputStream class. It allows us to manage the incoming streams; **getOutputStream()** of the OuputStream class. It allows us to manage the outgoing streams.These two methods allow us to manage the input and output streams.
In general, the type of input and output is **BufferedReader** for reading,
PrintWriter for writing.

The Server Side of a Socket

- We creating new project named Machine01
- We create a new class **"ServerProgram"**

The Client Side of a Socket

- We will create a new project named Machine02
- We create a new class named: **"ClientDem"**

Required Steps.

- Before we linking the BD with Snort and we get this table:
- By some sql query in java we will extract the ip addresses
-

```
+--------------------+
| Tables_in_snort    |
+--------------------+
| data               |
| detail             |
| encoding           |
| event              |
| icmphdr            |
| iphdr              |
| opt                |
| reference          |
| reference_system   |
| schema             |
| sensor             |
| sig_class          |
| sig_reference      |
| signature          |
| tcphdr             |
| udphdr             |
+--------------------+
exit
```

The following steps are required to create a new Database using JDBC application −

- Import the packages: Requires that we include the packages containing the JDBC classes needed for the database programming. We used:
- package org.o7planning.tutorial.socket;import java.sql.*;

- **Open a connection:** Requires using the **DriverManager.getConnection()** method to create a Connection object, which represents a physical connection with aselected database.

- Connectioncon=DriverManager.getConnection("jdbc:mysql://localhost:9999",snort","snort");

- Selection of database is made while we prepare database URL. We following this example tomake connection with Snort database.

- Clean up the environment: try with resources automatically closes the resources.

There are three different kinds of statements but in our work, we used:

Statement: Used to implement simple SQL statements with no parameters. Statement

```
stmt=con.createStatement();
```

Executing Queries

To execute a query, call an execute method from Statement such as the following:

- **executeQuery:** Returns one ResultSet object.In our work we following this code:

```
ResultSet rs=stmt.executeQuery("select:*from snort");
```

After you execute the SQL query, we might add a loop like this to read the results:

```
while(rs.next()) {
                String iphdr=rs.getNString("iphdr");
                System.out.println(iphdr+ "\n");
                }
                        con.close();
```

Now let us compile the above example as follows

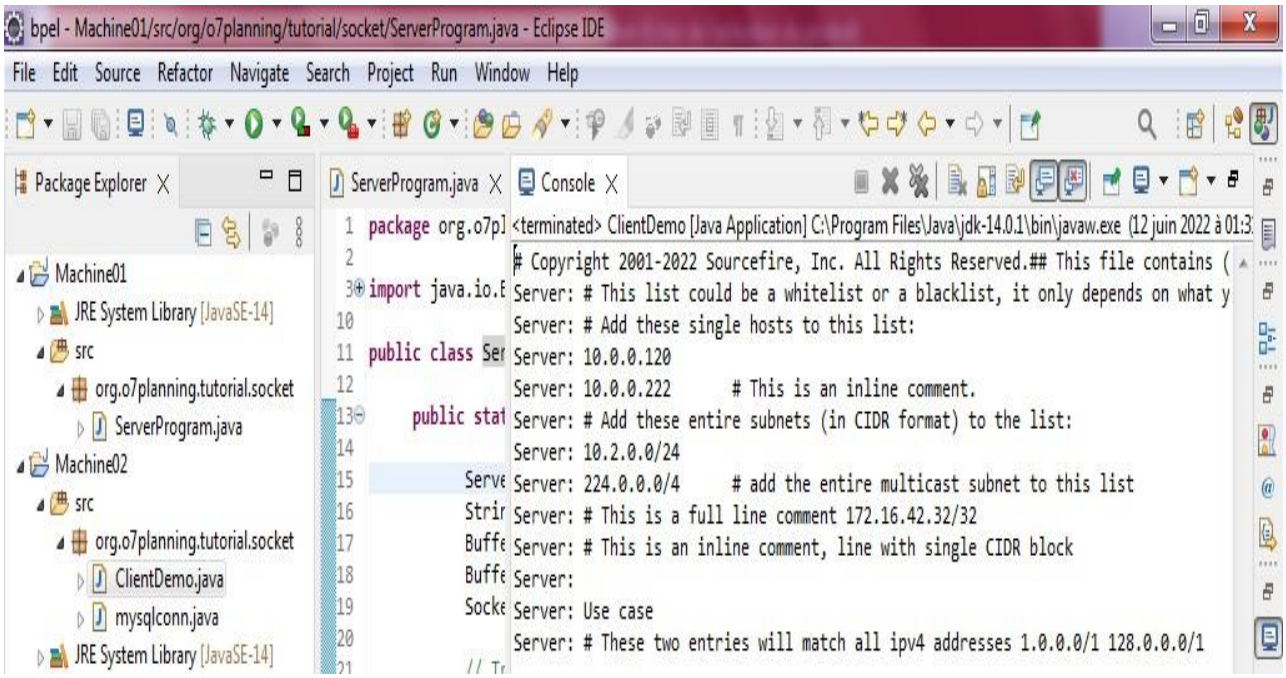
```
C:\>javac JDBCExample.java
C:\>
```

When you run JDBC Example, it produces the following result

```
C:\>java JDBCExample
Connecting to a selected database...
Connected database successfully...
C:\>
```

IV. The result

By the coordination of ids and by using the socket like a method of communication we get ablacklist that sends to the second machine (server)



V. Conclusion

In this last chapter, we have presented our proposed approach; we consider these advantages in order to build a distributed system for the coordinate of intrusion detection systems. We used Socket programming in Java for communication.

General conclusion

General conclusion

As a result, of this study examining the implementation of the intrusion detection system with SNORT in order to build a distributed system for the coordinate of intrusion detection systems. We used a concept of agent and several means such as JDBC, and Socket programming in Java.

First, we presented a synthesis on the computer networks, the knowledge on the generality of computer networks is essential to understand the functioning of the communication exchange such as the importance of the OSI reference model as well as the TCP/IP model. Then, we took an overview on the flaws and attacks that can threaten the computer security, as well as the known protective measures to protect it from hackers. At the end, we have performed a coordinate intrusions detection with SNORT.

For the realization of our approach we started with SNORT by setting up different sensors to detect intrusions that threaten our system. Thereafter we defined the analyzers which arise on the database generated by SNORT, the results are processed to generate the security rules that will be used by the different interconnected IDSs.

In fact, thanks to this approach, we can prevent network intrusions that can affect the network, the company can establish dynamic security policies and correct the fault in the network according to the types of attacks detected as well as to know at any time if it is the target of an intrusion attack.

As a perspective of this study, the use of mobile agents to increase coordination qualities and the deployment of this achievement on a multi-agent system platform, among other JADE or FIPA.

For an evaluation of the results and tests of our approach, we propose to apply it to a dataset such as KDD99 or DARPA which are intended for the evaluation of IDSs.

Bibliography

[1] https://www.tutorialsmate.com/2020/05/types-of-computer-networks.html

[2] https://www.researchgate.net/figure/Open-Systems-Interconnection-OSI-reference-model_fig2_242584084

[3] Memoryof master "BenbrahimEmbarka_AmicheSelyna"

[4] https://www.guru99.com/tcp-ip-model.html

[5] https://network-byte.com/data-encapsulation-and-decapsulation/

[6] Laurent Poinsot «Introduction à la sécurité informatique», support de cours,UniversitéParis 13.

[7] Les virus informatique clusif 2005, page 10

[8] Les virus et les spam, page 37

[9] Philippe Biondi, Architecture expérimentale pour la détection d'intrusions dans unsystème informatique, Article de recherche, Avril-Sptembre 2001

[10] Le grand livre de la sécurité informatique. SecuriteInfo, Editions du 6 nouvembre2006

[11] Laurent Bloch-Christophe Wolfhugel. Sécurité informatique .EYROLLES, 2emeedition. 2005.

[12] K.GHERBI, Réseaux virtuel privé.

[13] M.Tran Van Tay, le système de détection des intrusions et le système d'empêchement des intrusions (ZERO DAY), Rapport de stage de fin d'étude, institut de la francophonie pour l'informatique, université de Québec à Montréal, Féverier 2005.

[14] https://www.sciencedirect.com/science/article/pii/S0022000014001767(Article)

[15] http://securinet.free.fr/intrusions.html

[16] Cédric Michel, Langage de description d'attaques pour la détection d'intrusions par corrélation d'événements ou d'alertes en environnement réseau hétérogène, thèse dedoctorat de l'Université de Rennes1,16 Décembre 2003.

[17] https://www.researchgate.net/figure/Basic-idea-of-a-cooperative-anomaly-and-intrusion-detection-system- CAIDS-built-with-an_fig2_228958064

[18] Jonathan-Christofer Demay, Génération et évaluation de mécanisme de détection d'intrusionsau niveau applicatif, Thèse de doctorat, école doctorale Matisse, université deRennes1 Juillet 2011

[19] http://igm.univmlv.fr/~dr/XPOSE2009/Sonde_de_securite_IDS_IPS/IDS.html#:~:text=Approche%20par%20sc%C3%A9nario&text=Ce%20principe%20de%20d%C3%A9tection%20implique,devient%20invisible%20par%2 0l'IDS.

[20] Hervé Debar, Benjamin Morin, Frédéric Cuppens, Fabien Autrel, Ludovic Mé, Bernard Vivinis Salem Benferhat, Mireille Ducassé, Rodolphe Ortalo, Détection d'intrusions : corrélationd'alertes. Article de synthèse, Caen, France, 2004.

[21] https://www.researchgate.net/figure/Classification-of-intrusion- detection-systems_fig3_221911299

[22] https://www.securiteinfo.com/conseils/choix_ids.shtml#:~:text=R%C3%A9activit%C3%A9
%20%3A%20Un%20I
DS%20doit%20%C3%AAtre,sont%20pour%20ainsi%20dire%20indispensables.

[23] Yann Berthier, Jean-Baptiste Marchand, Détection d'intrusions et analyse forensique.

[24] Thierry Evangilista, Les IDS Les systèmes de détection d'intrusions informatiques édition DUNOD, Paris 2004.

[25] Summer '92 USENIX - June E-June 12,lgg} - San Antonio, TX

[26] Architecture-de-SNORT-Dans-larchitecture-proposee-nous-allons-utiliser-SNORT_fig2_301297336

[27] Sarker, I.H., Abushark, Y.B., Alsolami, F., Khan, A.I.: IntruDTree: A Machine Learning Based Cyber Security Intrusion Detection Model, p. 754. Symmetry. Multidisciplinary Digital Publishing Institute (2020)

[28] Memory of master "University Belhadj Bouchaib d'Ain-Témouchent" [Arlabosse, 2004].

[29] Ferber 95, Cohen & Levesque, 88; 90

[30] Bond, 82, Rao & George, 92, Cohen & Levesque, 87; 90. 1995,Ferber, 1997.

[31] Chaib-Draa et al., 89, 2001

[32] Wathiq Laftah Al-Yaseen et al, Adriana Leite, et al 2017

[33] NedaAfzali et al2014

[34] http://www.sestream.com/docCom/Snort.pdf

[35] http://univbejaia.dz/xmlui/handle/123456789/5296;jsessionid=174D73F4BEC745FC38B662 3C40228B76

[36] https://www.researchgate.net/figure/Fig3-Architecture-de-SNORT-Dans-larchitecture-proposee- nous-allons- utiliser-SNORT_fig2_301297336

[37] https://doc.rero.ch/record/327843/files/IlirKadriu_TB.pdf

[38] https://snort.org/
[39] Durfee Edmund H., “Scaling Up Agent Coordination Strategies,” University of Michigan. IEE July 2001.
[40] Durfee E. H., Lesser V. R., “Partial Global Planning: A Coordination Framework for Distributed Hypothesis Formation”, © IEEE 1991.

Résumé:

Avec l'évolution des ordinateurs, de l'information et des réseaux, la vulnérabilité aux intrusions a augmenté. Afin de faire face à ce phénomène, plusieurs travaux et recherches ont vu le jour.
L'objectif principal de cette étude est la détection d'intrusion pour sécuriser un réseau local en utilisant un réseau d'IDSs basé sur des systèmes multi-agents et un IDS Open Source, qui est le SNORT.
Dans ce travail nous proposons une approche coordonnée dans la détection d'intrusion, qui a combiné l'utilisation de plusieurs technologies, entre autres le développement d'applications distribuées, la consultation d'une base de données (JDBC), et les systèmes de détection d'intrusion.

Mots clés:

Sécurité Internet, SDI, SNORT, approche collective, JDBC, Socket, M.A.S.

Abstract:

With the evolution of computer, information and networks, the vulnerability to intrusions has increased. In order to face this phenomenon, several works and researches were born.

The main objective of this study is the detection of intrusion to secure a local network by using a network of IDSs based on multi-agent systems and an Open Source IDS, which is the SNORT.

In this work we propose a coordinate approach in intrusion detection, that have combined the use of several technologies, among other the development of distributed applications, consultation of a database (JDBC), and intrusion detection systems.

- **Key words :**

Internet security, IDS, SNORT, collective approach, JDBC, Socket, M.A.S.

الملخص:

ولمواجهة هذه الظاهرة بدأت عدة أعمال وابحاث .ومع تطور أجهزة الكمبيوتر والمعلومات والشبكات أزداد احتمال حدوث غارات
والهدف الرئيسي من هذه الدراسة هو الكشف عن الاختراق لتأمين شبكة محلية باستخدام شبكة من IDSsقائمة على أنظمة
متعددة الوكلاء ونظام IDSمفتوح المصدر IDSوهو نظام .SNORT
ونحن نقترح في هذا العمل مقاربة منسقة للكشف عن الاختراقات والتي جمعت بين إستخدام العديد من التقنيات مثل تطوير التط
بيقات الموزعة واستطلاع قاعدة بيانات JDBCوأنظمة اكتشاف الاختراق.

الكلمات الأساسية:

أمن الإنترنت وSDI وSNORT وGDBC وSOKET وM.A.S