Introduction

This research study named "**security in IP networks"** is aimed to give a deep vision of the existing risks in the networks connected to Internet as well as of the principal existing systems of safety.

Internet, also named the network or network of networks, has become the last decade in a phenomenon that society has revolutionised. From the appearance of the television no other has been seen social phenomenon of such a depth or that evolves so fast.

Of many factors that have converged in this new phenomenon to catapult it massively to current society, we can emphasise three principally:

- The growth of the computers in all the areas of society (companies, universities, governments…) it has contributed to computerize almost any aspect of our life.

- The rapid change in the communications technology (faster, cheaper, better) has accelerated even more the launching of Internet.

- The universal character of Internet that permits the general and permanent connectivity of the whole planet in an economic and practically instantaneous way, it converts into an essential tool for practically any type of communication.

Consequently, each day hundreds of million of people throughout the world use Internet as part of their work and fun. Equal way than in any other service used by a great quantity of people (as the metre or the roads), safety is a basic factor that must always be taken into account.

> **Safety** (l. securitate) : *Quality of insurance* [WWW1].
> **Surely, - ra** (l. securu): *Free of any danger or risk* [WWW1].

From a sociological point of view, in any social group a small percentage of its population is spiteful [CZ95]. Internet has reached in 2002 more than 160.000.000 of connected computers [WWW5] by adding a total by considering of 580.000.000 of users throughout the world [WWW6][WWW7].

If only the 1 per one hundred of the population belongs to this sector we have almost 6 million (5.800.000) possible attackers. Also only meaning that one for thousands we have the amount of almost six hundred thousand (580.000) potential dangers.

The aim of this study concentrates precisely on the analysis of the dangers and more common threats that exist in Internet as well as the new safety mechanisms that aim to provide a solution to them.

1.1 Summary of the chapters

The structure that presents this work is divided into five chapters that will be grouped in two blocks. The first part refers to the theoretical research work and of first four chapters is made up, while the second part is made up of chapter five where the experimental part made is presented.

1. **The TCP/IP protocols**: In the first chapter an explanation in depth of the family of protocols TCP from version 4. The characteristics and more important functionalities that present the protocols IP, ICMP, UDP and TCP as well as its inter-relationship and paper that play in the communication of systems connected to Internet.

   Is also explained the transfer process of the datagrams by Internet (package routing process) until local destination network (LAN) is reached. The local delivery process where the owner of specified IP address is found using ARP/RARP is explained too.

2. **Denial of service DOS / DDOS**: In this second chapter we will make a historical review of the change in the attacks to computer networks in Internet, centring us on the study and classification of the attacks of denial of service or DOS.

   DOS Attacks are those intended to secure in a total or partial way the ending of an existing service. These attacks are based on the use of different technologies that try collapse service in itself or the computer that it supports through a flood of fraudulent requests.
   DOS Distributed attacks (DDOS) are characterised by the synchronisation of several different computers that focus their attacks in a coordinated way towards a common destination.

   In the final part of this chapter we will make an exhaustive analysis of a real DDOS registered in Internet on 11 January 2002.

3. **Intrusion Detection Systems (IDS)**: In this third chapter we will make an explanation of the intrusion detection systems or IDS. We will comment on the taxonomy into which the detection systems are divided:

   - Computer IDS systems or HIDS.
   - Network IDS systems or NIDS.

   We will focus our research work mainly in NIDS, a change in the primitive firewalls that only filtered the existing network traffic between Internet and the network LAN. Among its new capacities they add that to analyze the existing traffic throughout the local network in search for anomalies or suspicious behaviour.

   We will also analyze its protocols of communication, their possible locations and architectures as well as the limitations that they can present. The concepts of false negative false positives will also be introduced and that refer to the erroneous detections that produce sometimes these systems or to the non detection of a strange behaviour by the IDS.

   Finally in this chapter we explain the famous "Mitnick attack" perpetrated by one of the most famous hackers than the world: Kevin Mitnick. These attacks lead Kevin to several years of jail. At present this classic attack is considered the minimum threshold of detection for a system IDS.

4. **Honeypots and Honeynets**: In the last matter of the research part these new tools will be described that is being produced as a result of the change in communications in Internet.
   The reduction in price of the connection costs and the increase in the width of band available amend the typical stages of attacks. Consequently the researcher Community offers a new tool of safety: the Honeypot.

   Honeypots are passive systems whose performance is based in being designed to be attacked and even committed by any attacker. The aim to have a system intended to be attacked is double:

- On the one hand permit the study of the behaviour and real technologies that use the hackers in a "real" environment. This environment can be formed so that it may even be capable of giving false information to possible attackers.

- On the other hand, the existence of a system with these characteristics allows us to divert the attention on our real systems and to prepare them for the attacks registered in the Honeypot.

The Honeynets are a specific type of Honeypots. The aim Honeypots is the existence of different grouped in a network "isolated" of the production network with the aim of creating a more likely environment for the possible attackers.

We will comment on both generations (GENE I and GENE II) of Honeynets existing as well as its characteristics and principal architectures. We will also introduce the virtual concepts of Honeynets and distributed that permit the minimisation of the necessary resources for implementation of these technologies.

5. **Analysis of a system connected to Internet**: In the fifth chapter the experimental party of this work make. Our aim is that to monitor for seven days a system connected permanently to Internet.

   We will analyze the different aims that the task required puts forward and we will set out the different requirements of the experiment. An architecture of network will be offered that satisfies our requirements and the different tools will be chosen (software and hardware) that will allow us to evaluate our experiment.

   The presentation of the data will be made by a daily report detailed with the data of the network traffic obtained (different requests and received attacks) that will be separated in traffic registered by type of service (SSH, WWW…) and by type of protocol to which it refers.

Also a weekly report will finally be presented that will contain the registered most relevant aspects for the seven analyzed days as well as the conclusions obtained from the experiment.

In the final part of this work the conclusions obtained will be presented during the realization of this report as well as the future lines of continuation that might be carried out.