

Intrusion detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses *vulnerability assessment* (sometimes referred to as *scanning*), is a technology developed to assess the security of a computer system or network.

The term “agent”, or software agent, has found its way into a number of technologies and has been widely used, for example, in artificial intelligence, databases, operating systems and computer networks literature. Although there is no single definition of an agent, all definitions agree that an agent is essentially a special software component that has autonomy that provides an interoperable interface to an arbitrary system and/or behaves like a human agent, working for some clients in pursuit of its own agenda. Agents may decide to cooperate for mutual benefit or may compete to serve their own interests. Therefore, an agent is autonomous, because it operates without the direct intervention of humans or others and has control over its actions and internal state. An agent is social, because it cooperates with humans or other agents in order to achieve its tasks. An agent is reactive, because it perceives its environment and responds in a timely fashion to changes that occur in the environment. In addition, an agent is proactive, because it does not simply act in response to its environment but is able to exhibit goal-directed behavior by taking initiative. Moreover, if necessary, an agent can be mobile; mobile agents have the ability to move from host to host, executing at each place and then keeping the results before moving to the next server. To be able to move, there must be an agent server, sometimes called agency, on each host that handles the incoming agents and executes them. This agency is also responsible for sending messages between agents and does some authentication if necessary.

As mentioned, the agent can migrate and this is the most powerful and important characteristic we could use to detect intrusions in a network. In other words, we use this capability to capture data in each network's node. This is more performant than capturing packets in one node; so, it is similar to a distributed detection system. After an agent has migrated to each node in local network, it starts to capture all the TCP packets that come to that node. After a period of time, the agent stops capturing and starts treating those packets by two different algorithms and make decisions according to the fact it is a scanner, suspicions or legitimated user.

There are many works in this field, we mention: Mobile Agents in Intrusion Detection System (2011), intelligent intrusion detection system framework using mobile agents (2009), a

Distributed Autonomous-Agent Network-Intrusion Detection and Response System (2005), Applying Mobile Agents to Intrusion Detection and Response (1999), an architecture for Intrusion Detection

Using Autonomous Agents (1998).

In this context, our objective is to realize an intrusion detection system based on mobile agents. Mobile agents make the system more performant because it will create agents that can migrate from a host to another. These agents are fully independent of the source host. They can capture data and decide if there is an intruder or not even without returning to the source host.

In this work we try to realize an application to detect TCP port scanning by mobile agents in Local Network, using the API Jpcap to capture packets and treat everyone by two different algorithms: Slow port scan and port scan. After that, the decision will be made by the agent whether it is a scanner IP or not. Concerning the port scan algorithm; if there is an intrusion the mobile agent will shut down the attacker host. Except when the attacker does not have the environment Aglets, the mobile agent cannot shut down the attacker host but avoids further scans from this host. In slow port scan, we choose other decision; suspicious IP or Scanner IP or legitimated IP. If it is a suspicious IP, the mobile agent will wait for more time to capture more packets. If this IP occurs three times in a suspicious list, the agent removes it from this list and adds it to the scanner list. If the same IP sends successive packets and has the same destination port or consecutive destination port, the IP will be removed from the suspicious list and added to the scanner list.

Our manuscript is organized in three chapters. The first one deals with the agent and mobile agent and its utility in Computing Science. The second one is about the intrusion detection systems, Port scanning and the tools which are used in this domain. The third chapter presents the conception of our application and the results obtained.