

An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. “From the two definitions stated above, it clearly appears that IDS’ function is different from other types of security devices such as firewall, intrusion prevention system (IPS), and so forth. The next question which arises is whether IDS comes in the form of hardware or software.

Mobile agent technology has benefited from the work done on intelligent agents. It emphasizes static autonomous agents capable of applying application domain knowledge, and the development of software systems capable of supporting mobile code on heterogeneous hardware (e.g., Java technology). Intelligent agents embody the ability to decompose and solve problems in a collaborative fashion. Agents observe their environment, reason about their own and other agents’ actions, interact with other agents, and execute their actions concurrently with them.

In this paper, we have used a mobile agent to capture and analyze packets to make a decision according to the Port Scan algorithm or slow port scan. A warning message will appear, if an intrusion is detected, and if the attacker PC continues scanning, the capturing agent will update the database by inserting the IP, MAC addresses and the name of hostname of the attacker PC, the mobile agent responsible of shutting down the PC will shut down the attacker PC.

To realize this system, we faced many problems. The most difficult, it consisted in dispatching the mobile agent to a remote host because we had to change the policy of Java to by changing the files in JDK folder installation. Besides, the coding of a mobile agent to capture, analyze and shut down the PC was so difficult to finish.

The objective of our system was to detect the intrusion using mobile agents, but we could use two different algorithms. We ameliorate the Port Scan algorithm using a database and take action after the intrusion has been detected. We ameliorated Slow Port scan by treating the suspicious IP and taking action after finding an IP scanner.

Our perspectives are trying to use the Internet, the subnets in LAN and use other programs to scan the victim PC because we use one program here to test our system which is Nmap.