Journal of Theoretical and Applied Information Technology
20th January 2014. Vol. 59 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A MULTI-AGENT BASED DISTRIBUTED INTRUSION PREVENTION SYSTEM AGAINST DDOS FLOODING ATTACKS

[1]A. SAIDI, [2] A. KARTIT, [3]M. EL MARRAKI

[1]ALaboratoire De Recherche En Informatique Et Télécommunications
Unité Associée Au CNRST (URAC 29), Faculty of Sciences,
Mohammed V-Agdal University, B.P.1014 RP, Agdal, Rabat, Morocco
E-mail: [1]abdelali.saidi@gmail.com, [2]alikartit@gmail.com, [3]marraki@fsr.ac.ma

ABSTRACT

Denial of service (DoS) attacks is a simple and very annoying type of intrusions. This kind of attacks attempts to make unreachable at least a service of equipment like it can stagnate the whole of a network. To launch a DoS attack, we have, nowadays, often tools to succeed. Some of these tools try to send a compromised network load to corrupt their targets by flooding it with SYN, UDP or ICMP packets [1],[2]. Our paper describes the conception of a multi-agent-based intrusion prevention system (IPS) that can apprehend these flooding attempts in a distributed way.

Keywords: *DoS Attacks, Intrusion Prevention, Multi-agent System, Distributed System,*

1. INTRODUCTION

With the distributed concept of Internet, and the easiest way to download tools to perform an unnumbered type of attacks, security administrators are faced with a huge challenge to protect their information system. For the flooding attacks, tools try to send as many packets as it have to make a service or a machine out of service.

Three types of flooding DoS attacks exists: SYN flood, UDP flood and ICMP flood.

- SYN flood attack: it consist on sending many TCP connection requests to a target. This latter will accept the establishment of the connection and notify the client. Except that, this one will never use them. Thereby, the server will be drown by unused connections and, eventually, will not reply to legitimate users requests.
- UDP flood attack: this kind of flooding attack consist on sending many UDP packets to different port of a target in random way. This target will check if there's any application on the relevant port, if not, he will be occupied to send ICMP replies and can't treat requests from legitimate clients.
- ICMP flood attack: or smurf attack. Consist on sending many ICMP packets with a spoofed IP source address. The owner of this IP address will be the destination of many ICMP responses and will be flooded.

2. DOS FLOODING ATTACKS: TECHNICAL DETAILS

2.1 SYN Flood Attack

When a client and a server try to establish a connection, they must proceed to the TCP three-way handshake. It means that the client begin by sending a request for synchronization (SYN). Then, the server acknowledges this request by sending back a SYN-ACK message to the client. Finally, the client sends an ACK message and the connection is done.

Unfortunately, malicious people found a way to compromise a server machine by corrupting the three-way handshake procedure. For this, they send a large number of SYN requests without acknowledging the SYN-ACK response server. When the legitimate employees try to contact the service, they won't find any free connection. Fig. 1 describes this connection establishment procedure corrupted.

Journal of Theoretical and Applied Information Technology
20th January 2014. Vol. 59 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

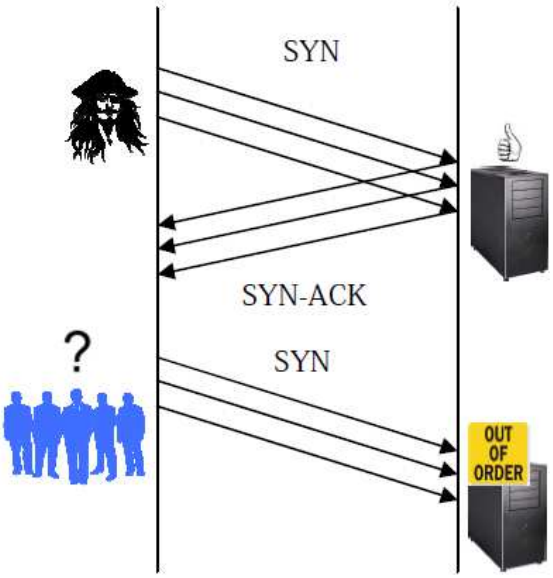

Figure 1: Syn Flood Attack

2.2 UDP Flood Attack

Unlike the TCP protocol, UDP come with a serious problem in case of bandwidth congestion. UDP protocol doesn't apply a congestion mechanism to have an idea about the state of the network and to avoid the congestion of his bandwidth. Therefore, some people may initiate an attack by sending randomly a large number of UDP packets to a target. Thereby, the network may stagnate (UDP connections consume the TCP ones). Moreover, the target will check for applications that are obviously listening on destination ports. And when it finds that there are no applications behind some ports, he would reply with an ICMP destination unreachable messages. This will increase the congestion problem and consume of the target's resources and the bandwidth because of the huge number of the sent UDP packets.

2.3 ICMP Flood Attack

Also called "Ping Flood" - and not to confuse with "Ping of Death Attack" - try to submerge a target with ICMP packets (pings). It can consume the target resources and put it in a denial of service. Also, if we forge oversized ICMP packets that fragment on route, the bandwidth will be affected and the network will stagnate.

NB: Normally, the attacker spoof his IP address not only to hide his identity, but also to avoid being flooded with responses.

3. THE INTERNE ARCHITECTURE OF AN INTRUSION DETECTION SYSTEM

The naturally work of IDS come with three basic components: the sensor, the analyzer SYN and the response module. Fig. 2 shows this common interne architecture of IDSs.

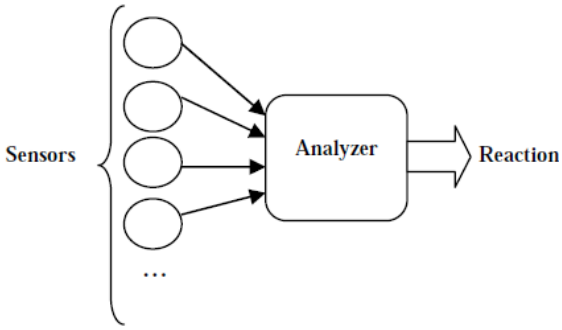

Figure 2: Common Internal Architecture Of Idss

- Sensor: This module is the collector of the system. It can be placed on a segment of the network, like it can be placed on a machine to grab specific data. If we deploy many collectors for this vocation from a whole network - like our case here - we will be placed in distributed detection.
- Analyzer: This is where collected data will be gathered to be treated. This element is the responsible of the detection.
- Reaction module: Here the module who's responsible of the counter measure to an intrusion. If it has a passive reaction, our system would be called an intrusion detection system, otherwise, if the reaction is a counter measures that try to prevent the intrusion, or at least, to curb damages, the system will be called an intrusion prevention system.

4 A MULTI-AGENT BASED INTRUSION PREVETION SYSTEM (MA-IPS)

4.1 Benefits of using a multi-agent system

Under the limited capacities of the only analyzing module in centralized DIDS, problems like single point failure, late response and lost of security data cause disgrace to security administrators. Thus, IDS were leader to a new concept: the distributed detection [4].

Also, with the use of multi-agent systems, this concept crowned by many benefits [5], [6], like:

- Great retention of the network bandwidth since the multi-agent

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

systems communicates with the lightest messages.

- Agents have a complete independency, a strong flexibility and a good scalability
- Also, there is a brilliant resilience that makes every agent well covered by its upper one.

4.2 The multi-agent DIPS framework

This following framework consists of a number of agents that work independently for the same vocation: the detection of intrusions in distributed manner.

Our multi-agent based DIPS has the goal to face distributed denial of service based on flooding techniques. Fig. 3 shows the said framework.

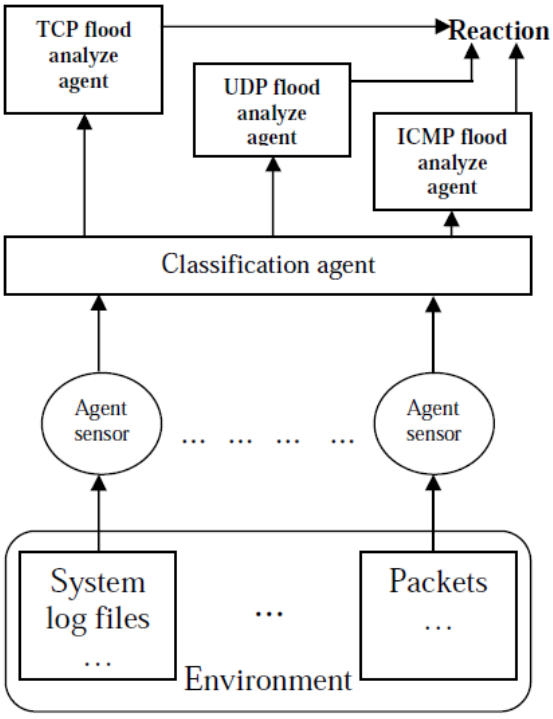

Figure 3: A Multi-Agent System Framework To Flooding Attaks Detection

The environment represents the controlled network. Security data that we may need for the detection can be collected from machines (system log files) or from network segments (packets).

According to the nature of the environment, two types of agent sensors impose themselves. The first one will keep an eye on specific system log files. And another one who will be placed in a segment of out network to wait for specific packets.

Latter agents, in the case of appearance of the specific security data, will transfer this data to another agent: Classification agent. This one is responsible to pre-treat received data and to classify it for further transfer. Relying on this work, this agent will forward each security data to the concerned analyzer.

We have three types of analyzer according to the three flooding attacks that we're trying to prevent. Every one will be able to look for flooding attacks even if they are distributed. This advantage is due to the work given by the classification module.

If any analyzer comes to detect a flooding attack, it will contact the reaction module to take some measures of prevention. This means:

- To curb damages by sending orders to a set of execution elements. This set contains agents implemented near to the TCP flood analyze agent UDP flood analyze Reaction sources of the gathered security data. Their duty would be to stop the specific flow that's responsible of the detected attack. And if it's necessary, to disconnect its computer.
- To warn the target of the TCP connections that will never be acknowledged, of the UDP contact that he don't have to look for their appropriate applications and for the ICMP requests that he must simply liberate and ignore.

On the reaction part, every flood attack analyze agent will contact some execution agents. The execution agents will be placed in critical nodes. The following figure represents the location of this agent's kind:

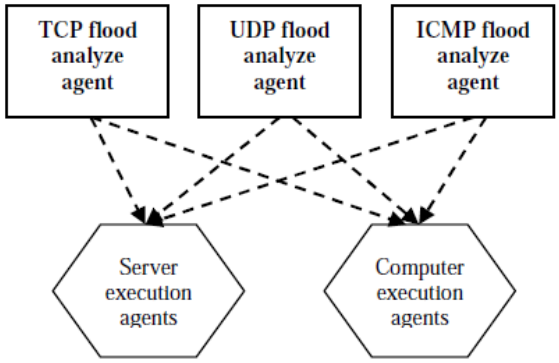

Figure 4: MA-IPS Reaction

Journal of Theoretical and Applied Information Technology
20th January 2014. Vol. 59 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The server execution agents have to free every senseless resource allocation. The TCP flood analyze agent will give it order to terminate unacknowledged requests. The UDP flood analyze agent order it to ignore the random port requests. The ICMP analyze agent order it to not respond to some pings.

The computer execution agents are placed in the local machines. Their aim is to stop interne flood attacks. Every analyze agent that detect an attack will give order to every execution agent deployed on sources of the attacks to stop its flooding data at least. It may disconnect this machine from the local network.

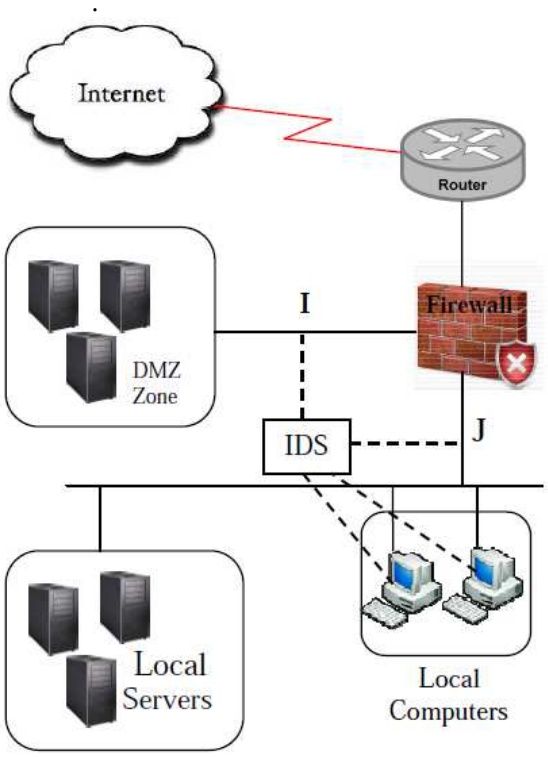

Figure5: Network Of Test

To collect our security data, sensor agents have to be deployed in many places of our LAN. The ones that collect specific system logs files will be placed in every employee's computer. Others will be placed I and J (Fig. 4) to keep an eye on Internet and employee's traffic way to DMZ zone. When a matter happens, this agents report it to communication agents of every deployed MA-IDS. This help local analyze agent to discover a one source attack and permit the others to have a global look on the every segment in the LAN (for distributed attacks).

Alerted by sensor agents, communication agents must restore security data and classify it according to its type and archiving it on a database. TCP traffic will be sent to the TCP flood analyze agent, UDP traffic will be sent to the UDP flood analyze agent and the ICMP traffic will be sent to the ICMP flood analyze agent. Thus, common flooding traffic will be gathered even if it's sent from different sources.

Here, every analyze agent must detect its type of flooding and take a decision. This latter is on the concern of reaction agents. Normally, in the case of detection, the analyze agent will give following orders:

- To bloc the source of the flooding attacks. This requires the deployment of a reaction agent near to every sensor agent.
- To terminate connections established in the concerned server (the victim). Also, this requires the deployment of reaction agents in our servers.

5 CONCLUSION

It's necessary for a security administrator to have a global view of the whole LAN to control it. For this aim, he may deploy many IDSs as it seems to be necessary. Deploying heterogeneous IDSs to form one global DIDS is absolutely not a solution.

The main features of a DIDS are: communication between its components and a fast analyze to assure a global view of the whole network and an efficient analyze locally. By distributing IDS's tasks, a LAN become one little system to monitor. And agents seem to be the more adequate technology for this work.

REFRENCES:

[1] S.T. Zargar, J. Joshi, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", *Communications Surveys & Tutorials, IEEE*, vol.PP, no.99, 2013, pp.1,24, 0.

[2] X. Chuiyi, Z. Yizhi, B. Yuan, L. Shuoshan , X. Qin, "A Distributed Intrusion Detection System against flooding Denial of Services attacks", *Advanced Communication Technology (ICACT)*, 2011 13th International Conference on, vol., no., pp.878,881, 13-16 Feb. 2011.

[3] C.V. Zhou, C. Leckie, S. Karunasekera, "A survey of coordinated attacks and collaborative intrusion detection", *Computers & Security*,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Volume 29, Issue 1, February 2010, Pages 124-140, ISSN 0167-4048.

[4] S.R. Snapp, J. Brentano, G.V. Dias, T.L. Goan, L.T Heberlein, C. Ho, K.N. Levitt, B. Mukherjee, S.E. Smaha, T. Grance, D.M. Teal, D. Mansur, "DIDS (Distributed Intrusion Detection System) - Motivation, Architecture, and An Early Prototype", *In Internet besieged, Dorothy E. Denning and Peter J. Denning (Eds.)*. ACM Press/Addison-Wesley Publishing Co. New York, NY, USA 211-227.

[5] W. Huang, Y. An, W. Du, "A Multi-Agent-Based Distributed Intrusion Detection System", *3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, vol.3, no., pp.V3-141,V3-143, 20-22 Aug. 2010.

[6] G.R Suryawanshi, S.B Vanjale, "Mobile Agent for Distributed Intrusion detection System in Distributed System", *International Journal of Artificial Intelligence and Computational Research (IJAICR.)*, Jan-June 2010 , issue of the journal. Published by: International Science Press. ISSN-0975-3974.

[7] C.V. Zhou, C. Leckie, S. Karunasekera, "A survey of coordinated attacks and collaborative intrusion detection", *Computers & Security, Volume 29, Issue 1, February 2010*, Pages 124-140, ISSN 0167-4048.

[8] A. Baláž, J. Trelová, M. Kostráb "Architecture of Distributed Intrusion Detection System Based on Anomalies", *Intelligent Engineering Systems (INES), 2010 14th International Conference on*, vol., no., pp.79,83, 5-7 May 2010.

[9] A. Kartit, A. Saidi, F. Bezzazi, M. El Marraki & A. Radi, "A new approach to intrusion detection system", *Journal of Theoretical and Applied Information Technology*, Vol. 36, No. 2, 2012, pp. 284-289.

[10] A. Kartit, M. El Marraki, A. Radi and B. Regragui, "On the security of firewall policy deployment", *Journal of Theoretical and Applied Information Technology*, Vol. 22, No. 2, 2010, pp. 84-92.

[11] A. Radi, A. Kartit, D. Aboutajdine, B. Regragui, M. El Marraki, A. Ramrami, "On The Three Levels Security Policy Comparison Between Svm And Decision Trees", *Journal of Theoretical and Applied Information Technology* pp 056-068 Vol 35. No. 1–2012.