International Journal of Computer Network and Security (IJCNS)
Vol 6. No.1 – Jan-March 2014 Pp. 40-45

available at : www.ijcns.com
ISSN: 0975-8283

ACHIEVING HIGHER NETWORK SECURITY BY PREVENTING DDOS ATTACKS USING HONEYPOT

H.C.Parimala[1], Kavitha Balamurugan[2]
Department of Electronics and Communication Engineering,
KCG college of Technology, Karapakkam, Chennai,
Tamil Nadu, India – 600097
Email: parimala.hc1991@gmail.com, kavitha@kcgcollege.com

ABSTRACT

In the recent years, Internet has become a widespread method to connect the computers all over the world. While the availability of continuous communication has provided many novel opportunities, it has also brought new possibilities for malicious users especially through the Distributed Denial of Service (DDoS) attacks. These attacks are mainly used for flooding a particular victim with massive traffic. Hence the early detection and the mitigation of these attacks have become inevitable to save the expensive resources of the network. In this paper, a technique combining the FireCol and honeypots is presented for the prevention of the DDoS attacks. The FireCol consists of a set of Intrusion Prevention Systems (IPSs) located at the Internet Service Providers (ISPs) level [6]. The honeypot is a trap set to detect and thwartthe attempts of unauthorized use of the information systems[8]. The evaluation of this technique using simulations with NS2 simulator for the detection of DDoS attacks and java for the implementation of low interaction honeypot server which is HoneyRJ [4] is presented showing the effectiveness of the solution in increasing the security and reliability of the network[11].

Keywords—IPS, HoneyRJ, DDoS attacks, detection, mitigation.

1. INTRODUCTION

Distributed Denial of Service (DDoS) attacks utilize multiple distributed attack sources. In general, the attackers use a large number of controlled web robots also referred to as zombies distributed in different locations to launch a large number of DoS attacks against a single target or multiple targets. With the rapiddevelopment of botnets in the recent years, the attack traffic scale caused by DDoS attacks has been increasing with the targets including not only business servers but also Internet infrastructures such as firewalls routers and Domain Name Systems (DNSs) as well as the network bandwidth [8]. In addition to maintaining low latency and good performance, filtering unauthorized accesses has become one of the major concerns of the server administrator.The enormousgrowth of computer or network attacks is becoming more and more difficult to identify and hence the need formore efficient intrusion prevention systemsincreases in step. The main problem with the currentintrusion prevention systems is the high rate of false alarmsand high overhead on the original server. Consequently, the use of honeypots helps in creating more secured systems [11].

2. RELATED WORK

A lot of research has been done on the DDoS attacks but some of the related research has been highlighted here. S.H.Khor et al [10] proposed an on demand overlay architecture that makes perpetrating DDoS difficult by proliferation of access channels to the server and local DNS (LDNS) segregation mechanism.A.El-Atawy et al [1] introduced a novel technique known as Relaxed Policy Expression which was shown to provide an efficient filter for unwanted packets or easy to accept (or reject) packets based on the policy definition and statistics of the incoming traffic. Feinstein.L et al [5] proposed methods to identify DDoS attacks by computing entropy and frequency-sorted distributions of selected packet

International Journal of Computer Network and Security (IJCNS)
Vol 6. No.1 – Jan-March 2014 Pp. 40-45
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0975-8283

attributes. Janakiraman.R et al [9] proposed a scheme of distributed intrusion detection systems running over peer-to-peer networks to guard the network as a whole against intrusion attempts.Ying Xuan et al [12] proposed a novel group testing based approach deployed on back-end servers for detecting application DoS attack but it seems to have high overhead.Francois.J et al [7] discusses the preliminary architecture of FireCol which involves providing distributed protection service only to the subscribed clients with minimal communication overhead.

3. PROPOSED WORK

The combination of FireCol and the honeypot servers [2] helps in obtaining the information about the attackers which helps in improving the overall security. This consequently tries to lower the risks that are directed to that particular network.But the existing work involves only blocking the traffic related to the corresponding attack by a group of IPSs. The architecture of the proposed system is depicted in Fig. 1. The methods in preventing the DDoS attacks involves the subscription to the FireCol service as the first step. When the client sends a request, the server adds the client with the subscribing rule along with its subscription period or time to live (TTL) and the supported capacity. The server then periodically issues a token to the customer with a TTL and a unique ID signed using its private key.

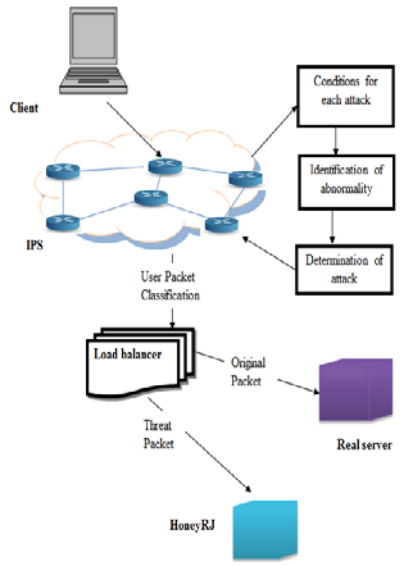

Figure. 1 System Architecture

The IPSs form virtual protection rings around the clients to defend and collaborate by exchanging selected traffic information.The ring level of each IPS is regularly updated. For this process the router first sends a request messageto the protected client containing a counter initialized to 0. The counter is incremented each time it passes through an IPS. The client then replies to the initiating router with the value of its ring level.

The value of the ring level is network dependent [6]. The system checks the incoming traffic for the presence of attacks through the database storedabout the attacks in each IPS [3]. When the client sends the data to the network, each packet is analysed and if there is any abnormality, the type of the attack is obtained by comparing with the database. Then the threat packet is forwarded to the honeyRJ by the load balancer and if it is a normal packet is it forwarded to the original server by the load balancer.

Honeypot is an information system resource whose value lies in unauthorized use of that resource. It is a server that is configured to detect anintruder by mirroring a real productionsystem.It isusedtolearn about an intruder's techniques as well as determine the vulnerabilities in the real system.This helps in reducing the false alarms.

Theapplication, HoneyRJ, is an implementation of alow-interaction honeypot. A low-interaction honeypot serves a number of limited functionality protocols with theintent of capturing the source of trafficcoming to the honeypot. A honeypotis located on an IP address that is used solely for the purpose of the honeypot and not for any legitimate services. Thus any connection to the HoneyRJ is malicious.The information of any node connected to the honeypot server is logged for later review.

A.Clone attack

It is one of the most severe attacks in many types of networks. In this type of attack the intruder compromises few nodes, replicates them and inserts arbitrary number of replicas into the network. Hence the intruder can carry out many internal attacks. In this system the IP address of the authorized node is utilized by the attacker to replicate that node.

The proposed work involves the use of random numbers for the detection of clone attack. Each and every node in the network is initialized with a new

International Journal of Computer Network and Security (IJCNS)
Vol 6. No.1 – Jan-March 2014 Pp. 40-45

available at : www.ijcns.com
ISSN: 0975-8283

random number when the network is initialized or every time the network is updated. These values are stored in the database of the IPS.

When an attacker tries to hack the network the IPS checks whether the random number alloted to that particular node is same as the number stored in its database . If they do not match it is confirmed to be a clone attack and then the attack packet is sent to the HoneyRJ for gathering information about the malicious node. Figure 2 shows the clone attack.

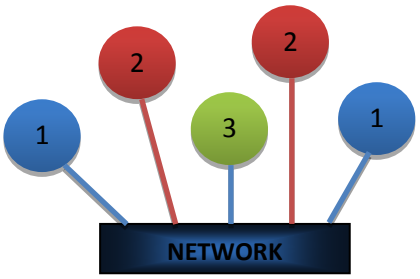

Figure. 2 Clone Attack

B. Ping of Death attack

This type of attack involves the attacker sending a malicious pingof size greater than 65,535 bytes to a computer.The maximum packet length of an IP packet including the header is 65,535 bytes. This can overflow the memory buffers allocated for the packet, causing denial of service for legitimate packets and could also crash the target computer [8]. Figure 3 shows the Ping of Death attack.

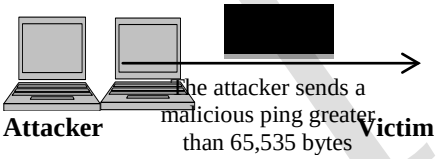

Figure. 3 Ping of Death attack

In the proposed work the total length field in the fragment of the packetis checked by the IPS and if it is greater than 65,535 bytes it is confirmed to be a ping of death attack and hence sent to the honeypot server.

4. SIMULATION RESULTS

The implementation involves the detection of clone and ping of death attacks and the mitigation is done with the honeypot server. The detection of attacks is simulated with the Network Simulator 2 and the implementation of the Honeypot server is simulated with Java.

A. Attacks Detection

The attacks are detected with the help of the database stored in the set of IPSs [3]. The detection of the clone attack andthe ping of death attack are shown in Fig. 4 and Fig. 5 respectively.

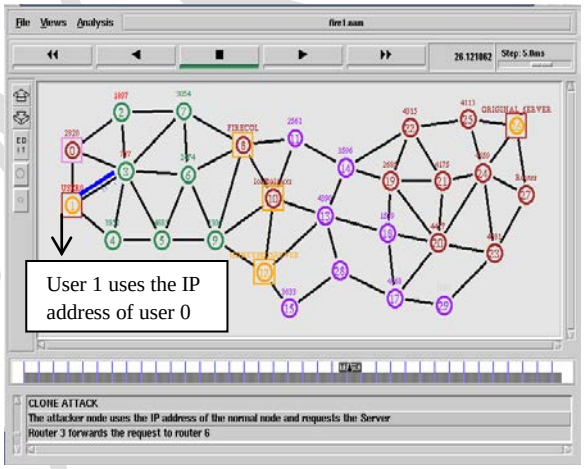

Figure. 4 Detection of Clone Attack

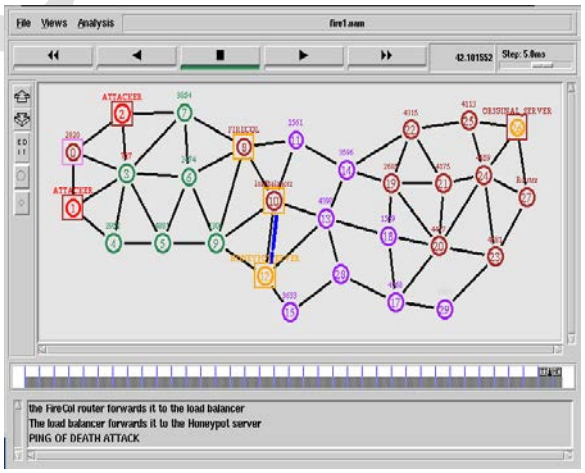

Figure. 5 Detection of Ping of Death attack

International Journal of Computer Network and Security (IJCNS)
Vol 6. No.1 – Jan-March 2014 Pp. 40-45
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0975-8283

B. ***Mitigation by Honeypot server***

HoneyRJ logs every connection into an individual file. This helps in obtaining information about the attacker and taking necessary actions against them for the prevention of future occurrence of the attacks from the intruders. When HoneyRJ launches, it creates a directory named with a timestamp in the configured logging directory. Each connection to the HoneyRJ creates a new text file within this directory named by the protocol name followed by a timestamp and it is given the extension log. The log files are stored as text documents which allow a user to easily read them and they are continuously updated as the connection progresses to allow a user to monitor active connections by viewing the log file [4].

A log file consists of the following information about each packet.

- Timestamp – It states when thepacket was sent or received.
- Source IP - The IP address the packet was sent from that is the IP of the machine HoneyRJ is running for a sent packet or the IP of the client for a received packet.
- Source Port - The port number the packet was sent from.
- Destination IP - The IP address on which the packet was received that is the IP of the machine HoneyRJ is running for a received packet or the IP of the client for a sent packet.
- Destination Port - The port number the packet was received from.
- Packet - The string contained within the packet.

Each packet sent or received is logged on a separate line.The window in Fig. 6 shows the Honey RJ main application window upon the initial startup where all the modules are put into the started state which indicates that all the modules are listening for the connections [4].

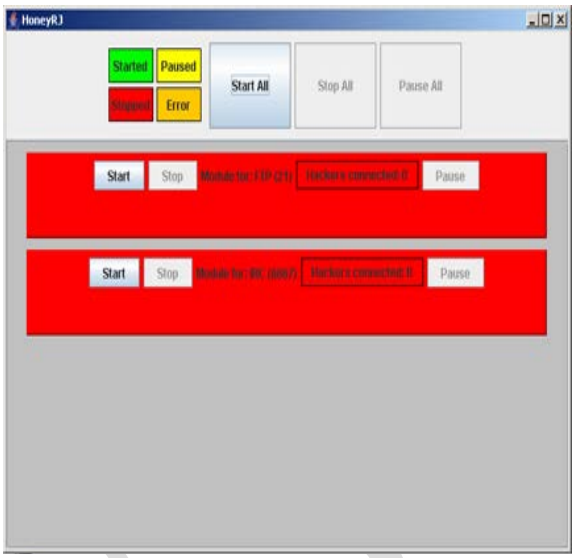

Figure. 6 HoneyRJ main application window

A module represents one protocol running within HoneyRJ. It provides the implementation of a protocol to allow HoneyRJ to communicate with clients as if it were a server running that protocol. Each module lists the common name of its protocol and the port on which it runs and also displays the number of currently connected clients.The verification of HoneyRJ listening for the connections is done by opening a Telnet session. The interaction of the Telnet session with the HoneyRJ's FTP protocol is shown in Fig. 7.

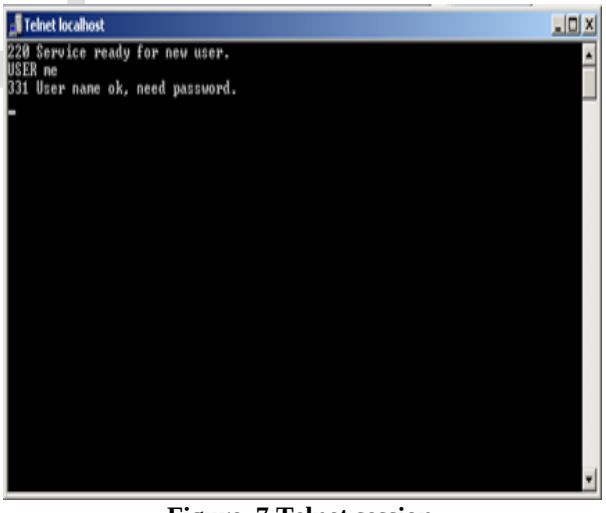

Figure. 7 Telnet session

After the Telnet session is opened the number of hackers connected becomes 1 in the main application

International Journal of Computer Network and Security (IJCNS)
Vol 6. No.1 – Jan-March 2014 Pp. 40-45
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0975-8283

window which indicates the presence of one connection to the FTP protocol and it is shown in Fig. 8.The log file that is obtained for the Telnet session with HoneyRJ is shown in Fig. 9.

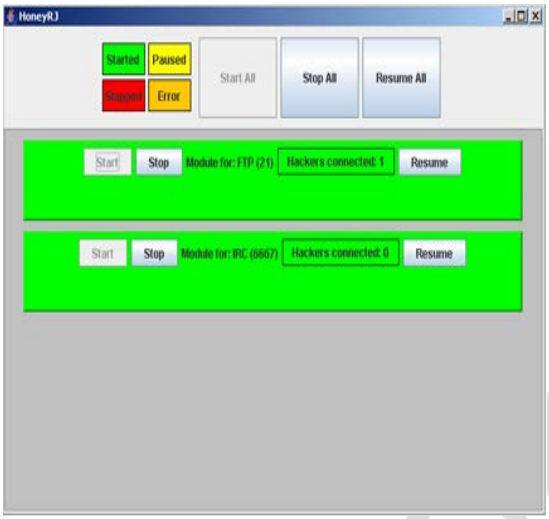

Figure. 8 Connection to the FTP protocol

****
*****Started at: Fri Feb 07 19:14:53 IST 2014*******
TIMESTAMP, SRC_IP : PRT, DST_IP : PRT, PACKET

Fri Feb 07 19:14:53 IST 2014, 127.0.0.1 : 60101, 127.0.0.1 : 21,220 Service ready for new user.

Fri Feb 07 19:15:24 IST 2014,127.0.0.1 : 60101, 127.0.0.1 : 21, 332 Need account for login.

Fri Feb 07 19:15:32 IST 2014,127.0.0.1 : 21, 127.0.0.1 : 60101, user

Fri Feb 07 19:15:53 IST 2014,127.0.0.1 : 60101, 127.0.0.1 : 21, 331 User name ok, need password.

*****Protocol FTP is finished talking to /127.0.0.1 using local port 21****

*****Stopped at: Fri Feb 07 19:15:58 IST 2014*****
****

Figure. 9 Log file

5. CONCLUSION

In this paper, the integration of two technologies IPS and honeypots have been discussed. The detection of the clone and ping of death attacks is done and sent to the Honeypot server in NS2 simulation. The information about the attacker is obtained through the simulation in Java. The simulation results showed that the proposed system is more efficient in overcoming the disadvantages of the IPSs and since the system differentiates the traffic from an authorized user and from the intruder, it consequently helps in reducing the communication overhead.The honeypots provide a new method for preventing the DDoS attacks.They serve as a good deception tool because of their ability to trap the attackers.Thus the proposed method provides early warning, identify flaws and improves the overall security awareness. The future work can be proceeded with the implementation of honeypot farms where the disadvantage of using honeypots to harm other nonhoneypot systems once their presence is detected can be prevented.

REFERENCES

[1] A. El-Atawy, E. Al-Shaer, T. Tran, and R. Boutaba, “Adaptive early packet filtering for defending firewalls against DoS attacks,” IEEE INFOCOM, Apr. 2009, pp. 2437–2445., in press

[2] M.Buvaneswari, T.Subha, “IHONEYCOL: A collaborative technique for mitigation of DDoS attack,” ICICES, Feb 2013, pp. 340-345., in press

[3] Chandrapal U.Chauhan, V.A.Gulhane, “Signature based rule matching technique in network intrusion detection system,” IJARCSSE, Vol. 2, Issue 4,Apr. 2012., in press

[4] Eric Peter and Todd Schiller, “A practical guide to honeypots ”

[5] Feinstein.L, Schnackenberg.D, Balupari.R, Kindred.D,“Statistical approaches to DDoS attack detection and response”, Proc. of the DARPA Information Survivability Conference and Exposition,Vol. 1,Apr. 2003,pp. 303-314., in press

International Journal of Computer Network and Security (IJCNS)
Vol 6. No.1 – Jan-March 2014 Pp. 40-45
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0975-8283

[6] Francois.J, Aib.I and Boutaba.R, " FireCol: A collaborative protection network for the detection of flooding DDoS attacks ," in networking, IEEE/ACM Trans.,Vol. 20, Issue 6, Dec. 2012, pp. 1828-1841., in press

[7] Francois. J, A. El Atawy, E. Al Shaer, and R. Boutaba, "A collaborative approach for proactive detection of distributed denial of service attacks," IEEE MonAM, Vol. 11, 2007., in press

[8] Honeypots, DDoS : en.wikipedia.org

[9] Janakiraman.R, Waldvogel.M and Qi Zhang , " Indra : A peer-to-peer approach to network intrusion detection and prevention," WET ICE, June 2003, pp. 226 – 231., in press

[10] S. H. Khor and A. Nakao, "Overfort: Combating DDoS with peer-to-peer DDoS puzzle," IEEE IPDPS, Apr. 2008, pp.1–8., in press

[11] RK Singh, T.Ramanujam, "Intrusion detection system using advanced honeypots," IJCSIS,Vol. 2, No. 1 June 2009., in press

[12] Yin Xuan, Incheol Shin, My T.Thai, Taieb Znati, "Detecting application denial of service Attacks: A group testing based approach", Parallel and Distributed Systems, IEEE,Vol. 21 , Issue 8 ,Sept. 2009, pp. 1203-1216., in press