ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 2, Issue 2, pp: (27-30), Month: October 2015 – March 2016, Available at: www.paperpublications.org

Network Security Using IDS, IPS & Honeypot

[1]Surabhi Malav, [2]Medankar Sanika Avinash, [3]Nagarkar Sanika Satish,
[4]Shah Charmi Sandeep

Abstract: **Various exploits are being used to compromise the network. These exploits are capable of breaking into any secured networks. To increase efficiency of network security, Honeypot was introduced by LANCE SPITZNER in 1999. Honeypots are virtual servers which appears as actual servers to attackers. Honeypot detect attacks with the help of IDS; trap and deflect those packets sent by attackers. Honeypot maintains logs of intruding activities. So, in the proposed system, the system handles multiple clients using the concept of honeypot. Intrusion detection system (IDS) monitor whole network and looks for intrusion. When any intrusion occurs honeypot will be activated. This activated honeypot will divert the traffic to dummy/virtual servers & back track the source (IP address) or origin of that attack.**

Keywords: **IDS, IPS, Honeypot, Virtual Server.**

I. INTRODUCTION

In present era, many attackers attack the network so as to gain the information or damage the system. These attacks are in the form of malware or more dangerous as Distributed Denial-Of-Service (DDoS) attack. There are many existing standalone systems are there to detect and prevent the network from attacks like Firewall, Intrusion-Detection-System(IDS) and Intrusion-prevention-System(IPS). They are not centralized &intruding into the network becomes easy for the attackers. To overcome the drawback of existing system concept of honeypot was introduced. Since all these systems were needed to be installed separately and also were architecture dependent, increased the complexity.

In this paper, we propose the system which combines specific features and services of Intrusion-Detection-System (IDS), Intrusion-prevention-System (IPS) and Honeypot.

The system will be architecture independent, centralized and more beneficial. To determine these security parameters is to build a formula to represent the idea of security.

Security=Visibility + Control

This formula is the base of this project.

II. MODULES

1. Intrusion-Detection-System (IDS).

A. Traffic Monitor.

B. Detection Engine.

C. Re-direction Engine.

2. Intrusion-prevention-System (IPS).

A. Recognize Intrusion.

B. Decision Making.

C. Re-direction Engine.

D. Backtracing.

3. Honeypot.

A. Database of Logs.

B. Database of Fake Information.

4. Web page with connectivity (Interface).

A. Webpage for Login.

B. Database of Authentication Information.

III. DESCRIPTION OF MODULES

1. Intrusion Detection System:

This module is to detect if any attacker tries to intrude the network. It will just detect the intrusion but will not recognize the type of intrusion. The intrusion detection module consists of following sub-modules:

A. Traffic Monitor:

Traffic Monitor will monitor the traffic of the network. This means it will check for every packet travelling through the network.

B. Detection Engine:

Every packet captured by traffic monitor undergoes detection. The Detection Engine will then check for the pattern of data present in the packet and match it with the patterns present in its database. If pattern of any packet is matched then it will open up the header part to obtain the IP address and TTL field of the sender.

C. Re-direction Engine:

When the Detection Engine will detect an intrusion that particular packet will then be forwarded to the Intrusion Prevention System (IPS).

2. Intrusion Prevention System:

This module is to prevent the intrusion from damaging the network. It will decide what action is to be performed depending on the pattern detected by the IDS. It consists of following sub-modules:

A. Recognize Intrusion:

Based on the pattern detected by the IDS this module will recognize the type of the intruding packet. The types of Intruding packet may be like the SYN packet, FIN packet, or just a normal packet requesting for the data.

B. Decision Making:

Once the type of packet is recognized then this module will take the decision of what action to take. It can be backtracing and blocking the IP address if it is a DOS attack (SYN packet or FIN packet) or re-directing the control to dummy server for other attacking packets. Depending on this decision the other two modules will be initiated.

C. Re-direction Engine:

If the Decision Making module decides to direct the control to the honeypot, this module will start the honeypot server.

D. Back tracing:

If the IPS recognizes the attack as DoS attack (SYN packet or FIN packet) then the decision making module will initiate this Back tracing module. Now this module will use TTL field and IP address obtained by the IDS to backtrace the path till we reach to this detected IP address and block it.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 2, Issue 2, pp: (27-30), Month: October 2015 – March 2016, Available at: www.paperpublications.org

3. Honeypot:

The honeypot server is a dummy server. The dummy server appears as an original server to the attackers. It services the attacking packets. Due to this honeypot server the original server is spared from any intrusion. This dummy honeypot server consists of the following sub-modules:

A. Database of Logs:

This database stores the log of all the traffic that is travelling through the network. It stores the information of all (each and every) the packets.

B. Database of fake information:

In this database all the fake information will be stored. Fake means all the false information. This information will be similar to that of original server. Whenever there will be request for information stored on the server by user other than authenticated user then this dummy server will provide it with the fake information from this database.

4. Web page with connectivity (Interface):

A. Web page for login:

This is HTML web page which provides the authorized users to login and start the application and also to view the database of logs. This page is connected with the database of authenticated user so as to authenticate the authorized users while logging in.

B. Database of Authentication information:

This database will store the mapping of username and password only for the authorized users. Whenever the authorized user try to login, the username and password mapping will be matched with the mapping of this database to authenticate the user to accept the honeypot.

IV. ARCHITECTURE OF PROPOSED SYSTEM

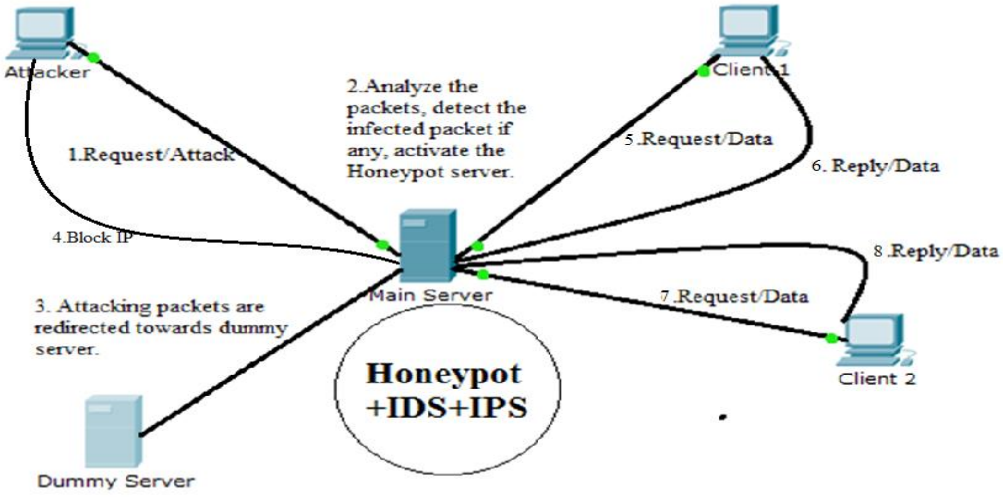

Fig.1 Architecture of proposed system

The proposed architecture supports multiple clients. For sake of convenience we will consider two authorized user .i.e. clients and one unauthorized user .i.e. attacker. It also consists of one main server and one dummy server. The main server consists of software which includes IDS, IPS and Honeypot. If attacker tries to attack on Main server then IDS will detect

that attack and control is passed to the IPS. Now IPS will recognize whether the attack is DoS attack or any other attack. If there is DoS attack, then by using the TTL field and IP address the source of attacker is blocked. But if the attacking packets are not of Dos attack then it is redirected to the dummy server, which is maintained by Honeypot. Honeypot not only maintain the fake server or dummy server but it will also maintain the logs of all the traffic in the network.

If one client wants to communicate with other client or one client want data from the server then also packets coming from those clients are analyzed for intrusion. If packets are found to be uninfected then they are transmitted to the main server and after processing reply to respective client is given.

If authorized user wants to see the logs of all the traffic travelling through the network then user can login through a web page and can see the logs.

V. CONCLUSION

The existing systems do not come as one package. These systems (i.e. IDS, IPS, and Honeypot) need to be installed as separate packages. The system which we have proposed is a single package consisting of all these modules (i.e. IDS, IPS and Honeypot). This reduces the complexity of installing the modules separately. Since the modules form one package it reduces the overall cost. Also, existing system is system architecture dependent and can be implemented in only specific network designs. This drawback is overcome in our proposed architecture which is system independent and can be implemented in any type of network design. Our project is web based application. This application is used by only authenticated users to check the intrusion and other log files and also maintain it. Since, it is web based application the authenticated user can access the server from anywhere and at any time in the network. Hence, through our project we are securing the network efficiently with reduced cost which can be afforded by many small corporate companies inorder to secure their networks.

REFERENCES

[1] "An implementation of intrusion detection system using genetic algorithm" Mohammad Sazzadul Hoque1, Md. Abdul Mukit2 and Md. Abu Naser Bikas3 1Student, Department of Computer Science and Engineering, Shahjalal University of Science and Technology, Sylhet, Bangladesh sazzad@ymail.com 2Student, Department of Computer Science and Engineering, Shahjalal University of Science and Technology, Sylhet, Bangladesh mukit.sust027@gmail.com 3Lecturer, Department of Computer Science and Engineering, Shahjalal University of Science and Technology, Sylhet, Bangladesh bikasbd@yahoo.com

[2] International Journal of Advanced Research in Computer Science and Software Engineering Research Paper www.ijarcsse.com "Study and Comparison of Virus Detection Techniques" Ankush R Kakad, Siddharth G Kamble, Shrinivas S Bhuvad, Vinayak N Malavade

[3] "Honeypot back-propagation for mitigating spoofing distributed Denial-of-Service attacks" Sherif Khattaba, Rami Melhema, Daniel Mosséa, Taieb Znatia, Department of Computer Science, University of Pittsburgh, PA 15260, USA Department of Information Science and Telecommunications, University of Pittsburgh, PA 15260, USA

[4] "A Dynamic Honeypot Design for Intrusion Detection", Iyad Kuwatly, Malek Sraj, Zaid Al Masri American University of Beirut Department of Electrical and Computer Engineering P.O.Box 11-0236 / 3623 Riad El-Solh / Beirut 1107 2020 Lebanon Emails {imk01, mas44, zoa01} @aub.edu.lb

[5] "A Technique for Detecting New Attacks in Low-Interaction Honeypot Traffic", S. Almotairi, A. Clark, G. Mohay, and J. Zimmermann Information Security Institute, Queensland University of Technology Brisbane, Queensland, Australia {s.almotairi, a.clark, g.mohay, j.zimmerm}@isi.qut.edu.au

[6] "Distributed Denial of Service Prevention Techniques", B. B. Gupta, Student Member, IEEE, R. C. Joshi, and Manoj Misra, Member, IEEE

[7] Navneet Kambow et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 2014, 6098-6101, "Honeypots: The Need of Network Security Navneet" ,Kambow, Lavleen Kaur Passi , Deparment of Computer Science, Shaheed Bhagat Singh State Technical Capmus, Ferozepur, India- Department of Computer Science ,Arya bhatta Institte of Engineering and Technology, Barnala, India.