Dos Attack Stopover by using Honeypot and Data Mining

Aishwarya Shrikant Patil[1] **Abhishek Satish Kale**[2] **Dr. Babasaheb Mohite**[3]

[1,2,3]Zeal Institute for Business Administration, Computer Application and Research, India

Abstract— DoS attack causes a thoughtful threat to many IT industries. This type of attack is hard to detect because there are many different ways for attacker or hacker to attack. The main purpose of cyber-attack is to making the network services out of network resources so that it becomes unavailable to authorized users. Due to change in behaviour of hacker, it is difficult to find out the malicious cyber-attacks or detect the malicious network traffic. The main aim of dos attack is to hack the websites such as banking sites, transactional sites and domain name servers. In this paper we discuss about dos attack and the prevention methods of dos attack. Then we discuss dos attack prevention by using honeypots and honeyd methods. We use different data mining algorithms and intrusion detection system to prevent the attack.

Keywords: DoS attack, DDoS attack, Network Security, Intrusion Detection, Honeypot, Honeyd

I. Introduction

When securing a network, there are many different aspects, tools and approaches that can be utilized. One tool in particular offers a large amount of usable flexibility for administrators; the honeypot. Honeypots differ and can be deployed in a number of different forms as well as filling the roles of other tools that are not available based on the needs of the network. The main role filled by honeypots of course would be detection. Keep in mind though that each individual honeypot must be configured and tailored to the individual network and what they need to detect. This paper will take a short look into honeypots, and then more specifically focus on the program Honeyd. Afterwards, it will go into the basics of how it works, some examples of usage, and how to realistically implement it into a network.

Frequently, network intrusion detection systems are the common form of threat detection seen in networks, also known as an NIDS.NIDS’s passively analyse the network traffic and index any alerts they find of suspicious or unauthorized activity they view. They (NIDS) work well enough, but the main issue with them is their inability to differentiate between malicious attempts on the network, and false-positives. Not only is this a problem when a network is small, but the effect this has on the NIDS as the network grows is exponential since it will be required to monitor larger amounts of traffic creating much larger logs, and requiring more resources to continue running it. Also, this tasks the network administrator with parsing huge files to even begin searching for malicious attempts. On the other hand, looking at this in a more positive light, this does not mean NIDS are not at all effective. They, like any other piece of defense are an added layer or protection for the network. No security overlay of a network should be reliant on just one method. Multiple tools and methods should be employed to best defend the network.

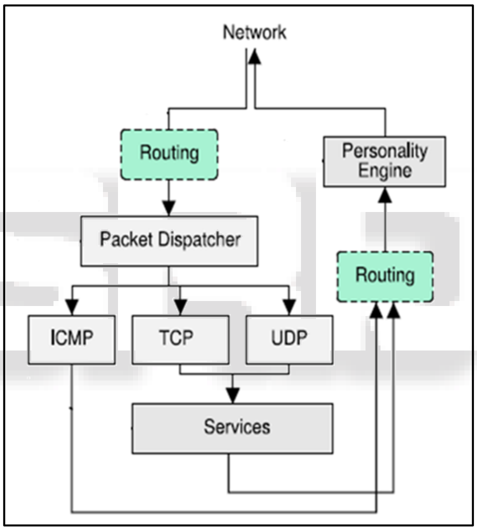
II. Objective

1) Capture information about attacks
2) System vulnerabilities
3) System responses
4) Capture information about attackers
5) Attack methods
6) Scan patterns
7) Identities

III. Motivation

Many modern control systems are inter-connected via computer network. Provide security using Dynamic Honeypots. Proposed system design and implements a self-configuring Honeypots with intrusion detection system. Proposed system used unattended web threat detection system based on the manydata mining algorithms and Honeypot techniques.

IV. Proposed System Architecture



V. Proposed System

The honeyd architecture contains various elements like protocol handler, a configuration of database, a central package dispatcher, a personality engine and optional routing components. In the figure shown upwards, the incoming packets are prepared by central packet dispatcher. Packet dispatcher is responsible for verification of packets checksum and checking the length of the packet. This framework is used by three major protocols, namely-ICMP,TCP and UDP protocols. For other protocols packets are discarded and logged. To find the honeypot configuration that states the IP address of destination the dispatcher must ask the query to configuration database before the packet is being processed. Sometimes specific configuration does not exists,at that time default configuration is used. The packet and corresponding configuration involves protocol specific handler. The ICMP Protocol Handler handles the ICMP requests.

All honeypot create response to echo requests and activity destination in-reachable messages by default. It handles all other requests depending on the organized personalities. The model can establish connections to absolute services For Transmission control protocol and user datagram protocol Services receive data on stdin and send their output to stdout. These Services are external as well as internal applications. The activeness of a service depends on the external application entirely.

The frame-work checks if the packet is part of an constituted connection when a connection request is received .To run the appropriate service a new process is created whenever the packet contains the connection request. The frame-work supports system and internal services instead of creating a new process for each connection. To set up a connection to a local service, the framework also supports redirection of connections. The redirection may be static or it can depend on the connection multiple (source address, source port address, destination address and destination port address).

VI. Literature survey

1) Cyber-attacks and defensive measure solutions: Categorization and state-of-the-art

Acyber attack can easily exhaust the computing and communication resources of its unfortunate person within a short time periodwith little or no progress warning in an existing system. Because of the sereness of the difficulty many detect execution have been planned to struggle these attacks. more, important advantage of each attack and detect system collection are represented and advantages and disadvantages of each proposed strategy are defined.

Drawback of this system are no same characteristics of cyber line that can be used for their detection.

2) Perception Of Distributed Denial of Service Attacks using mining

The agents can then defence network in flood attacks against a network server. The experimental results show a classifiable and predictive data of the server attacks. Our agents can successfully defence various server attacks.

Disadvantages of system are this system uses alarming agents to detect the cyber-attacks which are not compatible with some servers.

3) Defence Based on Package ID Attack Detection – SYN flood Spoof Source cyber Attack

Package Determination Attack Detection Method is used for detection when attackers try to send flood SYN package with spoof source especially, there packets have information fields as the normal SYN package. SYN package used to defence type of DDoS attack mentioned above.

Drawbacks of this system To defence SYN flood packages, it cannot check each SYN packet sent to server.

4) DoS attack prevention using Data mining Algorithms

It presents a comprehensive survey of preventing DDOS attack recognize by data mining techniques with the use of identifying DDOS attack patterns and analyse patterns by machine learning algorithms. There are some leading machine learning algorithms used to recognize the DDOS attack such as k-Nearest Neighbours algorithm, support vector machines (SVM), Random Forest as well as Naïve Base. The result shows the highest accuracy rate of preventing DoS attack recognizing by data mining algorithms.

Drawback of the system are They are having multiple attack vectors, multiple sources, a mix of benign and malicious traffic, and packet differentiation at various levels of the network stack, flash crowds, filter placement and throughput .

VII. Future scope of system

Prevention from intrusion and block attackers by recording their IP address. Using data mining concept create outlier of data from attackers IP addresses. Intrusion detection system introduce unattended web attack catching system based on the multiple mining algorithms and honeypot techniques that automatically will detect the intrusion over network.

VIII. Advantages

1) It uses minimum Resources
2) Information security is achieved
3) Cost is reduced
4) Maintenance is easy
5) Encryption of IPV6 protocol
6) New data mining tools and honeypot techniques are used
7) Small set of data and probably high values

IX. Conclusion

The dynamic honeypots is plug and play solution to detect the DoS attack and the intrusion on network. The virtual honeypots uses the technique known as honeyd which are used to detect attacks and to prevent network resources and information. The intrusion detection system introduces unattended web attack detection system based on multiple data mining algorithms and honeypot techniques that automatically detect the intrusion over network

Acknowledgments

The author be thankful to the publishers used for creation Their do research outcome offered as well as teacher for their important direction. We in addition to thank the organization authority in support of provide the vital facilities also support. lastly, we would like to make bigger a sincere thanks to our the entire associate and unit member.

References

[1] Todd Vollmer and Milos Manic, “Cyber-Physical System Security With Deceptive Virtual Hosts for Industrial Control Networks,” IEEE Trans. Ind. Informat., VOL. 10, NO. 2, MAY 2014

[2] Wira Zanoramy Ansiry Zakaria, Miss Laiha Mat Kiah,” A review of dynamic and intelligent honeypots” , doi: 10.2306/scienceasia1513-1874.2013.39S.001

[3] O. Linda, T. Vollmer, and M. Manic, “Improving cyber-security of smart grid systems via anomaly detection and linguistic domain knowledge,” in Proc. IEEE Symp. Resilience Control Syst., Salt Lake City, UT, USA, Aug. 2012.

[4] M. Roesch, “Snort: Lightweight intrusion detection for networks,” in Proc. 13th Conf. Syst. Admin., Berkeley, CA, USA, Nov. 7–12, 1999, pp. 229–238.

[5] A. Lakhina, M. Crovella, and C. Diot. Diagnosing Network-Wide Traffic Anomalies. In ACM Special Interest group on Data Communication, Portland, August 2004.

[6] Gaia Maselli, Luca Deri, Stefano Suin” Design and Implementation of an Anomaly Detection System: an Empirical Approach” University of Pisa.