Research Journal of Computer and Information Technology Sciences ______________________ISSN 2320 – 6527
Vol. **3(3),** 1-3, June (**2015**) *Res. J. Computer and IT Sci.*

Collection system Infected systems using Stationary and Event driven IP Sinkholes

Shahsavar Razieh and Askar Zadeh Majid
Department of Computer engineering, Qeshm international Branch, Islamic Azad University, Qeshm, IRAN

Available online at: www.isca.in
Received 23rd April 2015, revised 15th May 2015, accepted 10th June 2015

Abstract

In relation to unknown identity of net users especially internet users، today we can face the increase of attacks on many kind of services. The reason of most of attack can be begin with a simple curiosity and can be continue with a destructive targets. For prevention, discrimination and stopping the attacks, in first step, we should able to recognize time and situation of attacks occurrence. Enemy recognition and knowing his plans can be increase our success against them. There are many different methods for attack recognition and thereby detect infected systems are available but in this article, collection system infected systems using stationary and event driven IP sinkholes is simulated.

Keywords: IP sinkhole, intrusion detection, kinds of attacks.

Introduction

Most of the networks are endangered with kinds of external and internal attack of hackers, in this condition, if the networks are not controlled it may cause damage or misused by hackers. This paper studied about system to collecting infected systems *using stationary and event driven IP sinkholes* and explained damages that a hacker using to attack victim and then the butnet definition and its applications, ways of extending Butnets and C and C server werede find. thereafter, its ways and tools of collating with bad software attacks including firewall, IDS, IPS and using honeypot server and IP-Sinkhole mechanism will be discussed as well as the target is to prevent unpermitted target and finally defined ideas and definition will be assemble and apply then advantages and disadvantages of this method will present[1,2].

Methodology

Here by using another technique of a sinkhole, the IP sinkhole, the system in Virtual Box was simulated, that the IP of infected systems, both inside and outside of the network toward the sinkhole was identified and conducted to understand the aggressive manner. Then it can understand what systems inside the network were infected and which traffic it has send so that it can shown destructive IPs and also turn on the Remove all mechanism for destructive IP's, so that finally the server can recognize the fault and also can clean the Bots.

Measures taken in collecting affected systems: Firewall is defined as a tool which control accessibility to a networks based on security policy. Firewall passes a good traffic and block the bad one. Firewall can increase net security. Firewall can block to pass useful data from network line but when this information doesn't pass the line it cannot do anything, this is one of its disadvantages[3].

IDS has a duty of identification and detecting of every illegal using of system from internal or external users.IDS can be divided in software and hardware[4].

Snort as a IDS comprises four parts: i. collecting data, to collect the information needed to connect to the network desired. ii. Initial analysis for preparing information for next stage. In this part input information can be classify based on content. iii. Engine identification can be done after preparing information, data go to this part. iv. Alarming after identifying attack, given information with specific format will send to this part. With setting a snort we can save file information (log) in directions collections of snort.

Honeypot is a kind of information source with false data which for collating hackers and collecting illegal activities in computer networks that are in the networks. Honeypots are computers which have tools for compromise. They are real or assembled and their target is preventing, detecting, response and research.

Because of invaluable nature of honeypot sources, every activity on them is considered illegal. Ahoneypot can be an extra computer in network or can be apply in a way that can resemble every weakness of a network. When a hacker searches a network to identify its weakness, with identifying weak points can attack honeypot but honeypot alarm the network security and start to collect the information for checking.

IP sinkhole generally can be defined as a changing the way of IP traffic of specific nets and stopping a traffic in a ISP nets, for different security goals including analyzing legal cases and avert attacks and identifying abnormal activities.

Most of the application of IP-Sinkhole are using different kinds of preyed nets for trapping, revealing and collecting data.

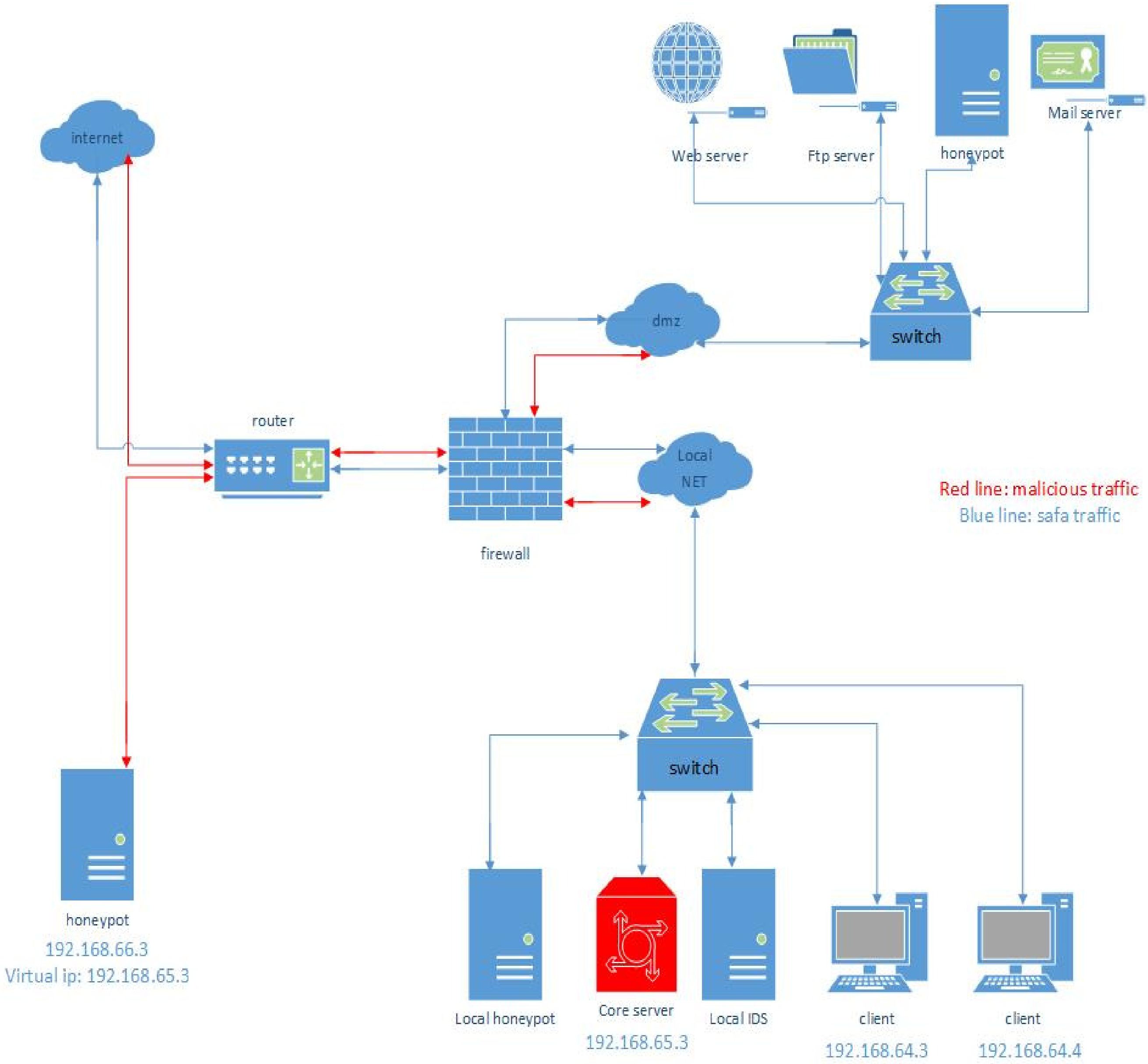

Figure-1
Schematic of the basic plan implementation

As seen in above picture, in this schema we use a router for detection. Our purpose from applying this system is to identify harmful IP which want to access target server illegally in order to deal with them. Therefore in direction of router and internal networks and DMZ, we put a Firewall, however firewall cannot analyze bad traffic it can just block a destructive traffic Based on the policies that have been applied. So if a destructive traffic for illegal accessory can pass from firewall, we have suggested that target server received C and C servers list from applied servers from specific sites in external nets, and destructive IP from specific Log of IDS, Firewall, honeypot and honeypot of DMZ, and according to access to router can send them to router and command toreconfigure to guide them to honeypot connected to router to prevent from illegal accesses and to collect destructive treats and improve security system of networks.

Conclusion

One of the advantages of this system is controlling the infected system and controlling illegal access of external net IP to internal nets and destructive IP access of internal networks to target server which can identify and collect attacks and hackers treats.

The advantage of our work in comparison to firewall is that firewall blocks the attack but IP-Sinkhole change the direction of traffic to the controlled direction until the new attacks will be identified and useful data will collected to find out that which systems are the target of attack to attempt to discover the Vulnerabilities to improve firewall and other system against them.

One of the advantages of honeypot is the simplicity, because honeypot doesn't have important content and no agent wants to access it. Therefore if someone came in and did something in it, is malicious.

In addition, data collected from honeypot is low but valuable because they are from hackers.

Generally with assembling damages in honeypot, we can provide conditions to identify bad behavior malware. after identifying hackers treats in using vulnerabilities we can identify them by IP which are collected with checking traffic in honeypot with external and internal system or also report provided a list of malicious IPs and if necessary using remove all mechanisms on them.

Using this system is not useful in vast networks because of router mechanism. Because if direction table be larger the router acts slower.

References

1. Zhu Z., Lu G., Chen Y., Fu Z., Roberts P. and Han K., Botnet research survey. In *Computer Software and Applications, 2008. COMPSAC'08. 32nd Annual IEEE International,* 967-972, **(2008)**

2. Mazzariello C., IRC traffic analysis for botnet detection, In *Information Assurance and Security, 2008. ISIAS'08. Fourth International Conference on,* 318-323, **(2008)**

3. Bau J., Bursztein E., Gupta D. and Mitchell J., State of the art: Automated black-box web application vulnerability testing, In *Security and Privacy (SP), 2010 IEEE Symposium,* 332-345 **(2010)**

4. Axelsson S., *Intrusion detection systems: A survey and taxonomy,* 99 Technical report, **(2000)**

5. Fuchsberger A., Intrusion detection systems and intrusion prevention systems, *Information Security Technical Report*, **10(3),** 134-139 **(2005)**