ISSN:0975-9646

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*

***Abstract* – Network forensics is basically used to detect attackers activity and to analyze their behavior. Data collection is the major task of network forensics and honeypots are used in network forensics to collect useful data. Honeypot is an exciting new technology with enormous potential for security communities. This review paper is based upon the introduction to honeypots, their importance in network security, types of honeypots, their advantages disadvantages and legal issues related with them. Research Paper also discuss about the shortcomings of intrusion detection system in a network security and how honeypots improve the security architecture of the organizational network. Furthermore, paper reveals about the different kind of honeypots their level of interaction and risks associated with them.**

Keywords—honeyd; honeypots; nmap; network forensics

I. INTRODUCTION

In the era of information and technology network security has become the core issue in every organizational network. Honeypots are integrated in network with firewall and Intrusion detection systems to provide solid secure platform to an organization. Firewall provide the filtering and generate logs to further analyze any malicious activity or any violation policy of access control list ,firewall rules. Different approaches like firewall demilitarized zone (DMZ) have been used but they are not effective for today's network security . Intrusion detection systems then introduced to overcome the shortcomings of existing network. Intrusion detection system silently monitor the network's traffic and give the alerts to tell about any kind of intruders based upon the database of signatures of existing intrusions. A number of issues were with IDS too as facing with an increasing number of false negatives and false positives[7]. Honeypots then introduced in the network to utilize the network's unused IPs and the attacker's behavior is analysed on these honeypots. Honeypots improve IDS too by decreasing the numbers of false positives.

With the integration honeypots network security accuracy increases than the only implementation of network Intrusion detection system. These are the increasing trends in information security mechanism. For instance, the well-known company Amazon possessing the world's largest database use database honeypots to deceicve attackers to reach their actual honeypots.

A. Honeypots

Honeypot is a unique security resource which is a part of security mechanism deployed in an organisation. These are the resources you want the black hat guys to interact with. Basically, honeypot is an IT resource whose value lies in an unauthorized or its illicit use [14]. It means the value of honeypots could be derived from the threats using them. Honeypots would have little value if attacker doesn't interact with them. Indeed, honeypots do not solve specific problems. Instead they are tools having applications to security. They can be used as early warning systems, slowing down and automated attacks and capturing new exploits to gathering intelligence on emerging threats. Furthermore, honeypots come in different sizes and shapes .they can be an emulated windows based application, an entire network to be compromised and attacked such as Honeynets. Also, honeypots don't even have to be computer. They may be credit card numbers, Excel spread sheets or login and passwords (known as honey tokens).

II. LEVEL OF INTERACTION OF HONEYPOTS

A. Low Interaction Honeypots

On the basis of interaction low interaction honeypots doesn't provide Operating system access to the intruder .It provides only services such as ftp ,http ,ssh etc. these low interaction honeypots plays the role of passive IDS where the network traffic is not modified. Some examples of low interaction honeypots are honeyd, specter ,BOF. Honeyd is an opensource tool and the facility of service emulation on hoenyd is unrestricted whereas specter is not an open source tool and developed by Netsec. The well-known example of low interaction honeypot is Honeyd. Honeyd is a daemon and it is used to simulate large network on a single host [2, 8]. It provides a framework to create several virtual hosts using unused IP addresses of the network with help of ARP daemon For instance, several virtual number of operating systems, server, switches, routers, can be configured on a single host. Furthermore, emulated services include FTP service listening on port 21 (Telnet), login to FTP server etc. Other low interaction honeypot is specter [12] and kFsensor [13]. Specter can monitor total of 14 Tcp ports. Out of these fourteen ports seven ports are called traps and seven are called services. Traps act as a listeners of ports i.e. when attacker makes connection with these ports the attempt is terminated and then logged. Services are more advanced wherever there is interaction between attacker and emulating services.

B. Medium Interaction Honeypots

Like low interaction honeypots these also do not provide OS access to attacker but chances to be probed are more than low interaction honeypots [9] .Some examples of medium interaction honeypots are Napenthes , Dioneae , honeytrap ,mwcollect .These honeypots also provide facad services to the attackers .Mwcollect and napenthes can be used to collect the spreading malwares.

C. High Interaction Honeypots

These are the most sophisticated honeypots .These are difficult to design and implementation .These honeypots are very time consuming to develop and have highest risks involved with this as they involve actual OS with them .In high Interaction Honeypots nothing is simulated or restricted[10]. Some example of High interaction honeypots are Sebek, Argos. As these honeypots involves real operating system the level of risk is increased by many extents, but to capture large amount of information by allowing an attacker to interact with the real operating system ,it is a kind of trade off [13].This helps in capturing and logging of attackers behavior that can be analyzed in later stage.

Table 1 Shows About the Various factors Associated with different Honeypots .

Various Factors Associated with Honeypots			
	Low interaction honeypot	**Mid interaction honeypots**	**High interaction honeypots**
Degree of involvement	Low	Mid	High
Real operating system	-	-	x
Risk	Low	Mid	High
Information Gathering	Connections	Requests	All
Compromised wished	-	-	x
Knowledge to run	Low	Low	High
Knowledge to Develop	Low	High	High
Maintenance time	Low	Low	Very High

III. PURPOSE OF HONEYPOTS

A. Research Honeypots

Research honeypots are basically used to attain information about the new ways of attacks, new attacks, viruses, worms which are not detected by IDS. These honeypots are used for research purpose. Mostly educational entities, military or government organizations, these kinds of honeypots are used to gather information about motives and new tactics about the black hat community. These honeypots never add direct value to the organization, difficult to maintain and deploy, complex in architecture, but provide extensive information which is worth to develop new policies to protect the organizational network. Research Honeypots are used to gain Information about black hat community Research honeypots are used [3] .Its primary function is to follow the footprints of attacker and gain knowledge about the new ways of attacks performed threats.

B. Production Honeypots

Production honeypots are easy to deploy, use and capture less information and are primarily used by companies or corporations. These honeypots are placed along with the production server inside the production network of the organization to improve overall security. A production honeypot is one which is used within organization to prevent attacks and mitigate risks .It provides immediate security to production resources [3].Production honeypot tend to duplicate the production network or provide some services such as Ftp, Http, SMTP to the attackers .Commercial organizations get more benefits from production honeypots. It addresses some challenges to IDS because of its simplicity .Sometimes attack is too recent to the vendors in such situations IDS doesn't give any alert as it uses it is limited to the signature based database for detection of intruders .Sometimes untuned IDS alarms too much on normal network traffic. This is called false positive .Honeypots address these challenges as all the traffic sent to honeypots is unauthorized that means there is no false positives no false negatives and large data sets to analyze.Table2: Represents honeypots based on their interaction level and based on purpose.

Table2: Types of Honeypots

Sr. no	**Honeypots**	**Types of Honeypots**	**Example**
1	On the basis of interaction	1)low interaction honeypots.	Honeyd, Kippo
		2) Medium interaction honeypots	Dionea, Napenthes
		3)High Interaction honeypots	Specter
2	On the basis of purpose	1) Research honeypots.	A standalone PC having any operating System installed like Linux.
		2) Production honeypots.	kF sensor, specter, Dioneae, Napenthes

IV. HONEYTOKENS

Honeytokens are the small sized honeypots . Unlike honeypots the standalone machines, honeytoken are the digital entities such as digital data created and solely analyzed which are used to capture digital thefts. They can be fake data sets which can't exist in real world, at least within a specific enterprise. These are used to track malicious outsiders and insiders engaging in unauthorized activity. Honey tokens may be a url address, an excel sheet or sometimes a fake record in the organization's database. For instance, a number of companies use honeytokens like fake email address, user account, database data and sometime s executables or false programs. Fake email accounts are used for early warning for spammers. The basic idea is that the fake email address is never used and thus would have no valid reason for receiving spams. Receiving unrequested email to that specific email address indicates that someone has accessed the company's internal email list. Another approach is to insert fake data in the company's data base that's unlikely to exist in the real world into a real database[15]. For example companies can insert celebrity names who have no direct connection to the organization such as Paul Stanley, Peter Criss. Any kind of unauthorized interaction with these fake names ensure us about the malicious activity against the information accessed from the database of organization.

V. ADVANTAGES OF HONEYPOTS

Being a part of network security mechanism honeypots have many advantages. Here we will highlight some specialties of honeypots.

A. Small data sets :

Any connection made with the honeypot is considered as malicious. So the thousands of alerts logged by organizations can be reduced to hundreds of entries.

B. Reduced False Positives:

Honeypots help in reducing false positives. The larger the probability that a security resource produce false positives or false alerts the less likely the technology will be deployed. Any activity with the honeypot is considered dangerous and making it efficient in detecting attacks.

C. Catching False negatives:

Catching false negatives with the help of honeypots is quiet easy because every connection made to honeypot is considered unauthorized. Traditional attack detecting tools becomes fail in detecting new attacks like signature based detection tools. These tools detect only those attacks whose signatures are already in their database. As per honeypot's approach, there is no need of predefined database.

D. Encryption:

Honeypots have the capability to capture the malicious activity if it is in encrypted form. Encrypted probes and attacks interact with the honeypots as end point where the activity is decrypted by the honeypot.

E. Working with IPv6

Hoeypots work in any IP environment, including IPv6. IPv6 is the new version of IPv4 and actively used by the countries like Japan and the department of defence. Many current technologies like firewalls and Ids sensors do not work on IPv6.

F. Flexible :

Honeypots are extremely adaptable in variety of environments. From a social security number embedded into a database, to an entire network of computers designed to be broken into.

G. Minimal Resources:

Honeypot require minimal resources. A simple Pentium computer can monitor millions of IP addresses.

VI. DISADVANTAGES OF HONEYPOTS

A. Single Data Point:

One huge drawback is generally faced by honeypots that they are worthless if no one attacks them. Obviously, they can accomplish wonderful things but if the attacker doesn't send any packet to honeypots then it would blissfully unaware of any unauthorized activity.

B. Risk:

Once compromised , honeypots can introduce risk to organisation's environment. Different kind of honeypots possess different levels of risk. Low interaction honeypots Introduce low risks but high interaction honeypots introduce high risks likely whole platform to the attacker. Sometimes a poorly contained honeypot puts the entire network at risk. Furthermore, honeypots do not fulfill their promice until one has the time to administer them properly. So, administration should be done on properly by administaror having keen knowledge on security devices .

VII. LEGAL ISSUES WITH HONEYPOTS

A . Entrapment:

A person is entrapped when he is induced by law enforcement officers or their agents to commit a crime that he had not no prevous intent to commit.Truely, entrapment is not an issue. There are some reasons like firstly, most individuals in the organization are not law enforced and they do not act under the control of law and they don't have procecution as intent. So, entrapment doesn't apply here. Also, for law enforcement honeypots do not represent entrapment, as honeypots ae not used to persuade or induce attackers. Attacker itself decide whether he wants to interact with the honeypot or not.

B. Privacy:

The next considerable issue is the privacy .It could be consider in two ways. Either in the files placed on compromised systems by intruders or the interception of communication relayed through the honeynets. There is less case law surrounding interception of communication that is relayed through a compromised host.

VII CONCLUSION AND FUTURE SCOPE

The trend of using honeypot is very traditional in network security. It has become necessity of the security for information to lure attackers to some other fake sites in the network than the actual site ,where real resources of information are available. Even these honeypots could be extended to honeynets, where attacker deals with the bunch of honeypots. The log files analyzed through these honeypots and honeynets could be used to enhance the Intrusion detection system to make it smarter in catching intrusions.

REFERENCES

[1] Spitzner, L. Open Source Honeypots: Learning with honeyd, Security Focus, 2003.

[2] Wikipedia. http://en.wikipedia.org/wiki/Honeypot_(computing).

[3] Karthik, S., Samudrala, B. and Yang, A.T. Design of Network Security Projects Using Honeypots. Journal of Computing Sciences in Colleges, 2004.

[4] Know your enemy Honeynets, http://www.honeynet.org/papers/key.html
SANS institute GIEC certification GSEC Assignments#1.4:Honeypots Stretegic Considerations,2002.

[5] Kreibich, C. and Crowcroft, J. Honeycomb – Creating Intrusion Detection Signatures Using Honeypots Proceedings of the Second Workshop on Hot Topics in Networks (Hotnets II), Boston, 2003, 51-56.

[6] Martin, W.W. Honeypots and Honeynets – Security through Deception. http://www.sans.org/reading_room/whitepapers/attacking/41.php, SANS Institute, 2001, As Part of the Information Security Reading Room.

[7] John Carroll, Computer Security, 3rd ed., Butterworth-Heinemann, 1997.

[8] Provos, Honeypot Background. http://www.honeyd.org/background.php.

[9] Baumann, R. and Plattner, C. White Paper: Honeypots, Swiss Federal Institute of Technology, Zurich, 2002.
[10] Sutton Jr., R.E. DTEC 6873 Section 01: How to Build and Use a Honeypot.
[11] Craig Valli,Honeyd-OS artifice Australian Computer, Network & Information Forensics Conference 2003.
[12] Netsec. (2012, 15th March). Specter. Available: http://www.specter.com/default50.htm
[13] A. N. Singh and R. Joshi, "A honeypot system for efficient capture and analysis of network attack traffic," in International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), 2011, 2011, pp. 514-519.
[14] Honeypots catching the insider threat lans spitzner.
[15] http://www.infoworld.com/d/security/beyond-honeypots-it-takes-honeytoken-catch-thief-216467