International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT217142

Honeypot : A Trap for Attackers

Syed Nasir Abas, Er. Parvinder Kaur
Shaheed Udham Singh Group of Institutions, Tangori, Punjab, India

Article Info
Volume 7, Issue 1
Page Number: 238-243
Publication Issue :
January-February-2021
Article History
Accepted : 15 Feb 2021
Published : 22 Feb 2021

ABSTRACT

A honey-pot is a type of toolkit used to deceive attackers, designed to detect an attacker attempting to compromise the production systems of any institute/organization. If designed and deployed correctly, a honeypot can act as an advance surveillance device and well as a threat intelligence gathering device. It is used to analyse the behavioural signature of the intruders trying to attack a system and to provide informational insights into potential system loop-holes.

Keywords: Honeypot, Honeynet, Cyber-Security, IDS, IPS.

I. INTRODUCTION

In the age of information and technology network security has become the main issue in every single 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 analyse 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 flow and give the alarms to tell about any kind of attack based upon the database of signatures of existing intrusions.

A number of issues are with IDS too as it may show an increasing number of false alerts and alarms [7]. Honeypots then introduced in the network to utilize the network's unused IPs and the attacker's behaviour is analysed on these honeypots. Honeypots improve IDS too as we use honeypots with IDS the number of false positives decreases. With the addition of honeypots network security accuracy increases than the only implementation of network Intrusion detection system.

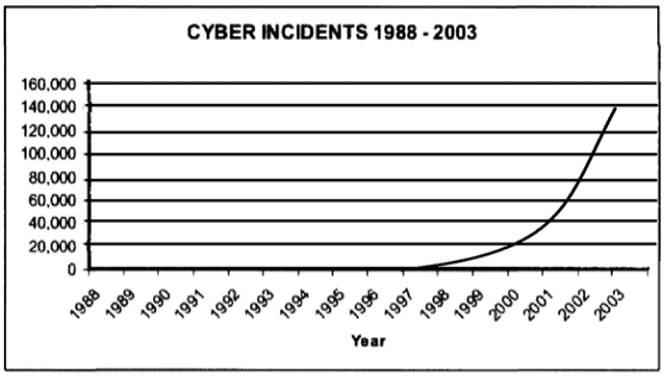
A. Honeypots

Honeypot is a unique security tool which is a part of security mechanism deployed in an organisation. These are the tools you want the black hat guys to interact with. Basically, honeypot is an IT technique 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 warning systems, slowing down and automated attacks and capturing new exploits to gathering intelligence on emerging threats.

II. TYPES OF HONEYPOT

Honeypots are basically classified into three types. The first classification is based on the level of interaction they offer to the malicious user high and low. Another classification is based on whether the client side or the server side of the interaction the honeypot is implemented. A third classification is based on the utilization of honeypots, i.e. either they are used for research or production purpose.



A. Low/High Interaction Honeypot:

Low Interaction Honeypots are defined by their limited response capabilities towards attacker's malicious payload. All services offered by low interaction honeypots are not actual services but they are simulated. That's why low interaction honeypots are not vulnerable and will not become infected by the malicious exploit tried against the deployed simulated vulnerability. On the other hand, high interaction honeypots have no limits in terms of responding to attacker's activities. It uses actual vulnerable service or vulnerable software versions. Thus, high interaction honeypots provide far more contingencies of how an attack can exploit the system or how a particular malware may execute in real-time. Since there is no simulated service, high interaction honeypots help in identifying zero-day/unknown vulnerabilities. But high interaction honeypots are more prone to infections if not correctly deployed. Also, high interaction honeypots increase the risk because attackers can use a real honeypot's vulnerabilities to attack and compromise actual production systems.

Terms	On the basis of Level of Interaction			On the basis of Implementation Environment	
	Low interaction Honeypots	*Medium interaction Honeypots*	*High interaction Honeypots*	*Production Honeypots*	*Research Honeypots*
Definition	Low interaction honeypots provide the emulated or simulated environment to attackers.	Medium interaction honeypots are more advanced than low level honeypots, but less advanced than high level honeypots.	High interaction honeypots provide the real operating system services to the attackers.	Production honeypots provide simulated services and operating system to work with.	Research honeypots provide real services in order to get huge information about the attackers.
Exertion of installation and configuration	It is easy to install and configure.	It is complex than low interaction honeypot but easier as compare to high interaction honeypots.	It is very difficult to install and configure.	Production honeypots installation and configuration depend upon the organization.	It is difficult to install and configure.
Implementation and maintenance	It is very easy to implement and maintain because of easy functionality and design.	It involves medium implementation and maintenance.	It requires complex method for implementation and maintenance process.	It requires medium level process for implementation and maintenance.	It is very difficult to deploy.
Collection of Information	Limited collection of information	Medium information gathering	Extensive collection of information	Medium collection of information	Huge collection of attackers details
Risk level	Low interaction honeypots involve very less risk because of providing simulated services to attackers	Medium interaction involves risk because of combination of both low and high level interaction honeypots.	It involves very high risk of revealing important information to the attacker because it provides real services and operating system to the attackers.	It involves high risk of losing organization resources to the attackers.	It involves less risk because it is designed for research purpose.
Tools deployed	BackOfficer Friendly, Honeyd, KFsensor.	Specter	Mantrap, honeynets	NetBait	Bigeye

B. Server/Client-Side Honeypot:

Server honeypot is a traditional honeypot technology. It is based on protecting server from any unknown attacks but it is not able to detect client-side attacks. Server honeypots act as though it is an actual production server, exposing some known software based or platform based vulnerable service and passively waiting to be attacked. However, to detect client-side attack, client system needs to interact with servers and to process malicious response data. Thus, for detecting client-side attacks, client honeypots are mainly used. The idea of Client Honeypot is to crawl the domain network, interact with malicious/to-be malicious servers and classify the servers based on their malicious nature.

C. Production/Research Honeypot:

Production honeypots are basically used by companies/organizations to palliate possible risks [4]. Production honeypots are replica of actual production servers deployed in organization. They are placed in the organizational networks for increasing the actual server's security. Most of the production honeypots are low-interaction which are easy to deploy. That is why they are not very useful in detecting any unknown attacks which are not included in vulnerabilities signature database. On the other hand, research honeypots are high interaction honeypots and it is mostly deployed in educational or research organizations. By using this type of honeypots, security researchers can get more information about attacks, vulnerabilities and the methods used by the attackers. This analysis helps an organization to design more secure production environment.

III. PURPOSE OF HONEYPOTS

A. Research Honeypots

Research honeypots are basically used to get information about the new types of attacks, new attacks, viruses, worms which are not spotted by IDS. These honeypots are used for research purpose by mostly educational units, military or government organizations, these kinds of honeypots are used to collect information about motives and new strategies about the black hat community. These honeypots never enhance direct value to the organization, difficult to maintain and deploy, complex in architecture, but provide extensive information which is worth to grow new policies to protect the organizational network. Research Honeypots are used to gain Information about black hat community [3]. Its main function is to follow the footprints of invader and gain knowledge about the new techniques of attacks performed threats.

B. Production Honeypots

Production honeypots are easy to deploy, use and gather less information and are mainly used by companies or corporations. These honeypots are to be found along with the production server inside the production network of the organization to advance 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 have a tendency to 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 tasks 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 its limited signature-based database for detection of attacks. Sometimes untuned IDS alarms and alerts 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 analyse.

IV. ADVANTAGES OF HONEYPOTS

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

A. Small data sets

Any communication 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 generate false positives or false alarms the less likely the technology will be deployed. Any activity with the honeypot is considered risky and making it effective in detecting attacks.

C. Catching False negatives

Catching false negatives with the help of honeypots is quite easy because every connection made to honeypot is considered unauthorized. Traditional attack sensing tools fail in detecting new attacks like signature-based detection tools. These tools notice 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 ability to capture the malicious activity if it is in encrypted form. Encrypted probes and attacks makes a connection with the honeypots as end point where the activity is decrypted by the honeypot.

E. Working with IPv6

Honeypots 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. Lot of 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 fixed into a database, to a complete network of computers designed to be broken into.

G. Minimal Resources

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

V. DISADVANTAGES OF HONEYPOTS

A. Single Data Point

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

B. Risk

Once system is compromised by an attacker, honeypots can introduce risk to organisation's environment. Different kind of honeypots have different levels of risk. High interaction honeypots make known to high risks likely whole platform to the attacker. Sometimes a poorly designed honeypot puts the entire network at risk. Furthermore, honeypots do not fulfil their promise until one has

the time to administer them properly. So, administration should be done on properly by administrator having keen knowledge on security devices.

VI. LEGAL ISSUES WITH HONEYPOTS

A. Entrapment

A person is tricked when he is convinced by law enforcement officers or their mediators to commit a crime that he has no previous intent to commit. Truly, 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 prosecution as intent. So, entrapment doesn't apply here. Also, for law enforcement honeypots do not represent entrapment, as honeypots ae not used to encourage or persuade attackers. Attacker itself decides whether he wants to communicate with the honeypot or not.

B. Privacy

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

VII. CONCLUSION AND FUTURE SCOPE

The trend of using honeypot is in latest network security. It has become need of the security for information to lure intruders to some other fake sites in the network than the actual site, where real resources of information are available and stored. Even these honeypots could be prolonged to honeynets, where attacker connects with the bunch of honeypots. The log files examined through these honeypots and honeynets could be used to improve the Intrusion detection system to make it advance in catching intrusions. Honeypot can be used with other well-established security tools such as IDS or Firewalls to make them more effective.

VIII. REFERENCES

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

[2]. Christian Doring, "Improving network security with honeypot."

[3]. The Government of the Hong Kong Special Administrative Region, "Honeypot security" February 2008.

[4]. Honeypots: Basic Concepts, Classification and Educational Use as Resources in Information Security Education and Courses

[5]. http://project.honeynet.org/papers/individual/Doering.pdf 6. http://security.rbaumann.net/download/honeyd.pdf

[6]. Setting Up And Running A Honeypot – Nepenthes,Brian Allen (ballen at wustl.edu) Network Security Analyst ,Washington University in St. Louis

[7]. http://www.pixel-house.net/midinthp.pdf

[8]. http://www.honeypots.net/.

[9]. http://www.honeynet.org/papers/kye.html.

[10]. http://www.honeyd.org/background.php.

[11]. http://cs.millersville.edu/~csweb/lib/userfiles/honeypot.pdf

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

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

[14]. Know your enemy Honeynets, http://www.honeynet.org/papers/key.html SANS institute GIEC certification GSEC

Assignments#1.4:Honeypots Stretegic Considerations,2002.

[15]. 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.

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

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

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

Cite this article as :

Syed Nasir Abas, Er. Parvinder Kaur , "Honeypot : A Trap for Attackers", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 1, pp. 238-242, January-February 2021. Available at
doi : https://doi.org/10.32628/CSEIT217142
Journal URL : https://ijsrcseit.com/CSEIT217142