GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec



SANS Security Essentials
GSEC Practical Assignment
Version 1.4b
Option 1

Production Honeypots: An Organization's view

Submitted by

Abhilash Verma

Date of Submission: 23-10-2003

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of Contents

1.0 ABSTRACT **2**

2.0 INTRODUCTION TO HONEYPOTS **4**

THE NEED 5
Figure 1: Vulnerabilities / Incidents graph *5*

3.0 CLASSIFICATION AND PLACEMENT **6**

Figure 2: Classification of Honeypots *6*
Figure 3: Placement of Honeypots *7*

4.0 PRODUCTION HONEYPOTS **8**

4.1 DETECTION 8
4.2 PREVENTION 9
4.3 REACTION 9

5.0 ADVANTAGES OF PRODUCTION HONEYPOTS **10**

6.0 DISADVANTAGES OF PRODUCTION HONEYPOTS **11**

7.0 PRODUCTION HONEYPOTS: MONITORING THE INSIDERS **12**

7.1 HONEYTOKENS 13
Figure 4: Placement of Honeytokens *14*

8.0 LEGAL ISSUES **15**

8.1 LIABILITY 15
8.2 PRIVACY 15
8.3 ENTRAPMENT 16

9.0 PRODUCTION HONEYPOTS: IMPROVING ROI **17**

9.1 AN OVERVIEW 17
9.2 CALCULATING ROI 18
Figure 5: Asset Valuation (different attributes) *18*
9.3 METHOD FOR CALCULATING ROI 21

10.0 THE FUTURE WITH DYNAMICS **25**

11.0 CONCLUSION **26**

12.0 REFERENCES **27**

© SANS Institute 2004, Author retains full rights.

1.0 Abstract

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Honeypot is a fairly new technology but has become a part of the Defense-in-Depth strategy of security-focused organizations. Still many organizations are not very sure about their potential in terms of their returns to the production activities and business processes. This paper is written during the research and planning for deploying a production honeypot in an organisation.

The focus of this paper is to help professionals, consultants or managers with understanding of production honeypots in order to aid deployment of the same in their organization. In this context the paper covers the basics of honeypots their classification and placement. Thereafter it focuses on Production honeypots describing their advantages and disadvantages. Then a comprehensive overview of internal honeypots is given with a brief idea of honeytokens (special form of Internal honeypots). Further, the legal issues associated with production honeypot deployment are discussed along with, how the organization is responsible for their functioning. Then the focus moves towards the business side, the Return On Investment (ROI) of deploying a production honeypot in an organization. A method to calculate the effective ROI of production honeypots is also suggested. And finally it talks about their future in the organization.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2.0 Introduction to Honeypots

Threat in today's environment is increasing with a high magnitude and effect in spite of having different security mechanisms in place. Just by having an anti virus software it is very difficult to say that the systems are free from virus threat. Same as sitting behind a firewall doesn't means that the network is out of reach of malicious activities and intents. This is all because every new virus or new attack finds some different way to penetrate the security infrastructure, which often goes undetected by the security technologies in place. The answer to this issue is to have some technology, which is designed to get compromised and is meant to welcome the attackers. Because this is the excellent way to learn new developments in the attackers community and their motive of penetrating into any security perimeter, it also has lots of other values and benefits discussed in the following sections.

The fundamental concept of honeypots originated from Clifford Stoll's paper "Stalking the Wily Hacker", wherein he mentioned about "catching flies with honey" but he did not used the term honeypot in his paper [1]. With the very first instance it suggested a way to catch the attackers by luring them to the arena of their interest. Thereafter in 1991 Bill Cheswick of AT&T Bell Laboratories wrote a paper "An Evening with Berferd" detailing his experiences monitoring a hacker who attempted to hack into their Internet gateway [2]. Bill responded to the commands the hacker attempted to perform on the system and then constructed an actual system for further study of his activities.

According to Lance Spitzner (active member of Project Honeynet [3]), **"**A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource" [4]**.**

The main goal is to distract the attacker from real systems and to gain valuable information about them with the tools and exploits they use. All the traffic from and to a honeypot is suspicious and unauthorized because of the fact that no production services are provided by this resource. All data collected by a honeypot is therefore interesting and it never generates big number of logs. It can further be used for prevention of attacks and can debar attackers from other systems by occupying their resources for long duration. The information gathering for an attack depends on the level of tracking enabled on the honeypot. Common tracking level includes technologies and methods like firewall, system logs, sniffers, IDS tools, integrity checkers and few others.

---

[1] Stoll, Clifford. "Stalking the Wily Hacker." URL: http://cne.gmu.edu/modules/acmpkp/security/texts/HACKER.PDF
[2] Cheswick, Bill. "An Evening with Berferd." URL: http://www.tracking-hackers.com/papers/berferd.pdf
[3] Spitzner, Lance. "The Honeynet Project." URL: http://www.honeynet.org/misc/project.html
[4] Spitzner, Lance. "Definitions and Value of Honeypots." URL: http://www.tracking-hackers.com/papers/honeypots.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The Need

As there are lots of security technologies already available to protect organization's security infrastructure then what is the need of introducing this new concept of attracting attackers rather than preventing them?

The simple answer is that all other technologies can prevent attackers according to the intelligence they have from their past learning and incidents. So most often it is difficult to detect new attacks or way of penetration by existing intelligence of the security technologies. According to the facts provided by CERT/CC, it is easy to analyze the ratio of incidents and vulnerabilities reported in recent years [5].

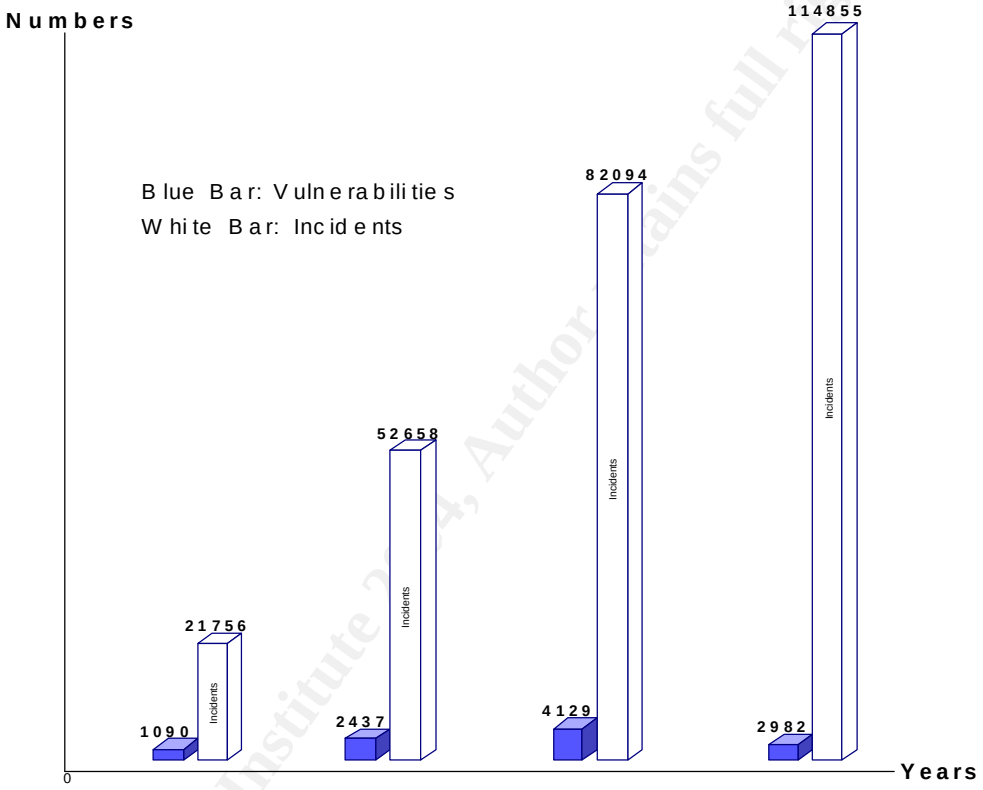


Figure 1: Vulnerabilities / Incidents graph

By the graph it is absolutely clear that the incidents are much more than the vulnerabilities discovered in a year. Attackers successfully exploit the known vulnerabilities by different ways, which are often not detectable by virtue of existing technologies. So there is a need to find out existing vulnerabilities, the way attackers can exploit them in the production environment and most importantly the kind of information they are interested in. Honeypots addresses all these issues to a good measurable extent. All this can be done in effective manner only if one can see the real incidents and is able to analyze them, which is the main focus of deploying honeypots in the security infrastructure.

[5] Cert/CC. "Statistics 1998-2003." URL: http://www.cert.org/stats/

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3.0 Classification and Placement

Honeypots are broadly classified via two methods: their usage and the level of involvement they provide. According to the usage they are classified as Production honeypots and Research honeypots. Production honeypots are used to reduce the risks in the business/production environment and thus are largely deployed in organizations. Research honeypots are meant to gather as much information as possible. Although research honeypots do not add security value to an organization, but they can help a lot in understanding the attackers community and their motives. This diagram will help to understand the classification level of honeypots with important attributes.

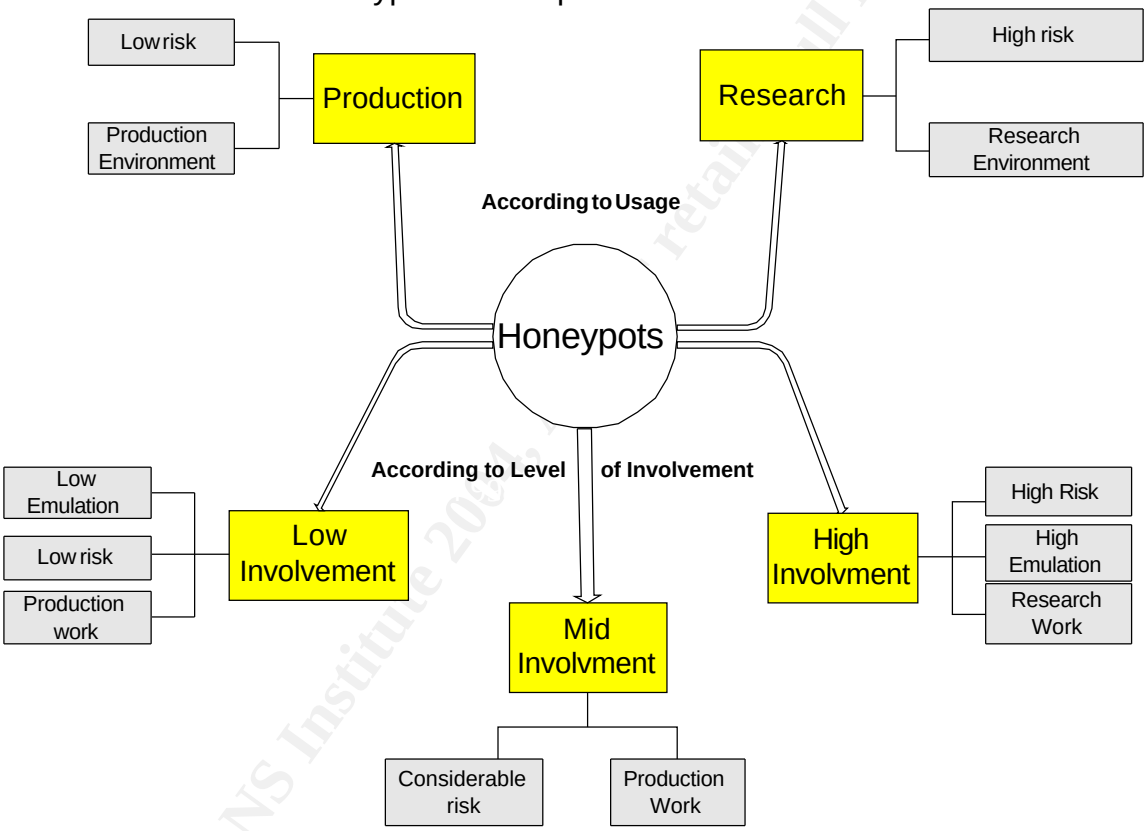


Figure 2: Classification of Honeypots

According to their level of involvement they are categorized into three types. Low involvement is the level in which the honeypots emulate simple services and the freedom given to attackers is minimum. They are passive in approach so attackers cannot use them to attack other systems, thus they are well suited for organizations and many production honeypots come into this category. Mid involvement honeypot provides more services than low level but doesn't provide a real operating system. The risk also increases with the level of emulation they provide to attackers. High involvement honeypot gives a real operating system to attack upon. This exposes the system to ample of risk and complexity.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

At the same time the possibility to accumulate information about the attack as well as the attractiveness of the honeypot increases a lot, so they are specially used for research purposes.

Honeypots can be placed externally as well as internally according to the purpose of their deployment. Conceptually they can be placed at three main locations in an organization.

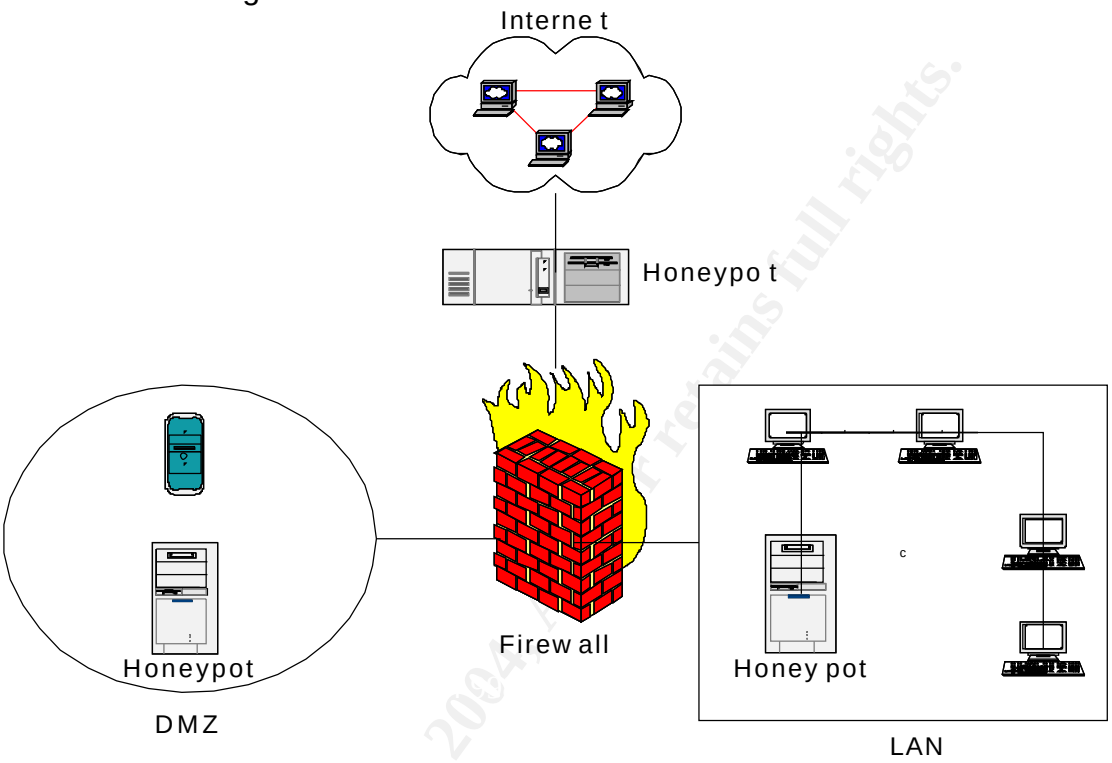


Figure 3: Placement of Honeypots

By placing them outside the firewall, risk to the internal network reduces but it limits their ability to emulate the production systems and generate logs, which are relevant to the internal network. Being inside the internal network, they can emulate the production systems as well as can monitor the attacks made from inside the network. They give proper logs of all the activities and can be easily integrated with other security technologies to get the best output. They help in taking legal actions against the attackers who break inside the internal network. Although being inside the network they introduce some risks, especially when the internal network is not secured against the honeypot through additional security mechanisms. By placing them inside the DMZ (De militarized zone), they can easily emulate the servers that are freely accessible to the public domains. This also increases the security of the production environment because of the limited access to internal network from the DMZ. Reto Baumann and Christian Plattner thesis can be referred for thorough understanding of classification and placements of honeypots [6].

[6] Baumann, Reto and Plattner, Christian. "Honeypots." Url: http://security.rbaumann.net/download/diplomathesis.pdf

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4.0 Production Honeypots

The concept of production honeypots is to emulate real production systems and have attackers spend time and resource attacking them as opposed to the production or critical systems and to learn the way they exploit vulnerabilities in production environment. Production honeypots mainly emulate specific services and sometimes operating systems to invite attackers. They can also emulate different backdoors, viruses and trojans to lure the attackers. For an example to examine attacks on web servers a production honeypot emulating the Web server and fake services can be deployed. The other very interesting part of production honeypots is that, they can be very well deployed internally to find out the internal loopholes and attackers within.

The value of production honeypots lies in all the three intrinsic security functioning of an organization. Lance Spitzner has talked about these three specific areas in his paper "Definitions and Value of Honeypots" [7]:

4.1 Detection

Production honeypots add extensive value to the organization's detection capability they are destined for. Often organizations are so overwhelmed with production activity, they don't have time and resources to spend through gigabytes of system logs for detecting the attacks. Even if they happen to surf through all the logs, still it won't be sufficient for complete detection because the extensive logs generated by security technologies suffer by false positives and false negatives.

Production honeypots are designed in such a way that either there is no false positive or very few because all the activities on production honeypots is taken as illegitimate, hence all the logs are relevant, important and reveal some problem, attack or any attempt made for the same. They are also at par with the risk of false negatives, when IDS systems fail to detect a valid attack. It is possible to launch an unknown attack that may not be detected by other security technologies but honeypots addresses this issue very well because they always detect any connection made to them via a known or unknown way by the virtue of system activity, not signatures.

A connection made to the production honeypot, is most likely a malicious activity like probe, scan or attack. If the honeypot initiates a connection, most likely means the system is successfully compromised. Thus, due to their elementary design they are best suited for detection. But they can never replace any technology for detection because they can't be placed on production systems. However they are very useful to complement the available detection technology.

[7] Spitzner, Lance. "Definitions and Value of Honeypots." URL: http://www.tracking-hackers.com/papers/honeypots.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4.2 Prevention

Production honeypots add to prevention capabilities by providing data to figure out possible ways an attacker takes to break into the organization's network and critical resources. By analyzing the attacks on honeypots many times new vulnerabilities are figured out, which attacker exploited to compromise the honeypot. These vulnerabilities may also be present on the real systems, which can then be patched to prevent the real systems from future attacks. They also make organization aware of the crucial resources and critical information attackers look for. Thus they encourage employing best practices, such as disabling futile and insecure services, patching up the system against exploits and using strong authentication mechanisms to prevent the attacks.

4.3 Reaction

Often after a system is compromised in a production environment the data gets polluted due to the continuous production work. So it cannot be used for further analyses making it difficult to even detect and preserve the evidences of the attack. The second challenge an organization faces after an incident is that the compromised systems cannot be taken off-line suddenly because it can affect the whole production process and the services they offer cannot be substituted easily. So incident response team faces difficulties in conducting an appropriate forensic analysis and study of the system.

Production honeypots score high by eliminating both the problems. They provide reduced data pollution because they do not come inside the production loop, and can be taken off-line without interrupting the production work. For example, if an attacker compromises a production server, the organization will first go for cleaning up the system and plugging specific holes so that it can continue the business. But in this process it will be very difficult to learn in detail or answer the following questions:

- What was the actual exploit?
- What was the vulnerability?
- What damage was done?
- What data has been taken away?
- Does the attacker still have internal access?
- And whether the team is truly successful in cleaning up the system?

However, if a honeypot were being used to emulate the production server with known vulnerabilities, then the chances of it being hacked would be very high. This in turn would help the response team to conduct a full forensic analysis and capture the evidences as legal proof.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

5.0 Advantages of Production Honeypots

Production honeypots carry lots of tangible and intangible advantages for an organization. Especially they add some advantages, which no other existing security technology provides.

- Production honeypots collect small amount of information. Instead of logging 1 GB of data a day, they log only 1 MB of data. Instead of generating 10,000 alerts a day, they generate only a few alerts. The information collected by honeypots is of high value, as it relates only to unauthorized or illegitimate activity. So it becomes much easier to analyze the data and derive value from it. They are designed to capture any tool, method or exploit which they have never seen before.

- They require minimal resources; an old box that is of minimum use to the organization can be configured to deploy a simple honeypot solution. It varies depending on the requirement, but usually requires fewer resources than most of other security technologies. They are versatile as one host can be set to emulate a wide number of services or operating systems.

- Unlike most security technologies, honeypots works fine in encrypted and IPv6 environment. The surrounding environment does not affect them because they simply welcome attackers rather than pushing them back.

- Information collected by them is of high value and no other technology can match some of the collected information. The gathered data can be used to learn about the attack, existing vulnerabilities and the ways intruders use to probe and gain access to the systems. The gathered data can be provided as legal proofs in the apprehension and prosecution of intruders.

- They are conceptually smooth, so there are fewer chances of mistakes in configuring and deploying them. They aid in flexible data gathering and have lots of configurable options. They can log data locally, to a central log server, put an alarm at the time of intrusion, send an e-mail to intrusion response group and can make entry in the incident database.

- One of the potential advantages of production honeypot is deterrence. On knowing that a production honeypot exist along with the original servers may inhibit attackers from trying to hack into the network and systems.

The intangible ones, are often realized after deploying and using them. For details on honeypot advantages refer to Lance Spitzner article [8].

[8] Spitzner, Lance. "Honeypots: Simple, Cost Effective Detection." Url: http://www.securityfocus.com/infocus/1690

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

6.0 Disadvantages of Production Honeypots

Like any other technology, honeypots also have some weaknesses. Their weaknesses vary a lot according to their deployment and use against the attackers. Here are the most common disadvantages of production honeypots:

- Production honeypots can only track and capture activities that directly interacts with them, they cannot capture attacks against the real systems. That is why they cannot replace any existing technology but can add a powerful layer to the Defense in Depth architecture.

- They might become a compromised host. Specifically, they have the risk of being taken over by the attacker and being used to harm other systems within or out of the organization. It could be a very difficult situation if the honeypot is used against third party systems but it hardly applies to production honeypots because of the limited emulation and interaction provided. The overall risk varies with the emulation provided to the honeypot, freedom provided to attackers and the kind of information the organization want to gather.

- If unlimited connections are allowed to and from the honeypot, then there might be loss of some of critical resources and services. The internal employees may suffer from Denial of Service and the network can face consumption of bandwidth.

- There is also a question of legality. The attacker is caught but did the organization entrap him/her? After the system is compromised some sensitive information may go out or attacker could use the compromised system to attack other legitimate systems. So the organization is liable for providing a platform that attackers can use for unauthorized activities.

- The production honeypots can be identified by any simple error in configuring them or any mistake in emulating their responses. If an attacker detects the presence of such system on any production network then they could attack that system using spoofed identity of production systems. This can create confusions for the administrators and attackers can find out other ways for intruding the production systems.

Most of the disadvantages can be taken care of by careful configuration and constant monitoring. For detailed information on disadvantages of honeypots refer to Lance Spitzner article "The Value of Honeypots (Disadvantages of Honeypots)" [9].

[9] Spitzner, Lance. "The Value of Honeypots (Disadvantages of Honeypots)." http://www.informit.com/isapi/product_id~{DF43639A-D77C-4836-ADA4-375967C20B4B}/element_id~{F98EFC44-99B4-43B2-A130-EB5A9C7BCB48}/st~{EA7ED0CD-2600-4D69-94DA-A2FB6D873AF1}/session_id~{06FC0599-097C-4772-8B50-5CDBAF8913D8}/content/articlex.asp

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

7.0 Production Honeypots: Monitoring the Insiders

Here the focus will go on a very important characteristic of production honeypots: finding out the attackers who are already inside the security perimeter. The hard fact is that an organization faces more loss from the attackers within their company as compared to the outside attackers. "The Computer Security Institute's 1998 Computer Crime Survey (conducted jointly with the FBI) reported the average cost of an outsider (hacker) penetration at $56,000, while the average insider attack cost a company $2.7 million." [10].

Looking at the figures collected in the survey the reality of business world and the necessity to track own employees can be realized well. Today for an organization production honeypots have come up as an excellent solution to find out the attackers within. They are often called as internal honeypots deployed to monitor resources against internal attackers. It is very easy for an internal attacker or an employee to penetrate the security infrastructure and resources due to the following facts:

- Physical / direct access to the system
- Knowledge of the processes being used
- Privileges to work with critical resources
- Additional access or privileges (group access)
- Motivation from external sources
- They know the ways, which security systems cannot detect
- A low risk factor because of the culture and faith of the organization
- Knowledge of the internal network, critical resources and production systems

Internal honeypots provides effective way to track employees only if their deployment has been kept a secret. The intent and method of internal attacks are quite different from an external attack. Employees have a greater fear of being caught, so they use very safe methods for executing any attack. The internal honeypots can take form of different servers or critical resources, which attracts the employees. It could be the Database Server, Mail Server, or machines named as "finance.<comp>.com", "payroll.<comp>.com", "hr.<comp>.com" (comp is the name of organisation). These systems will provide fake services and resources and open access to them will be offered through the internal network. The functioning like monitoring, data collection etc. will be the same as production honeypots. These systems can also attract the external attackers specially the ex-employees, who can take advantages of the internal knowledge they carry about the organization.

[10] Shaw, Eric D. Ruby, Keven G and Post, Jerrold M. "The Insider Threat To Information Systems." URL: http://www.nnsi.doe.gov/C/Courses/CI_Awareness_Guide/Treason/Infosys.htm

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

There is also one different form of internal honeypots, which does not provide any services to attract attackers but can have some interesting resources that are always there in normal practice but often not monitored. This form of internal / production honeypots are called honeytokens.

7.1 Honeytokens

Honeytoken is a honeypot, which is not a computer [11]. By the definition of honeypots it is easy to make out that a honeypot is not necessarily a computer system rather it can be any resource, which is meant to attract attackers and used for only illegitimate purposes. Honeytokens are entities, which carry some special meaning with them and often looks attractive to the employees. Some of them for example are:

- Username / Password
- Financial sheets
- Payroll data
- Employee's appraisal data
- Tax calculation sheet
- Credit card information
- Encryption keys
- Server configuration files
- R & D Reports
- Corporate presentation
- Proprietary information
- Any confidential document

There could be many other things, which may be more suitable and applicable to different production environments. To detect access to these honeytokens is very easy, most of the times system logs can be used to find out the access by unauthorized users with lots of details or IDS systems can also be used with simple and direct rule set to monitor these resources. The value of honeytokens lies in their simplicity and advantages. Most of the disadvantages, which were discussed for production honeypots are not applicable to honeytokens and they can be deployed at minimal costs with great findings.

The concept of honeytokens is new as well as very interesting and lots of research can be done to utilize this concept well in different kind of organizations. Here the concept of one kind of honeytokens is presented as an example. The figure below represents how these different honeytokens are placed in organization XYZ.

[11] Spitzner, Lance. "Honeytokens: The Other Honeypot." Url: http://www.securityfocus.com/infocus/1713

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

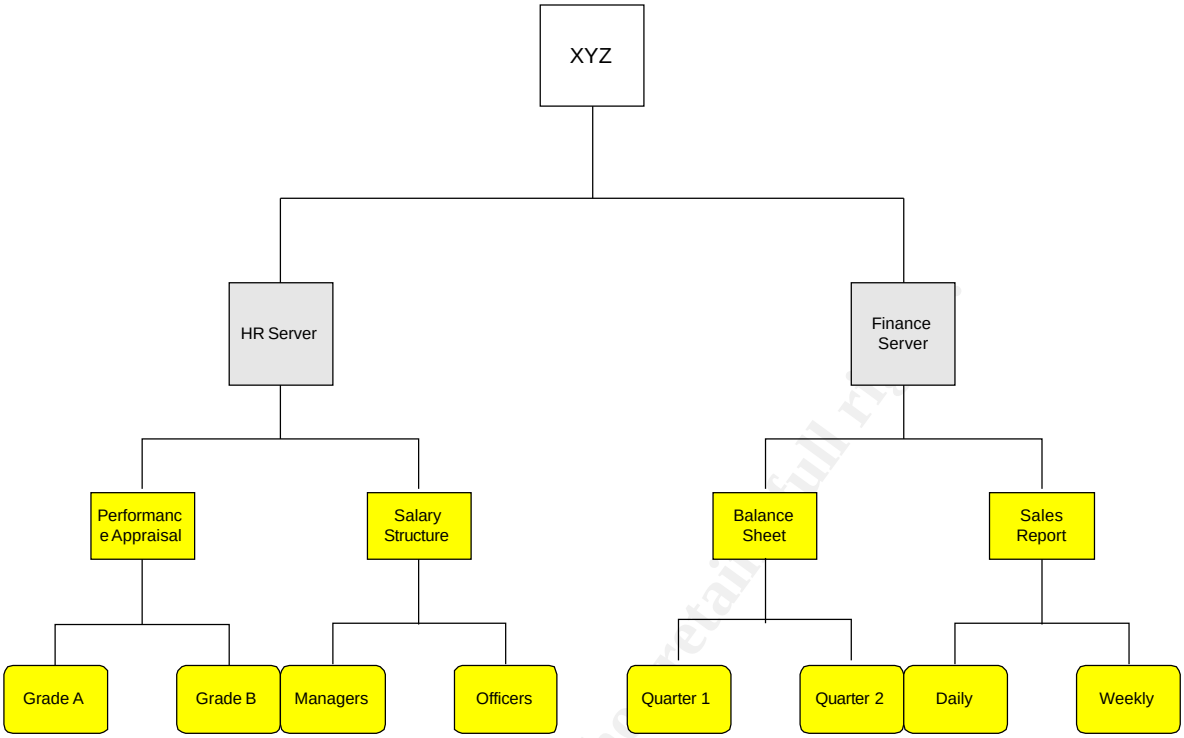


Figure 4: Placement of Honeytokens

This picture figures two server systems, which are the critical system present in the organization XYZ. This table will help you to understand it better:

HR Server	**(Machine)**	**Finance Server**	**(Machine)**
Performance Appraisal	(Folder)	Balance Sheet	(Folder)
Salary Structure	(Folder)	Sales Report	(Folder)
Grade A	(File)	Quarter 1	(File)
Grade B	(File)	Quarter 2	(File)
Managers	(File)	Daily	(File)
Officers	(File)	Weekly	(File)

Now share the Honeytokens (folders) on the network with access rights to everyone and enable object level auditing on them. Auditing can also be enabled on the files put inside the folders. A normal tendency of internal attackers is to look for and explore shared resources on the network. Thus log of all the employees accessing these resources can be created and analyzed.

This is just one way of looking at it and there can be several other ways in which the unauthorized use of resources and illegitimate activities inside the network can be detected and monitored. There can be many other ways also to use the concept of internal honeypots effectively.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

8.0 Legal issues

Honeypots being a new technology do not have many examples of legal issues or cases against them. But for an organisation it is very important to foresee all the possibilities, which can affect the organisation by any means. There is no such rule or legal regulation defined by court of law but there are some issues, which an organisation should consider before deploying a production honeypot. Lance Spitzner has talked about the legal issues in his paper "Honeypots: Are they legal" [12].

8.1 Liability

The liability factor comes when the organization is responsible for some actions made against others. The honeypot can potentially be held liable if it is used to attack or harm third party systems. Liability is more of a civil issue than criminal, because if proper precautions would had been taken to keep the system secure, the attacker would not have been able to harm others using the system. So the organization shares the fault for any damage occurred during the attack on third party systems using its resources. An organization should show diligence in protecting third party resources.

8.2 Privacy

Honeypots can capture extensive amount of information about attackers, which can violate their privacy. For privacy issue there are different laws followed by different countries. So if honeypot is in place A, but the attacker is coming in from place B, which law applies to the privacy of attacker is a question. A common law, which most of the countries follow is, it is illegal to capture any communications of an individual in real time without their knowledge or permission. There are two prime concerns to determine if a honeypot does violate an individual's privacy:

- For which purpose the honeypot is being used?
- How much information does it collect?

For an organization, honeypot is used for detection and to capture unauthorized activities thus enabling organization to take proper actions against the breach. It is most likely not considered a violation of privacy as the technology is being used to protect the organization.

[12] Spitzner, Lance. "Honeypots: "Are they legal"." Url: http://www.securityfocus.com/infocus/1703

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Production honeypots that are used to protect an organization would fall under the exemption of service provider protection category.

Second is the type of information being collected, there are two categories of information: Transactional and Content. Transactional is the information, which supports the actual data externally. It would be the data, which is used for completing the transaction or communicating the message. Content data is the actual data being communicated. For an example while sending a letter the transactional data is the address of the receiver and the sender, time, date etc. And the content data would be the exact message, which goes inside the envelope. So content data has got more privacy issues than transactional data. This distinction is important, as different honeypots capture different types of information. Production honeypots capture mainly transactional information because organizations are often interested in the origin of attack but some content data can also be collected, depending on the need and extent of emulated services.

Privacy issues are also affected by consent. When the attackers consent to monitoring, they waive their right to privacy. By placing appropriate warning banners on honeypots stating attacker's consents to logging, their privacy rights can be waived and chances of legal actions can be minimized.

Banners become an exception when the attacker doesn't know the language in which the banner is written or when the attacker bypasses the banner by entering into the system using some other way.

8.3 Entrapment

Entrapment is a legal defense, which is used to avoid a conviction and production honeypots cannot be charged with entrapment. The organization will not be prosecuted for entrapment rather it is a defense to a criminal prosecution. It is considered illegal when someone is coerced or induced to do something they would not do normally. Honeypots does not induce anyone rather attackers find their own way and break into the honeypots on their own initiative and consent. This makes it a defensive method and thus the organization is safe from legal actions against entrapment.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

9.0 Production Honeypots: Improving ROI

9.1 An Overview

Why does one go for insurance of vehicle? The simple answer is that the vehicle is an important asset to protect. The investment is worth because he/she knows its value and the risks associated with it. The risks are because of the vulnerabilities in the system and the threats, which takes advantage of existing vulnerabilities. In this case it is very easy to understand all the factors because they are familiar, but when one talks about security investment the situation changes dramatically because of the unawareness of baseline concept. For a detailed overview of security ROI, refer to S. Berinato article "Finally a Real Return On Security Spending." [13].

Return on Investment (ROI) is the key issue for managers because it is the driving factor for an organization. In business arena the CxO's will invest money in a particular solution if it is going to return some considerable amount of tangible and intangible value to their business in a defined span of time.

The condition becomes difficult for security services and technologies because security is often seen as an instrument of Insurance, which people do not consider as a serious issue. For calculating ROI of security services and technologies both the quantitative and qualitative factors must be considered. Quantitative ROI focuses more towards the hard value in numbers, which are easy to calculate and demonstrate. Whereas Qualitative ROI does not assign any numeric value rather it addresses intangible values like developing and magnifying the brand image, protection of confidential information, increasing the productivity and efficiency of the organization etc. The intangibles can be difficult to calculate and demonstrate to the bosses but they are as critical as the tangibles and a balance of hard numbers and soft numbers needs to be achieved in order to demonstrate a comprehensive and effective ROI.

In validating the ROI argument the most important issue is to assess the worth of an asset organization wants to protect. It is dealt in more details in the next section with a diagram, which depicts different attributes of an asset to calculate its value against deploying the security technologies (more focused on the deployment of production honeypot). Before asset valuation here are a few questions, which should be asked with reference to the ROI estimation and calculation of a production honeypot:

- What asset is to be protected?
- What is its criticality to the business model?

[13] Berinato, Scott. "Finally a Real Return On Security Spending." URL: http://www.cio.com/archive/021502/security.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- What are the threats associated with the asset?
- What will be the cost of deploying the production honeypot?
- Other ways to protect it, are they feasible and more cost effective?

9.2 Calculating ROI

There have been many findings for calculating Return on Investment of security technologies and products. In case of production honeypots there are some differences due to the way they work and the security (value) they provide. In order to do the calculation first thing to do is identifying the critical assets, which can be protected using the production honeypot. It can be a production process, a service, confidential information, customer or employee data and several others. As asset evaluation is very critical for the whole process this is being discussed here in accordance with the diagram below:

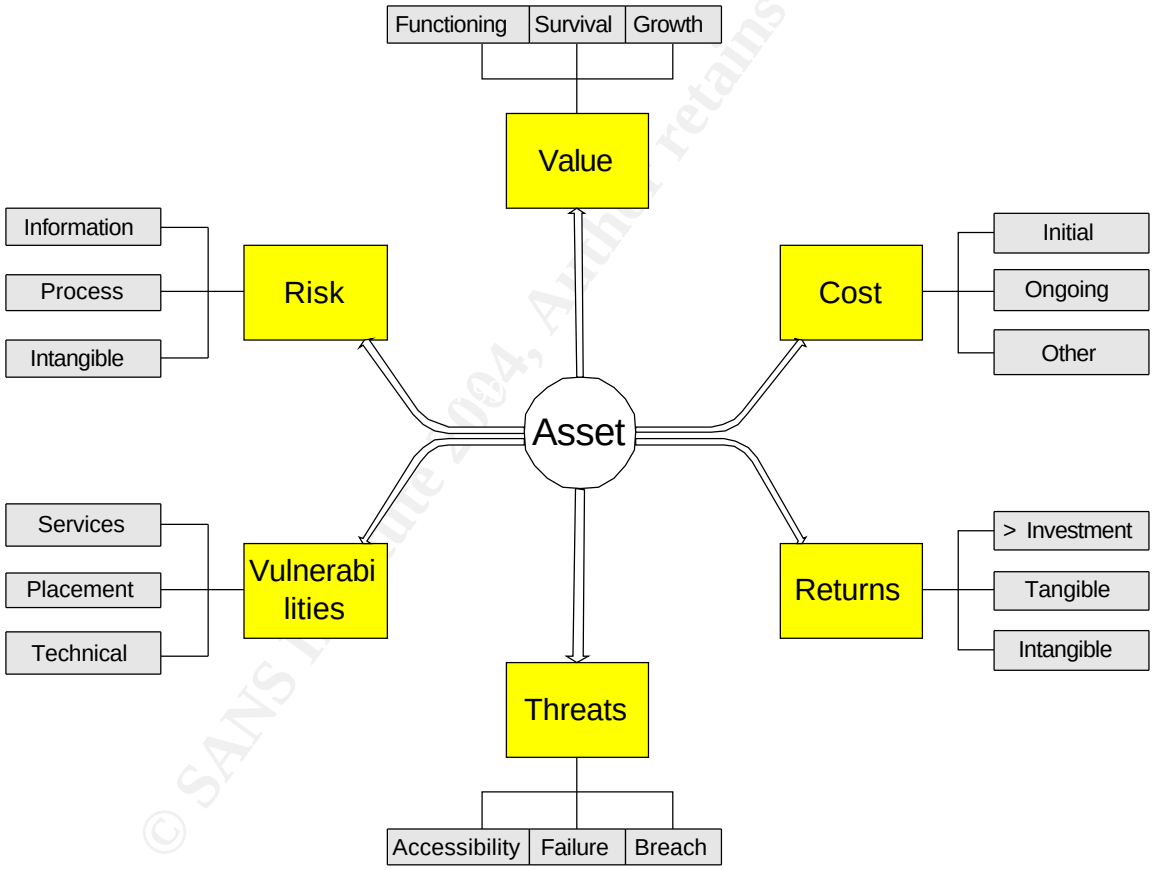


Figure 5: Asset Valuation (different attributes)

This diagram is depicting most of the attributes related to the assets, which can be protected by deploying production honeypots. The parameters used are some of the common but they may differ according to asset, production environment and the organization.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Threats:
Threats are associated with most of the assets, the need is to evaluate what are the real threats, which can affect the asset and in turn the business process.

- Accessibility to asset means how the attackers can access the asset to perform any malicious activity. It can be the physical access as well as the access through different services running on the asset. In case of information asset, it has a great impact because just the accessibility to it can cause severe tangible and intangible damages.

- Failure is the break down of the asset and thus it is unable to operate and provide any of its services. It more happens on the services part, as it can be a failure of the system or due to any present bug in the service itself.

- Breach means breaking the security infrastructure, getting hold of the asset and then making it inefficient or taking away critical information. In case of breach the unavailability of services and information loss can be tremendous.

Vulnerabilities:
The threat can affect assets only through present vulnerabilities in them. Evaluating the asset to find out existing vulnerabilities is very important.

- Services are often found to be vulnerable, through which the attackers break into the asset. Sometimes there are services executing, which are not even required and are quite vulnerable to attacks.

- Placement means the physical as well technical positioning of asset like the servers should be placed in locked server room and they should be placed behind a firewall to prevent attackers from getting access to them.

- Technical vulnerabilities are inherent to the asset architecture like loopholes in the operating systems or the basic applications.

Risks:
Risks are basically generated by the two factors of an asset discussed above: Threats and Vulnerabilities. It is the multiplication of the two and can have different forms depending upon other factors:

- Risk to the information is most critical because in any case of security incident there are more chances of information being lost. Loss of information can have tangible as well as intangible faces, which is very difficult to predict in hard values.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Risk to the process means how the failure of an asset or loss of information will affect the production/business process or other dependent processes. It is a very important factor because most of the information systems are interrelated and even unavailability of one could cause the whole process to stop.

- The intangible risks are hard to measure but make a great impact. It could be the loss of brand image due to unavailability of asset and its services, loss of customer faith on the assets and production environment, loss of reliability due to loss of confidential information and it can also go up to legal proceedings.

Value:
Value here means the business value carried by the asset and its criticality for the business / production process.

- Functioning, is the value of asset due to its individual functioning and the services it provides. It also covers the value it carries for the production process and other dependent processes and resources.

- How important is the asset for survival of the organization? There are some assets on which the complete production process depends and unavailability of those assets will stop the production and there will be a question of survival. The critical information as an asset can also question the survival of an organization if it is gone out without consent.

- Each asset contributes to the growth of the organization and intangible values provided by the asset plays an important part in it.

Cost:
Every asset has a fixed and variable cost associated with it. Variable cost keeps changing due to different factors and asset's application in the process.

- Initial cost is the price at which the asset has started functioning. In terms of information the initial cost could be very high. For example a formula developed by some pharmaceutical company, which is being used to make life saving drugs. This formula is only a piece of information, which sometimes even takes several years and millions of dollar to develop.

- Ongoing cost is the current price of the asset in the market. It is also the maintenance cost of information asset, which organization is utilizing to do its business.

- Other cost could be the depreciated cost of any asset and it could also be the future cost of critical information preserved by the organization.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Returns:
This property is used to justify the investment on deploying the production honeypot in any organization. Here returns means the value an asset will provide if it is being secured by the deployment of production honeypot.

- The basic fact is that the returns should always be greater than the investments otherwise there is no reason to go for deploying the production honeypot to protect an asset.

- Tangible returns are the hard values the asset has provided because of the applied security mechanism.

- Intangible returns are the soft values provided and are very important to consider because most of the times intangible returns are found more effective than thought of and are a very positive value provided by production honeypot.

After doing complete asset evaluation there is a clear picture of how effective will be the deployment of production honeypots in the organization in terms of protecting different assets. In the next section there is one method discussed for calculating the ROI of production honeypots. An example will also be followed along with the method to have a better understanding of the concept.

9.3 Method for calculating ROI

This method/formula will provide a way to calculate the effective ROI of production honeypots. This formula is based on the tangible returns of production honeypots because they can be shown in form of figures but Intangible returns cannot be shown as hard facts, so the pure intangibles values cannot be proved and thus cannot be justified in a formula. Hence they are shown at the end of this formula for understanding purpose.

The example taken along with the formula is of organization "XYZ", which provides online auction facility to its customers. Here a production honeypot is deployed to emulate as the Web Server, which is one of the main asset of the organization. The incident considered is unavailability of services due to DoS (Denial of Service) attack. The figures (values) are taken as an assumption and probability of such an incident and its related effects.

The first step will lead to calculating the savings done by the production honeypot:

$$\text{Savings} = \text{SPS} + \text{SNV} + \text{SOA}$$

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

SPS is the saving done on production systems by making the attacker attack a non-production system, which is the honeypot rather than the real production systems. What damage has been made to the production honeypot and what would be the losses if the same had been with production system can easily be calculated.

Probability of the incident	80%
Probability of the risk transfer to production honeypot	50%
Loss due to the incident	100,000 $

So, SPS would be:

SPS = ((80/100) * (50/100)) * 100,000 $ = 40,000 $

SNV is the saving done by finding out new vulnerabilities in real production systems through the analysis of attacks on production honeypot. There are always some hidden vulnerabilities in the systems, which is not known. When attackers exploit these vulnerabilities on the honeypot they come in front with details so that the real systems can be patched for the same. So here the estimation of losses incurred if the same exploits would have been executed on real systems will be the savings.

Probability of loss by exploiting unknown vulnerabilities	20%

So, SNV would be:

SNV = (20/100) * 100,000 $ = 20000 $

SOA is the savings done by other actions could be getting reimbursement by taking legal actions against the attack and attacker. It can also include the savings on manpower for maintenance of the honeypot system in comparison to other technologies and systems.

Probability of taking legal actions	50%
Probability of savings by taking legal actions	10%
Savings on manpower	10,000 $

So, SOA would be:

SOA = ((50/100) * (10/100)) * 100000 $ + 10000 $ = 15000 $

So the final savings would be:

Savings = 40000 $ + 20000 $ + 15000 $ = 75000 $

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Here the intangible savings done by production honeypot is not included because it cannot be quantified. For a better understanding it can be represented as:

SSR is the savings done as soft returns. It is in terms of improved efficiency, less downtime, better service, customer faith, magnifying the brand image etc. All this is really difficult to quantify in numeric values but it all adds to the business and production environment, so it needs to be taken into consideration.

The second step will lead to calculating the cost incurred:

Cost = CDH + COR

CDH is the total cost of deploying production honeypot. This cost is often less than most of the security technologies in place.

Cost of deploying the production honeypot	2000 $

So, CDH would be: 2000 $

COR is the cost occurred to recover from the incident. Cost of recovery for a honeypot system is very less but if the attacker has used the honeypot to attack on other systems and thus there is loss of resources, loss of confidential information, loss of availability or any other then recovering from these loses will also be calculated against the honeypot. It also includes the losses made to third party systems, which can escalate up to a higher level. This additional cost can be easily checked because it depends on the emulation provided to production honeypot and freedom provided to attackers. It is not feasible to put this cost here because this is a typical production honeypot by which in any case the attacker cannot reach any system outside the internal network. In internal network also the attacker has very limited access. This recovery cost also includes the cost incurred in taking the legal actions against the attacker and may be few others.

Probable cost of recovery for the honeypot	500 $
Probable cost of recovery for other systems	15000 $
Probable cost for the legal actions taken	5000 $

So, COR would be:

COR = 500 $ + 15000 $ + 5000 $ = 20500 $

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

So the total Cost would be:

Cost = 2000 $ + 20500 $ = 22500 $

Now after calculating the savings done by the production honeypot and the cost associated with its deployment and other actions taken, the effective ROI can be calculated by subtracting the cost from savings.

ROI = Savings - Cost

ROI = 75000 $ – 22500 $ = 52500 $

The effective ROI in percentage value would be:

ROI = (52500 * 100) / 21500 = 244.18 % (approx)

So the final returns are far greater than the investments, hence it would be feasible and very effective to go for deploying such a production honeypot, which will emulate as the web server of organization “XYZ”.

The ROI also differs according to the types of production honeypots. While considering honeytokens (special form of internal honeypots) ROI increases exceptionally because the cost factor for honeytokens is very less, so the savings done by any means of using honeytokens is the ROI only.

So the use of this formula may differ according to usage of production honeypots, type and effect of security incident and other related factors.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

10.0 The Future with Dynamics

According to the features of production honeypots, the only thing they require is proper configuration according to specific needs. But in this changing environment the requirements for production activities changes frequently and thus there will be a constant need to change or reconfigure the production honeypot accordingly and it also require a professional to take care of all such activities. Thus to make them more easy to use and to avoid this manual interaction Lance Spitzner has introduced the concept of Dynamic Honeypots [14].

This new concept is going to be excellently implied in organizations and they would prefer going for dynamic production honeypots because it will cut the cost to a great extent and will reduce the worries of changing production environment. It just needs one system to be configured and then put it online to learn about the network. In the first go dynamic production honeypots will learn the overall configuration of the production environment as what operating systems are being used, what servers are deployed and what services they provide etc.

To get this information they take various ways, the most effective could be active and passive fingerprinting. Passive fingerprinting would be preferred because it first captures the network activity and then analyzes it passively rather than actively on the network. After gathering all the information it finally maps the entire network and then starts deploying the honeypots mirroring original production systems. It not only does this for the existing environment rather it keeps analyzing the network activities and looks for changes in the production network. As soon as any change is detected it analyzes the new activity and accordingly configure a new honeypot or service.

To avoid manual interaction it uses Virtual honeypots on the same system to emulate different critical machines. There are few points on how this concept will bring an effective future to production honeypots and will as well provide organizations with greater flexibility and control:

- For dynamic honeypot just single system needs to be configured manually and rest the system does on its own.
- They use virtual honeypots, thus saves the physical resources.
- They can detect any change in the network automatically.
- There are very less chances of error in the auto configuration they do.

This concept is very effective and requires lots of research to be done for effectively deploying dynamic production honeypots in any organization.

[14] Spitzner, Lance. "Dynamic Honeypots." Url: http://www.securityfocus.com/infocus/1731

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

11.0 Conclusion

The breach of security today has become a common incident / problem across organizations. These incidents cause lots of damage in tangible as well as intangible senses. The threat from inside the organization is much more challenging than the external one. Attackers come up with new ideas and means of breaking into the systems and resources, so organization's need to have some protection mechanism that can save them from new or unseen risks. Production honeypots meet this requirement up to a remarkable level by protecting the organization with different features and adding various values. Organizations should also look at the risks involved in the process of protecting their resources using production honeypots and the legal factors associated with them.

For an organization to have an effective security plan, it needs to continually improve the protection measures for the critical resources by finding out new vulnerabilities. And production honeypots are found to be the best way to find out security holes in the systems, thus they give a chance to patch the holes and improve the overall security of production systems. As there are new attacks every moment, so someone needs to continually watch for any type of new attacks and get proper information and that's what the production honeypot exactly does. Production honeypots would find their place in most of the organizations very soon on the need basis. They should not be taken as independent security solution because they are designed to complement the present security architecture by adding specific values. They also provide the best way to learn about the attackers community, which increases efficiency of the organization. Thus production honeypots are worth to be included in the security architecture of any organization in one or the other form.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

12.0 References

Stoll, Clifford. “Stalking the Wily Hacker.” Volume 31. May 1988.
URL: http://cne.gmu.edu/modules/acmpkp/security/texts/HACKER.PDF
(Last Accessed 23 Oct. 2003).

Cheswick, Bill. “An Evening with Berferd In Which a Cracker is Lured, Endured and Studied.” 1991. URL: http://www.tracking-hackers.com/papers/berferd.pdf
(Last Accessed 23 Oct. 2003).

Spitzner, Lance. “The Honeynet Project.” April 1999.
URL: http://www.honeynet.org/misc/project.html
(Last Accessed 23 Oct. 2003)

Spitzner, Lance. “Definitions and Value of Honeypots.” 29 May 2003.
URL: http://www.tracking-hackers.com/papers/honeypots.html
(Last Accessed 23 Oct. 2003).

“CERT/CC. Statistics 1998-2003.“ 17 October 2003.
URL: http://www.cert.org/stats/ (Last Accessed 23 Oct. 2003).

Baumann, Reto and Plattner, Christian. “White Paper: Honeypots.” Mar 2002.
URL: http://www.open.ch/en/downloads/whitepaper_honeypot.pdf
(Last Accessed 23 Oct. 2003).

Spitzner, Lance. “Honeypots: Simple, Cost-Effective Detection.” 30 April 2003.
URL: http://www.securityfocus.com/infocus/1690
(Last Accessed 23 Oct. 2003).

Spitzner, Lance. “The Value of Honeypots.” 10 January 2003.
URL: http://www.informit.com/isapi/product_id~{DF43639A-D77C-4836-ADA4-375967C20B4B}/element_id~{F98EFC44-99B4-43B2-A130-EB5A9C7BCB48}/st~{EA7ED0CD-2600-4D69-94DA-A2FB6D873AF1}/session_id~{06FC0599-097C-4772-8B50-5CDBAF8913D8}/content/articlex.asp
(Last Accessed 23 Oct. 2003).

Shaw, Eric D. Ruby, Keven G and Post, Jerrold M. “The Insider Threat To Information Systems.” September 1998.
URL:http://www.nnsi.doe.gov/C/Courses/CI_Awareness_Guide/Treason/Infosys.htm. (Last Accessed 23 Oct. 2003).

Spitzner, Lance. “Honeytokens: The Other Honeypot.” 17 July2003
Url: http://www.securityfocus.com/infocus/1713
(Last Accessed 23 Oct. 2003).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Spitzner, Lance. “Honeypots: Are They Illegal?” 12 June 2003.
URL: http://www.securityfocus.com/infocus/1703
(Last Accessed 23 October 2003).

Berinato, Scott. “Finally a Real Return On Security Spending.” 15 February 2002.
URL: http://www.cio.com/archive/021502/security.html
(Last Accessed 23 Oct. 2003).

Spitzner, Lance. “Dynamic Honeypots.” 15 September 2003.
Url: http://www.securityfocus.com/infocus/1731
(Last Accessed 23 Oct. 2003).

Even, Loras R. “What is a Honeypot?” 12 July 2000.
URL: http://www.sans.org/resources/idfaq/honeypot3.php
(Last Accessed 23 Oct. 2003).

Spitzner, Lance. “Strategies & Issues: Honeypots - Sticking It to Hackers.”
04 April 2003.
URL: http://www.networkmagazine.com/article/NMG20030403S0005
(Last Accessed 23 Oct. 2003).

Berinato, Scott. “Return on Security Investments - Calculated Risk.” December
2002. URL: http://www.csoonline.com/read/120902/calculate.html
(Last Accessed 23 Oct. 2003).

Garfinkel, Simson. “You Can Catch More Spies with Honey.” May 2003.
URL: http://www.csoonline.com/read/050103/machine.html
(Last Accessed 23 Oct. 2003).

McLean, Greg and Brown, Jason. “Determining the ROI in IT security.”
April 2003.
URL: http://www.camagazine.com/index.cfm/ci_id/14138/la_id/1.htm
(Last Accessed 23 Oct. 2003).

Raman, Raghu. “Return on investment for information security.”
Express Computers India. 29th September 2003 (2003).

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.