Global Information Assurance Certification Paper

Honeypots or Honey Delusions

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4b

Option 1 - Research on Topics
in Information Security

Submitted by: Samir Suljkanovic
Location: Online

Paper Abstract: This is a general research on information regarding honeypots. This research is based on numerous internet articles and books that I have read in the past. This paper is supposed to give a reader an overall overview on what Honeypots are, which types of honeypots we have, and how and where they should be used.

Table of Contents

List of Figures

Abstract/Summary

The main goal of this paper was to gather information on honeypots with the aim to answer the question whether the idea of installing the honeypot as a security tool in a company is a good one or a bad one.

Reader will also learn what honeypots are, which types of honeypots we have, and how and where they should be used.

All the gathered information here presented are the result of my research impressions of the books and Internet materials that I read.

We have to keep in mind that honeypots are not a solution but just one of good tools, and we have to keep in mind that it always depends on what really we are trying to achieve.

Introduction

"Information is the oxygen of the modern age.
It seeps through the walls topped by barbed wire,
it wafts across the electrified borders. "

- Fortieth President of the USA, Actor

The importance of the information dates from who knows when and in the present day it became even more important due to the days we live in – the days of new technologies coming up annually.

This practical work of mine will present you a brief preview of one of the very powerful internet security tools that enable us to gather very useful and necessary information on how the intruders are trying to steel wished data from us.

It will also present the importance of knowing the advantages as well as the disadvantages of this detection tool.

As an Internet Security Analyst, and working daily with lots of information, I had a chance to witness how the certain information can be really important to some emergency actions just as the oxygen is important to us to breathe**.**

In order to preserve oxygen, we have to keep environment clean, in same concept - in order to preserve information, we have to keep systems clean of intruders.

In this paper I research one of the tools which is used in combination with other tools to obtain information which serves to preserve other information.

Defining Honeypots

Due to the dynamic nature of the honeypots it is really difficult to define them.

Honeypots do not solve any problems related to security of your networks and systems and instead of that, they are deployed to gather information and for that purpose they may use number of security applications.

You can find many definitions on honeypots, from many different sources, books, internet, etc. but none of the definitions will completely describe and give you an overview on what honeypot actually is.

I found more definitions of honeypots but I will quote only three of them:

"A honeypot is a resource whose value is in being probed, attacked or compromised." [1]

"Honeypots are non production computer assets set up for the express purpose of being a potential target for unauthorized activities. Although honeypots can mimic any computer resource (e.g., router, print server), they most often mimic legitimate production servers and workstations."[2]

"A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource."[3]

According to all of the definitions I read so far, I got a conclusion that honeypot is a system or a program that simulates single or multiple computers in a network, with the purpose to attract hackers, and convince them to exploit honeypot in order to gain information on how the hackers did it, which tools and methods they used, and all of that in order to better protect our real production systems.

With this in mind, honeypot should be as close as possible image of real production system in order to achieve the goal and as such could also present potential danger, but we will talk about that in next few chapters.

Honeynets are networks of honeypots, as well as high-interaction type of honeypots.

[1] Honeynet Project, 2004
[2] Roger A. Grimes
[3] The Honeynet Project – "Know your enemy" p18.

Related to Honeypots I encountered also terms Honeynet project, as well as The Honeynet Research Alliance.

"The Honeynet Project is a non-profit (501c3) research organization of security professionals dedicated to information security with goal to learn the tools, tactics, and motives of the blackhat community and share these lessons learned. Founded in October, 1999, all of our work is Open Source and shared with the security community."[4]

"The Honeynet Research Alliance is a trusted forum of other Honeynet research organizations. These organizations subscribe to the Alliance for the purpose of researching, developing and deploying Honeynets and sharing the lessons learned."[5]

There are also lots of other information related to honeypots, which I will not explain here, as this paper is a research strictly on honeypots.

History of Honeypots

I believe while describing honeypots it is very important to mention Honeypots history. Honeypot concept exists for more then a decade.

According to the Honeypots: Tracking Hackers by Lance Spitzner, following list summarizes some key events in history of honeypots:

- 1990/1991 – First public works documenting honeypot concepts – Clifford Stoll's The Cuckoo's Egg and Bill Cheswick's "An Evening With Berferd".
- 1997 – Version 0.1 of Fred Cohen's Deception Toolkit was released, one of the first honeypot solutions available to the security community.
- 1998 – Development began on CyberCop Sting, one of the first commercial honeypots sold to the public. CyberCop String introduces the concept of multiple, virtual systems bound to a single honeypot.
- 1998 – Marry Roesch and GTE Internetworking begin development on a honeypot solution that eventually becomes NetFacade. This work also begins the concept of Snort.
- 1998 – BackOfficer Friendly is released – a free, simple to use Windows based Honeypot that introduced many people to honeypot concepts.
- 1999 – Formation of the Honeynet Project and publication of the "Know Your Enemy" series of papers. This work helped increase awareness and validate the value of honeypots and honeypot technologies.
- 2000/2001 – Use of honeypots to capture and study worm activity. More organizations adopting honeypots for both detecting attacks and for researching new threats.

[4] Honeynet Project, 2004
[5] Honeynet Project, 2004

- 2002 – A honeypot is used to detect and capture in the wild a new and unknown attack, specifically the Solaris dtspcd exploit.[6]

Types of Honeypots

While researching materials on honeypots I was able to understand that there are two types of honeypots:

a) Low-interaction honeypots
b) High-interaction honeypots

Level of activity that honeypot allows to an attacker depends on the level of interaction.
List of both low-interaction and high interaction solutions can be found at:
http://www.tracking-hackers.com/solutions/

a) Low-interaction honeypots

Low-interaction honeypots normally work just by emulating operating system and services on it. For example, you may have emulation of outgoing e-mail server which may or may not support SMTP commands, you can also have other services like FTP server, which may or may not support different FTP commands, etc.

The advantage of low-interaction honeypots is in their simplicity because they are easier to deploy and require less risk. Those emulated services mitigate risk by preventing attacker to take over control on an operating system, which he or she can use to attack other targets.

The disadvantage is, however, that emulated services are limited, and it is easier for an attacker to detect a low-interaction honeypot regardless of how good emulation is.
There are many examples of the low-interaction honeypots like Specter, Honeyd, etc.

Specter (http://www.specter.com**)**

Specter is a smart honeypot or deception system. Specter includes internet services such as SMTP, FTP, POP3, HTTP and Telnet.

It simulates a complete computer system, providing an interesting target to hackers to distract them from attacking the real production systems.

[6] Spitzner, Lance, p 33.

Scepter logs everything what is going on and notifies administrators about all activities.
SPECTER automatically investigates the attackers while they are still trying to break in. SPECTER provides massive amounts of decoy content and it generates decoy programs that will leave hidden marks on the attacker's computer.
Automated weekly online updates of the honeypot's content and vulnerability databases allow the honeypot to change constantly without user interaction.

Honeyd (http://www.honeyd.org**)**

Honeyd is a very flexible tool to create virtual honeypots developed by Niels Provos. Honeyd is OpenSource and first it was built to operate on UNIX systems. Honeyd can emulate actual operating system, not just services. This means that it can behave like UNIX OS, Linux OS, Windows, or any device Cisco router, etc.

Honeyd works on the concept of monitoring unused IP addresses, any time it detects attempt of connection to unused IP address Honeyd will intercept connection and interact with the attacker pretending to be the victim.

Honeyd requires help of Arpd which is used for ARP spoofing.
Arpd actually monitors the unused IP space and directs attacks to the Honeyd honeypot.
Honeyd by default logs any connections to UDP and TCP ports, even though it may be configured to monitor specific ports like 25 SMTP, 21 FTP, etc.
Honeyd captures and logs all of the interaction between attacker and emulated service.

All of the emulated services work the same way, on certain actions of an attacker there is certain reaction. If the attacker does something what is not expected, then emulation does not know what to do, how to respond. In such cases Honeyd gives an error message.

Honeyd spoof the replies, making not only the emulated services, but emulated IP stacks behave as the operating systems would. he level of emulation and sophistication depends on what honeypot technology you chose to use.

According to Provos Niels and Honeyd Research: Honeypots Against Spam:

> Honeyd can be used effectively to battle spam. Since June 2003, Honeyd has been deployed to instrument several networks with spam traps. We observe how spammers detect open mail relays and so forth.

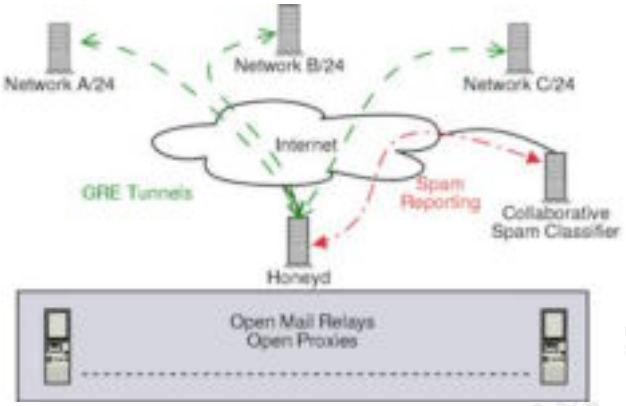

Figure 1 - Overall architecture of Honeyd system in battle against spam

> The networks are instrumented with open relays and open proxies. We intercept all spam email and analyze why we received it. A single Honeyd machine is capable of simultaneously instrumenting several C-class networks. It simulates machines running mail servers, proxies and web servers. Captured email is sent to a collaborative spam filter that allows other users to avoid reading known spam.
>
> Curiously, this setup has also been very successful in identifying hosts infected with worms. [7]

One of the ideas that fighting spam with honeypots work on is to create database of fake e-mail addresses. Due to the nature of spammers they collect information on email addresses which they use then to send spam mail messages.

"One of the main paths used by spammers to reach mail servers is going through open proxies that accept and freely transmit requests. Those open proxies play the role of screeners for the spammers that hide beyond them."[8]

This tells us that we should run open proxy on the honeypot, and then monitor traffic on certain ports.

b) High-interaction honeypots

High interaction honeypots are more complex then low-interaction honeypots as they involve real operating systems and applications.

Everything that hacker interacts with is real, no emulation, which means if you want to run specific service on specific operating system, then you must install machine with that specific operating system and that service.

[7] Honeyd - Provos Niels
[8] Oudot Laurent

"An example of a high interaction honeypot is Honeynets. Neither is better then the other."[9]

The advantage of high-interaction honeypots is that lot of information can be collected with them, by deploying real system as decoy and by giving the attacker access to the system. Lot of information can be learned such as information on new techniques, vulnerabilities, rootkits, trojans, etc.

High-interaction honeypots also provide an open environment that captures all activity. While this is the advantage, it is also an disadvantage due to increased risk.
Once hacker takes over a honeypot system, he can use this system to attack other systems. To prevent harming other systems in the network certain technologies have to be implemented that will stop hacker to harm other non-honeypot systems.

High interaction honeypots can do anything low-interaction honeypots can do, and even more, which is also the advantage, but they are also more complex to deploy and maintain.

As I already said before in this section one of the examples of high-interaction honeypots is Honeynets, other example would be Symantec Decoy Server previously known as ManTrap.

Honeynets

Honeynet is a type of a honeypot. It is a high-interaction honeypot due to its implementation which allows attackers to interact with real systems, applications, and services.

In Honeynet which is network of systems designed to interact with attackers these systems can be any type of system with services that are working on these systems. Honeynets are flexible and as such that means that I can run everything, any operating system, Cisco routers, VAX VMS, UNIX, etc.

In deployment of Honeynets attention must be made as wrong architecture of Honeynet may lead to expose our selves, or company to great risks, besides not meeting the goal of honeypots to capture and collect attacker's activities.

If attacker breaks into a Honeynet he may launch attack on other system, which will successfully compromise the victim's system. This is risk which has to be encountered in deployment of a Honeynet, before actual Honeynet is deployed.

The second thing about Honeynets is a risk of detection, as attacker can discover honeypot and then either avoid it, or eliminate its capability for capturing

[9] Tracking hackers FAQ

information, which would then present the third bad thing, which can be even completely disabling the Honeynet functionality.

On top of all of this, compromised honeypots may be used as a storage for illegal material which can be linked to us, or a company we work for, which is deploying honeypot, and since this is our property, we would be responsible for it.

Symantec Decoy Server

Key Features:

- Detects unauthorized access and system misuse to provide enterprises with cost-effective prioritization of threats
- New! Includes the improved ability to automatically create simulated email traffic between users to enhance the decoy environment
- New! Improved response mechanisms include frequency-based policies and the ability to shut down systems based on attacker activity
- New! Improved reporting and logging eases report creation and enhances prioritization efforts and incident resolution
- Provides early detection of threats, supplying information crucial to maintaining a secure network infrastructure
- Enables stealth monitoring and containment, plus live attack analysis
- Detects both host- and network-based intrusions while eliminating the inefficiencies and time penalties of false positives
- Offers centralized management, policy-based response, and comprehensive reporting and trend analysis for enterprise environments

Symantec Decoy Server provides early detection of internal, external, and unknown attacks, unauthorized use of passwords and server access to help prioritize threats, and increased network protection against intrusions. [10]

Uses of Honeypots

Preventing

Purpose of the prevention is to keep attackers out of our systems, and networks.

One of the preventing measures of being attacked again by attackers that honeypots do provide is the one that honeypots when operating in stealth mode do gather data of all attacker's moves without attacker knowing he is being watched.

[10] Symantec Decoy Server

Preventing attacks by honeypots is done in several ways and the first one is the one against automated attacks, mainly as worms or auto-rooters, as these attacks are based on tools that randomly scan entire networks in search for vulnerable systems. In case any vulnerable systems are found, the next task of these automated tools is to attack and take over the system.

Detecting

As mentioned before, one of the disadvantages of honeypots is that honeypots cannot capture attacks against other systems, unless the attacker do interacts with the honeypots.

However, at the same time this is also the advantage of honeypots, as for example Network IDS, collects millions of events from which most of them is false positive, honeypots may collect only hundred alerts, which makes collection of data easier to capture and analyze.

"Any traffic on a honeypot can be assumed to be suspicious because the system wasn't meant for internal use in the first place, and the information collected about these attacks can be used proactively to update vulnerabilities on a company's live network."[11]

Gathered detected data, and especially those of malicious activity, can be later used for detecting attacks, predicting next attacks, or doing a research on the new or unusual way the attackers attack.

Also, extreme effectiveness of detecting attacks provides honeypots' effective reduction of false positives so brand new attacks stand out and cannot be missed out to be detected.

With honeypots is easy to capture, analyze and identify new attacks. Any activity on honeypot as mentioned is not part of normal traffic, and it should not be there.

No matter which protocol attacker uses, honeypots will detect and log all of the IP activity.

Another advantage of honeypots vs. NIDS is that IDS may fail to capture encrypted attacks. Honeypots capture all of the information.

Cost to deploy Honeypots is not significant, as honeypots require minimal resources.

[11] Clancy, Heather

Responding

Responding to attacks is primarily done by collecting data and evidence of an attacker's activities. An excellent way to figure out how an attacker broke in is to use Symantec Decoy Server previously known as ManTrap.

Honeypots – Legal Issues

Although the information gained from honeypots can help us to effectively track and hunt down attacker, it may in some cases interfere with laws, as sometimes information obtained this way is not acceptable by the courts.

> Courts have traditionally held, however, that providing a *mere opportunity* for a criminal to commit a crime does not constitute entrapment. To entrap involves using persuasion, duress, or other undue pressure to force someone to commit a crime that the person would not otherwise have committed. Under this holding, setting up a honeypot or Honeynet would be like the (perfectly legitimate) police tactic of placing an abandoned automobile by the side of the road and watching it to see if anyone attempts to burglarize, vandalize, or steal it.
>
> It should also be noted that entrapment only applies to the actions of law enforcement or government personnel. A civilian cannot entrap, regardless of how much pressure is exerted on the target to commit the crime. (However, a civilian could be subject to other charges, such as criminal solicitation or criminal conspiracy, for causing someone else to commit a crime.) [12]

According to this information obtained through honeypots is legal to be used in legal prosecution as proof against attackers which compromise systems.

Conclusion

As an Internet Security Analyst, and working daily with lots of information, I had a chance to witness that the certain information really can be important to some emergency actions just as the oxygen is important to us to breathe, so we can't allow leakage of information, and we have to plan accordingly.

Many companies' certain information are hunted daily by certain attacks, and security is becoming problem one of IT industry, and request for security is growing, with growth of companies and client needs.

[12] Shinder, Debra Littlejohn and Tittel, Ed

Hackers are finding new methods and are developing new techniques to compromise systems, while security experts look for new methods of protection against hacker attacks.

Honeypots are not new, the concept of honeypots was mentioned.

Not always is possible to predict what hacker will do, and not always is practical to patch the systems completely, and to perfectly secure them.

All we can do is to study, to learn from attackers and Honeypots is really flexible and valuable tool which can allow us to learn those lessons directly from the attackers.

However, deployment of honeypots depends on level of interaction and it can be simple or very complex task.

Costs especially for companies that already deal with big risks should not exceed costs which these companies encounter through identity thefts and other fraudulent activities, and losses.

As this paper also presents honeypot that can serve in battle against spam, which also presents costs to the companies which lose lot of money on fighting spam.

Honeypots are really flexible security tool, but they do not solve or fix detected problems but detect and gather information on the malicious attacks and should be deployed in combination with other security tools, and properly planned before and secured in phase of deployment.

Complete conclusion is that honeypots are not delusion, there is nothing illusive in honeypots and I believe honeypots will advance in the future, and become one of the most used security tools.

References

Honeynet Project, Defining Virtual Honeynets, Know Your Enemy, last time modified: 27 January, 2003, URL: http://www.honeynet.org, last time visited on November 11, 2004
1) http://www.honeynet.org/papers/virtual/)
3) http://www.honeynet.org/misc/project.html
4) http://www.honeynet.org/alliance/

Roger A. Grimes, Distract intruders away from your legitimate resources, Honeypots for Windows, last time modified: April 2004, URL: http://www.winnetmag.com/Windows/Articles/ArticleID/41976/pg/1/1.html , last time visited on November 11, 2004

Honeynet Project. Know Your Enemy SE, Boston, MA 02116, May, 2004.

Security Focus, Open Source Honeypots: Learning with Honeyd, last time modified: January 20, 2003, URL: http://www.securityfocus.com/infocus/1659, last time visited on November 11, 2004

Honeyd - Provos Niels, Honeyd Research: Honeypots Against Spam, last time modified: December 5, 2003, http://www.honeyd.org/spam.php, last time visited on November 11, 2004

Oudot, Laurent, Fighting Spammers With Honeypots: Part 1, last updated November 26, 2003, http://www.securityfocus.com/infocus/1747, last time visited on November 11, 2004

Tracking hackers – FAQ, last time modified: 25 March, 2004, URL: http://www.tracking-hackers.com/misc/faq.html#faq6, last time visited on November 11, 2004

Spitzner, Lance, Honeypots: Tracking Hackers, Boston, MA 02116, December 2002.

Symantec, Symantec Decoy Server, last time modified: 2004, URL: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=157, last time visited on November 11, 2004

Clancy, Heather, Honeypots: Protecting Networks With Decoys That Lure Hackers last time modified: November 3, 2003, URL: http://computercops.biz/article3964.html, last time visited on November 11, 2004

Shinder , Littlejohn Debra and Tittel Ed, Implementing Cybercrime Detection Techniques Scene of the Cybercrime: Computer Forensics Handbook, Rockland, MA, Syngress Publishing, 2002