MULTI-FACETED RECONNAISSANCE – A HONEYPOT APPROACH

GIAC GSEC Practical (v1.4b)
Koon Foong LEONG, Vincent
9 September 2003

TABLE OF CONTENTS

Abstract

With the scourge of prevalent software vulnerabilities and the ever-increasing hacking activities, a dangerous Internet has evolved as the world becomes more connected. Sophisticated hacking techniques are on the rise and patching alone is a never ending catch-up game. This phenomenon has triggered a vital need to understand these types of attacks and the underlying methodologies used, so as to enhance detection capabilities and forensic expertise, which in turn help to build better and more secure software. There are various ways to hack and in each successful attempt, embeds unique exploit patterns. To fully dissect such patterns, honeypots are deployed in different environments, anticipating for that enlightening moment of information warfare. This paper provides insights to deploying multi-faceted Honeypots for pervasive information gathering and analysis, as well as its associated legal issues that may surface.

In this paper, we will discuss the types the honeypots, their roles, and the issues one needs to consider in deploying honeypots in different environments. As honeypots are usually deployed in tandem to a live system, we then take a closer look at the various components making up a honeypot as well as the ways to make the honeypots more attractive to the attackers. Finally, we will explore cross boundaries issues pertaining to the use of honeypots in this aspect.

1. Introduction

Perimeter defenses such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), are essential components but they are mostly reactive in nature, largely dependent on signature updates. To be connected to the Internet means there is at least one active service, waiting to be exploited. Firewalls can help control these open doors, react and perform according to specific sets of rules; however, firewalls and virtual private networks (VPNs) alone cannot prevent all intrusions and do little to prevent attacks from within the organization itself. IDS & IPS can share this load by operating in a different space; both help scrutinize data packets by signatures.

While an IDS behaves more like a burglar alarm, the IPS has an emergency door that can potentially disconnect an organization from the outside world when malicious signatures are detected, creating an inadvertent denial-of-service (DoS) to a business. By the time an IDS triggers the alarm, a successful attack could have taken place. As can be seen, a multi-layer approach kind of active defense is highly essential, and hence, a honeypot based solution may just be the magic bullet.

2. What's a HoneyPot?

When there is something alluring, it is only a matter of time before an inevitable attack occurs. A honeypot serves to capture this important role, acting as a decoy along side with critical services. According to the Honeynet Project website, a

Honeypot is defined as "*a resource with a variety of different uses and whose value lies in its unauthorized or illicit use*". [1] http://www.tracking-hackers.com and Book: Honeypots-Tracking Hackers, by Lance Spitzner

Just like bees are attracted to honey, a honeypot is technically a system that is put on a network with the intention of getting probed and attacked, in order to gain information on an attacker, (the malicious bees). This concept is a radically different approach to other forms of security and one that is increasingly being recognized to be highly effective in detecting security threats. By allowing intruders to interact with the honeypot, detailed information can be gathered on the techniques and tools that they use. Because there is no legitimate use for the honeypot, all connections it receives are suspicious. This results in very few false positive alerts.

On the contrary, a honeypot is useless if it is incapable of distracting adversaries or if malicious users do not attack or at least try to attack it. As honeypots are closely monitored network decoys deployed in tandem to valuable machines, they can provide early warnings about new attacks and exploitation trends and they allow in-depth examination of adversaries during and after exploitation. By itself, a honeypot resource has no real use, its value lines in the wealth of information gathered. If someone connects to it, that user is highly considered a malicious one and ought to be investigated.

3. Types of Honeypots

A honeypot in its most basic form is like a 'published' decoy, running an operating system without patches installed and using typical defaults and options. It contains no physical data, but running an application that is designed to record all activities of the invader. This type of honeypot is not going to be very useful. While it may attract the script kiddies, the intelligent hacker may not be easily fooled, given the idea of an empty, unpatched virgin box.

Since maintaining a honeypot requires a considerable amount of attention, the highest value that it can offer is nothing more than a learning experience, and hence, the decoy has got to be as close to the real thing as possible. Currently, not much research is being done with old vulnerabilities which may trigger a zero-day avalanche on the Internet. While most honeypots are idle almost all the time, some are kept patched in hopes to capture this significant moment.

There basically two main types of Honeypots:

(a) Research Honeypots
(b) Production Honeypots

Research Honeypots

One of the biggest issues we facing today is that we do not know who these attackers are. The techniques, tools and methods employed by these attackers. Without this knowledge is equivalent to having an IDS without signatures, our defenses is only as strong as its weakest link, and we are literally exposing ourselves to such external threats from the Internet. This is where Research Honeypots can provide some answers to the these questions.

Research Honeypot has only two purposes:

- To research on the attackers.
  - Who are these folks?
  - What do they want?
  - Study their methods and techniques.
  - Capture their tools, exploits used, as well as keystrokes and conversations.
  - Do they work alone?

- To assess general trend in the security industry.
  - Why do they attack?
  - Are there any hidden conspiracies?
  - Can we predict the next possible attack?
  - Is there an underground storm, and D-days breeding somewhere?

For years, the security community has difficulties in providing good answers to this question besides providing prophecies. Though, research honeypots can provide us the platform to study an attack in real-time or a threat in detailed, it must be noted that such honeypots do not provide added security to existing infrastructure; as the name suggests, it is purely used for research purpose only.

Deploying Research Honeypots

Let’s take a closer look at some of the issues with deploying Research Honeypots.

Not only does research honeypot not provide any added security value, its deployment on the contrary, introduces vulnerabilities into your existing network, creating a new level of security risk. While it is inevitable for a honeypot to be attacked for it to be successful, a typical research honeypot will have certain ports open, sprinkled with a few doses of *vulnerable services* running as baits, and not all hell breaks loose. Thus, if someone successfully penetrates the research honeypot, there is a possibility that your network might actually get compromised as well.

More importantly, research honeypots are complex to deploy and maintain, as they capture extensive information, and are used primarily by research, military, or government organizations, and hence, security risk must be taken into account in such experiments.

Production Honeypots

Apart from the complexity of research honeypots, production honeypots are relatively easy to use, as they capture only limited information, and are used primarily by companies or corporations to enhance their defenses against external attacks.

Production honeypots form an active part of your network defenses, usually deployed in tandem to production machines, and they serve the following purposes:

- Actively tricks the attacker into attacking the Honeypot system instead of the actual systems, and hence, any traffic going to the honeypot is 99% of times malicious. If the attacker discovered that he has been switched, he is likely to go away which then creates a natural win as defenders.

- Helps in Detection of Attacks
  - Reduces False Positives
  - Reduces False Negatives as it detects almost all attacks.
  - Monitors and captures attacks in Real-time
  - Offers comprehensive Logging
  - Works with Encryption and Ipv6 Environments.

- Helps in Computer Forensics because:
  - Evidence is NOT tampered.
  - Honeypot can immediately be disconnected, as soon as sufficient data is gathered.

- Less risky than Research Honeypots.

4. Deployment Considerations for Honeypots

On the basis of implementing Honeypots, they can be categorized into two levels [reference: Lance Spitzner, “Honeypots-Definition and Values”, 29 May 2003, URL: http://www.tracking-hackers.com/papers/honeypots.html]:

(a) Low-Involved Honeypots
(b) High-Involved Honeypots

Low-Involved Honeypots

A typical Low-Involved Honeypot is one that is relatively patched and comes with a few open ports which the attackers are likely to connect, and hence, the security administrator knows exactly what ports to monitor; however, the attacker will NOT be allowed to do anything else such as launching an external attack on this type of honeypot.

Due to tight security configurations on a Low-Involved honeypot, less data will be captured as it does not allow much malicious activities to be performed. Though, this may not give us much insight into the attacker, it is able to divert an otherwise harmful or DDoS type of attacks against critical services. Therefore, a Low-Involved honeypot are usually deployed as Production Honeypots because they are less resource intensive and are also relatively less risky.

High-Involved Honeypots

A High-Involved Honeypot, on the contrary, has a few ports open, plus a few vulnerable services running, and hence, the attacker is enticed to execute more malicious activities after a successful compromise on such a honeypot. With the existence of vulnerable services, High-Involved honeypots are relatively very risky as the attacker can potentially do anything he wants on such honeypots.

As more harm can be done, more data can be captured, and hence, such deployment is considered to be extremely resource hungry as it is likely to involve a team of forensic experts just for data analysis purposes. Such honeypots are typically deployed as Research Honeypots as they help gather more essential information on the tools, techniques and methods used by the attacker, besides tracing the attacker.

5. Pros and Cons of Honeypots

Another fundamental aspect of honeypot is that it provides comprehensive logging facility. A honeypot is not only capable of capturing malicious activities in real-time, the information gathered provides significant insights on the attack.

It provides centralized logging and does it more efficiently than an IDS, which might drop a few lines in the event of high activity and bandwidth. Honeypot also works well with encryption and in IPv6 environment.

Though substantial effort is needed to make a honeypot attractive, if it is not appealing enough and no one attacks the honeypot, it is practically useless. While having a honeypot helps divert malicious traffic to it, it can also introduce varied amounts of risk to the overall security of the network involved.

Thus, for a Honeypot to be considered successful, a malicious user must attack it and the overall security risk introduced must not be too high.

Profiling the Attackers

Once a honeypot is compromised, the attacker has been successfully fooled and is likely to set up a shop on the compromised box. What is interesting to us is this 'shop'. Most compromised boxes are used for hosting W4R3Z, spam, and DDOS clients. If the attacker installs an FTP (File Transfer Protocol) server and starts uploading 'warez', we can assume that he is relatively harmless, however, if the attacker immediately goes for a fake credit card database, we may have a problem to worry about as this may offer some clues on a brewing syndicate.

6. Some Popular Honeypots

Honeypots	Resource Measure	Emulations	Traps & Services	Platform
NFR's ***BackOfficer Friendly (BOF)***	Low	FTP, Telnet, HTTP, SMTP, POP3, IMAP.	▪ FTP, Telnet, HTTP, SMTP, POP3, IMAP. ▪ Records scans, probes etc.	▪ Windows based, *Freeware* ▪ Unix *Commercial*

NetSec's ***Specter***	Low	Different OSes (Windows 95/98/NT, MacOS, Linux SunOS / Solaris Digital Unix NeXTStep, Irix Unisys Unix)	▪ DNS, IMAP4, SUN-RPC, SSH, SUB-7,BOK2, Generic. ▪ FTP, Telnet, HTTP, SMTP, Finger, POP3, Netbus.	Windows based *Commercial*
HoneyD **&** **HoneyD Windows**	Low	Run arbitrary services, and adapted to spoof certain OSes.	▪ Creates virtual hosts on a network. ▪ Enables a single host to claim multiple addresses	▪ Open Source ▪ Windows based *Freeware*
Symantec's ***ManTrap***	High	Enables stealth monitoring and containment plus live attack analysis	▪ Effective attack detection and deterrence for critical networks via advanced decoy technology ▪ centralized management, policy-based response, and comprehensive reporting and trend analyses for enterprise environments	▪ Windows based ▪ Solaris *Commercial*
Bait and Switch	High	▪ Multifaceted honeypot for active system defense. ▪ Redirects and switch hostile traffic.	▪ Effective system based on snort, linux's iproute2, netfilter, and custom code.	Unix *Commercial &* *Freeware*

[2], [reference: http://www.networkintrusion.co.uk/honeypots.htm]

7. Concepts of HoneyNets

Honeynets

We have so far touched on the types of Honeypots and some of the resource considerations in deploying them. When many honeypots are being deployed, whether in a research environment, or to enhance defenses in critical production systems, a network of honeypots, known as a *Honeynet* [5] is created.

Like its individual honeypot, a Honeynet is a network consisting of computers which have been setup with the sole intention of being attacked. Thus, it involves multiple honeypots serving different purposes, running simultaneously, to simulate a real world production network, and hence, a honeynet is rather resource intensive and is usually used for research study. We can term it as a massive decoy if we want.

Typically, a honeynet involved a collection of High-Involved honeypots deployed in synergy to gather information about the attacker. Within such a honeynet network, real computers with real applications are setup, to entice attackers. All activities are recorded by these collective research honeypots.

So how do different honeypots interact within a honeynet? This can be easily configured through firewall rules updates to redirect the malicious traffic when certain poison files or port are touched. Resultant actions may inform critical services to ignore attacker and perform a rate-limiting on the respective service connections.

A good example of such honeypot is the *Bait and Switch* active defense system. [Source: http://violating.us/projects/baitnswitch/, website].With the help of an IDS, triggering a malicious signature will switch the attacker to one of the honeypots, which can be a mirror of a production server, having the same IP and MAC address. Certain amount of efforts is required to fool the attacker into believing that he is still on the production box. This leads us to the next concept of Honey-Tokens.

8. What are Honey-Tokens?

Honey-Tokens

As the name implies, Honey-tokens [6] simply means the baits that are used to lure would be attackers or the real black-hats. If honey is to bees, then the nectar is to the tokens. Just as a honeypot having no value by itself besides awaiting a successful compromise, honey-tokens are the mechanisms present on a honeypot to facilitate such an attack. They have created a new dimension for honeypots, especially for the insider threats.

These tokens can exist in many forms, from vulnerable open ports and services, to every little application such as a spreadsheet, a database entry, or even a bogus login prompt, running on a honeypot. This may also include pieces of data such as credit card details, email addresses, password files, and false business data [3]. Besides being attractive, they are cost effective, simple to deploy, and highly effective.

In short, honey-tokens are everything a honeypot is, except they are not a computer. The point to note is that no one should be accessing or interacting with these tokens, unless they have ill intentions.

9. Legal Issues Concerning Honeypots

While honeypots offers a whole new dimension to information gathering, it raises the basic question as to whether such data collected are admissible in court. Since a honeypot is not a real system and contains no real data, are we then allowed to sue the attacker for an unauthorized intrusion and subsequently claim damages? Or will we be sued for having those entrapments?

With such diverse international laws in different countries, which may even include privacy acts and other related legislations; the existence of honeypots may surface inherent complex legal issues ahead. Though, we can challenge the notion that entrapment is a form of active defense and should not be considered as an offense, however, we may have a hard time arguing our case on such honeypots deployment. Interestingly, there is hardly anybody prosecuting on the basis of such entrapments. Most importantly, some efforts have to be coming from the law enforcement angle or the government side of things, otherwise, it may all just end up in a honeypot with teeth but could not bite.

The most worrisome and yet the trickiest issue is concerning privacy. Some countries, such as the United States has the ECPA (Electronic Communications Privacy Act) [4], which creates some contradictions with regards to unauthorized interception of electronic communications. This may apply to personal information being captured on honeypots. The worst is yet to come which is about captured conversations among multiple parties such as chat-rooms hosted on a honeypot. Thus, it can be a tough tussle if we venture into lots of legal issues regarding privacy. Unfortunately, there are currently no laws regarding prohibiting honeypots.

In Singapore's context, there is no privacy law per se but there is an established Model Data Protection Code to ensure that all consumer data are handled strictly in accordance to the stipulated guidelines in the Code for all electronic transactions over the Internet.

10. Conclusion

Honeypots have evolved to become a highly flexible security tool deploy in tandem with critical systems as well as for research purposes. As a security resource whose value lies in being probed, attacked, or compromised, they can offer a wealth of information essential for detailed forensic analysis and prediction of trends.

We have also seen the two different types of honeypots: Research and Production honeypots, their differences, as well as their level of involvement which may call for additional overheads and resource constrains.

While there will always be legal issues to be sorted out with regards to privacy violations, honeypots can still serve as an agent for active defense, which will likely to find their deployment into research facilities, the military, and government organizations.

Finally, with the growth of honeypots around the world, we can tap each other like storm centers, on the collective effort to create the largest surveillance system ever to keep a sharp eye on malicious Internet activities, and with the ability to better managed security vulnerabilities, to provide for a more integrated global security management.

References:

- [1] Lance Spitzner, “Honeypots: Tracking Hackers”, Addison-Wesley Pub Co, September 2002, ISBN: 0321108957

- [2] Lance Spitzner, “Know Your Enemy: Revealing the Security Tools, Tactics, and Motives of the Blackhat Community”, Addison-Wesley Pub Co, August 2001, ISBN: 0201746131

- [3] Kevin D. Mitnick and William L. Simon, “The Art of Deception: Controlling the Human Element of Security”, John Wiley & Sons, October 2002, ISBN: 0471237124

- [4] Title 18. Crimes And Criminal Procedure, Part I – Crimes Chapter 119--Wire and Electronic Communications Interception and Interception of Oral Communications
  (a) http://cio.doe.gov/Documents/ECPA.HTM,
  (b) http://www.cybercrime.gov/usc2701.htm
  (c)http://www.cybercrime.gov/usc2511.htm
  (d) http://floridalawfirm.com/privacy.html]

- [5] Lance Spitzner, “Honeypot Farm”, 13 August 2003, URL: http://www.securityfocus.com/infocus/1720

- [6] Lance Spitzner, “Honeytokens: The Other Honeypot”, 21 July 2003, URL: http://www.securityfocus.com/infocus/1713

- Lance Spitzner, “Honeypots: Are They Illegal?”, 12June 2003, URL: http://www.securityfocus.com/infocus/1703

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

- Lance Spitzner, Specter: A Commercial Honeypot Solution for Windows”, 8 April 2003, URL: http://www.securityfocus.com/infocus/1683

- Lance Spitzner, “Open Source Honeypots, Part Two: Deploying Honeyd in the Wild“, 12 March 2003, URL: http://www.securityfocus.com/infocus/1675

- Lance Spitzner, “Open Source Honeypots: Learning with Honeyd”, 20 January 2003, URL: http://www.securityfocus.com/infocus/1659

- Lance Spitzner, “The Value of Honeypots, Part Two: Honeypot Solutions and Legal Issues”, 10 October 2001, URL: http://www.securityfocus.com/infocus/1498

- Lance Spitzner, “The Value of Honeypots, Part One: Definitions and Values of Honeypots, 10 October 2001, URL: http://www.securityfocus.com/infocus/1492

- Lance Spitzner, “Know Your Enemy: A Forensic Analysis”, 23 May 2000, URL: http://www.securityfocus.com/infocus/1255
- Lance Spitzner, “Passive Fingerprinting”, 3 May 2000, URL: http://www.securityfocus.com/infocus/1224
- Kevin Poulsen, “Use a Honeypot, Go to Prison?”, 16 April 2003, URL: http://www.securityfocus.com/news/4004
- Official Honeynet Research project website, URL: http://www.honeynet.org/
- Network Honeypots, URL: http://www.networkintrusion.co.uk/honeypots.htm
- http://project.honeynet.org/
- http://www.honeypots.net/
- “Hackers caught in security honeypot”, URL: http://zdnet.com.com/2100-11-526520.html?legacy=zdnn
- “Building a Honeypot”, URL: http://rootprompt.org/article.php3?article=210
- “Honeypot for spam harvesters”, URL:http://www.kungfugrippe.com/previously/002462.php
- http://sourceforge.net/projects/single-honeypot
- http://violating.us/projects/baitnswitch/