International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 5 Issue: 2
ISSN: 2454-4248
48 – 51

A Study on Honeypot Technology for Future: Principles and Applications

Manish Mathur[1], Naresh Mathur[2]
Assistant Professor, CSE
Shekhawati Institute of Engineering and Technoloy, Sikar
ermanishmathur@gmail.com,nareshmathurer@gmail.com

Abstract-Honeypot is an exciting new technology with enormous potential for the security community. It isresource which is intended to be attacked and compromised to gain more information about theattacker and his attack techniques.

They are a highly flexible tool that comes in many shapes andsizes. This paper deals withunderstanding what a honeypot actually is, and how it works.Thereare different varieties of honeypots. Based on their category they have different applications. Thispaper gives an insightinto the use of honeypots in productive as well as educative environments.This paper alsodiscusses the advantages and disadvantages of honeypots, and what the futurehold in store forthem.

Keywords:*Honeyypot, Honeyd, Honeynet, firewall*

*****

I. INTRODUCTION

The Internet is growing fast and doubling its number of websites every 53 days and the numberof people using the internet is also growing. Hence, global communication is getting moreimportant every day. At the same time, computer crimes are also increasing. Countermeasuresare developed to detect or prevent attacks - most of these measures are based on known facts,known attack patterns. Countermeasures such as firewalls and network intrusion detectionsystems are based on prevention, detection and reaction mechanism; but is there enoughinformation about the enemy?

As in the military, it is important to know, who the enemy is, whatkind of strategy he uses, what tools he utilizes and what he is aiming for. Gathering this kind ofinformation is not easy but important. By knowing attack strategies, countermeasure scan beimproved and vulnerabilities can be fixed. To gather as much information as possible is one maingoal of a honeypot. Generally, such information gathering should be done silently, withoutalarming an attacker. All the gathered information leads to an advantage on the defending sideand can therefore be used on productive systems to prevent attacks.

A honeypot is primarily aninstrument for information gathering and learning. Its primary purpose is not to be an ambush forthe blackhat community to catch them in action and to press charges against them. The focus lieson a silent collection of as much information as possible about their attack patterns, usedprograms, purpose of attack and the blackhat community itself. All this information is used tolearn more about the blackhat proceedings and motives, as well as their technical knowledge andabilities. This is just a primary purpose of a honeypot. There are a lot of other possibilities for ahoneypot - divert hackers from productive systems or catch a hacker while conducting an attackare just two possible examples. They are not the perfect solution for solving or preventingcomputer crimes.

Honeypots are hard to maintain and they need operators with good knowledgeabout operating systems and network security. In the right hands, a honeypot can be an effectivetool for information gathering. In the wrong, unexperienced hands, a honeypot can becomeanother infiltrated machine and an instrument for the blackhat community.

A honeypot is aninformation system resource whose value lies in unauthorized or illicit use of that resource.

II. TYPES OF HONEYPOTS

Honeypots come in many shapes and sizes, making them difficult to get a grasp of. To better understand honeypots and all the different types, they are broken down into two generalcategories, low-interaction and high-interaction honeypots. These categories helps to understandwhat type of honeypot one is dealing with, its strengths, and weaknesses. Interaction defines thelevel of activity a honeypot allows an attacker.

2.1 LOW-INTERACTION HONEYPOTShave limitedinteraction; they normally work by emulating services and operating systems. Attacker activity is limited to the level of emulation by the honeypot. For example, an emulated FTP service listening on port 21 may just emulate a FTP login, or it may support a variety of additional FTP commands. The advantage of a low-interaction honeypot is their simplicity. These honeypots tend to be easier to deploy and maintain, with minimal risk. Usually they involve installing software, selecting the operating systems and

 ISSN: 2454-4248
48 – 51

services you want to emulate and monitor, and letting the honeypot go from there. This plug and play approach makes deploying them very easy for most organizations. Also, the emulated services mitigate risk by containing the attacker's activity, the attacker never has access to an operating system to attack or harm others. The main disadvantages with low interaction honeypots is that they log only limited information and are designed to capture known activity.The emulated services can only do so much. Also, its easier for an attacker to detect a low-nteraction honeypot, no matter how good the emulation is, skilledattacker can eventually detecttheir presence. Examples of low-interaction honeypots includeSpecter, Honeyd, and KFSensor.

2.2 HIGH-INTERACTION HONEYPOTS are different; they are usually complex solutions as they involve real operating systems and applications. Nothing is emulated; the attackers are given the real thing. If one wants a Linux honeypot running an FTP server, they build a real Linux system running a real FTP server. The advantages with such a solution are twofold. First, extensive amounts of information are captured. By giving attackers real systems to interact with, one can learn the full extent of the attackers behavior, everything from new rootkits to international IRC sessions. The second advantage is high-interaction honeypots make no assumptions on how an attacker will behave. Instead, they provide an open environment that captures all activity. This allows high-interaction solutions to learn behavior one otherwise would not expect. An excellent example of this is how a Honeynet captured encoded back doorcommands on a non-standard IP protocol . However, this also increases the risk of the honeypotas attackers can use these real operating system to attack non-honeypot systems. As result, additional technologies have to be implemented that prevent the attacker from harming other non-honeypot systems. In general, high-interaction honeypots can do everything low-interactionhoneypots can do and much more. However, they can be more complex to deploy and maintain.Examples of high-interaction honeypots include Symantec
A few examples of honeypots and theirvarieties are:

BACKOFFICER FRIENDLY

BOF (as it is commonly called) is a very simple but highlyuseful honeypot developed by Marcus Ranum and crew at NFR. It is an excellent example of alow interaction honeypot.

It is a great way to introduce a beginner to the concepts and value ofhoneypots. BOF is a program that runs on most Windows based operating system. All it can do is emulate some basic services, such as http, ftp, telnet, mail, or BackOffice. Whenever some attempts to connect to one of the ports BOF is listening to, it will then log the attempt. BOF also has the option of "faking replies", which gives the attacker something to connect to. This way one can log http attacks, telnet brute force logins, or a variety of other activity (Screenshot). The value in BOF is in detection, similar to a burglar alarm. It can monitor only a limited number ofports, but these ports often represent the most commonly scanned and targeted services.

SPECTER

Specter is a commercial product and it is another 'low interaction' production honeypot. It issimilar to BOF in that it emulates services, but it can emulate a far greater range of services and functionality. In addition, not only can it emulate services, but emulate a variety of operating systems. Similar to BOF, it is easy to implement and low risk. Specter works by installing on a Windows system. The risk is reduced as there is no real operating system for the attacker to interact with.

One of the unique features of Specter is that it also allows for information gathering, or the automated ability to gather more information about the attacker. Some of this information gathering is relatively passive, such as Whois or DNSlookups. However, some of this research is active, such as port scanning the attacker.

HONEYD

Created by NielsProvos, Honeyd is anextremely powerful, OpenSource honeypot. Designed to run on Unix systems, it can emulate over 400 different operating systems and thousands of different computers, all at the same time. Honeyd introduces some exciting new features. First, not only does it emulate operating systems at the application level, like Specter, but it also emulates operating systems at the IP stack level. This means when someone Nmaps the honeypot, both the service and IP stack behave as the emulated operating system. Currently no other honeypot has this capability (CyberCop Sting did have this capability, but is no longer available). Second, Honeyd can emulate hundreds if not thousands of different computers all at the same time. While most honeypots can only emulate one computer at any point in time, Honeyd can assume the identity of thousands of different IP addresses.

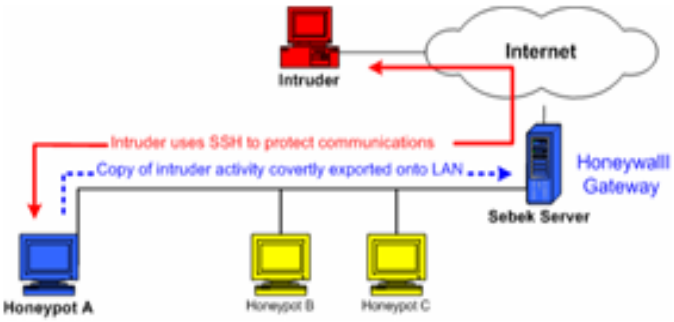

Figure 2.1 Architecture of Honeyd

 ISSN: 2454-4248
48 – 51

Honeyd is primarily used for detecting attacks. It works by monitoring IP addresses that are unused, that have no system assigned to them. Whenever an attacker attempts to probe or attack annon-existent system.

HONEYNETS

Honeynets represent the extreme ofresearch honeypots. They are high interaction honeypots, one can learn a great deal, howeverthey also have the highest level of risk.

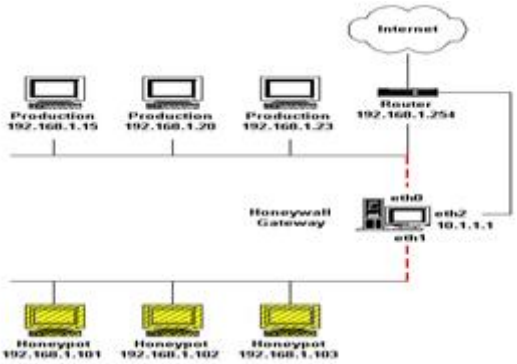

Figure 2.2 Architecture of Honeynet

This gives the attacker the flexibility to interact with the victim systems, but prevents the attacker from harming other non-Honeynet computers. Honeynets are primarily research honeypots. They could be used as production honeypots, specifically for detection or reaction, however it is most likely not worth the time and effortWe have reviewed six different types of honeypots. No one honeypot is better than the other, each one has its advantages and disadvantages, it all depends on what is to be achieved. For example, BOF and Specter represent low interactions honeypots. They are easy to deploy and have minimal risk. However, they are limited to emulating specific services and operating systems, used primarily for detection. Mantrap and Honeynets represent mid-to-high interaction honeypots. They can give far greater depth of information,however more work andgreater risk is involved.

Sometimes, honeypots are also classified as Hardware based andSoftware based honeypots.Hardware-based honeypots are servers, switches or routers that have been partially disabled and made attractive with commonly known misconfigurations. They sit on the internal network, serving no purpose but to look real to outsiders. The operating system of each box, however, has been subtly disabled with tweaks that prevent hackers from really takingit over or using it to launch new attacks on other servers.Even if the hacker figures out that it's a software honeypot, the box on which it's running should be so secure or isolated that he couldn't do anything but leave anyway. Software emulation might be more useful for corporate environments wherebusiness secrets are being safeguarded.

III. HOW DOES A HONEYPOT GATHER INFORMATION

Obviously a honeypot must capturedata in an area that is not accessible to anattacker. Data capture happens on a number of levels.

Firewall Logs-A Packet Sniffer (or similar IDS sensor). The IDS should be configured topassively monitor network traffic (for an added level of invisibility, one might set the system up to have no IP address or, in some instances, the sniffer could be configured to completely lack an IP stack). This will capture allclear text communication, and can read keystrokes.

Local and Remote Logs-These should be set up just as it would on any other system, and will possibly be disabled, deleted, or modified by an experienced hacker, but plenty of useful information will still be available from all theprevious capture methods.

Remotely Forwarded Logs-Will capture data on a remote log and then instantly forward the data to a system even further out of the range of the attacker, so that theattacker cannot be warned that all his activities are watched or try to modify the captured data.

IV. MERITS AND DEMERITS

4.1 MERITS

Honeypots have a large number of merits in its favour. They are :

- **Small data sets of high value:** Honeypots collect small amounts of information. Instead of logging a one GB of data a day, they can log only one MB of data a day. Instead of generating 10,000 alerts a day, theycan generate only 10 alerts a day.
- **Minimal resources:** Honeypots require minimal resources, they only capture bad activity. This means an old Pentium computerwith 128MB of RAM can easily handle an entire class B network sitting off an OC-12 network.
- **Encryption or IPv6:** Unlike most security technologies (such as IDS systems) honeypotswork fine in encrypted or IPv6 environments. It does not matter what the bad guys throw at ahoneypot, the honeypot will detect and capture it.
- **Simplicty:** Finally, honeypots are conceptually very simple. There are no fancy algorithms to develop, state tables to maintain, or signatures to update. The simpler a technology, the less likely there will be mistakesor misconfigurations.

 ISSN: 2454-4248
48 – 51

4.2 DEMERITS

Like any technology, honeyopts also have their weaknesses. It is because of this they do not replace any current technology, but work with existing technologies.

- **Limited view:** Honeypots can only track and capture activity that directly interacts with them. Honeypots willnot capture attacks against other systems, unless the attacker or threat interacts with thehoneypots also.
- **Risk:** All security technologies have risk. Firewalls have risk of being penetrated, encryption has the risk of being broken, IDS sensors have the risk of failing to detect attacks.
- honeypots are most likely not a form of entrapment as you are not coercing them into breaking into the honeypot. The bad guy has already decided to commitunauthorized activity, one is merely providing a different target for the blackhat to attack.Therefore, in most cases involving honeypots, entrapment is not an issue.

V. FUTURE OF HONEYPOTS

Mr. Lance spitzner who has played a major role in the development of honeypots has made certain predictions about the future of honeypots. They are as follows:

- **Government Projects:** Currently honeypots are mainly used by organizations, to detect intruders within the organization as well as against external threats and to protect theorganization. In future, honeypots will play a major role in the government projects, especiallyby the military, to gain information about the enemy, and those trying to get the governmentsecrets.
- **Ease of Use:** In future honeypots will most probably appear in prepackaged solutions, which will be easier to administer and maintain. People will be able to install and develophoneypots at home and without difficulty.
- **Closer Integration:** Currently honeypots are used along with other technologies such as firewall, tripwire, IDS etc. As technologies are developing,in future honeypots will be used in closer integration with them. For example honeypots are being developed for WI-FI or wireless computers. However the development is still underresearch.

VI. CONCLUSION

A honeypot is just a tool. How one uses this tool is uptothem.Honeypotsare in their infancy and new ideas and technologies will surface in the next time. At the sametime as honeypots are getting more advanced, hackers will also develop methods to detect suchsystems. A regular arms race could start between the good guys and theblackhat community.

Let`s hope that such a technology will be used to restore the peace and prosperity of the worldand not to give the world a devastating end.

VII. REFERENCES

[1]. Spitzner, Lance.“Honeypots Tracking Hackers”. Addison-Wesley: Boston,2002
[2]. Spitzner,Lance. “The value of Honeypots, Part Two:Honeypot Solutions and legal Issues” 10Nov.2002
[3]. Spitzner, Lance.“Know Your Enemy:Honeynets”. 18 Sep. 2002.
[4]. www.honeypots.net
[5]. www.honeynet.org