iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** IV **Month of publication:** April 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

An Approach for Intrusion Detection using HoneyPots to Improve Network Security

Mohd. Junedul Haque
College of Computers and Information Technology, Taif University, KSA

Abstract— For every consumer and business that is on the Internet, viruses, worms and crackers are a few security threats. There are the obvious tools that aid information security professionals against these problems such as anti-virus software, firewalls and intrusion detection systems, but these systems can only react to or prevent attacks-they cannot give us information about the attacker, the tools used or even the methods employed. Given all of these security questions, honeypots are a novel approach to network security and security research alike [1]. Honeypot is a well designed system that attracts hackers into it. By luring the hacker into the system, it is possible to monitor the processes that are started and running on the system by hacker. In other words, honeypot is a trap machine which looks like a real system in order to attract the attacker. The aim of the honeypot is analyzing, understanding, watching and tracking hacker's behaviours in order to create more secure systems. Honeypot is great way to improve network security administrators' knowledge and learn how to get information from a victim system using forensic tools. Honeypot is also very useful for future threats to keep track of new technology attacks.

Keywords—Firewalls, Honeypots, Intrusion detection systems, network.

I. INTRODUCTION

Global communication is getting more important every day. At the same time, computer crimes are increasing. Countermeasures are developed to detect or prevent attacks - most of these measures are based on known facts, known attack patterns. As in the military, it is important to know, who your enemy is, what kind of strategy he uses what tools he utilizes and what he is aiming for. Gathering this kind of information is not easy but important. By knowing attack strategies, countermeasures can be improved and vulnerabilities can be fixed. To gather as much information as possible is one main goal of a honeypot. Generally, such information gathering should be done silently, without alarming an attacker. All the gathered information leads to an advantage on the defending side and can therefore be used on productive systems to prevent attacks [1].

II. DEFINITION OF HONEYPOT

"A honeypot is security resource whose value lies in being probed, attacked, or compromised". A honeypot is a system that is built and set up in order to be hacked. Honeypot can be used in different scenario as intrusion detection facility (burglar alarm), defense or response mechanism. Moreover, Honeypot can be deployed in order to consume the resources of the attacker or distract him from the valuable targets and slow him down that wastes his time on the honeypot instead of attacking production systems. The main functions of a honeypot are :

A. to divert the attention of the attacker from the real network, in a way that the main information resources are not compromised.
B. to capture new viruses or worms for future study.
C. to build attacker profiles in order to identify their preferred attack methods, similar to criminal profiles used by law enforcement agencies in order to identify a criminal's modus operandi.
D. to identify new vulnerabilities and risks of various operating systems, environments and programs which are not thoroughly identified at the moment.

III. LEVEL INTERACTION OF HONEYPOT

The level of interaction is defined as the range of attack ossibilities that a honeypot allow an attacker to have, where as it can be classified as high- interaction honeypot and low interaction honeypot [2]. Interaction measures the amount of ctivity that an intruder may have with honeypot. In addition, honeypots can be used to combat spam. Spammers are constantly searching for sites with vulnerable open relays to forward spam on the other networks. Honeypots can be set up as open proxies or relays to allow spammers to use their sites .This in turn allows for identification of spammers.

©IJRASET 2015: All Rights are Reserved

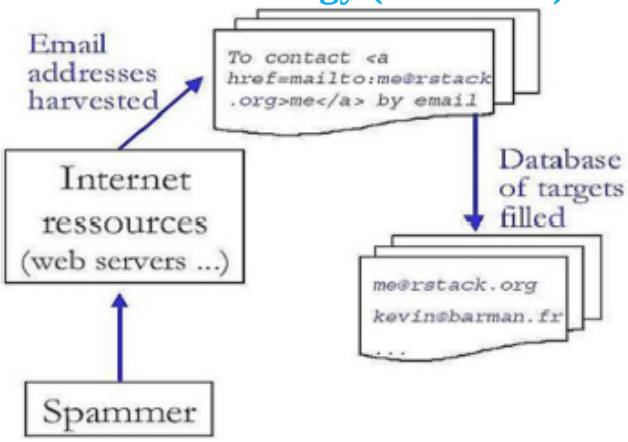


Figure 1: level interaction of honeypots

We will break honeypots into two broad categories, as defined by Snort ,two types of honeypots are:

Production honeypots

Research honeypots

The purpose of a production honeypot is to help mitigate risk in an organization. The honeypot adds value to the security measures of an organization. Think of them as 'law enforcement', their job is to detect and deal with bad guys. Traditionally, commercial organizations use production honeypots to help protect their networks. The second category, research, is honeypots designed to gain information on the black hat community. These honeypots do not add direct value to a specific organization. Instead they are used to research the threats organizations face, and how to better protect against those threats.

A. High- Interaction Honeypot

In high- interaction honeypot, attacker interaction with real operating systems, services and programs and it can be used to observe the attackers behavior, their tools, motivation and explored vulnerabilities. This kind of honeypot must have a robust containment mechanism in order to prevent, once compromised, its use to attack other networks. One goal of a hacker is to gain root and to have access to a machine, which is connected to the internet 24/7. A high- interaction honeypot does offer such an environment. To facilitate the deployment of installed inside virtual machineusing virtualization software such as VMware, Qemu and Xen. Using virtualization software, the attacker may run specialized code to detect that his code is running inside a virtual machine environment or perform timing attacks to identify honeypots. And performance of applications running in the guest operating system is reduced. However, an effort is made in the architecture to reduce the load of high-interaction honeypots by preprocessing the traffic using low-interaction honeypots as much as possible. Example of high-interaction honeypot is honeynet.A honeynet is a network of multiple systems. Honeynet can collect in-depth information about attackers, such as their keystrokes when they compromise a system, their chat sessions with fellow black hats, or the tools they use to probe and exploit vulnerable systems. This data can provide incredible insight on the attacker themselves. The advantage with honeynet is that they collect information based on the attackers' actions in the wild [3].

B. Low-Interaction Honeypot

On low- interaction honeypot, there is no operating system hat an attacker can operate on. Tools are installed in order to emulate operating systems and services. And they interact with the attackers and malicious code. This will minimize the risk significantly. This kind of honeypot has a small chance of eing compromised. It is production honeypot. Typical use of low-interaction honeypot includes; port scans identification, generation of attack signatures, trend analysis and malware collection. On the other hand, this is also a disadvantage. It is not possible to watch an attacker interacting with the operating system, which could be really interacting. Example of low interaction honeypot is honeyd. Honeyd is an open source low-interactivity honeypot system that creates virtual hosts that can be configured to run arbitrary services and their personality can be adapted so that they appear to be running certain operating systems. Honeyd , enables a single host to claim multiple

©IJRASET 2015: All Rights are Reserved

Volume 3 Issue IV, April 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

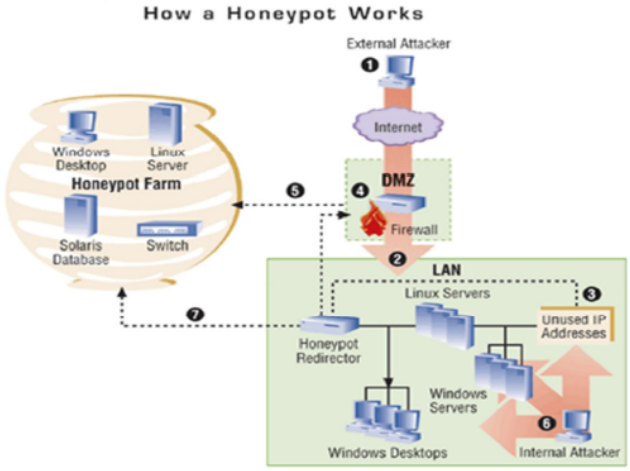


Figure 2: how a honey pot works

addresses. Honeyd improves cyber security by providing mechanism for threat detection and assessment. It also deters adversaries by hiding systems in the middle of virtual systems. It is possible to ping the virtual machines or to trace out them. Any type of service on the virtual machine can be simulated according to a simple configuration file. Instead of simulating service, it is also possible to proxy it to another machine.A complete picture of how honeypot work is shown in following [3].

C. Comparison between low- interaction honeypot and high interaction honeypot

	Low-interaction honeypot	High-interaction honeypot
Degree of Involvement	Low	High
Real Operating System	No	Yes
Risk	Low	High
Compromise Wished	No	Yes
Knowledge to Run	Low	High

Table 1: Summarizes of Low and High-Interaction Honeypot

IV. BUILDING A HONEYPOT

To build a honeypot, a set of Virtual Machines are created. They are then setup on a private network with the host operating system. To facilitate data control, a stateful firewall such as IP Tables can be used to log connections. This firewall would typically be configured in Layer 2 bridging mode, rendering it transparent to the attacker. The final step is data capture, for which tools such as Sebek and Term Log can be used. Once data has been captured, analysis on the data can be performed using tools such as Honey Inspector, PrivMsg and SleuthKit. Honeypot technology under development will eventually allow for a large scale honeypot deployment that redirects suspected attack traffic to honeypot. In the figure an external attacker:

A. Penetrates DMZ and scans the network IP address.
B. The redirection appliance.
C. Monitors all unused addresses, and uses Layer 2 VPN technology to enable firewall.
D. To redirect the intruder to honeypot.
E. Which may have honeypot computers mirroring all types of real network devices.
F. Scanning the network for vulnerable systems is redirected.
G. By the honeypot appliance when he probes unused IP addresses.

©IJRASET 2015: All Rights are Reserved

V. ADVANTAGES OF HONEYPOTS

A. They collect small amounts of information that have great value. This captured information provides an in-depth look at attacks that very few other technologies offer.
B. Honeypots are designed to capture any activity and can work in encrypted networks.
C. They can lure the intruders very easily.
D. Honeypots are relatively simple to create and maintain.

VI. DISADVANTAGES OF HONEYPOTS

A. Honeypots add complexity to the network. Increased complexity may lead to increased exposure to exploitation.
B. Here is also a level of risk to consider, since a honeypot may be comprised and used as a platform to attack another network. However this risk can be mitigated by controlling the level of interaction that attackers have with the honeypot.
C. It is an expensive resource for some corporations. Since building honeypots requires that you have at least a whole system dedicated to it and this may be expensive [5].

VII. LEGAL ISSUES PERTAINING HONEYPOTS

Most of the research found in this area concluded that there are three major legal spectrums concerning honeypots:

A. Entrapment

Entrapment is when somebody induces the criminal to do something he was not otherwise supposed to do.Honeypots should generally be used as defensive detection tools, not an offensive approach to luring intruders.

B. Privacy

The second major concern is what information is being tracked: operational data and transactional data. Operational data includes things like addresses of user, header information etc while transactional data includes key strokes, pages visited, information downloaded, chat records, e-mails etc. Operational data is safe to track without threats of security concern because IDS system routers and firewalls already track it. The major concern is transactional data. The more contents a honeypot tracks, more privacy concerns get generated.

C. Liability

Is the owner of the honeypot liable for any damage done by that honeypot? They will be safe as long as honeypots are used for directly securing the network.

VIII. SOME HONEYPOTS AND HELPFUL SOFTWARE

A. Back Officer Friendly By NFR

This product is designed to emulate a Back Officer server. BOF (as it is commonly called) is a very simple but highly useful honeypot developed by Marcus Ranum and crew at NFR. It is an excellent example of a low interaction honeypot. . It is a great way to introduce a beginner to the concepts and value of honeypots. 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 BackOrrifice.

B. Tripwire by tripwire

This product is for use on NT and UNIX machines and is designed to compare binaries, and inform the server operator, which has been altered. This helps to protect achines from would be hackers and is an excellent way to determine if a system has been compromised.

C. Specter

Specter is a commercial product and low interaction production honeypot. It is similar to BOF, but it can emulate a far greater range of services and a wide 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. Specters value lies in detection. It can quickly and easily determine who is looking for what. As a honeypot, it reduces both false positives and false negatives, simplifying the detection process, supporting a variety of alerting and logging mechanisms. One of the unique features of Specter is that it also allows for information gathering, or the automated ability to gather more

©IJRASET 2015: All Rights are Reserved

information about the attacker.

D. Mantrap

Mantrap is a commercial honeypot. Instead of emulating services, Mantrap creates up to four sub-systems, often called 'jails'. These 'jails' are logically discrete operating systems separated from a master operating system. Security administrators can modify these jails just as they normally would with any operating system, to include installing applications of their choice, such as an Oracle database or Apache web server, thus making the honeypot far more flexible. The attacker has a full operating system to interact with, and a variety of applications to attack. All of this activity is then captured and recorded. Currently, Mantrap only exists on Solaris operating system [5].

IX. FUTURE WORK

Honeypots are a new field in the sector of network security. Currently there is a lot of ongoing research and discussions all around the world. Several companies have already launched commercial products. A comparison of available products showed that there are some usable low- to high-involvement honeypots on the market. In the sector of research honeypots, self-made solutions have to be developed as only these solutions can provide a certain amount of freedom and flexibility which is needed to cover a wide range of possible attacks and attackers. There is an inherent scope for the research community to be misled by script kiddies, hile sophisticated attackers plan more devastating attacks on computer systems across the globe. Although fingerprinting a honeypot is easier said than done, most attackers worth their salt would stay away from any computer system that they deem to be monitoring their activities. Thus in reality, for honeypots to be truly effective, they require to be residing very close to a legitimate resource, probably even on the same network. This would definitely serve as a precursor to any attacks on the production system making honeypots a true window to the future.

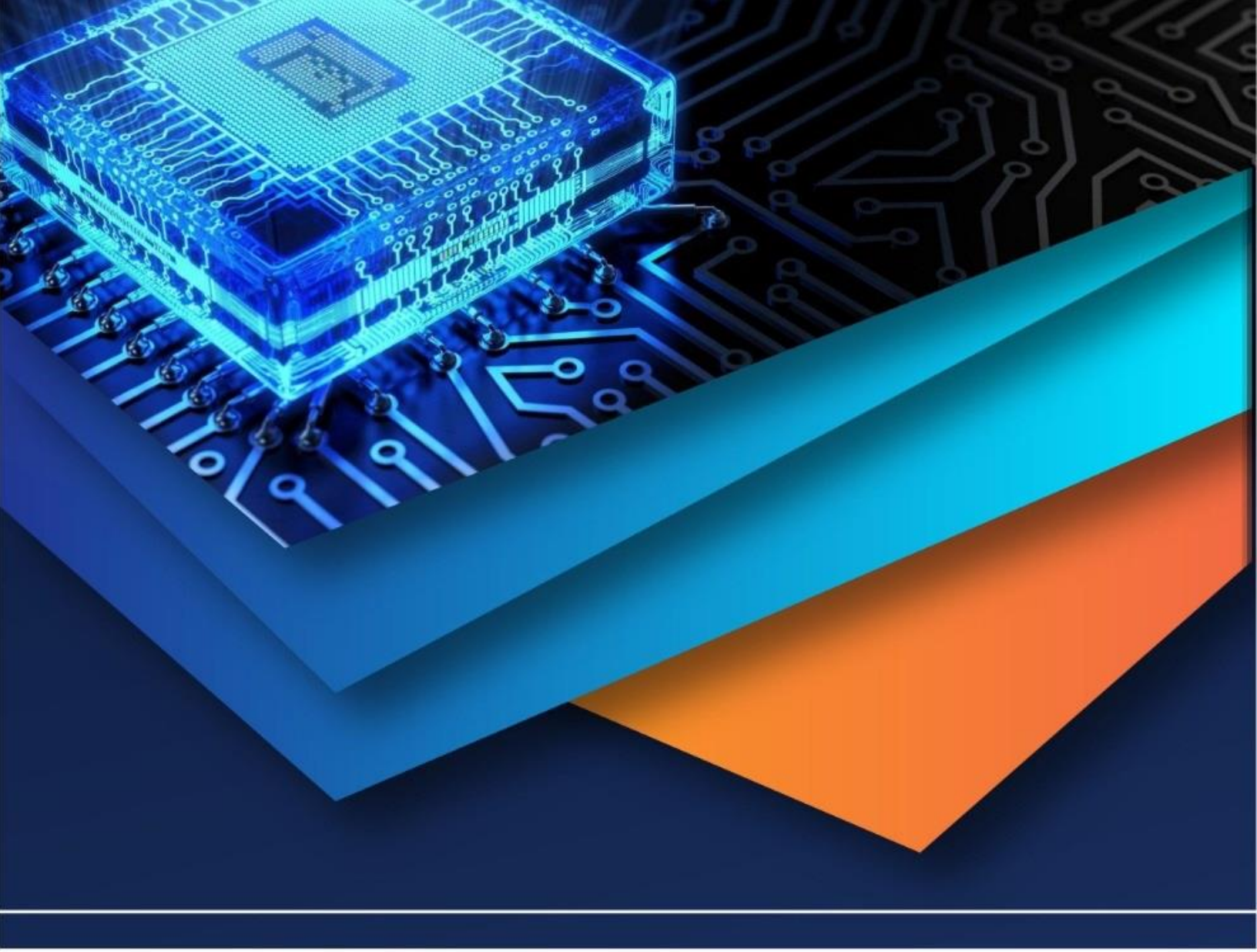
X. CONCLUSION

Honeypots are positioned to become a key tool to defend the corporate enterprise from hacker attacks it’s a way to spy on your enemy; it might even be a form of camouflage. Hackers could be fooled into thinking they've accessed a corporate network, when actually they're just banging around in a honeypot, while the real network remains safe and sound. Honeypots have gained a significant place in the overall intrusion protection strategy of the enterprise. Security experts do not recommend that these systems replace existing intrusion detection security technologies; they see honeypots as complementary technology to network- and host-based intrusion protection. The advantages that honeypots bring to intrusion protection strategies are hard to ignore. In time, as security managers understand the benefits, honeypots will become an essential ingredient in an enterprise-level security operation. We do believe that although honeypots have legal issues now, they do provide beneficial information regarding the security of a network .It is important that new legal policies be formulated to foster and support research in this area. This will help to solve the current challenges and make it possible to use.

REFERENCES

[1] Alata E. & Nicomette V. & Kaâniche M. & Dacier M. & Herrb M.,2006.Lessons learned from the deployment of a high-interaction honeypot, EDCC'06.
[2] Glasvezel Networks Nederland Fiber to the Home Project (FTTH),2009.Honeypot Software,Honeypot Products,Deception Software [Online] (Updated 23 October 2009) Available at : http://www.honeypots.net/honeypots/products [Accessed 5 May 2010].
[3] McFarland B.,2005. Ethical Deception and Preemptive Deterrence in Network SecurityGCFW Practical Version 4.1 , SANS Institute 2000-2005.
[4] Mokube,I. & AdaM.,2007.Honeypots:Concepts,Approaches,and Challenges. ACMSE 2007, March 23-24, 2007, Winston-Salem, North Carolina, USA ,pp.321-325.
[5] Phillipe JM. 6 mois de capture de logiciels malveillants [Online](Updated 24 july 2007).

©IJRASET 2015: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)