ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 2, Issue 12, December 2017

A Review to Track Hackers by Using Honeypots

[1] S. Gomathy, [2] M. Rajeswari, [3] J. Rathiga
[1][2] III Year B.Sc, [3] II Year B.Sc
[1][2][3] Dept of Computer Science, Holy Cross Home Science College, Tuticorin

Abstract:-- **Attacks on the internet keep on increasing and it causes harm to our security system. In order to minimize this threat, it is necessary to have a security system that has the ability to detect zero-day attacks and block them. "Honeypot is the proactive defense technology, in which resources placed in a network with the aim to observe and capture new attacks". This paper proposes a honeypot-based model for intrusion detection system (IDS) to obtain the best useful data about the attacker. The ability and the limitations of Honeypots were tested and aspects of it that need to be improved were identified. In the future, we aim to use this trend for early prevention so that pre-emptive action is taken before any unexpected harm to our security system. Honeypots are decoy computer resources set up for the purpose of monitoring and logging the activities of entities that probe, attack or compromise them. Honeypot does work as an Intrusion Detection System which detect the attacker in a network. Activities on honeypots can be considered suspicious by definition, as there is no point for users to interact with these systems. In this paper, we proposed a honeypot system in the wireless network to attract the attackers. We have used different fake websites to do so. Honeypot helps in detecting intrusion attacking on the system. The information gathered by watching a honeypot being probed is invaluable. The honeypot act as a normal system in the network having fake detailor invaluable information. It gives information about attacks and attack patterns. The Honeypot will make the attacker to attack the particular sites and side by side monitor its illegal steps to confirm about its identity. This proposed work will make the IP address of attacker to be blocked for further access of any site in the network. The proposed model has more advantages that can response accurately and swiftly to unknown attacks and lifetime safer for the network security. In future the network can be preserved by getting the information regarding the attacker from the Honeypot system. Honeypots are going to become a critical weapon in the good guys' arsenals. They don't catch only the lame hackers. Sometimes they catch the new tools and are able to reduce their effectiveness in the wild by letting security practitioners quickly react before they become widespread. They don't catch just the script kiddies outside your firewall but the hackers who work for your own company. They don't catch just unimportant stuff; sometimes they catch industrial spies. They can be time- and effort-consuming to set up and operate, but they're fun, instructive, and a terrific way for a good guy to gain an education on computer forensics in a real-world, low-risk environment.**

Key words: - Open source software, Intrusion detection, Graphical user interfaces, Information systems, Alarm systems, Computer graphics, User interfaces, Universal Serial Bus, Real time systems,

INTRODUCTION

Now the time, computer crimes are increasing. Countermeasures are developed to detect or prevent attacks – most of these measures are based on 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. 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. Network administrators usually use a firewall and an intrusion detection system (IDS) to protect their network. The firewall can control the inbound and outbound traffic according to the type of service requested, the user name, and the IP address of packets. The IDS can be deployed between the local area network and the Internet or any other important gateway for detecting suspicious packets [1]. However, sometimes administrators might forget to update the firewall rules. Moreover, the IDS system that uses anomaly detection has a high false-positive ratio [2]. The use of a honeypot can overcome the inherent deficiencies of the IDS and firewall. More importantly, we can treat it as a platform for security education in a university [3]. If a honeypot is deployed in front of a firewall, it can be treated as an early-warning system. If we deploy it behind the firewall, it can serve as part of a defense-in-depth system and can be used to detect attackers who bypass the firewall and IDS or threats from insiders [4].

FEATURES:

A honeypot is primarily an instrument for information gathering and learning. A honeypot is an information system resources whose values lies in the unauthorized zed or illicit use of that resource. Its primary purpose is not to be an ambush for the blackhat community to catch them in an action and to press charges against them. All this information is used to learn about the blackhat proceedings and motives, as well as their technical knowledge and abilities. There are lot of other possibilities for honeypot – divert hackers from productive systems or catch a hacker while conducting an attack are just two possible examples.

When most people think of honeypots they think of some of our favorite cartoon characters (Winnie the Pooh) indulging in a large container of honey. However, in computer jargon the term has quite a different meaning. In computer terminology, a honeypot is a trap set to detect, deflect or in some manner counteract attempts at unauthorized use of information systems. A honeypot is a security resource who's value lies in being probed, attacked or compromised.

TYPES:

The purpose of a production honeypot is to help mitigate risk in an organization. Commercial organization use production honeypots to help protect their networks. Research honeypots designed to gain information. Instead they are used to research the threats organizations face, and how to better protect against those threats. Although most honeypots have a similar general purpose, there are actually different types of honeypots that fulfill different function. There are two main types of honeypots:

Production - A production honeypot is one used within an organization's environment to help mitigate risk. The purpose of a production honeypot is to help mitigate risk in an organization. Commercial organization use production honeypots to help protect their network.

Research – A research honeypot add value to research in computer security by providing a platform to study the threat. Research honeypots designed to gain information.

There are more technical list of the types of honeypots. Here are some of the types.

Honeypots can generally be divided into different categories, low-interaction, medium-interaction and high-interaction honeypots respectively.

- •honeyd (low-interaction) - a GPL licensed daemon, that is able to simulate big network structures on a single host.
- •mwcollect, nepenthes (medium-interaction) - Honeypot where malware infects a simulated environment
- •Spam honeypots - Honeypot programs created by administrators which masquerade as abusable resources in order to discover the activities of spammers.
- •E-mail trap - An e-mail address that is not used for any other purpose than to receive spam can also be considered a spam honeypot.

DRAWBACKS:

DRAWBACKS OF LOW-INTERACTION:

This architecture provides a restricted framework within which emulation is carried out. Due to the limited number of services and functionality that it emulates, it is very easy to fingerprint.

FEATURE	GEN-I	GEN-II
Number of virtual systems/ services that can be deployed	Large	Small
Data Control	Limited	Extensive
Level of interaction	Low	High
Ability to discover new attacks	Low	High
Risk	Low	High

A flawed implementation (a behavior not shown by a real service) can also render itself to alerting the attacker. It has constrained applications in research, since every service which is to be studied will have to be re-built for the honeypot.

DRAWBACKS OF HIGH-INTERACTION:

To simulate an entire network, with routers and gateways, would require an extensive computing infrastructure, since each virtual element would have to be installed in it entirely. In addition this setup is comprehensive: the attacker can know that the network he is on is not the real one. This is one primary drawback of GEN-II. The number of honeypots in the network is limited. The risk associated with GEN-II honeypots is higher because they can be used easily as launch pads for attacks

COMPARISON:

•A typical low interaction honeypot is also known as GEN-I.

•A typical high interaction honeypot is known as GEN-II

ADVANTAGES:

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. Honeypots are designed to capture any activity and can work in encrypted networks. They can lure the intruders very easily

DISADVANTAGES:

Honeypot add complexity to the network. Increased complexity may lead to increased exposure to exploitation. There 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. 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.

LEGAL ISSUES PERTAINING HONEYPOTS:

There are three major legal spectrums concerning honeypots:
1. Entrapment 2. Liability 3. Privacy

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.

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.

PRIVACY: The major concern is what information is being tracked: operational data and transactional data. 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.

HELPFUL SOFTWARE OF HONEYPOTS:

CYBERCOP STING BY NETWORK ASSOCIATES:

This product is designed to run on Windows NT and is able to emulate several different systems including LINUX, SOLARIS, CISCO, IOS and NT. It is made to appeal to hacker for looking as if it has several well-known vulnerabilities.

BACK OFFICER FRIENDLY BY NFR:

This product is designed to emulate a Back Orifice Server. BOF (as it is commonly called) is very simple but highly useful honeypot developed by Marcus Ranum and crew at NFR. It is an excellent example of a low-interaction honeypot. BOF is a program that runs on most Windows based Operating System.

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 help to protect machines from would be hackers.

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.

MANTRAP:

Mantrap is commercial honeypot. Instead of emulating services, Mantrap creates up to four sub-systems, often called 'jails'. These 'jails' are logically discrete operating system. 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.

APPLICATIONS:

Much work has been performed using the concept of honeypots

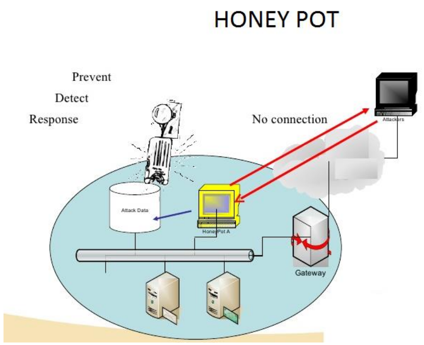
1.TARPITS 2. HONEYTOKENS

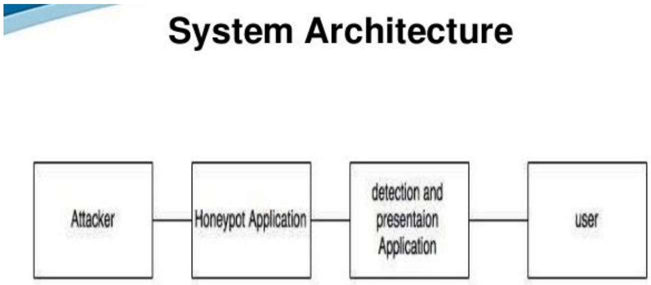
TARPITS:

One of the easiest ways to identify vulnerable systems is by using a tool called a scanner or a spider. This brute forces attacks on a whole range of IP addresses, attempting to find vulnerable hosts. A tarpit blocks a scanner by responding to its first TCP setup message, but ignoring the rest. This simple approach causes the scanner to allocate buffers, start timers and retry, since it believes it has found a valid host. This process repeats until the scanner exhausts its memory and CPU resources and crashes or slows down to an almost unproductive speed.

HONEYTOKENS:

It is a data entity whose value lies in the inherent use of data. Honey tokens are entities such as false medical records, incorrect credit card numbers and invalid social security numbers. This concept is especially useful in preventing larger classes.





3. What are the ethical issues concerning Honeypots?

The use of honeypots is a very controversial topic and although deemed legal to use, how ethical are they really? Some experts deem honeypots as a cause for entrapment and according to M.E. Kabay, author of 'liability and ethics of honeypots' , "As for entrapment, although this is not a legal problem, this does not mean that the way a honeypot entices attackers is not unethical." The argument is that since it is both unethical and illegal to lure someone into stealing an object, why is it legal or ethical to lure an individual into commiting a computer crime?

Other experts consider honeypots not only unethical, but a disadvantage to the computer world since they are in essence “building the better hacker” because more and more hackers are training themselves to be aware of honeypots and working around them, thus making secure systems a difficult ideal to achieve.

On the other hand some system security experts voice their opinion on the premise that honeypots merely use the “Attack first, before being attacked” approach. According to B. Scottberg, author of 'Internet Honeypots' "tracking an intruder in a honeypot reveals invaluable insights into attacker techniques and ultimately motives so that production systems can be better protected. You may learn of vulnerabilities before they are exploited." This viewed is a valid support concerning the ethics of honeypot applications for organizations that use them. In many cases, honeypot use cannot be labelled as being unethical because of its apparent advantages. The article, 'Combat Viruses' by Kurt Kleiner, proves that in some systems, honeypots have been known to contain and fight computer viruses. In another article, 'Using honeypots to fake out an attacker', Mark Edmead lists the most common advantages of using honeypots in security systems.

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. Honeypots do help in understanding the threats network systems face, but production honeypots should not be seen as a replacement for a standard IDS. If not configured correctly they can be used to access the real production system or be used as a launch pad for attacks against other systems.

REFERENCES:

1. Hongyan Zhang, "Research and application of honeypot technology in network security[J]", Science&Technology information, 2008.

2. Tengyun Ma, "Network security warning system based on Honeypot Technology[J]", Shandong University, 2013.

3. E Balas, C. Viecco, "Towards a Third Generation Data Capture Architecture for Honeynets", Proceeedings of the 6th IEEE Information Assurance Workshop, 2005.

4. Naveen, Sharanya. “Honeypot” Retrieved 1 June 2016.

5. Lance Spitzner(2002). Honeypots tracking hackers. Addison-Wesley.

6. Katakoglu, Onur (2017-04-03). “Attacks Landscape in the Dark Side of the Web”. Retrieved 2017-08-09.

7. Kaushik, Gaurav; Tyagi, Rashmi (2012). “Honeypot: Decoy Server or System Setup Together Information Regarding an Attacker”. VSRD International Journal of Computer Science & Information Technology.

8. Edwards,M. “Antispam Honeyspots Give Spammers Headaches”. Windows IT Pro. Retrieved 11 March 2015.

9. “Know Your Enemy: Genll Honey Nets Easier to deploy, harder to detect, safer to maintain”. Honeypot Project. 12 May 2005. Retrieved 14 June 2013.