Volume-7,Issue-2 (Feb-17)
ISSN (O) :- 2349-3585

HONEYPOTS FOR NETWORK SECURITY

Karthikeyan R[1], Dr.T.Geetha[2], Vijayalakshmi S[3], Sumitha R[4]
[1,2]Asst.Prof, [3]P.G.Scholar, [4] P.G.Scholar,
[1,2,3,4] Dept of MCA, Gnanamani college of Technolgy, Namakkal, INDIA

ABSTRACT - A honey pot is a non-production system which offers sweet bait to the intruders, black hat community [1] hat can enhance the ability of system administrators to identify system vulnerabilities. This paper presents a survey on recent advances in honey pot research from a review of 20+ papers on honeypots and related topics. A recent technology in the area of intrusion detection is honey pot technology that unlike common IDSs tends to provide the attacker with all the necessary resources needed for a successful attack. Honey pots provide a platform to study the approaches and tools used by the intruders, thus acquiring their value from the unauthorized use of their resources.

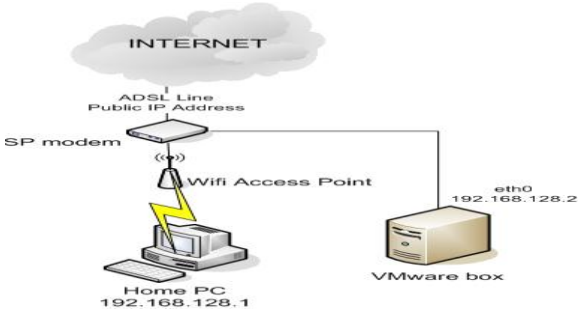
KEYWORDS: Honey pots, Intrusion Detection System, Security, Legal Issues

INTRODUCTION

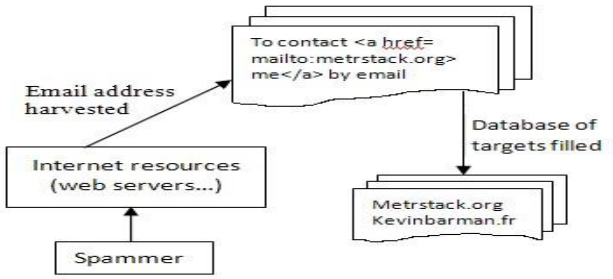
The underlying goal of computer security is to defend computers against attacks launched by malicious users. There are a numerous ways in which researchers and developers can work to protect the software that they write. Some are proactive, like code reviews and regression testing, while others are reactive, like the pwn2own contest where new vulnerabilities are used to exploit browsers. One class of tools that can take on aspects of both is **honeypots**.The term honey pot or honey trap was used during the cold war as a name for employing ensnarement to gain information from an enemy. In computer terminology, a **honey pot** is a trap set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. From few research papers, we come to know about, the Cuckoo's Egg where Cliff Stoll's hunt for a hacker using honey pot like methods are used. He posted fake data he knew the hacker would find interesting to keep the hacker occupied in his system while he was tracing him. Thanks to these medications which gave accurate information about various types of attacks which can be recorded. The term honey pot was first presented by Lance Spitzner in 1999 [2] in a paper titled "To Build a Honeypot".The idea behind these systems is to provide systems or services that deceive the intruder. Honey pots can be used as tools to gather information which can be used to enforce and strengthen existing intrusion detection tools or network firewalls. Honey pots should not be viewed as a solution to network security; they should be seen as an aid to it.

What is HONEYPOTS?

Honey pot is a unique security resource which is a part of security mechanism deployed in an organization. These are the resources you want the black hat guys to interact with. Basically, honey pot is an IT resource whose value lies in an unauthorized or its illicit use it means the value of honey pots could be derived from the threats using them.Honeypots would have little value if attacker doesn't interact with them. Indeed, honey pots do not solve specific problems. Instead they are tools having applications to security. They can be used as early warning systems, slowing down and automated attacks and capturing new exploits to gathering intelligence on emerging threats. Furthermore, honey pots come in different sizes and shapes .they can be emulated windows based application, an entire network to be compromised and attacked such asHoneynets. Also, honey pots don't even have to be computer. They may be credit card numbers, Excel spreadsheets or login and passwords.



LEVEL OF INTERACTION OF HONEYPOTS



Low Interaction Honey pots

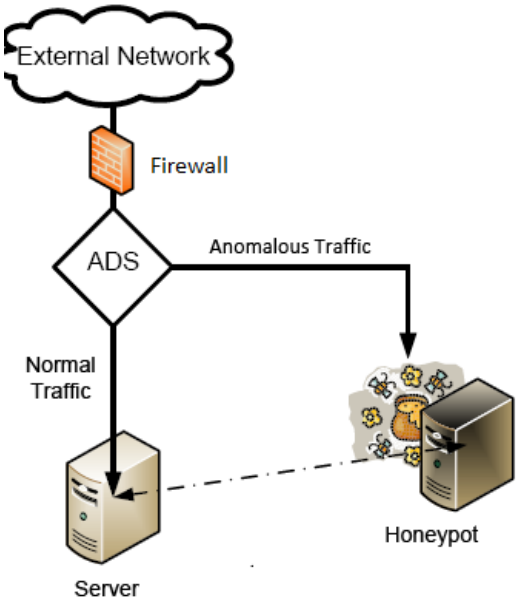
On the basis of interaction low interaction honeypotsdoesn't provide Operating system access to the intruder .It provides only services such as ftp ,http ,sash etc. these low interaction honey pots plays the role of passive IDS where the network traffic is not modified. Some examples of low interaction honey pots are honeyed, specter, BOF. Honeyed is an open source tool and the facility of service emulation onhoenyd is unrestricted whereas specter is not an open source tool and developed by Netsec. The well-known example of low interaction honey pot is honeyed. Honeyed Isa daemon and it is used to simulate large network on a single host. It provides a framework to create several virtual hosts using unused IP addresses of the network with help of ARP daemon For instance, several virtual numbers of operating systems.

Medium Interaction Honey pots

Like low interaction honey pots these also do not provide OS access to attacker but chances to be probed are more than low interaction honey pots .Some examples of medium interaction honey pots are Nepenthes, Diocese, honey trap, mwcollect.These honey pots also provide facadservices to the attacker's .Mwcollect and napenthes can be used to collect the spreading malwares.

High Interaction Honey pots

These are the most sophisticated honey pots .These are difficult to design and implementation .These honey pots are very time consuming to develop and have highest risks involved with this as they involve actual OS with them .In high Interaction Honey pots nothing is simulated or restricted[10]. Some example of High interaction honey pots are Sebeka, Argos. As these honey pots involves real operating system the level of risk is increased by many extents, but to capture large amount of information by allowing an attacker to interact with the real operating system ,it is a kind of trade off [13].This helps in capturing and logging of attackers behavior that can be analyzed in later stage.



HOW HONEY POT WORK?

IMPLEMENTATION

A honey pot's implementation has essentially two objectives. The first one is to seem plausible to attackers. The honey pot should look like it had some real value. Besides, it should not be easy to detect it. The other objective is to collect information from thehoneypot. Without this the honey pot is more or less useless.Honeypots can be divided into *physical honey pots* and *virtual honey pots* according toothier implementation. Physical honey pots are covered in subsection 3.1, whereas subsection discusses virtual honey pots. As a case study, *Honeyed* [Pro04] by Niles Provosts presented in subsection 3.3. Honeyed is a software framework for implementing virtualhoneypots and virtual networks of honey pots.

Physical honey pots

A physical honey pot is a real computer with a complete software stack. The computers connected into a network and has a dedicated network address. A physical honeypotis presumably the most plausible honey pot as almost everything is authentic and the environment does not have special restrictions. This allows practically the same level of interactivity as a real production system. However, outbound

ISSN:-2349-3585 |www.ijrdt.org

network connections are typically restricted and carefully monitored so that the honey pot cannot be used to launch further attacks. Physical honey pots are relatively expensive and very time-consuming to maintain [Spi02]. Firstly, the honey pot requires a dedicated physical machine. A complete network of physicalhoneypots requires networking equipment, too. Secondly, monitoring and analysis are somewhat difficult. Monitoring probes have to be hidden so that an attacker cannot detect them. Besides, a successful exploit can affect almost the whole software stack. Lastly, physical honey pots entail relatively high risk since there is real possibility for a takeover.

Virtual honey pots

A virtual honey pot simulates the honey pot system in software. This has various advantages over a physical honey pot. A virtual honey pot is easier and safer to operate since only the necessary functionality needs to be implemented [BKH06]. In addition, simulation allows implementing even complex networks of honey pots relatively few resources [Pro04].Because a physical honey pot runs a real operating system; it is almost always a highinteractionhoneypot. Virtual honey pots are more varied in terms of interactivity. A very simple low-interaction honey pot could consist of just a dummy service. A more complicated honey pot could implement a virtual network stack and allow running multiple services. A high-interaction honey pot could be implemented with a virtual machine Ana real operating system. Virtual honey pots tend to be easier to monitor than physical honey pots. A virtual honeypotcan be designed from the start to log every interaction. Although a honey pot based on a virtual machine is rather similar to its physical counterpart, the virtual machine itself can enforce monitoring. This allows capturing information even of attempts to exploit the actual operating system.

Honeyed

Honeyed is a framework for creating virtual honey pots. It operates in the network level and can simulate various TCP and UDP services. Thereby Honeyed is a low-interaction honeypot.The framework can simulate both individual network hosts and complete networks. The following treatment in this section is based on Niles Provost' article [Pro04].The main components of Honeyed are a packet dispatcher, protocol handlers, a personality engine and a routing component. A configuration database specifies how the other components operate. It describes a virtual network topology and contains a set of templates. A template is a specification for a honey pot. Templates are bound to network addresses in order to actually create virtual honey pots.

Applications

In this section a few examples of how to use honey pots are presented. Network decoys used for confusing attackers are discussed in subsection 4.1. In subsection 4.2, a few methods to prevent spam are covered. These two cases are relatively traditional, whereas the following ones are a Littlemore recent. In subsection 4.3, it is presented how honeypotscan automatically collect malware samples.

Network decoys

Honey pots are useful for monitoring networks [Pro04]. For monitoring, honey pots are deployed in such parts of a network that are not used for production. When an attacker probes the network, some traffic should eventually hit one of the honey pots. As n arrive at honey pots, warnings are rather reliable. However, honeypotsare useless if the attacker is aware of them. Neither can they detect the absence of attacks. Besides of network monitoring, honey pots can be used for confusing attackers by implementing decoy systems [Pro04]. The attacker might not be able to tell which systems have real value and which do not. Because of this, the attacker may have to work harder and use more time targeting the system. This makes detection easier. Nevertheless, the setup of plausible decoys can be rather tedious, and they involve risk, as well.

Prevention of spam

Spammers abuse open mail relays and open proxies to hide their identity [Pro04]. An open mail relay accepts any sender without authentication to send mail further. Open proxies accept any client in the network to make connections through it. Honey pots masquerading as open mail relays or open proxies can be used to capture spam and reveal its sources. Captured spam makes it possible to improve filtering. Knowing a source of spam might allow switching off the spammer from the network. Alternatively, a honey pot can collect source addresses of attempted mail deliveries. The

ISSN:-2349-3585 |www.ijrdt.org

addresses are temporarily added into the actual mail server's blacklist. This helps to filter out sources that almost certainly try to send spam.Honeypots seem to have been effective to some extent since spammers have developed methods to detect false open proxies [Kra04]. A simple test is to try to send mail back to itself via the proxy. The proxy is very likely a honey pot if it claims a success.

Collecting malware

A suitable honey pot can automatically collect samples of malware that spread autonomously. This allows large-scale capture of currently active malware. This in turn allows, for example, research on live data and constant refinement of intrusion detection and antivirus software [BKH06]. Manual capture of malware would be just too slow. The objective of a malware-collecting honey pot is essentially to download the actual malware and record the details of that event. The Nepenthes platform is a low-interaction honey pot which achieves this in the following way [BKH06]. The platform emulates set of known vulnerabilities that are remotely exploitable. When a network connection might lead to an exploit, the honey pot captures the connection's payload. It is then analyzed whether the payload contains machine executable code or network addresses.

Detection of malicious Web content

Vulnerabilities in Web browsers might allow malicious Web pages to install malware into the system. Exploited pages are rather common nowadays, and thus their manual detection and analysis is not practical [WBJ06]. Client honey pots can automate detection at least partially and help out in analysis.HoneyMonkey is a high-interaction client honey pot for detecting exploits [WBJ06]. The system consists of a set of Windows XP instances with different levels of patches running in virtual machines. The system is given a list of URLs that a modified Web browser within a virtual machine visits one by one. Between the URL visits, the state of the system, files and registry, is checked. If there were any modifications outside the browser's working area, the URL would be reported as an exploit and marked for further analysis. In that case, the exploited virtual machine instance is discarded and a clean one is started.

LEGAL ISSUES PERTAINING TO HONEYPOT:

Most of the research found in this area concluded that there are two major legal spectrums considering honey pots:

1. ENTRAPMENT: Entrapment is when somebody includes the criminal to do something he was not otherwise supposed to do. Honey pots should generally be used as defensive detective tool, not an offensive approach to luring intruders.

2. 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.

SOME COMMERCIAL HONEYPOTS AND HELPFUL SOFTWARE:

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 honey pot developed by Marcus Regnum and crew at NFR. It is an excellent example of low interaction honey pot.

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

ADVATAGES OF HONEYPOTS:

1. 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.

2. Honey pots are designed to capture any activity and can work in encrypted networks.

3. Honey pots are relatively simple to create and maintain

DISADVANTAGES OF HONEYPOTS

1. Honey pots add complexity to the network. Increased complexity may lead to increased exposure to exploitation.

2. There is also level of risk to consider, since a honey pot 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 honey pot.

CONCLUSION

Honey pots are positioned to become a key tool to defend the corporate enterprise from hacker attacks it's a way to spy on

ISSN:-2349-3585 |www.ijrdt.org

your enemy; it might even be a form of camouflage. Hackers could be fooled into thinking they have accessed a corporate network, when they are actually hanging around in a honey pot-- While the real network remains safe and sound. Honey pots have gained a significant place in the overall intrusion protection strategy of enterprise. Security experts do not recommend that these systems replace existing intrusion detection security technologies; they see honey pots as complementary technology to network-and host – based intrusion protection. The advantages that honey pots bring to intrusion protection strategies are hard to ignore. In time, as security managers understand the benefits, honey pots will become an essential ingredient in an enterprise –level security operation. We do believe that although honey pots have legal issues now, they do provide beneficial information regarding the security of a network. It is formulated to foster and support research in this area. This will help to solve the current challenges and make it possible to use honey pots.

REFERENCES

[1]. P.Diebold,A. Hess, G,Schafer. A Honey pot Architecture for Detecting and Analyzing Unknown Network Attacks. In Proc. Oh 14th Kommunikationin Verteilten systemen2005(KiVS05), Kaiserslautern, Germany, February 2005

[2]. Honey pots: White Paper. Reto Baumann, http:// www.Rbaumann.net, Christian Plattner, http:// www.

[3]. Christianplattner.net R.Karthikeyan,"A Survey on Position Based Routing in Mobile Adhoc Networks" in the international journal of P2P Network Trends and Technology, Volume 3 Issue 7 2013, ISSN:2249-2615.

[4]. Spitzer, Lance. Honey pots, Tracking Hackers. Pdf version. Addison Wesely, 2002.

[5]. Spitzer, Lance. Honey pots- Definitions and Value of Honey pots. http://www.infosecwriters.com, March 6, 2003.

[6]. R.Karthikeyan," Improved Apriority Algorithm for Mining Rules" in the International Journal of Advanced Research in biology Engineering science and Technology Volume 11, Issue 4, April 2016, Page No:71-77.

[7]. Honey net project, the. (2007a). know your enemy: Honeynets. Retrieved on 7 October 2007 from http;//www.Honeynet.org/papers/honeynet/index.html.

[8]. C.Ganesh,B.Sathyabhama,Dr.T.Geetha " Fast Frequent Pattern Mining using Vertical Data Format for Knowledge Discovery "International Journal of Engineering Research in Management & Technology. Vol.5, Issue-5, Pages: 141-149.

[9]. Research infrastructures action, Sixth frameworkprogramme, D1.4: Architecture Integration, page 36.

[10]. R.Karthikeyan,"A Survey on Sensor Networks" in the International Journal for Research & Development in Technology Volume 7, Issue 1, Jan 2017, Page No: 71-77. Niles Provost: Honeyed- Virtual Honey pot, http://www.honeyd.org/, Provost 2002.