PROTECTION METHOD AGAINST UNAUTHORISED ISSUES IN NETWORK-HONEYPOTS

K.Meenakshi[#1], M.Nalini Sri[*2]

[#1] IV/IV B-TECH,ECM DEPARTMENT, KL UNIVERSITY
[*2]ASST.PROFESSOR, ECM, KL UNIVERSITY

***Abstract*— From common man to huge organization everyone uses network daily for data transfer or for business purpose based on their requirement.But there is no full security to the services provided by the internet. So everyone has to follow some measures to prevent themselves from security attacks by adopting some security measures.Some of them are *firewalls ,antivirus software, authorization of accesing methods,detection of threats methodology etc.*. Honey pots is one of the method to prevent threats and intrusions during network accessing during the daily use of internet. This method will not give full protection to the network but can reduce the loss due to insecurity in the network. This paper brings awareness about threats in the network and the prevention of it by using a method HONEYPOTS. By adopting this measures the problems arising in the network will be reduced and one day we can use the fully secured network as for every problem there will be a solution.**

***Keywords*—honeypots,spammers,honeynets,low-interaction honeypots:honeyd.**

I.INTRODUCTION

The rapid growth of the Internet has provided hackers and other attackers with the ability to inflict major financial and public relations damage on an organization. Attackers are constantly developing new tools to exploit the applications necessary for an organization to maintain an Internet presence. As attackers develop more clever and imaginative methods to subvert or exploit the firewall, it has become apparent that advanced and layered security technologies are necessary to protect against hacker attacks.

One such technology that has gathered considerable attention from industry analysts and trade media is decoy-based intrusion protection, also known as "honeypot" technology. Honeypots, considered by many as the hottest new intrusion protection technology, are used to contain and control an attack. They are used much like deception techniques in warfare that divert enemies into attacking false troops or airfields. These systems can be applied to defend networked assets from today's savvy attackers waging a new kind of war on the enterprise.

Honeypots were once used primarily by researchers and generally placed outside the firewall to discover hackers on a network system. Using the honeypots, researchers could study their tactics, tools, movements, and behaviour. Today honeypots play an important part in enterprise security. Resellers and other distributors who understand the evolution of decoy-based intrusion protection into a critical 'behind the firewall' enterprise security technology will be better able to create a comprehensive intrusion protection strategy for their clients in any vertical industry. This article defines honeypots, describes their advantages, and outlines how they act as complementary components of an overall intrusion protection strategy.

II DESCRIPTION

A honeypot is a system that detects, contains and monitors unauthorized access (or other system misuse) as it happens. As a complement to network- and host-based intrusion detection systems (IDSs), honeypots act as decoy systems and divert attacks from key resources while also providing early detection of internal and external attacks.

Unlike firewalls or Intrusion Detection Systems, honeypots do not solve a specific problem. Instead, they are a highly flexible tool that comes in many shapes and sizes. They can do everything from detecting encrypted attacks in IPv6 networks to capturing the latest in on-line credit card fraud. Its is this flexibility that gives honeypots their true power. It is also this flexibility that can make them challenging to define and understand.

Because honeypots have no "production value," meaning they conduct no authorized activity, any activity that takes place within a honeypot is likely the interaction of somebody or something with malicious intent. Such activity can be monitored by IT managers to gain valuable information that helps them respond to an attack more quickly, protect against future attacks and even help an organization track and prosecute attackers. Most importantly, since the honeypot is attacked, attacks to your client's production systems are avoided.

SPAMMERS

Spammers abuse vulnerable resources such as open mail relays and open proxies. Some system administrators have created honeypot programs that masquerade as these abusable resources to discover spammer activity. There are several capabilities such honeypots provide to these administrators and the existence of such fake abusable systems makes abuse more difficult or risky. Honeypots can be a powerful countermeasure to abuse from those who rely on very high volume abuse (e.g., spammers).These honeypots can reveal the apparent IP address of the abuse and provide bulk spam capture (which enables operators to determine spammers'. For open relay honeypots, it is possible to determine the e-mail addresses ("dropboxes") spammers use as targets for their test messages, which are the tool they use to detect open relays. It is then simple to deceive the spammer: transmit any illicit relay e-mail received addressed to that dropbox e-mail address. That tells the spammer the honeypot is a genuine abusable open relay, and they often respond by sending large quantities of relay spam to that honeypot, which stops it. The apparent source may be another abused system—spammers and other abusers may use a chain of abused systems to make detection of the original starting point of the abuse traffic difficult.This in itself is indicative of the power of honeypots as anti-spam tools. In the early days of anti-spam honeypots, spammers, with little concern for hiding their location, felt safe testing for vulnerabilities and sending spam directly from their own systems. Honeypots made the abuse riskier and more difficult.Spam still flows through open relays, but the volume is much smaller than in 2001 to 2002. While most spam originates in the U.S., spammers hop through open relays across political boundaries to mask their origin. Honeypot operators may use intercepted relay tests to recognize and thwart attempts to relay spam through their honeypots. "Thwart" may mean "accept the relay spam but decline to deliver it." Honeypot operators may discover other details concerning the spam and the spammer by examining the captured spam messages.

TRAPPING EMAIL

An e-mail address that is not used for any other purpose than to receive spam can also be considered a spam honeypot. Compared with the term spam trap, the term "honeypot" might better be reserved for systems and techniques used to detect or counter attacks and probes. Spam arrives at its destination "legitimately"—exactly as non-spam e-mail would arrive.An amalgam of these techniques is Project Honeypot. The distributed, open-source Project uses honeypot pages installed on websites around the world. These honeypot pages hand out uniquely tagged spamtrap e-mail addresses. and Spammers can then be tracked as they gather and subsequently send to these spamtrap e-mail addresses.

DATABASE HONEYPOT

Databases often get attacked by intruders using SQL Injection. Because such activities are not recognized by basic firewalls, companies often use database firewalls. Some of the available SQL database firewalls provide/support honeypot architectures to let the intruder run against a trap database while the web application still runs as usual

DETECTION

Just as honeypots are weapons against spammers, honeypot detection systems are spammer-employed counter-weapons. As detection systems would likely use unique characteristics of specific honeypots to identify them, a great deal of honeypots in use makes the set of unique characteristics larger and more daunting to those seeking to detect and thereby identify them. This is an unusual circumstance in software: a situation in which "versionitis" (a large number of versions of the same software, all differing slightly from each other) can be beneficial. There's also an advantage in having some easy-to-detect honeypots deployed.Fred Cohen, the inventor of the Deception Toolkit, even argues that every system running his honeypot should have a deception port that adversaries can use to detect the honeypot. Cohen believes that this might deter adversaries.

HONEYNETS

Two or more honeypots on a network form a *honeynet*. Typically, a honeynet is used for monitoring a larger and/or more diverse network in which one honeypot may not be sufficient. Honeynets and honeypots are usually implemented as parts of larger network intrusion detection systems. A *honeyfarm* is a centralized collection of honeypots and analysis tools.The concept of the honeynet first began in 1999 when Lance Spitzner, founder of the Honeynet Project, published the paper "To Build a Honeypot

TYPES OF HONEYPOTS

Honeypots can be classified based on their deployment and based on their level of involvement. Based on deployment, honeypots may be classified as:

1. production honeypots
2. research honeypots

Production honeypots are easy to use, capture only limited information, and are used primarily by companies or corporations; Production honeypots are placed inside the production network with other production servers by an organization to improve their overall state of security. Normally, production honeypots are low-interaction honeypots, which are easier to deploy. They give less information about the attacks or attackers than research honeypots do.

Research honeypots are run to gather information about the motives and tactics of the Blackhat community targeting different networks. These honeypots do not add direct value to a specific organization; instead, they are used to research the threats organizations face and to learn how to better protect against those threats. Research honeypots are complex to deploy and maintain, capture extensive information, and are used primarily by research, military, or government organizations.

III CLASSIFICATION

Based on design criteria, honeypots can be classified as

1. pure honeypots
2. low-interaction honeypots
3. high-interaction honeypots

(i)Pure honeypots are full-fledged production systems. The activities of the attacker are monitored using a casual tap that has been installed on the honeypot's link to the network. No other software needs to be installed. Even though a pure honeypot is useful, stealthiness of the defense mechanisms can be ensured by a more controlled mechanism.

(ii)Honeyd:Low-interactionhoneypot

Honeyd is a low-interaction honeypot. Developed by Niels Provos, Honeyd is OpenSource and designed to run primarily on Unix systems (though it has been ported to Windows). Honeyd works on the concept of monitoring unused IP space. Anytime it sees a connection attempt to an unused IP, it intercepts the connection and then interacts with the attacker, pretending to be the victim. By default, Honeyd detects and logs any connection to any UDP or TCP port. In addition, you can configure emulated services to monitor specific ports, such as an emulated FTP server monitoring TCP port 21. When an attacker connects to the emulated service, not only does the honeypot detect and log the activity, but it captures all of the attacker's interaction with the emulated service. In the case of the emulated FTP server, we can potentially capture the attacker's login and password, the commands they issue, and perhaps even learn what they are looking for or their identity. It all depends on the level of emulation by the honeypot. Most emulated services work the same way. They expect a specific type of behavior, and then are programmed to react in a predetermined way. If attack A does this, then react this way. If attack B does this, then respond this way. The limitation is if the attacker does something that the emulation does not expect, then it does not know how to respond. Most low-interaction honeypots, including Honeyd, simply generate an error message. You can see what commands the emulated FTP server for Honeyd supports by review the source code.

Some honeypots, such as Honeyd, can not only emulate services, but emulate actual operating systems. In other words, Honeyd can appear to the attacker to be a Cisco router, WinXP webserver, or Linux DNS server. There are several advantages to emulating different operating systems. First, the honeypot can better blend in with existing networks if the honeypot has the same appearance and behavior of production systems. Second, you can target specific attackers by providing systems and services they often target, or systems and services you want to learn about. There are two elements to emulating operating systems. The first is with the emulated services. When an attacker connects to an emulated service, you can have that service behave like and appear to be a specific OS. For example, if you have a service emulating a webserver, and you want your honeypot to appear to be a Win2000 server, then you would emulate the behavior of a IIS webserver. For Linux, you would emulate the behavior of an Apache webserver. Most honeypots emulate OS' in this manner. Some sophisticated honeypots take this emulation one step farther (as Honeyd does). Not only do they emulate at the service level, but at the IP stack level. If someone uses active fingerprinting measures to determine the OS type of your honeypot most honeypots respond with the IP stack of whatever OS the honeypot is installed on. Honeyd spoof the replies, making not only the emulated services, but emulated IP stacks behave as the operating systems would. The level of emulation and sophistication depends on what honeypot technology you chose to use.

(iii)Honeynets:High-interactionhoneypot

Honeynets are a prime example of high-interaction honeypot. Honeynets are not a product, they are not a software solution that you install on a computer. Instead, Honeyents are an architecture, an entire network of computers designed to attacked. The idea is to have an architecture that creates a highly controlled network, one where all activity is controlled and captured. Within this network we place our intended victims, real computers running real applications. The bad guys find, attack, and break into these systems on their own initiative. When they do, they do not realize they are within a Honeynet. All of their activity, from encrypted SSH sessions to emails and files uploads, are captured without them knowing it. This is done by inserting kernel modules on the victim systems that capture all of the attacker's actions. At the same time, the Honeynet controls the attacker's activity. Honeynets do this using a Honeywall gateway. This gateway allows inbound traffic to the victim systems, but controls the outbound traffic using intrusion prevention technologies. This gives the attacker the flexibility to interact with the victim systems, but prevents the attacker from harming other non-Honeynet computers.

IV WORKING OF HONEYPOTS

1. Prevention
2. Detection
3. Response

(i) PREVENTION: Honeypots can help prevent attacks in several ways. The first is against automated attacks, such as worms or auto-rooters. These attacks are based on tools that randomly scan entire networks looking for vulnerable systems. If vulnerable systems are found, these automated tools will then attack and take over the system (with worms self-replicating, copying themselves to the victim). One way that honeypots can help defend against such attacks is slowing their scanning down, potentially even stopping them. Called sticky honeypots, these solutions monitor unused IP space. When probed by such scanning activity, these honeypots interact with and slow the attacker down. They do this using a variety of TCP tricks, such as a Windows size of zero, putting the attacker into a holding pattern. This is excellent for slowing down or preventing the spread of a worm that has penetrated your internal organization. One such example of a sticky honeypot is LaBrea Tarpit. Sticky honeypots are most often low-interaction solutions (you can almost call them 'no-interaction solutions', as they slow the attacker down to a crawl :). Honeypots can also be protect your organization from human attackers. The concept is deception or deterrence. The idea is to confuse an attacker, to make him waste his time and resources interacting with honeypots. Meanwhile, your organization has detected the attacker's activity and have the time to respond and stop the attacker. This can be even taken one step farther. If an attacker knows your organization is using honeypots, but does not know which systems are honeypots and which systems are legitimate computers, they may be concerned about being caught by honeypots and decided not to attack your organizations. Thus the honeypot deters the attacker. An example of a honeypot designed to do this is Deception Toolkit, a low-interaction honeypot.

(ii)PROTECTION: The second way honeypots can help protect an organization is through detection. Detection is critical, its purpose is to identify a failure or breakdown in prevention. Regardless of how secure an organization is, there will always be failures, if for no other reasons then humans are involved in the process. By detecting an attacker, you can quickly react to them, stopping or mitigating the damage they do. Tradtionally, detection has proven extremely difficult to do. Technologies such as IDS sensors and systems logs haven proven ineffective for several reasons. They generate far too much data, large percentage of false positives, inability to detect new attacks, and the inability to work in encrypted or IPv6 environments. Honeypots excel at detection, addressing many of these problems of traditional detection. Honeypots reduce false positives by capturing small data sets of high value, capture unknown attacks such as new exploits or polymorphic shellcode, and work in encrypted and IPv6 environments. You can learn more about this in the paper Honeypots: Simple, Cost Effective Detection. In general, low-interaction honeypots make the best solutions for detection. They are easier to deploy and maintain then high-interaction honeypots and have reduced risk.

(iii)RESPONSE**:** The third and final way a honeypot can help protect an organization is in reponse. Once an organization has detected a failure, how do they respond? This can often be one of the greatest challenges an organization faces. There is often little information on who the attacker is, how they got in, or how much damage they have done. In these situations detailed information on the attacker's activity are critical. There are two problems compounding incidence response. First, often the very systems compromised cannot be taken offline to analyze. Production systems, such as an organization's mail server, are so critical that even though its been hacked, security professionals may not be able to take the system down and do a proper forensic analysis. Instead, they are limited to analyze the live system while still providing production services. This cripiles the ability to analyze what happened, how much damage the attacker has done, and even if the attacker has broken into other systems. The other problem is even if the system is pulled offline, there is so much data pollution it can be very difficult to determine what the bad guy did. By data pollution, I mean there has been so much activity (user's logging in, mail accounts read, files written to databases, etc) it can be difficult to determine what is normal day-to-day activity, and what is the attacker. Honeypots can help address both problems. Honeypots make an excellent incident resonse tool, as they can quickly and easily be taken offline for a full forensic analysis, without impacting day-to-day business operations. Also, the only activity a honeypot captures is unauthorized or malicious activity. This makes hacked honeypots much easier to analyze then hacked production systems, as any data you retrieve from a honeypot is most likely related to the attacker. The value honeypots provide here is quickly giving organizations the in-depth information they need to rapidly and effectively respond to an incident. In general, high-interaction honeypots make the best solution for response. To respond to an intruder, you need in-depth knowledge on what they did, how they broke in, and the tools they used. For that type of data you most likely need the capabilities of a high-interaction honeypot.

PROS

Honeypots provide multiple advantages as part of a complete security infrastructure. The first and greatest advantage of a honeypot is its intrusion detection capability. Although other intrusion detection technologies are critical, honeypots specifically provide detection of things other security solutions aren't designed to detect, such as new types of attacks (also called "zero-day" attacks), attacks that have bypassed other defenses, attacks using encryption or tunneling, and attacks utilizing stolen credentials. For example, since a honeypot can emulate a real server it is indistinguishable from a production server to an attacker. Because a person with real credentials would not be interacting with a non-production system like a honeypot, any interaction with a decoy server using those credentials would be considered extremely suspicious. Honeypots can also detect "zero-signature attacks"

–attacks that are not discernable from traffic and have no unique patterns to match.

Second, honeypots provide zero "false positives." Many intrusion detection technologies by nature will produce a certain amount of false positives. This is because there is always a chance that valid traffic will match the characteristics the IDS uses to detect attacks. There are no false positives with a honeypot.*Any* communication with a honeypot is suspect simply because the device is not used for any purpose other than detecting attacks. In other words, there is no invalid traffic to produce false positives.

Third, honeypots are able to divert an attack or control the activities of an attacker. Because an IT manager has complete control over the level of activity that is allowed inside a honeypot, activities are rendered harmless because they are attacking a non-production decoy-system.

Honeypots can also detect and record incidents that may last for months. These so-called "slow scans" are impossible to detect using conventional IDSs as the time involved makes them appear to be normal traffic.

Determining a hacked production system can be difficult since it is hard to differentiate between normal day-to-day activity and intruder activity. By capturing only unauthorized activity, honeypots can be effective as an incident response tool because they can be taken offline for analysis without affecting business operations. The newest honeypots boast stronger threat response mechanisms, including the ability to shut down systems based on attacker activity and frequency-based policies that enable security administrators to control the actions of an attacker in the honeypot.

One of the greatest advantages of honeypots is their ability to bolster network security and provide an added level of protection when combined with traditional IDSs. In contrast to the large number of alerts many IDSs can create, honeypots collect data only when someone is interacting with them, creating small data sets that make it easier and more cost-effective to identify and act on unauthorized activity.

More and more organizations are moving to encrypt all their data, either because of security issues or regulation (such as HIPAA). Not surprisingly, more and more attackers are using encryption as well, which in some cases can blind a firewall or IDS's ability to monitor the network traffic. With a honeypot, it doesn't matter if an attacker is using encryption; the activity will still be captured.

V CONCLUSION

Honeypots have gained a pivotal role in the overall intrusion protection strategy of the enterprise. Security proposals do not recommend that the systems replace existing intrusion detection security technologies because honeypots is a complementary technology to network and host based one. The method involved in this honeypots concept reduces the effects of intrusions and attacks during the accessing of network services. Honeypots does not rectify all the defects occurred during consumption of internet services but it will definitely reduces the damage due to those effects.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.

ACKNOWLEDGMENT

1.V.SamsonDevakumar,ProjectManager,E-World Software development training center, SCRWWO, Vijayawada.

2.V.Saikrishna,Programmer,E-world software development training center, SCRWWO ,Vijayawada.

RFERENCES

http://en.wikipedia.org/wiki/Addison-Wesley

http://www.net-security.org/secworld.php?id=4085

http://jackpot.uk.net/

http://assist.babylon.com/babylonassista/dnsassist/main?domain=llama.whoi.edusmtpot.py

http://sourceforge.net/projects/spamhole/

http://all.net/dtk/index.html

http://en.wikipedia.org/wiki/Honeypot_%28computing%29

http://www.philippinehoneynet.org/

http://old.honeynet.org/papers/gen2/