NCCS
College of IT & Management
[Affiliated to TU]

National College of Computer Studies

Paknajol, Kathmandu

Report on
HoneyPot Security

Submitted by:

Atullya Maharjan

Programme: Bsc.CsIt 1st Semester

Roll. No: 5

Email:atulmzn1@gmail.com

Submitted to:

Dadhi Ram Ghimire

TU Lecturer

Abstract

A honeypot is a system created to engage with cyber attackers and gather information about their tactics and tendencies. Over the past three decades, a lot of research has been done in the area of network intrusion detection. Intrusion detection is becoming a difficult procedure as networks become quicker and as reliance on the Internet grows on both a personal and business level. The difficulty in this situation is not only in being able to actively monitor numerous systems, but also in being able to respond swiftly to various situations. It is advisable to have a firm understanding of what a honeypot should and should not do before using one. The operating systems and services a honeypot will use should be understood in detail. The dangers involved should be considered, and strategies for addressing or lowering these risks should be understood. Having a strategy for what to do in the event that the honeypot is hacked is also advised. A honeypot policy addressing security risks should be documented in the case of production honeypots. Legal issues pertaining to honeypots or their operation should also be considered. In this essay, we define the comparatively recent term "honeypot." A computer called a "honeypot" was created expressly to assist in learning the goals, aptitudes, and methods used by the hacker community. It also goes into great detail on the principles of honeypots and their contribution to the field of network security. The paper then makes a suggestion for and develops an intrusion detection tool utilizing the honeypot concept and some of the currently practiced intrusion detection techniques.

Table of content

Contents

1. Introduction/Background 1

2. BACKGROUND 2

3. Types of Honey pot Security 3

3.1 Research Honeypots: 3

3.2 Production Honeypots: 3

4. Security Issues: 4

5. Role of Honeypots in Network Security: 6

6. Security of the gateway: 7

7. Working: 8

8. Benefits of using Honeypot 9

9. Result 10

10. Conclusion 11

References 12

List of Figures

Figure 1 HonePot 2
Figure 2 Approaches for Preventing Honeypot Detection and Compromise 6
Figure 3 Working of HoneyPot 9

1. Introduction/Background

One who makes an attempt to get access to a working computer is known as an invader. Popular terms for this persona include hacker, black hat, and cracker. A honeypot is a security mechanism that creates a virtual trap to lure attackers. An intentionally compromised computer system allows attackers to exploit vulnerabilities so you can study them to improve your security policies. You can apply a honeypot to any computing resource from software and networks to file servers and routers. Honeypots are a type of deception technology that allows you to understand attacker behavior patterns. Security teams can use honeypots to investigate cyber security breaches to collect Intel on how cybercriminals operate. They also reduce the risk of false positives, when compared to traditional cyber security measures, because they are unlikely to attract legitimate activity. [1]

The number of computers connected to a network and the Internet is increasing with every day. When combined with the increase in networking speed has made intrusion detection a challenging process these systems existed as a part of the commercial/in-use networks and used techniques like pattern matching or anomaly detection. Another type of security systems are system integrity checkers, which are, typically host based. The problem that these systems face is that they are running on computers, which are in use on a daily basis. These systems frequently deal with numerous connections and data transfers, which generates enormous log files and makes it challenging to effectively distinguish between regular traffic and intrusion attempts. Many of these systems are also known to generate many false positives or in some cases false negatives. Additionally, these systems offer incredibly little information into the tools and techniques used by the black hat group. [1] and [3].

A program, device, or system placed on a network as bait for attackers is known as a honeypot. The goal is to fool the attacker by giving the honeypot the appearance of a trustworthy system. In most cases, honeypots are virtual computers that imitate real machines by pretending to have open ports and operating services, which are features that one might find on a conventional system on a network. The purpose of these active services is to draw attackers' attention so that they will invest important time and resources into trying to exploit the machine while the attacker is being observed and recorded by the honeypot. The idea behind these systems is to provide systems or services that deceive the intruder. Such systems help in learning the methods that intruders use and they also can be viewed as a decoy to distract hackers from the real systems and services. Honeypots can be classified as deception systems. By definition a honeypot is “a security resource whose value lies in being probed, attacked or compromised”. Honeypots can be used as tools to gather information which can be used to enforce and strengthen existing intrusion detection tools or network firewalls. Honeypots should be considered a help to network security rather than a solution to it. We examine the goals behind the installation of honeypots, as well as the security and legal concerns associated with it. Additionally, we examine the configuration of a honeypot network and give some analysis based on the data gathered from it. We conclude by providing a review of current honeypot technology. In this thesis, we examine the emerging idea of honeypots and how intrusion detection systems use them. A network of honeypots was created and put into operation as part of the thesis project. The honeypots were kept online for a period of time and any network communication or events related to it was recorded and analyzed [2] and [4].

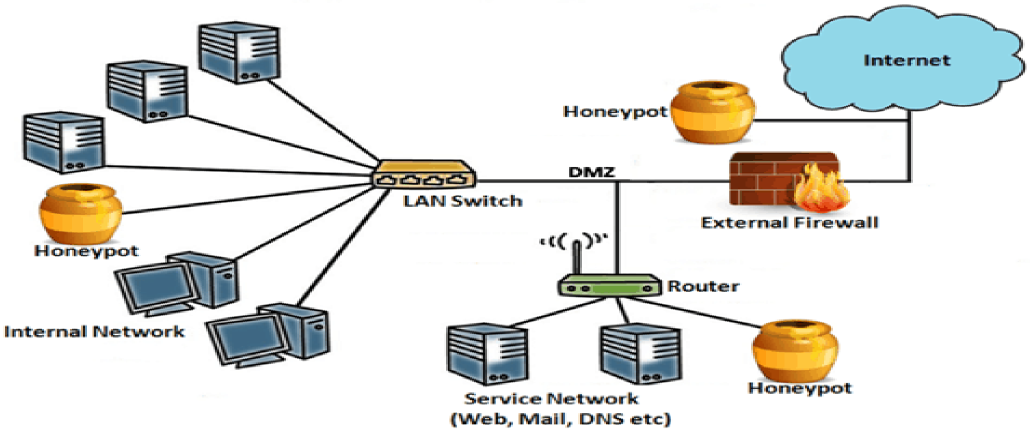

Figure 1 Honeypot

2. BACKGROUND

A program, device, or system placed on a network as bait for attackers is known as a honeypot. The goal is to fool the attacker by giving the honeypot the appearance of a trustworthy system. In most cases, honeypots are virtual computers that imitate real machines by pretending to have open ports and operating services, which are features that one might find on a conventional system on a network. Currently, there are two categories of honeypots based on the purpose they serve:

3. Types of Honey pot Security

3.1 Research Honeypots:

A research honeypot, on the other hand, is a type of honeypot that's used to collect information about the specific methods and tactics hackers use. Like production honeypots, they consist of fake data that looks sensitive and valuable to hackers. Research honeypots also collect information about attacks and vulnerabilities.

Research honeypots typically aren't used by businesses. Rather, they are used by government and research organizations. That's essentially how they differ from production honeypots. While production honeypots are used within a business's network, research honeypots are deployed elsewhere — typically on multiple networks or locations.

Research honeypots are also more complex than production honeypots. As a result, they require more work to deploy. Because of their complexity, though, research honeypots provide more information about attacks and vulnerabilities. [5]

3.2 Production Honeypots:

The most common type, a production honeypot is a type of honeypot that's used to collect cyber security-related information within a business's or organization's production network. Once deployed, the production honeypot will wait for an attack. If an attack occurs, it may collect data such as originating Internet Protocol (IP) addresses, traffic frequency and volume, directories accessories and more.

Production honeypots are popular among businesses because they are easy to use while revealing essential information about cyber threats and vulnerabilities facing their networks. With that said, production honeypots generally don't reveal as much information as their research counterparts. [5] Even redundant layers can be helpful in cases where the black hat detects the honeypot and tries to clear his traces in the logs. The logs should be checked on daily basis and, if possible, even more frequently. There are many questions that need to be answered beforehand with regard to the possibility of a honeypot being compromised. How do we find out the honeypot is compromised? How quickly will we be alerted? How do we backup the compromised system for analysis? What is the next step? Do we let the hacker know about the existence of the honeypot? Do we allow the attacker to continue? If yes, how do we restrict damage to other computers? The answers to all these questions should be carefully thought out and planned [1], [6] and [7].

4. Security Issues:

Honeypots don't offer security to an organization (they aren't a security technology), but when set up and used properly, they improve current security procedures. One could argue that honeypots produce some kind of security risk, which the administrator must manage. Depending on how they are deployed and implemented, there is a security risk. Two perspectives exist about how honeypot systems should manage their security threats. There are tools for creating phony services, vulnerabilities, or even honeypots. They deceive any attacker to think they are accessing one particular system or service. A properly designed tool can be helpful in gathering more information about a variety of servers and systems. Such systems are easier to deploy and can be used as alerting systems and are less likely to be used for further illegal activities. Honeypots that are real systems: This is a viewpoint that states that honeypots should not be anything different from actual systems since the main idea is to secure the systems that are in use. These honeypots employ real systems and servers that are in operation in the real world and don't spoof or imitate anything. These honeypots lessen the likelihood that the hacker will be aware that he is on one. Because of their great risk, these honeypots cannot be placed everywhere. They require a managed setting and administrative experience. A compromised honeypot is a potential risk to other computers on the network or for that matter the Internet. Many systems are compromised and used in attacks such as Denial of Service. The honeypot must be constantly supervised at regular intervals. A network dedicated to honeypots helps not only in supervising honeypots but also helps in detecting attacks and restricting the honeypot from being used to attack other computers. Honeypots don’t guarantee every attack will be detected. Honeypots can only detect attacks from traffic directed at them. So a smart hacker who detects a honeypot in a network that he is trying to compromise will avoid sending any traffic to the honeypot. If this happens the honeypot will be completely oblivious of any ongoing attacks on other computers in the network. Although they don't provide any new knowledge, honeypots that run services with known defects or user-made holes can be used to collect statistics or identify black hat or black hat systems. An administrator could be charged with negligence if he intentionally or un-intentionally allows a compromised honeypot to be used to attack other systems. Also any information (false or genuine) that the hackers gain from the honeypot can sometimes adversely affect the organization. [8] and [9].

Legal issues:

A honeypot should be used as a teaching tool at first. However, there is a notion that honeypots might be used to "trap" hackers. This idea might be seen as an attempt to trap someone. According to the law, entrapment refers to "the conception and planning of a crime by an officer and the procurement of its performance by one who would not have committed it but for the craftiness, persuasion, or deceit of the officers." Organizations or educational institutions cannot be accused of entrapment because this legal term solely pertains to law enforcement. The question of whether the attacker would have committed the crime absent "encouragement activity" is crucial to proving entrapment. International Journal on Computer Science and Engineering and intercepting of communication. Systems designed to be used by no one are called honeypots. They shouldn't be breaking any privacy regulations because they don't offer any user accounts or services of any type to the general public. Before using honeypots, one should also be aware of the various privacy rules in each country. There is some risk associated with honeypots. The administrators or researchers who employ honeypots are accountable for any security hazards they may pose. An administrator is accountable for every compromised system under his control as a result.

5. Role of Honeypots in Network Security:

Honeypots are one element in a comprehensive cyber security strategy, it is crucial to keep in mind. The honeypot will not sufficiently defend the organization against a wide range of hazards and threats if it is used in isolation.

Organizations can utilize honeypots, just like cybercriminals can. In an effort to divert attention from actual attacks on the legitimate system, malicious actors may flood the honeypot with intrusion attempts if they realize the honeypot is a ruse. Hackers may purposefully give the honeypot false information. This muddles the machine-learning models and algorithms used to analyze activities while maintaining their anonymity. In order to safeguard the company, it is essential to use a variety of monitoring, detection, and repair technologies as well as preventative measures.

Honeypots and related technologies have received a lot of interest over the last two years. The use of honeypots is one of the newest network security techniques currently accessible. Project Honey net's key priorities are the installation and examination of honeypots. Given how frequently honeypots are used in research, their use in production systems seems impending. [6]

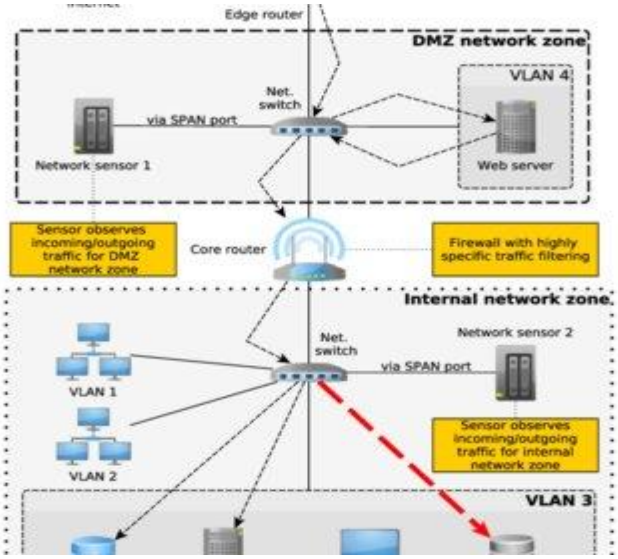
Edge router
DMZ network zone
VLAN 4
Net. switch
via SPAN port
Network sensor 1
Web server
Sensor observes incoming/outgoing traffic for DMZ network zone
Core router
Firewall with highly specific traffic filtering
Internal network zone
Net. switch
Network sensor 2
via SPAN port
VLAN 1
VLAN 2
Sensor observes incoming/outgoing traffic for internal network zone
VLAN 3

Figure 2 Approaches for Preventing Honeypot Detection and Compromise

6. Security of the gateway:

Since the gateway is the focal point of all administrative and monitoring operations, its security was of utmost importance. The newest updates were installed, and all services on the gateway were disabled aside from those that were strictly necessary. A secure shell server was set up on a non-standard port so that the gateway and firewall could be remotely managed. The system was made as secure as feasible by disabling any superfluous user accounts and services. Finally, Nessus, a potent scanner that aids in finding security gaps in a computer that hackers might exploit, was used to test it. Nessus produces comprehensive reports and graphs that can be read in html format. [2] and [7].

Attracting Hackers:

On a honeypot email list at securityfocus.com, a topic on "attracting hackers" generated a lot of thought-provoking responses. Many people appear to believe that simply placing a system online suffices and that there is no need to attract hackers. Additionally, attracting might not be a good idea because it could put the network's other computers' security at risk. It was agreed not to take any additional measures to draw hackers. In the honeypot community, luring hackers is a contentious subject. Many experts believe that a honeypot should never actively luring a hacker but, by definition, should passively wait for probes, scans, and attacks. In this thesis, the key honeypots that could have been accomplished were as follows:

- Having the honeypot connect to IRC networks, particularly those connected to hackers, will undoubtedly draw hackers. Some of the attacks are carried out directly through the IRC client.
- To check if you can provoke retaliation from known hackers, scan their networks from the honeypot. Although it exposes your network to threats like denial of service, this will undoubtedly draw them in.
- Last but not least, avoid installing unpatched software or patching known problems. You can capture script kids who just used an automated hack tool or heard about a way to hack into a system if it isn't patched.

7. Working:

The honeypot fools hackers into thinking it's a legitimate target by having the appearance of a real computer system, complete with apps and data. A honeypot could, for instance, imitate a business's customer billing system, which is frequently targeted by thieves looking for credit card details. Once the hackers are inside, it is possible to trace them and analyze their activity to find out how to safeguard the real network. Honeypots are made attractive to attackers by building in deliberate security vulnerabilities. For instance, a honeypot might have ports that respond to a port scan or weak passwords. Vulnerable ports might be left open to entice attackers into the honeypot environment, rather than the more secure live network.

A honeypot functions by acting as a purposefully weak spot in security. These devices often take the form of a virtual machine (VM) that has been purposefully compromised and installed in a reachable location on the network. These VMs frequently lack crucial security upgrades, have unprotected ports, and have needless services enabled that a hacker could use against them. A honeypot device will typically feature administrator accounts with no passwords or accounts with weak passwords, making it simple for an attacker to elevate their privileges. In contrast to a firewall or anti-virus, a honeypot isn't designed to solve a particular issue. Instead, it's a tool for information that can assist you in understanding current hazards to your company and recognizing the advent of fresh threats. The information gathered from a honeypot can be utilized to prioritize and concentrate security efforts. [3]

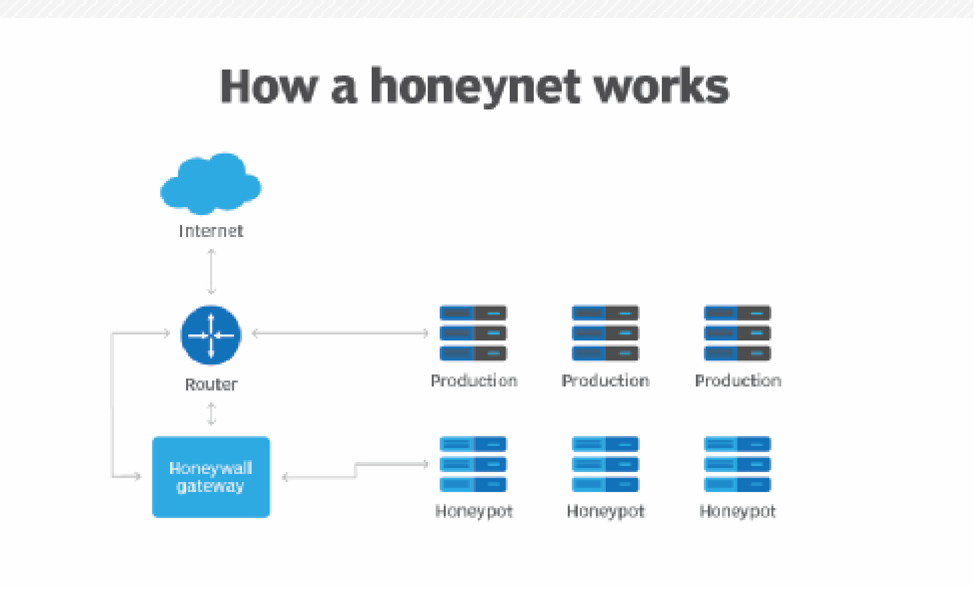

Figure 3 Working of Honeypot

8. Benefits of using Honeypot

Using honeypots is an excellent approach to find weaknesses in important systems. A honeypot, for instance, can demonstrate the serious threat that assaults on Iot devices pose. It may also make recommendations for methods to enhance security.

Comparing a honeypot to a real system to look for intrusions provides a number of benefits. For instance, a honeypot should never receive valid traffic, thus any activity that is recorded is almost certainly a probe or intrusion attempt. That makes it much simpler to identify patterns, such as the use of similar IP addresses (or IP addresses that are all from the same nation) to conduct network sweeps. In contrast, when you are focusing on enormous volumes of genuine traffic on your core network, such warning indicators of an attack are simple to miss in the cacophony. The main benefit of adopting honeypot security is that you might only see these malicious addresses, which makes it much easier to spot an attack.

Honeypots are also resource-light because they only handle a little amount of traffic. They don't place a lot of demands on the hardware, so you may set up a honeypot utilizing outdated computers that you no longer use. The amount of internal work required to set up a honeypot is further reduced by the availability of ready-written honeypots from internet repositories for software. [3]

9. Result

Despite the fact that the honeypots have never been penetrated and we have yet to witness a full infiltration, they have enough evidence to show that even modern systems are susceptible to attack. These honeypots provided no public benefits, and they were not promoted in any way either. They were concealed by a number of networks. If the honeypot was situated on a public ISP network, it would be more likely to be compromised. However, since your computers will unavoidably be checked, scanned, and attacked, it really doesn't matter where they are placed. The honeypots were in use for five months. Here, five months of logging's interesting and noteworthy results are discussed. No Internet-connected PC is impervious to probes, scans, and attempted attacks, as this clearly shows. Port scans typically occurred simultaneously on both honeypots, indicating the usage of scripts or other tools to generate the scans. The pertinent systems were the only ones that the exploit attempts were aimed at. For instance, the mod-SSL flaw was directed only at the Linux honeypot which was running apache. Despite being online for a shorter amount of time, the Windows honeypot experienced more connection attempts. There could be a number of reasons behind this figure. Windows is the most widely used operating system for personal computers. They are typically not patched or maintained properly, which makes them easy to exploit

10. Conclusion

We examined the idea of honeypots and how network security might benefit from them in this study. The idea of honeypots represents a big advancement in the security industry. A proactive method of intrusion detection and prevention is provided by honeypots. They also actively investigated problems with intrusion detection systems and the difficulties these systems encountered. They are particularly useful to system administrators as a training resource. On a personal and professional level, security precautions will be just as crucial as the Internet has been. Honeypot usage and related technologies are expanding. Honeypots will be used as a security technique in businesses more frequently as knowledge and interest about them grow. It is feasible to create honeypot tools that simplify the various tasks performed by honeypots, including logging and source tracing. A few items that could be improved are system modules for sophisticated keystroke logging, better filtering tools, and utilities to record encrypted communication. One might even consider an out-of-the-box honeypot distribution with a patched kernel to make honeypot deployment straightforward for system administrators.

References

[1]"Introduction / Background" https://www.imperva.com/learn/application-security/honeypot-honeynet/

Yasser Alosefer and Omer Rana, "Honeyware: a web-based low interaction client honeypot", Third IEEE International Conference on Software Testing, Verification, and Validation Workshops (ICSTW), pp. 410 – 417, 2010.

[2] Xiaoyan Sun, Yang Wang, Jie Ren, Yuefei Zhu and Shengli Liu, "Collecting Internet Malware Based on Client-side Honeypot", 9th IEEE International Conference for Young Computer Scientists (ICVCS 2008), pp. 1493 – 1498, 2008.

[3]"Working of Honey pot and Benfits"

https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot

https://hide.me/en/blog/what-is-honeypot/

[4] Jian Bao and Chang-peng Ji, and Mo Gao, "Research on network security of defense based on Honeypot", IEEE International Conference on Computer Application and System Modeling (ICCASM), vol. 10, pp. V10-299 - V10-302, 2010.

[5]"Types of Honeypot"https://logixconsulting.com/2020/06/22/production-vs-research-honeypots-whats-the-difference/

[6] "Roles of Honeypot" https://www.crowdstrike.com/cybersecurity-101/honeypots-in-cybersecurity-explained/

[7] Xinliang Wang, Fang Liu, LuYing Chen, Zhenming Lei, "Research for Scan Detection Algorithm of High-Speed Links Based on Honeypot", 2nd IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC), pp. 66-70, 2010.

[8] Anjali Sardana, R. C. Joshi, "Honeypot Based Routing to Mitigate DDoS Attacks on Servers at ISP Level", IEEE International Symposiums on Information Processing (ISIP), pp. 505-509, 2008.

[9] Babak Khosravifar, Maziar Gomrokchi, Jamal Bentahar, "A Multi-Agent-based Approach to Improve Intrusion Detection Systems False Alarm Ratio by Using Honeypot", IEEE

International Conference on Advanced Information Networking and Applications Workshops, pp. 97 – 102, 2009.