International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 06 | June - 2021 ISSN: 2582-3930

Network Security using Honeypots

A1: Amrutha M
3rd Year
MCA, Dayananda Sagar College of Engineering

A2: Prof.Alamma B H
Assistant Professor,
Dept of MCA,
Dayananda Sagar College of Engineering

Abstract- the main target of this document is on guaranteeing network security exploitation the popular network security tool, Honeypot. knowledge on malicious activity on the net and to raised understand the methods and techniques attackers use to compromise target systems. It' essentially a defense mechanism. solely hackers are caught, and also the different traditional folks might or might not stop them from connecting to it.

IndexTerms - Honeynet, Blackhats, Tracking Hackers

I. INTRODUCTION

There is tremendous growth in the network and in the connection of people who use the Internet. With the rapid growth of Internet technology, users can easily get their information and transfer messages quickly. The rapid growth of the Internet means that hackers will control the network using malicious code, system vulnerabilities, and program weaknesses if we do not also value basic network security. Attacks, theft and manipulation of information by hackers can then cause great damage and data loss also increases. This creates this security problem.Honeypot is a security mechanism configured to detect, redirect, and counter attempts at unauthorized use of information.

A honeypot is a resource that purports to be a real target. The main goal is either to collect data about malicious activity on the Internet and to improve understanding of the strategies and techniques that attackers use to compromise the target systems. They can be referred to as additional internet security systems and are an additional layer or system. Also, measures to reduce security threats like viruses, worms, and internet attacks, which are normal honeypots, are a security resource whose values have been attacked or compromised. Honeypots are highly flexible security tools with different security applications that do not solve a single problem. Instead, they have multiple uses, e.g. Information gathering, Prevention, Detection. An example of a honey pot system installed on a traditional internet security system.

The Honey Pot system is set up to make it easier for intruders, but with minor changes to the system, so your activities can be recorded or tracked. The general idea is that once an intruder breaks into a system, it will return for later visits. During these subsequent visits, additional information may be collected and additional attempts to access files, security, and system may be monitored and stored on Honey.

II. LITERATURE SURVEY

Yogendra Kumar Jain, "Honeypot-Based Secure Network System", International Journal of Computer Science and Engineering, ISSN: 0975-3397, January 2019.

Here the author explains the concepts of honeypots and their contribution to field network security. Mohit Arora “Different types of honey pots”

September 2015. Here the author explains the different types of honey pots.

III METHODOLOGY

Thanks to the Internet, which enables us to communicate in the world, the way we see the world has changed tremendously at the speed of light, but this ability to share details over the vast Internet gives intruders the opportunity to exploit other people's personal information and poses a threat to the nation. to the security of our entire nation. Honeypots are deception systems that are used to detect intruders or malicious activity.

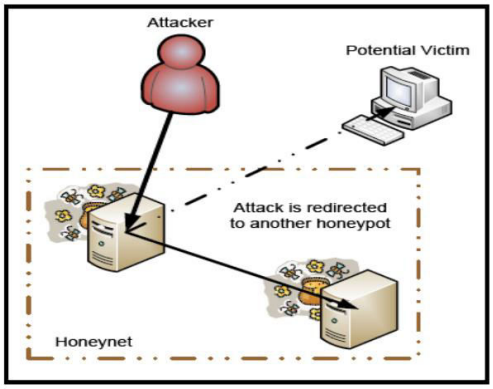

Fig. 1: Honeypot architecture

This is a fundamental process in which the attacker attacks a computer (potential victim) that is nothing more than a hack for hackers (honeypot) when many systems attack together. The attack is redirected to another honeypot network. as shown in figure.

IV.CLASSIFICATIONOF HONEYPOTS

1.Production honeypots

Production honeypots are placed by a company among the assembly network beside alternative production servers to boost their overall security status. it's placed below the production network to extend the general security of the company. Production honeypots function deception systems in entire networks associated servers, usually as a part of an intrusion detection system (IDS). In general, production honeypots are low-interaction honeypots that are easier to line up. they supply slightly less data concerning an attack or aggressor than analysis honeypots. These are simple to use. They collect solely restricted information and are principally utilized by corporations or corporations.

2.Research Honeypots

Research bait-collect a large amount of data, mainly for research, military or government organizations. Research bait is difficult to maintain and install. Collect information about the strategies and motivations of the attacker community against various networks. Research decoys because they have no direct value to any particular organization. Therefore, they are used to investigate the initiators of threats and to help us better protect ourselves from these threats.

V.LEVELS OF INTERACTION

1. Low Level Interaction

Low-interaction honeypots are services hackers impersonate with a restricted set of the practicality they'd expect a server to try and do with the intent of discovering sources of unauthorized activity. For example, the hypertext transfer protocol service provided on low-interaction honeypots would solely support the commands necessary to spot that a best-known exploit is being attempted. In addition, they replicate the services often requested by attackers. as a result of they use comparatively few resources, multiple virtual machines may be hosted on one physical system with none problems. quick response times and fewer code are required, reducing the quality of virtual system security.

2. Medium Level Interaction

Some authors classify 3 classes of honeypots, known as honeypots with medium interaction, as a result of they provide extended interaction over honeypots with low interaction, however not up to systems with high interaction solely offer partial implementation of services and typical and complete interaction with the system not thus powerfully enable interactive honey pots. you'll

implement the machine-readable text transfer protocol. Protocol have great deal of whole to emulate (set up) the implementation of a wide glorious businessperson like Apache.

3.High Level Interaction

In step with current researchers, the generation makes use of extraordinarily lively honeypots. victimisation digital machines, more than one honeypots is hosted on one bodily machine. however one some of the honey pots is compromised, others will nevertheless be used. These honeypots mimic the sports of actual structures that host a range of services, permitting the entrant to behave with the device as in any historic package deal to seize the most quantity of facts regarding the attacker' techniques. Extremely interactive honeypots, while offering plenty of protection due to they may be tough to spot, have the maximum downside that they may be extraordinarily expensive to maintain

VI.CLASSIFICATION OF HONEYPOTS

The honeypot classification is used to identify various threats. The various honeypots use the spam identity with applications and data, tricking cybercriminals into believing it is a legitimate target.

1. **Spam traps** are also known as email traps. The fake email address will not be used for any purpose, just to use the spam trap. It is 100% sure that all incoming email is spam. Some organizations involved in the fight against spam post specific email addresses on a website to encourage spammers to use collection software to collect and send spam email.

2. **The Decoy database** can be used to monitor software vulnerabilities and detect attacks that exploit an insecure system architecture or use of SQL injection, exploitation of SQL services or abuse of authorizations.

3. **Malware honeypot** is used to detect malware.The characteristics of the malware are analyzed in order to develop anti-malware software. The malware honeypot uses the known methods of spreading and attacking malware.

4. **Honey nets** can't produce a efficient net. The aggregate of honey networks and honey pots is used as a part of a bigger community intrusion detection. Honeynets gives a centralized series of honeypots and evaluation tools.

VII.NETWORK SECURITY ISSUES

There are many techniques in network security for detecting malicious users and abusing computer systems. Cloud computing is an evolving technology. Many companies are moving into the lump computing environment, but there are still some network security issues. To be safe, we need to find a new tool that needs to store data in a safe state. Virtualization plays a dominant role in the components of cloud computing. Provides virtual systems, hardware resource platform networks, and storage devices. The following security issues can potentially be resolved:

1. Cross Virtual Machine (side channel attacks): The attacker can attack via the side channels. The attacker receives information via the side channel. This information is lost due to the theft of the cryptographic key.
Possible solution: The security of the key if it contains the replacement method. It can beused withinside the key vicinity with ranges of safely generated as a one-time password (OTP).

2. Escape of the virtual machine: The Virtual Machine Manager (VMM) manages malicious data that the user can remove from the administrator, from whom he communicates directly with the host operating system.

Possible solution: If an unauthorized user tries to interact with the operating system host, the alarm is triggered. generates the manager. The alarm generates a popup message or an SMS warning.

3. Virtual machine rollback: Rollback gives users more flexibility. The virtual machine is reverted to its previous state. The previous status cannot be static. If the user provides a reset command, the previous state is disabled. Possible solution: This status always checks whether the previous status is correct, if it is correct the user can check this status**.**

4. Sharing virtual machine images: In this state, the attacker is using a thread that resides in the image and is forwarded to others. As a result, data can be corrupted or leaked in a variety of ways.
Possible solution: Share any image. Be vigilant and security functions should be incorporated into the cryptographic technique for data encapsulation. Encapsulate the image as text and then share it.

5.Virtual machine isolation: A single virtual machine contains more than one virtual machine and has its own guest operating system. If one operating system fails, the user can use another operating system.
Possible system: The virtual machine on a single system must be protected from independently with antivirus so that the sharing of hardware resources does not affect other virtual machines.

6.Virtual Machine Migration - The host virtual machine can migrate from one system to another. It consists ofa cold migration that actions the digitalsystem from one factsmiddle to another.
• Another important issue is that the suspended virtual machine can migrate the virtual machine's suspension to different data centers.VMotionpermits switching from a powered-on digitalgadget to a brand new host system.VMotion moves the configuration storage from the hard disk or virtual hard disk.
Possible solution: In this process security is provided at all levels. In addition, the entire process is migrated while it is not in an inactive state so that the attacker cannot benefit from it.

A.ANALYSIS OF ALGORITHM

Here we have a new algorithm in the cloud computing platform that has been developed. Every technology has to save the data. The stored data must be protected with a good security system. Data security is difficult when computing in the current cloud.
Network due to the emerging attack of an intruder that is difficult to track There are various threats in the cloud computing environment: DDos (Distributed Denial of Service), DNS hijacking, information leakage, data loss, etc. The hacked data can be hacked using the Scan Fingerprint App User ID, Password, and One-Time Password (OTP). If you fix some of the network security problems, you have a possible solution, such as: B. a pop-up message or an SMS warning message that must be sent to the registered phone number Protected with the double security cryptographic method. The cryptographic method can be used at the firewall network level. It protects the data with double security protection for the network (see Fig. 1).

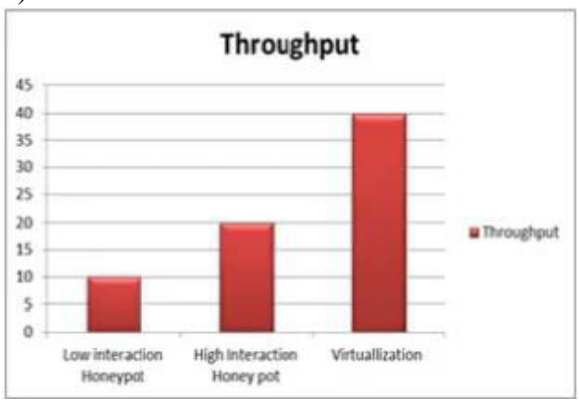

Fig. 1: This graph shows the performance for various forms of virtualization and Protea cynaroides techniques.
Displays performance virtualization and honeypot types. Little interaction from honeypots deals with the minimal system by which the system degrades performance. Highly interacting honeypots require maintenance to ensure system security, and

security is degraded, which affects performance. We will try to work on all factors such as cost, safety and maintenance. It will be complex, but performance will increase.

B.EXPECTED OUTCOME

According to our proposed algorithm, the system triggers any hacking attack that can gain deeper access to the data. With this penetration method, the administrator can continuously monitor the hacker's tricks and protect him by implementing various techniques. To ensure the authenticity of the data through honeypot, various types of honeypot techniques record the activities swept. Using table 1, we have various honeypots and virtualizations of our algorithm to get an overview.

Parameters	Low Interaction	Medium Interaction	High Interaction	Virtualization
Cost	NO	NO	YES	YES
Maintenance	NO	YES	YES	NO
Security	NO	YES	NO	YES
Complexity	NO	NO	NO	YES

Table 1: This table shows the different techniques according to the parameter.

The low-interaction honeypot has a minimal system requirement: it must be a small and manageable network and it must be protected. They do not save any real data in the network. In the middle honey pot, the interaction is a combination of low and high interaction.

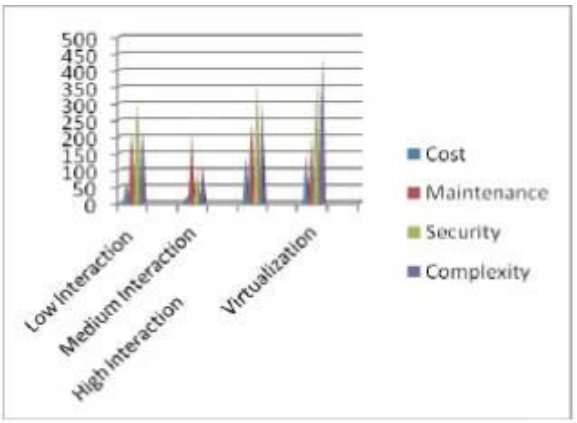

Figure 2: Graphical representation shows the different types of honeypots and the effects of parameter virtualization.

Honeypots in which the attacker has no direct communication with real data. With high interaction, the requirements on the honeypot system are high, require maintenance and the costs are also high. In Figure 2 are the effects of factors such as cost, safety, maintenance of these techniques may increase. Work efficiency. The virtualization algorithm works on Cloud-SIM, KF-Sensor etc. because the exit from the virtual environment will be desirable.

VIII. Conclusion

Like all technologies, honey pots have their drawbacks, the best of that is their restricted field of vision. Honeypots solely track activities directed against them and lose attacks against alternative systems. For this reason, security specialists don't suggest that these systems replace existing systems. Instead, they see honeypots as a complementary era to host- and network-primarily based totally intrusion protection.The advantages that honey pots give for intrusion protection solutions are onerous to ignore, particularly currently that production of honeypots begins in production. Over time, as deployments become a lot of prevalent, honeypots might become an integral a part of an enterprise security process.

IX. References

1. Big/ip: http://www.bigip.com/bigip/
2.HoneypotProject: http://www.honeypot.org
3. Tekerek M., “Bilgi GüvenliğiYönetimi”, KSÜ Fen veMühendislikDergisi 11(1), s. 132, 2008.
4. CSI/FBI Computer Crime and Security Survey. http://www.gocsi.com/forms/fbi/pdf.jhtml
5. Paul Innella and Oba McMillan. An Introduction to Intrusion Detection Systems. http://www.securityfocus.com/infocus/1520
6.SnortWebsite. http://www.snort.org/about.html
7. Lance Spitzner. Definitions and Value of Honeypots. http://www.tracking hackers.com/papers/honeypots.htm