International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 01, January-2023

Honeynet Security Systems for Shielding Intrusions in Networks

Shreedevi Pramod
Department of Computer Science and Engineering,
Brindavan College of Engineering,
Dwarkanagar, Bagalur Main Road, Yelahanka, Bengaluru,
Karnataka-560063

***Abstract*:- One of a network's key components has been security, particularly server-level server security. The necessity to create a system that can identify threats from parties without authorization (hackers) is caused by these issues. A honeypot is a device used to divert intruder's attention so that they believe they have broken into a network and are retrieving crucial data when, in reality, they have only reached an isolated place. A technique for stopping or prohibiting the use of unapproved effort in an information system. An example of a honeypot is a honeyd. Compared to kinds with high interaction, Honeyd is a honeypot with low interaction, which means the risk is lower. While using the honeypot, the actual system is not directly affected. The aim of installing a honeypot and firewall is why a Mikrotik firewall is utilized and can be used as an administrative tool to view reports on Honeyd generated activity, and administrators can view reports that are recorded in the logs to help establish network security policies.**

Keywords: Honeypot, hacking, security, forensic analysis of honeypots, network.

INTRODUCTION

In the field of intrusion detection technologies, honeypot devices are frequently employed. A honeypot is a system that is used to lure attackers, intruders, and malicious users away from the primary systems. The objective of honeypots is to divert attackers away from crucial systems while gathering crucial data about their nefarious activity. A honeypot is first and foremost a computer system. Like a real computer, it has files and directories. However, the computer's goal is to draw hackers in so that users may see and track their behavior. Therefore, it might be described as a phoney system that imitates a real system. The system frequently has event logs and monitors. All accesses and activity to the honeypot are tracked by this device [1]. This makes anyone who accesses the honeypot a suspect. Honeypot can be compared to a trap because it is intended to catch the enemy. The honeypot's entire data set is documented. These records are examined to discover new attack trends that endanger crucial resources. The effectiveness of honeypots and the issues they aid in solving depends on how you create, implement, and use them. If a honeypot is not assaulted, it serves no use. Figure 1 depicts a honeypot system.

Specifications of Honeypot Systems:

1) Honeypots are important in thwarting attacks and malicious actions.
2) It increases response and assault detection times.
3) It extracts the attack methodologies, system behavior, and intrusion behavior profiles.
4) It catches the adversary's behavior patterns in the act.
5) It keeps track of all the Intruder's activity.
6) They can be physically deployed or can be virtually set up.
7) There should be no false alarms in honeypots.

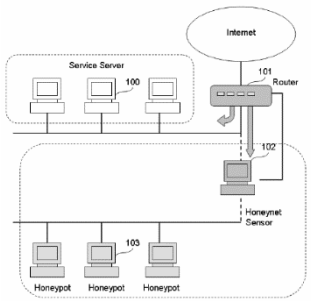

Figure 1: Honey pot systems

Using honeypots, valuable data is gathered. It collects accurate information that is simple to comprehend. This makes data analysis simple. A system or computer that has been "sacrificed" so that hackers might attack it is known as a honeypot. The computer facilitates each hacking attack carried out to breach the system. This technique aims to educate the server administrator on hacker infiltration techniques so that they can foresee them and prepare to secure the real system [2]. Any action done by a hacker

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 01, January-2023

attempting to connect to the honeypot will be discovered and recorded by the honeypot. A honeypot is a repository for information systems that is typically built to trap and notice attempts to break into the system. The honeypot often consists of machines, data, and network components that resemble Additionally, honeypots offer a monitoring feature to keep an eye on any intrusions by attackers. Ports being attacked, attackers typing instructions, and attackers altering a honeypot server are all examples of known actions.

The network administrator can use this as input to patch the system and set up the original network section for early detection. It is suggested that a distributed system be used to address the current weakness in the centralized control system and show experimental findings that successfully enhance the performance of safety defence systems [3]. The limitations of firewall technology, several intrusion detection systems, and intrusion prevention systems, which could detect previous attacks but not new ones, have mostly been addressed by the usage of honeypot technology. The present study discusses honeypot technology in light of the existing gap in the honeypot system and suggests a distributed system to address the shortcoming in the centralized control system to enhance network security. It also presents experimental findings that successfully enhance the performance of the safety defence systems. Unlike other security measures, honeypots do not experience resource exhaustion [3].

MATERIALS

They only collect information aimed at them, which explains why. Less money will be needed to purchase the gear necessary to install honeypots as a result. They cost a lot less because they don't need modern hardware like disc drives or RAM with a lot of space. Since they don't need complex configurations or algorithms, they are simple. In addition, using them is much simpler. What we need to do is just deploy them and monitor. The ability to immediately catch malicious activity makes honeypots very valuable. It illustrates the degree to which the system has security mechanisms. While there is a chance that some false positive alarm messages from different security systems will be sent, honeypots won't because intruders access them most often. Honeypots also assist in understanding a variety of new vulnerabilities, threats, and attack tactics.

RESULTS

Honeypots were designed after studying them at various levels of contact. Honeyd was used to install honeypots at the initial level of engagement, the reasoning behind it and correctly implementation was provided. Results obtained on Honeyd revealed that while it is the most appreciated, low-interaction honeypot, but its age is a concern. The project is open source, however some of it needs to be upgraded and nobody seems to be doing so. However, as hacker tools advance, it is simple to spot this honeypot. By utilizing a more recent version of Nmap, the false operating systems will not be identified as Honeyd uses an older version of Nmap's fingerprint to generate phoney virtual operating systems, and Nmap will identify that there is a problem. The scripts that are tied to various ports are another restriction of Honeyd. It is possible to determine which ports are open with a simple scan, but the attacker will quickly understand the service is false once he tries to connect on a port. The script for a Web server, for instance, should be sending back responses when connected through telnet, but nothing is. Another issue is that it is impossible to tell whether or not the system is under assault. mainly due to the absence of an alarm system that may alert you to an attack. It's also not very sensible to acquire information. The hacker will stop the attack as a result of being able to recognize the target's issue promptly. Without investing a lot of time, even inexperienced burglars might breach the honeypot. due to the fact that well-known techniques like Nmap are simple to use and widely popular. It can be done without using any additional strategies. The medium level interaction honeypot Nepenthes configuration was our next step. In the implementation phase, we described how it functions and how we researched it. However, we also discovered several issues with Nepenthes. Nepenthes is first and foremost used to catch malware online. It mostly serves this purpose. Since risks to internet users are growing dramatically every day, it must be deployed extremely quickly. New threats were too fast for Nepenthes to handle. Nepenthes won't be able to detect malware as new threats emerge and it is out of current. The shellcode also causes an issue. Shellcode managers need to think about and comprehend shellcode.

New exploits also cannot be captured since new threats cannot be. Additionally, a significant has come out while we are examining the issues and security weaknesses in our experiment. Nepenthes structure has security issues. Transport layer security is not available on nepenthes. A protocol called "transport layer security" provides security for internet-based communications. To deploy honeypots, we believe it to be a serious issue. Malware such as "LSASS, PNP, DCOM, ASN1, ms06-070, and ms08-067" are present on port 445 and are interconnected with one another. It was not sure about the responses either when this kind of interference occurs. The space between modules is left in a large mess.

CONCLUSION

Observing the attacks, honeypot is successful in detecting suspicious activity, capturing the attacker's IP, and is stored in a separate folder on the server trap honeypot. As of this writing, the author has come to the conclusion that the honeypot and firewall can cooperate in restraining the incident that occurred so the attacker can't enter easily because the attacker into the trap honeypot that has been made. Like other technologies, honeypots have some downsides, with their small field of view being the biggest. According to some researchers, honeypots only record activity that is directed at them and miss attacks against other systems. Security professionals advise against using these systems to replace current security solutions because of this. Instead, they view honeypots as an addition to host- and network-based intrusion protection. Particularly now that production honeypots are starting

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 01, January-2023

to be deployed, it is difficult to dismiss the benefits that honeypots bring to intrusion-protection solutions. In the future, as deployments increase, honeypots might be a crucial component of a security operation at the corporate level.

BIBLIOGRAPHY

[1] https://www.knowledgehut.com/blog/security/honeypot
[2] Liu Dongxia, Zhang Yongbo, (2012). "An Intrusion Detection System Based on Honeypot Technology", In the Proceedings of 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE2012), Hangzhou, pp. 451-454.
[3] Maheswari V. & Sankaranarayanan P.E. (2007). Honeypots: Deployment and Data Forensic Analysis, International Conference on Computational Intelligence and Multimedia Applications.
[4] McFarland B. (2005). Ethical Deception and Pre-emptive Deterrence in Network Security GCFW Practical Version 4.1, SANS Institute 2000-2005.
[5] Yu Zheng., Zheng Li., Xialong Xu and Qingzhan Zhao (2022) Digital Communications and Networks, 8(4), 422-235.