HONEYPOT FOR SECURITY SYSTEM

AUTHORS:

M.Sumithra[1a],P.Ramaguru[2b] M.VarunKumar[2c],S.VigneshKumar[2d],V.Vetrivel[2e], R.SanthaKumar[2f]

[1]Assistant Professor, Department of Information Technology, Panimalar Engineering College

[2]II-Year Students, Department of Information Technology, Panimalar Engineering College

ABSTRACT:

Our security system suffers as a result of the ongoing rise in online attacks. Having a security system that can recognize and prevent zero-day attacks is essential to lessen this threat. A network's resources are set to monitor and record new threats as part of the proactive protection technique known as a honeypot. The intrusion detection systems (IDS) concept proposed in this research uses honeypots to gather user information about the attacker. We evaluated Honeypots' potential and its bounds, and we also found several areas that still needed work. In the future, we want to capitalize on this trend by acting early to avoid damage to our security system by taking preventive measures.

KEYWORDS:

Honeypot, Honeycomb, Honeynet, IDS, Load balancer, and Honeywell Security and protection.

1. INTRODUCTION:

People can readily retrieve their information and send messages swiftly thanks to the internet's rapid development
in technology. But, because of how quickly the internet is expanding, if we don't prioritize basic network security at the same time, hackers will be able to take control of the network using malicious code, system flaws, and software
weaknesses. Hence the hacker assault, destruction, theft, and manipulation of information may result in tremendous harm. For personal or educational use,
permission to create hard or digital copies of all or parts of this work is allowed without charge, provided that copies are made and disseminated without this notice and the complete citation on the first page. A computer system that has been set up to be compromised to gather information on black hats is called a honeypot. A honeypot is similar to any other computer system in that it has discs and folders just like actual computers do, but it serves a very distinct and separate purpose. Only white and black hats are known for using genuine systems in this way. Risk cannot be eliminated, but security may help organizations manage risk and safeguard their precious assets. A honeypot is an information system resource whose value lies in the unauthorized or illicit use of that resource. There are several things to note. As previously mentioned, honeypots add a layer of security rather than replacing any of the conventional security measures. It won't stop assaults. Attacks on genuine systems are diverted, and information about the attack is gathered. A honeypot, however, only detects offenses against itself. Some systems will be fully unaffected by attacks.

2. LITERATURE SURVEY:

LANCE SPITZNER we examine new developments in the honeypot. There has been a discussion of a few noteworthy ideas and their analyses. The advantages and disadvantages of using honeypots in mixed environments with IDS in education have been discussed. We also describe the use of the signature method in the honeypot for traffic analysis in this paper. We conclude by summarising each of these elements.

Dantu suggested a brand-new design that locates worms by keeping track of the frequency of their outgoing links. By restricting the rate at which new outgoing connections are created using a closed feedback loop control, the new architecture slows down the worms.
This work's main addition is in the planning,

The closed-feedback loop control for throttling outbound links needs to be tuned and performance tested. Dantu used the Proportional, Integral, and Derivative (PID) algorithm, which limits outgoing connections to a predetermined set point to prevent worm outbreaks.

Fairbanks order to get around a limitation in data gathering within the Linux Virtual File System (VFS) and potential file changes by attackers, Fairbanks suggested a novel approach. The drawback is the failure to distinguish file names from inodes. Since their links are unidirectional, it is difficult for forensic studies to easily identify the file names that iinodestriggered some warnings for potential security irregularities. (only from filenames to their inodes). By changing the VFS code in the Linux kernel, the suggested solution eliminates the issues by allowing the kernel to save a data structure known as "entry" that includes the reverse link from an i-node to its filename. Dentry saving via USB to a distant file

3.T TYPES OF HONEYPOTS:

Honeypots can be divided into two categories: production and research. Production honeypots are designed to detect internal network intrusions and deceive any malicious actors. Production honeypots are placed next to your actual production servers and use the same services as those servers.

3.1 RESEARCH HONEYPOT:

These honeypots are only utilized in research settings. Giving the black hats complete access to breach and infiltrate the security system is the main goal in this situation to learn as much as possible about them. It is simple to learn about the tools used and other relevant information about black hats by giving them such access.

3.2 PRODUCTION HONEYPOT:

This kind of honeypot is intended to safeguard businesses against malicious behavior carried out by black hats. To improve the company's overall security, this honeypot is positioned underneath the production network.

3.2.1 PREVENTION:

From a business standpoint, they are only interested in their security in this case and have little desire to learn about black hats. They thus install firewalls, employ strong passwords, experiment with encryption methods, use digital signatures, and issue digital certificates, in addition to offering well-known security services. They merely take these actions to keep black hats from accessing their precious resources.

3.2.2 DETECTION

As prevention doesn't always work, an intrusion detection system is another option for preventing attacks. This technology will enable us to determine whether or not the system has been compromised, but it won't stop hackers from assaulting the system.

3.3 BASED ON INTERACTION:

- **LOW INTERACTION HONEYPOT:**

  These honeypots only communicate with external systems to a limited extent. An illustration of this kind of honeypot is FTP. Attackers cannot interact with an operating system, but they can use software to mimic the functionality of an operating system and network services on a host operating system to create targets to attract or detect attackers. The key benefit of this kind of honeypot is that it doesn't require any complicated architecture and is very simple to set up and maintain. There are several disadvantages to this system in addition to this benefit. In other words, it won't react to threats correctly. As a result, it is more difficult to assist in the identification of fresh vulnerabilities or attack vectors.
- **HIGH INTERACTION HONEYPOT:**

  This honeypot is the most sophisticated. A very high level of interaction between this kind of honeypot and the intrusive system exists. It provides a more authentic experience.

  This poses a very high chance of the entire honeypot being captured by the attackers and provides more information about potential attacks. The most difficult and time-consuming to manage and develop are high-interaction honeypots. High-interactive honeypots are more helpful when we wish to record the specifics of vulnerabilities or exploits that are not yet public knowledge. In the event of "0-Day attacks," this honeypot is the greatest option. Using honeynets as an illustration, which are frequently utilized for research.

- **MID-INTERACTION HONEYPOT:**

  Also called mixed-interactive honeypots, these are. Low-interaction honeypots are less advanced than medium-interaction honeypots, which are more advanced than high-interaction honeypots. It gives the attacker a more convincing impression of the operating system so that more sophisticated attacks may be recorded and examined. One example is Honeytrap, which handles some unidentified threats by dynamically creating port listeners depending on TCP connection attempts taken from a network interface stream.

3.4 ADVANTAGES :

1. Honeypots are set up just to collect data on attacks as they are noted in log files.
2. As they are the only ones who are aware of the honeypot, black hats are the ones that target it.
3. Since honeypots are only intended to collect a particular type of data, such as malicious traffic, they are not very large.
4. Honeypots give us knowledge about recently developed assaults and technology.
5. Honeypots are straightforward to set up. They don't use sophisticated algorithms.
6. In addition to catching fraudulent communications, honeypots also catch new tools employed by black hats.
7. Honeypot also picks up some misleading negative and positive data.

Honeypots have a wide range of uses since they can be used to block harmful traffic from reaching crucial systems, detect attacks in progress before they affect essential systems, and gather intelligence on attackers' tactics.

4. APPLICATION:

The honeypot application domains are covered in this section. Its implementation, use with IDS, and applicability in educational settings are all covered in this article.

4.1 HONEYPOT ON THE INTERNET

The honeypot project tracks genuine Internet computer intrusions. Their most recent findings show that a random PC is checked numerous times each day. A program known as a honeypot is a closely scaled compartment designed to attract an attacker and effectively divert them away from production systems for conversion investigation. It can take the shape of enticing services, an entire OS, or even an entire network. Here, a honeypot keeps track of every log file and every attack-related action.

There are several social problems associated with honeypots, such as the problem of entrapment, wherein the system cannot be accessed implicitly by an attacker who has been attracted to the honeypot on purpose. On a honeypot, viewing files and intercepting communication like chat or email are both prohibited by privacy laws. As no authorized account or privileges exist, the attacker's data are not secured. Even while there is case law on the loss of the right to privacy when storing data on a stolen computer or data on a hacked computer without the owner's consent, there is little to no case law on intercepting conversations transmitted through a compromised computer.

4.2 DEPLOYMENT OF INTRUSION DETECTION SIGNATURE

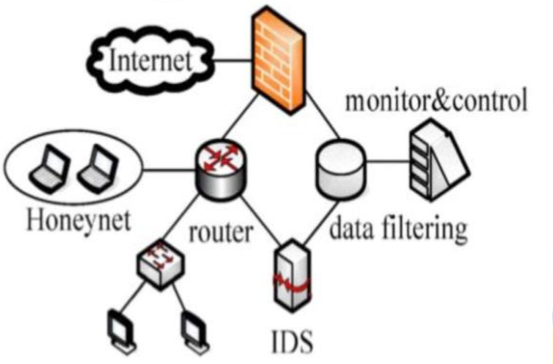
This phenomenon typically has to do with signature generation. At the moment, creating signatures is a laborious manual process that necessitates in-depth familiarity with each programmed function that is intended to be held. Very detailed signatures result in false negatives whereas overly simplistic ones frequently provide significant numbers of false positives. The idea of Honeycomb, a system that automatically creates signatures for malicious communication, is applied for the same reason. Here, compliance tests on traffic recorded by honeypots use pattern detection algorithms and packet headers**.**

The discussion of attack signatures is meant to clarify the distinctive components of assaults. Currently, there is no such standard for specifying these signatures. Because of this, several systems offer signature languages with variable expressiveness. A strong signature needs to be both flexible and specific enough to capture several iterations of the attack while also containing the distinctive elements of the exploit it aims to address. Either a failure in one area or another result in a significant number of false positives or false negatives.

The system only supports signatures for the Bro and Snort NIDSs in this way. Through the use of regular expressions, the inclusion of traffic moving in one way, and the encoding of attacks with many stages, Bro has a controlling signature language. The signature language of Snort is currently less expressive than that of Bro. As a result, Snort is included here due to its current reputation and big signature repository. Here, a popular open-source honeypot for low-level interactions called honey is extended. In Honey, hosts are simulated using persona networking personas. It exploits the imitation systems to reply to traffic directed to nonexistent hosts, interrupting it. In terms of operating systems and active network services, each host can be individually customized.

4.2.1 ARCHITECTURE OF HONEYCOMB

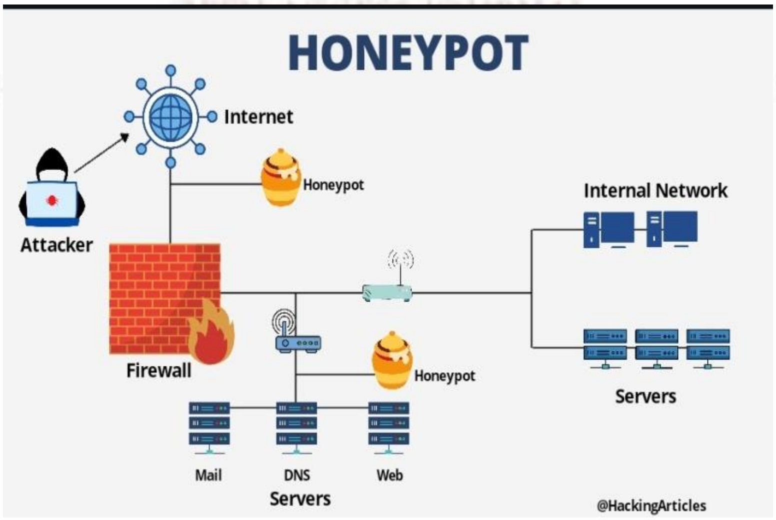
Here, a plug-in infrastructure and event callback hooks are two brand-new ideas that have been added to Honey. The plug-in technology enables us to create extensions that are logically distinct from the honey code base. Hooks provide a way to integrate the plug-in into honeypot activities during event callbacks. At the moment, hooks enable a plug-in to be informed when packets are received and delivered, when data is passed to and received from the subsystems, and when changes are available regarding the connection state of honey. A honey plug-in is used to implement Honeycomb. as displayed below.



IMPLEMENTATION OF HONEYPOT?

A honeypot is typically installed in the demilitarized zone (DMZ), a remote area of the network. Web and mail servers, among other public-facing services, are situated in the DMZ, which is connected to the internet. The corporate network and the sensitive data that is kept there are separated from the DMZ by a firewall. Consider the DMZ as a safe buffer zone between private networks and the internet. It allows traffic into the network while still securing its most crucial components.

On fake servers within the DMZ that the invader thinks are real are placed honeypots. They employ standard protocols and realistic methods. They sometimes use fictitious statistics to appear more convincing. For instance, Honeypot might mimic a false server with fictitious credit card information or files that look like they contain it from the outside. The honeypot simulates all of the typical limitations, access control processes, and protocols that a real network would have to maintain the security of the data.



RESULT:

The value of a sinkhole is in the information it collects about the styles and geste of bushwhackers while the bushwhacker believes they are not being watched. Other network monitoring tools, similar to intrusion discovery systems(IDS), do not give the same position of information as a sinkhole. For case, an IDS observers networks to identify suspicious exertion, shoot out cautions, and stop bushwhackers as fast as possible. While an IDS does collect and dissect information about bushwhackers, that is not its main purpose. Attack patterns linked. Security experimenters, merchandisers, businesses, and other associations can use the information a sinkhole generates to uncover patterns in the way cyber bushwhackers operate and also acclimatize their products and strategies to fight the attack. Vulnerabilities to be renovated. Businesses can use honeypots for network surveillance and defense and to identify vulnerabilities that need to be renovated.

CONCLUSION:

Honeypots are positioned to emerge as a crucial tool for protecting business networks from hacker intrusions.It serves as a means of spying on your adversary and may even serve as concealment. When lurking in a honeypot, hackers could be persuaded to believe they have gained access to a business network while the real network is kept secure. Honeypots have become a key component of businesses' overall intrusion security strategies. Security professionals advise against replacing current intrusion detection security solutions with these systems; instead, they view honeypots as complementary tools to network- and host-based intrusion defense.

REFERENCE:

[1] M. Sumithra and Dr. S. Malathi, " honeypots in cybersecurity ", International Journal of Imaging Systems and Technology, Vol. 31, Issue No.1, pp. 223-235, 2021

[2] K. Sridharan , and Dr. M. Chitra "SBPE: A paradigm Approach for proficient Information Retrieval , Jokull Journal" , Vol 63, No. 7;Jul 2013

[13] M. Sumithra and Dr. S. Malathi, “honey pots survey”, International Journal Of Curent Research and Review, Vol. 13, Issue 12, 2021.

[4] B.Buvaneswari and Dr.T. KalpalathaReddy,“honeypots and architecture survey ,ISSN : 1674-0440,Vol.46,No.1,Pp.525-528,2019.

[5] K. Sridharan , and Dr. M. Chitra "Web Based Agent And Assertion Passive Grading For Information Retervial", ARPN Journal of Engineering and Applied Sciences, VOL. 10, NO. 16, September 2015 pp:7043-7048

[6] M. Sumithra and Dr. S. Malathi, “Segmentation Of Different Modalitites Using Fuzzy K-Means And Wavelet ROI”, International Journal Of Scientific & Technology Research, Vol. 8, Issue 11, pp. 996-1002, November 2019.

[7] M. Sumithra and S. Malathi, “ A Survey of Brain Tumor Segmentation Methods with Different Image Modalitites”, International Journal of Computer Science Trends and Technology (IJCST) – Vol. 5 Issue 2, Mar – Apr 2017

[8] B.Buvaneswari and Dr.T. Kalpalatha Reddy, “High Performance Hybrid Cognitive Framework for Bio-Facial Signal Fusion Processing for the Disease Diagnosis”, Measurement,ISSN: 0263-2241, Vol. 140, Pp.89-99,2019.

[9] M. Sumithra and Dr. S. Malathi, “A Brief Survey on Multi Modalities Fusion”, Lecture Notes on Data Engineering and Communications Technologies, Springer, 35, pp. 1031-1041,2020.

[10] M. Sumithra and S. Malathi, “A survey on Medical Image Segmentation Methods with Different Modalitites”, International Journal of Engineering Research and Technology (IJERT) – Vol. 6 Issue 2, Mar 2018.

[11] B.Buvaneswari and Dr.T. KalpalathaReddy,“ELSA- A Novel Technique to Predict Parkinson's Disease in Bio-Facial”,International Journal of Advanced Trends in Computer Science and Engineering, ISSN 2278-3091,Vol.8,No.1,Pp. 12-17,2019

[12] K. Sridharan , and Dr. M. Chitra , Proficient Information Retrieval Using Trust Based Search On Expert And Knowledge Users Query Formulation System, Australian Journal of Basic and Applied Sciences, 9(23) July 2015, Pages: 755-765.

[13] B.Buvaneswari and Dr.T. Kalpalatha Reddy, "ACPT- An Intelligent Methodology for Disease Diagnosis",Journal of Advanced Research in Dynamical and Control Systems,ISSN : 0974-5572,Vol.11,No.4,Pp.2187-2194,2019.

[14] Sumithra, M., Shruthi, S., Ram, S., Swathi, S., Deepika, T., "MRI image classification of brain tumor using deep neural network and deployment using web framework", Advances in Parallel Computing, 2021, 38, pp. 614–617.

[15] K. Sridharan , and Dr. M. Chitra "RSSE: A Paradigm for Proficient Information Retrieval using Semantic Web" , Life Science Journal 2013;10(7s), pp: 418-425