IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12358

Honeypot for Monitoring the Network

Rishav Baid [1], Mir Aadil [2]

Masters Student, School of CS & IT, Jain University, Bengaluru, India[1]

Assistant Professor, School of CS & IT, Jain University, Bengaluru, India[2]

Abstract: A security tool is called a honeypot help to spot and stop unwanted behavior on a computer or network. In essence, it is a trap that is set up to entice attackers by simulating weak systems or sensitive information, and then watching and analyzing their behavior. A honeypot's objective is to acquire details about the methods, tactics, and techniques used by attackers so that the network's overall security can be enhanced. In addition to identifying and isolating compromised systems, honeypots can be used to divert attackers away from more valuable systems. Security experts and researchers utilize honeypots to better understand the tactics and motives of attackers. They are able to acquire data that will help strengthen network security, as well as to detect and monitor novel sorts of threats. There are various kinds of honeypots, such as low-interaction ones that just imitate a tiny section of a system and high-interaction ones that simulate an entire system. Low-interaction honeypots are frequently simpler to install and keep up, but they reveal less about the attacker's activities. On the other side, high-interaction honeypots offer more comprehensive data but demand more resources and are more difficult to set up and manage. In general, a honeypot is a useful tool for enhancing network security and guarding against cyberattacks.

IndexTerms – Honeypot, sockets, TCP, UDP Honeynet, Honeywall, Intrusion Detection

I. INTRODUCTION

This security system is perfect for keeping an eye on your network and safeguarding your data from malicious activity and illegal access; it will also alert you of the attacker's details. We will first examine what a honeypot is and how it functions in order to get a better knowledge of it. A potent network surveillance tool is called Honeypot. During the network administrator's absence. Honeypot is separated into three subcategories that serve its aim. "Honey net" is another name for a honeypot. This software uses the digital signature of data flow to identify different security threats and attacks. It is not thought to be completely proof, though, as other anti-honeypot technologies can also detect it, or another bypassing tool can utilize it to go around it. Today's honeypots are widely employed in the forensic, cyber, and research fields. Denial of service (DoS) assaults, malware, and phishing attempts are just a few of the attacks that can be found using honeypots. Additionally, they can be used to identify and monitor advanced persistent threats (APTs), which are persistent, targeted attacks intended to steal confidential data.

There are so many various types of honeypots, ranging from simple, unreliable ones that just pretend to provide the most basic services to complex, high-interaction ones that pretend to be operating systems and networks in their entirety. Some honeypots also come equipped with the capacity to log and analyses the attacker's activities, including keystrokes, network activity, and malware samples. One of the key benefits of installing a honeypot is that it provides security teams with an early warning system. If an attacker tries to target a honeypot, the security team is alerted right away, and they can then take the appropriate action, such as isolating the offender, gathering and examining evidence, or enhancing the organization's general security posture. It's crucial to keep in mind that honeypots shouldn't be utilized in place of firewalls, intrusion detection systems, or antivirus software. Honeypots should be thought of as an additional security mechanism that works in conjunction with these current security measures.

The conventional strategy for information security has been a defensive one over the years, but new tactics that are more aggressive in nature seem to be a complement to the current approaches. The most recent state-of-the-art option uses a variety of honeypots that are typically grouped into honeynets or honeyfarms in order to aid security professionals in learning from attacks and enhancing the security of their systems. The purpose of this thesis is to provide an overview of the features offered by such systems, an introduction to the world of honeypots, and an explanation of the theoretical underpinnings of such systems. In addition, this paper will go over how a standalone honeypot software solution developed as part of this effort was implemented. The honeypot framework will upgrade the present options and give the Honeyd framework new capabilities. Computer security is a subject that is developing quickly in the age of information and technology. The threat environment has changed recently at the same rapid rate as the number of interconnected systems. The need for better early warning detection systems and better countermeasures that stop adversaries from accessing computer systems has grown as the number of sophisticated attacks on computer networks has risen.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023
DOI: 10.17148/IJARCCE.2023.12358

II. LITERATURE REVIEW

It became clear that the study of Honeypot can be categorized into four main areas: utilizing honeypot output data to improve threat detection accuracy, configuring honeypots to reduce the cost of maintaining honeypots while also improving threat detection accuracy, preventing attackers from detecting honeypots, and legal and ethical issues surrounding the use of honeypots. Honeypots have undergone numerous changes since they were first introduced at the end of the 1990s in order to deal with the numerous new security dangers that affect both experienced Internet users and security defenders. A new poll was focused specifically on the most current obstacles to and advancements in honeypots, was necessary due to the recent changes, which have been sufficiently quick to affect hardware, software, and even user demographics. (Bringer, M. L. et al., 2005)

In 2016, more than 1.966.324 virus warnings were found, according to Kaspersky Lab, in an effort to steal money by using online access to bank accounts. In addition, the ransomware malware affected 753.684 distinct computer users, of which 179.209 had their PCs encrypted. Additionally, 121.262.075 various dangerous items, including scripts, exploits, executable files, and others, are detected by the Kaspersky antivirus programmed. This indicates that among computer users, 34.2% experienced at least one web attack. Due to the high prevalence of computer malware (viruses, worms, Trojan horses, rootkits, botnets, backdoors, and other harmful software), traditional signature-based methods are no longer effective at identifying new variants that did not previously appear to be dangerous. (Sharma, S and Kaul, A., 2018)

A programmed device, or system that is being used on a network to draw attackers is known as a honeypot. The honeypot is intended to fool the invader into thinking it is a legitimate system. Honeypots are inherently virtual machines that mimic real machines by simulating services that might be found on a typical machine on a network and open ports. This indicates that an attack on a honeypot and potential subjugation are to be expected. Honeypots don't solve any problems. A honeypot is a security resource that is valuable when it is examined and attacked. Simply explained, a honeypot is a software program that is created specifically to "catch" people who try to hack into some other people's computers and attract attention to them. A new variety of Mobile Ad-hoc Networks (MANETs) is the Vehicular Ad-hoc Network (VANET), which has several useful applications in the intelligent traffic system. Since human lives are on the line in applications on VANETs, interaction between nodes (vehicles) must be established in the most secure way possible. Different security techniques are created to ensure protection for VANETs, with intrusion detection systems being the most well-liked (IDSs). IDS has already shown its value in identifying malicious nodes in conventional networks, but applying IDS to networks resembling VANETs is somewhat different and challenging because of its peculiar features, including resource-constrained nodes, high node mobility, particular protocol stacks, and standards. (Verma, A. S. et al, 2020).

In order to study and fight against assaults against IoT, IIoT, and CPS environments, honeypots and honeynets can be crucial. By luring attackers in and tricking them into believing they have access to the real systems, they can help. Honeypots and honeynets can strengthen the defense against malevolent entities by working in conjunction with other security measures such as firewalls and intrusion detection systems, or IDS. (Franco, J.et al, 2021)
From 20% to 35% more new malware and attacks were detected during the pandemic years of 2020–2021. According to the 2021 Data Breach Investigation Report, money is typically the key driving force behind security issues. Organizations often examine their overall security policies, and more significantly, enhance network security by installing numerous defense system, one of which is Honeypot, to provide an effective risk mitigation plan in advance of and in response to intrusive attacks. It works as a deception technique created to entice and engage only attackers for the goal of trapping and gathering data about invasive attempts. Honeypot systems' logged attack data can be thoroughly studied, and the lessons acquired can then be applied to network security guidelines to strengthen network security. (Ikuomenisan, G., & Morgan, Y., 2022)

III. SURVEY TO PROTECT MEASURES AGAINST SERVER ATTACK USING HONEYPOTS

It would be the aim of a research to learn how firms are adopting honeypots to safeguard their servers from cyberattacks in order to take security precautions against server attacks. The questionnaire could ask inquiries about:

3.1. Deployment of Honeypots:

- **Perimeter Defense**: Honeypots can be deployed at a network's perimeter to defend against external threats and give early notice of attacks.
- **Internal Defense**: Honeypots can also be installed within the internal network to find dangers like insider assaults or highly sophisticated persistent threats that have gotten past perimeter defenses.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023
DOI: 10.17148/IJARCCE.2023.12358

- **Virtualized Environment**: To offer scalable and affordable security solutions, honeypots can be installed in virtualized environments like cloud computing platforms or virtual computers.
- **Hybrid Deployment**: To provide thorough coverage and minimize the possibility of false positives, honeypots can be established in both physical and virtual environments.
- **Custom deployment**: Honeypots can be deployed in customized configurations, tailored to the specific needs and requirements of the organization, to provide the most effective protection against specific types of attacks.

3.2. Types of Honeypots:

- **Low Interaction Honeypots**: Honeyd is the most popular low interaction honeypot. Using unassigned IP addresses, Honeyd may populate a network with virtual hosts. A set of simulated services and a particular operating system behavior can be specified for each host. The ease of use and adaptability of Honeyd make it a viable option for hosting a whole minimal contact honeynet. However, the interaction offered by the simulated services is what allows for attacks to be collected, and creating these services is frequently a challenging task.

- **High Interaction Honeypots**: A number of tools have been created by the Honeynet Project to assist researchers in setting up a honeynet and analyzing suspicious network data. One of these solutions, called Honeywall, was specifically developed to manage honeypots with high interaction rates. It offers both a reverse firewall to manage outbound connections from possibly hacked honeypots and a web interface to monitor the data collecting. Through the Sebek kernel module, Honeywall incorporates system monitoring features as well.

- **Hybrid Honeypots**: Researchers have developed more scalable and intelligent architectures as a result of the need to gather detailed attack processes on large IP spaces. When we offer our Honeybrid architecture, these projects are considered hybrid honeypot architecture. It uses GRE tunnels to direct traffic from dispersed networks into a centralized farm of honeypots, which makes it easier to deploy and manage high interaction honeypots on large IP spaces. The disadvantage is that it doesn't offer any filtering mechanisms that can stop high contact honeypots from becoming overloaded.

3.3. Effectiveness of Honeypots:

- **Early warning and detection:** Honeypots can provide early warning of attacks and allow organizations to respond quickly, before the attack can spread to other parts of the network.
- **Attack analysis:** Honeypots can provide valuable information about the methods and tactics used by attackers, which can be used to improve overall security and prevent similar attacks in the future.
- **Decoy for attackers:** By deploying a honeypot, organizations can distract potential attackers and redirect their efforts away from critical systems and sensitive data.
- **Compliance:** Honeypots can be used to demonstrate compliance with security regulations and standards, such as PCI DSS.

However, there are drawbacks and difficulties with using honeypots, such as:

- **False positives:** Honeypots have the potential to generate false alerts, which add to the workload of security employees and reduce the efficiency of the system.
- **Resource requirements:** Honeypot deployment and maintenance might need significant resources, such as staff, hardware, and software, which not all businesses may have access to.
- **Attacker sophistication:** More sophisticated attackers might be able to find and avoid honeypots, which would lessen their effectiveness.

In general, honeypots can be a useful tool for detecting and preventing server attacks, but they should be used in conjunction with a thorough security strategy that includes numerous layers of defense and a skilled security team. The objectives and needs of the company, as well as the resources and knowledge at the security team's disposal, will determine the precise effectiveness of honeypots.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12358

3.4. Pre-Existing Software of Honeypots

- **Honeyd:** Honeyd is an open-source honeypot written in Python. It allows the user to set up virtual honeypots that imitate various types of servers and services. Honeyd can emulate a wide range of services such as web servers, SMTP servers, FTP servers, and even custom protocols. Honeyd can be used to monitor and detect attacks on networks and to analyse the behaviour of attackers. It can be configured to log and alert on different types of events and can also be integrated with other security tools such as Snort and Nessus. Overall, Honeyd is a powerful and versatile tool for setting up honeypots in a network environment.

- **Cowrie:** Cowrie is an open-source, medium interaction SSH honeypot that is written in Python. It is designed to mimic a real SSH server, and is used to capture information about attacks that are targeted at SSH services. It can also be used to study the behavior of attackers and to identify new attack patterns. Overall, Cowrie is a powerful tool that can help improve the security of SSH services in a network environment.

- **Dionaea:** Dionaea is an open-source honeypot that is written in Python. It is designed to mimic different types of services, including SMB, HTTP, FTP, and MySQL. Dionaea can be used to capture malware samples, log and alert on various types of events, and study the behavior of attackers. Dionaea is a powerful tool that can help organizations detect and analyze attacks that are targeted at different types of services. It can also be used to study the behavior of attackers and to identify new attack patterns.

- **Glastopf:** Glastopf can be useful for detecting and analyzing attacks that are targeted at web applications. It can also be used to study the behavior of attackers and to identify new attack patterns. It is designed to mimic vulnerable web applications and services, and is used to capture information about attacks that are targeted at web applications.

3.5. Algorithm use in Honeypot

There is no one specific algorithm that is used in honeypots, as the implementation of honeypots can vary greatly depending on the specific requirements and goals of the system. However, some common techniques that are used in honeypots include:

- **Signature-based detection:** This involves using known attack signatures to identify and respond to potential threats. This technique can be effective in detecting well-known attacks, but may miss more sophisticated or novel attacks.
- **Anomaly detection:** This involves analyzing network traffic and behaviour to identify deviations from normal patterns, which can indicate potential malicious activity. This technique can be effective in detecting previously unknown attacks, but may generate false positives.
- **Machine learning:** This involves using artificial intelligence algorithms to analyse network traffic and identify potential threats. Large datasets of network traffic can be used to train machine learning algorithms to identify complicated behavioural patterns that are suggestive of malicious activities.

IV. PROPOSED METHODOLOGY

- **Identify the potential attack vectors**: The first step in setting up a honeypot is to identify the potential attack vectors that are likely to be targeted by attackers. This could include web applications, network protocols, or specific services that are commonly targeted by attackers.
- **Choose a honeypot software or platform**: There are many different honeypot software and platforms available, each with its own strengths and weaknesses. Some popular options include Honeyd, Kippo, and Snort.
- **Configure the honeypot:** Once the honeypot software or platform has been chosen, it must be configured to mimic the targeted attack vectors. This includes setting up virtual machines, configuring network interfaces, and configuring the software to mimic specific services or protocols.
- **Deploy the honeypot:** Once the honeypot has been configured, it should be deployed in a location that is likely to be targeted by attackers. This could include the perimeter of a network, or a specific subnet within a network.
- **Monitor the honeypot:** The honeypot should be monitored for activity, and any suspicious activity should be investigated. This could include unauthorized access attempts, attempted data exfiltration, or other malicious behaviour.
- **Analyse the data:** Any data collected from the honeypot should be analyzed to identify patterns and trends in attacker behaviour. This information can then be used to improve the security of the network or organization.
- **Update the honeypot:** As attackers continue to evolve their tactics, it is important to update the honeypot to reflect

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12358

the latest attack vectors. This could include updating the honeypot software or platform, or configuring it to mimic new services or protocols.

- **Continuously monitor:** The honeypot should be continuously monitored to ensure that it is still providing valuable information and is able to detect new threats

4.1 System Architecture

The honeypot framework that has been used draws a number of ideas from Honey's conceptual design. The architecture of the implemented honeypot and the connection between the various modules are shown in Figure 4.1, and more information about these aspects will be provided below. By establishing a daemon that responds to ARP requests for IP addresses that match the user specified network address space, the framework is able to intercept any incoming traffic. To any ARP request that receives no response, the daemon transmits the hardware addresses of a user-specified interface from the honeypot machine. By pretending that those computers exist, the honeypot is able to claim all unassigned IP addresses on a LAN. A dispatcher module that handles incoming packet processing and records the intercepted traffic. For the interface the honeypot is configured to listen, a dispatcher is spawned. The module takes care of basic packet filtering, routing inside the simulated virtual network, and live traffic capture for that interface. To filter out our own outgoing packets, for each captured packet, determines whether the source address of the Ethernet frame belongs to one of the simulated machines. Further filtering is carried out for faulty IP checksums and unsupported protocols. The Ether Type values contained in the captured Ethernet frame serve as the basis for the protocol filtering; packets of unsupported protocols are logged and then discarded. The honeypot listens for ARP queries and responds to them with a response that includes the hardware address of the honeypot host. IP protocol packets are accepted, and further data extraction and recording are done. The original checksum for arriving IP packets is taken from the header and contrasted with a newly calculated IP checksum. The packet is logged and dropped if the checksum verification is unsuccessful. The dispatcher also discovers the router in charge of maintaining the target device and the configuration of the related device.

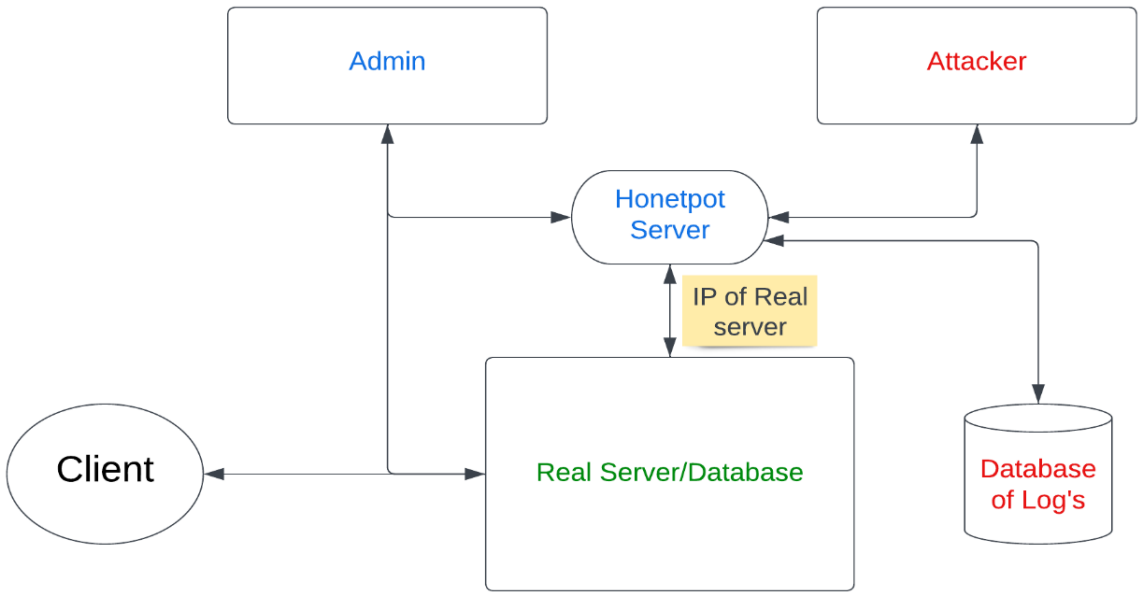

Fig.4.1

- **Network Layer**: This layer is in charge of safely directing traffic to and from the honeypot. Moreover, it will offer defence against malicious traffic and other potential attack points.
- **Host Layer:** This layer is in charge of housing the honeypot and any services it needs. Also, this layer will be in charge of upholding the system's security and preventing illegal access.
- **Application Layer:** This layer is in charge of managing the honeypot and all of its supporting services. It will be in charge of setting up and maintaining the system as well as providing the honeypot with the essential capabilities.
- **Data Layer**: The data gathered by the honeypot will be stored and managed by this layer. Additionally, it will give the tools required for data analysis and reporting.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12358

4.2 Flow Diagram

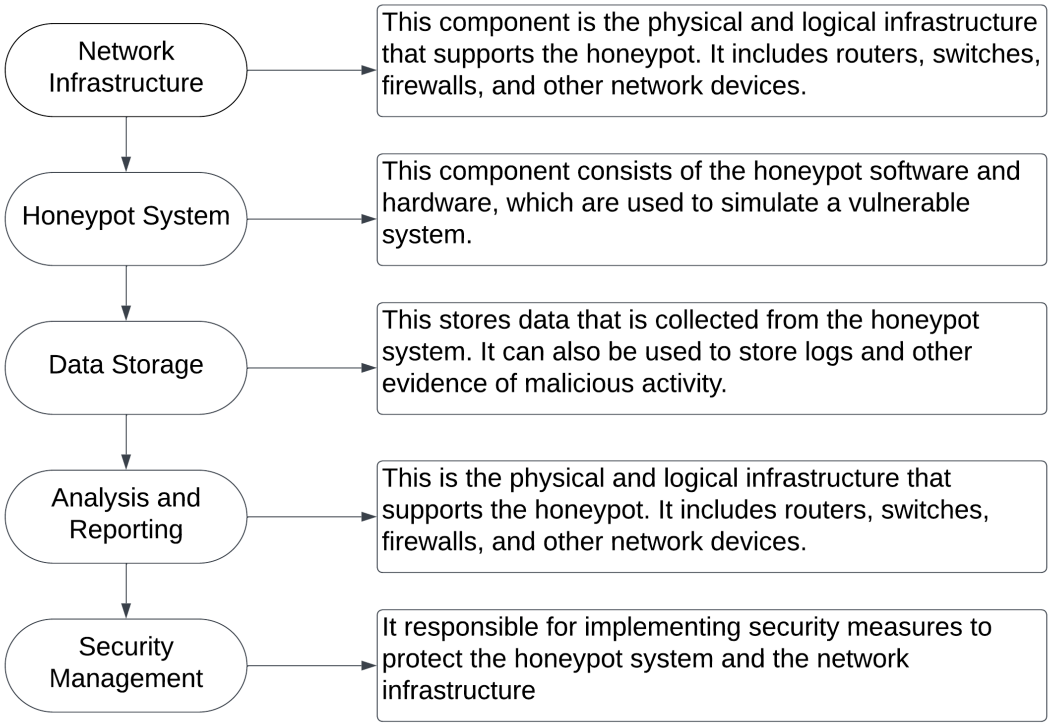

Fig.4.2

V. CONCLUSION

It is necessary to increase protection in the expanding IT industry. The use of preventative and investigative methods to strengthen IT security. In order to strengthen our security, we must be aware of potential intruders, assailants, hackers, etc. Our machine can be hacked by others. Our network is continually being scanned by attackers looking for open ports and weak spots. But I can't protect my network or system if the adversary isn't aware of it. To halt a hacker, we must think like a hacker. Honeypots can be used to either gather information or simply confuse and deflect assaults. Both people and businesses can use a variety of free honeypot programmes that run on Linux and Windows. Every technology has benefits and drawbacks, and this is true of honeypots as well as other technologies.

It is an effective tool for tricking people, catching trespassers who capture information, and sending out notifications when someone tries to communicate with them. This footage of the intruders offers important details for evaluating their attacking strategy and tactics. Since honeypots record and gather info. The system does have some drawbacks. Only actions that immediately affect them are tracked and recorded. It is unable to identify attacks against other network platforms. Perhaps the most contentious disadvantage of honeypots is this one. i continue my work on a honeypot design that strives to offer Honeyd-like functionality and realise its characteristics to the most recent fashions.

A huge number of unused IP addresses can be assumed by the honeypot, which can then imitate devices on that network. These gadgets can be plugged onto any network topology, which the honeypot framework simulates. The network's devices have the ability to mimic any operating system that is listed in Nmap's fingerprint database. A variety of Nmap scans that require host discovery, port scanning, or OS detection can trigger responses from the honeypot. Due to Honeyd's design's very constrained logging capabilities, improvements have been made.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023
DOI: 10.17148/IJARCCE.2023.12358

REFERENCES

[1] Bringer, M. L., Chelmecki, C. A., & Fujinoki, H. (2012). A survey: Recent advances and future trends in honeypot research. International Journal of Computer Network and Information Security, 4(10), 63.Tekerek M., "Bilgi Güvenliği Yönetimi", KSÜ Fen ve Mühendislik Dergisi 11(1), s. 132, 2008.
[2] Franco, J., Aris, A., Canberk, B., & Uluagac, A. S. (2021). A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems. IEEE Communications Surveys & Tutorials, 23(4), 2351-2383
[3] Ikuomenisan, G., & Morgan, Y. (2022). Meta-Review of Recent and Landmark Honeypot Research and Surveys. Journal of Information Security, 13(4), 181-209.
[4] Sharma, S., & Kaul, A. (2018). A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud. Vehicular communications, 12, 138-164.
[5] Verma, A. S., & Dubey, A. (2020). A Review on Honeypot Deployment. LJP London Journal of Research in Computer Science and Technology, 20(1). Can, O.; Sahingoz, O.K., "A survey of intrusion detection systems in wireless sensor networks", 6th International Conference on in Modeling, Simulation, and Applied Optimization (ICMSAO), pp.1-6, 27-29 May 2015

