Black Sea Journal of Engineering and Science
doi: 10.34248/bsengineering.1531420

Open Access Journal
e-ISSN: 2619 – 8991

Research Article
Volume 7 - Issue 5: 954-959 / September 2024

ANALYSIS OF CYBER ATTACKS USING HONEYPOT

Hakan Can ALTUNAY[1]*

[1]*Ondokuz Mayıs University, Çarsamba Chamber of Commerce Vocational School, Department of Computer Technologies, 55200, Samsun, Türkiye*

Abstract: In the cybersecurity world, the concept of a honeypot is generally referred to as trap systems that have real system behaviors, intentionally leave a security gap, and aim to collect information about cybercriminals who want to access them. It is a computer system that sets itself as a target to attract cyberattacks like bait. It is used to imitate a target such as cyberattackers and to learn about attack attempts, ways of working, or to distract them from other targets. In this study, a VoIP-based honeypot was used to determine the profiles of cyberattacks and attackers. A network environment was created using a low-interaction honeypot to analyze the behavior of cyberattackers and identify the services frequently preferred by these individuals. The honeypot in the network environment was monitored for a period of 90 days. 105,308 events were collected regarding protocols such as Telnet, SIP, SSH, SMB, and HTTP. There was no complex malware attack on the observed system. The service that was most attacked was determined to be Telnet. It was determined that many attacks occurred from the same IP address, indicating that automatic scanning tools were used. According to the results obtained, the proposed method performed a detailed analysis of the services from which cyberattacks came and the behaviors of the people who carried out these attacks. In addition, the highest level of understanding of user interaction was achieved thanks to the VoIP-based honeypot.

Keywords: Honeypot, Cyberattack, SIP, SMB, SSH

***Corresponding author:** Ondokuz Mayıs University, Çarsamba Chamber of Commerce Vocational School, Department of Computer Technologies, 55200, Samsun, Türkiye
E mail: hakancan.altunay@omu.edu.tr (H. C. ALTUNAY)
Hakan Can ALTUNAY https://orcid.org/0000-0002-0175-239X

Received: August 10, 2024
Accepted: September 03, 2024
Published: September 15, 2024

Cite as: Altunay HC. 2024. Analysis of cyber attacks using honeypot. BSJ Eng Sci, 7(5): 954-959.

1. Introduction

Sending voice, video or messages over IP (Internet Protocol) is called Voice Over Internet Protocol (VoIP). Since it works over the internet or computer networks, it is usually cheaper, sometimes free (Wang et al., 2005). For this reason, it is one of the most preferred telecommunication communication methods today. Gateway devices are used to convert analog lines to VoIP (Franco et al., 2021). VoIP converts voice information into digital signals that travel over the internet. If you are calling a regular phone number using broadband service, the signal is converted to a regular phone signal before reaching the destination (Rashid et al., 2024). All of this is done through a broadband internet connection instead of a regular or analog phone line (Spahn et al., 2023). The hardware required to make this possible is a broadband high-speed internet connection (Zhu et al., 2024). This problem can be solved with a computer, adapter or a phone manufactured for this purpose. While some VoIP services support the use of your regular phones connected to a VoIP adapter, others only work on a computer or a special VoIP phone (Srinivasa et al., 2022).
When examining the types of fraud on VoIP, hackers and fraudsters first try to take over the VoIP system and then earn income by calling high-priced places. Therefore, in this study, it is suggested to establish a honeypot system to test the security in the systems and detect the attacks or hijacking methods (Diap et al., 2021).
Attacks on a network can be detected using honeypots. In traps using honeypots, critical data is given the impression that it is stored in a computer on the network. In fact, this computer forms the basis of the honeypot trap. (Bartwal et al., 2022). This structure, designed using honeypots, collects information about the methods of cyberattackers and is used to detect attacks and monitor activity (Bringer et al., 2012). They mimic the behavior of real systems and are isolated from the host system (Conti et al., 2022).

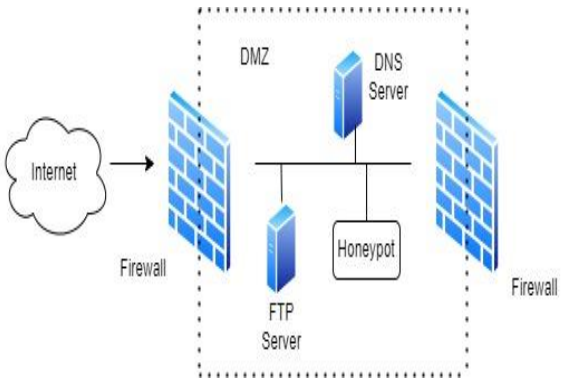

Figure 1. Location of honeypot in the network .

Honeypots are divided into three groups. They are called low-interaction, high-interaction, and pure honeypots

(Dai et al., 2021). Low-interaction honeypots focus on imitating services such as remote authentication services and file transfer services (Akiyama et al., 2018). Their main advantage is that they consume relatively fewer resources than high-interaction honeypots and are easier to install. Their disadvantage is that the service they emulate is limited to detecting security vulnerabilities only (Abdulqadder et al., 2023). High-interaction honeypots, unlike low-interaction, emulate multiple services at the same time (Javadpour et al., 2024). The advantage of high-interaction honeypots is that since there are many services for attack, it can be more convincing that the honeypot is a real system (Lanka et al., 2024). However, implementing and maintaining such honeypots is more difficult. Pure honeypots are systems where the activities of attackers are monitored and recorded (Ackerman et al., 2020). No special software is required in these systems and the task is performed using normal systems (Altunay et al., 2024). However, expert knowledge is needed to prevent these systems from causing security vulnerabilities in the network (Adiou et al., 2022).

In this study, experiments were conducted to determine attacks and attackers using data obtained from the honeypot environment. Statistical data about attacks and attackers, such as time, region, service type, attack content, attack type, frequency, and attack origin region and attacker fingerprint were analyzed, and how cyber attackers implement certain types of attacks was explained. In addition, when attack packets from different countries were examined in the study, it was seen that they generally perform the same types of attacks. The malware loaded into the honey trap was analyzed to understand how the attacks were carried out. The results obtained from the malware will help to prevent attacks or minimize their impact by classifying the packets coming over the network.

The general structure of the study is as follows. In Section II, a literature review on VoIP honeypot solutions was conducted, and the related studies were explained in detail. In Section III, information about the established honeypot environment was provided. In Section IV, the results obtained in the experimental study were shared. In the last section, the obtained values were discussed and future planned studies were mentioned.

2. Related works

Initially, the idea of honeypots was explained by Lance Spitzner, who evolved honeypots into honeypot networks (Spitzner et al., 2003). In 1998, a honeypot software called Cybercop Sting was prepared. It is also known as Decoy Server. Decoy Server could simulate services such as Telnet and SMTP (Østvang and Houmb, 2019). Although it had a very limited usage and logging ability, it was very useful in analyzing attacker attacks. There are studies in the literature that suggest using honeypot systems to capture malicious traffic in VoIP systems. Carmo et al. (2011), built a SIP (Session Initation Protocol) specific honeypot system called Artemisa and created a collection of attack traces. However, in networks using Session Initiation Protocol (SIP), different methods are applied to detect attacks other than SPIT (Spam over Internet Telephony). Attacks on this protocol, which initiates and manages interactive user sessions including voice, video, instant messaging and other multimedia sessions, are increasing day by day. In order to analyze the attacker's behavior and capture the original attack traffic, it is important that the attackers do not realize that they have accessed the honeypot. Provos and Holz describe how attackers can detect that they are inside a honeypot, especially in virtualized environments (Provos and Holz, 2007). However, since virtualization is currently used in production systems, it is not a definitive proof of a honeypot. A simple statistical analysis of VoIP attacks on virtualized low-interaction honeypot environments is given by Valli (2010).

Nassar et al. (2007) proposed an IDS to detect cyberattacks on the SIP protocol. The focus of this intrusion detection system is on a honeypot. In the study, attacks were prevented by using a honeypot with a low level of interaction. Script-based operation in service implementation and relational interpretation of situations in managing security events are the limitations of the honeypot.

In order to be able to examine and interpret the work performed by the attacker in detail, it is necessary to have information about details such as protocol, service, status and port information. It is important to have a more general view of the attack behavior. Another study proposed a honey trap-based model that deploys predefined software images and stores attack information in a database (Safarik et al., 2013). Dionaea is used as a database in the proposed model. In the evaluation part of the model, the obtained data is transmitted to a central server and detailed analysis is performed. The most significant disadvantage of the model suggested in the study is its high resource usage. In addition, the installation and maintenance of the hardware on which it will operate at remote points also requires time and cost. Gruber et al., (2011) analyzed real-world attacks obtained from honeypot solutions and revealed the current security status of VoIP systems.

Hoffstadt et al., (2012) recorded 47.5 million SIP messages in the customized SIP honeypot system they established and examined the collected data with statistical packet analysis.

3. Proposed Model

In order to investigate the behavioral analysis of the attackers, data must be collected reliably. In case the server where the honeypot is installed is compromised by the attacker in any way, the data must be transferred to another reliable server. The attacker must not be able to access the previous monitoring logs in any way. In this way, the privacy and personal information of the

attackers are also protected. In this study, some data was used to sample the attacks. In particular, the password that the attackers try most often, or the determination of the most used password in the data set can be given as an example. During the experimental study, the entire data set was used, and some information was filtered. The data collected from the servers where the honeypot was running was stored in a database on another server. MySQL database was used in the study. The data in the database was analyzed in detail using SQL queries. Code fragments written in Python were also used during the analysis process. In order to determine whether the incoming requests are from automatic scanning systems or real user behavior, the time of the incoming requests, access time, frequency, repetition, IP addresses, and the attempted passwords and commands were evaluated as parameters.

There are different approaches to design honeypot systems. Each of these approaches focuses on different attack scenarios. However, hybrid models are required to obtain the attacker profile, penetration models and attack behavior. In hybrid models, the material and moral damages that the attacker can cause can be revealed in advance by in-depth analysis of the attacker's behavior. The honeypot environment shown in Figure 1 was designed for both general security analysis and to collect and analyze attacks against VoIP systems. This heterogeneous infrastructure connected to the Internet allows to catching different attackers and get a broad perspective on the VoIP security status. In the simulation environment, all packets from the other side are recorded for statistical analysis, and malware and commands used for the attack are extracted and stored through deep analysis of the packets. In the test environment we prepared, a simulated service environment that can respond to all message types and status flows specified in the RFC standard document was created. Known attack scenarios such as identity theft, call dropping, and interception were modeled and constructed in the test environment. In order to perform fraudulent activities, an open SIP trunk service has been integrated to the internet and easy-to-guess passwords have been assigned to sections such as the web interface, SIP trunk management console, and PBX telnet/SSH services. A unique identification method has been applied to correlate data across different honeypot software and locations. A summary value has been obtained by combining IP, time, protocol, and message type information within each request. The basic components of our honeypot environment and the applications used to collect data are as follows.

Firewall is used to minimize the impact of cyberattacks by detecting abnormal situations on the network. Attacks such as demanding high fees for any service or fee fraud against users can also be detected by the firewall. (Agarwal, 2022). HoneyDrive, a virtual machine image that contains pre-installed and configured honeypot services for many services, is used. All important honeypot related software is included in HoneyDrive. In addition, many scripts and utilities such as Kippo-Graph, HoneydViz, DionaeaFR, an ELK are available in HoneyDrive to analyze, enhance and visualize data. In addition, there are almost 90 malware analysis, forensics and network monitoring tools. Asterisk IP PBX, an open source Internet Telephone PBX infrastructure based on Linux, is used. Finally, Flowroute SIP Trunk Service Management, a paid software, is used. Calls are made through this service via Asterisk.

4. Results

In order to identify security threats in the global VoIP system compromise phases and to obtain information about active attackers, findings obtained from different components of the honeypot solution and their correlations are presented. Therefore, normalization, classification and analysis processes were performed to compare the collected data. In order to provide a better understanding of the collected data, a statistic is presented in Table 1. Although it is not appropriate to compare the numbers directly, it gives an idea about the results of the following analyses. The honeypot system provides a wider target IP address range. In addition, all SIP requests are collected with the honeypot. The results show that the source of the attacks is similar.

Table 1. Number and types of data collected.

Types of Data	Number of data collected
Number of Urls	194
Number of IPs	29375
Number of collections	106781

No complex malware attack was observed in the honeypot system we observed. However, as seen in Figure 2, attacks were carried out via different services, especially Telnet port 23. Attacks via SIP port are in second place. It is also seen that more than one attack was carried out using the same IP address. This situation shows us that automatic scanning and attack tools are being used. Attackers use self-concealment methods such as Tor and VPN. In this way, they gain access from different countries. In password attacks, the combination of admin/123456 and admin/admin was tried. Another striking point is that when the commands used in password attempts and SSH sessions are examined, it is seen that IoT devices are also used for this purpose.

The network using the honeypot was attacked 4 times via the SSH service and operating system commands were run. However, although there was a lot of VoIP message traffic, no full conversation was made and no fraud was committed. After the attackers took over the service, they created new users, viewed the content of files containing passwords, and set up programs to include them in the botnet network, while a serious increase in computing applications aimed at generating bitcoins has recently been observed.

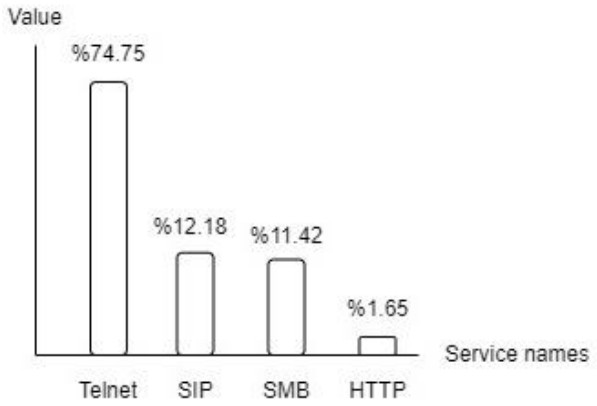

Figure 2. Attack rates on services.

In the attack attempts made for the services, only 1.67 percent of successful access was achieved and in only 48 percent of these accesses, the attacker ended the session without performing any action. It was evaluated that the biggest factor in this situation was the fact that the attempts were made with automatic tools and the attacker gave up because it was a low-interaction honeypot. In password attempts, the attackers tried known information such as team, city, date of birth, with different variations. There were no methods such as not repeating the same password or waiting for a while between attempts that could lock the account. When the time spent in the attack cases was examined, it was observed that the most time was spent trying the password and then searching for valuable information on the machine.

Our honeypot system collected 765 malware samples. The most common type is the Conficker malware. The results show that the attackers perform a comprehensive IP scan and use a wide IP range when performing SIP-based VoIP attacks. When we examine the sources of the detected IP addresses, as seen in Figure 3, the attackers mostly come from Russia, India, China, Spain, the USA, and Germany.

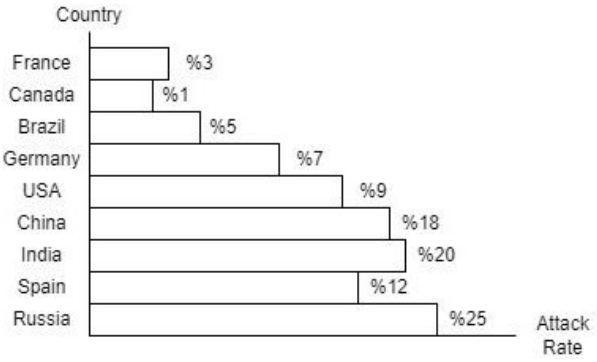

Figure 3. Distribution of attacks by country.

In order to understand the attack behaviors on the VoIP side and to recognize the tools they use, the SIP User Agent devices used were examined. The User-Agent information, which is a parameter within the SIP protocol, can be expressed as introducing itself with a text. Attackers come to the system by introducing themselves in this way. Attackers introduce themselves in this way and come to the system. They have carried out many attacks using the User Agent in a four-week period. The "Asterisk PBX" and "friendly-scanner" agents were preferred as User Agents. This situation shows that the attackers are trying to hide their VoIP attacks. Because instead of the commonly used attack tools, they have developed new tools and carried out SIP-based VoIP attacks. In order to carry out the fraudulent activity, the attacker first scans SIP-based VoIP devices with SIP OPTION messages using the User Agent. Then, they perform a Registration Hijacking attack on the devices they find with SIP REGISTER and INVITE messages. The striking point here is that messages directed to the same target are seen from the same IP address using different User-Agents.

5. Discussion and Conclusion

This article shares the results of a flexible and low-interaction honeypot system that was established to examine attacks on VoIP systems and the behavior of attackers. Honeypots are useful solutions for capturing information, generating alarms, attracting attackers, and trapping them. Thanks to honeypot environments, it is possible to obtain statistical analyses such as what type of attacks, how often they occur and from which country. For example, the tools used by attackers, the identification of new types of attacks, the collection of malware samples, help us discover future defense methods against unknown attacks. In addition, honeypots are preferred as an effective method to monitor the behavior of hackers and increase the effectiveness of developed security tools.

The results obtained from the honeypot system show that hackers use different methods and try to infiltrate in this way. Our future research aims to detect new malware families and zero-day attacks. It is planned to establish a high-level honeypot environment and create live traffic with critical services and transfer copied data from real interactions to the environment. In this way, all the behaviors and reactions of the attackers will be recorded, and more detailed analyses will be performed. As the number of detected attacks increases, precise analyses that can further improve VoIP security protection mechanisms will be possible.

Author Contributions

The percentages of the author contributions are presented below. The author reviewed and approved the final version of the manuscript.

	H.C.A.
C	100
D	100
S	100
DCP	100
DAI	100
L	100
W	100
CR	100
SR	100
PM	100
FA	100

C=Concept, D= design, S= supervision, DCP= data collection and/or processing, DAI= data analysis and/or interpretation, L= literature search, W= writing, CR= critical review, SR= submission and revision, PM= project management, FA= funding acquisition.

Conflict of Interest

The author declared that there is no conflict of interest.

Ethical Consideration

Ethics committee approval was not required for this study because of there was no study on animals or humans.

References

Abdulqadder IH, Zou D, Aziz IT. 2023. The dag blockchain: a secure edge assisted honeypot for attack detection and multi-controller based load balancing in sdn 5g. Future Gener Comput Syst, 141: 339-354.

Ackerman P. 2020. Modern cybersecurity practices: exploring and implementing agile cybersecurity frameworks and strategies for your organization. BPB Publications, Delhi, India, pp: 243.

Adiou ML, Benzaïd C, Taleb T. 2022. Topotrust: a blockchain-based trustless and secure topology discovery in sdns. International Wireless Communications and Mobile Computing (IWCMC), May 30- June 03, Dubrovnik, Croatia, pp: 1107–1112.

Agarwal Y. 2022. Apache Log4j Logging Framework and Its Vulnerability. MSc Thesis, Metropolia University of Applied Sciences, Department of Information Technology, Metropolia, Finland, pp: 67.

Akiyama M, Yagi T, Hariu T, Kadobayashi Y. 2018. Honeycirculator: distributing credential honeytoken for introspection of web-based attack cycle. Int J Info Secur, 17(2): 135-151.

Altunay HC, Albayrak Z, Çakmak M. 2024. Autoencoder-based intrusion detection in critical infrastructures. Curr Trends Comput, 2(1): 1-12.

Bartwal U, Mukhopadhyay S, Negi R, Shukla S. 2022. Security orchestration, automation, and response engine for deployment of behavioural honeypots. IEEE Conference on Dependable and Secure Computing (DSC), June 22-24, Edinburgh, UK, pp: 1-8.

Bringer ML, Chelmecki CA, Fujinoki H. 2012. A survey: Recent advances and future trends in honeypot research. Int J Comput Network Info Secur, 4(10): 63.

Carmo R, Nassar M, Festor O. 2011. Artemisa: an open-source honeypot back-end to support security in VoIP domains. 12th IFIP/IEEE International Symposium on Integrated Network Management, May 23-27, Dublin, Ireland, pp: 361-368.

Conti M, Trolese F, Turrin F. 2022. Icspot: A high-interaction honeypot for industrial control systems. International Symposium on Networks, Computers and Communications (ISNCC), July 19-22, Shenzhen, China, pp: 1-4.

Dai B, Zhang Z, Wang L, Liu Y. 2021. APT Attack heuristic induction honeypot platform based on snort and open flow. International Conference on Smart Computing and Communication, December 29-31, New York, US, pp: 340-351.

Djap R, Lim C, Silaen KE, Yusuf A. 2021. Xb-pot: Revealing honeypot-based attacker's behaviors. 9th International Conference on Information and Communication Technology (ICoICT), August 3-5, Virtual, pp: 550-555.

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 Commun Surv Tutor, 23(4): 2351-2383.

Gruber M, Fankhauser F, Taber S, Schanes C, Grechenig T. 2011. Security status of VoIP based on the observation of real-world attacks on a honeynet, IEEE International Conference on Privacy, Security, Risk and Trust, October 9-11, Boston, US, pp: 1041-1047.

Hoffstadt D, Marold AE, Rathgeb E. 2012. Analysis of SIP-based threats using a VoIP honeynet system. IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, June 25-27, Liverpool, UK, pp: 541-548.

Javadpour A, Ja'fari F, Taleb T, Shojafar M, Benzaïd C. 2024. A comprehensive survey on cyber deception techniques to improve honeypot performance. Comput Secur, 140: 103792.

Lanka P, Gupta K, Varol C. 2024. Intelligent threat detection—AI-driven analysis of honeypot data to counter cyber threats. Electronics, 13(13): 2465.

Nassar M, Niccolini, S, State R, Ewald T. 2007. Holistic VoIP intrusion detection and prevention system. The 1st International Conference on Principles, Systems and Applications of IP Telecommunications, July 19-20, New York, US, pp: 1-9.

Østvang ME, Houmb SH. 2019. Honeypot technology in a business perspective. Ring, M., Wunderlich, S., Grüdl, D., Landes, D., & Hotho, A. (2017). A toolset for intrusion and insider threat detection. Data Analyt Decis Sup Cybersecur, 2019: 3-31.

Provos N, Holz T. 2007. Virtual honeypots: From botnet tracking to intrusion detection, Addison-Wesley Professional, Boston, US, pp: 440.

Rashid SZU, Haq A, Hasan ST, Furhad MH, Ahmed M, Ullah AB. 2024. Faking smart industry: exploring cyber-threat landscape deploying cloud-based honeypot. Wireless Networks, 30(5): 4527-4541.

Safarik J, Voznak M, Rezac F, Partila P, Tomala K. 2013. Automatic analysis of attack data from distributed honeypot network. Mobile Multimedia/Image Process Secur Appl, 2013: 8755.

Spahn N, Hanke N, Holz T, Kruegel C, Vigna G. 2023. Container Orchestration Honeypot: Observing Attacks in the Wild. 26th

International Symposium on Research in Attacks, Intrusions and Defenses, October 16-18, Hong Kong, pp: 381-396.

Spitzner L. 2003. The honeynet project: Trapping the hackers. Secur Privacy Magaz, 1(2): 15-23.

Srinivasa S, Pedersen MJ, Vasilomanolakis E. 2022. Interaction matters: a comprehensive analysis and a dataset of hybrid IoT/OT honeypots. 38th Annual Computer Security Applications Conference, December 5-9, New York, US, pp: 742-755.

Valli C. 2010. An analysis of malfeasant activity directed at a VoIP honeypot. The 8th Australian Digital Forensics Conference, November 30, Perth, Australia, pp: 168-174.

Wang W, Liew SC, Li VO. 2005. Solutions to performance problems in VoIP over a 802.11 wireless LAN. IEEE Transact Vehicular Technol, 54(1): 366-384.

Zhu H, Liu M, Chen B, Che X, Cheng P, Deng R. 2024. HoneyJudge: A PLC Honeypot Identification Framework Based on Device Memory Testing. IEEE Transact Info Forens Secur, 19: 6028-6043.