Contents lists available at GrowingScience

International Journal of Data and Network Science

homepage: www.GrowingScience.com/ijds

The effect of using honeypot network on system security

Wael Ahmad AlZoubi[a*] **and Maen T. Alrashdan**[b]

[a]*Ajloun University College, Al-Balqa Applied University, Jordan*
[b]*Jadara University, Jordan*

CHRONICLE

Article history:
Received: February 12, 2022
Received in revised format: March 29, 2022
Accepted: May 14, 2022
Available online: May 14 2022

Keywords:
Honeypot
Network security
Network threats

ABSTRACT

For the development of technologies and networks that have been evolving and expanding day by day. In this generation, these facilities allow users to interact more efficiently. Safety is therefore very important to consider preserving the network and database and the need to detect a potential attack before an attack occurs. Network security has become the main issue, particularly in the industries, and there are many techniques to be used to protect network systems. One of them is called Honeypot, a software that is used to detect unauthorized misuse of information systems and to evaluate the actions and behavior of the attacker. Honeypot is, in other words, a trap for any attackers to log in to the network. If the behavior of these attackers is detected, the information will be used to improve network security. Using Honeypot does not cause attackers to notice they are being detected. This research is primarily focused on Honeypot, which is a ground-breaking new technology that has the potential to provide security communities with protection and how it is important for its use to enhance the network security framework.

1. Introduction

As how internet technology is universal, and still continues to expand on a regular basis. The security system is much necessary and needs to be updated to avoid the acts of all up-to-date attackers. Such issues also emerged in a wide number of different ways. Intrusion Detection System (IDS) is used to determine whether there is an issue in a network or in a system to recognize any dangers. Then, any forms of such attackers will be registered in the database. IDS is also known as the software, methods and resource for gathering, defining, analyzing and reporting certain data. There are two types of honeypots: low-interaction and high-interaction. Low-interaction honeypots have limited interaction where they are typically limited by imitating the services and the operating systems and the action of the attacker is generally restricted to the emulation level. High-interaction honeypot, meanwhile, addresses more radical solutions and is engaged in actual system difficulties and nothing is emulated. Anti-virus companies are now using honeypot to offer new enhanced security software. This research is done to define how honeypot is a very promising technology for enhancing network security, particularly in industries.

2. Literature review

Honeypot is a non-production method for manipulating attackers and identifying what tactics and behavior attackers use. Honeypot's target is not just to see the alerts being treated and withdrawn. Honeypots will detect the attackers and adapt from the attacks, and then the honeypot automatically modifies and improves the system to protect it accordingly (Artail, 2006).

* Corresponding author.
E-mail address: wa2010@bau.edu.jo (W. A. AlZoubi)

doi: 10.5267/j.ijdns.2022.5.010

This honeypot typically functions as a virtual machine and operates as an actual computer system connected to a network. Honeypot is used to identify the attacker and consider the approaches of attacking their activities. Honeypots are used to detect the attackers and connect from their attacks, and further improve the framework as security requirements after that transition. This may be used to investigate the entire program from a PC connected to a PC framework (Singh et al., 2013).

Honeypot is not used to detect the IDS, only the firewall to see the particular problem. It can be used as a part of the protection systems to see what type problems and an easy solution would be given to fix the problem based on the design and the objectives of usage. Consequently, in comparison to other forms of gear for data protection, it is not to have the alternative to refer to a honeypot that can provide a general response to each problem arrangement that can perceive its system as accessible as a firewall and discovery system for interruption. Honeypot structures are used to analyze and distinguish malignant behavior and associations. They have set up two interchange search honeypots in their executed program. The first one has an option for self-propagation and was intended to collect malicious software. The second is designed to catch all the harmful activities like a trap mechanism (Koniaris et al., 2014).

In particular, the generated framework has been used with the ultimate goal of safety against polymorphic worm assaults. The created system also has the potential to disengage suspicious traffic and collect various useful information about noxious traffic and worm assaults (Paul & Mishra, 2013). Points of concern about advancements in virtualization They also investigated the interruption identification and the settled virtualization condition of honeypot systems (Beham et al., 2013). Li et al. (2014) suggested setting up a honeypot-based interruption identification system for blended cooperation. They explain why they built the framework to balance out the structure and update security. Chawda and Patel (2014) proposed a honeypot disseminated system for exploring new vulnerabilities. They used low collaboration honeypot structures in their output framework to assist powerlessness as a front-end content platform.

Usage of honeypot systems and applications for detection of interruptions on dispersed networks. Has explained the basic overview why feasibility interruption detection frameworks were estimated by using both interruption recognition frameworks and honeypots (Pomsathit, 2012). Normally, honeypots are sent for the purpose of catching connections with incompetent enemies. The caught companies help analysts to understand assailant examples and conducts, honeypots have been used to facilitate the wave of new signatures for network intrusion detection systems (John et al., 2011). We ought to be hacked for keeping the troublemakers in-over structured computers. Security is customarily simply secured. There has been little a group could do to step up the troublemakers and confront them. Honeypots change fundamentals. They are a concept that helps one to target associations (Spitzner, 2002).

Honeypots are one of a kind in that they are not a single apparatus that deals with a specific problem. Rather, they are an invention which is highly adaptable and can accommodate a wide variety of jobs. How to use and convey such inventions is up to the user. Hajivali et al. (2013) applied an Agent Based User Authentication and Access Control Model for Cloud servers. Sawehli et al. (2020) mentioned the importance of applying different access with different security strategies in an organization. Others highlighted the lack of knowledge to implement any security strategy of any systems. Chuen et al. (2020) suggested using the image to remember the passwords.

The internet traffic flow increased rapidly every year because of some factors such as broadband internet access and changing the services from voice to data, this in turn doubled the need for multimedia live streaming and other bandwidth consuming services to be done in high-speed manner.

Jain and Singh (2011) defined the honeypot concept as a program, or machine placed somewhere on a network as temptation for invaders, they classified the honeypots into two types according to their use, they are: *research honeypots* which are used by inquisitive users or researchers and *production honeypots* which are installed by organizations as a part of their security structure. An intrusion detection tool based on some of the existing intrusion detection methods as network firewall and the idea of honeypots was proposed and designed.

production honeypot is one of the essential kinds of honeypots that assembles cybersecurity-related data from a company's production system. The production honeypot will be activated when an attack happens, whenever an attack appears, the production honeypot starts gathering data such as Internet Protocol (IP) addresses, traffic frequency and traffic volume. This type of honeypots is simple to be used and so it is common among companies while it generally doesn't divulge as much information as research honeypots do.

Research honeypots are used to gather information about techniques and strategies hackers use. The main difference between research honeypots and production honeypots is that they are used mainly by governments and research centers. Besides, it is considered as being more complicated than production honeypots and so it gives more information about any possible risks and vulnerabilities (Verma, 2004). One of the areas that benefit from the honeypot approach is decision support systems (DSS) (Hadidi et al. 2020), where the primary purpose of DSS is to improve methods to help in the process of decision-making and use in different companies and organizations.

Honeypots are a very vital criteria of the security effort of any company or organization, where comprehensive information must be collected about any threat and invaders, this collected information helps in building a strong protection plan. A honeypot misleads invaders to think that they are cooperating with a real system, thus hiding its uniqueness. One of the greatest dangers to any honeypot is fingerprinting which allows an invader to know the identity of the honeypot. Several methods have been proposed to fingerprint a honeypot preventing it from working properly; fingerprinting detection is a very difficult task. (Naik et al., 2018) proposed a smart and vigorous honeypot system depending on the dynamic fuzzy rule interpolation (D-FRI). One of the interesting things about the proposed system is its ability to discover confident types of fingerprinting danger in the absenteeism of identical rules, whereas the proposed system is also capable to learn and sustain a dynamic rule base for a more precise definition of possible fingerprinting risks based on the existing network traffic circumstances. Here is a brief explanation of indirect variables that affect network security.

2.1 Login attempts

One of the most important variables that affect network security is the number of trials to use this computer network. If the same user tries to go through the network, the system will register these trials and deal with this user as a suspicious user, so that it will be easy to put him on the blacklist and may block him in the next trials which will increase the overall system security.

2.2. System Real Working Condition

The time of using any computer network is important in classifying network users. Any user of the computer network tries to access the network several times outside the work time will be considered as a suspicious user which will increase the overall computer network security.

2.3. prompt activity

Honeypot is sometimes considered a robust event analysis tool that provides real-time monitoring and detection of malicious events on computer network endpoints. Honeypot allows the network administrator to visualize warnings in a detailed timeline while immediate alerts keep him informed if an attack takes place. In reality, Honeypot helps the network security staff prevent any malicious threats before they can even harm any device in the network, and so, the overall performance of network security will be increased.

3. Problem statement

As a norm, web applications are commonly used on the web nowadays, which also in a vague way gives the assailants the invitation to hack the sites and obtain confidential information and data. The web application's vulnerabilities let the aggressors waltz right into the servers or may even get inside the system. From that point, assailants can exploit the sites with various attacks and can inflict overwhelming harm to webmasters or corporate holders. Until now, webmasters need to stay updated on all times with the objective of battling site vulnerabilities. The primary objective of this research paper is to find the vulnerabilities of the current network structure and reinforce it with improved security features, thus emphasizing people to be more mindful of the safety of their network, this is the most important aspect. Once people discover that their system has such weaknesses on their network that can allow external exposure or intruders, they will be more aware of the vulnerability and will be adamant about investing in proper enhanced security measures that can lead towards a more protected network. This research paper's goal is to explore various types of security features and merge them into a device which will make it more difficult for the attacker to obtain access through the network to the user's private or private company. An analysis will be carried out on a virtual computer to find the vulnerabilities, and the outcomes of the analysis will be used to further improve the existing active defense network infrastructure using Honeypot to make it more secure and efficient. (Nitin Naik, 2018).

The question is generated from the problems indicated on the statements of problem:

Research Problems:

1. The vulnerabilities could result in information leaks that could cause the user loss.
2. There are still many vulnerabilities in the current network.
3. Security level of the current network is not very secure.

Research Questions:

1. How to determine the unsafe links?
2. How can the vulnerabilities be improved?
3. How to prevent the private information from leaking?

Research Objectives

1. To strengthen security features of the existing network system,
2. To implement the use of a more enhanced security system,
3. To identify and resolve current vulnerabilities in the network system.

Outcome of this project will be a virtual machine. A honeypot is an extra security measure that can be used to help secure a network from attackers alongside a firewall as well as other security solutions. As the name implies, Honeypots are expected to get the attention of a hacker with the intention of attracting their efforts to attack the honeypot as opposed to an environment where they may cause real trouble. They have all the duties of being a basic section point into a device that will prevent aggressors from taking a gander at specific frame pieces. They are an intentional gap in frame defense which can be attacked without causing harm. They allow IT groups to gain considerable insight into programmers striving to access their systems. Unlike a firewall, which is specifically designed to keep out external attackers, a honeypot may also identify threats and attacks inside. Many companies are completely unaware of attacks from inside. A honeypot gives greater perceptibility and makes IT protection groups to defend against attacks that are missed by the firewall to forestall. Honeypots have tremendous advantages, and they have been implemented by various organizations as an additional protection against internal and external attacks. The system is designed to analyze hackers in motion and learn what strategies they have employed.

4. Research methodology

Quantitative surveying will be used in this research to assess the solutions for the problems addressed by the study. By using quantitative survey, this will enable us to derive evaluation from detailed information provided by respondents in the form of feedback from the individual that said a connection with the current security features corresponding to the research questions. In previous research, current operating systems have been shown to have few vulnerabilities which are still unresolved. This opens attacker possibilities to those who seek to access something that is meant to be the privacy of the victim and misuse it for money or anything else. A sample size of 150 will be used for this survey to make the evaluation of the respondents not limited to the perspective of the respondent but generally. The queries should contribute to the respondent's opinion on their network's current safety and security level.

5. Results

5.1 Reliability and Mean and Descriptive Statistics

The study's validity and reliability were assessed using Cronbach's alpha. Internal consistency is measured using Cronbach alpha, which determines how tightly a group of elements is linked. One method for determining dimensionality is exploratory factor analysis. Cronbach's alpha, in other words, is considered as a reliability or dependability coefficient, not a statistical test (Tavakol & Dennick, 2011). Cronbach alpha can also be calculated as a function of the total number of test items and the average inter-correlation between them. The highest Cronbach alpha value was 0.92 for system real working conditions. The highest reliability value was 0.83 for efficiency of logging attempts and the alpha value was 0.89 for prompt activity, these values point to the acceptance of reliability. The Mean and Standard Deviation D.S. where the Mean averages ranged between (3.75-3.94), all were high as shown in Table 1. Also, this study examined the average variance extracted (AVE) and specified that all AVE values were greater than the recommended value of (0.50) (Hair et al., 2017), therefore, the convergent validity is satisfied as presented in Table 1.

Table 1
Reliability and Mean and Descriptive Statistics (S.D) and Average Variance Extracted (AVE)

Variable	Cronbach's alpha	Mean	S.D	AVE
Logging Attempts	0.83	3.75	0.76	0.715
System Real Working Condition	0.92	3.94	0.82	0.731
Prompt Activity	0.89	3.91	0.89	0.655

5.2 Durbin-Watson

The Durbin-Watson test was also applied to verify the correlation between the independent variables and their effect on the overall system security. As shown in Table 2.

Table 2
(Durbin-Watson) test of Independent Variables

Variable	Durbin-Watson
Logging Attempts	1.796
System Real Working Condition	1.856
Prompt Activity	1.843

Table 2 shows that all values of Durbin-Watson for the independent variables are less than the value of 3; these values are acceptable and indicate the absence of a self-correlation problem in all independent variables of the study.

5.3 Multiple Regression

In order to determine the relationship between the roles of system real working conditions in improving the overall network security in a private or public computer network, Multiple Regression analyses were used. Therefore, Table 3 shows that:

Table 3
Result of Multiple Regressions Analysis on the Relationship between the of Prompt Activity and Network Security in Computer Networks

Variable	"t" value	"t" sig	β	R	R^2	"F" value	"F" sig	Result
Logging Attempts	7.147	0.001	0.219	0.951	0.9044	412.21	0.015	Accepted
System Real Working Condition	6.391	0.002	0.221					Accepted
Prompt Activity	8.108	0.000	0.213					Accepted

Table 3 reveals a statistically significant association between the importance of the prompt activity to the network in enhancing system security. The F-value, in this case, was 412.21, which was statistically significant at 0.01 the value of R was 0.951, and the value of R^2 was 0.9044. Also, the prompt activity appears to play a greater role in network security with a "t" value of 8.108. As for the Efficiency of prompt activity, the t value was 6.391, while the Independence and Objectivity of prompt activity obtained a "t" value of 7.147. Hence, all objectives were satisfied.

6. Overview of the Proposed System

The honeypot is a computer system running on the web aimed at baiting and stunting others (e.g., programmers) who are attempting to hack into their computer system illegally. Honeypot is practically triggered using system complexity to strike an attacker, usually allowing the possible security vulnerabilities to have an excellent disguised position. Because honeypot is unable to give the outside aid genuine incentive, the whole effort to connect would be deemed suspicious. Another use of honeypots is to delay the attack on the true target, make the attacker lounge in a honeypot with the specific intent that the possibilities of a legitimate system administration to be recognized are decreased extraordinarily and the program recognition easily discerns the trespasser's effort. A short while later, the security vulnerabilities that may exist in the system should be resolved and the hostile capabilities and objectives of this adversary should be attained. Honeypot systems combine critical screens and incentive logs. Incentive log to identify an invader for accessing and collecting private data, and the equivalent can be used as system verification. Because every entry into the honeypot system, the system is given the expectation of a successful attack, so the system operator must not expose the system to real working conditions, prompt activity, logging, detecting intruders, collecting digital evidence, and performing a better-investigated work on the computer crime scene.

7. Conclusion

According to the study above, the concern of the security level, but honeypot, is not a solution to network security, but a good tool that complements other security technologies to construct an alternative active defense system for network security. Working with firewalls and IDS, honeypot provides a unique way to avoid, detect and respond to attacks. Honeypot can serve as a useful deception tool for product system prevention as it is capable of trapping a decoy system attacker. Honeypot is reinforced with IDS, reducing false positives and false negatives. Control of information routing provides a versatile response to attacks. Different forms of honeypot share similar data-control and data capture technologies. Experts are working on the two to make honeypot easier to launch and harder to detect. In one computer, a virtual honeypot produces a large number of honeypot systems. Dispersed honeypot requires multiple honeypot systems in an individual network to have high communication between attacks and the system. They all make future honeypots less costly to apply and easier to implement.

References

Artail, H., Safa, H., Sraj, M., Kuwatly, I., & Al-Masri, Z. (2006). A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks. *computers & security*, *25*(4), 274-288.

Beham, M., Vlad, M., & Reiser, H. P. (2013, June). Intrusion detection and honeypots in nested virtualization environments. In *2013 43rd Annual IEEE/IFIP international conference on dependable systems and networks (DSN)* (pp. 1-6). IEEE.

Chawda, K., & Patel, A. D. (2014, February). Dynamic & hybrid honeypot model for scalable network monitoring. In *International conference on information communication and embedded systems (ICICES2014)* (pp. 1-5). IEEE.

Chuen, Y. S., Al-rashdan, M. A. E. N., & Al-Maatouk, Q. U. S. A. Y. (2019). Graphical password strategy. *Journal of Critical Reviews*, *7*(3), 2020.

Hadidi, S., Al-Rashdan, M., & Hadidi, M. (2020). Impact web on decision support systems on the organizations. *International Journal of Science and Technology Resources*, *9*(4), 1450-1452.

Hair Jr, J. F., Sarstedt, M., Ringle, C. M., & Gudergan, S. P. (2017). *Advanced issues in partial least squares structural equation modeling*. Sage publications.

Hajivali, M., Moghaddam, F. F., Alrashdan, M. T., & Alothmani, A. Z. (2013, October). Applying an agent-based user authentication and access control model for cloud servers. In *2013 International Conference on ICT Convergence (ICTC)* (pp. 807-812). IEEE.

Jain, Y. K., & Singh, S. (2011). Honeypot based secure network system. *International Journal on Computer Science and Engineering*, *3*(2), 612-620.

John, J. P., Yu, F., Xie, Y., Krishnamurthy, A., & Abadi, M. (2011, March). Heat-seeking honeypots: design and experience. In *Proceedings of the 20th international conference on World wide web* (pp. 207-216).

Koniaris, I., Papadimitriou, G., Nicopolitidis, P., & Obaidat, M. (2014, June). Honeypots deployment for the analysis and visualization of malware activity and malicious connections. In *2014 IEEE international conference on communications (ICC)* (pp. 1819-1824). IEEE.

Li, S., Zou, Q., & Huang, W. (2014, April). A new type of intrusion prevention system. In *2014 international conference on information science, electronics and electrical engineering* (Vol. 1, pp. 361-364). IEEE.

Naik, N., Shang, C., Shen, Q., & Jenkins, P. (2018, June). Intelligent dynamic honeypot enabled by dynamic fuzzy rule interpolation. In *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)* (pp. 1520-1527). IEEE.

Paul, S., & Mishra, B. K. (2013, February). Honeypot based signature generation for defense against polymorphic worm attacks in networks. In *2013 3rd IEEE International Advance Computing Conference (IACC)* (pp. 159-163). IEEE.

Pomsathit, A. (2012, May). Effective of unicast and multicast IP address attack over intrusion detection system with honeypot. In *2012 spring congress on engineering and technology* (pp. 1-4). IEEE.

Sawehli, A., Al-Rashdan, M. A. E. N., & Al-maatouk, Q. U. S. A. Y. (2019). APU high-speed Internet access: A literature. *Journal of Critical Reviews*, *7*(3), 2020.

Singh, G., Sharma, S., & Singh, P. (2013). Design and develop a Honeypot for small scale organization. *International Journal of Innovation Technology Exploration Engineering (IJITEE)*, *2*(3), 170-174.

Spitzner, L. (2002). Hosus (honeypot surveillance system). *login: Magazine of Usenix and Sage*, *27*, 2002-12.

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education, 2*, 53.

Verma, A. (2003). Production honeypots: An organization’s view. *SANS Security Essentials*, *1*, 28.