GLOBAL RESEARCH NETWORK
ONLINE RESEARCH HUB

AMERICAN JOURNAL OF SOCIAL AND HUMANITARIAN RESEARCH

ISSN: 2690-9626
Vol.3, No 5, 2022

Integrated Intrusion Detection and Prevention System with Honeypot on Cloud Computing Environment

Gulomov Sherzod Rajaboyevich
PHD, Associate Professor, Head of the Department of "Information Security", Tashkent University of Information Technology named after Muhammad al-Khwarizmi, Uzbekistan

Salimova Husniya Rustamovna
Master's degree, specialty "Information Security", Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan

Bobomurodov Sharofiddin Azimjon o'g'li
Bachelor degree, Faculty of Radio and Mobile Communications, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan

ABSTRACT: Security issues become one of the important aspects of a network, especially a network security on the server. These problems underlie the need to build a system that can detect threats from parties who do not have access rights (hackers) that are by building a security system honeypot. A Honeypot is a diversion of intruders' attention, in order for intruders to think that it has managed to break down and retrieve data from a network, when in fact the data is not important and the location is isolated. A way to trap or deny unauthorized use of effort in an information system. One type of honeypot is honeyd. Honeyd is a low interaction honeypot that has a smaller risk compared to high interaction types because the interaction with the honeypot does not directly involve the real system. The purpose of the implementation of honeypot and firewall, firewall is used on Mikrotik. Can be used as an administrative tool to view reports of Honeyd generated activity and administrators can also view reports that are stored in the logs in order to assist in determining network security policies.

KEYWORD: Honeypot, low interaction, firewallmikrotik, wireless.

Introduction: Network security systems are often at the moment still seen as the result of several factors. Factors related to the safety of this network vary, depending on the basic ingredients, but normally there are at least some things in the concept of security such as securities, integrity, and availability. In network security, there is also the risk of computer networks that are all forms of threats both physical and logic that directly or indirectly disrupts the ongoing activities within the network. The Risks in computer network caused by several factors such as weakness of network operating system, weakness of network communication system and weakness of computer hardware. This security can be combined with non- repudiation, authenticity, possession, utility. The Internet is a network of networks. It is based on the concept of packet switching. Though the services offered by Internet are extensively used from a layman to multi-millionaire it also has its own defects. Many attacks on Internet are being identified and reported. Some of the common types of network attacks are saves dropping, data modification, identity spoofing, password-based attacks and denial of service attacks. To overcome all these types of attacks an organisation usually installs an intrusion detection system to protect the confidential data exchanged over its network. The local network is then connected to the Internet thereby availing the employees to be online on the fly. Information security has three main objectives namely 1.Data confidentiality 2.Data integrity 3.Data availability. Data confidentiality ensures that the secure data can be accessed only by authorized persons. Data integrity allows secure modification of data. Data availability ensures that the data is available readily to authorized persons. Small scale industries often do not prefer on intrusion detection systems due to its installation and maintenance costs. In the computer network is very important for network security, especially related to applications involving various interests, there will be many things that can disrupt the stability of the computer network connection, whether related to hardware (physical security, power resources) and related to software (System, configuration, access system, etc.). Disruption of the system can occur due to accidental factors performed by the manager (human error), but not least also caused by a third party. Disturbances can include destruction, infiltration, theft of access rights, misuse of data or systems, to criminal acts through computer network applications. Security of the system should be done before the system is enabled. The use of the system should be done before the actual system is enabled. Overall.

Honeypots also have some disadvantages because there are some important advantages of using honeypots.

- You can capture data only if the hacker actively attacks the system. If he does not attack the system, he cannot catch information. If an attack occurs on another system, the honeypot cannot identify it. This can damage the system other than the attack on the honeypot system and cause big problems.
- Honeypot fingerprint has a disadvantage. It is easy to understand whether a skilled hacker is attacking a honeypot system or an actual system. Fingerprinting allows you to distinguish between the two. It is not the result of our experiments.
- Honeypots can be used as zombies to reach other systems and damage your system. This can be very dangerous.

Materials: Honeypot can literally be a computer which can act as a source for attacks. It attracts the hackers to try hacking it which in turn may log the techniques used by the attackers. This log is useful to prevent such attacks to the legitimate network. Honeypot computer usually do not have any important data or information to be secured. It only has fake services running on its ports to attract the attackers.

Methods: Production honeypots are easily deployed in the live environment that may capture only some amount of information about the attacks. Research honeypot deployment is complicated and used mainly for research purposed by government organizations. On the basis of design, honeypots can be divided into 1.Pure honeypots, 2.High-interaction honeypots, and 3.Low-interaction honeypots. Pure honeypots are complete production systems. The honeypot computer is linked to the network and taps the attacks. Low-interaction honeypots allows restricted interaction with attackers and hence they are not infected by the attacks. High-interaction honeypots are vulnerable to attacks. No emulation takes place and hence more prone to get infected by attacks. Honeynet is a collection of honeypots installed to trap the attacker activities and log them.

Results: We studied all level of interaction honeypots and configured them. The evolution of honeypots can also be understood by looking at the ways these systems are being used in association with IDSs to prevent, detect and help respond to attacks. Indeed, honeypots are increasingly finding their place alongside network- and host-based intrusion-protection systems. Honeypots are able to prevent attacks in several ways. The first is by slowing down or stopping automated attacks, such as worms or autorooters. These are attacks that randomly scan an entire network looking for vulnerable systems. (Honeypots use a variety of TCP tricks to put an attacker in a "holding pattern.") The second way is by deterring human attacks. Here honeypots aim to sidetrack an attacker, making him devote attention to activities that cause neither harm nor loss while giving an organization time to respond and block the attack. As noted above, honeypots can provide early detection of attacks by addressing many of the problems associated with traditional IDSs, such as false positives and the inability to detect new types of attacks, or zero-day attacks. But increasingly, honeypots are also being used to detect insider attacks, which are usually more subtle and more costly than external attacks. Honeypots are also helping organizations respond to attacks. A hacked production system can be difficult to analyze, since it's hard to determine what's normal day-to-day activity and what's intruder activity. Honeypots, by capturing only unauthorized activity, can be effective as an incident-response tool because they can be taken off-line for analysis without affecting business operations. The newest honeypots boast stronger threat-response mechanisms, including the ability to shut down systems based on attacker activity and frequency-based policies that enable security administrators to control the actions of an attacker in the honeypot. Honeyd is a type of Open Source Honeypot application written by NielProvos. Honeyd is a simple daemon that keeps virtual hosts on the network. The host can then be configured to run various services. TCPnya Personality Can run as a particular operating system, to fool scanner fingerprints like Nmap or probe. Actually honeyd powerful enough and Provides a complete feature, but the configuration is not easy because it does not have a GUI (Mustofa&Aribowo, 2013). Honeyd is a low interaction honeypot type honeypot that performs network simulation as a whole like service FTP, SSH, HTTP, router in one machine / PC and can add multiple hops, packet losses, and latency (Tambunan, et al, 2013).

Recognizing the motives of an attacker can be a great help in understanding the threats. To help you understand the motivational issues, the Department used MICE abbreviations for money, ideology, compromise (which you did not want to do) and the self. Social group admission and status. Here are some of the many reasons why an attacker could try to break into the system as a target. Almost all these motivations have been confirmed using honeypots.

- **Denial of Service:** A DoS attack is an attack designed to remove a victim's computer system or network. This is typically done by populating the intended destination (such as a web server) with network traffic. The more traffic the victim receives, the more effective the attack. Attackers attack thousands (if not thousands) of systems that will be used to attack. The more computers you own, the more traffic you can run on your destination. Many blackhats use other DoS attacks to remove other blackhats. The IRC war is an example of an individual attempting to knock someone out on an IRC channel using a DoS attack.
- **BOTs:** BOTsare automated robot that work on behalf of an individual in a preprogrammed way. They are most commonly used to maintain IRC control. As more computers are hacked, more BOTs can be fired and more IRC channels can be controlled. With many BOTs, individuals will not be able to control IRC from denial of service (DoS) attacks.
- **Credit Cards:** A hacked computer has become a form of call. Blackhats will replace the hacked account with a stolen credit card. The more computers are hacked; the more money you can

make. This behavior is documented in the Honeynet Project's "Know Your Enemy: Motives" article.

- **Bragging Rights:** Many Black Hat organizations have the ability: Your position is based on your strengths and your skills. To increase your status, you must demonstrate your skill. Often you need to break into another site. The more sites you enter, the more you get. We often see people who modify websites, damaging the system, to be proud of their skills and try to improve their position.
- **CPU Cycles:** Some worms were developed to replace the CPU cycles of the client system to win the contest. The more computers the worm is infected with, the more the combined CPU cycles are used. The more machines and processing power the attacker handles, the greater the chance of winning the contest.
- **Corporate Espionage:** An organization may attempt to breach a competitor's security in order to gain a competitive advantage. This is a common motive for advanced blackhats because it involves financial interests.

Conclusion: Honeypots are a potential tool in the world of security. They provide an added benefit if they are used with firewalls or intrusion detection systems. They are available for commercial as well as research purposes and are quite flexible to fulfill our requirements. Honeypots have been used in various deception techniques like Honey farms, Simple port listener, honeypots as mobile code throttlers, Random Servers, digital breadcrumbs. Thorough care must be taken while deploying honeypots as it involves substantial amount of risk. Hence, a tight risk analysis needs to be done prior to deployment. Also strict rules must be framed for the maintenance purpose. They are cheaper, flexible, provide low false positive rate, can extract encrypted data. Laws and legal issues must be considered for deploying honeypot systems. Honeypots can reap great benefits if they are used in a smart way by using various new technology trends.

After reviewing all papers and related background information, we can identify some of the following problems. The challenge is to simplify the process, improve data analysis, and increase the value of the honeynet, including expanding the dataset used for pre- and post-response IDS analysis. If you need multiple devices, you can install a control sensor, depending on your network configuration, to monitor and connect the embedded device.

Such a system can develop an embedded system or appliance combined with a Web-based user interface when the system administrator enters minimal information at the deployment stage.

Another problem is to materialize the subprogram command to increase efficiency or to ensure that the user specifies subprogram commands to suit the environment and data collection requirements. Exciting system users can not configure the system.

Increase the scalability and reliability.

REFERENCES

1. Anagnostakis, Kostas G., et al. "Detecting Targeted Attacks Using Shadow Honeypots." Usenix Security Symposium. 2005.
2. Borisaniya, Bhavesh, et al. "Incorporating Honeypot for intrusion detection in cloud infrastructure." IFIP International Conference on Trust Management. Springer, Berlin, Heidelberg, 2012.

3. Dahbul, R. N., C. Lim, and J. Purnama. "Enhancing Honeypot deception capability through network service fingerprinting." Journal of Physics: Conference Series. Vol. 801. No. 1. IOP Publishing, 2017.

4. Rodrigues, Marcos, and OlamilekanShobayo. "Design and Implementation of a Low-Cost Low Interaction IDS/IPS System Using Virtual Honeypot Approach." Covenant Journal of Informatics & Communication Technology 5.1 (2017): 48-64.

5. Diansyah, TengkuMohd, et al. "Analysis of Using Firewall and Single Honeypot in Training Attack on Wireless Network." Journal of Physics: Conference Series. Vol. 930. No. 1. IOP Publishing, 2017.

6. Cao, Jianhong, et al. "Dipot: A distributed industrial Honeypot system." International Conference on Smart Computing and Communication. Springer, Cham, 2017.

7. Singh, Abhay Nath, Shiv Kumar, and R. C. Joshi. "Intrusion Detection System Based on Real Time Rule Accession and Honeypot." International Conference on Network Security and Applications. Springer, Berlin, Heidelberg, 2011.

8. Tiwari, Ritu, and Abhishek Jain. "Design and analysis of distributed Honeypot system." International Journal of Computer Applications 55.13 (2012).

ISSN 2690-9626 (online), Published by “Global Research Network LLC"
under Volume: 3 Issue: 5 in May-2022 https://grnjournals.us/index.php/AJSHR