International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 6, September-October 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Data Security using Honeypot System

Rupesh Ananda Mote[1], Kirti Mule[2]

[1]Student, [2]Assistant Professor,
[1,2]Department of MCA, Bharati Vidyapeeth' Institute of Management & information Technology,
Navi Mumbai, Maharashtra, India

ABSTRACT

The internet and computer technology are widely used today to make rapid progress. The increasing use of the internet and computers has led to an increase in information theft attacks. This type of honey pot is used in internet and computer field. This is a great option to use to catch an attack. Records disruptive data at the time of hacking and attacks trades outside the network framework. It can be sent for removal and capture from the attacker's genuine targets.

In this paper the different types of honey pot and in addition the use of conceivable arrangements in a productive environment is simplye described honeypot is a set of dynamic resistive clamps for safety arrangements. It does not interfere, it keeps a record of the honeypot hacking process tools and the movement of different types of new hacking. Honeypots are used either inside or outside the firewall to determine the process of the interloper and the vulnerabilities within the genuine authentic framework.

KEYWORDS: *datasecurity, honeypot, ids, firewall*

How to cite this paper: Rupesh Ananda Mote | Kirti Mule "Data Security using Honeypot System" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-6, October 2020, pp.576-578, URL: www.ijtsrd.com/papers/ijtsrd33418.pdf

IJTSRD33418

1. INTRODUCTION

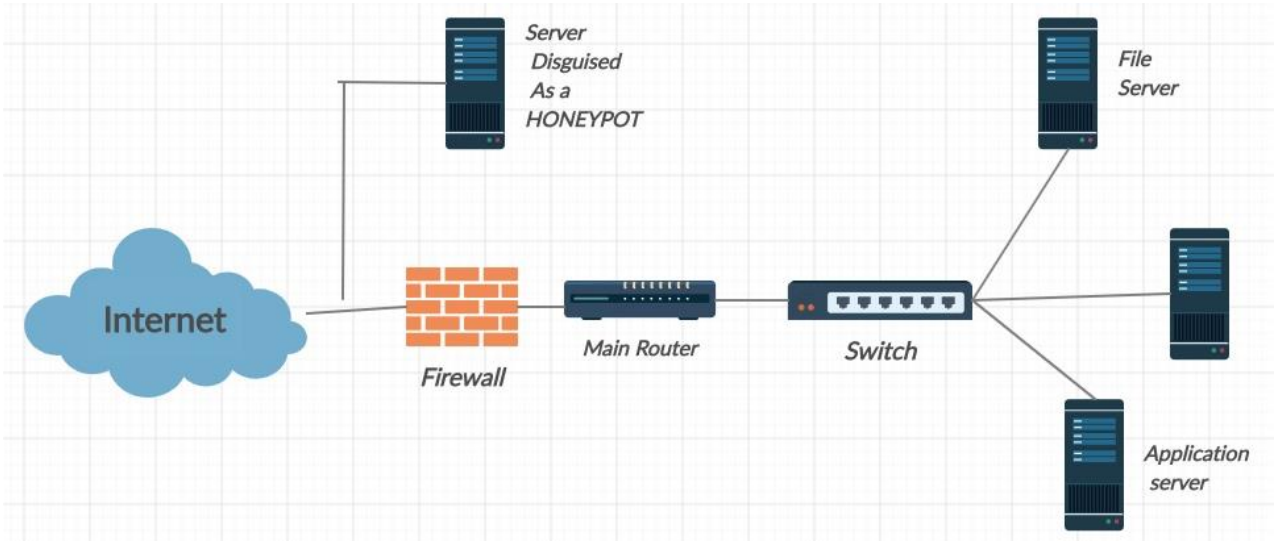
In technical wording, a honeypot is a number of sets of trap to redirect, identify or check endeavors at the not approved utilization of the data frameworks. Honeypot contains a computer, computer information, or a piece or piece of the system side. But he is really segregated and under observed and the attackers seem to have data or valuable assets. This type of honeypot is like keeping an eye on a criminal after a police secret inspection and catching. This honeypot are categorize by their various level of technical interaction. Honeypot with low communication is pretended to be an administrator, to show mimicked administrations from an open port and network to a completely reproduced set of network service. Honeypots use low association honeypots basic content bids to respond to attacker input. New collaboration honeypots are safe as a result of limited capabilities and are difficult to set up.

The disadvantage is that the administration's answers are not fully realized, making it difficult for them to isolate the attackers. Its use is restricted to the logging of interrupt data about devices and computerized attacks and intercept identification. Highly cooperative honeypots have been created, emphasizing that do not purify from medium and high cooperation honeypots is an authentic administration [3].

The main goal is to create a secure correspondence framework that will filter every message and mail exchange between clients for malware and spam. The honeypot framework is used to check every mail or message for unsolicited spam and malware that is stored in the database as a spam word and malware icon. [1] .Honeypot framework will check every mail or message and if it is detected by any spam or malware, alert the director about the action and the message or mail stored in the spam table.

2. Related work

Honeypot is a non-production system, which is used to abuse attackers and track down attack strategies and activities. The goal of honeypots is not just to handle the risk and reduce it yet. Some take honeypots as a framework to lure attackers and review their exercises, so different meanings of honeypots are easy to understand, while others consider innovation to identify attacks or genuine frameworks designed to strike. The feature of the word honeypot in spritzer is as follows: honeypot is a property whose neck is being attacked or traded. That means relying on honeypot to test, to be assaulted and possibly tortured. Honeypots do not settle for anything. They provide us with additional, critical data. In secure defenses, honeypots are used to isolate attackers and take advantage of their attacks and then to change and create a similar framework for protection.



The escape clauses of system security can be secured with the help of data provided by honeypots. Honeypot can be identified as a system-related pc framework for checking the vulnerabilities of a pc or the entire system. Escape clauses can be analyzed as a whole or independently of any framework because it is a high-tech tool to learn about attackers and their systems on the network. Phonepots are usually virtual machines that act like authentic frameworks.

3. Honeypot based on categories:

3.1. research honeypot:

These are honeypots that are controlled by experts and used to secure the data and information of the programmer society. The lessons learned by analysts are used to notice as early as possible, modify attack decision disruption identification frameworks, and outline better tools for security. These are Volunteer controlled, non-beneficiary investigation a teaching foundation for association or data collection about black's thought processes and strategies. The group is focusing on different systems. These are not honeypots increase the value of a particular organization. Instead they are used to find in and out of the association of dangers. Find out how to stay safe from those dangers. This the data is then used to protect against those threats. Inquiry honeypot has the complexity of sending and keeping detailed data and they are used primarily by research, the military, or by government organizations.

3.2. production honeypots:

These honeypots are determined by activities as one system security backbone. These act as honeypots Early warning frame. The objectives of these honeypots are to reduce the risks in the enterprise. It gives data manager about previous attacks. It's hard to use but just caught on data is and is used primarily by or through organizations undertaking; the products are kept in honeypots Coordinate with other generation servers from generation to generation association to enhance their general state of safety. Usually, generation honeypots are less collaborative honeypots, which are less in demand. They pay less data instead of checking about attacks or aggressors let's do a honeypot. Is the inspiration behind the generation honeypot to help moderate risk in association. Honeypot Enhances the association's safety efforts. Of honeypots just give it some fake administration, it works as one working framework and administration emulator. These honeypots are still easy to plan in addition to the plan notable. The attacker can easily use the basic charges recognize that honeypots do not contribute less the driver honeypot is this type of honeyd. Unusual state cooperation gives honeypots authentic just like a working frame, something authentic come to administration with some genuine insecurity allow to capture and record attackers' data exercise and activity. This is an authentic machine a framework, with a system interface with arrangements. An example of this type of honeypot is honeynet.

4. Classification of honeypot

A. Low-interaction honeypots :honeyd

Like the other low-level interaction honeypots, honeyd has no operating system installed. These are some of the goal setting sharewares that we can use. It is configurable, so anyone can create their own services and decide which port to open and how to listen. The hacker will not find any computer or system with the actual operating system, so the main point here is to configure the virtualized network stack. Honeyder basically takes the tcp traffic that the hacker generates. On honeyd, we configured a templates that look like a real system with windows xpOS system and IP_address. Thus, when a hacker establishes a connection with honeyd, honeyd generates fake messages and returns them to the hacker to deceive the hacker. Honeyd is capable of creating many fake ip addresses and running them simultaneously to hackers trying to attack the machine. Unlike other less interactive honeypots, honeyd can handle many different operating systems at the same time. There are two other major benefits to using honeyd. First of all, it can capture connections on any port. This utility makes it easy and great to find network traffic. Another advantage is being able to change services.

B. Medium-interaction honeypots : nepenthes

Now, we come to the part where we talk about the middle ground. Medium level honeypots are often used on the internet for users to learn and be aware of new threats, such as worms and new viruses. Thus, honeypots are used to detect these types of malware and botnets. Their simulation algorithm is based on virtualizing logical response to incoming requests. They do not virtualize the entire operating system requirements and they do not mimic the detailed application protocol. When the request arrives at medium interconnection honeypot the message is viewed and checked and fake responses are generated

Nepenthes is based on five modules which are vulnerability, fetching, shellcode parsing, logging, submission modules. Vulnerability work allows us to create insecure services. Shellcode takes the parsing payload and monitors it and retrieves information about the extracted data. If any important data is found to check, malware is found to bring functionality and the middle part is introduced. You can log in the information you have using nepenthes logging function. Nepenthes is used for most malicious software that spreads over the internet.

C. High-interaction honeypots: honeywall

Following a typical high interactive honeypot factorsare: resources of interest, data control, data capture and external entries. This is also known as gen 2 honeypots and got started development in 2002. It captures and provides better data control mechanism. This increases the level of complexity to deploy and sustain compared to low-communication honeypots.

Makes a copy of the high-communication honeypot a variety of hosting production system activities service and therefore, attackers may be allowed to dump garbage his time in many services. Multiple honeypots can be hosted on a single physical machine by operating a virtual machine. Therefore, it can be restored more quickly if there is a honeypot compromise. In general, provide high-interactive honeypots more security reasons are hard to find, but they are Expensive to maintain. Must have a physical computer if there are no virtual machines, monitoring is done for each honeypot is available which can be extremely expensive.

5. Impingement detection system (ids):

Checking the disruption identification framework (ids) arranges movements and detects any suspicious or unexpected action and alerts the framework or framework manager. Occasionally ids may respond to a move or an impossible or bad action in this way, for example, by preventing the client or resource ip from coming within the framework. The id is easy to implement as it does not affect the existing framework.

The hids framework runs on a host machine or gadget that differentiates between harmful actions on that host. Hids responds to clients with messages / bundles and any suspicious activity.

Nids works on the net between gadgets. This window scans the movement of information for any inconsistencies or harmful actions in this gadget in the system. This framework is responsible for checking and announcing the entire system instead of the host alone.

6. Firewall protection:

The firewall features a secluded section / leave point that allows unauthorized customers to be kept out of protected protection, but sensitive administration is denied access or otherwise left out of the frame and protected against a variety of ip malformations and coordinate ambushes single stiffer point does because security capabilities are integrated into a solitary framework or set of frameworks. The firewall itself is impenetrable for access. This reduces the use of a reliable framework with a secure working os. A firewall is a collaborative programming and equipment that separates an organization's incoming system and different systems. Firewalls cannot block attacks from an internal framework (intranet).

7. Conclusion

Honeypot can be anything from windows to linux. Compared to other disruption identification frameworks, honeypots do not run any beneficial parts on the framework in this light do not create false alarms or log records like other disruption identification framework. There is no compelling reason for monitoring based on interruption signs or definition information, as honeypot logs every byte that goes into the framework system. This information encourages analysts to photograph the attackers. Honeypots have their focus and burden. They are undoubtedly useful tools for catching attackers, capturing data and creating alarms when someone is communicating with them. Exercise of attackers provides useful data for examining their deadly attack mechanisms and techniques. Honeypots only get more information and they don't add because of the chronic information of the demands that come to them.

REFERENCES

[1] *Linnaeus University reference PDF book, School of computer Science,Physics and Mathematics

[2] Thorsten Holz, ―Learning More about Attack Patterns with Honeypots,‖ Proceedings of Sicherheit 2006,

[3] Phillip Porras and VitalyShmatikov, ―Large-Scale Collection and Sanitization of Network Security Data: Risks and Challenges,‖ Proceedings of the Workshop on New Security Paradigms

[4] Bao, J., Gao, M. "Research on network security of defense based on Honeypot", International Conference on Computer Applications and System Modelling, 2010.

[5] Phrack magazine, http://www.phrack.org

[6] Levine, J., Grizzard, J. "Using honeynets to protect large enterprise networks," Security & Privacy Magazine, IEEE, vol. 2, pp. 73-75, 2004.

[7] Michael D. Bailey, Evan Cooke, Farnam Jahanian, Niels Provos, Karl Rosaen, and David Watson, ―Data Reduction for the Scalable Automated Analysis of Distributed Darknet Traffic,

[8] Vinu V. Das, ―Honeypot Scheme for Distributed Denial-of-Service

[9] Abdallah Ghourabi, Tarek Abbes, and Adel Bouhoula, ―Honeypot Router for Routing Protocols Protection

[10] Tobias Lauinger, VeikkoPankakoski, Davide Balzarotti, and EnginKirda, ―Honeybot, Your Man in the Middle for Automated Social Engineering,‖ Proceedings of USENIX Symposium on Networked Systems Design and Implementation,

[11] Spitzner, L.: Tracking Hackers. Addison Wesley,September 2002.

[12] Zanoramy, W., Zakaria, A., et. al, "Deploying Virtual Honeypots on Virtual Machine Monitor".

[13] Qassrawi, M., Hongli, Z. "Deception methodology in virtual Honeypots", Second International Conference on Network Security, Wireless Communication and Trusted Computing, 2010.

[14] Kuwatly, I., Sraj, M. A, "Dynamic Honeypot Design for IntrusionDetection".

[15] SatishMahendraKevat, "Review on Honeypot Security", IRJET Vol. 6, June-2017.