INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2929 - 2933
RECEIVED : 25.02.2018 PUBLISHED : 24.03.2018
March 24, 2018

HONEYPOT NETWORKING-AN HACKER TRACKING SYSTEM

[1]Arockiadoss.A, M.Phil, Research Scholar, K.M.G College Of Arts & Science, Gudiyattam.

[2]Prof.P.Daniel Sundarraj, Head, & Asst. Professor, PG & Research Department Of Computer Science & Applications

Abstract:

Honeypots is a trap set to detect, deflect or counteract attempts at unauthorised intrusion. Honeypots are closely monitored decoys that are employed in a network to study the trail of hackers and to alert network administrators of a possible intrusion. Its system are setup to gather information regarding an attacker or intruder into your system. It does not replace other traditional internet security systems, they are additional level or system. It is being extensively used by the research community to study disputes in network security, such as Internet worms, spam control, DoS attacks, etc. In this paper, we favor the use of low-interaction honeypots as an effective instructing tool to study disputes in network security. We serve as a foundation for this claim by demonstrating a set of projects that we have carried out in a Website, which we have deployed specifically for running various web applications under supervision. The design of our projects acts as a service provider for Honeypot security to various websites. Our project tackles the challenges in installing a honeypot in organizational website, thus determining various security compromises that are performed on it over the Internet by attackers/hackers. In addition to a classification of honeypots, we present a framework to implement honeypot which can be used by any organization to test their website applications/portals and trace characteristics of hackers.

Keywords: Honeybots, Secuirity, Hackers.

1. INTRODUCTION

Honeypots are closely supervised decoys that are employed in a network to read the track of hackers and to alert network administrators of a possible intrusion. Using honeypots provides a cost-effective solution to increase the security structure of an organization. Even though it is not a panacea for security breaches, it is useful as a tool for network adaption and intrusion detection. Production honeypots are easy to use, capture only restricted information, and are used primarily by companies or corporations; They are placed inside the production network with other production servers by an organization to improve their overall attribute of security. Normally, production honeypots are low-interaction honeypots, which are easier to arrange. They give less information about the attacks or attackers than research honeypots do. Research honeypots are run to gather information about the motives and tactics of the Blackhat community targeting different networks. These honeypots do not add direct value to a specific organization; instead, they are used to research the threats that organizations face and to learn how to better protect against those threats.[1] Research honeypots are complex to deploy and maintain, capture extensive information, and are used primarily by research, military, or government organizations. Specter is a commercial honeypot supported by NetSec, a network security company.Specter is a smart honeypot or deception system simulates a complete machine, providing an interesting target to lure hackers away from the real machines. Specter offers common Internet services such as SMTP and FTP which appear perfectly

normal to the attackers but in fact are traps for them to mess around and leave traces without even knowing that they are connected to a fake system which does none of the things it appears to do it Instead logs everything and notifies the appropriate people. Further more, Specter automatically investigates the attackers while they are still trying to break-in.

2. RELATED WORK

Honeyd is a prepackaged OpenSource honeypot designed for the UNIX platform by Neils Provos. It is a low interaction honeypot; therefore, there is no operating system to interact with and it is designed primarily to detect attacks or unauthor-ized activity. Since it is an OpenSource solution and highly customizable, theuser may configure it to listen on any port he/she wants and to adjust the level of emulation to meet his/her specifications. &server level honey pots. Hence there has been always a need for website owners & web development companies for high Interaction website monitoring tools for the attacks. Websites & CMS developed in technologies such as PHP, ASP ,CGI, Javascript , and Ajax have made it much easier for people to build and deploy services on the Internet. Unfortunately, this has opened a wide possibility for new attacks since it is accidentally Introduce new vulnerabilities into it. Therefore, web saites have increasingly been the focus of attackers. Although a lot of web administrator has a lot of choice to choose the more stable and secure open source content management system & websites as their favorite instant deployment medium, they still need to monitor for vulnerabilities and threats that have been occurred on the web servers. For that reason, the web administrator needs an easier way on how to analyze the long and unstructured log file for every server. The best way is to pass on the threat and monitor it on single point like having a proxy within the network to log any [HTTP] hyper text transport protocal request. This project will propose a proper way on how to help the web administrator monitor their entire webserver HTTP request by looking at the log server only instead of having to read every each server log file. scripts could be JavaScript and SQL injections. These sniffers will then acquire the information and store it in our database. All unauthorized activities would then be tracked and stored in an administrative website for future analysis.

3. PROPOSED SYSTEM

Honeypot is term that belongs to the computer system, it's a trap set in order to detect, reflect or somewhere take some counter measures to any unauthorized activity performed by an authorized or an unauthorized person or a system. Honeypot has its own need like it needs a computer system, data and a network on which that computer system will work means that computer system has to be on a network so that activities on a computer system over a network could be monitored. A honeypot is a system with informThe above architecture describe the working of honeypot server. user accesses the website xyz's Data through the internet ,the client server communicate with the honeypot through/via internet. Mean while ,the user is accessing the website xyz's data the honeypot server extracts the necessary characteristics of user and stores the data in the database. the admin accesses the honeypot servers database .the admin accesses the honeypot servers database , to extracts data and perform analysis to check whether the user accessing the website xyz's data is a genuine user or malicious attacker. In this paper, we have proposed honeypot who focus more on web based attacks. This honeypot tool basically aim to work with website and determine the attacks performed on the web based applications. In this honeypot it collect and log data with small amounts of false positives value and negatives value , as it logged data only from the target web

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2929 - 2933
RECEIVED : 25.02.2018 PUBLISHED : 24.03.2018
March 24, 2018

page. The data has high value.hence, we have implemented the database for storing user log data ,GUI designing of the overview,log and Attack Signatures.

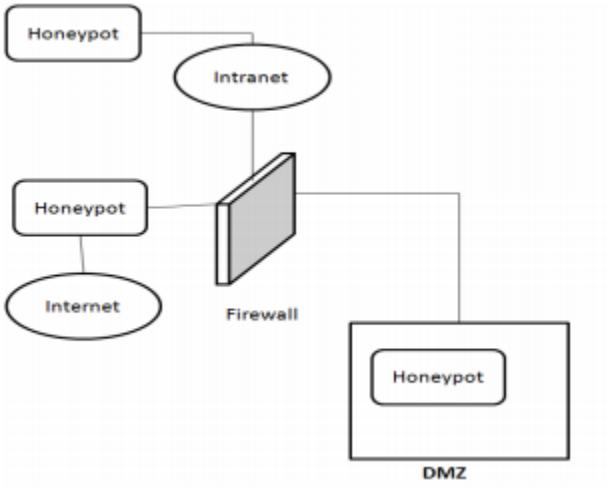

Fig.1.

work on advanced detection features. They used to show is security measures taken to secure a system is good enough to handle a hard attack by attacker or not? This help in knowing what are the security holes in the system. It is possible that a legal access to the system has some unidentified activities to do in it, at that time this honeypot can be used show the harmful intention of person. Because of using advanced detection features, this type of honeypot are capable of capturing those attacks which are not caught by other honeypots. These types of honeypots are easy to use and have limitation of capturing limited information and mostly used in companies or corporations.

4. ANALYSIS

Blackhat attackers are those who are skilled hackers and they utilize their ability in illegal works. A honeypot operator is aware of tools and tricks used by blackhat attacker. So, when a blackhat attacker attacks the system, operator use some of the tools for resolving issues created by attacker in such a way that attacker could not guess what's happening. These honeypot provides a real-live sight of how attack happen. High-Interaction Honeypot are mainly used as production honeypot and Research Honeypot. These honeypots are complex to understand as they involve real operating system and real applications. But these honeypots have high interaction with system so, capture the most unwanted activity performed by the attacker on a computer system and this is their own advantage as well. Other than this, these honeypots do not make any prediction about the behavior of the attacker activity on a system. High interaction honeypot does all the activities that are performed by low interaction honeypot and addition to that they have some other useful features as well. In this position there is direct access of honeypot to the internet. There is no firewall between them. Because of these features, these places honeypots are more open and frankly can be harm by the attackers but these honeypots are also helpful in detecting different unwanted activities. This type of placement is mainly used in case of research honeypots. phases have different working principals. In Training stage, Statistical models were used for generating malware family activities based on detection models. Investigation stage, extract features from statistical models for the purpose of testing data and also matching units which are used for comparing data with malware family activity in order to find whether coming data is somewhere belongs to harmful device or not. In Training stage, Classification is used for

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2929 - 2933
RECEIVED : 25.02.2018 PUBLISHED : 24.03.2018
March 24, 2018

separating malwares in different family. After this separation of malware data, NetFlow is used for executing these samples. NetFlow generates extraction from that data and this extracted data is utilized further between IP addresses and forwarded to destination port.

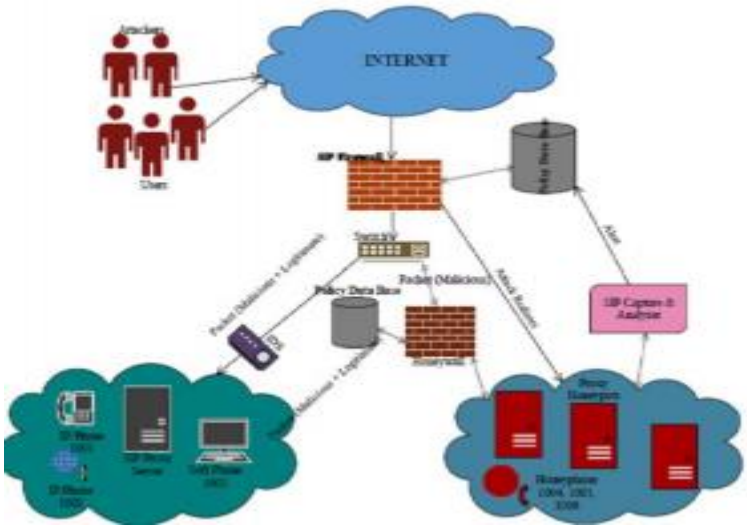

Fig.2.

Other than this, there is modelling unit which is used for combining all vectors with respect to the malware families with their respective families. In matching unit, all the generated feature vectors are evaluated for classification with respect to every model of detection in training stage with the help of clustering algorithm. If outcome of this unit generates any alert, it shows that there is some issue in internal IP of a specific trace i.e. that specific IP is infected. Honeypot is a Sensitive device i.e. it has to be installed where a safe environment is available because in case of unsafe environment there are more chances of accessing IP address and Port number of honeywall so honeypot needs to be provided a safe environment. Honeypot provides an adequate step for improving efficiency rate of system relates to their security.

CONCLUSION

Honeypot is a computer technology which is spreading day by day in virtual environment. It's a technology which is not just for a big organization but this is also beneficial for a single computer system as it provides an additional step in security of a computer system. This technology has lots of benefit but also has some of its disadvantages as well and at present research is on to improve the efficiency of honeypot and trying to overcome its disadvantages. Presented paper discusses about honeypot in complete detail as paper gives all basic requirement of honeypot starting from its history and also discusses some of the latest models which had improved their efficiency just because of addition of honeypot is respective basic design. Paper had discussed all the related aspect of honeypot. If we talk about the future work in the field of honeypot then there is still a big scope as honeypot could be used in many more basic models of intrusion detection system and also could be helpful in improving network security.

REFERENCES

[1] Sepideh Poyan Raad, Hasan Asgharian and Dr Ahmad Akbari, "Secure VoIP Architecture based on Honeypot Technology", in 7th International Symposium on Telecommunications (IST'2014), 978-1-4799-5359- 2/14/$31.00 ©2014 IEEE.

[2] Xiangfeng Suo, Xue Han and Yunhui Gao, "Research on the application of honeypot technology in Intrusion Detection System", in 2014 IEEE Workshop on Advanced Research and Technology in Industry Applications (WARTIA), 978-1-4799-6989-0/14/$31.00©2014 IEEE.

[3] Fatih Haltaş, Abdulkadir Poşul, Erkam Uzun, Bakır Emre and Necati Şişeci, "An Automated Bot Detection System through Honeypots for Large-Scale", in 2014 6th International Conference on Cyber Conflict, 2014 © NATO CCD COE Publications, Tallinn.

[4] Michael Beham, Marius Vlad and Hans P. Reiser, "Intrusion Detection and Honeypots in Nested Virtualization Environments", in 978-1-4799-0181- 4/13/$31.00 ©2013 IEEE.

[5] Sounak Paul and Bimal Kumar Mishra, "Honeypot Based Signature Generation for Defense against Polymorphic Worm Attacks in Networks", in 978-1-4673-4529- 3/12/$31.00_c 2012 IEEE. [6] Osama Hayatle, Hadi Otrok and Amr Youssef, "A Game Theoretic Investigation for High Interaction Honeypots", in First IEEE International Workshop on Security and Forensics in Communication Systems, 978-1-4577-2053- 6/12/$31.00 ©2012 IEEE.

[7] Liu Dongxia and Zhang Yongbo, "An Intrusion Detection System Based on Honeypot Technology", in 2012 International Conference on Computer Science and Electronics Engineering, 978-0-7695-4647-6/12 $26.00 © 2012 IEEE.