ISSN: 2278-4632
Vol-10 Issue-5 No. 9 May 2020

Performance Analysis of Open Source Honeypot Systems

Shambhavi Rai,Manikandan K

Student, School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India
Associate Professor, School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India

Abstract - As the quantity of gadgets connected to a system is expanding everyday we have to guarantee some legitimate safety efforts. Honeypots are exceptionally planned systems that emulate the objective system and draw in the programmer, in the interim all the exercises of the programmer are firmly checked and when any strange movement is distinguished the framework is either cautioned about it or the data of the programmer is put away for future references. Here,we examine about the ongoing patterns and advances in honeypots and survey three open source and effectively accessible research honeypots and play out an exhibition investigation dependent on different parameters.

Key Words: Honeypots, Firewall, Internet Of Things(IoT), Malware, HoneyBOT, KF Sensors, Valhala Honeypot, Zenmap

1.INTRODUCTION

System Security has gotten extremely significant as the entirety of our gadgets these days are associated with a system in one structure or the other. Different advancements like Firewall, Intrusion Detection frameworks, Anti-Viruses are utilized to forestall any undesirable and strange exercises on our gadgets and to forestall the misfortune and abuse of our own information. Honeypots is one such innovation that can be utilized to give extra security to our gadget and information. It can either forestall the assaults or assist us with picking up data about the interlopers by continually observing their activities.Various honeypots existing nowadays incorporate the followings.

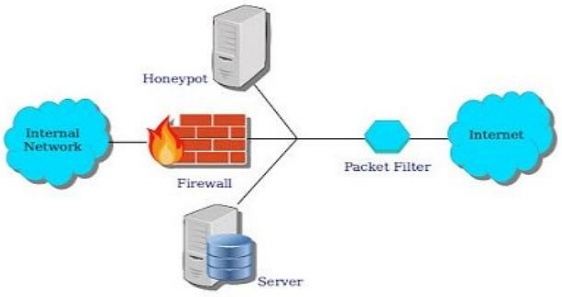

Fig -1: A Simple Honeypot

of Things IoT gadgets, Medical gadgets and other Embedded Operating Systems.

1.2 Malware Honeypots

In these sort of honeypots existing information about the assailants are utilized to additionally forestall any assault on the system. Malware is distinguished dependent on past information about the action example of programmers. These days this innovation is generally utilized in the security of cryptographic forms of money burglary.

1.3 Spam Versions

A lot of defenseless assets are accessible of web for instance open servers that permits mail from anyplace on the web and forward it to it's goal. Spammers regularly misuse this framework and right now demonstrate be a successful countermeasure. IP address and other data about the spammer can be uncovered and along these lines can be utilized to forestall the maltreatment of these open mail transfers and intermediaries.

1.4 Email Trap

Otherwise called spam traps these sort of frameworks are extraordinarily intended to get spam sends from the spammer and afterward the data picked up in the process can be utilized for backtracking the spammer. Task Honeypot is one such innovation that install honeypot pages in the middle of the pages of a site and can additionally be utilized in the backtracking procedure.

1.5 Database Honeypots

Robbery and loss of information is one of the most significant risk to the databases and to maintain a strategic distance from this one sham database is made and at whatever point somebody endeavor to take or change or erase information utilizing SQL infusions data about them is recorded in the framework and can be additionally used to forestall such sort of assaults on the principle databases.

ISSN: 2278-4632
Vol-10 Issue-5 No. 9 May 2020

2. LITERATURE REVIEW

Recognize, redirect and counter, these are the three essential functionalities of a honeypot. It tends to be utilized alone or with the mix of Intrusion Detection framework and Intrusion Prevention System [1]. Different elements that can be utilized to decide the qualities of a honeypot are level of communication, organization condition, asset type, administrations, versatility and usage[2]. With increasingly more innovative work right now new procedures like CAPTCHA , Intrusion Detection Systems and Honeypots are presently consolidated to create security frameworks for the system[3] . In view of their job these honeypots can be isolated into research and creation honeypots every last one of them giving security to the framework by drawing in programmer yet in a marginally unique way[4] . Auto responsive honeypots has additionally been created which can be extremely helpful in counteraction of forswearing of administration assaults[5] . With the presentation of honeypots in 1990, a great deal of improvement have been done till 2020. Be it in business office or research division, honeypots have developed as a drifting innovation [6]. A great deal of honeypots were accessible for kali linux working framework and a couple for windows at first, leap forward came when Java was utilized to execute easy to understand and no problem at all available honeypots in windows too[7] . With more research honeypots began taking new structures and shape for instance presentation of game hypothesis in honeypots to control the programmer expanded the effectiveness of honeypot manifolds[8] . Honeypots can be put with firewall either behind it or before it, or it tends to be joined with De hostile area[9] . Other than that different system log administrator devices like wireshark can likewise be consolidated to create powerful outcomes utilizing honeypots [10].

3. CLASSIFICATION

A honeypot can be arranged dependent on three classes specifically, connection level, organization modes, sending classifications. These classifications are additionally explained in detail in the accompanying subsections.

3.1 Interaction level

In view of collaboration level the honeypots can be grouped into three classifications to be specific, high communication honeypots, medium association honeypots and low cooperation honeypots.

An high level interaction honeypot impersonates the objective system and give access to all the assets and other information. In these honeypots the data gain about the programmer is high anyway the hazard associated with the procedure are fundamentally high as well since the assailant has total access to all the assets.

A medium level interaction honeypot copies the objective system and give access to a couple of assets and other information. In these honeypots the data gain about the programmer is medium and the hazard associated with the process is less when contrasted with high level honeypot since the aggressor approaches just a couple of the assets.

A low level interaction honeypot mirrors the objective system and give access to a predetermined number of assets and other information. In these honeypots the data gain about the programmer is relatively low anyway the hazard associated with the procedure are low also since the assailant approaches a set number of assets.

3.2 Deployment categories

In view of arrangement classifications the honeypots can be ordered into two classes in particular, production honeypots and research honeypots.

Production honeypots are utilized by an association where there is a functioning danger to the assets of the association. Their motivation is to recognize and forestall dangers.

Research honeypots then again are utilized by the system security organizations to gain helpful data about the programmer by checking and recording their exercises.

ISSN: 2278-4632
Vol-10 Issue-5 No. 9 May 2020

3.3 Deployment modes

In light of Deployment modes the honeypots can be arranged into three classes to be specific, deception mode, intimidation mode and reconnaissance mode.

In deception mode, as the name recommends the aggressor is hoodwinked by a copy arrange that looks totally like the constant system. The assailant feels that the reaction it is getting is by the continuous system, the object is to ensure that the programmer utilizes each hacking instrument he has with the goal that most extreme measure of data can be increased about him. This is additionally a case of significant level connection honeypot.

In intimidation mode, the assailant is cautioned about the measures taken on the off chance that the framework distinguishes any irregular action. An admonition is given that the exercises of the assailant are being observed and this drives off a couple of the aggressors, and the others that are still left are checked and their data is put away for future reference.

In reconnaissance mode, the devices are the strategies utilized by the programmer are recorded and this data id further used to create interruption location frameworks. Both the inside just as outer assaults are checked

4. OPEN SOURCE HONEYPOTS

Different open source and free honeypots are accessible on web for our utilization like HoneyBOT, KF Sensors, Valhala Honeypot. These three honeypots were examined and broke down by assaulting the system utilizing ZenMap which is a product that get to the open ports of the framework and consequently giving honeypots a picture of assault. Reaction time and other data were checked and recorded by these systems.An exchange off is done dependent on the investigation of these frameworks and test perceptions.

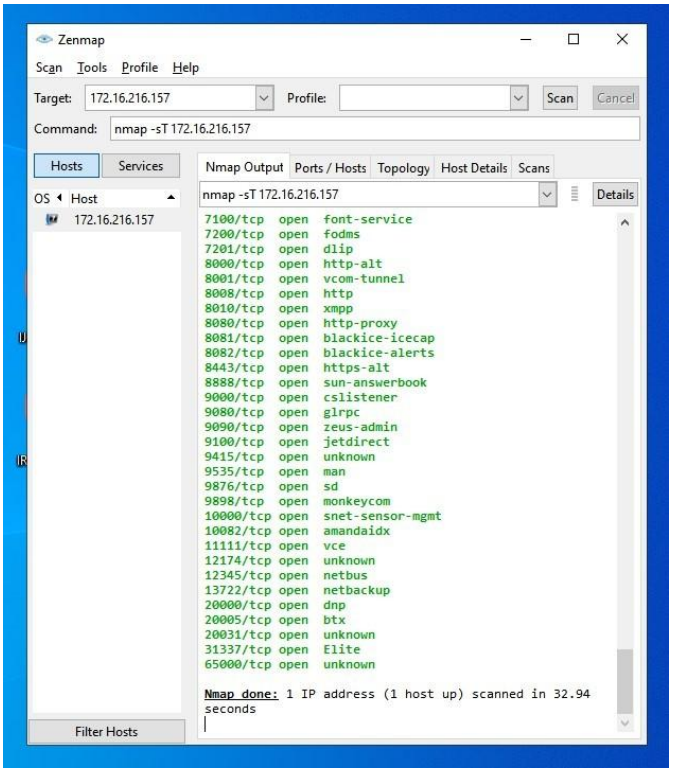

Fig -2: ZenMap Accessing Ports

4.1 HoneyBOT

HoneyBot is a medium level honeypot that reproduce various protocol like echo, smtp, dcom, telnet,radmin, socks, http, ident, pop3 and so forth. There is a choice of including and erasing typical and irregular exercises. An alarm is produced incase of any pernicious action.

4.2 KF Sensors

It is typical financially utilized honeypot which is structured in a manner to draw in the attackers.It reenacts vulnerable trojans and framework administrations. It is now arranged to follow all the UDP and TCP ports. It very well may be altered by the client after the establishment

4.3 Valhala Honeypot

Contrasted with HoneyBot and KF Sensors this honeypot covers a lesser data transfer capacity and can be utilized to screen a predetermined number of ports including ftp, telnet, reverberation, smtp, pop3 and so on. Security settings of these ports and conventions can be changed and altered to a constrained broaden.

ISSN: 2278-4632
Vol-10 Issue-5 No. 9 May 2020

5. TRADE OFF BETWEEN EXISTING HONEYPOTS

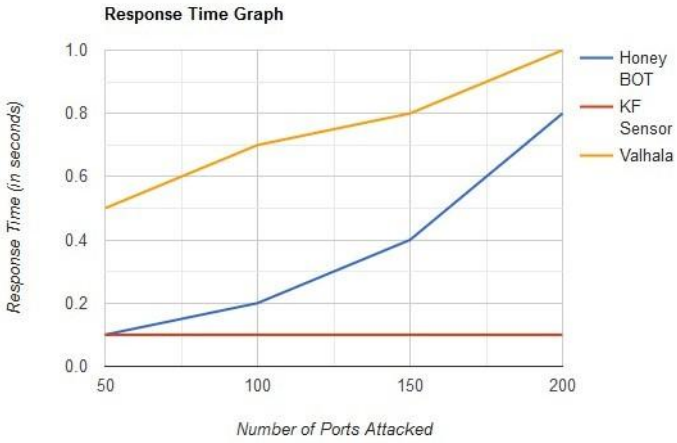

Chart -1: Response Time Graph

Table -1: Comparative study between existing system

	HoneyBOT	KF Sensors	Valhala Honeypot
Level of Interaction	Medium	Medium	Low
Deployement Mode	Deception	Intimidation	Intimidation
Deployment Category	Production	Production	Research
Complexity	Medium	High	Low
Cost	Free	Free	Free
Adaptability	High	Medium	Low
Portability	Medium	Medium	Low
Detection	Yes	Yes	Yes
Prevention	Yes	Yes	No

6. CONCLUSIONS

Honeypots are a decent safety effort for little scope enterprises and a decent research instrument for huge scope businesses. Joined with firewall and interruption detection frameworks it can go about as a security framework that is exceptionally hard to enter. Concentrate ought to be done on making these honeypots increasingly basic and simple to convey so that even individuals with least information can access and use it like Anti-virus. Anyway aggressors continue reviewing their skills and are persevering and subsequently consistent innovative work should be done right now to stay aware of the hackers and keep the gadgets, servers, databases safe.

7. REFERENCES

[1] Rajbhar, Vivekanand. "INTRUSION DETECTION& PREVENTION USING HONEYPOT." International Journal of Advanced Research in Computer Science 9.4 (2018).

[2] Campbell, Ronald M., Keshnee Padayachee, and Themba Masombuka. "A survey of honeypot research: Trends and opportunities." 2015 10th international conference for internet technology and secured transactions (ICITST). IEEE, 2015.

[3] Fraunholz, Daniel, Marc Zimmermann, and Hans D. Schotten. "An adaptive honeypot configuration, deployment and maintenance strategy." 2017 19th International Conference on Advanced Communication Technology (ICACT). IEEE, 2017.

[4] Sekar, K. R., et al. "Dynamic Honeypot Configuration for Intrusion Detection." 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI). IEEE, 2018.

[5] Abdullahi, Mukhtar Ahmad, S. Aliyu, and S. B. Junaidu. "AN ENHANCED INTRUSION DETECTION SYSTEM USING HONEYPOT AND CAPTCHA TECHNIQUES." FUDMA JOURNAL OF SCIENCES-ISSN: 2616-1370 3.3 (2019): 202-209.

[6] Kumar, Dinesh, and Akshay Girdhar. "Network monitoring & analysis along with comparative study of honeypots." 2017 International Conference on Intelligent Sustainable Systems (ICISS). IEEE, 2017.

[7] La, Quang Duy, et al. "Deceptive attack and defense game in honeypot-enabled networks for the internet of things." IEEE Internet of Things Journal 3.6 (2016): 1025-1035.

[8] Toor, Jashanpreet Singh, and Er Abhinav Bhandari. "DEPLOYMENT OF LOW INTERACTION HONEYPOT IN A PRIVATE NETWORK." International Journal of Advanced Research in Computer Science 8.7 (2017).

[9] Kakade, Nilesh, et al. "JAVA Based Honeypot: Intrusion Detection System." (2018).

[10] Kevat, Satish Mahendra. "Review on Honeypot Security." International Research Journal of Engineering and Technology (IRJET) 4.06 (2017): 1200-1203.

