International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 06 | June - 2021 ISSN: 2582-3930

A SURVEY ON HONEYPOT DETECTION SYSTEM IN NETWORK SECURITY USING RASPBERRY PI

Prof. Latha D U[1], Prithvish N A[2], Prajwal M Somanakatti[3],
Sanjay K S[4], Subhash R[5]
[1]Assistant Professor, [2,3,4,5]Students
Department of Computer Science and Engineering, Vidya Vikas Institute of Engineering and Technology, Mysuru.

***Abstract:** This paper presents the survey on role of honeypot in network security, as there are various cyber-attacks are emerging in day-to-day life, privacy become a myth in internet security, many kinds of measures are taken to avoid cyber criminals, among that honeypot is a technology which is built to monitor the traffic in public network, and to find the details of attackers. This device attracts the attackers to execute some exploits and make them fall into the trap. Honeypot is installed with the server to monitor incoming traffic from all the ports, if anyone tries to scan or take a remote connection from the server, honeypot will log all the information of the intruder to the database and gives alert to the administrator, it never going to stop the attack, instead it collects all the information from the attacker through which the intention of the attacker can be determined.*

***Keywords:** Exploit, Raspberry pi, Honeypot, Cybercrime, SSH, Attacker, Network, Nmap and Hacker.*

I. INTRODUCTION

Nowadays, a term "online" comes almost in every field of life, if something is online, security is the biggest concern to be taken care. System tools or software is used which can only prevent or block the attacks, but they cannot provide us the information about the attacker, hence, honeypot is an efficient approach in the field of network security.

A. History of Honeypots:

In 1991, honeypot's idea started with two publications, The Cuckoos Egg" and "An Evening with Breford". "The Cuckoos Egg" by Clifford Stoll implemented his method to catch a hacker that was in his corporation searching for the secrets. And "An Evening with Breford" by Bill Chewick, he and his colleagues made an attempt to catch a hacker who tried to escape from his traps. These two writings led to the start of honeypots.

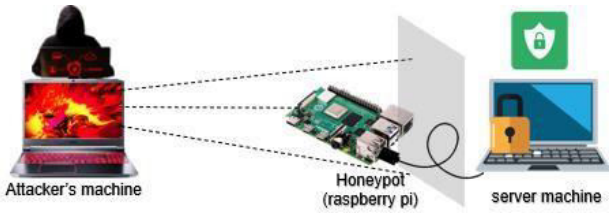
Deceptive Toolkit was the first type of honeypot which was let out in the year 1997. The agenda of this kit was to use deception to attack back. The initial commercial honeypot named Cybercop Sting was released in 1998. It came out to the market in the year 2002. From then honeypot technology drastically enhanced. The Philippine Honeypot project was started in the year 2005 to improve computer security.

B. Definition of a Honeypot:

It is defined as a device in the internet security which explicitly set up to attract and trap those who try to penetrate network traffic of other computer systems. Honeypot is a trap; it is computer system that is present to be a part of the network but have been installed to attract hackers. Honeypot can be defined as an "information system resource whose

Usually honeypots are installed with firewalls, honeypots and firewalls works in opposite direction, honeypots allow all incoming traffic but blocks all traffic that goes out.

In network firewalls most of the honeypots are installed for monitoring traffic and tracking attackers. Honeypot is a special tool to gain the information and tactics of bad guys.



II. LITERATURE REVIEW

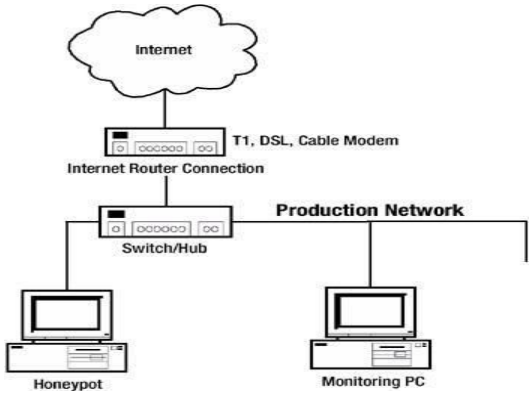
C. Types of Honeypots:

Honeypot appears to be a real system and its task is to fools any person who try to penetrate into the computer system. Based on the deployment, honeypot is classified into two different types and they are

a) Production Honeypot
b) Research Honeypot

a) Production Honeypot

These honeypots are of advanced version as they are built to function with advanced features. They show the security measures that has to be taken care to secure a system. They help in retrieving security holes in the system. Honeypots facilitates a fake system to attack, at



that time it is possible to determine the harmful intention of the attacker. Since it has advanced features, this kind of honeypots can capture the attacks which are not caught by other honeypots. These kinds of honeypots are handy in use and widely used in companies.

b) *Research Honeypot*

A research honeypot has its different purpose for attackers compared to production honeypot. A research honeypot works on the basis of knowing the tricks used by the black-hat hackers. Black-hat hackers are skilled hackers who use their capability in illegal works. A honeypot handling person knows the tools and tricks which are used by black-hat attacker. So, when black-hat attacker tries to attack the system, honeypot person implements some tools to solve problems created by hacker in such a way that hacker cannot even notice what's happening. These honeypots help in live sight of attacks. Based on design criteria, honeypots are classified into four types:

1) Pure Honeypots
2) High-Interaction Honeypots
3) Low-Interaction Honeypots
4) Medium-Interaction Honeypots

1) *Pure-Honeypot*
Pure honeypots are based on production systems. In here, attacker's activities are logged using simple tap which is deployed in the network. There is no need of installing any other software after installing this tap. Pure honeypots give strength to the defense mechanism of a controlled mechanism.

2) *High-Interaction-Honeypot*
High-Interaction honeypot is used both in production honeypot and Research honeypot. These honeypots are bit complex to analyze as they have real operating system and real applications.

3) *Low-Interaction-Honeypot*
These are the honeypots which have limited interaction with the system, it is used for detecting the suspicious activity which are mostly used as production honeypots. The implementation of these honeypots is easy compared to other honeypots; they are simple to configure in the network. These honeypots have limitations that they can log activities up to certain limit and they can capture only known activities.

4) *Medium-Interaction-Honeypots*
These honeypots come between low interaction and high interaction honeypots. These honeypots are highly capable than low-interaction honeypot because it can perform all the activities which is performed by low interaction honeypots but not as much as high interaction honeypot. These honeypots are used as production honeypots but they have more rate of failure.

III. RESEARCH METHODLOGY

Honeypots are used in various fields of technology, there are many purposes for honeypots in a network for instance it can be used in web, databases, cloud, SSH, Malware analyzer, ICS/SCADA and any other services, based on the usage honeypots are classified and developed in the network, this phase explains some of those honeypots.

- *Database Honeypots*
Databases often get attacked by attackers using SQL injection or any other tools, those activities are not detected by basic firewalls, companies tend to use SQL database firewalls which provide fake database to the attacker and fools him and make him fall into the trap and all other activities functions normal.

- *Web-Interaction Honeypots*
Most of the time websites are attacked, web applications, cross-site scripting vulnerabilities shows major vulnerability, possible to deface the website by converting the site into bots, send spam, drive-by-download attacks. Web honeypots can create virtual environment for attackers who tries to penetrate malicious code to the website.

- *Distributed Honeypot*
These are the types of honeypots which are independent of centralized control therefore information of the source attack can be tracked automatically. In these types of honeypots attack information of other subnets can be collected by hidden communication, even the honeypot existed in the same network will not know about this communication. This provides better security and centralized control.

- *SSH Honeypot*
In LAN, local IP address are assigned by router which can be known using some IP scanners within the network through which one can try connect with SSH port using default port or can perform port scanning to obtain the socket address, while in the public internet, one can brute-force/dictionary attacks against remote services running in the server. But SSH honeypot facilitates fake file system to the attacker, when he starts to run exploits, honeypots log all the commands and send an alert to administrator about the attack. Later his intention can be determined by viewing his interaction history.

A. Research Design

The SSH honeypot Cowrie based on Kippo is implemented in Raspberry pi, some of the ports in the server will be kept open, attacker finds open ports as attractive to penetrate some malicious code, he tries to login through remote server, but honeypot redirects all the traffic from default port 22 to 2222 or specified port by the honeypot operator, this honeypot is connected to MySQL database in the backend which logs all the activities which is done by the attacker and simultaneously sends data to the cloud database, an android application which is installed on the phone gives alert to the respective person about the attack and performed activities, also it downloads the attacker's malicious file and send through the application, this application is android based, which can show timestamp, session ID, brute force log, number of success/failure attempts and commands entered by the attacker, later the intention of the attacker can be determined.

Similarly, another honeypot based on SSH is implemented which is a software, built inside the ports, a breadboard is designed with LED lights and buzzer using GPIO pins in raspberry pi, on detecting some traffic in ports will turn on lights and buzzer. Later an E-mail alert or WhatsApp alert is sent to the given ID using API.

B. Sampling procedure

The sampling procedure of this project is collecting the most commonly used usernames and passwords, commonly used ports in network protocols and collection of different social engineering tools.

C. Data gathering

MySQL server, a central monitoring server which is running in the honeypot stores all the information about the attack, also send to the android application, Incoming traffic will be processed via a python script.

D. Data analysis

Data can be analyzed through querying the MySQL database or through android application, The outputs present the tables that shows the statistics page which represents the data.

E. Advantages of Honeypot

- *Data Collection*
  Honeypot stores only the limited data with high value, this reduces the effect of redundancy, honeypot gives the exact information which is required for the analysis purpose for the easy understanding.
- *Simplicity*
  Honeypots have friendly design which is easy to implement, an efficient device to trick the attackers, these are the reasons which is favorable to the company organizations.
- *Network Security*
  Honeypot has various applications in the field of network, it provides a fake network to attract attacker and to prevent organization from the attacks. Honeypots gives an additional benefit by tracking attacker's activity and logging to the database.

F. Disadvantages of Honeypot

- *Narrow Field of View*
  If an attacker breaks into network and attacks other systems, honeypots will be unaware of all those activities because honeypots only respond when activity is directed to them.
- *Common features*
  Honeypots are designed in such a way that when someone falls into the trap of fake emulator, it gives the static output for the commands entered by the attacker, which is easily recognizable by the attacker, if any black-hat finds a honeypot, he could spoof the identity of other systems of the organization and can attack the honeypot, later honeypots may give false alerts that attacks are coming from the company's system.
- *Risk*
  By risk mean, different honeypots show different levels of risk, if an attacker launch an attack to the honeypot, he can even break out honeypot security using few emulated services and then use the honeypot to perform attacks against company or organization. Risk is variable, based on how one deploys and configures the honeypot.

IV. RESULTS

This phase describes the results and outcomes of the project. Based on the tests performed on the honeypots, first step is the discoverability of the honeypot if any person gains authorization to the honeypot. Based on that commonly used usernames, passwords, commands and malware uploads and frequency of those are analyzed.

- *Usernames, Passwords & Commands*
  This section analyses the most common data collected from the honeypot, the purpose of these analytics is to know what common credentials are used by attackers and to know most frequently used CLI commands.

Username	Frequency	Passwords	Frequency
root	1,77,748	123456	2,265
bin	1,519	changeme	823
oracle	1,037	password	575
test	720	-	418
admin	529	qwerty	288
user	421	root	276
testuser	245	1q2w3e4r	272

- Commands

Command	Frequency
uname -a	10
ping	8
ifconfig	6
tracert	5
arp	5
netstat	5
route	4

V. CONCLUSION

Honeypot is a computer technology which is spreading day by day in network security. This technology gives security not only to organizations but also gives additional security to the computer system. It has lots of benefit and has some of its disadvantages, at present research is on improving the efficiency of honeypot and trying to overcome its disadvantages. This paper discusses about role of honeypot and its types in network security, coming to the future work, honeypot could be used in many models in intrusion detection system and could be helpful in enhancing the security. Many researches are going on in order to improve the efficiency of the honeypot. This can be planned to send all the logs to the centralized system, can be monitored through sensors. Finally, we plan to evaluate the effectiveness of the solutions objectively.

VI. REFERENCES

[1] Kippo - SSH Honeypot - Google Project Hosting- Google-Code. https://github.com/desaster/kippo.

[2] The Honeynet project research organization https://www.honeynet.org/

[3] libssh, The SSH Library. https://www.libssh.org/

[4] Cowrie SSH and Telnet Honeypot effort. https://github.com/cowrie/cowrie/

[5] Thorsten Holz, ―Learning More about Attack Patterns with Honeypots, Proceedings of Sicherheit 2006, February 2006, pp. 30-41.

[6] Raspberry Pi Foundation, Raspberry Pi 4 Model B https://www.raspberrypi.org/products/raspberry-pi-4-model-b/

[7] Raspberry Projects – Physical computing with python https://projects.raspberrypi.org/

[8] Nmap – Open-Source Network Scanner https://nmap.org/book/man.html

[9] Medusa – Login Brute-forcer for remote authentication https://en.kali.tools/?p=200

[10] Android for Developers – Online official website https://developer.android.com/index.html

[11] Cowrie SSH honeypot – The Documentation https://cowrie.readthedocs.io/en/latest/

[12] MySQL – Backend database – Android App Connection https://developer.android.com/reference/java/sql/Connection

[13] Live Honeypot Statistics- Logs collected from SSH Honeypot https://securehoney.net/stats.html

[14] Lance Spitzner, L. (2002). Honeypots: tracking hackers, volume - 01. Publisher: - Addison-Wesley Professional.