IMPLEMENTATION AND BEHAVIOUR ANALYSIS OF HONEYPOT

[1]Mintu Patel, [2]Needa Mugut, [3]Shubham Telkar

[1], [2], [3]Student
[1,2,3]School Of Engineering,
[1,2,3]Ajeenkya DY Patil University, Pune, India

Abstract : Honeypot is a mechanism to collect data about the attacker's method and pattern of attack and also get useful information about the intrusive activity. It is a well-designed system used to attract hackers into it. The aim of the honeypot is examining, understanding, observing and following hacker's behaviors in order to make more secure system. When a honeypot is positioned in front of a firewall, it can serve as an early warning system, while when positioned behind a firewall, it can serve as part of a defense-in-depth system and can be used to detect attackers who evade the firewall and the intrusion detection system (IDS). This paper deals with the basic features of honeypots, their use in computer networks and their implementation. It explains the different types on the basis of levels i.e. low level interaction honeypot, medium level interaction honeypot, high level interaction honeypot and functions of honeypots. We will also make a real- life scenario, using honeypots. Different types of honeypot are used in this paper to demonstrate how the honeypots are works in real-time environment and how it react at the time of malicious activity.

Index Terms **- firewall, intrusion detection, computer networks, implementation.**

I. INTRODUCTION

Computer network security has progressively become a very wide field of research. Networking has opened various new fields to explore beyond the limitation. This situation has led to the introduction of new threats to computerized systems. With the increasing rate of cyber-attacks, information safety has become an important issue all over the world. Different techniques have been used to support the security. Firewall filters and create logs to further examine any bad practices. Intrusion detection systems are used to overcome the limitations of existing network. Intrusion detection system observes the network's traffic and notifies the alerts about any kind of intruders. Various issues were seen with the IDS while facing with an increasing number of false negatives and false positives. Honeypots were then introduced in the network to analyze, understand, observe and follow hacker's behavior to secure the system. Honeypots improve IDS by decreasing the numbers of false positives. With the integrated honeypots network security accuracy increases rather than the only implementing Intrusion detection system. Deployed honeypots l must look realistic and is capable for generating logs for all unauthorized activities. Hardware-based honeypots are deployed in big organization as it is expensive and complex to install. Software based low-interaction honeypot are more suitable for the medium and small sized companies. On the basis of detected malicious logs behavior of attacker, tools and methods used by the attacker so that evidence can be obtained and further actions can be taken. In addition of Honeypot in an existing security system can build an active protection system.

1.1 Types of Honeypots

Low Interaction Honeypots

Low Interaction Honeypots allow only limited amount of interface for an attacker . Low Interaction Try to pretend like a large network but works on a single physical host, but can hardly be used to gain information on the application layer. Therefore when it comes to the detection of new botnets and learning about emerging malware technologies, the same restrictions apply here as with application layer based net flow observation.

Medium Interaction Honeypots

Medium Interaction Honeypot provides more emulated services . Scripts makes it more interactable. As attacker assume it as real system try to gain access and attempt various malicious activity and this provides intruder information save in honeypot system log file. These kind of honeypots emulate various services but fail to stimulate as operating system or real system. Also it cannot implement all details of an application protocol. But it interact sufficiently with the intruder to inject the payload in the system, Which is downloaded and extract the shell code and analyzed it. Developing this honeypot is more complex and time consuming and also initially decide the goals for deployment of this type of honeypot.

High Interaction Honeypots

High Interaction Honeypots make use of the real vulnerabilities of a system or software .High-interaction honeypots are highly complex solutions as they consist of real operating systems and applications. In High Interaction Honeypots nothing is outdid everything is real. High Interaction Honeypots provides more information of an intruder or how it progress or how it executed the particular malware in real-time. Since there is no outdid service, High Interaction Honeypots helps in identifying unknown vulnerabilities. But High Interaction Honeypots are difficult to identify by the attacker. High Interaction Honeypots are risky as operating system can be use for attack and can be compromise with the main system. High Interaction Honeypots are used to detect day attack vectors and automatically adapt to any new command and control protocol.

Examples and Functions

There are a large number of open source or commercially available honeypot , such as the following:
Kippo - Kippo records and even allows for replay of the attack.
Glastopf- A low-interaction honeypot that pretend known web vulnerabilities such as SQL injection.
Honeyd- A mid-interaction honeypot that simulates multiple services and hosts on a single machine via virtualization. As a result, it presents a more convincing environment to hackers. Honeyd download the payload and store in honeypot log file for analysis.
Thug- A client-side honeypot that pretend as a web browser. It is designed to automatically interact with the malicious website to explore its exploits and malicious artifacts, often in the form of JavaScript.
Ghost-USB - This mounts as a "ghost" USB drive to serve as a honeypot for malware that uses USB drives to replicate.
Dionaea – Its an malware detecting honeypot which replicates the malwares for analysis purpose.
Tpot - This honeypot provide all in one platform by providing various types of honeypots like Kibana for graphical interface.

Advantages

1. Any activity with the honeypots is unauthorized by definition, therefore reduces false positives.
2. Honeypots are designed to identify and capture new attacks and hence false negatives are reduced.
3. Though it collects data in small sets, it is valuable and easier to analyse.
4. Honeypots act as endpoints, where the activity is decrypted, so the encrypted activities are captured.
5. It is highly flexible as it is extremely adaptable and can be used in a variety of environments.

Disadvantages.

1. Honeypots have limited field of view as they can only see what interacts with them and cannot detect attacks on other systems.
2. Sometimes honeypots can be risky as attacker may take over the honeypot and use it to attack other systems.
3. Fingerprinting: Means attacker can easily identify the honeypot.

II. LITERATURE REVIEW

Navneet Kambow has overview of types of honeypot and its advantages and disadvantages. The author also analyzes the log files through these honeypots and honeynets could be used to enhance the Intrusion detection system to make it smarter in catching intrusions.
Yogendra Kumar and Surabhi Singh has focused on legal issues and they define honeypot as entrapment i.e. "Entrapment is the conception and planning of an offense by an officer, and his procurement of its commission by one who would not have perpetrated it except for the trickery, persuasion, or fraud of the officers."
Marcin Nawrocki∗ , Matthias Wahlisch and other co-authors have made an survey paper on various honeypot software and analyze data and also categorise on the basis of ports.

Ty		First	Last		Services / Applications	Design / Details
	DTK [31]	1997	1999	✓	SMB, SSH, DNS, FTP, Netstat(++)	implement many known vulnerabilities
low	BOF [32]	1998	1999	✓	Back Orifice, Telnet, SMTP(+)	waste intruders time, easy deployment
	NetFacade [42]	1998	2002*	✓	*not specified*	class C network emulation
	CyberCop String [33]	1999	1999	✓	Telnet, FTP, SendMail, SNMP	emulating different network devices
	Specter [44]	1999	2005	✓	SMTP, FTP, HTTP and Telnet(+)	commercial deployment, decoy files
	Sandtrap [57]	2002*	2002*	✓	dialup modem	war dialing trapping
	single-honeypot [43]	2002	2002	✓	*all ports, but no emulation*	mere logging, KISS architecture
	HoneyWeb [68]	2002	2003	✓	HTTP	various web server header emulation
	LaBrea [39]	2002	2003	✓	*all ports, but no emulation*	simple TCP tarpit by SYN/ACK
	SMTPot [58]	2002	2003	✓	SMTP	spam accumulation, KISS
	THP [46]	2002	2003	✓	SSH (shell), HTTP, FTP	coexistence honeypot and real services
	Jackpot [55]	2002	2004	✓	SMTP	delay spam, utilizing spam databases
	FakeAP [79]	2002	2005	✓	802.11b AP beacons	p.o.c wireless honeypots
	HoneyBot [34]	2002*	2007*	✓	SSH, SMTP, FTP, HTML(++)	windows vulnerabilities and GUI
	BigEye [8]	2003	2003	✓	HTTP, FTP	emulation of different web servers
	Spamhole [59]	2003	2003	✓	SMTP	silent dropping of emails
	Spampot [60]	2003	2003	✓	SMTP	platform independence
	HoneyPerl [36]	2003	2003	✓	HTTP, FTP, SMTP, Telnet(+)	extensibility by modules
	Decoy Server [45]	2003*	2003	✓	SMTP, POP3	fake email server traffic
	Smoke Detector [8]	2003*	2004*	✓	FTP, HTTP, IMAP, SSH, SMB(++)	honeypot as a hardware
	NetBait [41]	2003	2007*	✓	*not specified*	honeypot as a service
	HoneyD [28]	2003	2008	✓	HTTP, POP3, SMTP, FTP(+)	emulating heterogeneous networks
	KFSensor [38]	2003	2015	✓	HTTP, SMTP, MSSQL, FTP(+)	commercial deployment of honeypots
	SpamD [56]	2003	2015*	✓	SMTP	tarpit against spam
	HOACD [35]	2004	2004	✓	*compare HoneyD*	live bootable CD (HoneyD, Arpd)
	ProxyPot [57]	2004*	2004*	✓	SMTP	email spammer identification
	Impost [37]	2004	2004	✓	*all ports, but no emulation*	full packet sniffing
	Kojoney [63]	2005	2006	✓	SSH (shell activity)	first dedicated SSH honeypot
	Mwcollect [53]	2005	2009	✓	*compare Nepenthes, Honeytrap*	merging Nepenthes and Honeytrap
	Nepenthes [47]	2005	2009	✓	FTP, HTTP, TFTP, MSSQL(++)	capture worm payload
	GHH [70]	2005	2013	✓	HHTP-Apache, PHP, MSSQL	crawler and search engines
	Honeytrap [51]	2005	2015	✓	HTML, FTP(+), *dyn. emulation*	attacks via unknown protocols
	HoneyPoint [90]	2006	2014	✓	*not specified*	ICS/Scada, back tracking intruders
	Dionaea [49]	2009	2013	✓	SMB, FTP, SIP, MYSQL(++)	nepenthes successor, capture payload

low	Kippo [65]	2009	2014	✓	SSH (shell activity)	emulate entire shell interaction
	Artemisa [73]	2010	2011	✓	VoIP, SIP	Bluetooth Malware
	bluepot [81]	2010	2015	✓	Bluetooth	Bluetooth Malware
	HoneySink [91]	2011	2011	✓	DNS, HTTP, FTP, IRC	bot sink holing
	HoneyDroid [83]	2011	2014*	✓	*compare Kippo, HoneyTrap*	p.o.c Android OS honeypot
	Glastopf [67]	2011	2015	✓	HTML, PHP, SQL	web applications, vulnerability types
	Kojoney2 [64]	2012	2015	✓	SSH (shell activity)	applying Kojoneys lessons learned
	Conpots [89]	2013	2015	✓	kamstrup, BACnet, mosbus	ICS and SCADA architectures
	IoTPOT [85]	2014*	2015	✓	telnet	IoT (ARM, MIPS, and PPC)
	honeypot-camera [86]	2014	2015	✓	HTTP	Tornado Web, Webcam Server
	Shockpot [87]	2014	2015	✓	Apache, Bash	Shellshock vulnerability
	Cowrie [66]	2014	2015	✓	SSH (shell activity)	Kippos successor
	Canarytokens [99]	2015	2016	✓	URLs, bitcoin, PDF	honeypot tokens
	elastichoney [69]	2015	2015	✓	elasticsearch	elasticsearch RCEs
nig	Sebek [97]	2003	2011	✓	Win32 and Linux systems	attackers OS activities, state-based
	Honeywall [93]	2005	2009	✓	*compare Sebek*, CentOS	live bootable CD
	HoneyBow [96]	2006	2007	✓	Win32 Systems	extraction of malware, state-based
	Argos [92]	2006	2014	✓	Linux, Windows XP-7	0-day exploits identification, tainting
	HIHAT [94]	2007	2007	✓	php-BB,-Nuke,-Shell,-Myadmin	PHP framework extension, state-based

OVERVIEW AND CLASSIFICATION OF CLIENT HONEYPOT SOFTWARE BY THEIR INTERACTION LEVEL TYPE. (+) INDICATES SOME ADDITIONAL SERVICES, (++) INDICATES MANY ADDITIONAL SERVICES, (*) MARKS VAGUE TIMESTAMPS.

Savita Paliwal try to give overview on different types of honeypot framework and it's function.

III. WORKING

Honeypot is a system to collect techniques. Honeypots are usually positioned behind the firewall. Honeypot mainly used to put on a variety of services and holes, to attract the occurrence of various attacks, attack data. When an intruder tries to access the system with a malicious activity, the administrator system will be notified. When someone tries to enter the system, a log is generated about all the entries. Even though the attackers gain access in the system and start downloading the data from the database, we can spoof them by storing the fake data which is done by honeypot, but intruder will not be able to know about the fake information. So, by this we can save our system by fooling the intruders. Simultaneously the logs will be generated, and the intruder information like IP address, hardware specification get saved in honeypot and also attack method, that can be used as evidence for further actions.

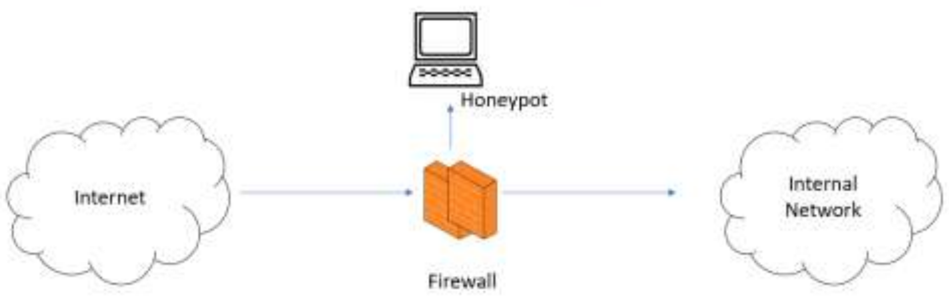


Fig.1. General Figure of honeypot

IV. SYSTEM REQUIREMENT

In our demonstration the following resources was deployed:

1. Virtual Machine (Vmware)
2. Honeypot Packages(Tpot and pentbox)
3. Or iso images disc can directly install in Virtual Machine

4.1 INSTALLATION OF TPOT

Tpot can install on various system which requires designated specification. Depended on goals of organization it can install in following ways:

Standard Installation

Honeypot Packages: adbhoney, ciscoasa, conpot, cowrie, dionaea, elasticpot, heralding, honeytrap, mailoney, medpot, rdpy, snare & tanner

Software or Tools: cockpit, cyberchef, ELK, elasticsearch head, ewsposter, NGINX, spiderfoot, p0f and suricata

Hardware: minimum 6-8GB for better function.

128 GB SSD or more for storing event.

Sensor Installation
Honeypots Packages: adbhoney, ciscoasa, conpot, cowrie, dionaea, elasticpot, heralding, honeytrap, mailoney, medpot, rdpy, snare & tanner
Software or Tools: cockpit
Hardware: minimum 6-8GB for better function.
128 GB SSD or more for storing event.

Industrial Installation
Honeypots Packages: conpot, cowrie, heralding, medpot, rdpy
Software or Tools: cockpit, cyberchef, ELK, elasticsearch head, ewsposter, NGINX, spiderfoot, p0f and suricata
Hardware: minimum 6-8GB for better function.
128 GB SSD or more for storing event.

Collector Installation (goal is to catching credentials)
Honeypots Packages:: heralding
Software or Tools: cockpit, cyberchef, ELK, elasticsearch head, ewsposter, NGINX, spiderfoot, p0f and suricata
Hardware: minimum 6-8GB for better function.
128 GB SSD or more for storing event.

NextGen Installation (Glutton replacing Honeytrap, HoneyPy replacing Elasticpot)
Honeypots Packages:: adbhoney, ciscoasa, conpot, cowrie, dionaea, glutton, heralding, honeypy, mailoney, rdpy, snare & tanner
Software or Tools: cockpit, cyberchef, ELK, elasticsearch head, ewsposter, fatt, NGINX, spiderfoot, p0f and suricata
Hardware: minimum 6-8GB for better function.
128 GB SSD or more for storing event.

For successful deployement of tpot must require a working, non-proxied, internet connection requires for all tpot installation.

4.2 INSTALLATION OF PENTBOX

Virtual Machine (Vmare)
Pentbox Package OR iso image
Harware: Just a normal system

V. ARHITECTURE

General architecture system design of honeypot architecture is shown in Fig-1. Entire network is firstly protected by a firewall, then data layers are separated from network inside the organization and outside customers' or operations' network. Organization network is then protected by a mechanism called as honeynet, which is a network of computers participation in honeypot architecture. For enhancement of security and detection IDS is implemented in the system. Monitoring control system stores the logs created by the honeynet and spectate all the incoming entries in the network. To monitored the system organization need special honeynet administrator.

Hosted Honeypots

Deployments of honeypot on a singular system are said to be hosted. Mainly consist of low interaction Honeypot. As it is deployed on singular physical system , it required minimum hardware and software resources.

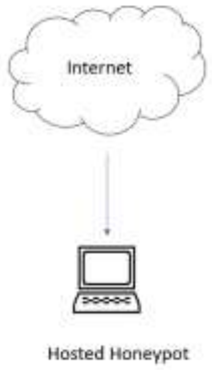


Fig2. Hosted Honeypot

Network (Honeynet)

Honeynets are nothing more than an architecture. To successfully deploy a honeynet, you must plan accurately and deploy the honeynet architecture. The gateway to the honeynet architecture is what we call a honeywall. This is a gateway device that differentiate honeypots from the rest of the world. Any traffic going to or from the honeypots must go through the honeywall. This gateway is traditionally a 2 layer bridging device, i.e. no exposable of main system while interacting with honeynets.Below we see a diagram of this architecture.

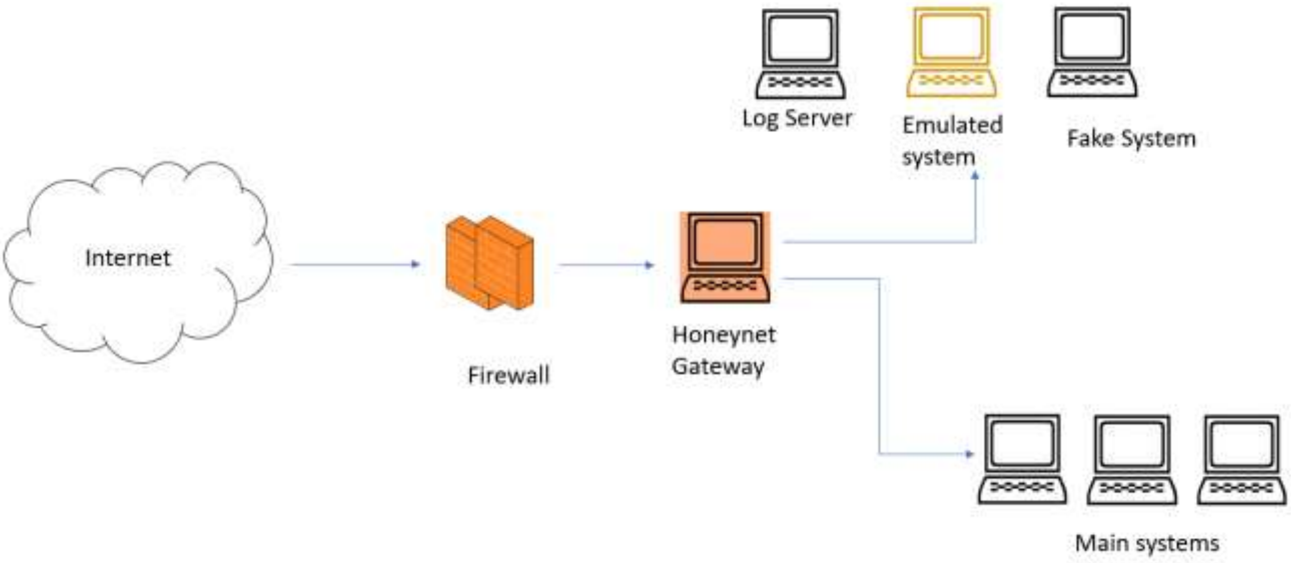


Fig.3. Architecture of honeynet

VI. ANALYSIS (REPORT)

Our hosted Network Detected various intruder and on that basis the following points reveal

1. Most of intruder can not differentiate between real system and honeypot.
2. Most attack was on port no. 80, 23 etc as it is easy to crack.
3. On unsuccessful attempt most of intruder did not attempt again.
4. Only External intruder detected.
5. The inflow traffic was increase after deploying honeypot.
6. The following data id of 1 week on that basis below table and diagram ae created

Sr. No.	Port No.	No. Of Attempts	Name Of Ports
1	80	39.39%	HTTP
2	23	21.21%	TELNET
3	21	27.27%	FTP
4	443	3.03%	HTTP over Secure Shell
5	25	9.09%	SMTP

Table no.01. Intruders attack on the basis of 1 week analysis

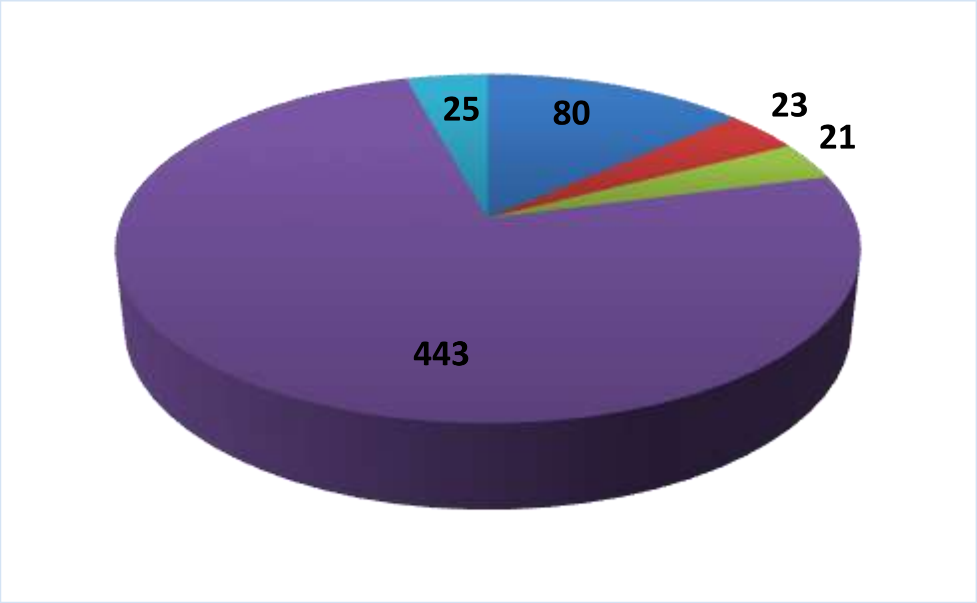
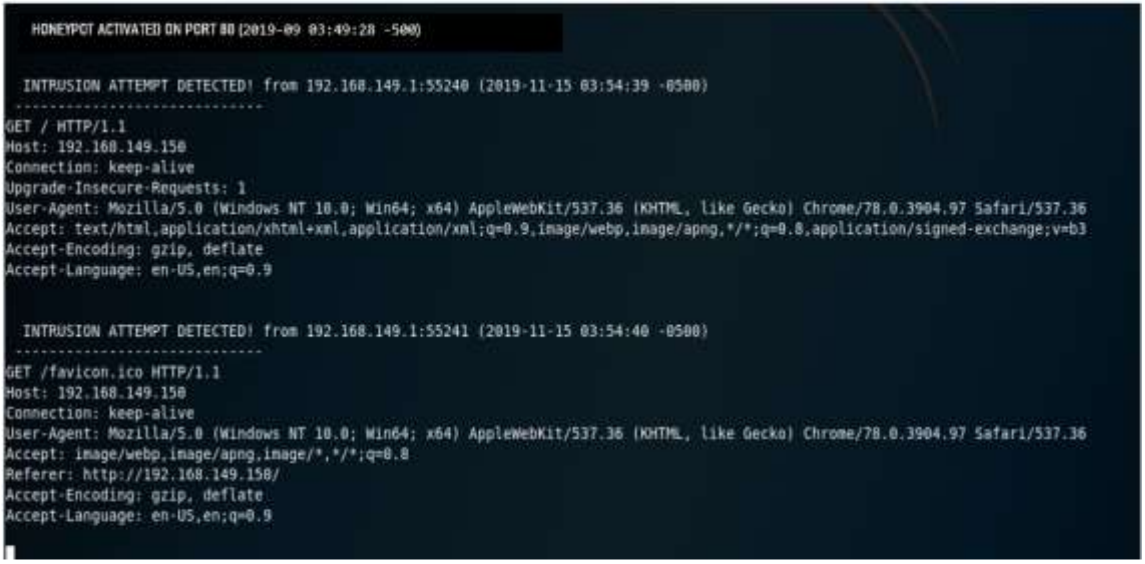


fig.05.Pie Diagram

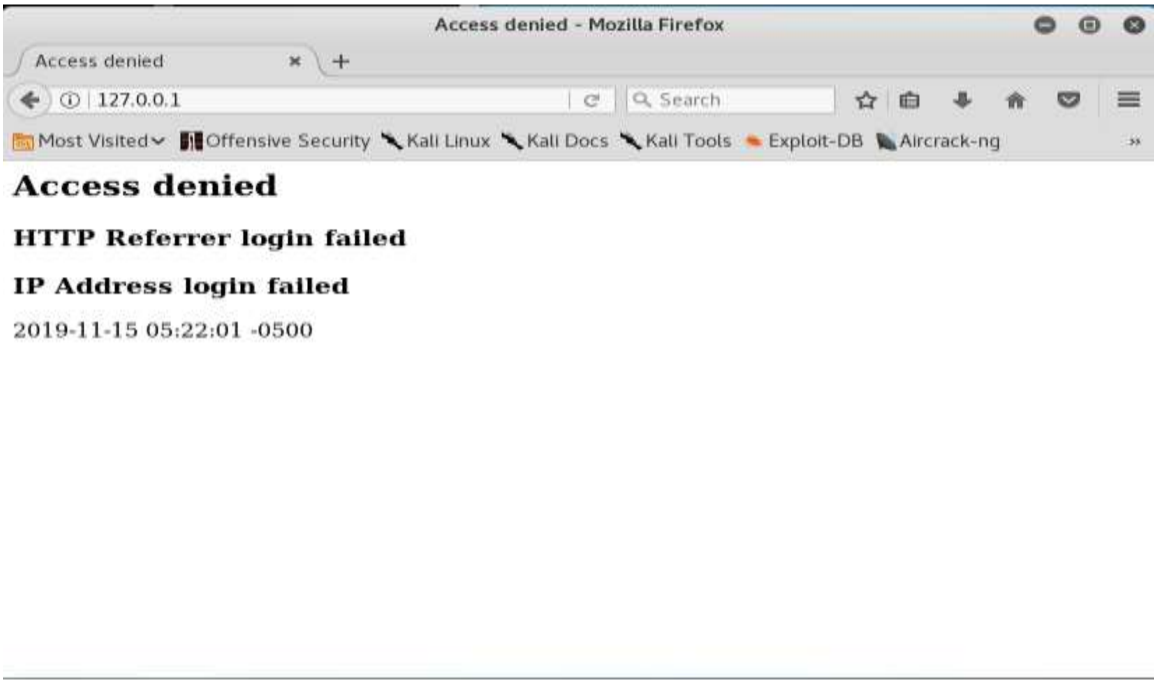


```
 HONEYPOT ACTIVATED ON PORT 80 (2019-09 03:49:28 -500)

 INTRUSION ATTEMPT DETECTED! from 192.168.149.1:55240 (2019-11-15 03:54:39 -0500)
 -----------------------------
GET / HTTP/1.1
Host: 192.168.149.150
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.97 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9


 INTRUSION ATTEMPT DETECTED! from 192.168.149.1:55241 (2019-11-15 03:54:40 -0500)
 -----------------------------
GET /favicon.ico HTTP/1.1
Host: 192.168.149.150
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.97 Safari/537.36
Accept: image/webp,image/apng,image/*,*/*;q=0.8
Referer: http://192.168.149.150/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Fig.5.IDS(pentbox) generates the alert.



Access denied

HTTP Referrer login failed

IP Address login failed

2019-11-15 05:22:01 -0500

Fig.6. Screen from attacker side

VII. CONCLUSION

Honeypot is a useful tool for attracting and trapping attackers, capturing information. Security is the essential element of any organization, though the security provided by the honeypots based on hardware setups are very expensive for small and medium scaled organization. A Software based honeypots are effective for them. Among all these types of Honeypot low-interaction Honeypot is the most used Honeypot, because it is easy to implement and manage but High-interaction Honeypot is most secure and efficient. These honeypots provide security as well as generates a log about all entries in the system which is very helpful to find the intrusive activity in the system. But the honeypot must need to upgrade their policy time to time for new methods and types of attacks. It can't be said as a solution but it is a good enhancement for the security system. Defining the malicious activity are totally depended on how the organisation set their goals and policy. From this paper also can concluded that it is very difficult to detect the internal intruder and complex solution lead to enhancement of security. High interaction Honeypot are complex to deploy but has high security levels.

VIII. REFERENCE

1. Navneet Kambow and Lavleen Kour Passi "Honeypots: The need of network security".
2. Yogendra Kumar Jain and Surabhi Singh "Honeypot based Secure Network System"
3. Marcin Nawrocki∗ , Matthias Wahlisch:" A Survey on Honeypot Software and Data Analysis"
4. Lance Spitzner "Honeypots: Catching the Insider Threat".
5. Monali S Gaigole **"**The Study of Network Security with Its Penetrating Attacks and Possible Security Mechanisms".
6. Maitri Shukla and Pranav Varma "Honeypot: Concepts, Types and Working".
7. Savita Paliwal "Honeypot: A Trap For Attacker"
8. https://dtag-dev-sec.github.io/mediator/feature/2015/03/17/concept.html
9. http://www.omnisecu.com/security/infrastructure-and-email-security/low-interaction-honeypots-and-high-interaction-honeypots.php
10. https://docplayer.net/10290859-Medium-interaction-honeypots.html
11. https://www.scribd.com/document/63436898/Report-Honey-Pots