Types of Honeypot and Comparative Study Based on Level of Interaction Using Single Honeypot

[1]Dhruvi Vadaviya,[2]Mahesh Panchal,[3]Dr. Abdul Jhummarwala, [4]Dr. M. B. Potdar
[1]Student,[2]Deputy Director,[3]Project Scientist, [4]Project Director
[1]Cyber Security,
[1]GTU School of Engineering & Technology, Ahmedabad, Gujarat, India

Abstract-- *Reaching the security of network systems is one of the most essential and popular technology in the area of information technology. One of the method applied for network security is the use of honeypots. Network safety includes recording and analysis of network activities and captures, to find out the proof about the source of the attacks to the device safety.*

Index Terms - Honeypot, Low-level interaction, High-level interaction, Medium level interaction, Honeyd, Intrusion detection, Network security

INTRODUCTION

As the use of the Internet increases, the risk of malicious intrusion increases day by day. The basic security of information sources is characterized by access, availability, and data integrity. Cyber security is a rapidly evolving battlefield between aggressive and defensive cyber capabilities. If a new abuse is discovered and a new type of attack is initiated, cyber defenders should detect these changes and develop countermeasures as soon as possible. Over the last decade, there have been a number of network security tools developed for organizations, such as firewalls, antivirus, and Network Intrusion Detection System (NIDS).

Many organizations today use firewalls, antivirus, and Intrusion Detection Systems (IDS) as part of network security defenses. Firewalls protect organizations by preventing attackers from accessing internal networks and tools. The firewall evaluates the header but ignores the information in the data packet. The antivirus used to prevent the spread of antivirus, the information and validation through certain final goals to control the innovation of the VPN, and even some of the data flow between the headquarters and other points over the public network, such as the Internet. Provides a mechanism that uses NIDS to respond to detected attacks and mitigate the impact of attacks when an organization can detect and identify attacks. NIDS alone is not enough to handle all threats and attacks on computer networks. The network intrusion prevention mechanism also helps to greatly reduce the impact of attacks over a computer network. Network intrusion in conjunction with NIDS, a strong authentication process and a preventive mechanism such as an existing firewall enhance the security of the computer network.

Firewalls play an important role in Network Intrusion Prevention System (NIPS). Even if these precautions continue to occur, computer security systems will still not protect your computer network, even if a new type of attack occurs.

The purpose of network security is to be able to protect the system both inside and outside the network, but it must be able to overcome network attacks, but it can be achieved by a network security method that can be protected.

In addition to these commonly used technologies, honeypots are now attracting much attention. A honeypot is a security tool designed to attack and collect attack data sets to measure and investigate network threats. Honeypots can help by gathering all the information about hackers. The actual information is kept secure on the production system. Honeypots are deliberately made vulnerable to fake services, usually making them look like real systems. Honeypots are typically entities with a specific function and are particularly attractive and can attract attackers to the surroundings. The main purpose of the honeypot is to gather the attacker's strategy. Honeypots can be used to protect computer networks with 'Network Intrusion Detection Systems (NIDS)' and 'Network Intrusion Prevention Systems (NIPS)'. It is distributed with the actual production system but does not expect any legitimate activity. Honeypot can learn to act because it can be thought of as a bait computer system that uses tricks to attract an intruder. Honeypots are computer systems that typically do not have common tasks on the network. By gathering useful information, system administrators can obtain information that can help improve system security. Honeypots also allow attackers to analyze how to exploit system and network vulnerabilities. For more information from the honeypot logs, you can perform forensic analysis on both the network traffic and the damaged host. Honeypots are a very effective way to study attackers' behavior. Honeypot technology is a technique that helps you get information about your goals and methods used to access the security of your current device with hackers, skill levels, attack frequency, and deception.

The Honeypot can log the behavior of the attacker and the scanner by pretending to be a normal machine or device, and then perform further analysis.

Honeypots can be in the form of emulated virtual environments or physical systems, but there is no real work to do. They keep attackers busy, utilize resources and research skills thoroughly. These systems prevent an attacker from freaking out and engaging in illegal activities. We have introduced advanced technology to review honeypot functionality using file system journaling. In order to achieve metadata archiving, file system abstraction provided more in-depth analysis.

As a result, system administrators can learn more about tools and techniques by investigating traces of intruders.

II. RELATED WORK

Honeypots can be grouped at the level of contribution or collaboration or interaction.: 1) Low level interaction, 2) Medium level interaction and 3) High-level interaction

Low-level interaction Honeypot:

This honeypot, called a honeypot, is used as a working framework and a management emulator. Low interaction honeypots emulate multiple decoys at the same time to monitor unauthorized traffic. A low interaction honeypot is a duplication of certain services on the server. These honeypots simply represent an additional perceptible outline. For this kind of legal level interaction honeypot is Honeyd. Honeyd is a small daemon that creates virtual hosts on the network. Honeyd is a network daemon that can control all unused IP addresses on a dedicated network. Honeyd improves network security by providing a mechanism for threat detection and evaluation. This deco can emulate the appearance of the operating system and vulnerable services, but provide little interaction with the other party. It also hides the enemy by hiding the actual system in the middle of the virtual system. Honeyd emulates a vulnerable service or a specific piece of software.

There is a limit to the interaction at a low level. It can help detect attacks, but these interactions can make it easier for low-risk intruders to discover these spoofed services. Low interaction is a disadvantage of Honeyd because it implements forged services.

Medium level interaction Honeypot:

'Medium Interaction Honeypots (MIHs)' can grab a malicious payload and provide far more interactivity to the other. Medium-level interaction honeypots allow limited interaction between the attacker and the system by sending the same request back to the sender. Medium interaction honeypots can emulate full service or specific vulnerabilities and can include a default file structure. They can emulate a variety of vulnerable services using the TCP/IP network protocol implemented and managed by the underlying operating system on which MIH runs. An example of a medium level honeypot is Daemon.

It also has limitations and emulates well-known vulnerabilities. Security programs focus on capturing malicious traffic that accesses emulated and vulnerable services.

High-level interaction Honeypot:

Enables the enemy to provide a full-featured operating system. Using HIH, security researchers can capture network activity as well as system activity. These capture the invader's data and record their movement and activity. However, the limitations of HIH are high resource consumption when used in large deployments. High interaction honeypots improve logging or use virtual machines. There are prices in these technologies. Each action performed by the attacker on the honeypot is longer than the normal system. However, advanced interaction honeypots replicate the entire server and all processes. If you use a high interactivity honeypot, you should update the data with the honeypot to make it look real. High-level interaction Honeypots can handle all requests and respond with a true response using a sandbox virtual machine running real software. High interaction honeypots are useful for forensic analysis because they can emulate the entire system and its functions and allow the attacker to trick you into showing more tricks. Honeypots with different interactions are different. Provide a real working system to communicate with the attacker.

There are also disadvantages of high level interaction honeypot, it has a more serious risk. Another disadvantage is that it is much more reliable, but the design and maintenance costs are much higher.

Honeypots are ordered into taking after classes on their utilization: 1) Research honeypots and 2) Production honeypots.

Research honeypots: These are the honeypots that are controlled and used to protect and learn the data of the programmer's community. Research honeypot, information gathering about threats So we can understand them and defend them. Information gathered by experts is used for early notification, assault decisions, improved disruption detection frameworks, and better device overviews for security.

Production honeypots: These are honeypots that companies have decided to be part of the system security spine.

Honeypots can be used for production purposes by preventing, detecting or responding to attacks. These honeypots fill with an early attention framework. The destination of these honeypots is to expel corporate hazards. Provide data to the administrator before a real assault occurs.

Architecture of Honeypot

Virtual PC can be used to provide intruders with falsified data. Since the placement of administrations is re-created in the system, the honeypot should resemble a true machine to the invader.

So, these are the principal governance bodies that allow honeypots to provide security to the system from programmers.

Working of Honeypot

The purpose of such a honeypot is to prevent as much as possible from compromising or including an intruder to attack the production system. Hybrid honeypot systems often require the ability to tightly control network traffic, for example, to redirect traffic from the front end to the back end for in-depth attack analysis.

Safe Execution Environment (SEE) allows you to deploy and test entrusted software without risking system compromise. This is done by creating a virtual environment in which the software has read access to the actual data. All probes for the honeypot are considered to have established a suspicious connection to the honeypot and are clearly malicious intentional.

In some hybrid honeypots, this type of hybrid honeypot system does not experience the same fingerprint problems because the backend appears to be placed directly on the production network.

The complete and initial response provided by Japonica will greatly reduce the risk of honeypot becoming a stepping stone to attack other hosts, but you need to control traffic to the honeypot. Leverage network data and analyze network activity by applying network intrusion detection systems as well as scenario attack graphs to detect suspicious or corrupted VMs.

Multiple instances of the worm can provide multiple successful connections, or you can use the list of known replicators to hide the exception detectors. Today, 'Software Defined Network' (SDN) technology is widely used in network security research in distributed systems. Because there are no assumptions about attackers and attackers, we use online machine learning approaches to discover enemy goals and actions over time.

Software Defined Networking (SDN) is a new networking paradigm that separates the underlying systems that forward traffic to selected objects (Data planes) and the ability to determine traffic directions (Control planes).

Improvements in real-time operation are required. Early birds suggest a more practical algorithm for payload selection and associate them with a range of unique sources that generate targeted infections and targets.

HoneyStat can generate very precise alerts with zero false positives and detect zero-day worms in the case of some classes of attacks (such as buffer overflows). Other recent honeypots include an additional template and a central server where all honeypot logs are collected.

Honeyware has been developed to overcome two key issues identified in current low interaction honeypots, IP tracking, and geographic location. Honeyware imitates a client browser that interacts with a web browser.

IP tracing is when a malicious server sends the malicious code back to the client after the client has made many requests to the server.

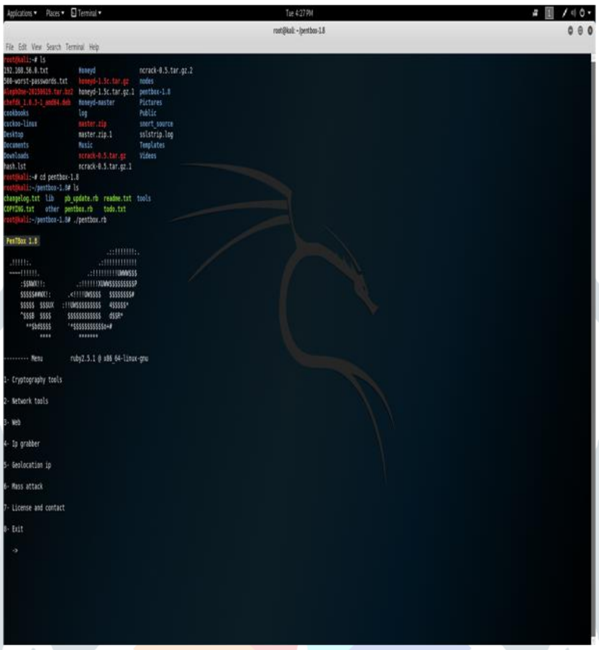
Client-based honeypots are used to detect malicious servers that attempt to exploit clients. Web honeypots are a means of gathering web attack information and developing context awareness of risk perception. On the other hand, server-based honeypots such as ours emulate vulnerable services or software and await attackers.

They also save a copy of the file that the attacker is trying to upload for later analysis. However, these Web honeypots emulate a limited number of vulnerabilities and cannot be easily extended because they require manual support.

III. METHODOLOGY

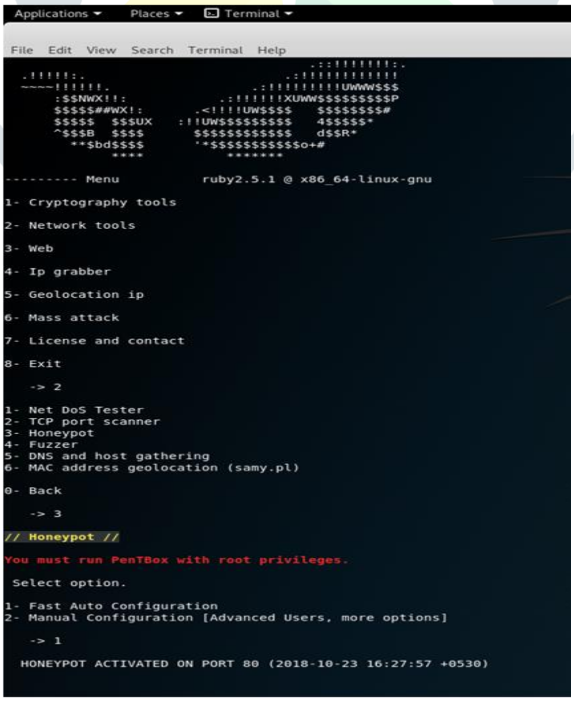
Honeyd is low-interaction honeypot which give user, attack's and attacker's basic information. As shown in below figures Honeyd give a basic information of assaults.

It's "ON" on port number 80, HTTP (Hypertext Transfer Protocol).



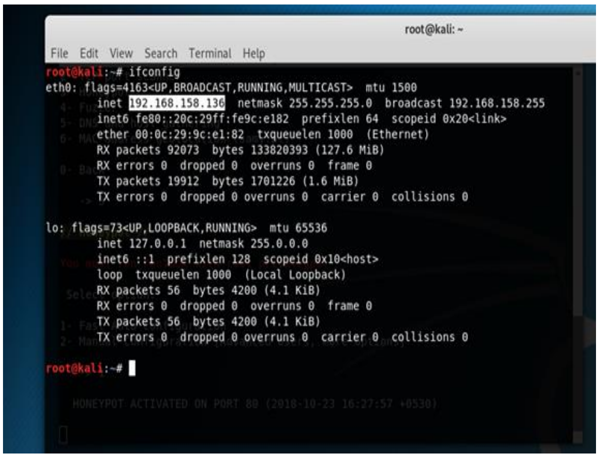
```
root@kali:~# ls
192.168.56.0.txt          honeyd                 ncrack-0.5.tar.gz.2
500-worst-passwords.txt   honeyd-1.5c.tar.gz     nodes
AlephOne-20150619.tar.bz2 honeyd-1.5c.tar.gz.1   pentbox-1.8
chefdk_1.0.3-1_amd64.deb  honeyd-master          Pictures
cookbooks                 log                    Public
cuckoo-linux              master.zip             snort_source
Desktop                   master.zip.1           sslstrip.log
Documents                 Music                  Templates
Downloads                 ncrack-0.5.tar.gz      Videos
hash.lst                  ncrack-0.5.tar.gz.1
root@kali:~# cd pentbox-1.8
root@kali:~/pentbox-1.8# ls
changelog.txt  lib    pb_update.rb  readme.txt  tools
COPYING.txt    other  pentbox.rb    todo.txt
root@kali:~/pentbox-1.8# ./pentbox.rb

 PenTBox 1.8
                                 .::!!!!!!!:.
  .!!!!!:.                        .:!!!!!!!!!!!!
  ~~~~!!!!!!.                 .:!!!!!!!!!UWWW$$$
      :$$NWX!!:           .:!!!!!!XUWW$$$$$$$$$P
      $$$$$##WX!:      .<!!!!UW$$$$   $$$$$$$$#
      $$$$$  $$$UX   :!!UW$$$$$$$$$   4$$$$$*
      ^$$$B  $$$$      $$$$$$$$$$$$   d$$R*
        **$bd$$$$      '*$$$$$$$$$$$o+#
             ****          *******

-------- Menu          ruby2.5.1 @ x86_64-linux-gnu

1- Cryptography tools

2- Network tools

3- Web

4- Ip grabber

5- Geolocation ip

6- Mass attack

7- License and contact

8- Exit

   ->
```

Figure 1. Starting of Honeyd



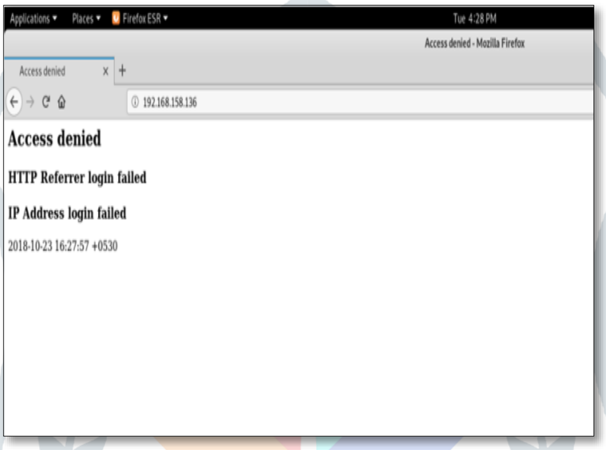
```
                                 .::!!!!!!!:.
  .!!!!!:.                        .:!!!!!!!!!!!!
  ~~~~!!!!!!.                 .:!!!!!!!!!UWWW$$$
      :$$NWX!!:           .:!!!!!!XUWW$$$$$$$$$P
      $$$$$##WX!:      .<!!!!UW$$$$   $$$$$$$$#
      $$$$$  $$$UX   :!!UW$$$$$$$$$   4$$$$$*
      ^$$$B  $$$$      $$$$$$$$$$$$   d$$R*
        **$bd$$$$      '*$$$$$$$$$$$o+#
             ****          *******

-------- Menu          ruby2.5.1 @ x86_64-linux-gnu

1- Cryptography tools

2- Network tools

3- Web

4- Ip grabber

5- Geolocation ip

6- Mass attack

7- License and contact

8- Exit

   -> 2

1- Net DoS Tester
2- TCP port scanner
3- Honeypot
4- Fuzzer
5- DNS and host gathering
6- MAC address geolocation (samy.pl)

0- Back

   -> 3

// Honeypot //

You must run PenTBox with root privileges.

 Select option.

1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]

   -> 1

  HONEYPOT ACTIVATED ON PORT 80 (2018-10-23 16:27:57 +0530)
```

Figure 2. Honeyd "ON" on Port no. 80 (HTTP)



```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.158.136  netmask 255.255.255.0  broadcast 192.168.158.255
        inet6 fe80::20c:29ff:fe9c:e182  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:9c:e1:82  txqueuelen 1000  (Ethernet)
        RX packets 92073  bytes 133820393 (127.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19912  bytes 1701226 (1.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 56  bytes 4200 (4.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 56  bytes 4200 (4.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# 
```

Figure 3. IP Address



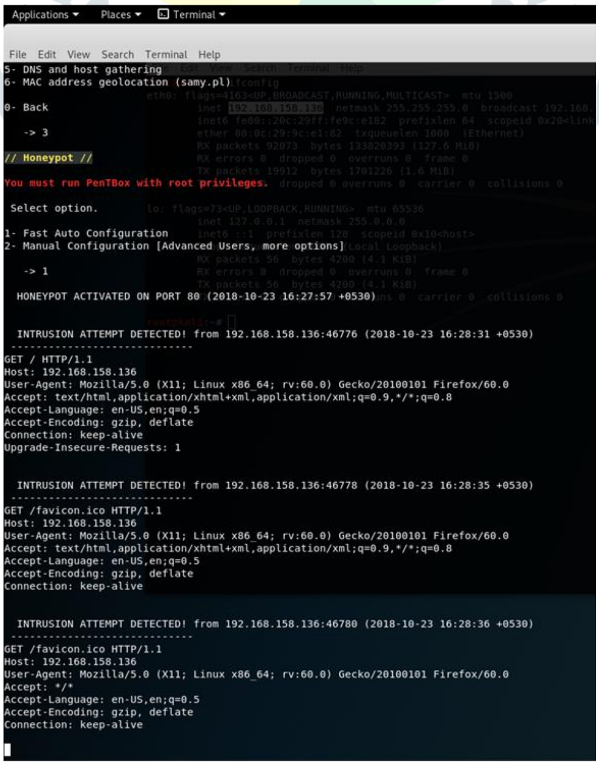
Access denied

HTTP Referrer login failed

IP Address login failed

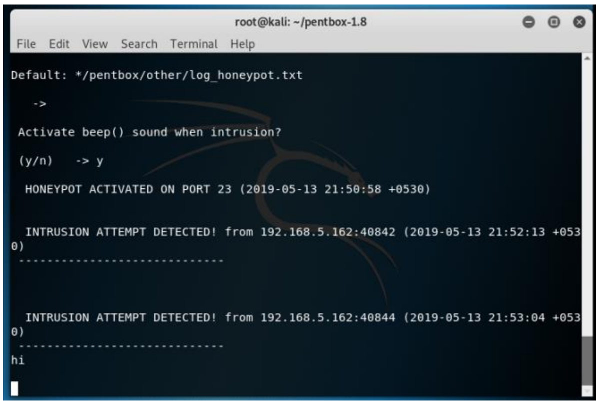
2018-10-23 16:27:57 +0530

Figure 4. Access denied for intruder



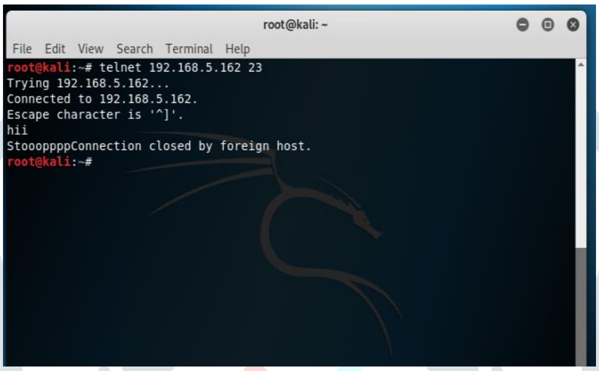
```
5- DNS and host gathering
6- MAC address geolocation (samy.pl)

0- Back

   -> 3

// Honeypot //

You must run PenTBox with root privileges.

 Select option.

1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]

   -> 1

  HONEYPOT ACTIVATED ON PORT 80 (2018-10-23 16:27:57 +0530)


  INTRUSION ATTEMPT DETECTED! from 192.168.158.136:46776 (2018-10-23 16:28:31 +0530)
 -----------------------------
GET / HTTP/1.1
Host: 192.168.158.136
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1


  INTRUSION ATTEMPT DETECTED! from 192.168.158.136:46778 (2018-10-23 16:28:35 +0530)
 -----------------------------
GET /favicon.ico HTTP/1.1
Host: 192.168.158.136
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive


  INTRUSION ATTEMPT DETECTED! from 192.168.158.136:46780 (2018-10-23 16:28:36 +0530)
 -----------------------------
GET /favicon.ico HTTP/1.1
Host: 192.168.158.136
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive

```

Figure 5. Intrusion Notification



```
Default: */pentbox/other/log_honeypot.txt

   ->

 Activate beep() sound when intrusion?

 (y/n)   -> y

  HONEYPOT ACTIVATED ON PORT 23 (2019-05-13 21:50:58 +0530)


  INTRUSION ATTEMPT DETECTED! from 192.168.5.162:40842 (2019-05-13 21:52:13 +053
0)
 -----------------------------



  INTRUSION ATTEMPT DETECTED! from 192.168.5.162:40844 (2019-05-13 21:53:04 +053
0)
 -----------------------------
hi
```

Figure 6. Honeypot "ON" on Port no. 23 (Telnet)



```
root@kali:~# telnet 192.168.5.162 23
Trying 192.168.5.162...
Connected to 192.168.5.162.
Escape character is '^]'.
hii
StooopppppConnection closed by foreign host.
root@kali:~#
```

Figure 7. Intrusion Notification

As shown in all above figures its shows that how low level interaction Honeypot Honeyd works and give a notification about assault and intrusion. In this type of Honeypot its shows only low level interaction information. Its gives limited and basic information related to assaults.

IV. RESULTS AND DISCUSSION

Various types of honeypots share common advances in information control and information capture. The use of individual honeypots is useful when focusing on specific attacks, but there are a limited number of applications to investigate other types of attacks. Using honeypots to collect information about an attack creates a single point of failure in traditional host-based IPS. Once the honeypot is identified, the attacker can blind the IPS against the attack by avoiding "interaction" with the honeypot. An attacker can detect the presence of a honeypot through fingerprint recognition and examine the results carefully at different OSI layers. Existing honeypot solutions can be easily detected and useless by using various honeypot tools. Because the honeypot is known to the attacker to avoid interaction with the honeypot, no countermeasures are created because information about the new attack cannot be collected.

V. CONCLUSION AND FUTURE SCOPE

Honeypot-based network intrusion collaboration systems can create dynamic rules during abnormal behavior or possible intrusion of the network. Honeypot is not an answer to system security, but instead complements other security technologies to create an optional dynamic protection framework for system security. There are two ways you can create a highly interactive honeypot by using a virtual machine or by enhancing the system's logging capabilities. Honeypots work in conjunction with IDS and firewalls to better address reactive behavior, identification, and reactive attacks. Currently, high interactivity honeypots mainly catch script children. Honeypots can be filled with cheat tools appropriate to the version of the item framework as a result of the abuser's ability to capture fake frameworks.

VI. REFERENCES

1. Yarlagadda Durga, Priya Solanki, Sai Krishnam Raju "Overview of Honeypot Technology", International Journal of Engineering Research in Computer Science and Engineering

2. Miguel Hernández y López, Carlos Francisco Lerma Reséndez "Honeypots: Basic Concepts, Classification and Educational Use as Resources in Information Security Education and Courses"Informing Science & IT Education Conference

3. Fan, Wenjun, and David Fernández. "A novel SDN based stealthy TCP connection handover mechanism for hybrid Honeypot systems." Network Softwarization (NetSoft), 2017 IEEE Conference on. IEEE, 2017.Sumitra Samal, Yashaswi Vaidya, Sidak Arora "Honeypots and Its Comparative Study with Intrusion Detection System in Network Security" International Journal of Research April 2018.

4. Gutierrez, Marcus, and Christopher Kiekintveld. "Adapting with Honeypot configurations to detect evolving exploits." Proceedings of the 16th Conference on Autonomous Agents and MultiAgent Systems. International Foundation for Autonomous Agents and Multiagent Systems, 2017.

5. Kumar, Praveen, and Ram Singar Verma. "A Review on Recent Advances & Future Trends of Security in Honeypot." International Journal of Advanced Research in Computer Science 8.3 (2017).

6. Chung, Simon P., and Aloysius K. Mok. "Collaborative intrusion prevention." 16th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE 2007). IEEE, 2007.

7. Prasad, Renuka B., et al. "Design and Efficient Deployment of Honeypot and Dynamic Rule Based Live Network Intrusion Collaborative System." International Journal of Network Security & Its Applications 3.2 (2011).

8. Holz, Thorsten, and Frederic Raynal. "Detecting Honeypots and other suspicious environments." Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC. IEEE, 2005.