# A DISCUSSION ABOUT HONEYPOTS AND DIFFERENT MODELS BASED ON HONEYPOTS

**[1]SNEHIL VIDWARSHI, [2]ATUL TYAGI, [3]RISHI KUMAR**

[1,2]M.tech (CS & E), [3]Assistant Professor (CS & E),
Amity University, Noida, (U.P.)
E-mail: [1]snehil.cse@gmail.com, [2]atultyagi06@gmail.com, [3]rkumar25@amity.edu

**Abstract**—Honeypot is trap spread for an attacker so that his/her activities over a network could be captured and an advanced security feature could be provided to the network. Honeypot trap the attacker in such a way that it becomes difficult for an attacker to know that their activity are under consideration. Honeypot helps in roviding a beneficial effect on a network security. This paper discusses about the honeypot and also provides different useful information about it. In this paper different type of honeypots were discussed along with the history of honeypots. Paper also throws light on some of the models which are based on honeypot. Applications, advantages and disadvantages of honeypots were also discussed. Paper provides a complete detail description of honeypot in a beneficial way.

**Keywords**—Honeypot, VoIP, NetFlow Generation, Cyber Threat Monitoring System (CTMS), Medium Interaction Honeypot.

## I. INTRODUCTION

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 information whose value depends on the unauthorized use of data. Honeypot works over internet as attack by attacker are done over a network. Honeypot is an electronic bait. Its looks to be the part of network but actually it have been deployed to track a hacker with his activities. If we compare honeypot and firewall, we will find a reverse working principal of both of these, as honeypot allows all incoming traffic to come in but stop them to move out whereas firewall stops an unauthorized activity to enter into a system.

Honeypot uses beware technology, is an elective means to save the network and search in order to design a tough system on a descriptive environment. Honeypot generates an alarm to the administrator of the system while attacker attacks the system and provided a wakeup call to the client in order to check out the activities of attacker.

While attacker is performing some activities on system, honeypot will find out the attacker and collect malicious activities along with that it will keep an eye on the behavior of the attacker and record his activities so that it becomes easy to estimate the level of attack and helps in knowing what tool will be required in order to reduce such activities in future.

Honeypot technology is used in network safety defense and different honeypot based distributed intrusion prevention model are developed [8].

This paper is divided into different sections and each section provides some beneficial knowledge of honeypot. Section I, Introduction provides proper knowledge of what is honeypot with the help of different definitions. Section II, throws light on the honeypot system, in which working principal and processing flow of honeypot system is discussed. Section III, Literature review, provides the knowledge of about History and different types of honeypot along with this, this section also discusses some of the models which are working based on honeypot. Some of the applications, advantages and disadvantages of honeypot were also discussed in this section. Section IV, discussion about the conclusion of this paper followed by references.

## II. HONEYPOT SYSTEM

Honeypot is a resource that works over a network, it is designed in such a way that it behaves as a host which attracts the attacker but its main motive is to being attacked by the attacker and get explored over the network, data on it may be fake but looks to be real which gives an illusion to the attacker that it's a real host because of which more attacker will focus on it. Its work is to store and obtain the activities performed by the attacker which is done because of the presence of software which is running in background and stores the network communication between attacker and honeypot host and different analytical tools were used for analyzing that data or activities performed by the attacker and find out the reason of attack. The working principal of honeypot is shown in following figure.

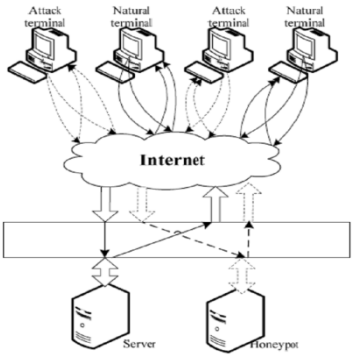


**Fig. 1. Honeypot Working Principal**

A simple honeypot system is basically a combination of three different modules i.e. Induced Module, Deceived Module and Analysis Module. All these three modules have their own functioning and have their own respective roles. Induced module works to attract the attacker towards the honeypot system. As we know that honeypot system have its own database so, deceived calls simulation over that data in database and generate a fake information which sent to the attacker. Activities performed by both of these modules are stored and are being analyzed by the Analysis module which adjust the activities of both of these modules. Below given figure shows the processing flow of Honeypot System.

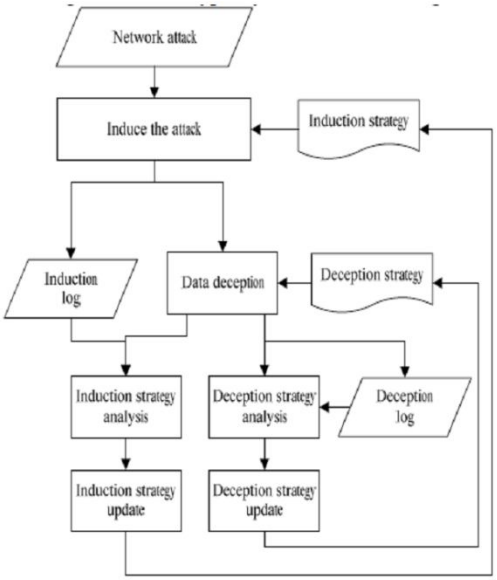


**Fig. 2. Basic Processing flow of Honeypot System**

## III. LITERATURE REVIEW

### *A. History of Honeypot*

In the year 1991, the idea of honeypot started as in this year publications like "The Cuckoos Egg" and "An Evening with Breford" was published. Clifford Stoll was the author of "The Cuckoos Egg" and in his publication he shared an experience of grabbing a Computer hacker which was searching for secrets in his corporation systems. Bill Chewick was the author of "An Evening with Breford" in which Bill and his friends shared their experiences of trapping a hacker in their system. These two publications are said to be the milestones in beginning of Honeypots.

In the year 1997, the first honeypot called Deceptive Toolkit was released in market. But the first commercial honeypot was released in year 1998 and that was known to be Cybercop Sting. In the beginning of the year 2001, honeypot their importance in attack prevention and they were shared and used all over the world. Since then a new era of honeypot had started and lot of research are still going on in this field. At present honeypot is used with different software or models in order to improve their efficiency for capturing hackers and their activities within a network.

### *B. Types of Honeypot*

Honeypot is a look like of a real system and its work is to trap or attract any person who try to penetrate anyone's computer system and based on the deployment, honeypot had been divided into different types and they are as follows:

a) Production Honeypot
b) Research Honeypot

*a) Production Honeypot*

These are the advanced version of honeypot as they 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.

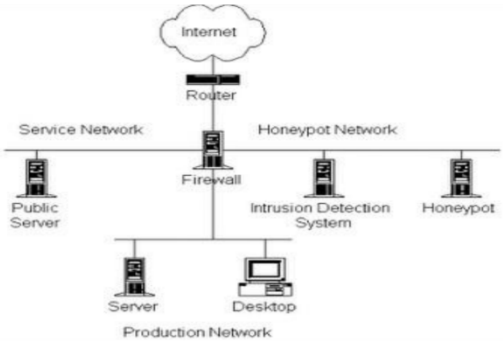


**Fig. 3. Production Honeypot**

*b) Research Honeypot*

A research honeypot has its different approach for attackers as compared to production honeypot. A research honeypot works on the principal of knowing

about the tricks used by a Blackhat attacker and by his community. 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. If we talk about the design criteria, then honeypots are divided in four parts:

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

*1) Pure Honeypot*

Pure honeypot are completely based on production systems. In this type of honeypot, attacker's activities are kept under view by using a simple tap which is installed on honeypot link to any network. After installing this tap, there is no need of installing any other software. Pure Honeypot provides strength to the defense mechanism of a controlled mechanism.

*2) High-Interaction Honeypot*

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.

*3) Low-Interaction Honeypot*

Low interaction honeypot are used for detecting malicious activity and they are used as Production Honeypots. These honeypots have limited interaction with the system and because of which they have limited working capability in capturing activities performed by the attacker on an individual system. There simplicity is their advantage as these honeypots are simple to understand as compared to high-interaction honeypot. There maintenance is also easy as compared to other honeypots. These honeypot have disadvantage that they have limited log to activities as well as they can capture only known activities.

*4) Medium Interaction Honeypot*

These honeypots lies between low interaction and high-interaction honeypots. These honeypots are more capable of low-interaction honeypot i.e. they perform all the activities performed by low-interaction honeypot and more but not as much as that of high-interaction. These honeypots are capable of using all services or particular vulnerability. The main task of these honeypots is to detect malicious activity on a system so, they are used as a production honeypot but along with these features they also have high rate of failure.

### *C. Different models Based on Honeypot System*

*a. Secure VoIP Architecture Based on Honeypot[1]*

*1) SIP Feature*

SIP is a Protocol which works by using text and this protocol was regulated by IETF. This protocol works on the principal of establishment, modification and termination of a particular session established between two different parties with the help of multimedia communication. This protocol has some of its messages types which are required for proper communication, they are;

1. OPTIONS 2. INVITE 3. REGISTER

*2) Attack Stages related to VoIP Network*

With respect to the SIP component, we have three different stages of attacks and they are as follows;

- **Devices Based on SIP and Server Scanning**
  While in the process of designing an attack for a SIP based system, there is a need of destination system in the network. So, it is necessary to find out the location where the destination system is available in the network. Devices working on SIP are liable to answer some of the messages types like; OPTIONS and INVITE.
- **Gathering Important and Starting Information**
  After discovering the destination for attack, next job for the attacker is to gather all the information related to device like IP address, calling Id of communicating parties etc. In order to gather these information related to authorize client and services provided, attacker can use the two message types of SIP features, these are; OPTIONS and REGISTER.
- **Attack to client**
  In this last stage, attacker collects all the remaining details and then finalize the design and Starts the attack. Like in case of SPIT spitter, REGISTER message type along with fake IDS, creates list related to active users, after that it develops and forward a voice spam to the client.

*3) Honeypot Deployment*

Honeypot have some of its components like altering tool, data analyzer, observe, note down etc. For deploying honeypot, we have to follow some of the steps and they are as follows;

- Establish the Goal for honeypot.

- Designing of Honeypot should be done in such a way that it looks like a real system and can artifice the attacker.
- Find the type of honeypot which will be required for deploying i.e. is it low interaction or high interaction honeypot.
- Along with that, honeypot should have tools which provide support to the honeypot and its component for data study, storing and checking.
- Also be ready with a healing strategy in order to reinstall honeypot back to its invariable position.

While deploying honeypot, it has three positions where it could be deployed. Based on the goal and working of honeypot best three locations are as follows;

- *External Position*
  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.
- *Internal Placement*
  In this placement, a honeypot is placed in system location i.e. in the network whereas firewall lies in between the network and outside the network. This placement is mainly used for detecting internal malicious harms to the system that undergo by other protecting walls.
- *DMZ Placement*
  In this placement, honeypot lies by the side of real server DMZ in order to find threats at that location.

*4) Designing of Architecture*

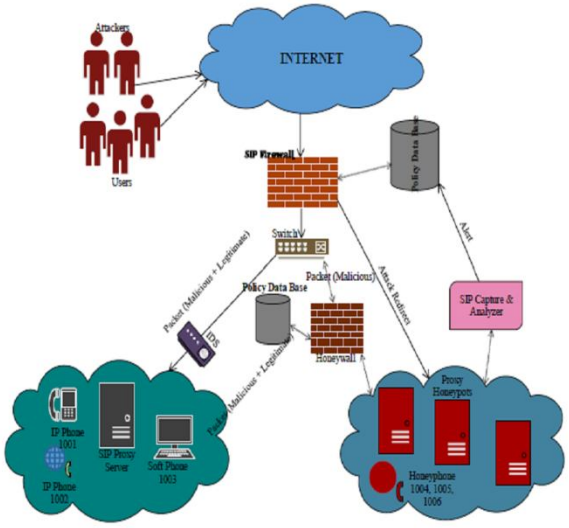


**Fig. 4. Secure VoIP architecture based on honeypot**

Above shown figure shows the behavior of Secure VoIP architecture based on Honeypot. This architecture has some of its main components and these are as follows;

- VoIP Honeypot
  This component works on the principal of using following SIP users, SIP proxy server and SIP end related to their placement. This component is placed with firewall within the network by the side of real location of component. This component causes high communication with the user. This behaves as same as that of a real system within the network which makes it difficult for the attacker to handle honeypot present in the system.
- SIP Firewall
  This firewall is placed alongside of network and has a duty of protecting internal network. This firewall allows the passing of packets in/out within the network based on the header information and based on rules of database.
- Honeywall
  One of the main component of this architecture is honeywall. Honeywall stands between the world outside and honeypot. It helps in setting up all the connections to honeypot but also handle those connections coming through the honeypot.
- SIP Storage
  This component has the duty of recording all the input and output request and response. This component works on database rules, find out the attack and then exposed the received data without any modification. At the end a warning is provided to defense system in order to stop further attack.

*b. Intrusion Detection Model Based on Honeypot Technology[2]*

In order to improve the efficiency of intrusion detection system with its different features like decreasing the missing data, capture hacker information, collecting proofs of detection etc. this model was proposed. This model is the combination of honeypot knowledge as well as Honeypot intrusion automation and electronic forensics automation. Below given figure represents the model of intrusion detection model based on honeypot technology.

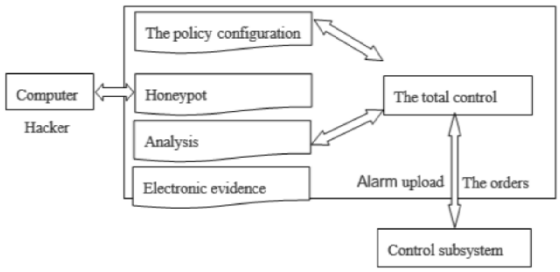


**Fig. 5. Intrusion detection system based on Honeypot Technology**

- Policy Module Configuration
  This configuration requires virtual machine grouping open, select to open or close some of the ports and holes. For a honeypot it requires; data handling, data storing and data storage.
- Honeypot Module
  This module is responsible for flow of in and out within a network which leads to any type of problem that must be recorded. While coming to the network there could be some problems like sniffer, malicious activities, and external network is shown to be breached etc. This module is used to handle all the incoming data and moving out of this model. This module helps in keeping the eye on the hacker along with his/her malicious activities but also allow some of the vulnerabilities to the system which allow the attacker to be functional.
- Real Time Analysis
  Honeypot module has working features of gathering with this module i.e. with real-time analysis module are within same network and used to find out whether there is interruption. For the purpose of analyzing, this module uses two of different analysis techniques i.e. Pattern Matching and Statistical Analysis. Statistical Analysis works for creation of statistical behavior of system or create a template which shows the normal behavior of the system. This template has a main issue with it as of selecting and updating. It is also not that much capable of analyzing unwanted activities.
- Electronic Evidence
  This module contains the basic original data which has effect of intrusion on it and this data is kept for protecting the further basic malicious activities. This module contains a huge database of information and this information is kept in compressed form by using different compression techniques so that by utilizing less space more data could be stored which is beneficial for analyzing malicious activities caused by the attacker.
- The Total Control Module
  Total control Module behave as the coordinator between different modules of this model and data which is interacting with this model. This module along with the work of coordination also generate subsystem alarm in case of malicious activity and generate some command to every control unit of each module.

*c. Automated Bot Control System based on Honeypot[3]*

*1) System Overview*

Bot Finder Honeypot (BFH) has two stages in it i.e. Training stage and Investigation Stage. Both these 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 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. 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.

*2) System Details*

- Cyber Threat Monitoring System (CTMS)
  For this model input data is required which is collected from different sensor locations in wide area. For this model in order to collect input data, different system is used called as Cyber Threat Monitoring System (CTMS). This system is divided into two different parts; Distributed Sensors and Malware detection Centre. These two parts have their own functioning like malware detection center has its sub modules like virtual servers which are required for hosting low and high interaction honeypot, network traffic etc. In this process, it is necessary to classify all the gathered input data via honeypot in order to generate different sample set so that they could also be analyzed at a same time.
- Honeypots, NetFlow generation and Classification Unit
  **Honeypot**—Honeypot has its specific features because of which it has its own importance in network security. It has its features like network traffic control, improving/handling network services, operating system and applications. Honeypots are defined based on their ability to handle malware activities i.e. low interaction or high interaction and also based on their roles on server and client side as well.
  **NetFlow**—Malware families works in virtual environment and their behavior varies according to the situation, in the same way this model also alters its setting based on the changing original manuscript of malware

activities like changing registration keys, contain VM keyboards, change MAC addresses based on Virtual Machine and also by finishing some of services of virtual machine which are related to malware activity.

**Classification Unit**—Classification module is also called as Virus Mu? (It means "Is it virus"). Thus is as similar as VirusTotal whose is executed by using actual version of different antivirus product by various vendors related to VMs. While some are in queue and if one of the files comes to be infected, a tag is assigned to that file and a new naming is started for other files and that infected file sent to its respective malware family name.

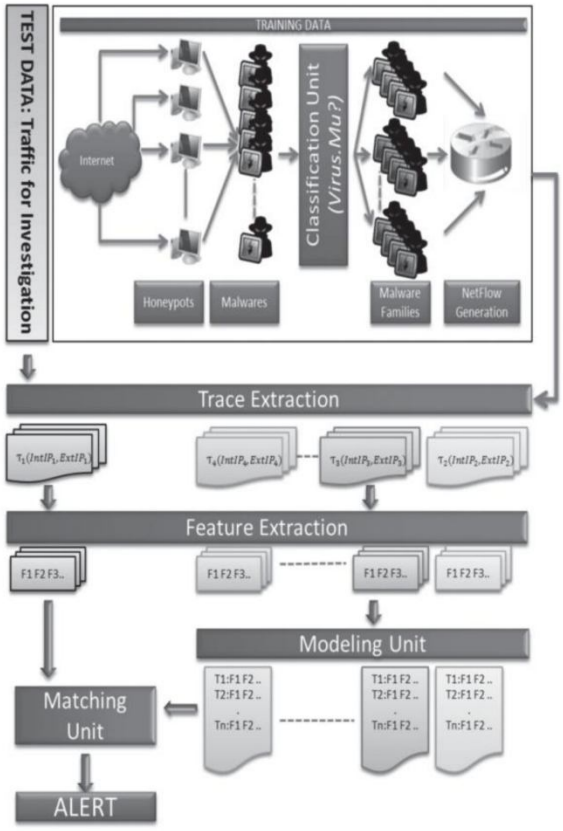


**Fig. 6. System Overview**

- Features

  **Trace Extraction**—This called to be preliminary phase of features. Some statistical models and computational features were used for extracting traces from data generated from NetFlow. Traces generated are used for representing continuous flow in linear order and are mostly used feature in terms of Bot detection algorithm.

  **Features Extraction**—After extracting features, model utilizes such as Average Time Interval, average connection time taken, average number of source byte, average number of destination byte, communication regulation and out coming data accumulation regulation. These all statistical feature are examined based on their flow pair.

- Model Creation and Detection Unit

  **Model Creation**—In a supervised learning algorithm, size and attribute are introduced first before introducing the training phase. So, in this model, unsupervised learning algorithm is used i.e. CLUES (Clustering Based on Local Shrinking) algorithm, for creating detection design for every malware family. In this phase, trace is analyzed for every six features of training data. CLUES algorithm is used foe clustering these features which gives rise to dynamic size cluster without fixing number of clusters. A single cluster have huge number of trace features for a specific malware family, which is generated by classification unit.

  **Detection**—Every feature belonging to investigation data set is being compared separately with every cluster of every detection model which belongs to malicious family. If first feature of a trace (T) is found to be in the scope of cluster of a model (M) then it will be a hit. After that weight of cluster will be added to total hit score. After calculating total hit score, if its value comes to be greater than same features total hit threshold, then count of this feature will relate to model-M.

- Distributed Processing

  Hadoop Distributed File System (HDFS) is used in this model for processing large files with write and read options. It has two parts in it; name node and data node. Name node is used for metadata for files and their management while data node is responsible for storing and retrieving data from that storage place. BFH model has modelling and matching unit and both of these two units' works on traces between IPinternal and IPexternal entity. Hadoop is a large database which has large data in it so main issue comes with it is to handle that data and to move that data on network, reading data and writing data to disk but this type of database provides an additional benefit of maximizing the probability of keeping traces in one data node and reduces chances of moving it over the network.

*d. Honeypot Based Signature generation against Polymorphic worm Attacks in Network[4]*

- Architecture

  Architecture of this model consist of two high interaction honeypots which are independent of each other; Honeytrap1 and Honeytrap2. Both of these honeypot have multiple level of physical honeypots. These honeypots are basically called as Research Honeypots. Main motive behind using two honeypot trap in a single system is to trap the attacker in such a

way that s/he could not be able to know what is going on and all his respective activities over the system could be stored and appropriate could be taken based on those activities. Honeypot used in this design is physical honeypot and these types of honeypots have mainly three layers of software named as; System Software, Sebeck Client and Application Software. Main protection in this system is provided to OS and Sebeck Client.

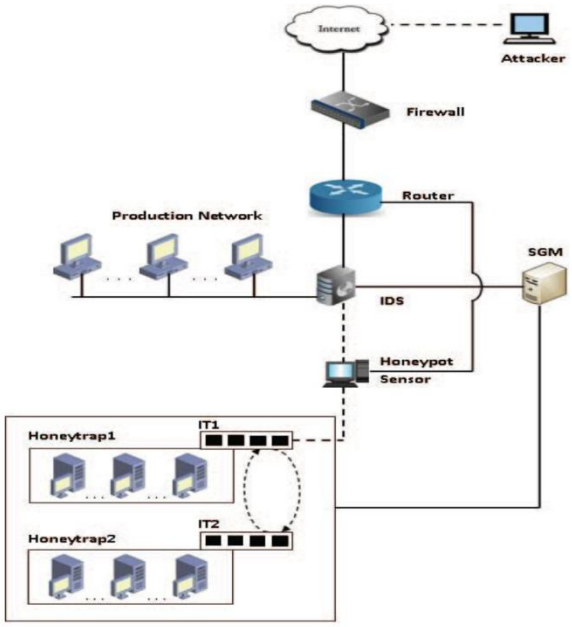


**Fig. 7. Architecture of Proposed honeypot system**

- Data Control
  There is layer bridging from router to honeypot network which separates the entire honeypot design from remaining network. This bridge allow the attacker to come into the system but it depends on the fate of attacker if it want to leave the system or not. Irrespective of the fact that attacker is in the system s/he could not be able to know IP address,
  MAC-address, Routing path etc. because bridge has dual functioning in layer.
  When honeytrap1 receives the attack, it makes an outbound connection and spread the attack in other system. From this trap, traffic is transferred to honeytrap2 with the help of internal translator 1 which works on router. Honeytrap2 also work same as that of honeytrap1 and try to make a connection to outside systems. Honeypot2 uses internal translator 2 for transferring traffic to honeytrap1. This system only allow a particular range of connections only because that will help in completing two purposes easily. First, system is capable of storing enough activities of malicious traffic, second this reduces the possibility of Denial of Service Attack.
- Data Capture
  In order to analyze malicious traffic correctly and to generate signature from that data, different phases of information would be required and for that single layer would not be so effective because of that, this module uses multilayer data storing system. Firewall checks the preliminary header information and also filter out any malicious activity. Second layer of this is between router and honeypot sensor. In this multilayer capture system honeypot is the last stage of storing. It stores different kind of data required for generating signature from warms.

### *D. Applications of Honeypot*

In present time honeypots are widely used in different fields and this paper discusses some of the fields where honeypot has their demands.

*a. Unsafe Environment*

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.

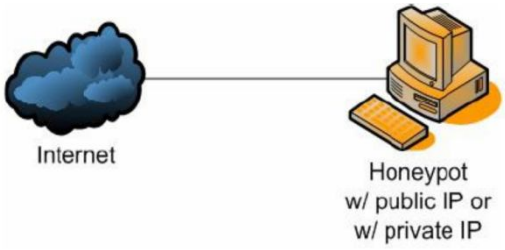


**Fig. 8. Unsafe Environment**

*b. Protected Environment*

In this a firewall is added to the honeypot which limits the access to honeypot system. This firewall helps in protecting the honeypot system related to IP address and Port Number as IP address and Port number can't be accessible to every client. This concept does not affect the continuity but add some limitations.

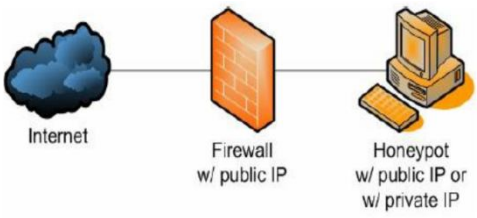


**Fig. 9. Protected Environment**

*c. Network Security*

Honeypot has different applications in field of providing security to network. Honeypot provide network lure in order to prevent network from attack in an organization. By following all the activities of honeypot one can easily find out the viruses and worms. Honeypots provides an additional benefit to the network security by tacking attacker's activity over the network.

### *E. Advantages and Disadvantages of Honeypots*

*a. Advantages*

1. Data Collection
   Honeypot do not require huge data so that it stores only limited data with high value. This reduces the effect of noise. Honeypot gives the exact data which is required and makes it easy for understanding.
2. Simplicity
   Honeypot have simple design, easy implementation which makes it a more favorable method to be used in organizations.
3. Resources
   Many security tools get overloaded in terms of their bandwidth as lot of activity done over network but this problem does not exist in case of honeypot as they store only those data which is coming to them.
4. Honeypot reduces the chances of False positive and False Negative.
5. Honeypots provides a good platform for those who deals in security in order of learning.

*b. Disadvantages*

1. All honeypots have this drawback; if attacker do not send packet to the honeypot, in that case honeypot will not be known of unwanted activity.
2. A Honeypot which is not properly contained will bring risk to rest of the network.
3. For fulfilling their promises, honeypot needs time so, one has to have time for administrating it correctly.

## 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. Research is going on in order to improve the efficiency of honeypot. This paper will help a newcomer to this field to know from where honeypot started and at which place this honeypot is standing at present time.

## 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.

[8] Deniz Akkaya and Fabien Thalgott, "Honeypots in Network Security", in Linnaeus University, Degree Project, 2010-06-29.

[9] Zhang Li-juan, "Honeypot-based Defense System Research and Design", in 978-1-4244-4520-2/09/$25.00 ©2009 IEEE.

[10] W. Y. Chin, Evangelos P. Markatos, Spiros Antonatos and Sotiris Ioannidis, "HoneyLab: Large-scale Honeypot Deployment and Resource Sharing", in 2009 Third International Conference on Network and System Security, 978-0-7695-3838-9/09 $26.00 © 2009 IEEE.

[11] Rajani Muraleedharan, and Lisa Ann Osadciw, "An Intrusion Detection Framework for Sensor Networks Using Honeypot and Swarm Intelligence", in Digital Object Identifier: 10.4108I/CST.MOBIQUITOUS2009.7084.

[12] S. Mukkamala, K. Yendrapalli, R. Basnet, M. K. Shankarapani and A. H. Sung, "Detection of Virtual Environments and Low Interaction Honeypots", in Proceedings of the 2007 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY 20-22 June 2007.

[13] Georg Wicherski, "Medium Interaction Honeypots", in April 7, 2006.
[14] Honeypot Project, "Know Your Enemy: Honeynets", in http://www.honeynet.org, last modified: 31 may 2006.
[15] K.G. Anagnostakis, S. Sidiroglou, P. Akritidis, K. Xinidis, E. Markatos and A.D. Keromytis, "Detecting Targeted Attacks using Shadow Honeypots", in 14th USENIX Security Symposium.

★★★