



VIT[®]
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

HONEYPOT BASED SECURITY APPROACH

CYBER SECURITY-CSE4003

UNDER GUIDENCE OF :-PROF NAVAMANI.T.M

TEAM MEMBERS:-

Names	reg no:
KALAGARA HARI	19BCI0185
M.SANDEEP	19BCE2571
M.PRANEETH	19BCI0177
GEETHIKA ATTHI	19BCE2225

Abstract A honeypot is a deception technique used to entice an intruder to compromise an organization's electronic information systems. A honeypot, when used correctly, can be used as an early-warning system as well as an advanced security monitoring tool. It can be used to reduce the threat of cyber- attacks on computer systems and networks. The system designers research the types of attacks and develop the system upgrade in such a way that it covers all of the system's loopholes. It will be a honeypot-like structure, not an exact honeypot, as the title suggests. Our system will not only record IP addresses and locations in this project, but it will also take screenshots of the user's system so that the photos can be analyzed later and the exact actions can be tracked. The honeypot's main goal is to attract hackers or attackers so that their actions can be recorded. This knowledge is extremely useful because it can be used to investigate device vulnerabilities or to research the most recent tactics used by attackers, among other things. The honeypot will be filled with enough knowledge to attract the attackers. (Honeypot is a sweet lure for attackers, hence the name.

Keywords Honeypot, Real time scenario, Attacker, Attract, Cyber Attacks, Image Capture, Keylogger, Screen Capture.



1. INTRODUCTION

we will be taking the screenshots of the user's system. This device may be installed inside the network, outside of the

Day by day, the number of users connecting to the internet has increased significantly, and with this rise in users comes an increase in malicious intrusions and risk. To detect these intrusions, various systems are being introduced, with honeypot being one of them. A honeypot is a trap set in computer technology to identify and detect unauthorized access to or use of sensitive data. The focus is on gathering as much information as possible about their pattern, programs used, and purpose for attack in a quiet manner. By detecting intruders, a honeypot produces a log that refers to an intrusive operation. It also aids in the reduction of data breach threats. “A honeypot is an information system resource whose importance lies in unauthorized or illegal use of that resource,” says Lance Spitzer, founder of The HoneyNet Project.

This project focuses on similar kind of structure in which we'll not only be taking the record of IP address and location but also,

network, or inside the DMZ. Any action taken by an intruder or attacker within the honeypot can be recorded. A honeypot can record access attempts, capture keystrokes, identify files that have been accessed and updated, and identify the programs that have been run inside the honeypot. We can also determine an attacker's ultimate motives if he is unaware that he is inside a honeypot. A honeypot is a tightly guarded computing resource that we want probed, intruded, attacked, or compromised.

Honeypots are used for two purposes:

Early warning: Honeypots are simple to set up and are more effective than other systems at capturing hackers and malware. With only a single link to it, this honeypot will detect and recognize the intruder.

Forensic analysis: Honeypot captures and isolates malware and attacker resources, then reports back to the user in a few days with a plan based on the data collected by the attackers.

2.LITERATURE REVIEW

The purpose of this literature survey was to study existing solutions concerning honeypot research. The study involved studying various sources available in the literature on honeypots as a network security measure. The literature reviewed indicates that honeypots are of interest when it comes to network security. The amount of information that is produced by countries indicates that honeypots have a role in network security. Honeypots can be used to catch network intruders and also to learn the techniques used by these intruders to gain access to network systems. This information can be applied to other honeypots or the system as a whole.

The Deceptive Toolkit, the first kind of honeypot, was published in 1997. The aim of this kit was to

use deception as a means of retaliation. The first commercial honeypot was released in 1998. Cybercop Sting was the name of the day. In 2002 it was told that the honeypot could be shared and used anywhere in the world. Honeypot technology has come a long way since then, and many users agree that this is only the beginning. In 2005, the Philippine Honeypot Project was established to promote computer security in the Philippines.

After doing a detailed research and analysis of existing methodologies use to implement honeypot, we prepared a literature review table of 12 papers that is given below:

S.NO.	TITLE (STUDY)	AUTHORS	YEAR OF PUBLICATIO N	METHODOLOGY
1	Personalized honeypot for detecting information leaks and security breaches	Ziv Rafalovich, Lior Arzi, Ron Karidi, Efim Hudis	2012	1. Detection and mitigation of particular types of attacks. 2. Logging history of events.
2	Honeypot in Network Security: A Survey	Abhishek Mairh, Debabrat Barik, Kanchan Verma, Debasish Jena	2011	1. Architecture of Honeycomb 2. Signature Algorithm
3	Security and Results of a Large-Scale High- Interaction Honeypot	Mamta Mittal, Lalit Mohan Goyal, Sumit Kaur, Iqbaldeep Kaur, Amit Verma, D. Jude Hemanth	2019	Stationary Wavelet Transform (SWT) and Growing Convolution Neural Network (GCNN) for automatic Segmentation
4	Novel dynamic honeypot system	Hu Yongquan, Wu Yinhe	2020	Virtual honeypot processing templates include a router and a honeypot host, the honeypot host having a plurality of virtual honeypots, each virtual honeypot having a valid IP address; the router is connected with the honeypot host.

S.NO.	TITLE (STUDY)	AUTHORS	YEAR OF PUBLICATION	METHODOLOGY
5	Honeypot-based data processing method, device and system	Wang Pei	2020	The method of claim analog TCP/IP protocol constructs a TCP feedback packet corresponding to the source packet
6	Dynamic service handling using a honeypot	Daniel J. QuinlanOskar IbatullinBryan BurnsOliver TavakoliRobert W. Cameron	2014	The method of claim comprises one of enterprise network or home network and the business application- specific functionality comprises one of e-mail, instant- messenger, firewall, event monitor, event logger, or auditing/journaling.
7	Method and system for improving honeypot trapping attack capability in IPv6 address space	Huang Youjun, Li Xing Wu, Jianping Wang Fei	2020	The method for improving honeypot trapping attack ability in the IPv6 address space according to claim 1, wherein the step of establishing the NS packet in the local segment in-use IPv6 address list included in the local link snooping DAD in S1 extracts an IPv6 address in the NS packet and adds the extracted address to the in-use IPv6 address list.
8	WEB reverse osmosis method, system, equipment and computer readable storage medium based on crawler honeypot trap	Bai Wanjian Liu Qing Deng Hua Xiao Fu Han Xiao Xiaodong Wang Hui Zhang Jinhua Liu Tao Hu Mengqi Zhang Chenyue Wang Ruixin Zhang Liping Ju Junjie	2020	The step of configuring the received access request data into at least one access decision data

S.NO.	TITLE (STUDY)	AUTHORS	YEAR OF PUBLICATION	METHODOLOGY
9	Virtual honeypot	Pushpa B R, Flemin Louies	2014	A method, comprising:configuring an exposed network address in a security appliance, the network address associatedwith a remote honeypot that is located external to a protected network
10	System and method for deploying honeypot systems in a network	Peter FagoneDavi dHendrie	2004	A method of deploying a honeypot system in one or more computer networksconnected to a public data network
11	Managed honeypot intrusion detection system	William Frederick Hingle KruseHassan SultanNicholas Howard BrownJamesLeon Irving, JR.Donald Lee BAILEY,	2016	A computer-implemented method, comprising: receiving a request toprovision one or more honeypot resources, the request specifying one or more computing resource services that are to be used topresent the one or more honeypot resources in conjunction with

		JR.		existing non- honeypot resources

Table1: Literature survey

3. TECHNICAL SPECIFICATIONS

In this project, a honeypot based approach for intrusion detection/prevention systems is proposed.

Language used: Python3

Technologies:

1. **Flask:** A web framework used to develop and integrate our honeypot backend with the web application using various tools, libraries and applications.
2. **Ngrok:** A cross-platform application used to create a secure tunnel from a public URL to our web application running on the system.
3. **WhatsApp** (Twilio API), **Telegram & Gmail:** For sending real-time alerts

The python **libraries and packages** used in the project are:

1. **Flask:** for Flask Connection
 - a. (Flask, render_template, flash, request, Session, redirect, jsonify)
2. **Cv2:** To store face capture image & video
3. **Numpy:** To work on image arrays
4. **Json:** To store data in a json file
5. **PIL (ImageGrab):** To send image on telegram
6. **Io:** To handle IO
7. **Requests:** To handle server & client requests
8. **Time:** For time related functions
9. **Flask_mail** (Mail, Message) : To send mail using flask
10. **Datetime** (date, datetime) : For date & time related functions
11. **json, simplejson:** To retrieve credentials from json file
12. **Os, twilio.rest-Client:** To send WhatsApp message.

4. Modules and their Description

Initially We will develop our own organisation website with a login portal which will be the system where the honeypot technology will be implemented. First, the input will be given by running the Python script (Hash-conversion), where the user will enter the correct login credentials like Username and Password of the specified authentic user of the system.

Login portal:

The user will then login to the portal on the web server.

If the Credentials are correct, as entered in the Python script, the user is legitimate and is successfully logged in and redirected to his/ her v-top account.

If the Credentials are entered incorrectly thrice, then the backend detection mechanism starts executing and the following things are implemented to detect and identify the intruder

IP Address, Location and other important details of the attacker's system are tracked and stored.

We have also carried out several other experiments in-order to inform the user regarding the intruder or attacker and the other activities carried out by him. Since all the information and activities of the intruder are stored we have experimented in informing through the following:

→ **Email:** Through this medium we informed the user about the IP address, location, city, country, organisation, Region along with the above information the real time Screenshots, Video-captures, Face captures of the intruder are attached to the mail, and embedded inline.

→ **WhatsApp:** Through this medium we shared the real time screen captures and the face captures of the intruder or attacker, along with other important details like date and time of attack, and whether the alerts have been sent successfully or not.

Keylogger script – All the intruder activity on the Web Server is tracked, each and every action that he does after the unsuccessful login attempts, are recorded and stored, along with the real time screenshots of the system.

Real time image of the Intruder is captured through his system's camera, without the knowledge of the attacker that the detection mechanism is running and capturing his face

INPUT:

- First, the input will be given in the Python script which will be the Login Credentials like Username and Password of the specified authentic user of the system. The backend will convert password to hash password for security purpose.
- This data gets stored in a JSON file containing username and hash password of a specified user, which would be used for logging into the web application.

→ **Telegram:** Through this medium, we shared the keylogger system screenshots (real time) of the attacker's system. All the admins of the system, who are living in geographically different locations, will be alerted at the same time.

Login portal of the Organisation website – Correct or Incorrect user credentials in the case of genuine users and attackers/intruders respectively.

OUTPUT:

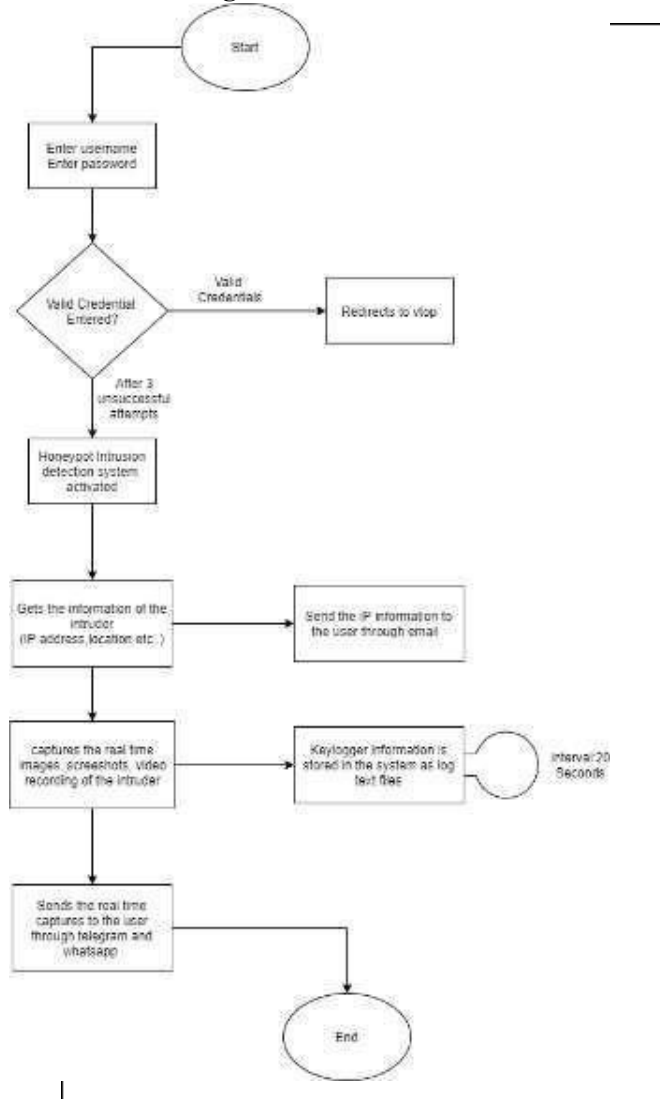
Genuine User: If the credentials are correct, the output after a successful login would be redirected to the VTOP portal of the user.

Intruder: If the credentials are invalid/wrong, after 3 unsuccessful attempts we will get the following things in output –

- Intruder's system information – IP Address, Location (Coordinates, City, Country), Region, other details like hostname.
- Keylogger information – Tracking of intruder's suspicious activities, storing it into a log text file, and a new folder is created with real time screenshots of the system.

Real time image and video captures of the intruder's face.

Block Diagram:



5. IMPLEMENTATION

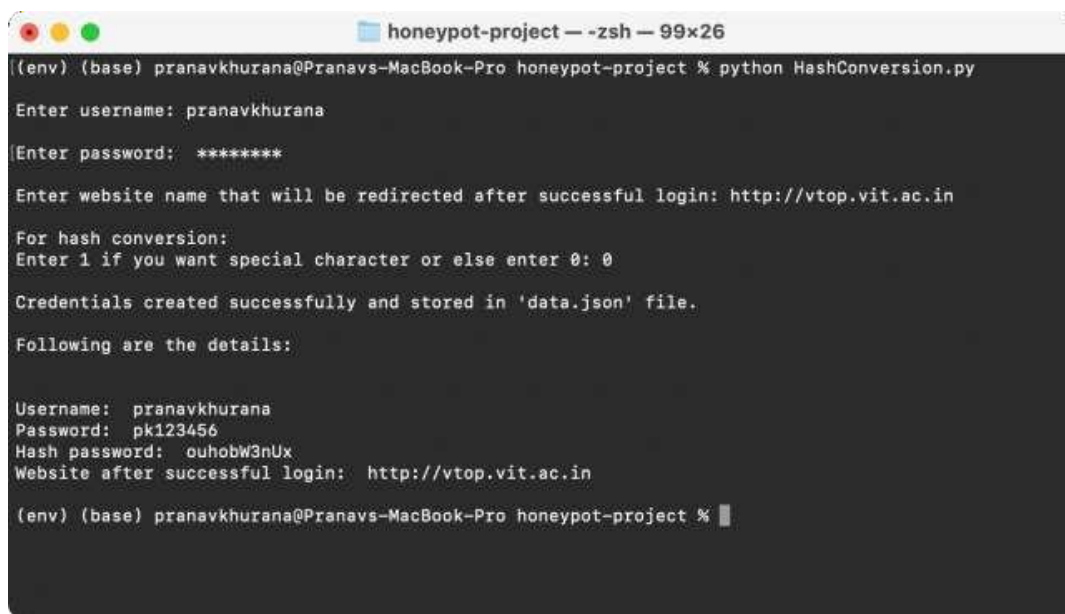
Our project's results aim to secure the intruder attacks by implementing the honeypot technology. When an attack is being performed on the system, the unusual attempts are detected through the methodology that we have proposed. A very strong system is implemented in the point of Information Security Management.

We implemented a honeypot like structure in which

we didn't focus on **recording the IP address** but we worked on recording the **real time screen shots** of the suspect system. If we find any **suspicious activity** like not able to login into the portal for more than twice then the portal will start taking the screenshots of the system and these images can be studied later to know the exact activity of the user. If the consumer is found to be suspect, legal action against him or her can be taken.

Implementation Screenshots Input:

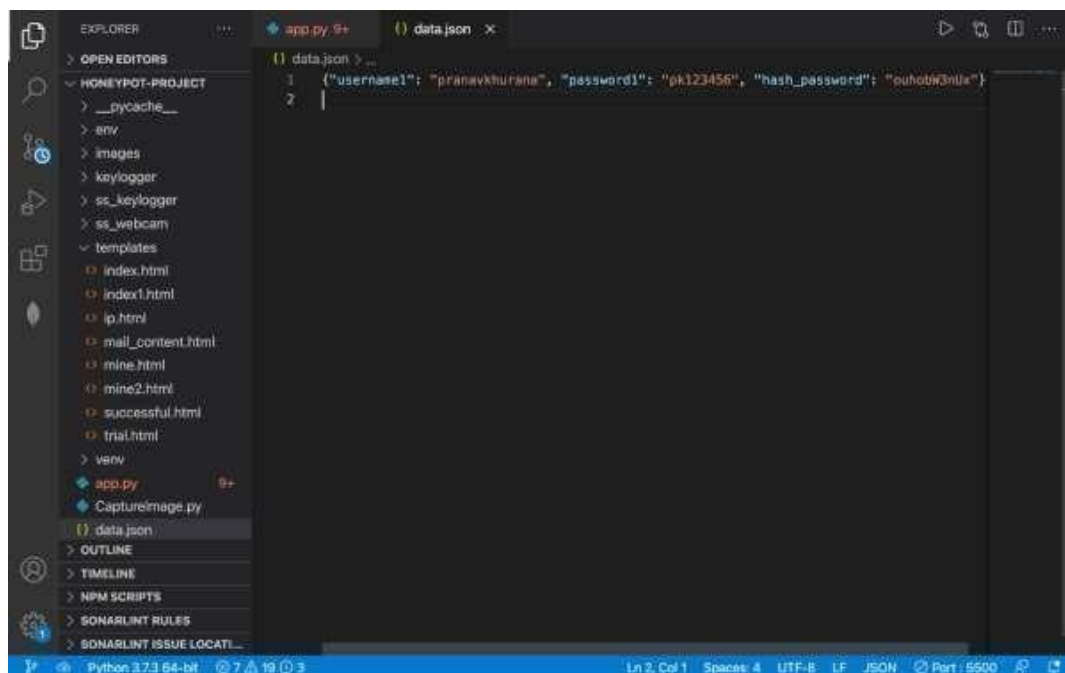
Login details are entered in python script – Hash conversion of password



```
honeypot-project — zsh — 99x26
(env) (base) pranavkhurana@Pranavs-MacBook-Pro honeypot-project % python HashConversion.py
Enter username: pranavkhurana
Enter password: *****
Enter website name that will be redirected after successful login: http://vtop.vit.ac.in
For hash conversion:
Enter 1 if you want special character or else enter 0: 0
Credentials created successfully and stored in 'data.json' file.
Following are the details:
Username: pranavkhurana
Password: pk123456
Hash password: ouhobW3nUx
Website after successful login: http://vtop.vit.ac.in
(env) (base) pranavkhurana@Pranavs-MacBook-Pro honeypot-project %
```

fig-1

The above credentials are updated in the data.json file:



```
EXPLORER
HONEYPOT-PROJECT
  __pycache__
  .env
  images
  keylogger
  ss_keylogger
  ss_webcam
  templates
    index.html
    index1.html
    ip.html
    mail_content.html
    mine.html
    mine2.html
    successful.html
    trial.html
  venv
  app.py
  CaptureImage.py
  data.json

data.json
1 {"username1": "pranavkhurana", "password1": "pk123456", "hash_password": "ouhobW3nUx"}
2
```

fig-2

Login Portal:

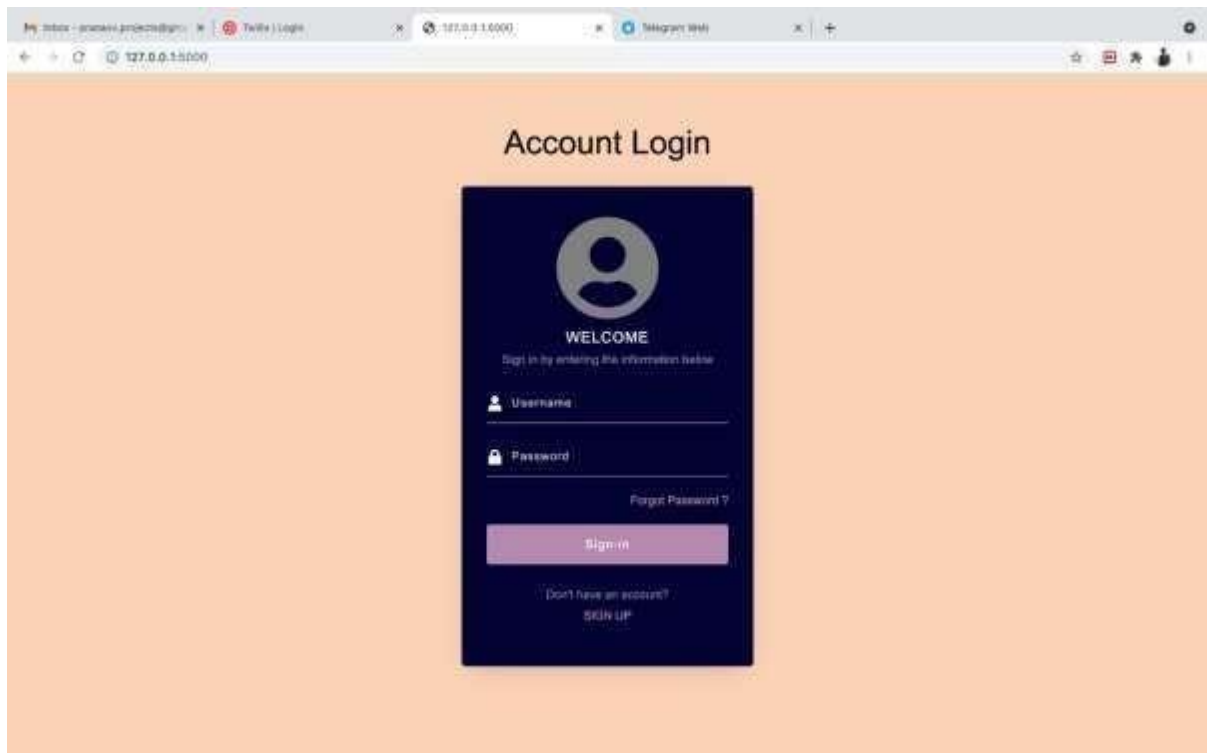


fig-3

Successful Login:

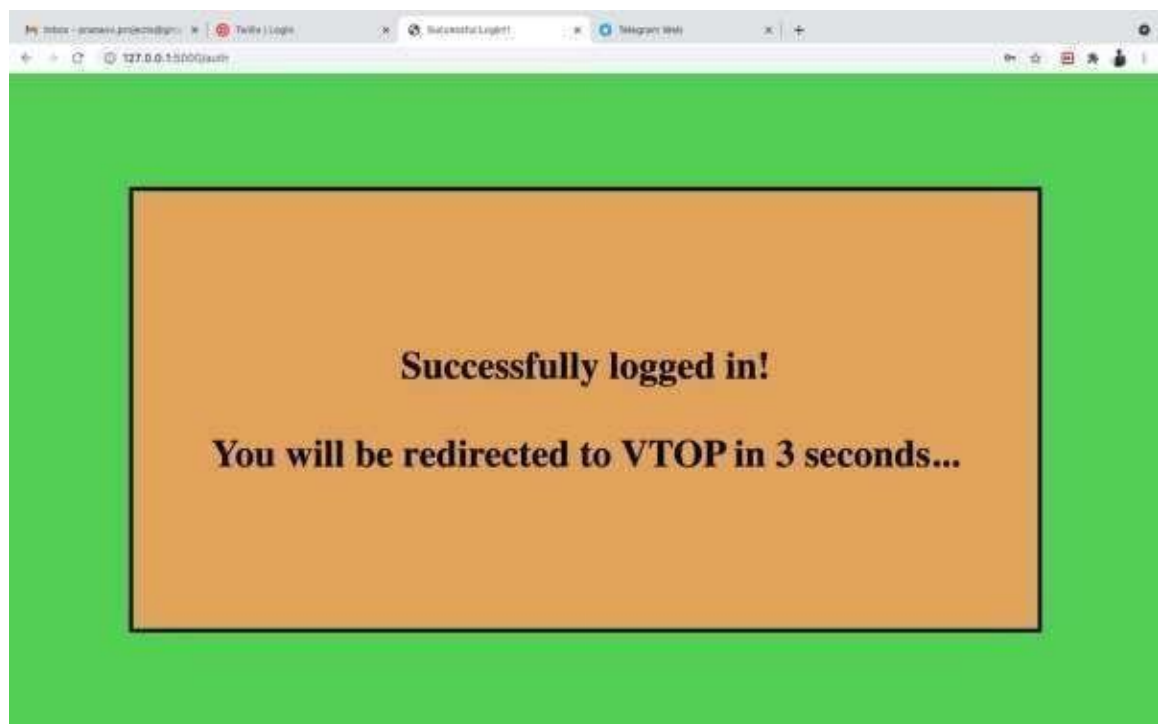


fig-4

Automatically redirects to v-top:

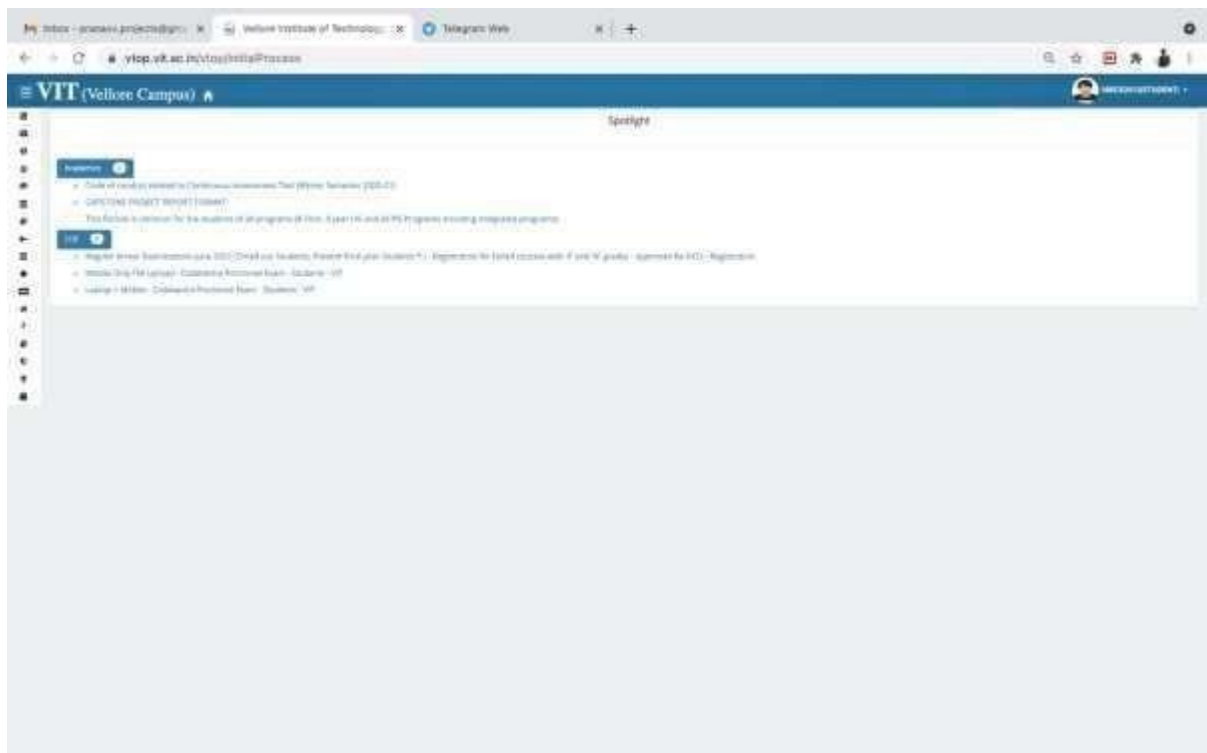


fig-5

Unsuccessful Login: After 3 unsuccessful login attempts, suspicious activity is detected which activates the honeypot in the backend.

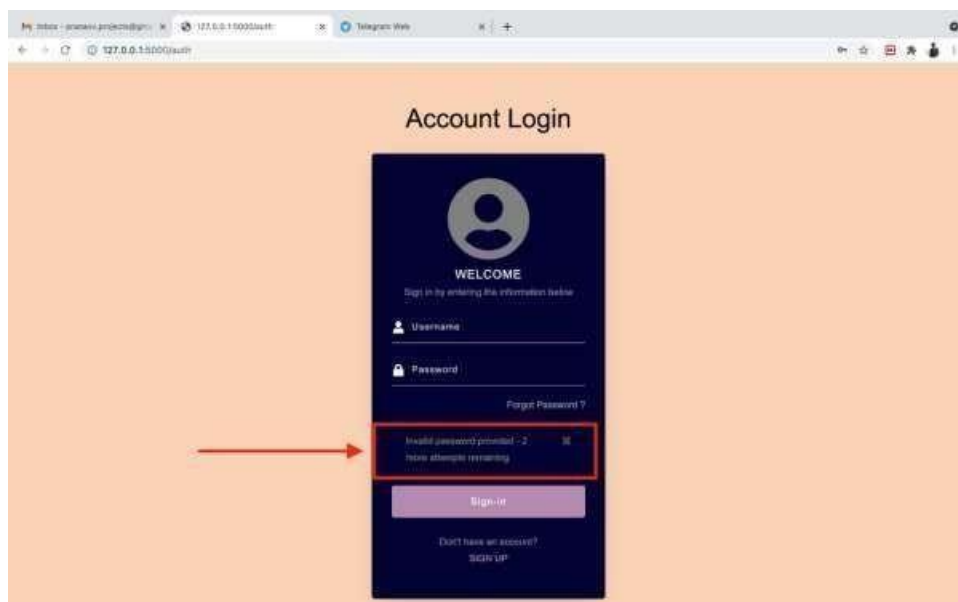


fig-6

Intruder Information is displayed:

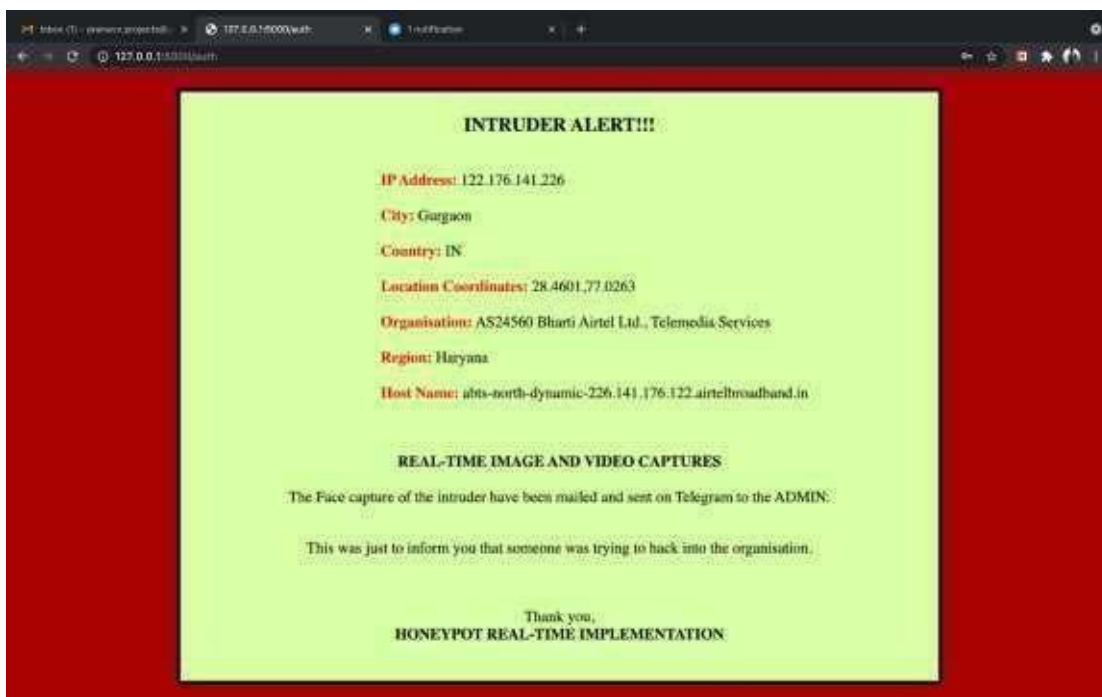
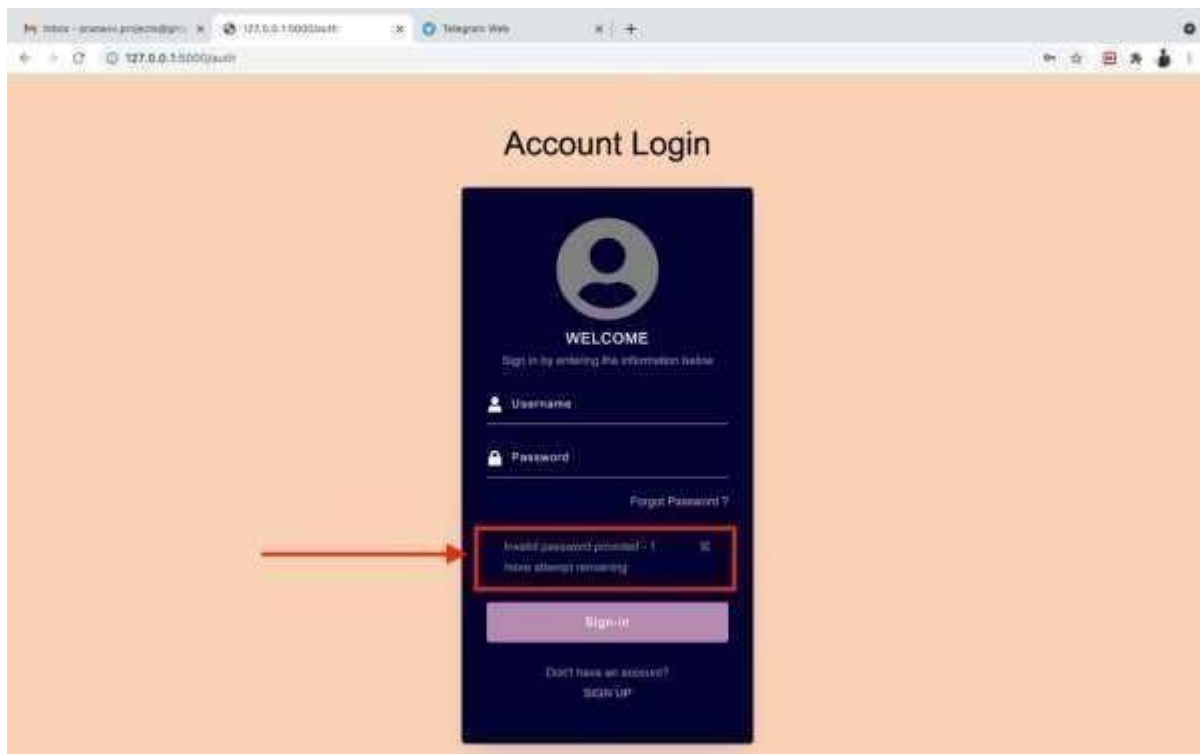


fig-9

Face Capture - Image & Video:

Real-time image and video of the intruder are captured and saved into the system.

Alert on Email

Date and time of the suspicious activity is mentioned in the subject.

IP address and location details of the intruder's system are alerted via mail:

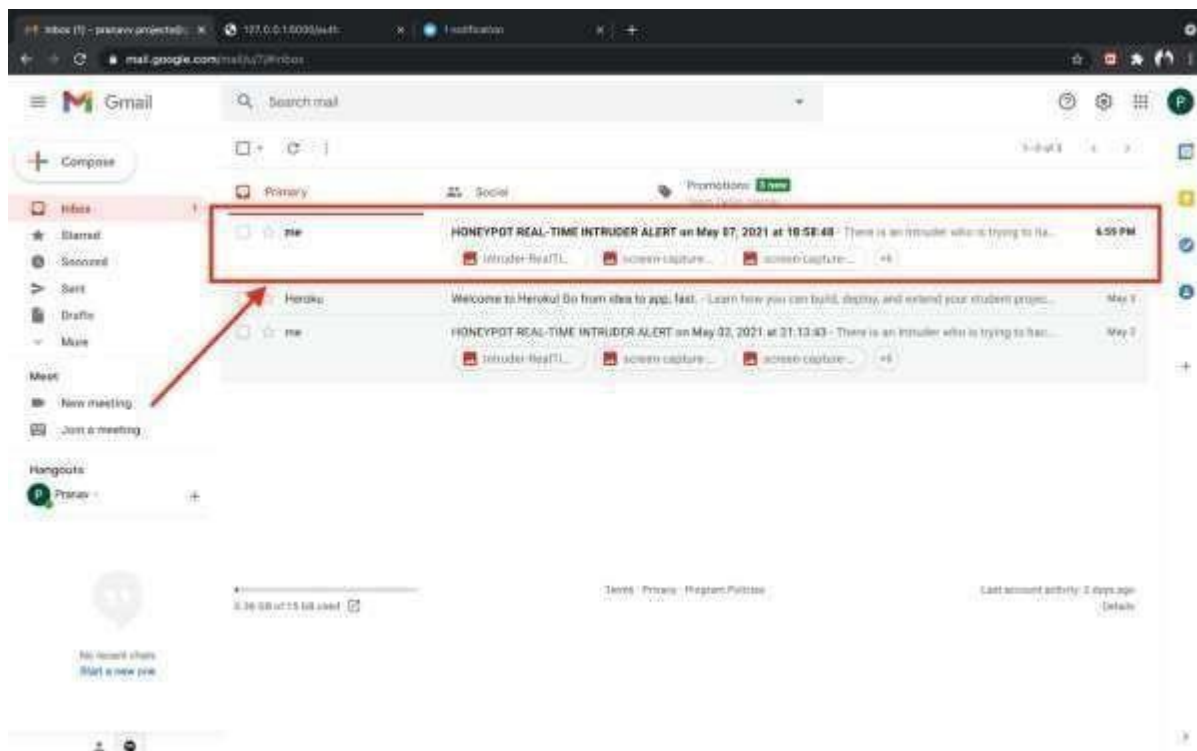


fig-10

Alert on Whatsapp

- Date and time of attack
- IP Address and location coordinates
- Face captures
- Keylogger screen captures

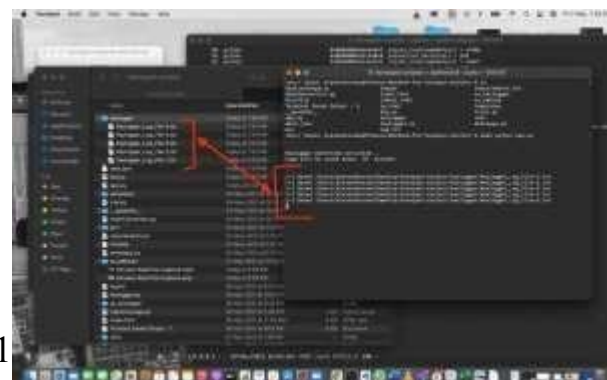


fig-11

Alert on Telegram:

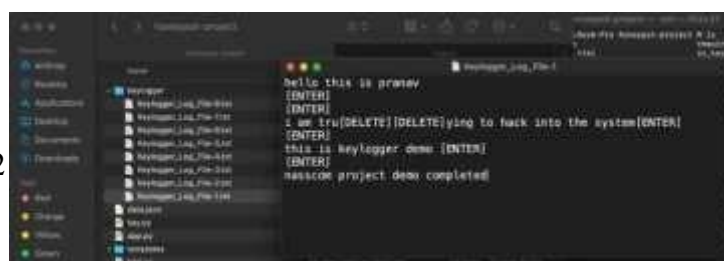
The keylogger system screenshots (real time) of the attacker's system are shared. All the admins of the system, living in geographically different locations, will be alerted at the same time.

Keylogger System Logs

Keylogger script records all the keystrokes pressed by the intruder, and stores them into a log text file. Logs are saved into the system in every interval of 20 seconds

fig-12

Saved in the text file, which can be easily verified by



the admins:

Command terminal records all the activities and prints a corresponding message depending on the activity.



Final Terminal Output:

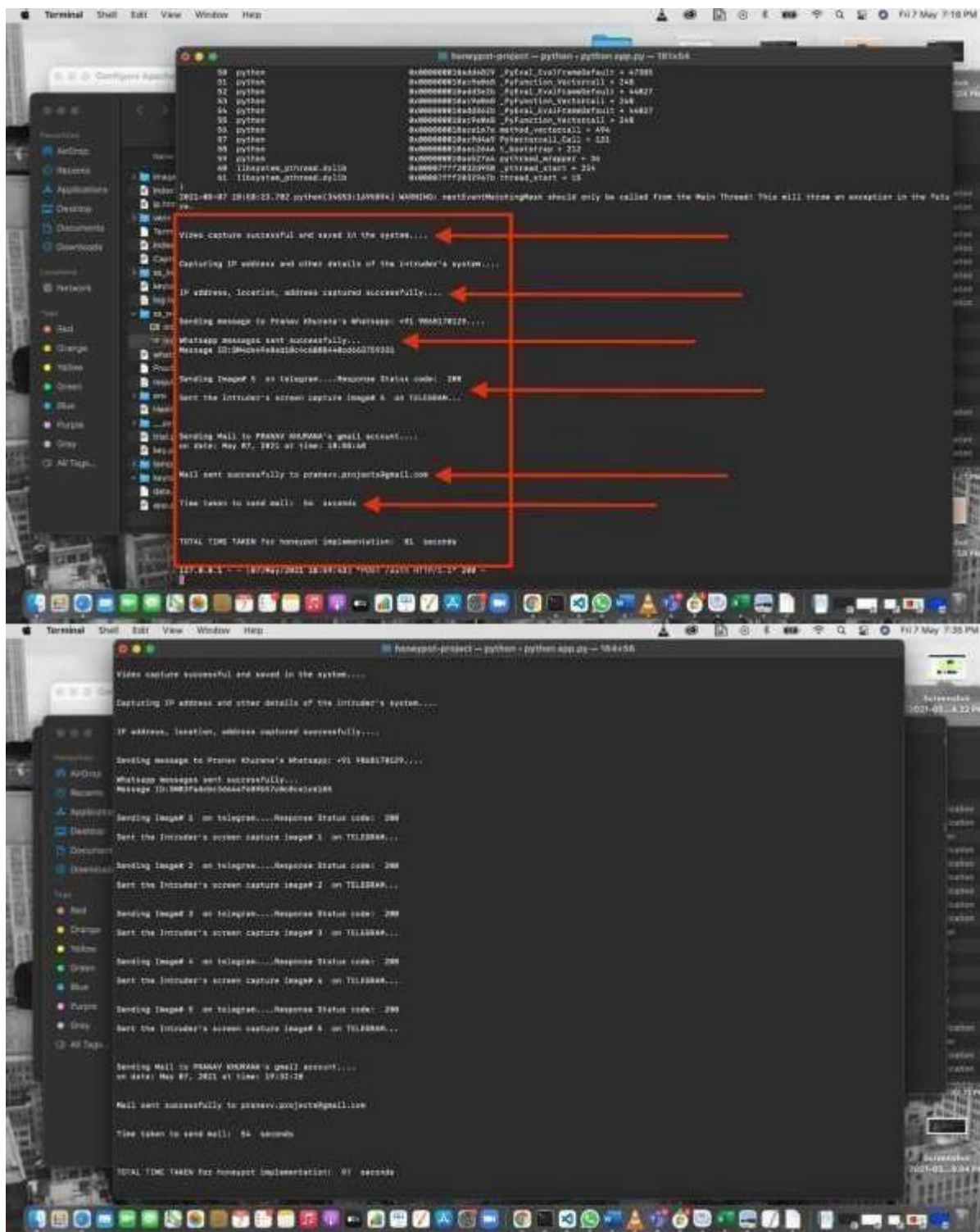


fig-14

6. CONCLUSION

In this project we implemented a very strong system in the point of cyber security. We implemented a **honeypot-based mechanism** in which we didn't just focus on recording the IP address, but we also worked on the **real-time implementation** by recording the **real-time screen shots** of the suspect system, and **face captures** of the suspected attacker. If we find any suspicious activity like not able to login in the portal for more than 3 times then the honeypot system will be activated in the backend which will start taking the screenshots of the intruder's system, **logging the activity** of the intruder (keylogger), and **alert the admins** via 3 important platforms: **WhatsApp, Telegram and Email**.

These images, screenshots and logs can be studied later to know the exact activity of the user. If the consumer is discovered to be a criminal, legal action will be taken against them. The need to strengthen network security has increased in recent years. Honeypots can be used to achieve this level of protection. They are extremely useful as **counter-measures** from intruders attacks on systems. Such that security experts and analysts can identify who they are dealing with and ensure that network security is still maintained despite the rapid changes in network attacks. However, if the attackers are aware of such a device or are able to circumvent it, the whole process is rendered useless. As a result, this fact must be taken into account when designing a honeypot such that the intruder believes it is a genuine device rather than a trap.

7. REFERENCES

1. L. Spitzner, "Honeypots: Tracking Hackers", 2002
2. Wikipedia.
[http://en.wikipedia.org/wiki/Honeypot_\(computing\)](http://en.wikipedia.org/wiki/Honeypot_(computing))
3. Navneet Kambow, Lavleen Kaur Passi, "Honeypots: The Need of Network Security", Vol. 5 (5), 6098-6101, 2014
4. Aaditya Jain, Dr. Bala Buksh, "Advance Trends in Network Security with Honeypot and its Comparative Study with other Techniques", V29(6), 304-312 November 2015
5. Sandeep Chaware, "Banking Security using Honeypot", IJSIA Vol. 5, No.1, 2011
6. The Honeynet Project, <https://www.honeynet.org/about>
7. Aaditya Jain , Bhunesh Sharma , Pawan Gupta, "Honeypot: An External Layer Of Security Against Advance Attacks On Network", IJRSE, Vol. No.2, Issue 04, April 2016
8. Honeypot System,
<https://www.sans.org/security-resources/idfaq/what-is-a-honeypot/1/9>
9. <https://www.sans.edu/cyber-research/security-laboratory/article/honeypots-guide>
10. Muhammet Baykara, Resul Daş, "A Survey on Potential Applications of Honeypot Technology in

Intrusion Detection Systems”,
Volume 2, Issue 5, September –

October 2015

11. Abhilash Verma, Production Honeypots: "An Organization's view", October 2003
12. Honeypot in Network Security: A Survey by Abhishek Mairh, Debabrat Barik, Kanchan Verma, Debasish Jena, March 2016.