# REPORT ON HONEYPOT

MINI PROJECT

Prashanjit Basu
INDIAN INSTITUTE OF ENGINEERING SCIENCE AND TECHNOLOGY, SHIBPUR | 2021CSB010

# HONEYPOT

A honeypot is a security tool that is used to detect and mitigate unauthorised access to a network or computer system. It is essentially a trap set up to attract and identify potential attackers. In terms of network security, a honeypot can be used to gather information about the methods and techniques used by attackers, as well as to identify the source of the attack. This information can then be used to improve the security of the network or computer system. Additionally, honeypots can be used to distract attackers from the actual production systems, thus reducing the risk of a successful attack.

## ABOUT THE HONEYPOT I HAVE PREPARED:

With the help of the socket library in python, which helps to send messages across a network. It provides a form of inter-process communication. The socket library is a low level programmer's interface that allows client to set up a TCP/IP connection and communicate directly to servers. Servers use sockets to listen for incoming connections, and clients use sockets to initiate transactions on the port server is listening.

Mainly using this concept, a detection honeypot can be prepared. Basically, the honeypot here is a python file, which stores values like the IP and a port, the get_socket_con.bind allows us to lay a pseudo layer on that connection/service (presently on a local host inside the firewall) , when accessed by a device or any attacker. The criteria gets completed and the rest of the code runs. Collecting the IP and other useful information like the device of attacker, the time of attack, the source, and some other technical terms get listed in a log text file. While a connection is established by any client to the desired IP an alarm is set to run to alert the user. The honeypot runs in a while loop unless interrupted by the user or as long as the device is active.

## MECHANISM OF THE HONEYPOT:

1) IP and a port are set by the user.
2) Socket to detect client connection and address.
3) Alert the user when a connection is made and note the IP of the incoming connection of client.
4) Display warning message/false data to the attacker.
5) Meanwhile extract the client connection details, and store it in a log file.
6) At last, alert the user with a beep alarm.
7) Repeat the code in the loop.