**MINI PROJECT**

**TOPIC: CYBER SECURITY USING HONEYPOTS**

**2022-23**

**Problem Statement: Designing SSH Honeypot**

**Name: Jai Anand**

**University Roll No: 2016792**

**Semester: 3**

**Section: B**

**Class Roll No: 51**

**ACKNOWLEDGEMENT**

In the successful completion of project “**Cyber security Using Honeypots** “, many people have helped me in one or the other means. I would like to thank all of them who gave their precious time to me.

Primarily, I would thank God for being able to complete this project with success. I would also thank **CSE department GEU and concerned faculty, under whose guidance I learned a lot about this project**. His suggestions and directions have helped in the completion of this project.

I would like to thank my parents and friends who have helped me with their valuable suggestions and guidance, moral support and have been very helpful in various stages of project completion.

Thank You

**Table of Contents**

|  |  |  |
| --- | --- | --- |
| S. No | Particulars | Page No. |
| 1) | **Abstract** | **4** |
| 2) | **Theory** | **5** |
| 3) | **Methodology** | **5** |
| 4) | **Tools Used** | **5** |
| 5) | **Approach** | **6** |
| 6) | **Working** | **6** |
| 7) | **Future Aspects** | **8** |
| 8) | **Conclusions** | **8** |
| 9) | **References** | **9** |

**Abstract**

Now a days cyber crimes are at their peak. As an aware person and programmer we need to figure out certain methods and build such software so that we may be able to protect our systems from black hat hackers. One such method to safeguard our system is the honeypots. Big companies and MNC’s often use honeypots to bait the hackers and to protect their confidential data/trade secrets for their organization. So what actually are honeypots?

**Theory**

Honeypot is a network security mechanism which is capable of detecting deflecting and fooling the attacker. On the basis of their deployment and usage honeypots can be classified under two major categories

1. Production Honeypots
2. Research Honeypots

A production honeypot is a type of honeypot that is used to collect information of a hacker deployed within a business or organizations’ production network. The production honeypot will wait for an attack. If an attack occurs, it will collect data such as originating IP addresses, traffic, etc.

Production honeypots are popular among businesses because they are easy to deploy while collecting essential information about vulnerabilities facing their networks.

A research honeypot is a type of honeypot that is used to collect information about the methods and tactics hacker uses. They consist of baited data/fake data called honey which attracts the hackers. Research honeypots are generally used by government organizations and researchers to evolve and improve cyber security in the systems. They are also used to explore new vulnerabilities of a system and new tactics a hacker me use to exploit a machine. They are hard and complex to deploy and also involve risk of losing your personal data also.

Classification of honeypots on the basis of level of interaction

1. Low level Interaction Honeypots
2. Medium level Interaction Honeypots
3. High level Interaction Honeypots

A low-interaction honeypot is a honeypot that simply captures connection attempts and alerts the security team an intrusion has been attempted. They generally can stimulate only a few recognized ports like TCP UDP SSH etc. They do not contain an operating system to interact with the hacker.

Example: Honey-D

A medium-level interaction honeypot which can give reply to only certain commands/requests of the hacker. They can expect certain activity and are designed to give certain responses beyond what a low-interaction honeypot would give.

Example: Kippo

A high-level interaction honeypot is considered to be the most advanced type of honeypots in general. These types of honeypots contain an operating system and hence are capable of generating and giving responses to the hacker/intruder. They are complex and require configuration for setup. It may or may not generate risk for the operator if real machine is compromised.

**TOOLS USED**

1. Socket
2. Argparse
3. Logging
4. paramiko

Sockets are helpful in sending and receiving messages across the network. It can be imported using the keyword socket and comes built in with the pip installer.

Argparse is a module (package) in python which is capable of sending messages through the command line to the shell. It is quite flexible and supports both conditional and static arguments.

Logging is a package in python which is used for creating logs and logfiles in python.

Paramiko library in python is used for creating the pipeline between the host and client i.e. is capable of creating a SSH connection between the two.

**Approach/Methodology**

The project shows how we can make a basic SSH honeypot and implement it using python. The honeypot runs **on port 2222** instead of **port 22** the basic SSH port for SSH connection. This is done so as if we provide port 22 open a hacker may be even be able to intrude in our main system ignoring the honeypot which is of course harmful for our device.

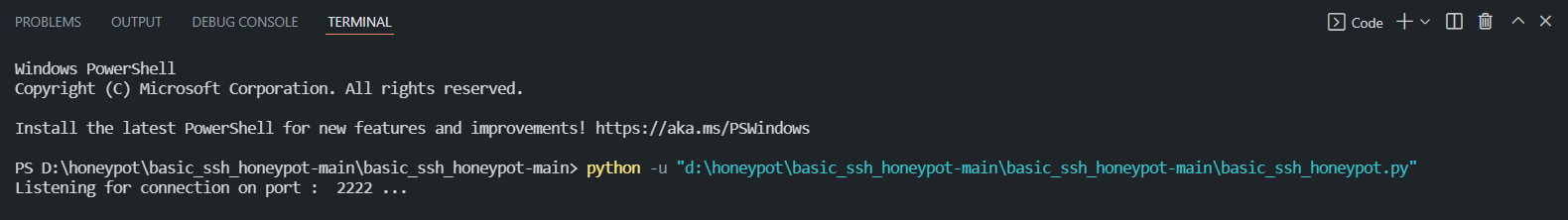
Our fake honeypot can send basic messages to the hacker intruding the shell. It logs all the commands of the hacker and is capable of keeping the hacker busy. The logs are automatically stored in the **ssh\_honeypot.log**.

**My SSH honeypot also keeps log of the hacker’s/intruder’s MAC address and username and password**.

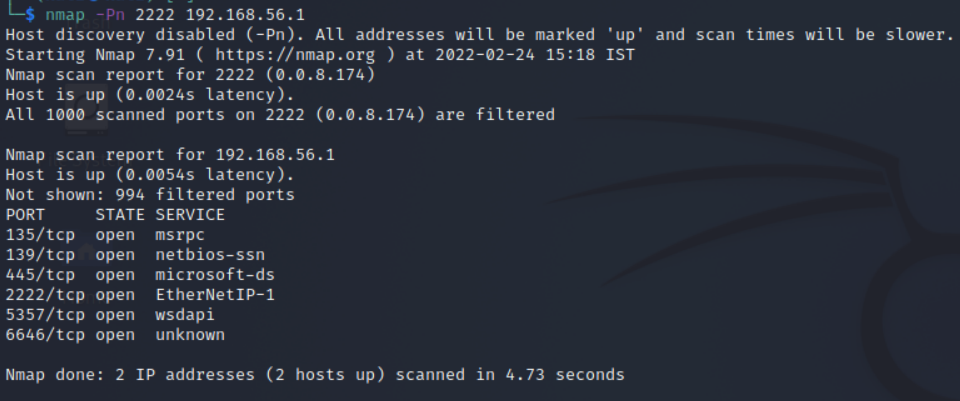
This Honeypot can be used in multi ways as a production and research both, since it can log what all hackers try after intruding the system and as a deflecting machine by consuming time of the hacker.

**Working**

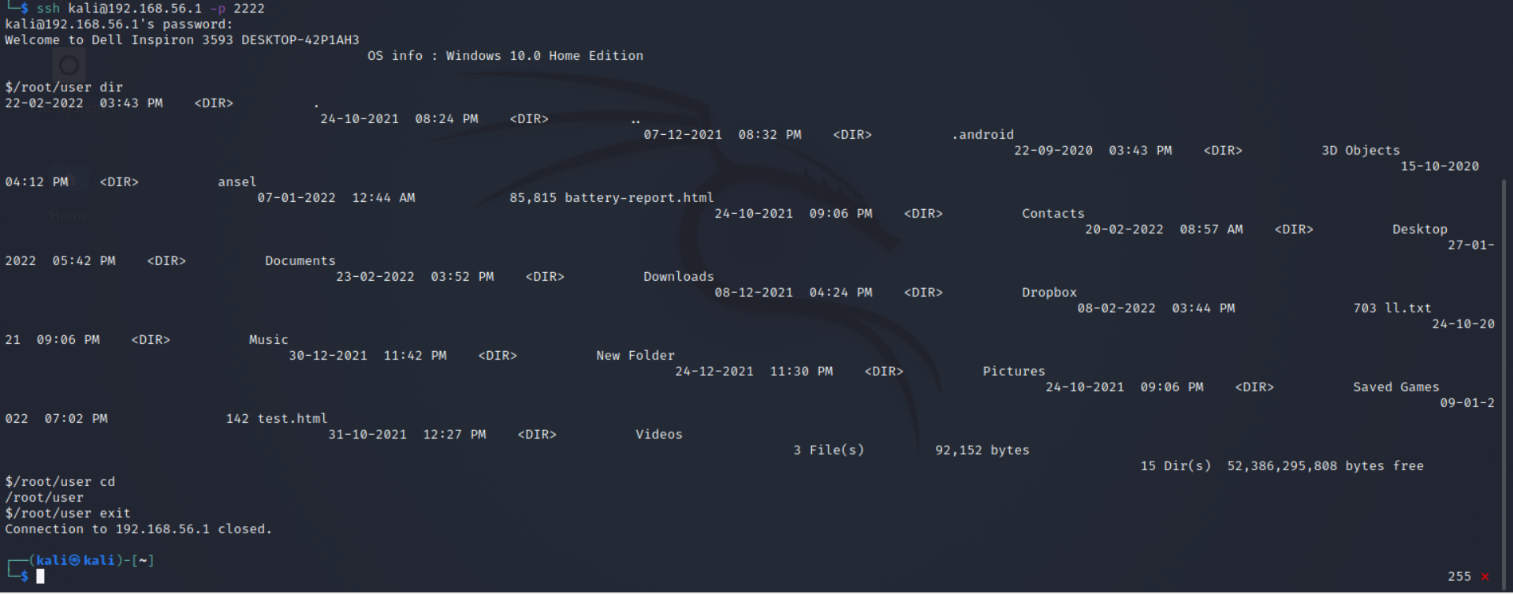
1. Starting the honeypot



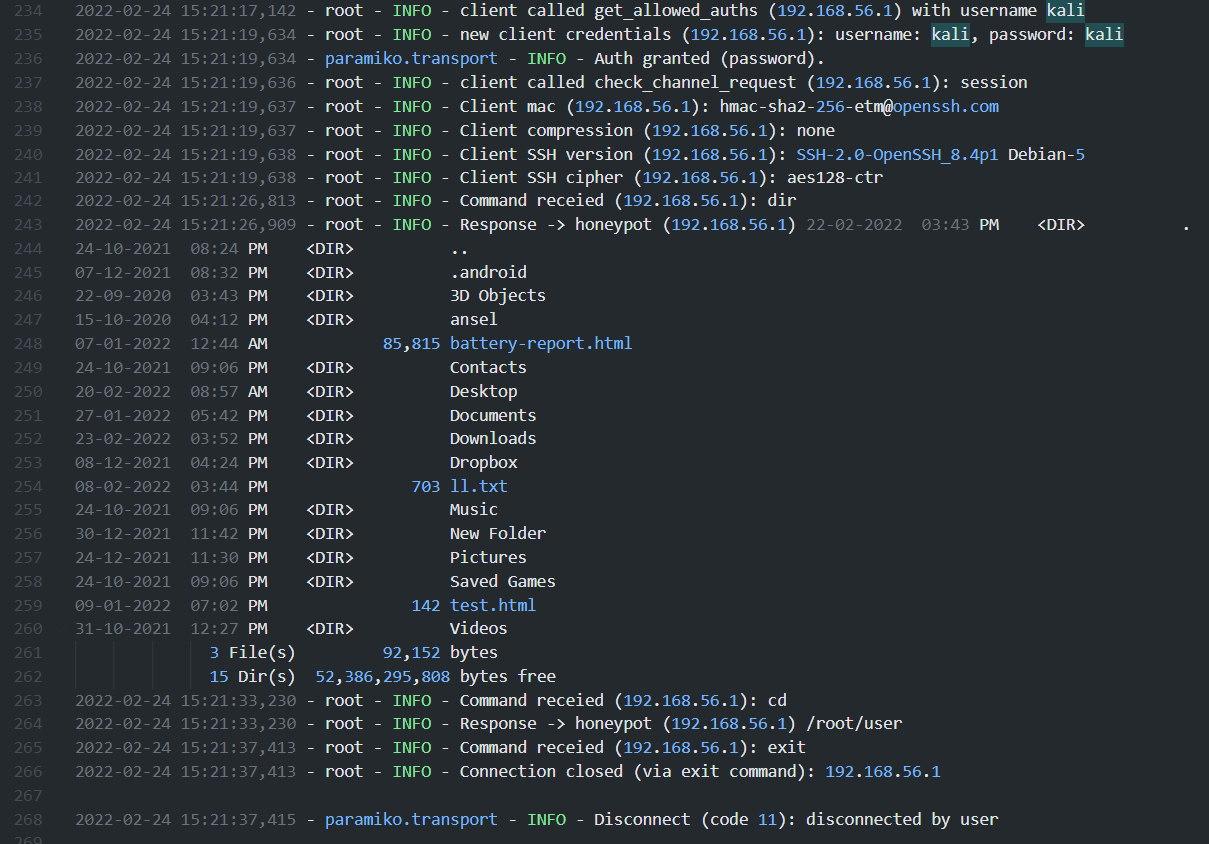
1. Check if the honeypot is working using n-map for it

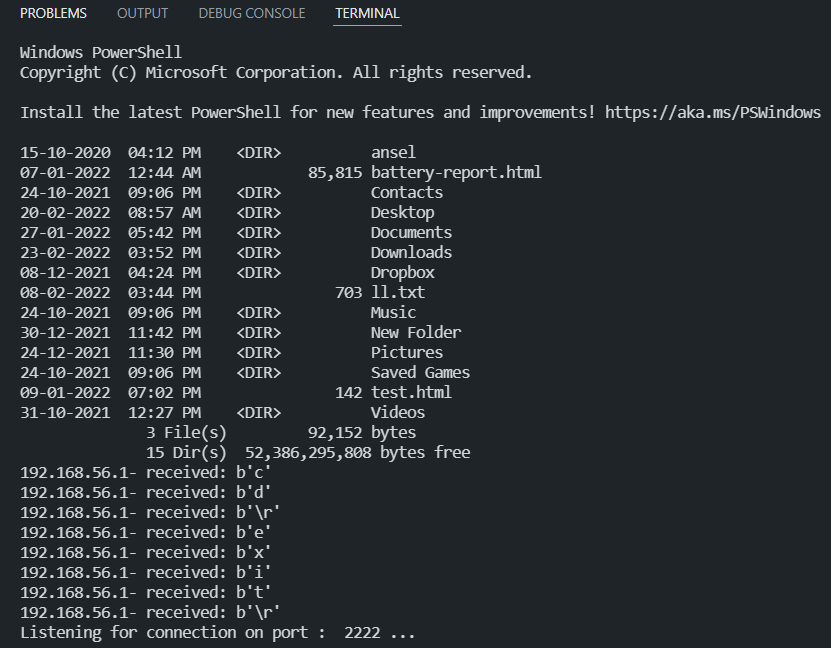


1. Waiting for hacker to intrude



1. Checking if the logs were recorded





**Future developments**

In future I will be able to build some method that my honeypot

1. sends a mail to the host user if someone is intruding the system.
2. Records only the correct username and password of the hacker using some algorithm techniques (AES or md5).
3. The honeypot would be able to interact more feasibly with the hacker.

**Conclusion**

This is the ending of my mini project of the 3rd semester which involved usage of paramiko library for SSH connections using the logging package for logging the details. It is an ideal thing to play around for and to innovate new ideas of cybersecurity techniques.

**References**

1. Paramiko documentation
   1. <https://docs.paramiko.org/en/stable/>
2. Logging documentation
   1. <https://docs.python.org/3/library/logging.html>
3. Argparse documentation
   1. <https://docs.python.org/3/library/argparse.html>
4. Google/ Youtube videos for concept
   1. <https://towardsdatascience.com/analysing-honeypot-data-using-kibana-and-elasticsearch-5e3d61eb2098>
   2. <http://travisaltman.com/honeypot-honeyd-tutorial-part-5-email-alerts/>
   3. <https://cs.lewisu.edu/~klumpra/camssem2015/nmapcheatsheet1.pdf> (n-map cheat-sheet)
   4. <https://www.javatpoint.com/linux-commands> (linux commands)
5. Socket documentation
   1. <https://socket.io/docs/v4/>
6. Stack-overflow for helping me to debug errors