iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** III **Month of publication:** March 2024

DOI: https://doi.org/10.22214/ijraset.2024.59594

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

Bluetrap: A Bluetooth Penetration Testing Tool for Security Assessment

Kallapu Karthikeya[1], Pakeeru Varun Reddy[2], Yamala Rohith[3], Reddyvari Venkateswara Reddy[4], MD. Shinaz Bhanu[5]
[1, 2, 3]*Student, Department of CSE (Cyber Security), CMR College Of Engineering & Technology, Hyderabad, Telangana, India*
[4]*Associate Professor, Department of CSE (Cyber Security), CMR College Of Engineering & Technology, Hyderabad, Telangana, India.*
[5] *Assistant Professor, Department of CSE (Cyber Security), CMR College Of Engineering & Technology, Hyderabad, Telangana, India*

Abstract: ***Bluetooth technology is everywhere, connecting devices for easy communication. But there are security dangers associated with this ease. Bluetrap is a strong framework to help security experts tackle Bluetooth vulnerabilities. This paper explores Bluetrap's many features for thorough testing. It includes easy device discovery, simulated attacks to find weaknesses, extracting important data like messages and contacts, detailed service checks, and smart file transfers. Using Bluetrap, security experts can understand Bluetooth systems deeply, find weaknesses, and boost overall security. The study emphasizes how crucial it is to do ethical testing and obtain consent before utilizing Bluetrap on any kind of gadget. In summary, Bluetrap provides a powerful tool for securing Bluetooth connections, ensuring safer communication in our interconnected world.***

Keywords: Bluetooth Penetration Testing, Bluetooth Security Framework, Bluetooth DoS Attack, Bluetooth Service Enumeration.

I. INTRODUCTION

With its ability to connect wearables, smartphones, and smart home appliances with ease, Bluetooth technology has become a necessary component of our everyday life. There is a chance that there will be security flaws with this convenience, though. Cyberthreats are growing along with the use of Bluetooth, endangering device operation and data privacy. To address these challenges, security professionals need effective tools to assess and strengthen Bluetooth-enabled environments.

Presenting Bluetrap, an all-inclusive framework for Bluetooth penetration testing that offers a multitude of features to enable security experts. Bluetrap delivers more than just basic device detection; by painstakingly compiling device names, MAC addresses, and signal strength, it offers a comprehensive view of surrounding Bluetooth devices and provides deep insights into the Bluetooth world. This initial reconnaissance lays the groundwork for further analysis. Bluetrap goes further by simulating Denial-of-Service (DoS) attacks, enabling security professionals to assess a device's vulnerability to such attacks by transmitting carefully crafted Bluetooth packets. This function is critical for locating flaws and putting mitigation plans into action. Beyond vulnerability assessment, Bluetrap offers valuable data extraction capabilities, potentially retrieving messages, contacts, and call logs from vulnerable devices.

This functionality is invaluable for security assessments and forensic investigations, allowing for the retrieval of crucial information. To gain a deeper understanding of a device's capabilities, Bluetrap meticulously identifies the Bluetooth services it offers. This service enumeration empowers security professionals to pinpoint potential vulnerabilities associated with specific services, enabling more targeted security measures. Bluetrap's functionality extends to file transfer, potentially leveraging the Bluetooth File Transfer Profile (FTP) service. This allows for the transfer of files to targeted devices, facilitating the deployment of testing tools or the delivery of exploit payloads (with proper authorization for ethical testing). Conversely, Bluetrap can retrieve files from devices running a Bluetooth FTP server, proving valuable for extracting data during security assessments.

II. LITERATURE REVIEW

1) *Tahira Ali, Rashid Baloch, Mohsan Azeem, Muhammad Farhan, Sana Naseem, Bushra Mohsin. A Systematic Review of Bluetooth Security Threats, Attacks & Analysis.*

An article which delves into Bluetooth security threats and hacking techniques, including bluebugging, bluejacking, and bluesnarfing. It provides an overview of the Bluetooth protocol stack, focusing on key layers such as L2CAP, RFCOMM, and OBEX. Additionally, it discusses the Java Bluetooth APIs and the significance of JSR-82 support for attack tools.

2) *Malik Zaka Ullah. An Analysis of the Bluetooth Technology.*
This thesis explores Bluetooth's widespread use for wireless data exchange and its susceptibility to security threats, which can lead to data theft, alteration, or device manipulation.

3) *Bluetooth Hacking: A Case Study, Dennis Browning*
This case study concludes that Bluetooth's increasing prevalence necessitates heightened security measures. It highlights the existence of critical security threats within Bluetooth and emphasizes the potential consequences for data and communication security. This underscores the need for further research and development of tools to address these evolving vulnerabilities.

III. OBJECTIVE

The primary objective of this project is to introduce Bluetrap, a comprehensive Bluetooth penetration testing framework designed to empower security professionals. Bluetrap transcends basic discovery tools by offering a multifaceted arsenal for meticulous Bluetooth security assessments.
Fundamentally, the goal of Bluetrap is to provide security experts the capacity to quickly scan and map the surrounding Bluetooth environment, obtaining vital data such as device names, MAC addresses, and signal strength. This detailed mapping serves as the foundation for targeted vulnerability assessments, allowing teams to prioritize potential risks.
Furthermore, Bluetrap empowers security professionals to evaluate a device's susceptibility to Denial-of-Service (DoS) attacks via controlled simulations. Security experts can learn a great deal about any flaws in a device by watching how it reacts and taking proactive steps to minimize them.
Beyond vulnerability assessment, Bluetrap facilitates the extraction of critical data like messages, contacts, and call logs from susceptible devices. This is helpful for forensic investigations and security assessments, which eventually results in a more thorough awareness of the security environment.
Additionally, Bluetrap grants a comprehensive understanding of a device's Bluetooth capabilities by identifying offered services. This allows security teams to pinpoint potential vulnerabilities and implement focused security measures.
Finally, Bluetrap facilitates strategic file transfers over Bluetooth for deploying testing tools or retrieving data during assessments. It is important to emphasize that Bluetrap is intended for authorized testing only. By equipping security professionals with these functionalities, By encouraging a proactive approach to Bluetooth security, Bluetrap helps users find and fix vulnerabilities before bad actors can take advantage of them.

IV. SYSTEM REQUIREMENTS

1) *Hardware:* A virtual machine (VM) or dedicated Linux server with enough RAM, CPU, and storage to carry out the assaults.
2) *Operating System:* The CLI tool must be compatible with the desired operating system. Common options include Linux-based distributions such as Ubuntu Server.
3) *Bluetooth Adapter:* For easy data transfer between devices, a dependable and stable Bluetooth connection is essential. Factors like signal strength and interference affect its effectiveness.
4) *BlueZ:* BlueZ is a collection of libraries and tools for Bluetooth support on Linux.

V. PROBLEM DEFINITION

Bluetooth penetration testing is important for uncovering and remedying security flaws in Bluetooth devices and networks, especially as Bluetooth technology gains traction across industries. However, pen testers encounter challenges in comprehending Bluetooth vulnerabilities and the tools needed for thorough assessments. To improve Bluetooth pen testing, defining precise research goals is essential, focusing on crafting methodologies, tools, and best practices to identify and mitigate Bluetooth security risks effectively.

VI. EXISTING SOLUTIONS

1) *BTScanner:* BTScanner is a Bluetooth scanning tool designed for discovering and gathering information about Bluetooth devices in each area. BTScanner is typically a command-line tool used in Linux environments. Its primary purpose is to identify nearby Bluetooth devices and provide details about them, such as device name, Bluetooth address (MAC address), device class.

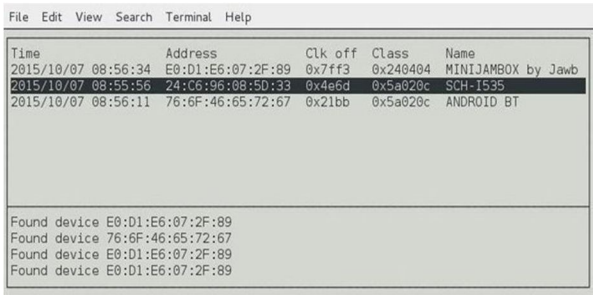


Fig-1: BTScanner

2) *BTCrawler:* Pen testing and ethical hacking are just two uses for the multipurpose Bluetooth device scanner known as BTCrawler. It provides a comprehensive overview of nearby Bluetooth devices, including their names, MAC addresses, device classes, vendors, signal strengths, and supported services.

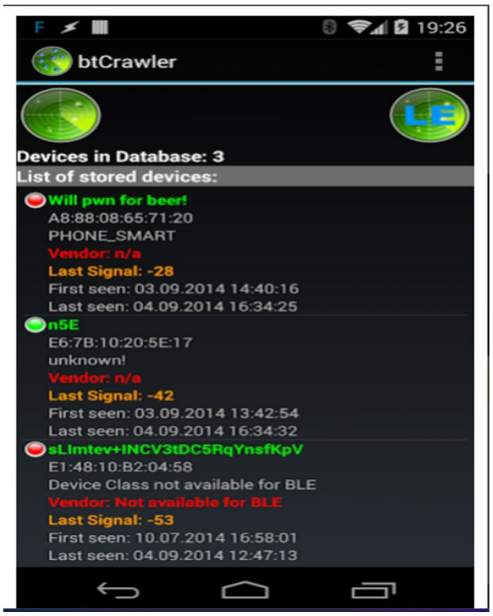


Fig-2: BTCrawler

3) *BTSnifer:* A hardware instrument called the Bluefruit LE Sniffer (v1.0) was created especially for recording and examining Bluetooth Low Energy. It is essentially a pre-programmed Bluefruit LE Friend board that acts as a dedicated BT sniffer, offering a more user-friendly experience compared to software-based options.

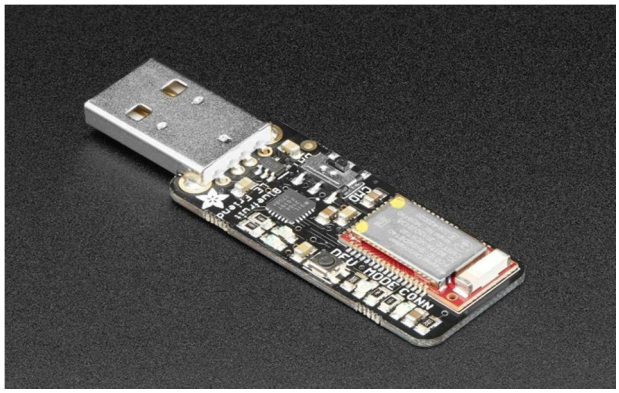


Fig-3: BTSnifer

VII. LIMITATIONS OF THE EXISTING SYSTEM

1) *Limited Scope of Existing Tools:* They may not provide features like data extraction, service enumeration, or advanced vulnerability evaluation. They might not offer functionalities like advanced vulnerability assessment, data extraction, or service enumeration.
2) *Evolving Technology:* The ever-changing nature of Bluetooth technology necessitates continuous updates to security measures. New features and protocols might introduce unforeseen vulnerabilities.
3) *Compatibility Issues:* Compatibility variations between different Bluetooth devices and software can hinder the effectiveness of some security tools.
4) *Ethical Considerations:* The potential for misuse of Bluetooth hacking tools necessitates emphasis on responsible testing practices and obtaining proper authorization before using such tools on any unauthorized device.

VIII. WORK FLOW

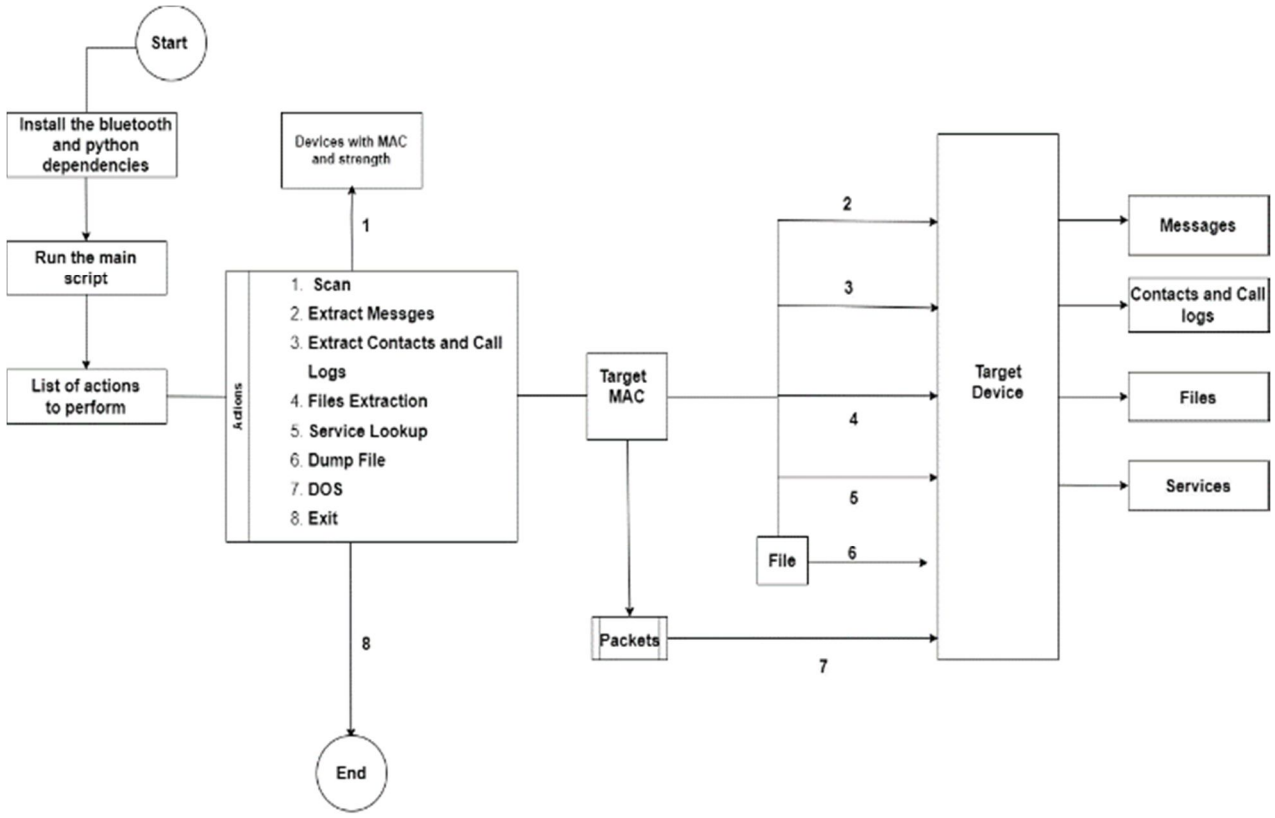


Fig-4: Work Flow

1) *Start:* This is the starting point of the workflow. Select a Linux machine.
2) *Installation of Dependencies:* In this step, we install all the dependencies, such as BlueZ and all the Python dependencies.
3) *Run the Main Script:* In this step, run the main script and get the list of actions that can be performed.
4) *Scan:* The scan gives the nearby devices their corresponding MAC addresses and strengths.
5) *Messages Extraction:* Messages in the inbox, outbox, and drafts are extracted to our device.
6) *Contacts and Call Logs Extraction:* Contacts, incoming, and outgoing calls are extracted to our device.
7) *Extraction of Files:* Extracting all files from devices that run FTP servers in one go.
8) *Service Lookup:* Different devices have different services running on different ports; with this, we can find services on that device.
9) *Dump File:* This option allows you to send a file from our device to the target device.
10) *DOS Attack:* Sending a lot of packets at a time, which makes the target device go down.

IX. ARCHITECTURE

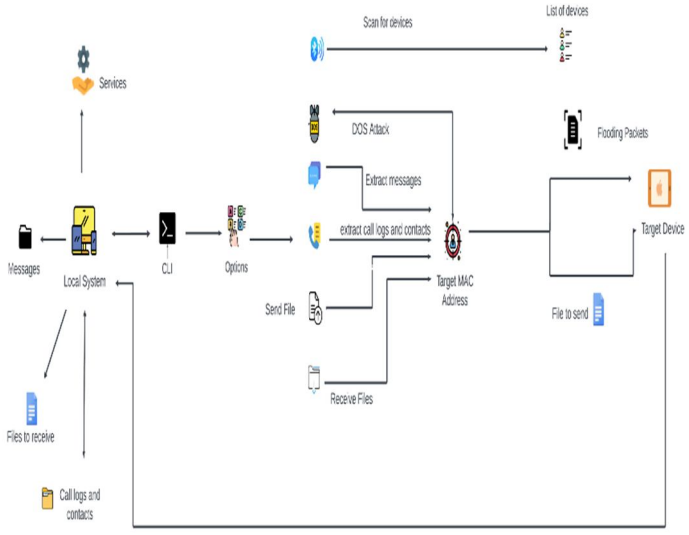


Fig-5: Architecture

1) The user will install all the dependencies and run the main script, which populates the list of actions that can be performed.
2) The scan option will use the Bluetooth library of Python to find nearby devices.
3) Messages, contacts, call logs, and files are extracted using OBEX (Object Exchange) protocol.
4) Services of a device are given by using the Bluetooth library when given with the MAC address of the device.
5) A DOS attack is performed by sending a lot of packets simultaneously to the target device, which makes it unavailable.

X. CONCLUSION

Our investigation into Bluetooth hacking explored attack techniques and security flaws, emphasizing the significance of moral evaluations. While acknowledging the challenges presented by evolving technology and compatibility issues, the project explored various weaknesses and assessment tools. In the end, this study seeks to strengthen Bluetooth security by identifying and resolving technological problems, promoting a more secure atmosphere for all users.

XI. RESULTS

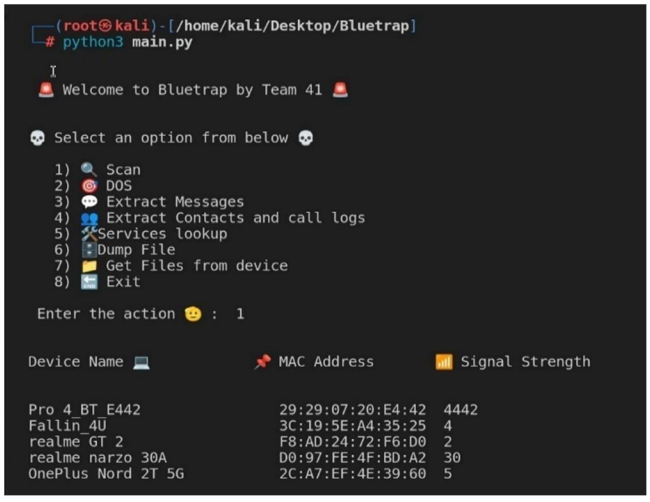


Fig-6: Bluetooth Scanning

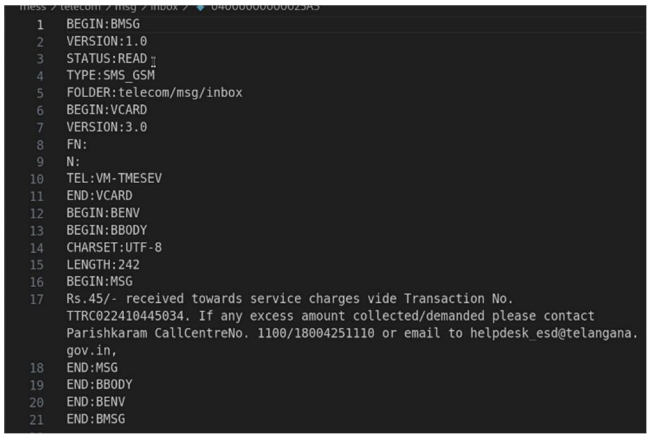


Fig-7: Message Extraction

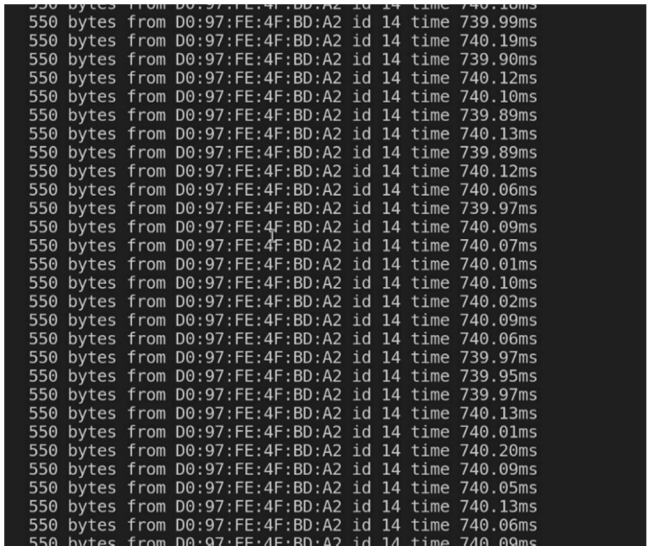


Fig-8: DOS Attack

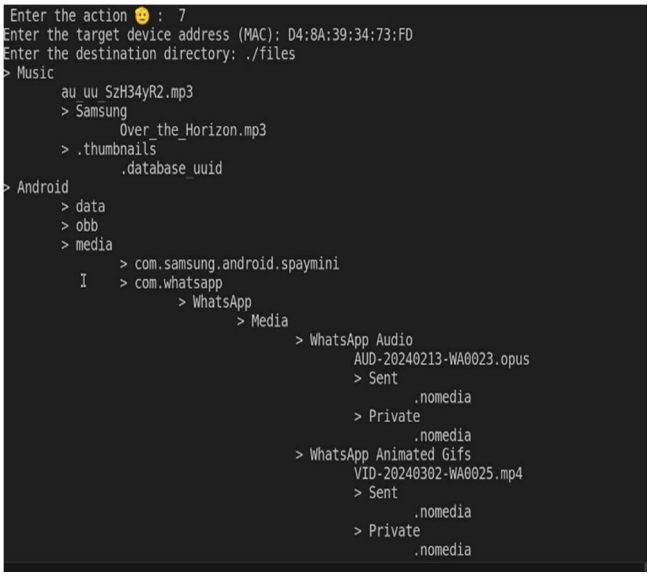


Fig-9: File Extraction

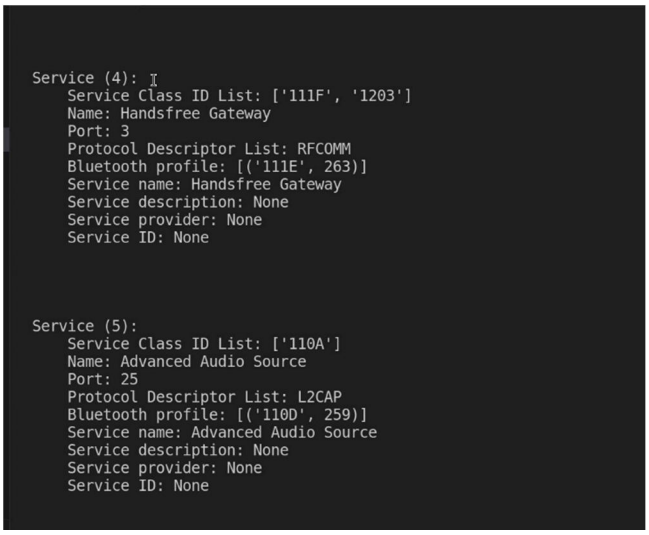
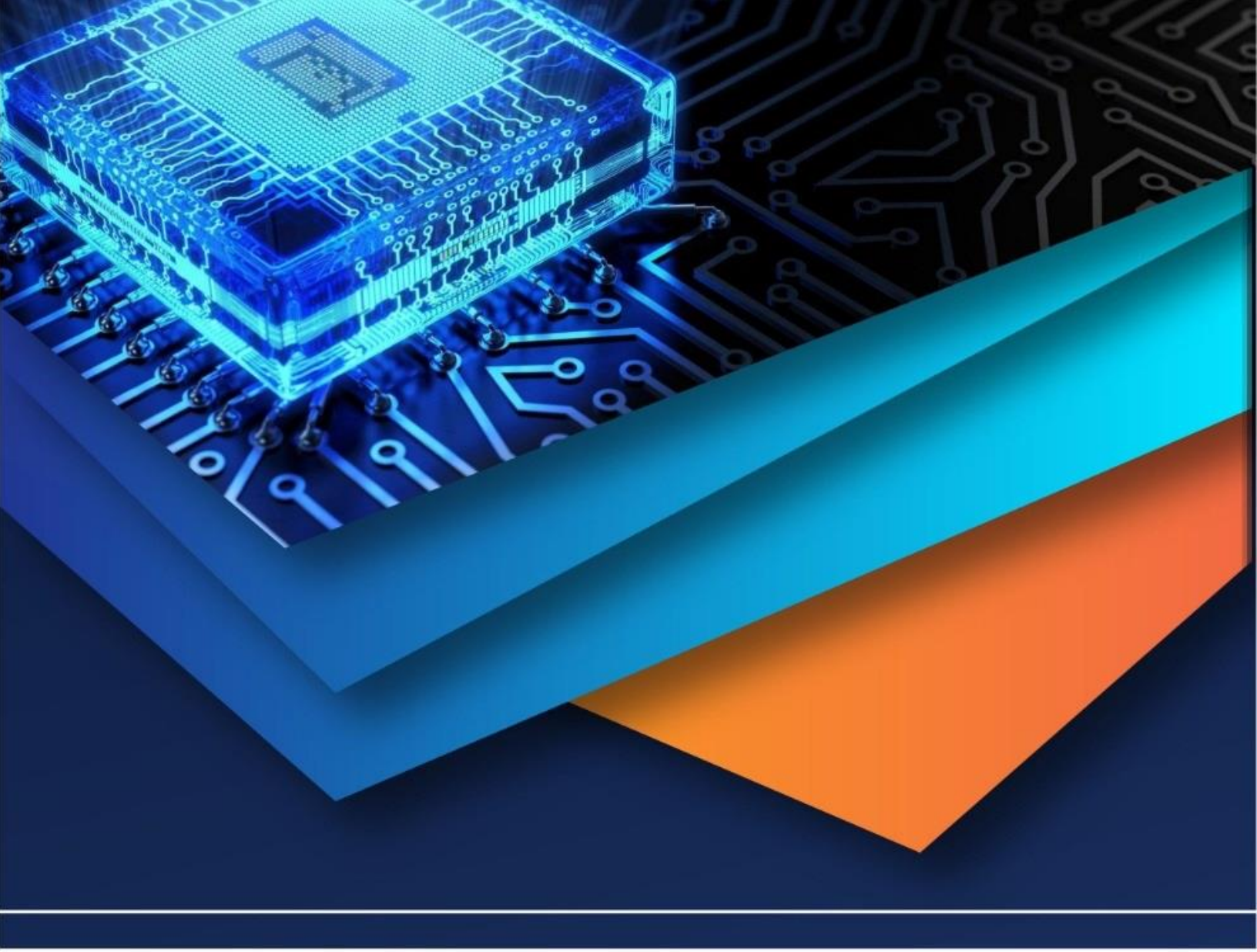


Fig-10: Service Lookup

REFERENCES

[1] Dennis Browning. Bluetooth Hacking: A Case Study.
[2] Nishit Kumar Patel, Hayden Wimmer, Carl M. Rebman. Investigating Bluetooth Vulnerabilities to Defend from Attacks.
[3] Robayet Nasim. Security Threats Analysis in Bluetooth Enabled Devices.
[4] Trapti Pandey, Pratha Khare. L & T Technology Services, Bluetooth Hacking, and its Prevention.
[5] Nateq Be-Nazir Ibn Minar, Mohammed Tarique. Bluetooth Security Threats and Solutions.
[6] Malik Zaka Ullah. An Analysis of the Bluetooth Technology.
[7] Bluetooth Hacking. Ethical Hacking and Countermeasures Version 6 Module XXXVII- ICEC.
[8] Andreas Becker. Bluetooth Security & Hacks.
[9] Adam Laurie, Marcel Holtmann, Martin Herfurt. Hacking Bluetooth enabled mobile phones and beyond.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY