ISSN No:-2456-2165

Cracking Wi-Fi using Python

Bhuvana Chandra Shetty, Thanushree T., Divya Lokannavar
Computer Science of Engineering
AMC Engineering College Bengaluru, India

Dr. Nirmala S.
Professor, AIML
AMC Engineering College Bengaluru, India

Abstract:- Ethical hacking of Wi-Fi passwords is a process of intentionally testing the security of a Wi-Fi network with the owner's permission. The main objective of ethical hacking is to identify and address any security vulnerabilities before malicious actors can exploit them. In an ethical hacking engagement, a certified and experienced security professional conducts various tests to determine the level of security of the Wi-Fi network. The tests may include network scanning, passwords cracking, social engineering, and other methods to identify weaknesses in the network's security. Once the security vulnerabilities are identified, the security professional works with the network owner to address the issues and improve the security of the network. This may involve changing default passwords, updating firmware, and implementing stronger encryption protocols. The benefits of ethical hacking of Wi-Fipasswords include enhancing the security of the network, preventing unauthorized access, and protecting the privacy of the network owner and its users. It is important to note that any hacking activity without the owner's consent is illegal and can lead to serious legal consequences.

Keywords:- *Wireless network, Wi-Fipasswords, Wi-Fi hacking, phishing using Python script, Wireless security protocols.*

I. INTRODUCTION

Ethical hacking of Wi-Fi passwords is a process of testing the security of a Wi-Fi network with the owner's permission. The objective is to identify potential vulnerabilities in the network's security and address them before malicious actors can exploit them[1]. The increasing reliance on wireless networks for personal and business use has made Wi-Fi security a critical concern. Hackers and cybercriminals can use a variety of methods to gain unauthorized access to Wi-Fi networks, steal sensitive information, and compromise the security of the network's users. Ethical hacking of Wi-Fipasswords involves simulating the techniques used by malicious actors to identify any security weaknesses in the network. By doing so, it allows network owners to take proactive measures to secure their networks and prevent unauthorized access[2][3]. In an ethical hacking engagement, a certified security professional uses various tools and techniques to test the network's security. The results of the tests are then used to identify potential vulnerabilities and develop a plan to address them in this paper we are using the brute force algorithm method to crack the Wi-Fi passwords.

A. Hacking of Wi-Fi

The challenge with public Wi-Fi is that it come with a multiplicity of security dangers. While big businesses may believe they are providing a useful service to their consumers, the security on these networks is likely to be weak or non-existent. Since the initial days of something like the 802.11b architecture in the late 1990s, mobile hotspots have proven infamously unsafe. Major 802.11 faults, including as fundamental security flaws, decryption flaws, and authenticity issues, have been uncovered since the standard's debut[5][9]. Since then, wireless operations have always been on the rise. The situation is getting enough that severe that the Wi-Fi Affiliation has established two intrusion prevention standards and guidelines to fightback against the aggressors. The Wi-Fi Secured Access (WPA) standard, which was established by the Wi-Fi Affiliation, represented as a temporary fix to a well WEP attack vectors it until IEEE released the 802.11i standard. This is now the approved Standard specification that includes the WPA patches for WEP, as well as various cryptographic procedures to make wireless networks even more secure.

- Most common attacks
- Jamming signals
- Unencrypted networks
- Malware distribution
- Mis configuration Attacks
- Sniffing and snooping
- Malicious hotspots[4]

➢ *Aircrack-ng:*

Aircrack is an all in one packet sniffer, WEP and WPA/WPA2 cracker, analyzing tool and a hash capturing tool. It is a tool used for Wi-Fi hacking. It helps in capturing the package and reading the hashes out of them and even cracking those hashes by various attacks like dictionary attacks. It supports almost all the latest wireless interfaces.

Reaver is a package that is a handy and effective tool to implement a the brute force attack against Wi-Fi Protected Setup (WPS) registrar PINs to recover WPA/WPA2 passphrases. It is depicted to be a robust and practical attack against WPS, and it has been tested against a wide variety of access points and WPS implementations. In today's time hacking WPA/WPA2 is exceptionally a tedious job.A dictionary attack could take days, and still will not succeed. On average Reaver will take 4-10 hours to recover the target AP's plain text WPA/WPA2 passphrase, depending on the AP. Generally, it takesaround half of this time to guess the correct WPS pin and recover the passphrase.

ISSN No:-2456-2165

➢ *Pixie WPS:*

PixieWPS is a tool used to perform the the brute force attack on WPS pins to crack them. It is a tool written in C language and has a lot of features like checksum optimization, Reduced entropy of the seed, Small Diffie-Hellman keys, etc.

➢ *Wi-Fite:*

When it comes to Wi-Fi Hacking Wi-Fite is one of the most useful tools when you have a lot of wireless devices across your location. It is used to crack WEP or WPA/WPS encrypted wireless networks in a row. It could easily be customized to automate the process of multiple Wi-Fi hacking. It comes packed with many features, few of them are listed below.

B. Hacking using phishing with Python script:

Phishing is a tactic that entails impersonating a trustworthy company or service in order to fool a user into revealing sensitive information or login credentials. Phishing may be utilised over Wi-Fi networks, despite the fact that it is typically connected with email or websites. It's crucial to tackle this subject carefully and ethically, though.Before carrying out any tests or gathering any data, it is crucial to adhere to ethical standards and get the required permits and approvals from the appropriate parties if you want to do research on the use of phishing on Wi-Fi networks. This might entail requesting permission from the network's owner or receiving ethical clearance from the appropriate institutional review board (IRB).[7][9]

It is crucial to take into account any dangers and outcomes before undertaking research on the use of phishing on Wi-Fi networks. Cybersecurity may be seriously threatened by phishing, thus any study on the subject needs to be done carefully and cautiously. It is crucial to make sure that any testing is carried out with the owner of the network's express written approval and correct authority, and that all necessary precautions are followed to prevent any harm or damage from being done to the target or their network.

II. SYSTEM ARCHITECTURE

A secure Wi-Fi network typically includes a Wi-Fi router, wireless access points (WAPs), clients, and network security measures such as encryption protocols, access control mechanisms, firewalls, and intrusion detection systems. Some potential vulnerabilities that an ethical hacker may look for include weak passwords, unsecured access points, outdated software, man-in-the-middle attacks, and rogue access points. It is important to remember that ethical hacking should only be conducted with the permission and consent of the network owner, and in a responsible and ethical manner.

- **Reconnaissance:** Gathering information about the target network, such as the type of Wi-Fi router being used and the security measures in place.
- **Scanning:** Using tools to scan the network for open ports, services, and vulnerabilities that can be exploited.
- **Enumeration:** Gathering more detailed information about the target systems and services that were identified during scanning.
- **Exploitation:** Attempting to exploit the identified vulnerabilities to gain unauthorized access to the network.
- **Post-Exploitation:** Once access has been gained, the ethical hacker may attempt to maintain access and escalate their privileges, in order to identify additional vulnerabilities or gather more sensitive information.
- **Reporting:** Finally, the ethical hacker should report their findings to the owner of the network, along with recommendations for improving security and addressing the vulnerabilities that were identified.

The most crucial phase of building any model is system design. shows our project's fundamental system architecture.

This project looked at WPA cracking, and it was discovered that WPA-PSK cracking is the sole method that can be used to compromise this security standard. According to the standard for PSK after authentication occurs key derivation. Key derivation consist softwo handshakes. The first is 4-Way Handshake for PTK (Pairwise Transient Key) and GTK (Group Transient Key) derivation. And the second one is Group Key Handshake for GTK renewal[7]. The cracking concept is based on imperfection in 4-Way Hanshake, where the PTK andGTK keys are derivated from PMK (Pairwise Master Key). In the WPA-PSK system PMK is derived from PSK. The way to derived KCK (Key Confirmation Key) fromPSK is visible in this figure. Subsequently is calculated PMK from PSK, then the PTK is derived and first 128 bits of PTK represents the Key Confirmation key [8]. KCK is so important for WPA-PSK passwords cracking, because it is used for computing MIC. Below fig. 1 represents the architecture of the system.

ISSN No:-2456-2165

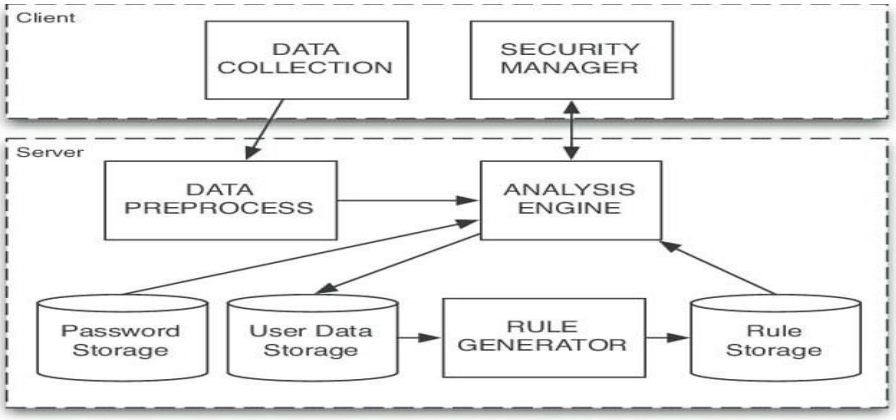

Fig. 1: Basic system architecture

III. EXISTING SYSTEM

The Wi-Fi encrypted protocols as everyone is aware of very much can be easily cracked, damaged, used and destroyed using several ways is also considered as a drastic and wide category flaw . The most popular and famous procedures or steps that almost every technically sound person knows in cracking the passwords and exploiting the user's network by not letting him know is using "aircrackng" To crack using this method quickly without much major thought or effort, the user has to have a laptop a desktop or a machine with Kali Linux. Along with it a remote card which supports monitor/injection mode. Aside from these apparatuses, the client additionally needs to get an outside remote card which can monitor/injection mode. The form of packets in the air is transmitted by Wi-Fi. By using 'airodump' the captured packets are dumped in the air. The users that are connected to victim's Wi-Fi are selected since cracking isn't possible for this a valid WPA handshake is needed The attacker captures handshake by sending de-authentication packets to the host which is connected to Wi-Fi [5][6]. This method tests Wi-Fipasswords through a wordlist basically performing a dictionary attack. Also, the time taken is very long. So to overcome this limitation the proposed project comes with much more reliable and standard cracking methods.Without adequate authorisation, passwords extraction from WLAN networks is seen as unethical and maybe illegal. With the right permission and the express legal approval of the network owner, there are ethical ways to evaluate the security of WLAN networks. Perpetration testing, sometimes known as a "pen test," is a popular technique for evaluating the security of a WLAN network. Pen testing simulates a cyberattack against a network to find possible security gaps and vulnerabilities. The objective is to identify potential attack vectors and offer suggestions for mitigating them. The owner's consent is required for penetration testing, and it's crucial to make sure the test doesn't harm the network or data.

- **Retreiving the saved passwords of WLAN networks:** The passwords for the WLAN networks that their PCs are typically connected to are frequently forgotten by the users. If the networks are permitted to join automatically, all previously entered passwords will be retained on the computer. On the other hand, if a third party gains access to the user system, he can retrieve the saved passwords. If the next two commands are entered into the Windows command prompt, a list of all the SSIDs to which the machine has connected using the "Connect Automatically" option will be shown. For each SSID, the passwords is saved as key content in the security settings. Fig 2 depictsthe basic system architecture for our project. In this project, an investigation of WPA cracking has been carried out, and it has been found out that WPA-PSK cracking is the only possible way to crack this security standard

- **Commands: C1. netsh wlan show profiles**
  C2. netsh wlan show profile key=clear

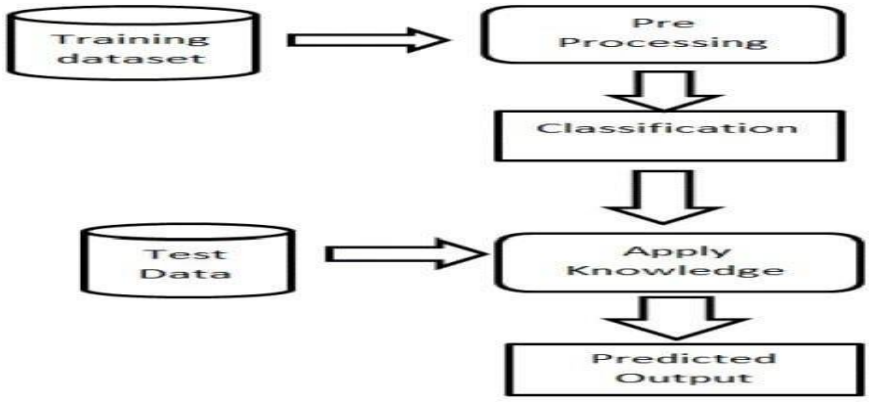

Fig . 2: Organization Structure.

ISSN No:-2456-2165

IV. DATA PREPARATION TECHNIQUES

Because of its simple syntax and readability, Python, an interpreted, object-oriented programming language comparable to PERL, has grown in popularity. Python is touted as being very simple to learn and portable, meaning that its statements may be understood in a variety of operating systems, including UNIX-based systems, Mac OS, MS-DOS, OS/2, and several versions of Microsoft Windows 98[4][8]. Python was developed by Guido van Rossum, a former resident of the Netherlands and a fan of Monty Python's Flying Circus at the time. The source code is publicly accessible and ready for reuse and modification. Significant numbers of people utilise Python.

Collect data from the ethical hacking process, including information on the tools and methods used, the results obtained, and any vulnerabilities identified.

Clean and organize the data to remove any inconsistencies or errors that may affect the accuracy of the analyze.

Use data analysis techniques to identify patterns and trends in the data, such as identifying common passwords patterns or weak spots in the network security.

Use the results of the data analysis to identify potential vulnerabilities and weaknesses in the network security. This can include identifying passwords that are easily guessable, outdated encryption methods, or open ports that may be vulnerable to attack[3][7].

Provide the owner of the Wi-Fi network with a detailed report that includes recommendations for improving the security of the network, such as upgrading encryption methods, changing passwords, and implementing additional security measures.

V. SYSTEM TESTING

System Testing is a level of the software testing where complete and integrated software is tested.Thepurposeof this test istoevaluatethe system'scompliance withthespecifiedrequirements.System Testing (ST) is a black box testing technique performed to evaluate the complete systemthesystem's compliance against specified requirements. InSystem testing, the functionalities ofthe systemare tested from an end-to-end perspective[6]. An accuracy of 75% in cracking Wi-Fipasswords using Python is a significant achievement. It means that out of 100 attempts, the passwords was successfully cracked in 75 cases, which is a good success rate. However, the remaining 25% may still pose a challenge, and the accuracy rate may vary depending on various factors, such as the complexity of the passwords, the security level of the Wi-Fi network, and the hardware and software used for cracking. It is also essential to note that cracking Wi-Fi passwords without the owner's consent is a serious offense and may result in legal consequences.

Testing	Accuracy of prediction
Performance	75%
Precision	0.8
Recall	0.8181

Table 1: Logistic Regression Classifier.

VI. METHODOLOGY

The brute force is a problem-solving strategy that involves extensively testing all viable solutions. The mechanism for employing the brute force is determined by the problem at hand. The generic approach, on the other hand.

The brute force is a technique for solving problems by exhaustively testing all possible solutions. The methodology for using the brute force depends on the specific problem you are trying to solve. However, the general approach involves the following steps:

- Identify the problem: You need to clearly understand the problem you are trying to solve and determine if a the brute force approach is appropriate.
- Define the solution space: You need to define the space of possible solutions. This includes determining the range of values that each variable can take, and how many variables are involved.
- Generate all possible solutions: Once you have defined the solution space, you need to generate all possible solutions. This can be done by systematically iterating through all possible combinations of values for the variables involved.
- Evaluate each solution: For each possible solution, you need to evaluate whether it satisfies the problem constraints and objectives. This may involve performing calculations or simulations.
- Select the best solution: Once you have evaluated all possible solutions, you need to select the one that meets the problem requirements and objectives.
- Optimize the solution: If necessary, you may need to optimize the selected solution further by refining the variables, or applying additional algorithms or techniques.

It should be noted that the brute force can be a very computationally expensive strategy, particularly for problems with huge solution spaces. In such circumstances, more efficient algorithms or techniques may be required to lessen the computing load.

VII. CREDENTIALS

Using penetration testing tools like Metasploit, a well-known open-source platform for creating, testing, and running exploit code, is one moral way to evaluate network security. Nmap is a programme for network discovery and mapping, and other tools like Wireshark may be used to capture and analyse network traffic.

It is crucial to make sure that any testing is done with the owner of the network's correct authority and legal agreement while doing research on the security of Wi-Fi networks. Furthermore, it's critical to take the necessary

ISSN No:-2456-2165

precautions to guarantee that any testing doesn't harm or damage the target or their network[6][3].

Consider adopting ethical hacking methods like passwords cracking if you're interested in learning more about a Wi-Fi network's credentials. For cracking passwords, a variety of programmes and tools are available, including Hashcat and John the Ripper.

Wi-Fi credentials are frequently compromised ethically for the following reasons:

- **Compliance:** Ethical hacking of Wi-Fipasswords may be motivated by compliance requirements, such as regulatory or industry-specific requirements for security testing.
- **Risk mitigation:** Organizations may use ethical hacking of Wi-Fipasswords as a proactive measure to identify potential vulnerabilities before they can be exploited by malicious attackers, thus reducing the risk of a security breach.
- **Reputation:** Ethical hacking of Wi-Fipasswords can help organizations demonstrate their commitment to security and their proactive approach to identifying and addressing potential vulnerabilities.
- **Security improvement:** By identifying weaknesses in the network security, ethical hacking of Wi- Fi passwords can help organizations implement stronger security measures and reduce the risk of a security breach.
- **Customer trust:** Customers may be more likely to trust organizations that demonstrate a commitment to security and a proactive approach to identifying and addressing potential vulnerabilities.

VIII. CONCLUSION AND FUTURE ENHANCEMENTS

The entire world is advancing towards technological advancement, and as a result, real-world processes are becoming more and more digitalized, increasing the danger of security. The workings of malevolent hackers, also known as crackers, who attempt to illegally breach security, and white hat hackers, also known as ethical hackers, who try to preserve security, were discussed in this study. Hacking is important since it deals with all sides of being good or harmful, much like the computer system. This essay also discusses the many sorts, strategies, and hacker assaults. Finally, it must be noted that ethical hacking is a tool that, when used properly, can contribute to a deeper comprehension of computers.

In a sense, any wireless network can be attacked in a variety of ways. Potential vulnerabilities include using the default SSID or passwords, WPS pin authentication, inadequate access control, and leaving the access point accessible in unlocked locations, all of which can lead to data theft of critical information. The architecture of kismet in WIDS mode may protect the network from DOS, MiTM, and MAC spoofing attacks. Regular software upgrades and the usage of firewalls, on the other hand, may assist protect the network from external intruders. Ethical hacking is the practice of identifying problems in a service, system, or institution's infrastructure that may be inject malicious code. By legitimately breaking into networks and searching for weakest places, they employ this approach to avoid invasions and privacy violations.

IX. RESULTS

For validating the task of retrieving the saved passwords of connected WLAN networks, the commands C1 and C2 are executed in the second author’s machine. When the command C1 is executed, the list of all WLAN networks or profiles (SSIDs) to which the machine is previously connected through the option “Connect Automatically”. The same can be observed. It can be observed that the machine was previously connected to five networks earlier and the user profiles in the graphic include the names of those networks. Executing the command C2 will allow you to crack profiles that have been obtained, as demonstrated above. The command was entered into the command line and run on one of the networks for confirmation. The command C2 will be in the format "netsh wlan show profile Redmi key=clear" and will be directed to the network "Redmi". Figure 3 displays a list of all user networks and passwords that have been documented in detail. The below fig 3 tells about cracked passwords using Python. The saved passwords will be put up but it won’t put up other networks passwords but it will be encypted with jumbled passwords.

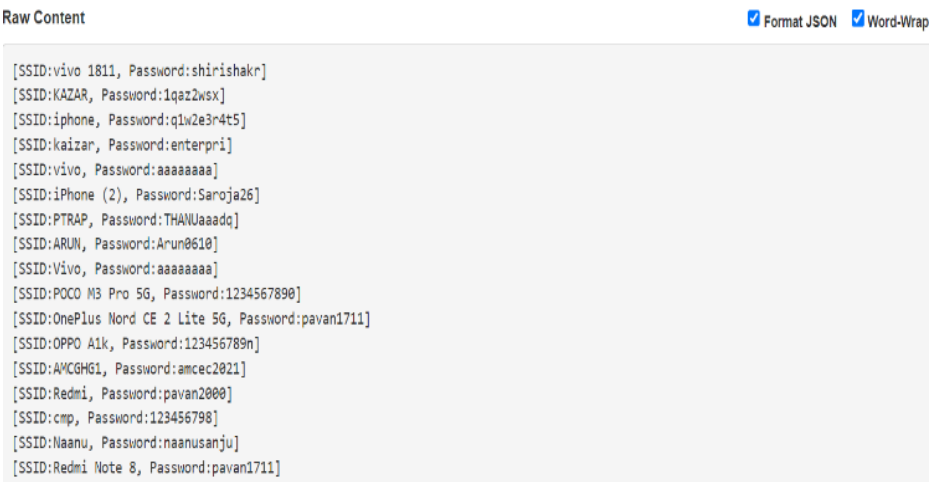

Fig. 3: Cracked Wi-Fi passwords

REFERENCES

[1.] Jamil and M. N. A. Khan, "Is Ethical Hacking Ethical?," Int. J. Eng. Sci. Technol., 2011.
[2.] R. Hartley, D. Medlin, and Z. Houlik, "Ethical Hacking: Educating Future Cyber security Professionals," Proc. EDSIG Conf., 2017.
[3.] Palmer, "Ethical hacking," IBM Syst. J., 2001, doi: 10.1147/sj.403.0769.
[4.] H.-R. Bae, M.-Y. Kim, S.-K. Song, S.-G. Lee, and Y.-H. Chang, "Security Attack Analysis for Wireless Router and Free Wi-Fi Hacking Solutions," J. Converg. Cult. Technol., 2016, doi: 10.17703/jcct.2016.2.4.65.
[5.] Z. Zhou, C. Wu, Z. Yang, and Y. Liu, "Sensorless sensing with Wi-Fi," Tsinghua Sci. Technol., 2015, doi: 10.1109/TST.2015.7040509.
[6.] D. Bharadia, K. R. Joshi, M. Kotaru, and S. Katti, "BackFi: High Throughput Wi-Fi Backscatter," Comput. Commun. Rev., 2015, doi: 10.1145/2785956.2787490.
[7.] Y. He, M. Chen, B. Ge, and M. Guizani, "On Wi-Fi Offloading in Heterogeneous Networks: Various Incentives and Trade-Off Strategies," IEEE Commun. Surv. Tutorials, 2016, doi: 10.1109/COMST.2016.2558191.
[8.] V. Kondrat, "Factors influencing consumer behavior," 2016. doi: 10.21661/r-80748.
[9.] M. (2012). Bansal A.& Arora, "Ethical Hacking and Social Security. Radix International Journal of Research in Social Science"