ISSN (O) 2393-8021, ISSN (P) 2394-1588

IARJSET

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁙ Peer-reviewed & Refereed journal ⁙ Vol. 11, Issue 6, June 2024

DOI: 10.17148/IARJSET.2024.11669

Wi-Fi Password Cracking

Dr Guruprakash CD[1], K Sai Manaswini[2], Meena D[3], Rakshitha GP[4], Varshini C V[5]

Professor, CSE Dept., Sri Siddhartha Institute of Technology, Tumakuru, Karnataka[1]

Student, CSE Dept., Sri Siddhartha Institute of Technology, Tumakuru, Karnataka[2-5]

Abstract: This attack can also help to quickly crack Wi Fi passwords and harvest Wi-Fi.Newtwork settings without the need for further orientation or Software. Using Python algorithms based on the operating system functionalities, it reduces this into three basic modules so that you can make most of your time - to drive changes.The first thing is it performs a deep dive into your Wi-Fi networks to create detailed profiles, with everything from connectivity type and status through to the name (SSID). This module teaches users so that they have the ability to understand more about their networks and how it behaves which in turn can enable them for better decisions making on network access/testing, etc. Finally, it gives a handy module for detecting all Wi-Fi networks names (a feature very helpful to identify the network formation).

I. INTRODUCTION

In today's highly connected world, Wi-Fi networks have become an essential part of everyday life, providing convenient and flexible internet access. However, with the increasing reliance on Wi-Fi, the need for effective management and security of these networks has grown significantly. Recovering lost Wi-Fi passwords and managing Wi-Fi profiles can often be a cumbersome task, typically requiring specialized software and intricate configurations. This project aims to address these challenges by introducing an innovative and efficient method for Wi-Fi password recovery and profile extraction using Python.Traditional methods for cracking Wi-Fi passwords often involve complex tools, lengthy processes, and require significant technical expertise. These methods can be timeconsuming and may not always provide accurate results. Our project leverages the inherent capabilities of the operating system combined with Python's powerful algorithmic capabilities to streamline this process, making it accessible and efficient for users with varying levels of technical knowledge.

The system is designed to be user-friendly, eliminating the need for additional software installations or complex setups. By incorporating three core modules, the projectprovides a comprehensive solution for Wi-Fi network management:

1. Network Scanning and Profile Extraction: This module conducts a thorough scan of connected Wi-Fi networks, extracting detailed profiles that include connectivity type, status, and SSID. It provides users with a clear overview of available networks, facilitating informed decisions for network access and troubleshooting.
2. Network Identification: The second module simplifies the process of identifying available Wi-Fi networks by retrieving and displaying their names. This feature is particularly beneficial in environments with multiple networks, helping users quickly locate and connect to the desired network.
3 Password Cracking: The final module employs advanced Python algorithms and OS tools to crack passwords for both current and previously connected Wi-Fi networks. This process is significantly faster than traditional methods, reducing waiting times.

II. OBJECTIVES

The primary objective is to develop a novel approach for efficiently cracking Wi-Fi passwords and extracting detailed Wi-Fi profiles without requiring additional software installations or complex configurations.

1. Comprehensive Network Scanning and Profile Extraction:
- Initiate a thorough scan of all connected Wi-Fi networks.
- This module will collect and display comprehensive profiles of available networks, including crucial information such as connectivity type, status, SSID (Service Set Identifier), security protocols and signal strength. By presenting this data in an organized manner, users will be able tomake informed decisions regarding network access and troubleshooting. This module aims to minimize manual intervention and simplify the process of network analysis

2. Network Identification and Name Retrieval:
- Provide a convenient module to retrieve the names of all available Wi-Fi networks.

DOI: 10.17148/IARJSET.2024.11669

- This feature is designed to simplify the identification of Wi-Fi networks in environments with multiple options. By displaying a list of names (SSIDs), users can quickly identify and select the desired network, reducing confusion and streamlining the connection process. This module enhances user experience by offering a clear and concise way to navigate through available networks.

3. Rapid Password Cracking Using Python Algorithms and OS Tools:

- Swiftly crack passwords for both current and previous Wi-Fi connections.
- This module leverages advanced Python algorithms and built-in OS tools to accelerate the password-cracking process. Traditional methods can be time-consuming and require specialized knowledge; this project aims to eliminate those barriers by providing a fast and accurate solution. The algorithms will be optimized for speed and reliability, ensuring that users can recover lost or forgotten passwords in a fraction of the time compared to conventional techniques.

4. User-Friendliness and Accessibility:

- Deliver a solution that is easy to use, even for individuals with limited technical expertise.
- The project prioritizes a user-friendly interface that guides users through each step of the process. Clear instructions and intuitive design elements will ensure that users can navigate the system effortlessly.
- This objective is crucial for making the tool accessible to a broader audience, including nontechnical users who need to manage their Wi-Fi connections efficiently.

III. METHODOLOGY

Cyber-attack is the technique of finding potential security holes in a computing device in order to gain access too individually or collective data, either ethically or unethically. The motive behind the hacking is totally depend to ethical hacking if that process is legal then he is Ethical Hacker he must have a Retain permission for penetrate on that system, server, company or any organization. If he has then and then he is Ethical Hacker otherwise we all know who that he a black hat hacker is.

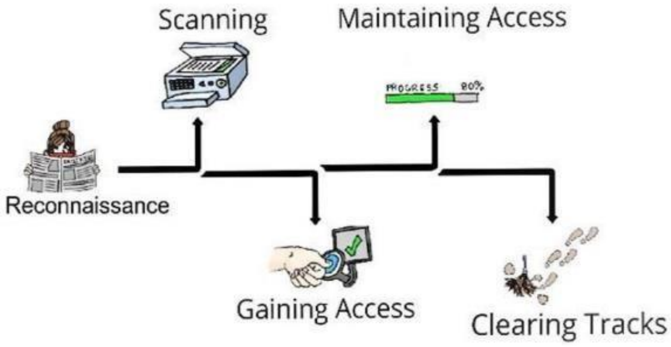


Figure 5.1: Maintaining Access of the System in the Particular Time.

Working:
Every phase is same for all hacking process nothing change for any hacker, doesn't matter if any black hat hackers or grey hat hackers doing anything. Only one thing is changing behind that hacking. The motive of Hacking or Penetrating that computer system, web server, website, mobile phone or anything else.

- The Maintaining Access Phase
- The Clearing Tracks Phase
- The Scanning Phase
- The Reconnaissance Phase
- The Gaining Access Phase
- Reconnaissance: Reconnaissance Surveillance has been the process of enhancing information about someone or something, they using different ways different technique for gather information, from other resource about a computer system, server, website or anything else, and collect lot of information from others way then they will go for the next phases The Scanning Phases.
- Scanning: After the active reconnaissance, Scanning is the phase where attacker collect information directly, attackers identify useful information about the target like ports information, Address, operating system, active host, server, installed serves, vulnerabilities, bugs etc.

DOI: 10.17148/IARJSET.2024.11669

- Gaining Access: After the scanning , they go for gaining access phases where they have already collect so much information about the target, because they already go with reconnaissance and scanning phases, they gain full access to that computer systems, networks, operating system or software At the computer system, application, network level, the attacker have full gaining access to yours device.
- Maintaining Access: After gaining full Access, there is another impotent step where we have to maintain the access. this is very impotent step because, if the user switch off his/her system than its difficult to gaining full access again and again it's better to maintain that access in most of the time attacker go with key logger, backdoors, rat, Trojans, payload, ransom ware, rootkit, spyware, worm etc. they just go with any of these after that they have full access of your device for long and long time. Figure 1 discloses the maintaining access of the WI-FI system.
- Clearing Tracks: On the last phase attacker erase all types of logs, malicious activity and everything related to that attack whatever they did with their server or system. At the other part penetration tester is doing same thing till now, at the last phases they have to submit their report on the basses of previous phases that process is known as
“Reporting” to system or server owner

To accelerate the WPA cracking, one possible way is to exploit the great computation power of GPU computation. GPGPU is the means of doing General Purpose computation (traditionally handled by the CPU) on a Graphics Processing Unit (GPU). GPUs are designed as computational accelerators or companion processors optimized for scientific and technical computing applications. Architecture of GPU and CPU are highly different. GPU is specialized for compute -intensive, highly parallel computation and therefore desi gned such that more ALUs are devoted to data processing rather than data caching and flow control. In the process, the most time - consuming step is the calculation of the PMK from the ESSID and Password, since it involves 8192 rounds of SHA1 calculation.

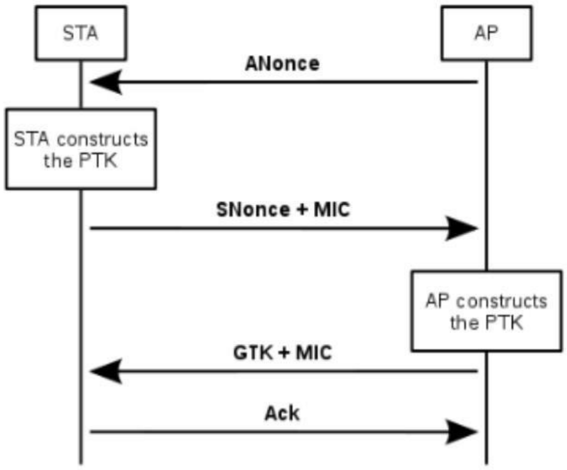


Figure 5.2: Scenario of four-way handshake

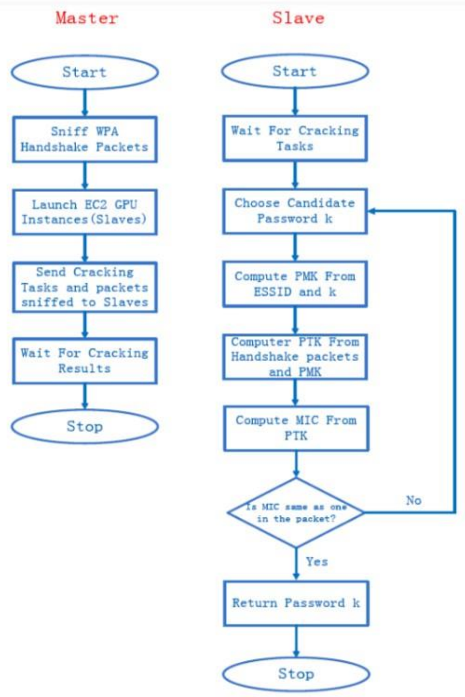

Master
Slave
Start
Sniff WPA Handshake Packets
Launch EC2 GPU Instances(Slaves)
Send Cracking Tasks and packets sniffed to Slaves
Wait For Cracking Results
Stop
Start
Wait For Cracking Tasks
Choose Candidate Password k
Compute PMK From ESSID and k
Computer PTK From Handshake packets and PMK
Compute MIC From PTK
Is MIC same as one in the packet?
No
Yes
Return Password k
Stop

Figure 5.4: Flowchart for a Brute-Force Attack

The image depicts the steps involved in a brute-force attack on a WPA-encrypted Wi-Fi network. Brute-force attacks are a hacking technique where a computer program tries a large number of possible passwords or encryption keys until it finds the correct one. In the context of Wi-Fi networks, a brute-force attack would target the WPA handshake, which is a sequence of messages exchanged between a client device (such as a laptop or smartphone) and a wireless router when the device

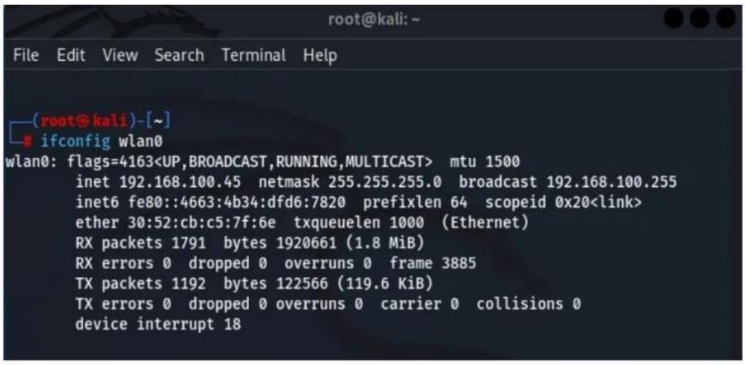
DOI: 10.17148/IARJSET.2024.11669

Wi-Fi Network Properties:

- ESSID – The network name
- BSSID – MAC address of the access point

•CH – Channel Number

- Beacons – Number of announcements packets sent by the access point
- ENC – Encryption Algorithm in use
- CIPHER – The detected cipher
- AUTH – The authentication protocol
- In terminal type ifconfig command to identify wlan0 name



```
┌──(root㉿kali)-[~]
└─# ifconfig wlan0
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.45  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::4663:4b34:dfd6:7820  prefixlen 64  scopeid 0x20<link>
        ether 30:52:cb:c5:7f:6e  txqueuelen 1000  (Ethernet)
        RX packets 1791  bytes 1920661 (1.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 3885
        TX packets 1192  bytes 122566 (119.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 18
```

Figure 5.3: ifconfig command

connects to the network. The flowchart above starts with two boxes labelled "Master" and "Slave," which suggests that this attack might be utilizing a distributed computing system. In a distributed computing system, a large task is broken down into smaller subtasks that are then executed on multiple computers. This can significantly speed up the attack process. The flowchart above starts with two boxes labelled "Master" and "Slave," which suggests that this attack might be utilizing a distributed computing system. In a distributed computing system, a large task is broken down into smaller subtasks that are then executed on multiple computers. This can significantly speed up the attack process. Here is a breakdown of the steps depicted in the flowchart:

1. **Start**: The attack begins on both the master and slave devices.
2. **Sniff WPA Handshake Packets (Master):** The master device captures the WPA handshake packets from the target wireless network. These packets contain information about the network's encryption, including the SSID (network name).
3. **Wait for Cracking Tasks (Slave):** The slave device waits for instructions from the master device.
4. **Launch EC2 GPU Instances (Slaves):** The master device launches EC2 GPU instances on Amazon Web Services (AWS). EC2 stands for Elastic Compute Cloud, and it is a service that allows users to rent virtual servers in the cloud. GPUs (Graphics Processing Units) are specialized processors that are well-suited for tasks that require a lot of parallel processing, such as brute-forcing encryption keys.
5. **Send Cracking Tasks and packets sniffed to Slaves (Master):** The master device sends the captured WPA handshake packets and the cracking tasks to the slave devices.
6. **Choose Candidate Password (Slave):** The slave device selects a candidate password to try.
7. **Compute PMK from ESSID and k (Slave):** The slave device computes the PMK (Pairwise Master Key) from the SSID and the candidate password. The PMK is a key that is used to derive other keys that are used to encrypt communication between a client device and a wireless router.
8. **Compute PTK from Handshake packets and PMK (Slave):** The slave device computes the PTK (Pairwise Transient Key) from the captured WPA handshake packets and the PMK. The PTK is another key that is used to encrypt communication between a client device and a wireless router.
9. **Compute MIC from PTK (Slave**): The slave device computes the MIC (Message Integrity Check) from the PTK. The MIC is a value that is used to verify the integrity of the handshake packets.
10. **Is MIC same as one in the packet? (Slave):** The slave device compares the computed MIC to the MIC that is contained in the captured WPA handshake packets.
11. **Yes (Slave):** If the MICs match, then the slave device has found the correct password.
12. **Return Password (Slave):** The slave device sends the cracked password back to the master device.
13. **Stop (Master & Slave):** The attack stops on both the master and slave devices.

Brute-force attacks can be very time-consuming, but they can be successful if the attacker has enough computing power and if the password being targeted is weak. There are a number of ways to protect your Wi-Fi network from bruteforce attacks, including using a strong password, enabling WPA3 encryption (which is more resistant to brute-force attacks than WPA2), and disabling WPS (Wi-Fi Protected Setup).

IV. RESULT ANALYSIS

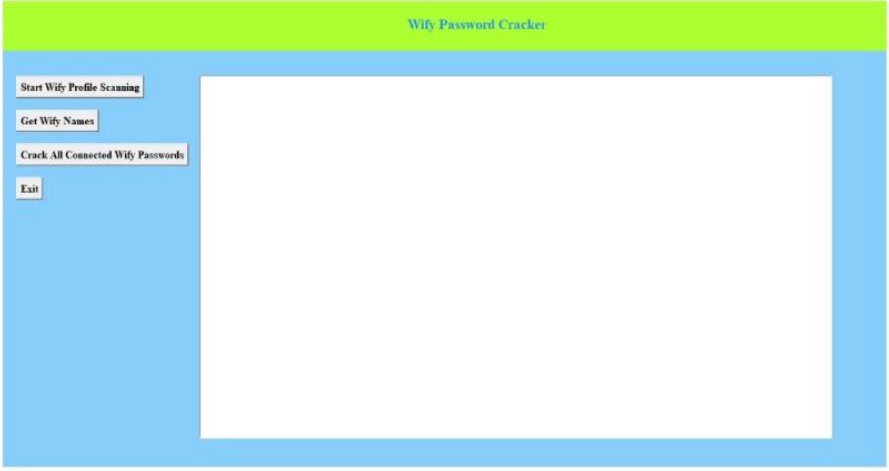

Wify Password Cracker
Start Wify Profile Scanning
Get Wify Names
Crack All Connected Wify Passwords
Exit

Figure 9.1: Wi-Fi profile scanning

Each Wi-Fi will have its own Profile which contains details like connectivity type, status, SSID and many more. So to extract all Wify details along with cracking Password we have used inbuilt OS tool which with python algorithm which will scan all current and previous connected WIFI and then display entire profiles. User can also extract names of all WIFI and can extract password also.

- Scanning for Available Networks: When you click the "Start W-Fi Profile Scanning" button, the application might attempt to scan for wireless networks in your vicinity. This could involve querying the operating system for a list of detectable Wi-Fi access points (APs).
- Displaying Network Information (if implemented):

display information about the detected networks, such as:

1. SSID (network name)
2. Signal strength
3. Cracked Wifi Passwords

V. CONCLUSION

Wi-Fi password cracking presents a complex issue with both legitimate and malicious applications. While the ability to recover forgotten passwords or assess network security holds value, unauthorized access to Wi-Fi networks poses a significant security risk.

- Focus on Strong Passwords: Implementing strong, unique passwords for each Wi-Fi network significantly reduces the risk of unauthorized access

. • Authorized Recovery: If you've forgotten your own Wi-Fi password, consult your router's manual or manufacturer for legitimate recovery methods.

- Network Security Assessments: Authorized penetration testing with proper consent can help identify network weaknesses without compromising security.

The Future: Ethical development in the Wi-Fi password cracking space can focus on:

- Security Assessments: Tools that identify vulnerabilities and suggest remediation strategies for authorized network administrators.
- Social Engineering Detection: Systems that raise awareness and help users avoid social engineering attacks targeting Wi-Fi passwords.

DOI: 10.17148/IARJSET.2024.11669

- Advanced Network Analysis: Extracting additional profile information and integrating with security frameworks for comprehensive network security solutions (with proper authorization). In conclusion, Wi-Fi password cracking remains a powerful tool, but its ethical application is crucial. By prioritizing strong passwords, exploring legitimate recovery methods, and focusing on authorized security assessments, we can ensure secure Wi-Fi networks for everyone.

REFERENCES

[1]. D. 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 Cybersecurity Professionals," Proc. EDSIG Conf., 2017.

[3]. C. C. 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 WiFi," Tsinghua Sci. Technol., 2015, doi: 10.1109/TST.2015.7040509.

[6]. D. Bharadia, K. R. Joshi, M. Kotaru, and S. Katti, "BackFi: High Throughput WiFi Backscatter," Comput. Commun. Rev., 2015, doi: 10.1145/2785956.2787490.

[7]. Y. He, M. Chen, B. Ge, and M. Guizani, "On WiFi Offloading in Heterogeneous Networks: Various Incentives and Trade-Off Strategies," IEEE Commun. Surv. Tutorials, 2016, doi: 10.1109/COMST.2016.2558191.

[8]. D. 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".