A logo for a college

Description automatically generated

**Hack Something Project Report- WPA Cracking**

**Hacking & Exploits**

**Prof. Mo Ghazouly Elghazouly**

**Group members:**

**Hetarth Sanghrajka (100900915)**

**Maisha Khatoon (100899259)**

# Hack something topic- WPA Cracking

## Introduction

WPA or Wi-Fi Protected Access cracking refers to a cyber attack technique used to undermine the security of wireless networks that employ the WPA security protocol. The integration of Wi-Fi networks into contemporary communication systems has become indispensable, as it offers a convenient means of internet connectivity to a vast number of individuals. To ensure the secrecy and integrity of data transferred via Wi-Fi networks, many security protocols have been devised, among which the Wi-Fi Protected Access (WPA) protocol stands out as a very prevalent choice.

This research examines the phenomenon of WPA cracking, investigating its operational principles, prospective consequences, and the need to establish resilient security mechanisms to safeguard against such assaults. By comprehending the complexities of WPA cracking and its implications for network security, people and companies may adopt proactive measures to safeguard their Wi-Fi networks from possible cyber attacks.

## Abstract

This article offers a comprehensive overview of WPA cracking, a malevolent approach used to breach the security of Wi-Fi networks safeguarded by the WPA protocol. The abstract provides a summary of the report's contents, including the technical elements of WPA cracking, its impact on network security, and the need to implement effective measures to mitigate such vulnerabilities. The primary aim of this initiative is to enhance understanding and consciousness of the susceptibilities associated with WPA, while also providing people and organizations with the necessary information and skills to effectively safeguard against potential WPA cracking efforts. This study aims to comprehensively examine the underlying mechanisms involved in WPA cracking, evaluate the possible consequences of successful assaults, and emphasize the need for proactive security measures in safeguarding sensitive data. This study also includes a practical implementation of how WPA Cracking works in real life.

## Objective

The main objective of this research is to do a thorough analysis of WPA cracking as a potential security vulnerability for Wi-Fi networks. The paper endeavors to enhance awareness about the significance of safeguarding Wi-Fi networks by comprehending the methodologies used by attackers to exploit flaws in WPA. Moreover, it underscores the need to implement optimal strategies to address the vulnerabilities associated with WPA cracking and safeguard valuable data from prospective cyber intrusions.

The objectives of this study are as follows:

* Understanding WPA Cracking: This paper aims to elucidate the underlying mechanisms of WPA cracking, elucidating the methodologies used by malicious actors to exploit weaknesses in WPA security protocols.
* Examining Consequences: This investigation aims to analyze the possible ramifications of successful WPA cracking attempts on persons and organizations, including unlawful entry into sensitive information and breaches of privacy.
* The purpose of this study is to underscore the importance of ensuring the security of Wi-Fi networks and the proactive security measures that may be taken to safeguard against WPA cracking and other cyber threats.
* Offering Best Practices: This paper aims to provide practical suggestions and best practices for people and businesses seeking to improve the security of their Wi-Fi networks and protect against potential WPA cracking efforts.

## Scope

The scope of this paper is to provide a thorough examination of WPA cracking, including several facets of its operation, implications for network security, and preventative measures. This research will explore the intricacies of WPA cracking, elucidating the assault methodologies used by cybercriminals to penetrate networks secured by WPA. The paper will clarify the importance of ensuring the security of Wi-Fi networks and the function of proactive security measures in safeguarding against WPA cracking and other cyber threats. This paper aims to provide practical ideas and best practices for people and companies to improve the security of their Wi-Fi networks and protect against potential WPA cracking efforts.

It is noteworthy that the scope of this paper is limited to the examination of WPA cracking, excluding other types of Wi-Fi security breaches, such as WEP cracking or brute-force assaults targeting vulnerable passwords. The primary aim of this study is to provide a thorough comprehension of WPA cracking, so empowering individuals to make well-informed choices to enhance the security of their Wi-Fi networks.

## How does WPA Cracking work?

The process of WPA cracking involves leveraging weaknesses within the WPA security protocol to illicitly get entry into Wi-Fi networks that are safeguarded. The cracking process encompasses several methodologies, each aimed at uncovering the pre-shared key (PSK) or password of a Wi-Fi network. The following is a comprehensive description of the prevalent techniques used in the process of WPA cracking:

* Brute-Force Attack: A brute-force attack involves the systematic testing of all possible character combinations by an attacker to discover the proper Pre-Shared Key (PSK). The approach is quite laborious and demands a significant allocation of resources, particularly when dealing with lengthier and more intricate passphrases. Nevertheless, the likelihood of success increases when the passphrase is weak or relatively short.
* Dictionary Attack: The dictionary attack is a method used by an adversary whereby they utilize a preassembled collection of frequently used words and phrases, referred to as a dictionary, to make educated guesses to ascertain the proper passphrase. The approach exhibits more efficiency compared to brute-force methods since it effectively decreases the total number of potential combinations that need to be tested. The efficacy of this assault is contingent upon the robustness of the selected passphrase.
* Rainbow Table Attack: The rainbow table attack involves the use of a precomputed catalog of hash values corresponding to a range of potential passphrases. During a rainbow table attack, the perpetrator engages in the process of comparing the hash value of the captured handshake with the entries contained inside the rainbow table, to identify a corresponding match. If a match is detected, the associated passphrase is disclosed.
* WPS Vulnerability: The WPS vulnerability pertains to the Wi-Fi Protected Setup (WPS) function, which serves to streamline the process of establishing connections between devices and Wi-Fi networks. Nevertheless, the Wi-Fi Protected Setup (WPS) protocol is susceptible to potential security breaches due to the possibility of brute-force attacks targeting the WPS PIN. Certain routers may exhibit suboptimal implementation of Wi-Fi Protected Setup (WPS), hence rendering them vulnerable to potential exploitation by malicious actors who may use PIN guessing techniques to illicitly infiltrate the network.
* Capture & Offline Attack: The Capture and Offline Attack technique involves the acquisition of the WPA handshake by an unauthorized individual when a legitimate user establishes a connection to the Wi-Fi network. The handshake protocol includes encrypted data that is essential for the derivation of the password. Subsequently, the assailant proceeds with the offline cracking process, systematically attempting many passphrases to decode the handshake and successfully get the correct passphrase.

It is essential to acknowledge that the efficacy of WPA cracking is mostly contingent upon the robustness of the passphrase. Passphrases that are lengthy and intricate, including a combination of capital and lowercase letters, numerals, and special characters, exhibit enhanced resilience against unauthorized access attempts. In this report, we have used Brute-Force Attack as the practical implementation of WPA Cracking.

## Impacts of WPA Cracking

The act of breaking WPA (Wi-Fi Protected Access) may result in significant repercussions for both people and companies. The ramifications of successfully breaking WPA (Wi-Fi Protected Access) attacks encompass:

* Unauthorized Network Access: The main consequence of WPA cracking is the illegal infiltration of the Wi-Fi network. Adversaries possess the capability to infiltrate the network under the guise of authorized users, so enabling them to intercept network communications and perhaps engage in malicious actions.
* Data Breaches: Data breaches occur when unauthorized individuals get access to a Wi-Fi network and intercept confidential information that is being transferred via the network. This includes personal information, login passwords, financial data, and other sensitive information.
* Privacy Breaches: Privacy breaches occur when the security of a network is compromised, leading to unauthorized access and potential exposure of sensitive information belonging to users connected to the network. One such method of breaching privacy is the cracking of WPA (Wi-Fi Protected Access), which undermines the confidentiality measures put in place to safeguard user data. The act of monitoring and eavesdropping on individuals' online activity by malicious actors might result in infringements of their privacy.
* Man-in-the-Middle (MitM): Man-in-the-Middle (MitM) assaults may be facilitated by the process of WPA cracking, which enables attackers to exploit vulnerabilities in the security protocol. This allows them to place themselves strategically between the user and the network, therefore gaining unauthorized access to communication channels. Consequently, the attackers can intercept and manipulate the sent data, posing a significant threat to the integrity and confidentiality of the communication.
* Data Tampering: Data tampering is a malicious activity when someone with malicious intent manipulates data that is being communicated across a network. This unlawful manipulation may result in several undesirable outcomes such as unauthorized modifications to messages, corruption of data, or the dissemination of false information.
* Reputation Impairment: Within enterprises, the successful execution of a WPA cracking assault has the potential to result in a substantial erosion of confidence among customers, partners, and stakeholders. The potential consequences of such actions include detrimental effects on the organization's reputation and subsequent financial losses.
* Legal & Compliance issues: The occurrence of data breaches arising from the cracking of Wi-Fi Protected Access (WPA) might give rise to legal ramifications and non-adherence to legislation about the safeguarding of data.

## The potential consequences to an individual or Organization

The potential consequences of WPA breaking may have severe implications for both an individual and organizations:

* Financial losses: Financial losses may arise in enterprises due to several factors such as data breaches, the theft of sensitive information, and possible legal fines or reimbursement to impacted parties.
* Loss of confidential information: The unauthorized disclosure of confidential information, including but not limited to customer data, intellectual property, and trade secrets, may result in significant negative impacts on a company's competitive position.
* Damage to reputation: The repercussions of a security breach caused by WPA cracking may have detrimental effects on the reputation of both persons and companies. It has the potential to degrade their standing, undermine trust, and impact their future interactions with consumers and clients.
* Identity theft & fraud: Identity theft and fraud are serious concerns that might arise because of WPA cracking. This unauthorized access to wireless networks can potentially lead to the abuse of personal information for unscrupulous purposes.
* Regulatory fines & legal consequences: Non-compliance with data privacy standards may lead to substantial financial penalties and legal consequences for corporations.
* The disruption of services: The disruption of services may occur when businesses experience successful WPA cracking, leading to network service disruptions that hurt productivity and customer satisfaction.
* Litigation & legal costs: Litigation and legal expenses may be significant for organizations as they navigate the consequences of a security breach.
* The destruction of trust: The loss of trust from consumers, clients, and partners may have enduring implications for both persons and organizations, impacting commercial relationships over an extended period.

## Practical Implementation

We are going to perform the whole implementation on Kali Linux on virtual machine for the WPA cracking.

Step 1:

A computer screen shot of a dragon

Description automatically generated

Step 2:

A screenshot of a computer

Description automatically generated

Step 3:

A screenshot of a computer

Description automatically generated

Step 4:

A screenshot of a computer

Description automatically generated

## Benefits of WPA Cracking

It is important to emphasize that the act of WPA cracking is inherently malevolent and constitutes a violation of federal statutes. Participating in the unauthorized breaking of WPA (Wi-Fi Protected Access) is considered a criminal act and may result in significant legal ramifications. Nevertheless, it is essential to consider the ethical and security implications while examining the advantages of researching WPA cracking. This knowledge may be crucial in enhancing the security of Wi-Fi networks for enterprises and enabling security experts to effectively safeguard against possible breaches. Several notable advantages encompass:

* Identification of Vulnerabilities: The identification of vulnerabilities may be achieved via the examination of WPA cracking methods, enabling security experts to discern weaknesses within their Wi-Fi networks and get insights into the possible avenues of attack that may be used by cybercriminals. This information enables individuals to implement proactive actions to enhance the security of their network.
* Improving Network Security: Gaining a comprehensive understanding of WPA cracking enables enterprises to effectively adopt enhanced security measures for safeguarding their Wi-Fi networks. By acknowledging the potential hazards linked to vulnerable passphrases and obsolete encryption techniques, organizations may implement more robust security protocols.
* Awareness & Education: The dissemination of research findings and engagement in the scholarly discourse around WPA cracking serve to enhance the level of knowledge about the significance of Wi-Fi security within both individual and organizational contexts. It promotes the adoption of optimal strategies and the maintenance of awareness about possible risks.
* Developing Countermeasures: The study of WPA cracking strategies facilitates the formulation of effective countermeasures. Security experts can develop tools and solutions that may effectively identify and thwart efforts to break WPA, therefore bolstering the overall protection of a network.
* Real-world simulations: Real-world simulations using ethical hacking and controlled simulations of WPA cracking may provide enterprises with a means to evaluate the susceptibility of their network to such assaults while ensuring little damage is inflicted. The simulations provide significant insights into vulnerabilities inside networks and potential avenues for improvement.
* Security Research: In the realm of security research, ethical researchers engage in the study of WPA cracking to analyze encryption methods, investigate possible flaws, and make valuable contributions to the enhancement of robust security measures.
* Testing Security Measures: The evaluation of security measures via ethical hacking, which includes controlled efforts to breach WPA, enables enterprises to assess the efficacy of their security protocols within a controlled setting. This practice helps in refining their security plan and maintaining an advantage over possible adversaries.

## Challenges in WPA Cracking

Despite the potential risks associated with WPA cracking, attackers encounter various hurdles while attempting to exploit this vulnerability.

* Strong Passphrases: The use of strong and intricate passphrases poses a considerable obstacle to the process of cracking WPA, as it substantially prolongs the time and resources necessary for such efforts. Consequently, it becomes arduous to get unauthorized access to securely safeguarded networks.
* Offline Attacks: The process of capturing the WPA handshake for offline cracking requires the attacker to be physically close to the target network, hence restricting the potential for remote attackers to carry out such attacks.
* WPA3 Enhancements: The implementation of WPA3 has resulted in increased complexity for cracking WPA, mostly attributed to its augmented security measures and heightened resilience against offline dictionary attacks.
* Rate limiting & lockout policies: Rate limitation and lockout rules are often used by Wi-Fi routers to mitigate the risk of brute-force assaults, therefore impeding the cracking process by reducing its speed.
* Storage & Computation requirements: The generation and storage of rainbow tables for WPA cracking need substantial computing resources and storage capacity.

## Best Practices in WPA Cracking

It is imperative to underscore that the act of WPA cracking is both unlawful and morally objectionable. Participating in unlawful hacking endeavors might result in legal prosecution and significant ramifications. Instead, people and companies should prioritize the implementation of optimal strategies to safeguard their Wi-Fi networks from possible security breaches. The below suggestions are the recommended best practices:

* Utilize Robust and Distinct Passphrases: Implement lengthy and intricate passphrases that include a combination of capital and lowercase letters, numerical digits, and distinctive symbols.
* Activate WPA3 (If supported): If your Wi-Fi devices possess the capability to implement WPA3, it is advisable to enable this protocol to use its augmented security attributes.
* Regular firmware updates: Regular firmware updates are essential for maintaining the security of Wi-Fi routers and access points. By ensuring that the newest firmware is installed, known vulnerabilities may be effectively addressed.
* Disable WPS: It is advisable to deactivate the Wi-Fi Protected Setup (WPS) feature on your wireless network, unless it is essential, to mitigate the risk of possible brute-force assaults.
* Network Segmentation: To mitigate the potential consequences of a successful breach, enterprises should implement the practice of segmenting their Wi-Fi network into distinct VLANs.
* Intrusion Detection & Prevention: The use of Intrusion Detection and Prevention (IDS/IPS) systems is recommended to identify and mitigate unwanted access attempts and possible assaults.
* Regular Security Assessments: Regular security assessments should be conducted to periodically evaluate the security of the Wi-Fi network and discover any vulnerabilities or weaknesses that may be present. These assessments should include vulnerability scans to thoroughly examine the network and ensure that any potential security issues are promptly addressed.

## Conclusion

The conclusion is designed to briefly outline the primary discoveries presented in the research and emphasizes the need of safeguarding Wi-Fi networks against potential WPA cracking. This statement underscores the need of adhering to established protocols to establish a strong and effective defense against cyber attacks. The section finishes by advocating for the prioritization of Wi-Fi security and the use of proactive measures to safeguard networks and data.

In summary, this paper provides insights into the concerning hazards linked to WPA cracking and the possible ramifications of vulnerable Wi-Fi networks. By comprehending the mechanics of WPA cracking, recognizing the need of safeguarding Wi-Fi networks, and implementing optimal strategies, people and businesses may effectively fortify themselves against malicious actors in the digital realm. Implementing these procedures would effectively enhance the security of the Wi-Fi environment and provide robust protection for sensitive information in an ever more linked global context.

## References

Pandikumar, T., & Yesuf, M. A. (2017). Wi-Fi security and testbed implementation for WEP and WPA cracking. International Journal of Engineering Science, 13571.

Georgios, G. (2014). Wi-Fi security and testbed implementation for WEP/WPA cracking demonstration. Kingston University London.

Mittal, S., Thakur, B., & Mangla, P. (2012). Improvement on WPA with RSA. International Journal of Engineering Research and Applications, 2(3), 1671-1674.

Alliance, W. F. (2003). Wi-Fi Protected Access: Strong, standards-based, interoperable security for today’s Wi-Fi networks. White paper, University of Cape Town, 492-495.

Chang, T. H., Chen, C. M., Hsiao, H. W., & Lai, G. H. (2019). Cracking of WPA & WPA2 using GPUs and rule-based method. Intelligent Automation and Soft Computing, 25(1), 183-192.