HACKER COMBAT COMMUNITY

How Are Passwords Cracked?

Overview of password cracking motives, techniques, tools, and defenses.

Hackercombat.com

Interception

Interception involves capturing data as it travels over a network. Cybercriminals use techniques like Man-in-the-Middle (MitM) attacks, where they insert themselves into a communication session between a user and an application to eavesdrop or alter the data being exchanged. For example, on an unsecured Wi-Fi network, an attacker could intercept data packets that contain unencrypted passwords. Similarly, using tools like packet sniffers, attackers can capture passwords as they traverse a network and then decode them if they're not properly encrypted.

Another form of interception is SSL stripping, where the attacker forces a connection to revert from a secure HTTPS connection to an unsecured HTTP version, making the data accessible. For instance, if a user logs into a site that has been compromised by an SSL stripping attack, their password and other sensitive information could be transmitted in clear text, easily captured by the attacker.

Searching & Brute Force

Searching and brute force attacks are about trying as many combinations as possible until the correct password is found. Brute force attacks use algorithms that systematically check all possible passwords by going through a list of potential options one by one. For instance, an attacker might use a brute force attack against a website's login page, attempting every combination of letters, numbers, and symbols until they gain access.

With the advancement in computing power, brute force attacks can now be executed faster and more efficiently than ever. Attackers can use powerful computers or botnets to try millions of password combinations in a short period, cracking weaker passwords with relative ease. They may also employ more sophisticated 'searching' tactics like using databases of common passwords or previously breached credentials, which can significantly speed up the process.