In the early days of computing, passwords were often stored in plaintext, meaning, anyone with access to the password file could easily read the passwords. As computer systems became more widespread, users started to use more complex passwords, and administrators began to use various encryption methods to keep passwords secure.

Nevertheless, as technology advanced, so did the techniques used by cyber criminals to crack passwords. As a result, security professionals developed various password cracking tools to test the security of password systems. One of the earliest password cracking tools was Crack,developed in the 1990s by Alec Muffett. As computer systems evolved, security professionals developed more advanced password cracking tools that used more sophisticated techniques to crack passwords.

Understanding password cracking tools are crucial in identifying and mitigating security vulnerabilities. Password cracking tools are applications designed with the purpose of revealing or recovering password authentications used for access to networks, web applications, files and more.

Password cracking tools are software applications designed to reveal or recover passwords for digital authentication mechanisms. These tools use various techniques, such as brute force, dictionary attack, and hybrid attack, to guess or crack passwords.

A brute force attack is a technique in which the password cracking tool tries all possible combinations of characters to guess the correct password. The tool starts with the simplest passwords, such as "password" or "123456," and gradually tries more complex passwords until it finds the correct one. This technique is time-consuming and requires a lot of computational power, but it is effective against weak passwords.

A dictionary attack is a technique in which the password cracking tool uses a pre-built list of words to guess the correct password. This list contains common words and phrases, such as "password," "admin," and "123456," which are often used as passwords. The tool matches the words in the list with the password until it finds a match. This technique is faster than a brute force attack and is effective against weak passwords.

A hybrid attack is a technique that combines the brute force and dictionary attacks. The tool uses a dictionary attack with variations, such as adding numbers or symbols to the words in the list. This technique is effective against strong passwords that are not in the dictionary.

A rule-based attack involves creating custom rulesets that define the structure of the password, such as the length, character set, and position of specific characters.

To use these techniques, the password cracking tool must have access to the encrypted password. This is usually obtained through following methods:

Network Sniffing: The password cracking tool can sniff the network traffic to capture the encrypted password. This is useful when the authentication mechanism sends the password in clear text or uses a weak encryption algorithm.

1. Brute Force: The password cracking tool can attempt to log in to the authentication mechanism using a list of usernames and passwords. If the login is successful, the tool has access to the encrypted password.
2. Stolen Password Database: The password cracking tool can use a stolen password database to crack the passwords. These databases are often obtained through data breaches or other security incidents.

Some information to know before continuing: A hashed password is a one-way cryptographic function that transforms a password into a fixed-length string of characters that represents the original password. Hashing is a process that takes the password as input and generates a unique string of characters as output, which is called the password hash. Hashing is a process that takes the password as input and generates a unique string of characters as output, which is called the password hash. The password hash is different from the original password and cannot be used to directly recover the original password

There are several password cracking tools available. John the Ripper is a popular password cracking tool that can crack passwords from various operating systems, including Linux, macOS, and Windows. It can also use different hashing algorithms, including MD5, SHA-1, and bcrypt. To use John the Ripper, the program needs to be provided with a password file, which contains hashed passwords. A hashed password is a one-way cryptographic function that transforms a password into a fixed-length string of characters that represents the original password. The program then uses the selected cracking method to try and crack the passwords. John the Ripper can also use wordlists and rulesets to modify dictionary words and increase the likelihood of cracking passwords.

Another password cracking tool utilized by penetration testers and hackers alike is Hashcat. Hashcat is a free, open-source password cracking tool that uses multiple techniques, including brute-force attacks, dictionary attacks, mask attacks, and hybrid attacks, to crack passwords. It can crack passwords from various operating systems, including Linux, macOS, and Windows, and can use different hashing algorithms, including MD5, SHA-1, and bcrypt. Hashcat also supports advanced features, such as distributed cracking, which allows multiple computers to work together to crack passwords more quickly, and session management, which allows users to save and resume cracking sessions. To use Hashcat, you need to provide it with a password file, which contains hashed passwords, and a ruleset, which defines the cracking method. Hashcat then uses the selected cracking method to try and crack the passwords.

Aircrack-ng is a free, open-source password cracking tool that is specifically designed to crack Wi-Fi passwords. It utilizes various methods, including dictionary attacks and brute-force attacks, to crack Wi-Fi passwords. To use Aircrack-ng, you need to capture packets from a Wi-Fi network using a wireless network interface card that supports monitor mode and packet injection. Aircrack-ng then analyzes the captured packets to determine the authentication key

and encryption key used by the network. Aircrack-ng can use various methods to crack the Wi-Fi password, including dictionary attacks, brute-force attacks, and rule-based attacks. Aircrack-ng also supports other features, such as the ability to generate traffic to speed up the cracking process and the ability to perform distributed cracking using multiple computers.

Cain and Abel is a Windows-based password cracking tool that uses various methods, including dictionary attacks and brute-force attacks, to crack passwords. It can access passwords from various sources, including Windows SAM files, NTLM hashes, and wireless network passwords. To use Cain and Abel, you need to provide it with a password file, which contains hashed passwords. The tool then uses the selected cracking method to try and crack the passwords. Cain and Abel can use various methods to crack passwords, including dictionary attacks, brute-force attacks, and hybrid attacks. Cain and Abel also has other features, such as the ability to perform network sniffing and password dumping, which can be useful for obtaining password hashes and cracking passwords.
Hydra is a free, open-source password cracking tool that is used to perform brute-force attacks on login credentials. It can be used to crack passwords for various protocols, including HTTP, FTP, SSH, Telnet, and many others. To use Hydra, you need to provide it with a list of usernames and a list of passwords. Hydra then uses the selected protocol and a selected cracking method to try and crack the login credentials. Hydra also supports other features, such as the ability to perform distributed cracking using multiple computers and the ability to resume cracking sessions.

Some lesser known password cracking tools are:
Medusa is a free, open-source password cracking tool that can perform brute-force attacks against various protocols, including HTTP, FTP, SSH, Telnet, and many others.

Patator is a free, open-source, multi-purpose password cracking tool that can perform brute-force attacks, dictionary attacks, and hybrid attacks against various protocols, including FTP, SSH, Telnet, and many others.

RainbowCrack is a free, open-source password cracking tool that uses rainbow tables to crack passwords. Rainbow tables are precomputed tables of password hash values that can be used to crack passwords quickly.

THC Hydra is a free, open-source password cracking tool that can perform brute-force attacks against various protocols, including HTTP, FTP, SSH, Telnet, and many others. It also supports parallelized attacks and distributed cracking using multiple computers.