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 (Lainhart, 2020).

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.

Security professionals developed various password cracking tools to test the security of password systems. John the Ripper is a popular password cracking tool that can crack passwords from various operating systems, including Linux, macOS, and Windows (J. the Ripper, n.d.). This tool 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.

References:
J. the Ripper. (n.d.). Retrieved April 7, 2023, from https://www.openwall.com/john/

Lainhart, J. (2020). Passwords and Their History. Retrieved April 7, 2023, from https://www.ntp.gov/docs/internetworks/PasswordHistory.pdf