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.

Stealing Passwords

Stealing passwords can be as simple as finding a written note containing login details or as complex as extracting passwords from databases. For example, a common method of stealing passwords is through database breaches where encrypted password data is extracted and then cracked using various techniques.

Another method is using malware that searches for and transmits saved passwords from a user's browser or password management software.

Attackers can gain physical access to a person's workspace and look for sticky notes with passwords or access an unattended computer where a user might have stayed logged in to sensitive accounts. These are rudimentary but sometimes highly effective means of stealing passwords.

Keylogging & Manual Guessing

Keylogging involves recording the keystrokes on a user's keyboard without their knowledge. Attackers can install keylogging software on a victim's computer through phishing emails or malicious downloads. Once installed, everything typed, including passwords, is logged and sent to the attacker. For instance, if a user types their banking details to log in to an online account, a keylogger can capture this information, allowing the attacker to access their financial services.

Manual guessing, on the other hand, relies on the attacker's ability to guess passwords based on user information. Common passwords like "123456," "password," or "admin" are often tried first. Attackers might also make educated guesses based on personal information publicly available or obtained through social engineering, such as using a pet's name, birthdate, or favorite sports team – details often shared on social media profiles.

Social Engineering

Social engineering manipulates individuals into divulging confidential information, such as passwords. A classic example is phishing, where attackers pose as a trustworthy entity in an electronic communication. For instance, users may receive an email that looks like it's from their bank, asking them to confirm their login details on a fake website that captures their credentials.

Another example is pretexting, where an attacker fabricates a scenario to compel a victim to release information. They might call an employee posing as IT support, claiming they need the employee's login details to resolve a non-existent issue. Through persuasive storytelling and exploiting trust, attackers using social engineering can bypass even the most sophisticated technical safeguards.

Shoulder Surfing

Shoulder surfing is the practice of directly observing someone entering a password. This can happen in any public place where individuals log into devices, like typing a PIN at an ATM or entering a password on a laptop in a coffee shop.

An attacker might simply glance over the user's shoulder or use more discrete methods, such as using binoculars or a hidden camera positioned to view a keyboard or screen.

In a work environment, shoulder surfing could occur when an employee enters login credentials while a visitor or another employee covertly watches. The simplicity of this technique makes it particularly insidious, as it requires no technical knowledge or tools – just an opportunistic observer in the right place at the right time.

Tips to enhance your security against password-cracking techniques

HACKER COMBAT COMMUNITY

- **Use Strong, Unique Passwords:** Create passwords that are long, complex, and use a mix of letters, numbers, and special characters. Avoid common words or phrases, and never reuse passwords across different accounts.

- **Enable Multi-Factor Authentication (MFA):** Add an extra layer of security by requiring a second form of authentication, such as a code sent to your phone or a fingerprint scan, in addition to your password.

- **Regularly Update Passwords:** Change your passwords periodically and immediately if you suspect they have been compromised.

- **Beware of Phishing Attempts:** Be cautious when clicking on links or downloading attachments from unknown sources. Verify the authenticity of emails or messages that request your login information.

- **Use Encrypted Connections:** Ensure that the websites you visit use HTTPS, especially when entering sensitive information. Avoid using public Wi-Fi for transactions or use a VPN to secure your connection.

- **Install Security Software:** Use antivirus and anti-malware software to protect your devices from keylogging and other malicious software.

- **Be Mindful of Shoulder Surfing:** Shield your keyboard when typing passwords in public places, and be aware of your surroundings.

- **Educate Yourself and Others:** Stay informed about the latest cybersecurity threats and best practices. Educate employees or family members about the importance of password security and how to recognize social engineering tactics.

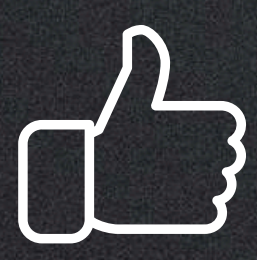
- **Adopt Passwordless Authentication:** Consider using passwordless authentication methods, such as biometrics (fingerprint or facial recognition), security keys, or mobile device authentication. These methods can provide a more secure and user-friendly alternative to traditional passwords.

- **Monitor Account Activity:** Regularly check your accounts for any unusual activity and set up alerts for suspicious actions.

HACKER COMBAT
COMMUNITY

Hackercombat.com

Was it helpful?


Like


Comment


Share


Save