Password Attack Definition

Password attacks involve exploiting a broken authorization vulnerability in the system combined with automatic password attack tools that speed up the guessing and cracking passwords. The attacker uses various techniques to access the system and steal confidential data. The username-password combination is one best known account authentication techniques, so adversaries have had time to craft multiple methods of obtaining guessable passwords.

Types of Password Attacks

Hackers typically rely on different techniques to obtain and authenticate with a legitimate user's password. These include:

Phishing Attacks

By far the most common form of password attack, a phishing attack involves a social engineering technique in which the hacker masquerades as a trusted site by sending the victim a malicious link. After assuming they are authenticating to a legitimate web server, the victim clicks on this link, providing the attacker with their account credentials.

Brute-Force Password Attacks

This type of password attack employs **trial-and-error** methods to guess a user's authentication information. The bad actor uses automated scripts to work through as many permutations as possible to guess the user's password correctly.

Dictionary Password Attacks

This attack method uses a **predefined list of words** most likely to be used as passwords by a specific target network. The predefined list is built from a website user's behavioral patterns and passwords obtained from previous data breaches. The lists are created by varying common combinations of words by case, adding numeric suffixes & prefixes, and using common phrases. These lists are passed to

an automated tool, which attempts to authenticate against a list of known usernames.

Password Spraying Attack

n this attack, the hacker attempts to authenticate using the same password on various accounts before moving to another password. Password spraying is most effective since most website users set simple passwords, and the technique doe not violate lockout policies since it uses several different accounts. Attackers mostly orchestrate password spraying in websites where administrators set a standard default password for new users and unregistered accounts.

Keylogging

While orchestrating a Keylogging attack, a hacker installs monitoring tools in the user’s computer to record the keys struck by the user covertly. A keylogger records all information that users type into input forms and then sends it to the malicious third party

Please check Exercise 001 for Password Attack.

Useful Link
https://www.open-systems.com/password-attack