The Best 12 Password-Cracking Procedures utilized by Programmers PART 1

Some of the most common, and most effective, methods for stealing passwords : PART 1

Harsh Patel 1 day ago · 3 min read

1. Phishing :

Phishing is a type of social engineering **attack** often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft. Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event. In this latter scenario, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data.

2. Social engineering :

Social engineering is the art of exploiting human psychology, rather than technical hacking techniques, to gain access to buildings, systems or data.

For example, instead of trying to find a software vulnerability, a social engineer might call an employee and pose as an IT support person, trying to trick the employee into divulging his password.

Famous hacker Kevin Mitnick helped popularize the term ‘social engineering’ in the ’90s, although the idea and many of the techniques have been around as long as there have been scam artists.

3. Malware :

Malware is the collective name for a number of malicious software variants, including viruses, ransomware and spyware. Shorthand for malicious software, malware typically consists of code developed by cyberattackers, designed to cause extensive damage to data and systems or to gain unauthorized access to a network. Malware is typically delivered in the form of a link or file over email and requires the user to click on the link or open the file to execute the malware.

Malware has actually been a threat to individuals and organizations since the early 1970s when the Creeper virus first appeared. Since then, the world has been under attack from hundreds of thousands of different malware variants, all with the intent of causing the most disruption and damage as possible.

4. Brute force attack :

A **brute force** attack uses trial-and-error to guess login info, encryption keys, or find a hidden web page. Hackers work through all possible combinations hoping to guess correctly.

These attacks are done by 'brute force' meaning they use excessive forceful attempts to try and 'force' their way into your private account(s).

This is an old attack method, but it's still effective and popular with hackers. Because depending on the length and complexity of the password, cracking it can take anywhere from a few seconds to many years.

Here's how hackers benefit from brute force attacks:

- > Profiting from ads or collecting activity data
- > Stealing personal data and valuables
- > Spreading malware to cause disruptions
- > Hijacking your system for malicious activity
- > Ruining a website's reputation
- Profiting from ads or collecting activity data.
  Hackers can exploit a website alongside others to earn advertising commissions. Popular ways to do this include:
- > Putting spam ads on a well-traveled site to make money each time an ad is clicked or viewed by visitors.
- > Rerouting a website's traffic to commissioned ad sites.
- > Infecting a site or its visitors with activity-tracking malware — commonly spyware. Data is sold to advertisers without your consent to help them improve their marketing.

Thankyou for Read :)

Cybersecurity Phishing Security Infosec Hjpatel