Ákos Lévárdy
ID:121314

Slovak University of Technology in Bratislava

Faculty of Informatics and Information Technologies in Bratislava

Principles of information security

Project specification

Ákos Lévárdy
ID:121314

Topic of the project:

Freely distributed password cracking tools

In my topic I will be focused on freely distributed password cracking tools. Firstly, I will describe how passwords are encrypted or hashed. Passwords are used everywhere for user authentication, which a widely adopted method due to its intuitive logic and ease of implementation for developers. Despite their popularity, passwords pose security risks as password crackers are crafted to extract credentials from compromised data obtained through breaches or hacks.

What is password cracking?

Most password-based authentication systems do not store a user's actual password. Instead, they store a password hash, which is the result of sending the password and a random value called a salt through a hash function.

I will compare different hash functions and describe how they work when in use. Basically, hash functions are designed to be one way. This means that it is very difficult to get the original password from the hashed output. It is important to know that hash functions are producing the same output for the same input. Comparing two hashes of a password is eventually the same as comparing two real passwords.

Password cracking tools:

There are many different tools for password cracking. The most popular ones are:

- **Hashcat**
- **John the Ripper**
- **Brutus**
- **Wfuzz**
- **THC Hydra**
- **Meduza**
- **RainbowCrack**
- **OphCrack**
- **L0phtCrack**
- **Aircrack-ng**

I will be comparing two of these password cracking tools – **Hashcat** and **John the Ripper**, analyze them, see how they work and then compare their performance.

Types of attacks on passwords:

There are various types of attacks on passwords, and they can be categorized into different methods based on their techniques.

Most common types of password attacks:

- **Brute Force Attack**
- **Dictionary Attack**
- **Rainbow Table Attack**
- **Phishing**
- **Keylogging**
- **Man-in-the-Middle (MitM) Attack**
- **Shoulder Surfing**

Ákos Lévárdy
ID:121314

Brute Force Attack - This involves trying all possible combinations of passwords until the correct one is found.

Dictionary Attack - Attackers use a predefined list of common words, dictionaries to try and guess the password.

Rainbow Table Attack - A precomputed table containing the hash values of commonly used passwords. This attack compares these hashes with the target system's stored password hashes to find a match.

Phishing – This attack tries to trick individuals into revealing their passwords by posing as a trustworthy entity.

Keylogging - Malicious software or hardware records keystrokes without the user noticing it and capturing sensitive information such as usernames and passwords.

Man-in-the-Middle (MitM) Attack - Intercepting communication between two sides to capture information, including passwords and usernames.

Shoulder Surfing - Observing someone entering their password without their knowledge.

Progress report 1

For the first progress report I will analyse the different hashing algorithms and compare the types of attacks on passwords. I will write about the history of some tools for password cracking and about how to defend our passwords with password managers and other tools.

Progress report 2

For the second progress report I will test two password cracking tools and then compare how they work and their performance. I will use John the Ripper and Hashcat on Kali Linux after I set up a Virtual box for it.

List of basic sources used:

10 most popular password cracking tools [updated 2020]

https://resources.infosecinstitute.com/topics/hacking/10-popular-password-cracking-tools/

What is password hashing?

https://stytch.com/blog/what-is-password-hashing/

What is password encryption?

https://nordvpn.com/blog/what-is-password-encryption/