Task 4: Password Security & Authentication Analysis

Tools Used: Kali Linux, John the Ripper, Hash Identifier

Introduction

Passwords are the most commonly used authentication mechanism in digital systems. Despite their widespread usage, weak password practices remain one of the leading causes of security breaches. This report analyzes how passwords are stored, how attackers exploit weak passwords, and how strong authentication mechanisms can improve security.

Password Storage and Hashing

Modern systems do not store passwords in plain text. Instead, passwords are stored as cryptographic hashes. Hashing is a one-way mathematical process that converts a password into a fixed-length value. Common hashing algorithms include MD5, SHA-1, and bcrypt. Older algorithms such as MD5 and SHA-1 are considered insecure due to their speed and vulnerability to attacks.

Hashing vs Encryption

Hashing and encryption serve different purposes in cyber security. Hashing is irreversible and is used to securely store passwords. Encryption, on the other hand, is reversible and is used to protect data during storage or transmission. Secure authentication systems rely on hashing rather than encryption for password protection.

Password Cracking Techniques

Password cracking involves recovering the original password from its hash. Dictionary attacks use lists of commonly used passwords to crack weak hashes quickly, while brute force attacks attempt every possible character combination. Tools such as John the Ripper automate dictionary-based attacks and demonstrate how weak passwords can be compromised within seconds.

Why Weak Passwords Fail

Weak passwords fail due to predictable patterns, short length, and reuse across multiple platforms. Passwords like 'password123' or 'admin' are included in most wordlists, making them easy targets for attackers. Lack of complexity significantly increases the risk of compromise.

Multi-Factor Authentication (MFA)

Multi-Factor Authentication adds an additional layer of security by requiring more than one form of verification. Even if a password is compromised, MFA prevents unauthorized access by requiring additional authentication factors such as one-time passwords or biometrics.

Conclusion

This task highlights the importance of strong password practices and modern authentication defenses. Understanding password hashing, cracking techniques, and the role of MFA helps improve overall security and reduces the risk of unauthorized access.

Author: Mohammed Nihal