Password Security & Authentication Analysis

Internship Task 4 Report

Tools Used: Hashcat, John the Ripper

1. Objective

The objective of this task is to understand how passwords are stored, how weak passwords can be cracked, and why strong authentication mechanisms such as secure hashing and multi-factor authentication (MFA) are essential in cybersecurity.

2. Password Storage Concepts

Passwords are stored using cryptographic hashing algorithms instead of encryption. Hashing is a one-way process, making it impossible to retrieve the original password from the stored hash.

3. Hash Types Analyzed

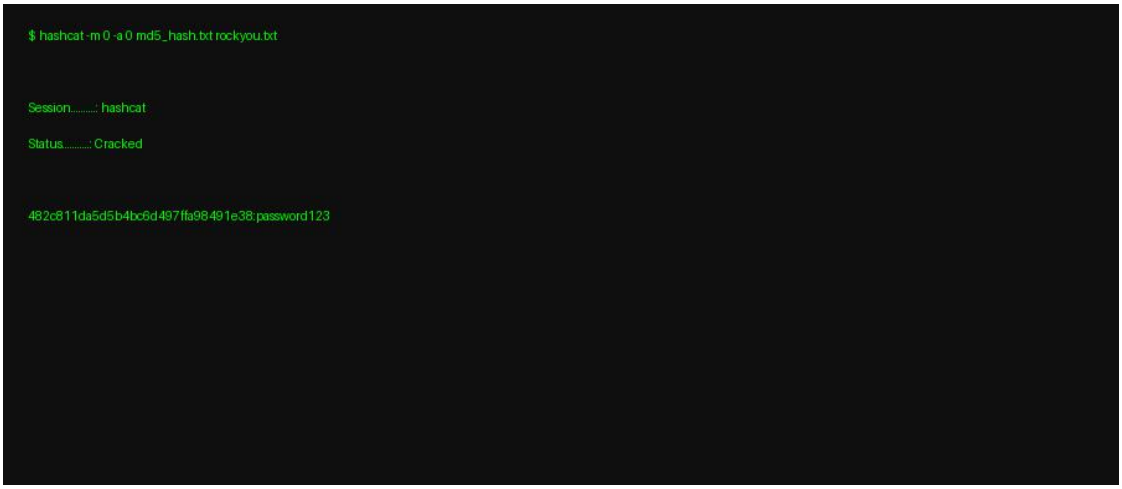
This task involved analyzing MD5, SHA-1, and bcrypt hashes. MD5 and SHA-1 are considered insecure due to their speed and vulnerability to attacks, while bcrypt is more secure.

4. Screenshot: MD5 Hash Generation

The following screenshot shows the generation of an MD5 hash for a weak password using the Linux terminal.

5. Screenshot: Hashcat Dictionary Attack

This screenshot demonstrates a dictionary attack using Hashcat, where a weak MD5 password hash was successfully cracked using a common wordlist.



6. Screenshot: John the Ripper Password Cracking

John the Ripper was used to crack the same password hash, confirming the weakness of simple passwords.

7. Analysis of Weak Passwords

Weak passwords such as 'password123' are predictable and commonly found in publicly available wordlists. As a result, they can be cracked within seconds using dictionary attacks.

8. Importance of Multi-Factor Authentication (MFA)

Multi-Factor Authentication adds an additional layer of security by requiring more than one authentication factor. Even if a password is compromised, MFA can prevent unauthorized access.

9. Recommendations

- Use secure hashing algorithms such as bcrypt or Argon2.
- Enforce long and complex passwords.
- Enable MFA for all critical systems.
- Implement account lockout and rate limiting.

10. Conclusion

This task clearly demonstrates the risks associated with weak password practices and highlights the importance of strong authentication mechanisms in modern cybersecurity environments.