IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 7, April 2025

Impact Factor: 7.67

Non-Hashed Passwords Cracking

Chakradhar Mhaske, Rohit Khade, Piyush Bhojane, Prof. Harihar

Navsahyadri Education Society's Group of Institutions, Polytechnic, Pune, Maharashtra, India

Abstract: *In the realm of cybersecurity, password protection plays a vital role in securing digital assets and personal data. While hashing is a widely accepted standard for storing passwords securely, many systems—due to poor design, legacy support, or misconfiguration—still store passwords in plaintext or reversible formats. This paper investigates the vulnerabilities and exploitation techniques associated with non-hashed (plaintext or symmetrically encrypted) password storage. We explore common scenarios where non-hashed passwords are exposed, analyze methods for retrieving them through system breaches, memory scraping, and forensic analysis, and demonstrate real-world case studies where such practices led to significant data breaches. The study also highlights the ease with which attackers can leverage these weaknesses using basic tools and scripting, emphasizing the critical need for secure password management practices. Recommendations are provided for detecting insecure storage methods and enforcing industry-standard hashing protocols to mitigate risks and enhance overall security posture. Non-hashed passwords stored in systems pose significant security risks, making them vulnerable to brute force and dictionary attacks. The objective of this project is to demonstrate and understand these vulnerabilities and how to effectively crack such passwords*

Keywords: cybersecurity

DOI: 10.48175/IJARSCT-25471