Topic 3 Discussion 2

Research the John the Ripper password-cracking tool used in Linux. How might this tool be used to bypass single-factor security methodologies? Considering NIST SP 800-63b changed our thinking on passwords, what are some current password requirements you would implement within a new organization to safeguard against such tools? Provide an example.

Hello Class,

John the Ripper is a powerful password-cracking tool commonly used in Linux systems. It is known for its ability to test and bypass single-factor security methodologies by attempting to crack passwords through various methods like brute-force attacks and dictionary attacks.

Testing Password Strength -  John the Ripper can test the strength of passwords by attempting to crack them using different techniques.

Brute-Force Attacks - It can perform brute-force attacks to systematically try all possible combinations until the correct password is found.

Dictionary Attacks - The tool can also use pre-existing wordlists to crack passwords based on common words or phrases.

Considering the advancements in password security outlined in NIST SP 800-63b, here are some current password requirements that can help safeguard against tools like John the Ripper:

Require the use of MFA to add an extra layer of security beyond passwords.

Enforce complex password policies that include a mix of uppercase and lowercase letters, numbers, and special characters.

Implement regular password changes to reduce the risk of long-term exposure to password-cracking tools.

Set minimum password length requirements to ensure passwords are not easily cracked.

Maintain a list of commonly used or compromised passwords to prevent their use within the organization.

For example, in a new organization, you could implement the following password policy:

Password Length - Require passwords to be at least 12 characters long.

Complexity - Mandate the use of at least one uppercase letter, one lowercase letter, one number, and one special character.

Regular Changes - Enforce password changes every 90 days to enhance security.

MFA - Enable multi-factor authentication for all user accounts to add an extra layer of protection.

By implementing these password requirements, organizations can strengthen their security posture and mitigate the risks associated with password-cracking tools like John the Ripper.

References:

*Chapter 4. Hardening Your System with Tools and Services | Red Hat Product Documentation*. (n.d.). Docs.redhat.com. https://docs.redhat.com/en/documentation/red\_hat\_enterprise\_linux/7/html/security\_guide/chap-hardening\_your\_system\_with\_tools\_and\_services

Openwall. (2019). *John the Ripper password cracker*. Openwall. https://www.openwall.com/john/

TechMindXperts. (2023, May 9). *John the Ripper: A Comprehensive Guide to Password Cracking*. Medium. https://medium.com/@techmindxperts/john-the-ripper-a-comprehensive-guide-to-password-cracking-9335f44ed3f5