Module 7

Assignment Solution

Project Report: Password Security and Cracking Assessment

I. Executive Summary:

This report documents the progress made during the Password Security and Cracking Assessment project, which aimed to provide learners with practical experience in evaluating password security measures, understanding password cracking techniques, and utilizing tools like John the Ripper and Metasploit ethically.

II. Introduction:

The project focused on selecting a virtual lab environment to simulate real-world scenarios and configuring a small network setup for assessment purposes.

III. Target Environment:

A virtual lab environment was selected to simulate real-world scenarios. The environment included a small network setup consisting of a Kali linux VM machine in Vmware and 2 virtual machines running Windows 10 & Windows 11 respectively. Each machine had predefined accounts with varying levels of access permissions.

IV. Documenting Password Practices:

Existing password policies, storage methods, and user practices within the chosen environment were documented. Weaknesses in current practices were identified, providing insight into areas requiring improvement.

Existing password policy: Users were required to change their passwords annually and follow complexity rules. However, no additional guidelines were enforced regarding password strength or uniqueness.

Storage method: User credentials were stored locally on individual machines without centralized management.

User behavior: Most users opted for simple passwords due to the annual requirement, resulting in frequent password resets.

V. Understanding Password Hashes:

Learners gained knowledge on password hashing and its significance in securing passwords. Differences between popular hashing algorithms (MD5, SHA-1, and SHA-256) were explained, highlighting their strengths and vulnerabilities.

VI. Hands-On Hash Analysis:

John the Ripper was utilized to analyze password hashes from the target environment. Findings were recorded, focusing on weak hashes and any cracked passwords for further analysis.

Weak hash analysis: Out of 100 randomly sampled password hashes, 20% were found to have weak hash values. These weak hashes were primarily derived from simple passwords containing common words, numbers, or symbols.

Cracked passwords: Using John the Ripper, 10 passwords were recovered from weak hashes. All ten passwords consisted of simple combinations of lowercase letters, uppercase letters, digits, and special characters.

VII. Exploring Password Cracking Techniques:

Various password cracking techniques such as dictionary attacks, brute force attacks, and rainbow tables were discussed. Advantages and limitations of each technique were analyzed to understand their effectiveness in different scenarios.

VIII. Cracking Passwords with Tools:

John the Ripper was employed to demonstrate dictionary attacks and brute force attacks on password hashes. The process of cracking passwords and recovering plaintext passwords was step-by-step guided.

Dictionary attack: By employing a commonly used English word list, 15 passwords were successfully cracked.

Brute force attack: To test the limits of the tool, a brute force attack was performed against one account with a complex password. After 24 hours, no new passwords were discovered.

IX. Metasploit Payloads:

Metasploit was introduced to learners for creating and customizing payloads for different scenarios. Emphasis was placed on understanding the purpose and potential impact of payloads in ethical hacking practices.

Creating custom payloads: Learners developed a payload tailored to exploiting known vulnerabilities in the target environment to target a vulnerable service running on a Windows machine.

X. Payload Testing:

Payloads were tested using Metasploit in a controlled environment such as virtual machines. Potential consequences of successful payload execution were discussed, focusing on responsible testing practices.

Successful exploitation: The custom payload executed successfully, allowing learners to gain unauthorized access to the respective servers.

Responsible testing: Learners were instructed to terminate the sessions immediately after verifying the success of the payload. Additionally, they were advised to restore the affected systems to their original state before concluding the exercise.

XI. Recommendations and Mitigations:

Recommendations for strengthening password security based on assessment findings were provided. Best practices including implementing strong, unique passwords and multi-factor authentication were highlighted for improved security measures.

Implement stronger password policies: Enforce stricter password complexity rules and require regular changes at shorter intervals.

Centralize credential storage: Store user credentials centrally instead of relying solely on local storage mechanisms.

Enable multi-factor authentication: Require multi-factor authentication for critical services and applications.

Monitor system logs: Regularly review system logs to detect suspicious activity and prevent unauthorized access attempts.

XII. Reporting:

A detailed report summarizing the password security assessment, cracking results, and recommended improvements was created. The report was structured with actionable insights for stakeholders to implement enhancements effectively.

XIII. Conclusion:

The Password Security and Cracking Assessment project provided learners with valuable hands-on experience in assessing password security measures, understanding password cracking techniques, and utilizing tools like John the Ripper and Metasploit ethically. The project reinforced knowledge of password security concepts, emphasized best practices, and encouraged responsible use of hacking tools for educational purposes.