Module 4 : Password Security & Breach Analysis Lab

Introduction

In this lab, you will learn how Unix-like systems store passwords and how attackers use dictionary and brute-force methods to crack them. You will examine `/etc/passwd` and `/etc/shadow` to understand password hashing and salts. You'll use provided tools (`crackSHA` , `crackMD5` , `crack512` , `crackPre`) to perform dictionary attacks on sample password files. Finally, you'll compare the speed of different hash algorithms (MD5, SHA-1, SHA-512) and experiment with creating and cracking your own password entries.

Key Concepts

- **Dictionary Attack**: Tries words from a list of likely passwords.
- **Brute-Force Attack**: Tries every possible combination.
- **Salts**: Random data added to passwords before hashing to make each hash unique.

Accessing the Lab Environment

1. **Log in to Labtainer**
   Navigate to:

   `https://<student-name>.lahilabs.com/`

   Replace `<student-name>` with your actual username. Use the credentials provided.
2. **Start the Lab**
   Open a terminal in Labtainer. Start the Password Cracking lab:

   `labtainer pass-crack`

   This will display paths to the lab manual and report template.

   Important:
   - Do not click GUI links for the manual or report.
   - Follow only this guide's instructions in the terminal.

Task 1: Examining Password Files

1. **View `/etc/passwd`**

`more /etc/passwd`

Observe the user accounts. No passwords are visible here.

2. **Try Viewing `/etc/shadow`**

   `more /etc/shadow`

   You'll get a "Permission denied" error.
   → **Record this error message in item #1 of the worksheet.**
3. **View `/etc/shadow` as Root**

   `sudo more /etc/shadow`

   Find the line with your username. It looks like:

   `student:$6$salt$hash:...`
4. **Identify Hash and Salt**

   - `$1$` = MD5
   - `$5$` = SHA-256
   - `$6$` = SHA-512

   → **Record the hash algorithm in item #3 and the salt in item #4 of the worksheet.**
5. **Check Password Age**

   `chage -l $(whoami)`

   → **Record the "Last password change" in item #5. Answer item #6 based on the date.**

Task 2: Dictionary Attacks on Sample Files

1. **Inspect the SHA-1 Password File**

   `cat htpasswd-sha1`

   Look for duplicate hashes.
   → **Record usernames that share a password in item #7.**
2. **Run Dictionary Attack with Tiny List**

   `./crackSHA htpasswd-sha1 tinylist`

   → **Record cracked accounts in item #8.**
3. **Run Dictionary Attack with Big List**

   `./crackSHA htpasswd-sha1 biglist`

- Observe the number of guesses, matches, and total time.
  → **Fill in items #9 and #10. Answer item #11 based on these results.**

Task 3: Comparing Hashing Speeds

1. **MD5 Attack**

   ```
   ./crackMD5 htpasswd-md5 biglist
   ```

   → **Record the results in item #12. Answer #13 and #14 based on your findings.**
2. **SHA-512 Attack**

   ```
   ./crack512 htpasswd-sha512 biglist
   ```

   → **Record the results in item #15. Answer #16 accordingly.**
3. **Brute-Force Time Estimation**
   Use the spreadsheet provided in the lab to estimate:

   - Time to brute-force a 15-character password
   - Time at 10 billion guesses/second

   → **Answer item #17.**

Task 4: Personal Password Experimentation

1. **Create a Custom Password File**

   ```
   htpasswd -sc htpasswd-me alice
   ```

   Then optionally add another user:

   ```
   htpasswd -s htpasswd-me bob
   ```
2. **View Your File**

   ```
   cat htpasswd-me
   ```
3. **Crack Your Own Passwords Using Precomputed Hashes**

   ```
   ./crackPre htpasswd-me calc
   ```

   → **Record your results in items #18 and #19.**

Completing the Lab

- Answer **all worksheet questions**.
- Submit the completed worksheet and your `htpasswd-me` file.
- When done, stop the lab:

  ```
  stoplab
  ```
