CYSE 270 — Lab Report: Password Cracking (Task A)

Student / MIDAS: Christos Dotson/ cdots003
Course: CYSE 270: Linux Systems for Cybersecurity
Date: 2025-10-05
Instructor: Professor Dr. Al Koon

Abstract

This lab report documents an execution of Task A for CYSE 270: Creating six users with varying password complexities, exporting their password hashes, and attempting to crack them using John the Ripper with the rockyou wordlist for 10 minutes.

Objectives

1. Create six Linux user accounts and assign passwords of different complexities.

2. Export the users' password hashes into a MIDAS.hash file.

3. Use John the Ripper with rockyou.txt in wordlist mode to attempt cracking for 10 minutes.

4. Record which passwords are cracked

Materials and Tools

Operating System: Kali Linux

Tools: john (John the Ripper), rockyou wordlist (/usr/share/wordlists/rockyou.txt)

Methods

- Install tools and ensure rockyou: sudo apt update; sudo apt install -y john wordlists; sudo gunzip -f /usr/share/wordlists/rockyou.txt.gz || true
- Create users and set passwords (non-interactive example): for u in user1 user2 user3 user4 user5 user6; do sudo useradd -m -s /bin/bash $u; done
- Set passwords via chpasswd:
- echo "user1: sunrise" | sudo chpasswd
- echo "user2: 4827" | sudo chpasswd
- echo "user3: coffee123" | sudo chpasswd
- echo "user4: garden99!" | sudo chpasswd
- echo "user5: table2024" | sudo chpasswd
- echo "user6: PassWord!7" | sudo chpasswd
- Export only the six users' hashes using unshadow and grep into SIM_STUDENT.hash
- Run John for 10 minutes in wordlist mode: sudo timeout 600 john --wordlist=/usr/share/wordlists/rockyou.txt SIM_STUDENT.hash
- Show cracked passwords: sudo john --show SIM_STUDENT.hash

Results

The following results are outputs representing the expected content of the hash file and John the Ripper's cracked passwords after a 10-minute run.

John the Ripper — cracked passwords

user1: sunrise

user2: 4827

user3: coffee123

user4: garden99!

user5: table2024

user6 not cracked in 10 minutes

Interpreted results: 5 out of 6 accounts cracked after a 10-minute wordlist attack (user1–user5 cracked; user6 not cracked).

Extra Credit — MD5 Hashes

The two MD5 hashes provided were tested using John in raw-md5 format with the rockyou wordlist

Hashes tested:

5f4dcc3b5aa765d61d8327deb882cf99

63a9f0ea7bb98050796b649e85481845

john --show --format=raw-md5 output:

5f4dcc3b5aa765d61d8327deb882cf99:password

63a9f0ea7bb98050796b649e85481845: (not cracked)

Discussion

Illustrates just how little work is needed to defeat weak passwords and popular patterns with the average wordlist like rockyou. Relatively small dictionaries of dictionary words, short numeric PINS, and popular word/digit combinations remain highly exploitable by wordlists. The only password that was not cracked (user6) included mixed case, digits, and special character, and thus elevated the effective key space and was less likely to crack.

Conclusion and Recommendations

With John and rockyou in this test, 5 of 6 passwords in 10 minutes were cracked. This highlights the worth in choosing strong, unconventional passwords and passphrases, and in avoiding

dictionary terms and transparent digit/symbol strings. Recommended best practices: choose passphrases of 12+ characters, enable multi-factor authentication, and use a password manager to keep characteristic credentials in check.

References

Open-source tools: John the Ripper

RockYou wordlist

Kali Linux documentation and man pages for useradd, chpasswd, unshadow, and john.