**PART A**

**EXPERIMENT NO. 7**

**A.1 AIM: -** To implement Dictionary Attacks on Passwords

**A.2 Prerequisite: -** Basic Knowledge of Dictionary Attacks

**A.3 Outcome**

After successful completion of this experiment students will be able to

1. Understand the concepts of dictionary attacks
2. Implement John the Ripper password cracking tool to implement dictionary attacks

**A.4 Theory**

A dictionary attack is a type of cyber-attack used to crack passwords or gain unauthorized access to computer systems. It involves systematically trying a list of words from a dictionary or wordlist, along with various combinations, to guess the correct password. Dictionary attacks are based on the assumption that many users use common and easily guessable passwords.

Working of Dictionary Attacks:

Wordlist Compilation: Attackers compile a list of commonly used words, phrases, and terms, as well as variations and combinations of these words. This list is known as a "dictionary" or "wordlist."

Password Guessing: The attacker then systematically tries each word in the dictionary and its variations as potential passwords. This includes trying words in uppercase, lowercase, with numbers, and with special characters.

Comparison: The attacker's tool compares each guessed password against the target system's password hashes (encrypted representations of passwords stored in the system's database).

Match Identification: If the guessed password's hash matches the hash stored in the system, the attacker has successfully cracked the password.

Unauthorized Access: With the cracked password, the attacker can gain unauthorized access to the target system, application, or user account.

John the Ripper is a popular and powerful open-source password cracking tool that can be used for various types of password attacks, including dictionary attacks. It supports a wide range of algorithms and hash types, making it capable of cracking passwords from various systems and applications. John the Ripper has several modes of operation, including dictionary attacks, brute-force attacks, and hybrid attacks. In the context of dictionary attacks, John the Ripper uses wordlists to systematically attempt to crack password hashes. It supports a variety of wordlist formats and can generate permutations and combinations of words to increase the likelihood of cracking passwords.

It's important to note that dictionary attacks are effective against weak passwords but are less likely to succeed against complex and unique passwords. To protect against dictionary attacks, it's recommended to use strong, unique passwords for different accounts, enable multi-factor authentication (MFA), and keep your software and systems up to date. Additionally, organizations can implement rate-limiting mechanisms to prevent multiple login attempts within a short period, which can thwart automated password cracking attempts.

**A.5 Procedure/Algorithm:**

**Task 1**

1. Create a new user

Sudo adduser (username)

Check if user is created by switch user

Su username

Exit from the new user login

Exit

1. Get the hash of the new user login password

cd /etc

Sudo cat shadow

Copy the hash and save it on desktop in a txt file

nano hash.txt

1. Crack the password

sudo john -format = crypt -- wordlist = /usr/share/wordlists/rockyou.txt hash.txt

If rockyou is zip file then unzip it using following commands:

Sudo gunzip [rockyou.txt.gz](http://rockyou.txt.gz)

**TASK 2**

1. Create a zip file with password

nano secrete.txt

1. Add text and save the file

Zip -e secrete.zip secrete.txt

1. Create a hash of the zip file

Zip2john secrete.zip > zip\_hash.txt

1. sudo john –wordlist = password.txt zip\_hash.txt

<https://youtu.be/piNkLNqDto4?si=6sJwE0NlJDNkJvni>

**TASK 3:**

Demonstrate password cracking in the lab environment using tools like hydra and

hashcat.

**Online Dictionary Attack using hydra**

1. Start kali linux and login.

2. Start SeedUbuntu VM and login

3. Scan SeedUbuntu VM using nmap (nmap 10.0.2.4). you will find that port 21,22 and 23

are open. We will attacker port 22

4. Go to Application Password Attacks Hydra-gtk

5. Set the target IP to 10.0.2.4 (IP of SeedUbuntu), port =22 and protocol to ssh. Also select

Show attempts and Debug options.

6. Create a file (user.txt) with common username like admin, administrator, user and seed.

7. Create another file(pass.txt) with common password like 123456, password, passw0rd,

p@ssword, pass@123, dees.

8. Click on password tab. Select username list and upload user.txt

9. Select password list and upload pass.txt.

10. Click on the start tab and start the attack.

11. After successful completion it will show username as seed and password as dees.

**Brute force attack using hydra**

**offline password cracking using hashcat.**

<https://www.youtube.com/watch?v=gjAMD_4aV4E>

Review question:

1. Explain online and offline attacks?

2. Explain dictionary attacks?

3. Explain brute force attack?

4. Explain password management in windows systems?

5. Explain password management in linux systems?

6. Explain some countermeasures against password cracking?

PART B

(PART B : TO BE COMPLETED BY STUDENTS)

***(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the Portal or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no Portal access available)***

| Roll No. | Name: |
| --- | --- |
| Class : | Batch : |
| Date of Experiment: | Date of Submission |
| Grade : |  |

**B.1 Output of Task1**

1. Screenshot of Task 1
2. Screenshot of Task 2
3. Screenshot of Task 3

**B.2 Observations and Learning**

**B.3 Conclusion:**

*(****Students must write the conclusion as per the attainment of individual outcome listed above and learning/observation noted in section B2. and B.3)***