Experiment No: 8

**Aim:** To Demonstrate on Password Cracking with its Prevention Method.

**Theory:**

Password cracking is the process of guessing or recovering a password from stored locations or from data transmission system. It is used to get a password for unauthorized access or to recover a forgotten password. In penetration testing, it is used to check the security of an application.

Programmers have developed many password cracking tools. Every tool has its own advantages and disadvantages. In this post, we are covering a few of the most popular password cracking tools.

**Passive online**

1. Eavesdropping on network password exchanges.
2. Passive online attacks include sniffing, man-inthe-middle, and replay attacks.

**Active online Guessing** the Administrator password. Active online attacks include automated password guessing.

**Offline Dictionary:** hybrid, and brute-force attacks.

Offline Attacks include Tools like:

1. Rainbowcrack
2. Bkhive
3. CUPP
4. Hashcat
5. John
6. Ophcrack

The purpose of password cracking might be to help a user recover a forgotten password (installing an entirely new password is less of a security risk, but it involves System Administration privileges), to gain unauthorized access to a system, or as a preventive measure by System Administrators to check for easily crackable passwords.

**Time needed for password searches**

The time to crack a password is related to bit strength which is a measure of the password's information entropy, and the details of how the password is stored.

**Easy to remember, hard to guess**

Passwords that are difficult to remember will reduce the security of a system because (a) users might need to write down or electronically store the password, (b) users will need frequent password resets and (c) users are more likely to re-use the same password.

**Assessment Tool used is Hydra**

Hydra is a brute force password cracking tool.

In information security, password cracking is the methodology of guessing passwords from databases that have been stored in or are in transit within a computer system or network.

A common approach, and the approach used by Hydra and many other similar pen testing tools and programs is referred to as Brute Force.

Brute force will take the list that the hacker built and will likely combine it with other known (easy passwords, such as ‘password1, password2′ etc) and begin the attack.

It is not considered as being very subtle – but hey it works!

**Prevention**

1. The best method of preventing a password from being cracked is to ensure that attackers cannot get access even to the hashed password. Many hashes used for storing passwords, such as MD5 and the SHA family, are designed for fast computation Use different passwords for each system.
2. Use variable-length passwords. This trick can throw off attackers because they won’t know the required minimum or maximum length of passwords.
3. Don’t reuse the same password within at least four to five password changes.
4. Use password-protected screen savers. Unlocked screens are a great way for systems to be compromised even if their hard drives are encrypted.
5. Don’t share passwords. To each his or her own!
6. Avoid storing user passwords in an unsecured central location, such as an unprotected spreadsheet on a hard drive.

**Other countermeasures**

1. Enable security auditing to help monitor and track password attacks.
2. Test your applications to make sure they aren’t storing passwords indefinitely in memory.
3. A good tool for this is WinHex.
4. Keep your systems patched.

**Other password-protection countermeasures include**

1. Stronger authentication methods. Examples smart cards, tokens, biometrics, or digital certificates.
2. Automated password reset.
3. This functionality lets users manage most of their password problems without getting others involved.
4. Password-protect the system BIOS.

This is especially important on servers and laptops that are susceptible to physical security threats and vulnerabilities.

**DEAD Analysis**

1. Select Backtrack 5

2. Open Applications >Backtrack >Privilege Escalation >Password Attacks >Offline Attacks

>CUPP and launch the Cupp tool

3. Enter the command to run program in interactive mode.

4. Now fill all the information it ask to you.

5. CUPP wills automatically making a dictionary pentest/passwords/wordlist/file.txt for you

LIVE Analysis

1. Open Applications >Backtrack >Privilege Escalation >Password Attack >Online Attacks

>hydra and launch the hydra tool

2. Now open shell and execute the ssl strip

3. Select the victim username.

4. Select the CUPP text file

5. Port

6. Single target

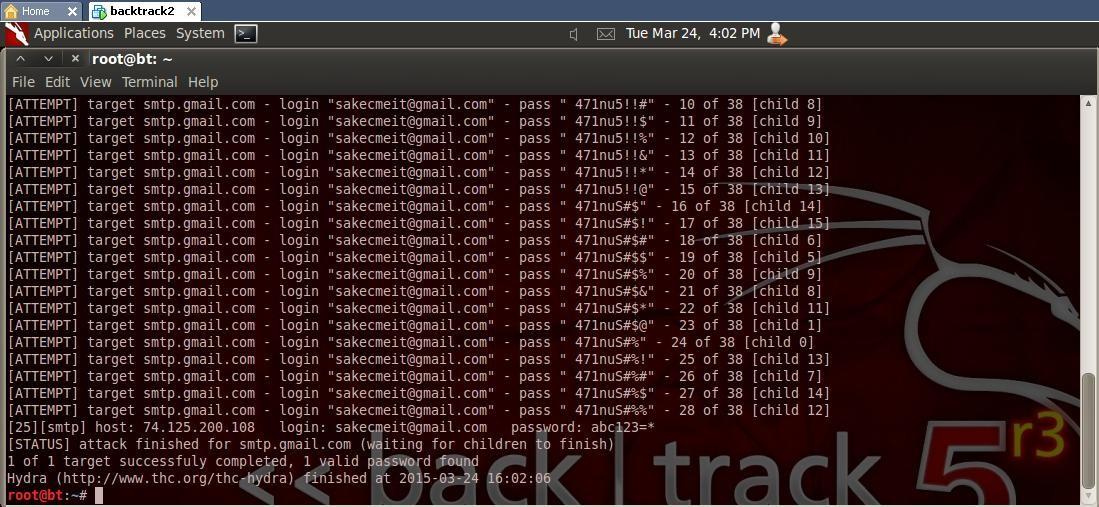
7. Username and password are matched and made visible on the Screen.

8. Wait For Some time .

9. Attack finishes for smtp.gmail.com

10. Target successfully completes

11. Result shows the one valid password



**Conclusion:**

Passwords should not be used on their own for authentication purposes. Instead, we need passwords to be part of multi-factor authentication. Alternatively, we must only use passwords once we have accepted the risks associated and the high probability of them failing us.