Lab Assignment-6(Cracking passwords)

Below are the passwords cracked

1. **abkuma_1**: abkuma:dude

```
Session completed
cadmin@i520-client:~/Desktop$ john --show abkuma_1
abkuma:dude
```

2. **abkuma_2**: abkuma:gandalf92
   Rule:$[0-9]$[0-9]

```
Session completed
cadmin@i520-client:~/Desktop$ john --show abkuma_2
abkuma:gandalf92
```

3. **abkuma_3**: abkuma:nil11cklaus22

   Rule: i2[1-2]i3[1-2]$[1-2]$[1-2]

```
Session completed
root@i520-client:/home/cadmin/Desktop# john --show abkuma_3
abkuma:ni11cklaus22
```

4. **abkuma_4**: abkuma:charters

```
Session completed
root@i520-client:/home/cadmin/Desktop# john --show abkuma_4
abkuma:charters
```

Below are the rules which are applied

```
# Wordlist mode rules
[List.Rules:Wordlist]
# Try words as they are
:
$[0-9]$[0-9]
i2[1-2]i3[1-2]$[1-2]$[1-2]
```

5.1. Explain how a “white hat” security professional might use john-the-ripper to make her institution more secure.

Answer

White hat people are ethical security hackers. They are the good people. They have the license and work for any kind of organization. They try to find some issues present in the system and inform the organization and discuss those issues so that the developer can work on those issues to make them more secure. So white hat people try to test the website by creating different custom rules to test the website in this way find the issues present in that website. In this way, they test the password and crack it using the dictionary attack. This makes the password difficult to crack by the hacker.

5.2. Why can john-the-ripper crack the passwords even though they are not in a form that is directly readable?

Answer

John-the-ripper is a very famous tool used for cracking passwords. It is also used to recover the password from the computer. It recognizes password hash types automatically and offers a customizable cracking of the password. It can decrypt the password. The tools like brute force using dictionary and dictionary attacks.

5.3. Explain how John the Ripper limits/reduces password cracking time?

Answer

John-the-ripper employs the mangling preprocessor, which optimizes wordlists to reduce cracking time. It uses different modes like wordlist mode, external mode, incremental mode, single crack mode. Using this mode makes John-the-ripper make it faster. Incremental mode is stronger and single crack mode is very fast. In this way, it reduces the cracking time.

5.4. What system policies for passwords would make user passwords considerably harder to crack by a password cracker such as john-the- ripper? What are the downsides of enforcing such policies?

Answer

Some of the policies make the password harder to crack. By applying salt mechanism. Encrypting the password using an encryption algorithm. Keeping different rules while creating a hard password like including various kinds of symbols, lower-case, upper-case combination. Also using key stretching in which the hash of the password is stretched. So, all these policies make the password difficult to crack.

5.5. How much does a salt of size N increase the processing required by precomputed dictionary offline attacks?

Answer

Salt is added to the password to make it more secure. The salt is appended to the dictionary which results in a new dictionary thus increasing the complexity to crack the password and increasing the computation time to crack the password. In this way, the salt increases the processing time. The process time is 2^N + Time required to crack the password.