Ethics in IT

Class 9

Lab 2

UNITED TRUST

bdeducation
Bangladesh Digital Education Research Limited
সময়ের পাঠশালা

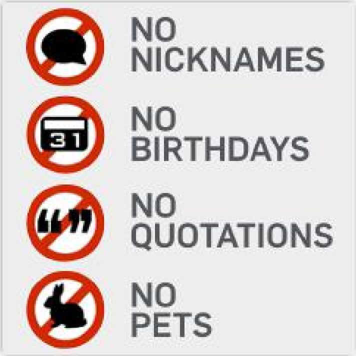
Lab Objectives:

- Password Hacking

Ethical Hacking - Password Hacking

We have passwords for emails, databases, computer systems, servers, bank accounts, and virtually everything that we want to protect. Passwords are in general the keys to get access into a system or an account.

In general, people tend to set passwords that are easy to remember, such as their date of birth, names of family members, mobile numbers, etc. This is what makes the passwords weak and prone to easy hacking.

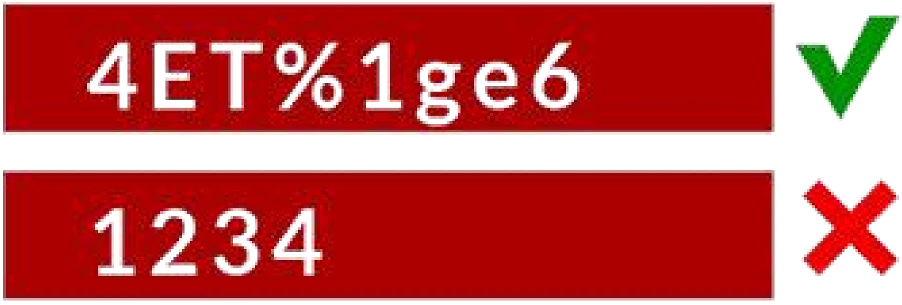


One should always take care to have a strong password to defend their accounts from potential hackers. A strong password has the following attributes −

√ Contains at least 8 characters.

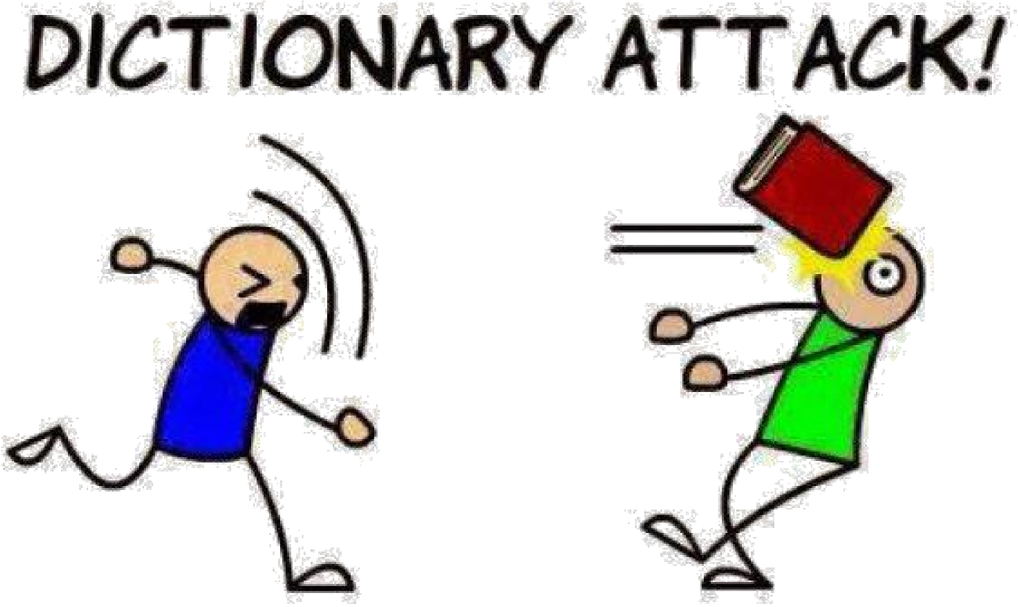
√ A mix of letters, numbers, and special characters.

√ A combination of small and capital letters



Dictionary Attack

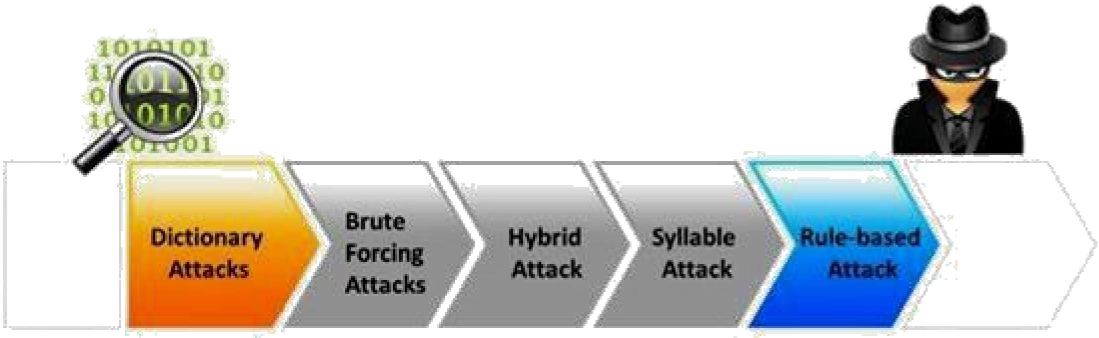
In a dictionary attack, the hacker uses a predefined list of words from a dictionary to try and guess the password. If the set password is weak, then a dictionary attack can decode it quite fast.



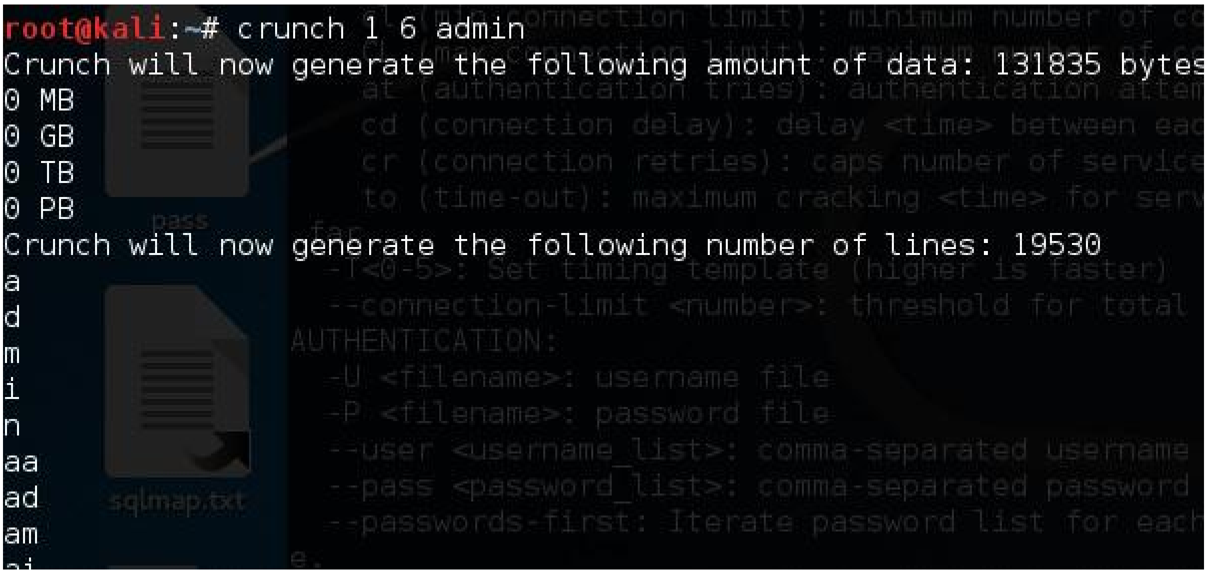
Hydra is a popular tool that is widely used for dictionary attacks. Take a look at the following screenshot and observe how we have used Hydra to find out the password of an FTP service.

Hybrid Dictionary Attack

Hybrid dictionary attack uses a set of dictionary words combined with extensions. For example, we have the word “admin” and combine it with number extensions such as “admin123”, “admin147”, etc.



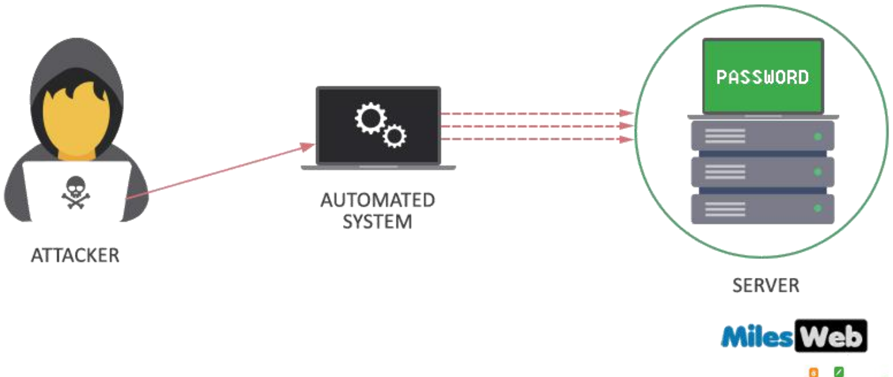
Crunch is a wordlist generator where you can specify a standard character set or a character set. Crunch can generate all possible combinations and permutations. This tool comes bundled with the Kali distribution of Linux.



```
root@kali:~# crunch 1 6 admin
Crunch will now generate the following amount of data: 131835 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 19530
a
d
m
i
n
aa
ad
am
ai
```

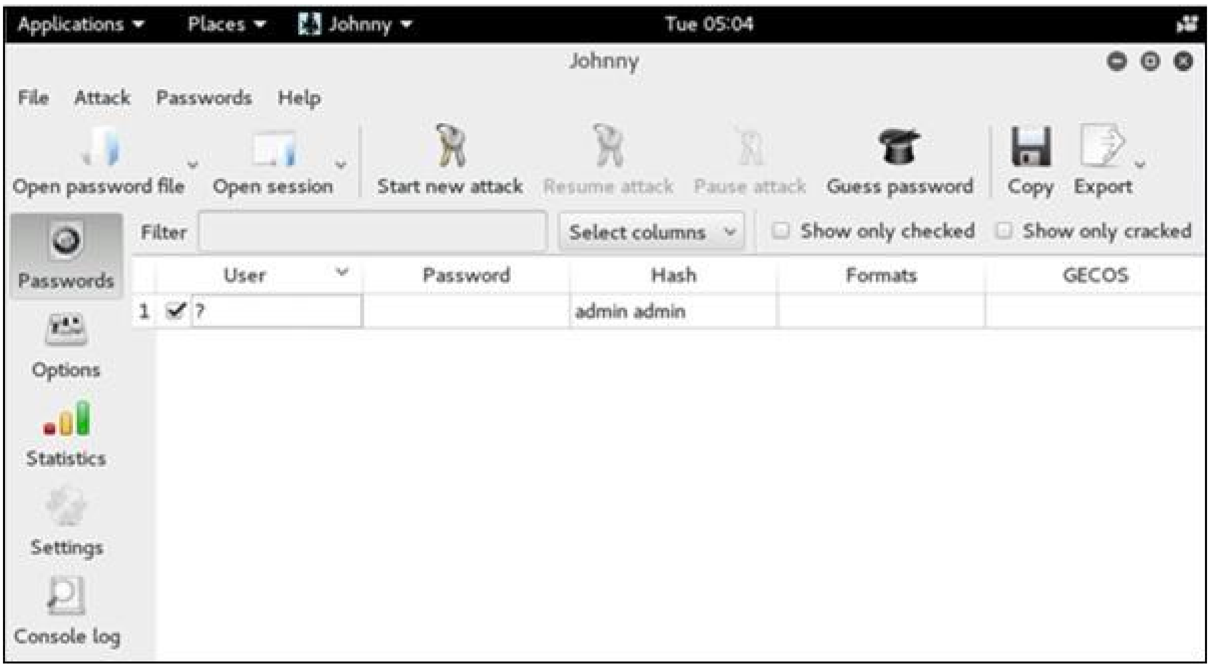
Brute-Force Attack

In a brute-force attack, the hacker uses all possible combinations of letters, numbers, special characters, and small and capital letters to break the password.



This type of attack has a high probability of success, but it requires an enormous amount of time to process all the combinations. A brute-force attack is slow and the hacker might require a system with high processing power to perform all those permutations and combinations faster.

John the Ripper or Johnny is one of the powerful tools to set a brute-force attack and it comes bundled with the Kali distribution of Linux.



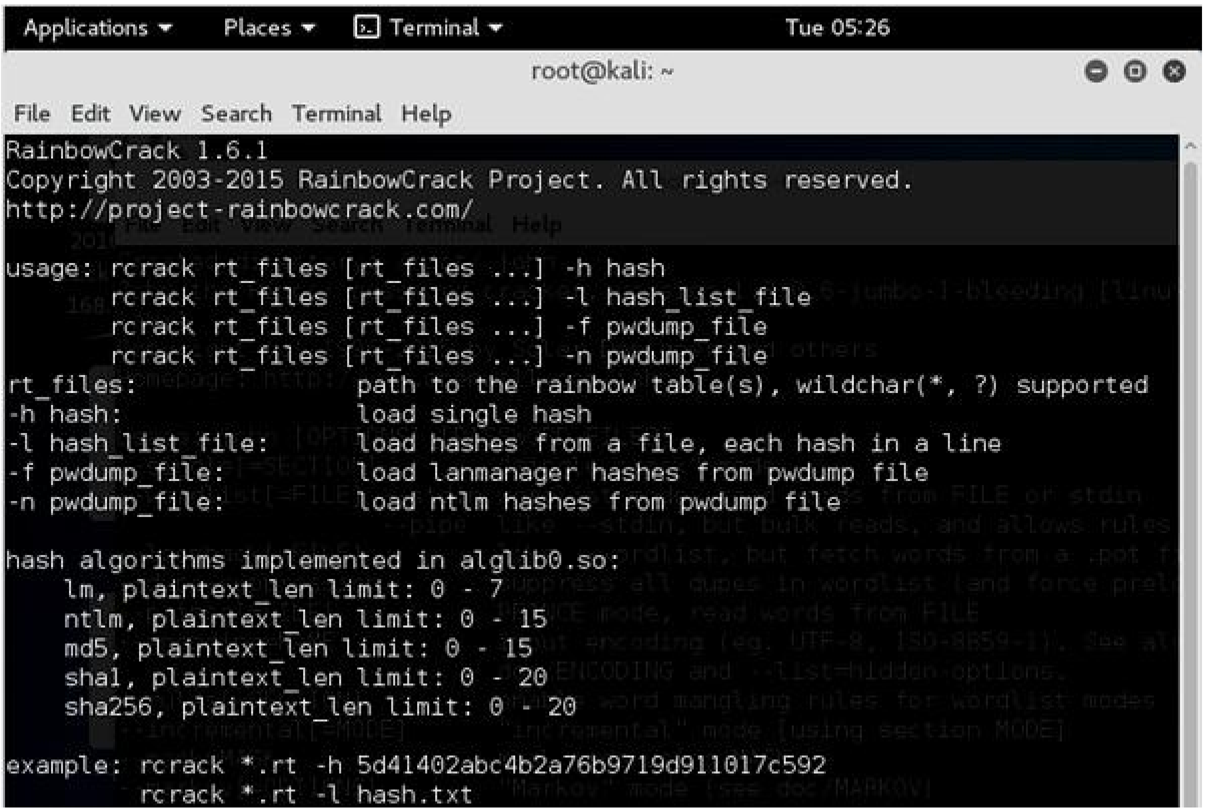
		User	Password	Hash	Formats	GECOS
1	✓	?		admin admin		

Rainbow Tables

A rainbow table contains a set of predefined passwords that are hashed. It is a lookup table used especially in recovering plain passwords from a cipher text. During the process of password recovery,

it just looks at the pre-calculated hash table to crack the password. The tables can be downloaded from http://project-rainbowcrack.com/table.htm

RainbowCrack 1.6.1 is the tool to use the rainbow tables. It is available again in Kali distribution.



```
RainbowCrack 1.6.1
Copyright 2003-2015 RainbowCrack Project. All rights reserved.
http://project-rainbowcrack.com/

usage: rcrack rt_files [rt_files ...] -h hash
       rcrack rt_files [rt_files ...] -l hash_list_file
       rcrack rt_files [rt_files ...] -f pwdump_file
       rcrack rt_files [rt_files ...] -n pwdump_file
rt_files:               path to the rainbow table(s), wildchar(*, ?) supported
-h hash:                load single hash
-l hash_list_file:      load hashes from a file, each hash in a line
-f pwdump_file:         load lanmanager hashes from pwdump file
-n pwdump_file:         load ntlm hashes from pwdump file

hash algorithms implemented in alglib0.so:
    lm, plaintext_len limit: 0 - 7
    ntlm, plaintext_len limit: 0 - 15
    md5, plaintext_len limit: 0 - 15
    sha1, plaintext_len limit: 0 - 20
    sha256, plaintext_len limit: 0 - 20

example: rcrack *.rt -h 5d41402abc4b2a76b9719d911017c592
         rcrack *.rt -l hash.txt
```

Quick Tips

- √ Don’t note down the passwords anywhere, just memorize them.
- √ Set strong passwords that are difficult to crack.
- √ Use a combination of alphabets, digits, symbols, and capital and small letters.
- √ Don’t set passwords that are similar to their usernames.