Semestral Project report

Free password-cracking tools

Principles of Information Security

Sultan Numyalai SS 2018/2019

STU FIIT in Bratislava

Contents

Introduction

We live in a time in which we are surrounded by all sorts of technological achievements, a wealth of computing technology whose performance is constantly increasing, at a time when the Internet is an essential part of our lives. To be without the Internet is often as "live without a hand", more and more devices are becoming part of this vast network, which the Internet undoubtedly is. We are even so far away that even conventional kitchen appliances such as refrigerators are available with internet connection. Data volumes in different data centres are increasing rapidly, creating daily data that is often very sensitive and tempting for a group of people to exploit against us. Likewise, each of us has an increasing number of accounts needed for a variety of Internet services such as mail account, internet banking, social networking and many others that need to be password protected.

The question of what a secure password is now very topical, as well as the question of whether there is an unmistakable password. Nowadays, there are several techniques to lure a victim to a password or to break a password. In this project, I would like to discuss the most widely used and effective password cracking techniques, a short history of password overcoming. I would also like to analyse a few free spreadsheet software that just serves to break the password, either online or physically on the PC in which it is located.

In the next part of the project I would like to point out how easy it is to break the password. would like to point out that protecting a secure password is meaningful and that human laziness and indifference in the field of information security can have serious consequences. Today, we share very sensitive data and therefore need to be protected from potential attackers.

I would also like to mention some specific cases from history where passwords and misused information have been broken.

Password Cracking

In cryptanalysis and, in general, in computer security, password cracking is a process of getting a password or a password. passwords from data that was either already stored on a storage device or transmitted using a computer system. Password break time depends on password strength or on its length in bits, which is one of the password security parameters. Most password cracking methods require a computer capable of producing many possible password shapes that should most likely be.

History

It is not easy to say which attack can be considered the first cyber-attack where the password or cipher was broken, but the 1932 attack is interesting to me. When Polish cryptologists Marian Rejewski, Henryk Zygalski and Jerzy Różycki broke the Enigma machine code. Enigma was an electromechanical encryption machine operating on the principle of rotating rotors. It was used in several modified versions, especially by the German armed forces before and during World War II. The Enigma cipher was regarded by the Germans as unbreakable and safe, and breaking this cipher had an impact on the course of the war.

Figure 1 : http://www.cryptomuseum.com/crypto/enigma/i/index.htm

One of the first attacks on computers such as those we know today is the 1981 AT&T attack. Known as Captain Zap, Ian Murphy is referred to as the first cracker to prove his guilt and then sentenced.
Murphy hacked into AT&T's computers and changed the internal clock that measured billing rates. People were given lower night rates when they called at noon, while people who called at night received daily rates. Murphy was sentenced to 1,000 hours of community service and received a 2.5 year term.

Today Murphy as well as other hackers own their own security firm, IAM Secure Data Systems, Inc. He is still working as a penetration tester.
Perhaps the most famous hacker group of the 21st century is Anonymous.

Established in 2003. In 2010 and 2011, the information about Anonymous began to penetrate into the mass media, which was caused by the great interest that aroused their activity associated with the hacktivist advocacy of WikiLeaks or Sony (Operation Sony). They also participated in the coups in Tunisia and Egypt in early 2011.

Password cracking techniques

There are many techniques, but I choose the most interesting and most used. However, almost no software uses just one attack most of the password cracking tools consist of an efficient combination of techniques.

Most Applied Techniques:

- Dictionary attack
- Brute force attack
- FMS attack
- Rainbow table attack
- Phishing
- Social engineering
- Malware
- Offline cracking
- Shoulder surfing
- Spidering
- Guess

Dictionary attack:

The dictionary attack uses a simple file containing words that can be found in a dictionary, hence its rather straightforward name. In other words, this attack uses exactly the kind of words that many people use as their password.

- **Dictionary attack example software**
- **Cain and Abel**
- **Crack**
- **Aircrack-ng**
- **John the Ripper**
- **L0phtCrack**
- **Metasploit Project**
- **Ophcrack**

Brute force attack

Like the dictionary attack, the brute force attack comes with an added bonus for the hacker. Instead of simply using words, a brute force attack lets them detect non-dictionary words by working through all possible alpha-numeric combinations from aaa1 to zzz10.

It's not quick, provided your password is over a handful of characters long, but it will uncover your password eventually.

It is based on going through individual combinations with the hope that at some point it will find the right one. The attacker systematically checks all possible passwords and passphrases until they are found correctly. Alternatively, an attacker may attempt to estimate a key that is typically created from a password using the key-deduction function. The performance of this technique is greatly affected by the computing power of the device on which the program runs, as well as the length of the password. As time goes on, the time to get a password grows exponentially.

According to US historical regulations, the length of symmetric keys was set to a maximum of 56 bits (e.g., Data Encryption Standard), these rules did not last long, today's symmetric encryption algorithms typically use longer keys, 128 to 256 bits.

There are physical arguments that a 128-bit symmetric key is safe enough against a brute-force attack. The so-called Lindauer limit resulting from the laws of physics determines, according to the formula kT * ln (2), the lowest necessary energy limit to break the key, where T is the processor temperature in Kelvin, k is the Boltzmann constant and the natural logarithm of 2 is 0.693. From principle, no computing device can use less energy than that resulting from the above formula. If we wanted to easily test all possible variants for a 128-bit symmetric key, (2128−1) tested bits would theoretically be needed. If we assume that the calculation takes place at a temperature (~ 300 K), then according to Von Neumann-Landauer formula approximately 1018 joules will be needed for the calculation, which corresponds to the consumption of 30 gigawatts per year.

Despite the seemingly low effectiveness of this attack, it is used quite often and sometimes there are situations where we have no choice but to brute force. Another thing that brute force carat attacks is advanced graphics processor technology that is much more powerful and well adapted to repetitive tasks.

Programs using brute force: Aircrack-ng, John the Ripper, Cain and Abel, L0pthcrack, Hashcat, DaveGrohl ...

Rainbow table attack:

is a list of pre-calculated hashes - the numeric value of an encrypted password used by most systems today (for example, LM or NT hash functions) - and that is the hash of all possible password combinations for any hash algorithm. Table password cracking time is the time it takes to search the list.

On the Internet, rainbow tables can be found for other hash algorithms than the LM hash or NT hash. There are eg. rainbow tables for hash created by MD5, SHA1 algorithm. Just choose the right rainbow table. If there is no rainbow table available on the Internet for your desired algorithm, password length, and character set used, you can buy or produce it.

However, the table itself will be huge and will require huge computational power and this is unnecessary if the hash that it tries to find has been modified by adding random characters to the password before using the hash algorithm.

FMS attack:

is named after its creators Fluhrer, Mantin and Shamir. It is an attack on the commonly used RC4 cipher. The attack allows cryptanalysis of a large number of captured encrypted communications to get the symmetric key of the RC4 cipher, allowing the attacker not only to listen to the encrypted communication, but also to change it.
Fluhrer's, Mantina's and Shamira's attack on certain key derivation methods, but they do not work on RC4-based SSL (TLS) because SSL generates decryption keys for RC4 hashing, which means that different SSL sessions have unrelated keys.
The Fluhrer, Mantina and Shamira (FMS) attack published in 2001 in Weaknesses in the Key Scheduling Algorithm of RC4 exploits weakness in the RC4 cipher key generation algorithm to reconstruct a key from several captured encoded messages. FMS attack has gained popularity in tools like AirSnort, aircrack-ng, which can be used on WEP encoded network.

Phishing:

Although there is no software or technique that uses huge computing power in this case, I think this technique can also be considered a free password cracking tool.

This is a fairly simple way to get a password: ask the user for a password. An unauthorized data e-mail leads an unsuspecting reader to a fake internet banking payment or other site in order to log in and remove a huge PC security problem.
Most of us have already happened to have received such a mail and, despite many warnings and recommendations, it is still a lot of people who are fooled and therefore this technique still has its application.

Nowadays, attackers try to tailor these mails as much as possible to the look and feel of mail from companies they publish. There were mails that contained company logos, contact details, and the sender's email address itself is quite similar to the original address, mostly these addresses differ only in one characte

Figure 2 Phishing

Malware:

Another way to get to the password and then break it is malware. The malicious code can be "packed" by an attacker to download content, and then an unsuspecting user, in addition to what he needed to download malware. Subsequently, a key logger or screen scraper can be installed by malicious software that records everything you write or receive screenshots during the login process, and then sends a copy of that file to an attacker for which it is easy to find your password. Protecting against this type of attack can be done by using an antivirus program as well as not downloading content from unknown and unsecured sites. There is also a malwar that encrypts your data and asks for ransom.

Offline cracking:

It's easy to imagine that passwords are safe when security systems lock users after three or four incorrect attempts. However, most password hacking takes place offline, using a hash set in the password file that was "retrieved" from the compromised system. Often, the goal in question was compromised by third-party hacking, which then provides access to system servers and all of the important user passwords. For example, the third-party device may be a network printer, where communication with the user can be easily captured.

Spidering:

Some hackers realize that many corporate passwords are made up of business related words. Studying corporate literature, sales materials, websites, and even competitors 'and customers' websites can provide ammunition to create their own word list to be used in brute attack.

Truly savvy hackers have automated this process and created a spider application. An example of such a program is Webscarab.

Brutus

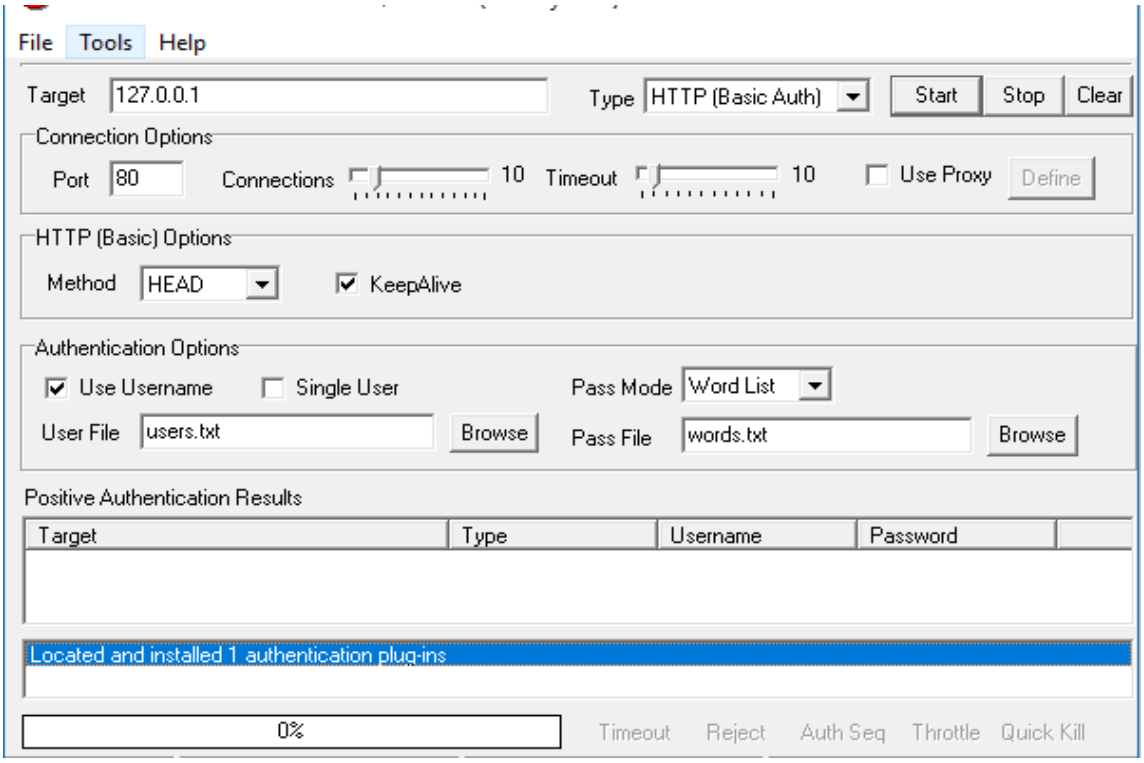
Brutus is one of the most popular tools for remote online password cracking. Its developers say it is the fastest and most flexible tool for breaking passwords. This tool is free and only available for Windows systems. It was released in October 2000.

It supports HTTP (Basic Authentication), HTTP (HTML Form / CGI), POP3, FTP, SMB, Telnet and other types such as IMAP, NNTP, NetBus etc. It is also possible to create custom authentication types. This tool also supports multi-stage authentication engines and is able to connect to 60 simultaneous targets. It also has recovery and retrieval options. So you can pause the attack process at any time and then continue whenever you want to continue

The advantage of this program from my point of view is that it provides a graphical interface that certainly makes it easier to work in this program, although working at the command line is also not difficult I think this adds to the attractiveness of this tool. Another advantage is the possibility of multiple types of attacks. We can choose Brute force, Dictionary attack or Combo. Support for multiple Internet protocols is also a plus.

I downloaded the 2004 version and then tried brute force attack and a dictionary attack on my own PC. Antivirus protection needed to be suspended. As a target I chose 127.0.0.1 which is localhost. For the dictionary attack, I had to make several edits: I added a username to the dictionary and also added my password to the dictionary as I use the 28-character passphrase. Then I launched the attack, as expected the password was revealed within seconds. However, without editing the dictionaries, my PC would be safe.

I also tried a brute force attack, already at the start I knew it would be unsuccessful because the program is limited to the length of passwords up to 16 characters and as I remember my password is 28 characters. This just confirms the well-known fact that effective defense against brute force attack is in the length of the password. I was successful in trying to break a shorter password. It all took a few minutes to overcome my expectations. The password breaking speed can certainly be greater, but my PC is not one of the most powerful ones that has certainly played a role in this experiment. Working with this program has come to me quite easily, the program can be quickly orientated and also offers a wide range of options.



Aircrack-NG

It is a tool for breaking wifi WEP or WPA passwords. It analyzes encrypted Internet packets and attempts to break the password using its algorithm. It uses FMS attack together with other useful techniques for breaking passwords. It is available on Linux and Windows as well as a live CD.

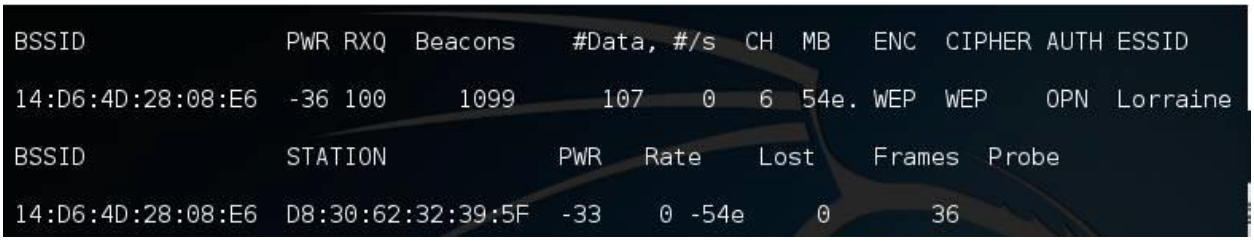
The Aircrack NG software consists of multiple tool packages. Since the program works via wi-fi to program functionality, we need a wi-fi card that can be switched to monitoring mode. Aircrack-ng is an offshoot of the older version of Aircrack ng means new generation.

The use of this program is mainly for penetration testing. The advantage in my opinion is the wide use and the possibilities of this software below are the individual components of the Aircrack-ng package. As a disadvantage, I see the need for a special Internet card with a monitoring mode in the event that our device does not have the necessary investment and card exchange to use it.

Following is a short tutorial about Aircrack NG

- Put the wlan interface into monitor mode with
- – # airmon-ng start wlan0
- – # airodump-ng wlan0mon

After determining the target, focus listeningon that one device.



BSSID	PWR	RXQ	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
14:D6:4D:28:08:E6	-36	100	1099	107	0	6	54e.	WEP	WEP	OPN	Lorraine

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
14:D6:4D:28:08:E6	D8:30:62:32:39:5F	-33	0 -54e	0	36	

After identifying the station

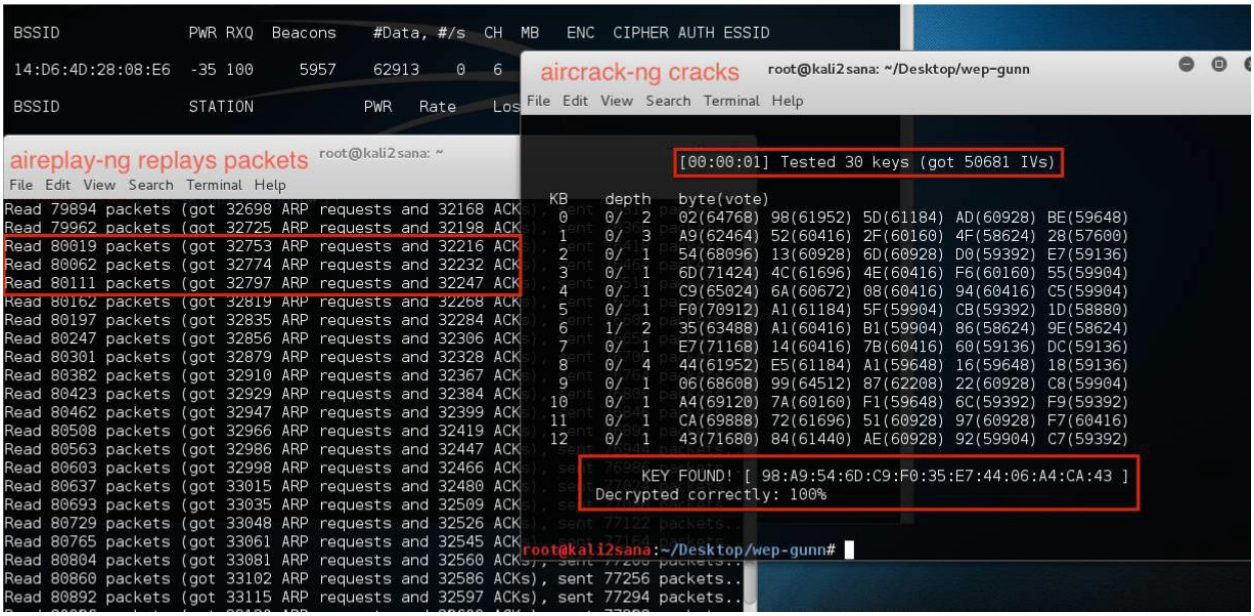
• # airodump-ng - - bssid <00:32:d8...> - -
channel 6 - - write <WEPCracking> wlan0mon

- Use airodump-ng to write all the packets to a traffic dump file
  - Need many data packets encrypted with the same key.
- In order to make this happen, will used aireplayng to inject packets into network to force the WAP into interacting with us.
- Do not yet know the WEP key, but can ID ARP
  - packets by the size of the fixed header.
- Packet injection – open another terminal
- # aireplay-ng -3 -b <BSSID> -h <clientspoofing> wlan0mon
- – 3 specifies ARP packets
- -3, --arpreplay

The classic ARP request replay attack is the most effective way to generate new initialization vectors (IVs), and works very reliably. The program listens for an ARP packet then retransmits it back to the access point. This, in turn, causes the access point to repeat the ARP packet with a new IV.

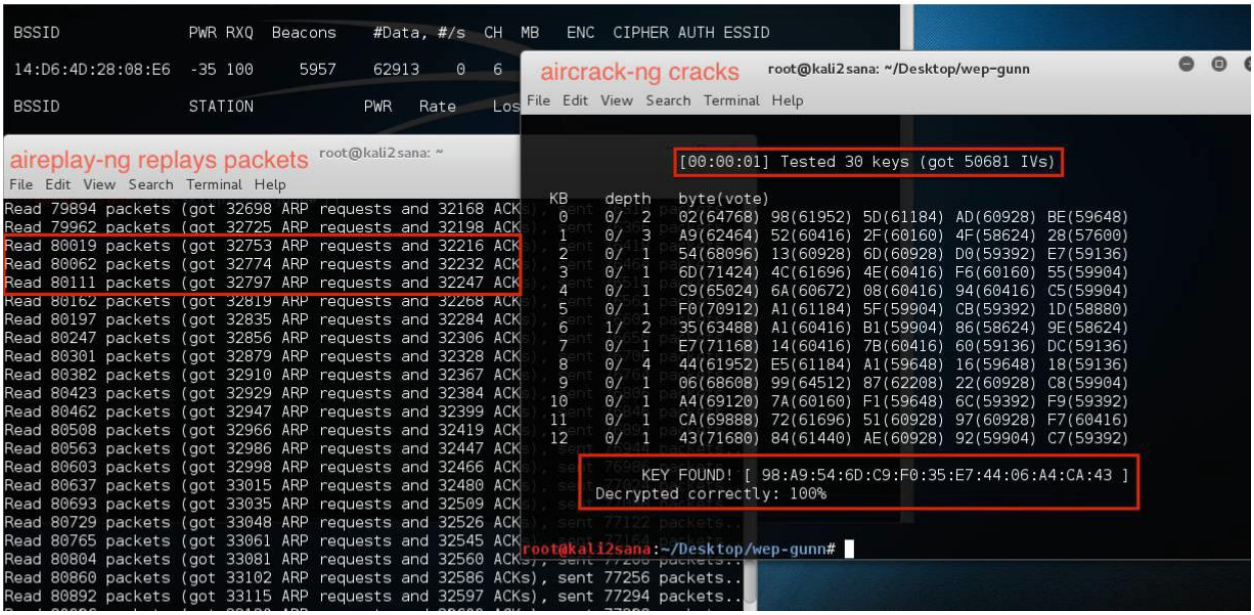
The program retransmits the same ARP packet over and over. However, each ARP packet repeated by the access point has a new IV. It is all these new Ivs which allow you to determine the WEP key.

- In order to crack the key, aircrack looks at the
- collected data packets in the file
- # aircrack-ng <WEPCrack*.cap>
- – Aircrack is an 802.11 WEP / WPA-PSK key cracker



The amount of time it takes to crack a key depends on the amount of traffic in the network because a large sample needs to be collected to compare and identify a collision.

The weakness in WEP stems from needing to reuse initialization vectors (IVs). Once they are reused, which is often, the key can be cracked.



Clean up

- Take it out of monitor mode
  – # airmon-ng stop <wlan0mon>
  – # service network-manager start

John the Ripper password cracker

John the Ripper is a fast password cracker, currently available for many flavors of Unix, Windows, DOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords.

It is one of the most popular password testing and breaking programs because it combines a variety of password breaking techniques in one package, as well as hash detection. It can be mailed to various encrypted password formats commonly used in UNIX, Kerberos AFS, Windows NT / 2000 / XP ...

One of the modes John can use is a dictionary attack. Text string samples are encrypted in the same format as the password being scanned, and encrypted string output is compared. It can also create alternatives to words in a dictionary and then try them out.

John also offers brute force mode. In this type of attack, the program goes through all the text, each string hashed and compared to the input hash. John uses a character frequency table to first try the text that contains the most common characters. This method is useful for breaking passwords that do not appear in dictionaries, but it takes a lot of time to get the result.

On the software page there is a complete documentation and step by step instructions on how to install the program and then start and use it.

Installing and running the program using the instructions on the official site is quite simple. However, I did not try the attack itself because it did not find a volunteer who would agree to attack his PC.

THC Hydra

THC is a fast tool for breaking Internet login passwords. According to the review I found when comparing similar programs, it is clear that the hydra is faster. The program provides the ability to easily add new modules. It is available on Windows Linux, Free BSD, Solaris and OS X. This tool supports various Internet protocols. Currently supports Asterisk, AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, http, SQL, MYSQL, SMTP, Telnet ...

Hydra uses a Brute force attack, as well as performing a quick dictionary attack against over 50 protocols. This program also has a graphical interface which also adds to its popularity.

According to available resources, it is relatively easy to use a hydra and the brute force attack is highly efficient.

Even though the brute force attack is not the best choice of attack, there are situations where we have no choice and it is for these situations that THC Hydra serves.

Prevention and Secure Password

Passwords are the first line of defense against cybercrime. The most important thing is to choose strong passwords and use a different password for each of your important accounts. It is also recommended to update your passwords regularly.

The term "password resistance" expresses the ability of a password to resist guesswork or revelation. The resistance of the password implicitly indicates how many attempts and how much time a potential attacker needs to get it, who does not know the password at the beginning.

As can be seen even today, most people use primitive passwords that each dictionary contains and it is very easy to break them.

What is a Secured Password?

Nowadays many sites where we register have different criteria for creating passwords. The most common criteria for a secure password are:

- Length of at least 8 characters - with increasing password length the time required to break the password with brute force increases.
- Capitalization - prevention against dictionary attack but there are programs that can modify words in the dictionary
- Using digit - same reason as capital letter
- Special character - same reason as digit and capital letter

On the Internet, there are many ways to protect yourself and how to create a secure password, here are some tips from Google:

- Use a unique password for each of your important accounts, such as your email or Internet banking account
- Passwords must be kept in a secret place that is not easily visible
- Use long passwords containing numbers, letters, and symbols
- Try to use a phrase that only you know
- Set password recovery options and periodically update them.

How to create a secure password:

1. Think of any sentence you can remember. This sentence will form the basis of your future password or so-called. passphrase. For example, you can use the phrase: "My son Ali is twenty-five years old".
2. First, verify that the system supports passphrase authentication directly. If you can use this sentence as an authentication element, use it as it is.
3. If the system does not support the passphrase method, change the phrase to password. Than? For example, use the first letter of each sentence word to create a future new word. There will be a word that does not make sense, but it will be memorable for you. Based on the above example, the word "mstmomdr" would be created.
4. Increase the complexity of the password. Combine, for example, uppercase and lowercase and fill in digits. In the phrase, for example, it is possible to replace the word "twenty-five" with a digit. For example, the password "mStmoM25r" may arise.
5. Include some symbols and special characters in your password. You can consciously use symbols in place of similarly looking letters. Can something like "m $ tm0M25r" arise
6. Test the password you created with one of the password resistance checking tools.

Conclusion

In this project, I learned a lot of things, whether password cracking techniques or how the individual software mentioned above works and I tried to look at the issue from multiple angles. Not only how to break the password but also how to defend against attacks. I also tried brutus on my own PC. The theme of password security is very timely as I know from my own experience and from documents found on the Internet that people neglect their protection in the world of computers. There are a number of password cracking programs, most of which are also very powerful, but performance doesn't seem to be needed as most people use short and weak passwords. According to the available resources in the room, even people with secure passwords cannot be able to, because with the increasing performance of computers, processors and other devices, the time required to break the password is reduced. I think it is important to educate ordinary people in this direction to understand what is really threatening them because the loss of personal data is certainly not a pleasant thing. In the project I tried in addition to the knowledge to bring my view of the issue.

Resources

- https://en.wikipedia.org/wiki/List_of_the_most_common_passwords
- https://www.darknet.org.uk/2006/09/brutus-password-cracker-download-brutus-aet2zip-aet2/
- http://www.hackingtools.in/free-download-brutus/
- https://en.wikipedia.org/wiki/Password_cracking
- http://resources.infosecinstitute.com/password-cracking-evolution/#gref
- https://www.aircrack-ng.org/
- http://www.openwall.com/john/
- Montoro, Massimiliano (2009). "Brute-Force Password Cracker". Oxid.it. Retrieved August 13, 2013.