Lesson # 1

Bruteforce. Introduction. Dictionaries and passwords.

What is brute-force?

One of the most basic technologies for hacking is bruterofce.
In this lesson it will be introduced well-known in hacking circles software for bruteforce.

Bruteforce is a technology of hacking where we enumerate passwords and usernames in order to get access to certain service. Bruteforce is known

Where brute-force can be used?

Brute-force atttack can be used to break almost any system that do not have specific protection from it.

Here is a short list of protocols and software hashing algorithms that can be cracked down by brute-force attack:

FTP, SMTP, RDP, Zip archive password, PDF password, Any database, Remote desktop, SMTP , SSH , etc.

Lets have a look on dictionary creating process..

Dictionary creation process:

Manual with extra information:

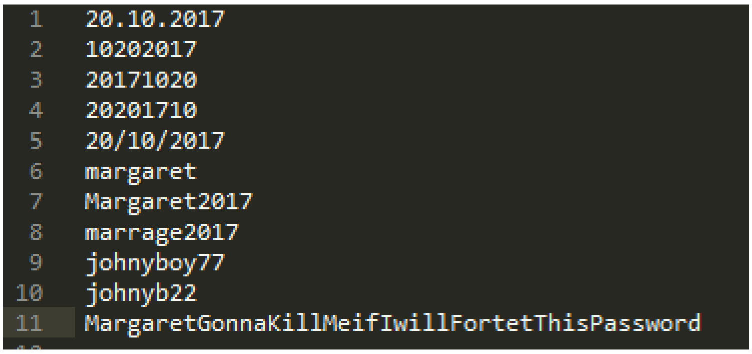
In first case we have our friend John who accidentally forget his password from his zip archive with photos from his marriage and his wife Margaret is very upset about this. In this situation we need to talk to our friend John and ask for questions. Questions should be like these ones:

When was your marriage? Date
What passwords do you usually put on zip archives?
What password do you remember you could put on this this archieve?
What passwords do you usually put on websites?
And so on.

Based on this answers we will do individual dictionary. John's dictionary. In this dictionary we will put: date of his marriage in different formats, passwords he talk, passwords he use on websites, his phone number, his wifi passwords, his wife's cats birthday, etc.

After we will shuffle and generate all this information using specific software for dictionary creation on one file. We will name it john.txt and place in on our folder where we put johns_marrage.zip and our software to break password.

Our text file named john.txt can be manually filled up based on information we have.
We will get something like:



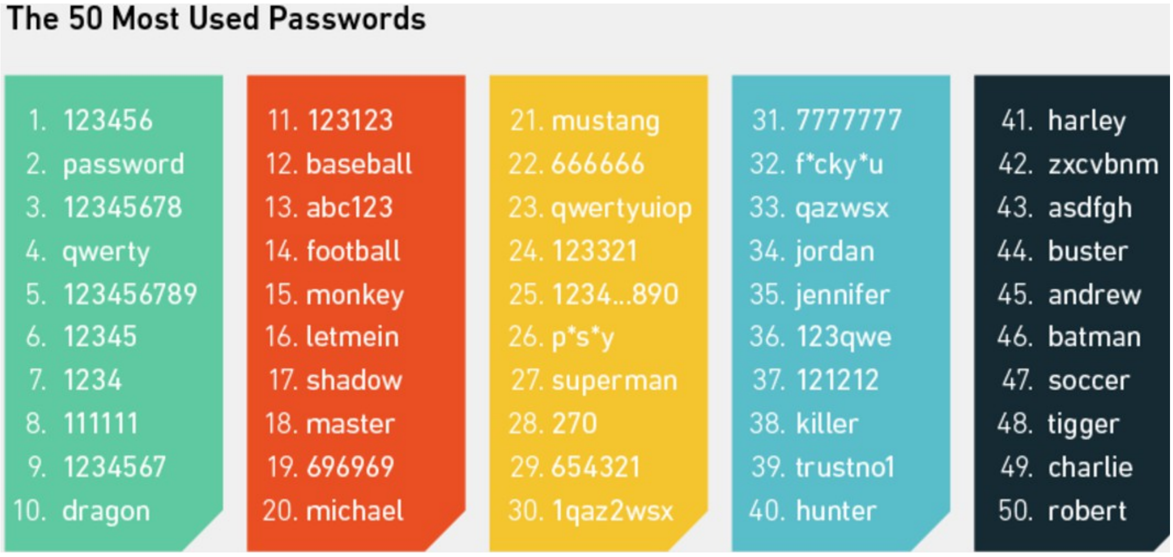
```
20.10.2017
10202017
20171020
20201710
20/10/2017
margaret
Margaret2017
marrage2017
johnyboy77
johnyb22
MargaretGonnaKillMeifIwillFortetThisPassword
```

After we have our dictionary done we can try to brute-force our achieve and could be lucky enough to crack this password down based on extra information we got from our friend.

This is a good example how to create simple manual dictionaries. But if we will not get our password we will need to use others dictionaries. Dictionaries like:

Manual without extra information:
Mostly based on thoughts and ideas of what password is set. As long as no information is provided and this is manual dictionary creation process it is mostly based on thoughts of one who is creating it.

Based on well-known passwords:
For example: 777777, johny, password, PassWord, pass123, SexyAngel, qwerty,dragon.



The 50 Most Used Passwords

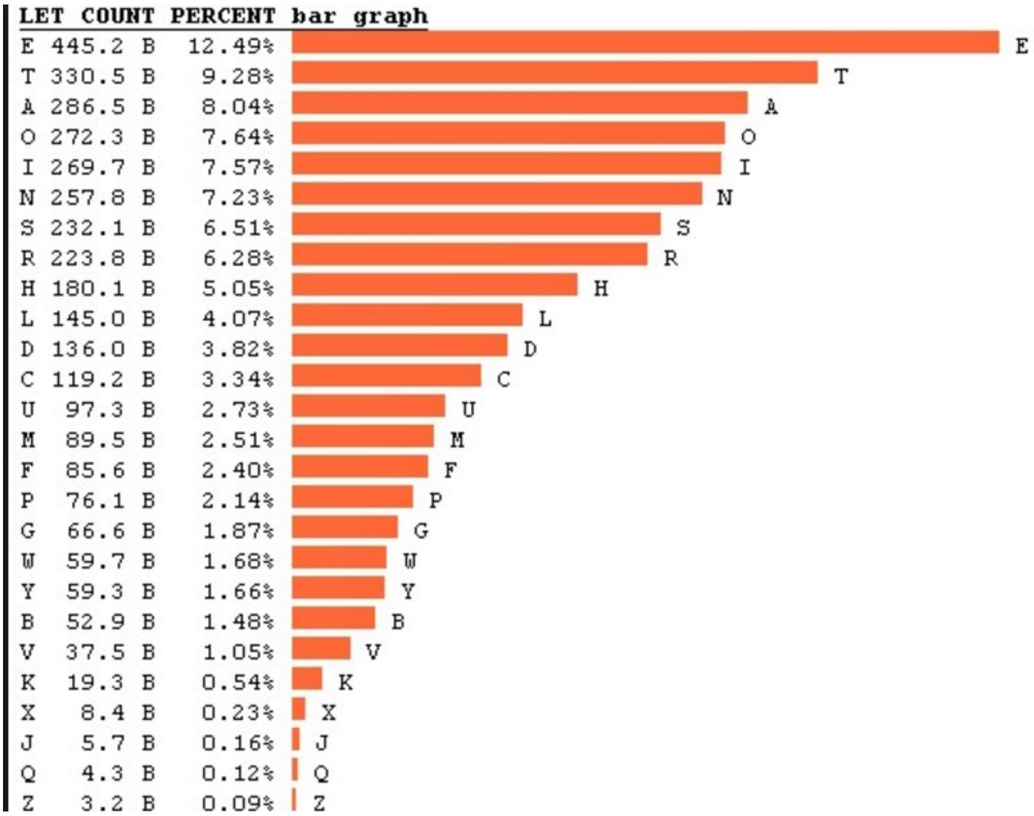
1. 123456
2. password
3. 12345678
4. qwerty
5. 123456789
6. 12345
7. 1234
8. 111111
9. 1234567
10. dragon
11. 123123
12. baseball
13. abc123
14. football
15. monkey
16. letmein
17. shadow
18. master
19. 696969
20. michael
21. mustang
22. 666666
23. qwertyuiop
24. 123321
25. 1234…890
26. p*s*y
27. superman
28. 270
29. 654321
30. 1qaz2wsx
31. 7777777
32. f*cky*u
33. qazwsx
34. jordan
35. jennifer
36. 123qwe
37. 121212
38. killer
39. trustno1
40. hunter
41. harley
42. zxcvbnm
43. asdfgh
44. buster
45. andrew
46. batman
47. soccer
48. tigger
49. charlie
50. robert

Based on location:

For example: bakerstr, londonstreet, Finesquare, macdonalds, CentralPark

Alphabet/Letters:

For example: aaaaa,bbbb,abcde,aaddffwwrr, zswdqdwqdwq,idwqdqwdqw,iioopppo



LET	COUNT	PERCENT	bar graph
E	445.2 B	12.49%	E
T	330.5 B	9.28%	T
A	286.5 B	8.04%	A
O	272.3 B	7.64%	O
I	269.7 B	7.57%	I
N	257.8 B	7.23%	N
S	232.1 B	6.51%	S
R	223.8 B	6.28%	R
H	180.1 B	5.05%	H
L	145.0 B	4.07%	L
D	136.0 B	3.82%	D
C	119.2 B	3.34%	C
U	97.3 B	2.73%	U
M	89.5 B	2.51%	M
F	85.6 B	2.40%	F
P	76.1 B	2.14%	P
G	66.6 B	1.87%	G
W	59.7 B	1.68%	W
Y	59.3 B	1.66%	Y
B	52.9 B	1.48%	B
V	37.5 B	1.05%	V
K	19.3 B	0.54%	K
X	8.4 B	0.23%	X
J	5.7 B	0.16%	J
Q	4.3 B	0.12%	Q
Z	3.2 B	0.09%	Z

This is top of most used letters and it is smart to create dictionaries using this statistics.

Numbers:

For example:12312312312,123457689,987765213,39732134

Numbers repeation:

For example: 777888777999, 122333444555, 778899, 112233,0009999

Mobile phones:

For example: +1-760-887-9998, +17608879998, 17608879998,7608879998

Adresses in specific area:

For example: ny,Newyork,california,Australia,CaNadA.bakerstreet,young.st

Words in English:

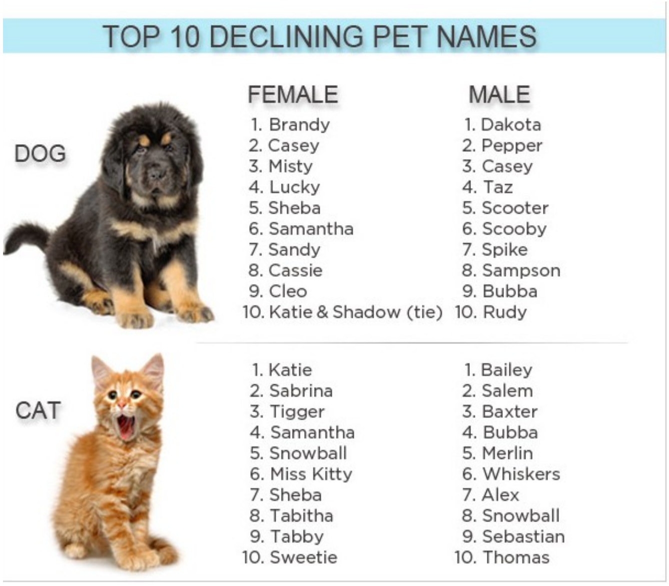
For example: forest, east, EaT, man, idea, East.

Words in other language:

For example: password, пароль, Passwort, fjalëkalim , contraseña

Top names for home pets:

For example: Brandy, Casey, Lucky



TOP 10 DECLINING PET NAMES

	FEMALE	MALE
DOG	1. Brandy	1. Dakota
	2. Casey	2. Pepper
	3. Misty	3. Casey
	4. Lucky	4. Taz
	5. Sheba	5. Scooter
	6. Samantha	6. Scooby
	7. Sandy	7. Spike
	8. Cassie	8. Sampson
	9. Cleo	9. Bubba
	10. Katie & Shadow (tie)	10. Rudy
CAT	1. Katie	1. Bailey
	2. Sabrina	2. Salem
	3. Tigger	3. Baxter
	4. Samantha	4. Bubba
	5. Snowball	5. Merlin
	6. Miss Kitty	6. Whiskers
	7. Sheba	7. Alex
	8. Tabitha	8. Snowball
	9. Tabby	9. Sebastian
	10. Sweetie	10. Thomas

Special symbols:

For example: !@#@@#!@,)()()@@#,*(#)~!!,#$@$@#$@#

Mixed:

For example: canada1987, eat123, P#SSW()RD, 1@2@3

Dates and time:

For example: 12.12.2012, 2018.10.10,20122011,20130809,215909,235959

Popular trands:

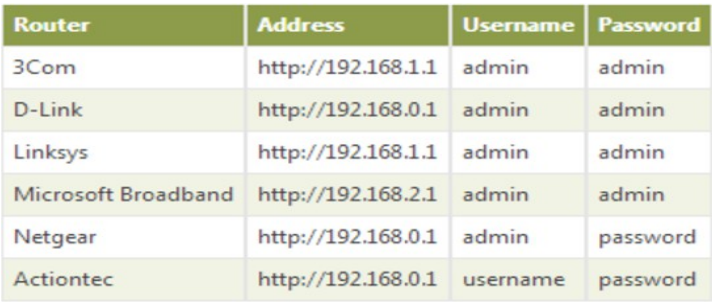
For example: gangnamnstyle, youtube,google,bitcoin,cryptocurrency,cybersport

Morph/combined:

For example: gangnamnstyle123, gangnamnstyle!, gangnamnstyle2017, 2016gangnamnstyle

Default passwords:

For example: admin, administrator, blank, test, developer



Router	Address	Username	Password
3Com	http://192.168.1.1	admin	admin
D-Link	http://192.168.0.1	admin	admin
Linksys	http://192.168.1.1	admin	admin
Microsoft Broadband	http://192.168.2.1	admin	admin
Netgear	http://192.168.0.1	admin	password
Actiontec	http://192.168.0.1	username	password

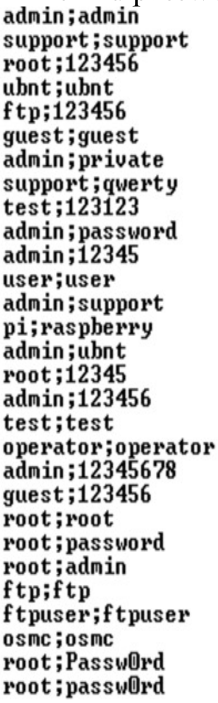
Birthday passwords:

For example: 10201982,19821712,1212,19921010

Specially removed:

(when we have someone who can not type " "a" and never uses 0":)
For example: bcdef,llow,anger,ornge,mllow ,123456789.

Here is an example of username and password compilation in one file:

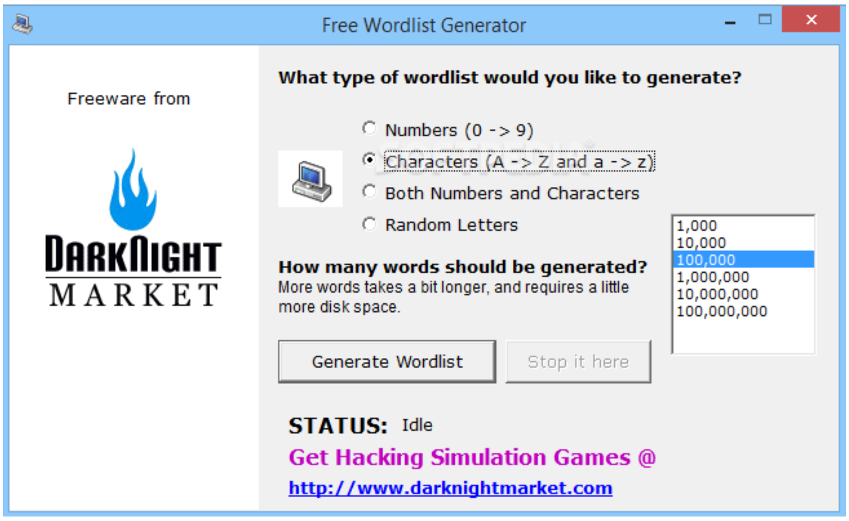


```
admin;admin
support;support
root;123456
ubnt;ubnt
ftp;123456
guest;guest
admin;private
support;qwerty
test;123123
admin;password
admin;12345
user;user
admin;support
pi;raspberry
admin;ubnt
root;12345
admin;123456
test;test
operator;operator
admin;12345678
guest;123456
root;root
root;password
root;admin
ftp;ftp
ftpuser;ftpuser
osmc;osmc
root;Passw0rd
root;passw0rd
```

password.txt file exampe

After we created dictionaty file it will be right to soft it based on our thoughts and logic.
We can http://softfie.com/download/soft/sortir.rar download it from here and sort our dictionary.

Software to generate dictionaries.



What type of wordlist would you like to generate?

○ Numbers (0 -> 9)
● Characters (A -> Z and a -> z)
○ Both Numbers and Characters
○ Random Letters

How many words should be generated?
More words takes a bit longer, and requires a little more disk space.

1,000
10,000
100,000
1,000,000
10,000,000
100,000,000

STATUS: Idle

Get Hacking Simulation Games @
http://www.darknightmarket.com

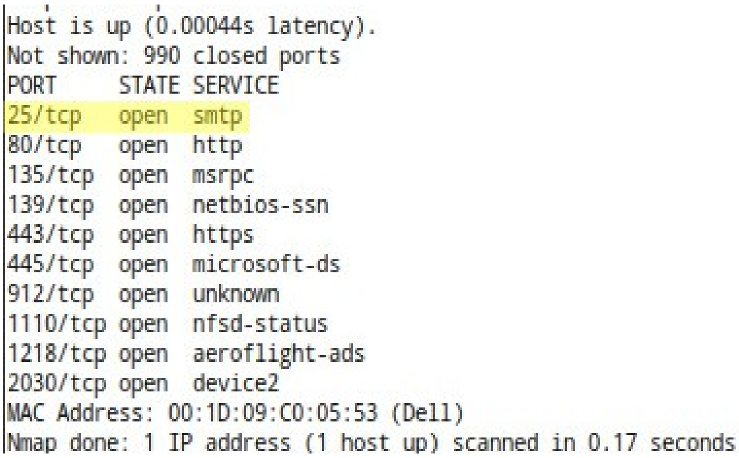
What do we need to know before we will brute-force?

Before talking about bruteforce we should take a look on protocols and ports.
Almost any webserver has some open ports with certain software running. Based on experience I can say that almost any web server has at least 3-5 open ports that could be attacked by brute-force.

21 port stands for FTP server, 22 port stands for SSH server at 80 port we can find http server with administration login and so on.

Right after we did port scanning we can see open ports and based on this information we can think of ideas of what service to brute-force.

For example: We scanned some server where we found open 25 port which usually stands for smtp server. After we get all information about this software and open specific bruteforce software and prepare all dictionaries we can start.

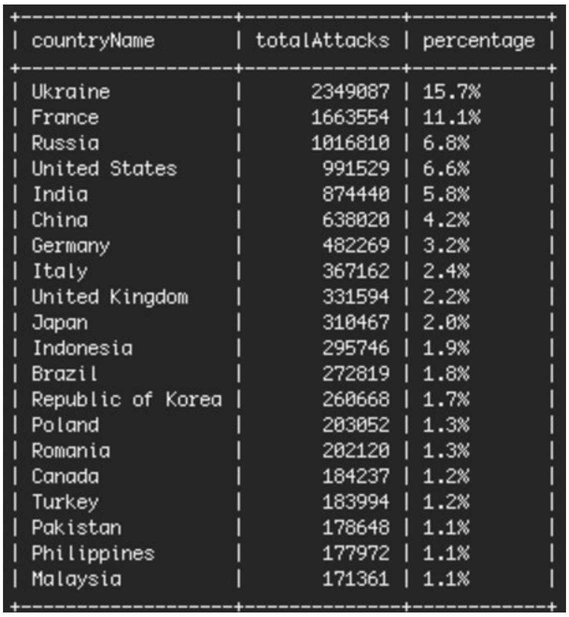


```
Host is up (0.00044s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
912/tcp   open  unknown
1110/tcp open  nfsd-status
1218/tcp open  aeroflight-ads
2030/tcp open  device2
MAC Address: 00:1D:09:C0:05:53 (Dell)
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

*Nmap port scanning.

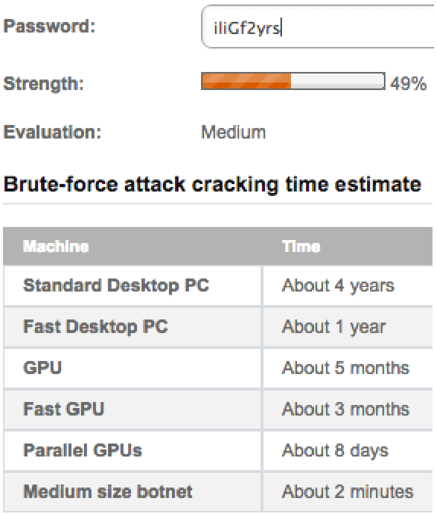
Statistics of bruteforce in World:

Statistics on attacks on servers by country.



```
+--------------------+--------------+------------+
| countryName        | totalAttacks | percentage |
+--------------------+--------------+------------+
| Ukraine            |      2349087 | 15.7%      |
| France             |      1663554 | 11.1%      |
| Russia             |      1016810 | 6.8%       |
| United States      |       991529 | 6.6%       |
| India              |       874440 | 5.8%       |
| China              |       638020 | 4.2%       |
| Germany            |       482269 | 3.2%       |
| Italy              |       367162 | 2.4%       |
| United Kingdom     |       331594 | 2.2%       |
| Japan              |       310467 | 2.0%       |
| Indonesia          |       295746 | 1.9%       |
| Brazil             |       272819 | 1.8%       |
| Republic of Korea  |       260668 | 1.7%       |
| Poland             |       203052 | 1.3%       |
| Romania            |       202120 | 1.3%       |
| Canada             |       184237 | 1.2%       |
| Turkey             |       183994 | 1.2%       |
| Pakistan           |       178648 | 1.1%       |
| Philippines        |       177972 | 1.1%       |
| Malaysia           |       171361 | 1.1%       |
+--------------------+--------------+------------+
```

Statistics of brute-force cracking estimate time:



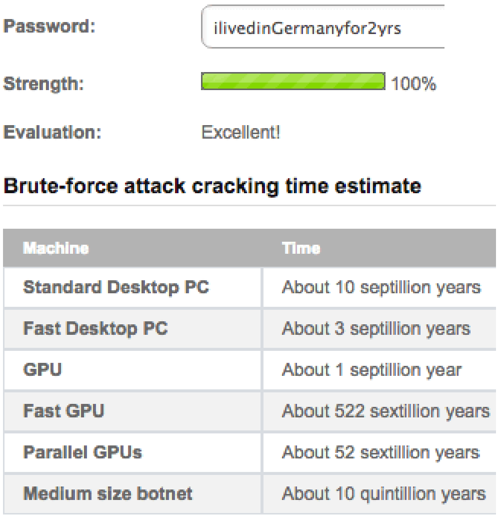
Password: iliGf2yrs

Strength: 49%

Evaluation: Medium

Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	About 4 years
Fast Desktop PC	About 1 year
GPU	About 5 months
Fast GPU	About 3 months
Parallel GPUs	About 8 days
Medium size botnet	About 2 minutes



Password: ilivedinGermanyfor2yrs

Strength: 100%

Evaluation: Excellent!

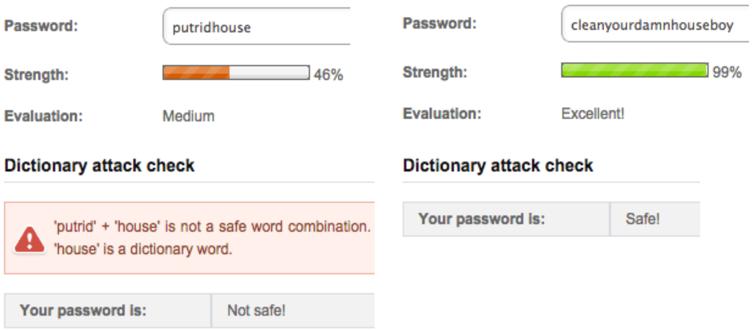
Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	About 10 septillion years
Fast Desktop PC	About 3 septillion years
GPU	About 1 septillion year
Fast GPU	About 522 sextillion years
Parallel GPUs	About 52 sextillion years
Medium size botnet	About 10 quintillion years

How to protect yourself from brute-force attacks?

Password strength:
It is well-known that based on password strength ability to crack it goes down.

Here is an example of password check. There are a lot of services



Password:	putridhouse
Strength:	46%
Evaluation:	Medium

Dictionary attack check

'putrid' + 'house' is not a safe word combination.
'house' is a dictionary word.

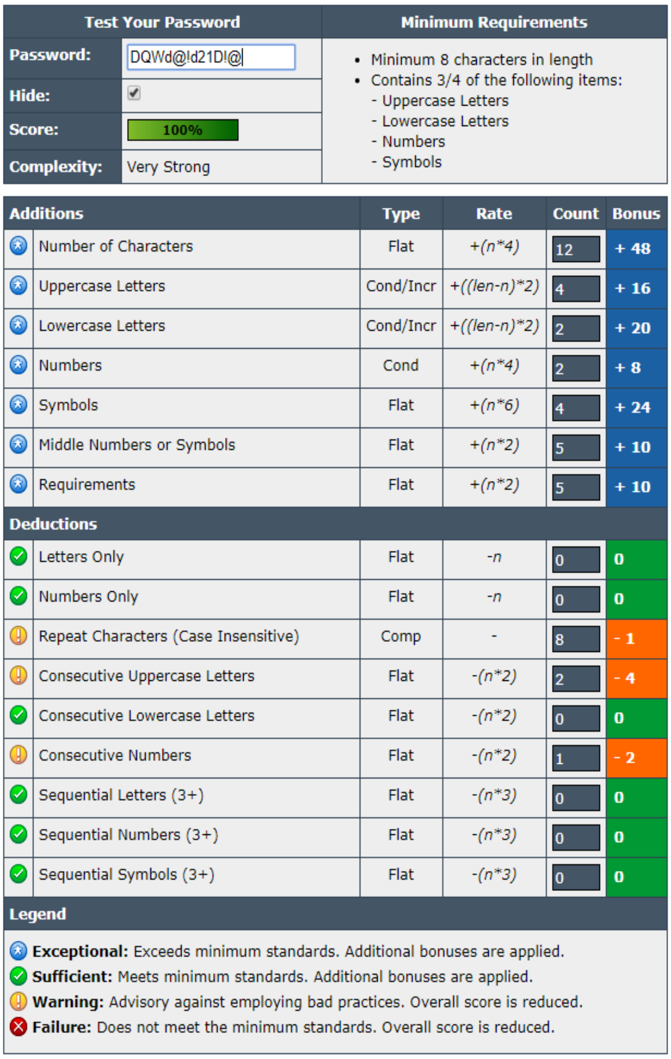
Your password is:	Not safe!

Password:	cleanyourdamnhouseboy
Strength:	99%
Evaluation:	Excellent!

Dictionary attack check

Your password is:	Safe!

Here is an example of password checker. *http://www.passwordmeter.com/*



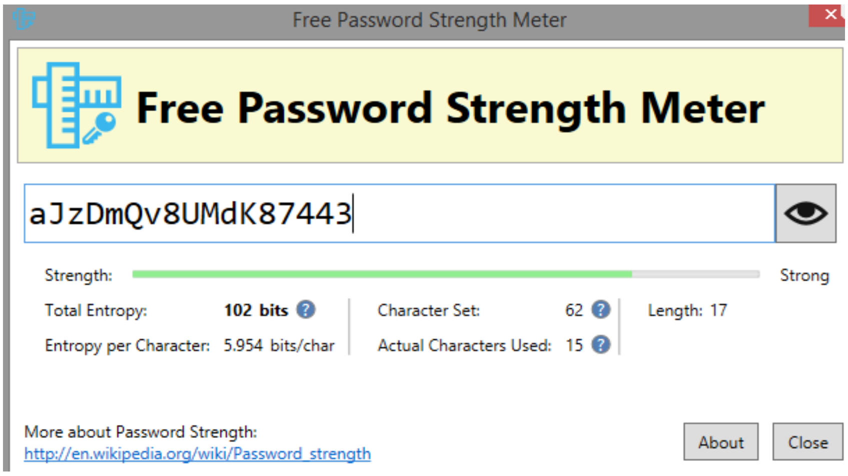
Test Your Password		**Minimum Requirements**
Password:	DQWd@!d21D!@	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☑	
Score:	100%	
Complexity:	Very Strong	

	Additions	**Type**	**Rate**	**Count**	**Bonus**
★	Number of Characters	Flat	+(n*4)	12	+ 48
★	Uppercase Letters	Cond/Incr	+((len-n)*2)	4	+ 16
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	2	+ 20
★	Numbers	Cond	+(n*4)	2	+ 8
★	Symbols	Flat	+(n*6)	4	+ 24
★	Middle Numbers or Symbols	Flat	+(n*2)	5	+ 10
★	Requirements	Flat	+(n*2)	5	+ 10
	Deductions				
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
!	Repeat Characters (Case Insensitive)	Comp	-	8	- 1
!	Consecutive Uppercase Letters	Flat	-(n*2)	2	- 4
✓	Consecutive Lowercase Letters	Flat	-(n*2)	0	0
!	Consecutive Numbers	Flat	-(n*2)	1	- 2
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
✓	Sequential Numbers (3+)	Flat	-(n*3)	0	0
✓	Sequential Symbols (3+)	Flat	-(n*3)	0	0

Legend

★ **Exceptional:** Exceeds minimum standards. Additional bonuses are applied.
✓ **Sufficient:** Meets minimum standards. Additional bonuses are applied.
! **Warning:** Advisory against employing bad practices. Overall score is reduced.
✗ **Failure:** Does not meet the minimum standards. Overall score is reduced.

**** But always remember – if you put your password it means it can go to dictionaty.txt file ;)***



Free Password Strength Meter

aJzDmQv8UMdK87443

Strength: Strong

Total Entropy: 102 bits

Entropy per Character: 5.954 bits/char

Character Set: 62

Actual Characters Used: 15

Length: 17

More about Password Strength:
http://en.wikipedia.org/wiki/Password_strength

URL for download.
https://securesafepro.com/passtrength-download.html

How to start brute-force?

Before we start to brute-force we scanned our target and generated dictionary. Now we have to use specific software to do our job.
We can choice software based on service running on server or situation we are facing, for example to bruteforce MD5 hash or FTP bruteforce should be used different software.

Now lets take a deep look on our software:
~~~~~~

Patator. Hydra.Brutus (Single bruteforce software with different protocols to choice)
https://github.com/1N3/BruteX (Mass scan)

MD5 brute , SALT password ,Handshake bruteforce ,Wi-Fi bruteforce
Windows NTLM, Hashcat, Router bruteforce, Virus admin panel bruteforce

Generate list:
https://github.com/Broham/PassGen Smart generator

Dictionary list:
https://github.com/duyetdev/bruteforce-database
https://github.com/danielmiessler/SecLists/tree/master/Passwords

Additional:
https://github.com/N3TC4T/InstaBrute
https://github.com/superhacker777/hikka webcamera bruteforce hikka (Hikvision)

Custom dictionary generator:
https://github.com/Mebus/cupp

Protection from ssl brutefoce:
https://jerrygamblin.com/2017/08/24/disallow-million-most-common-passwords/
~~~~~~

IPBOX