# Learn about Brute Force attack

Brute force attack mechanism has its advantages. It can also be used to check network security and recover forgotten passwords.

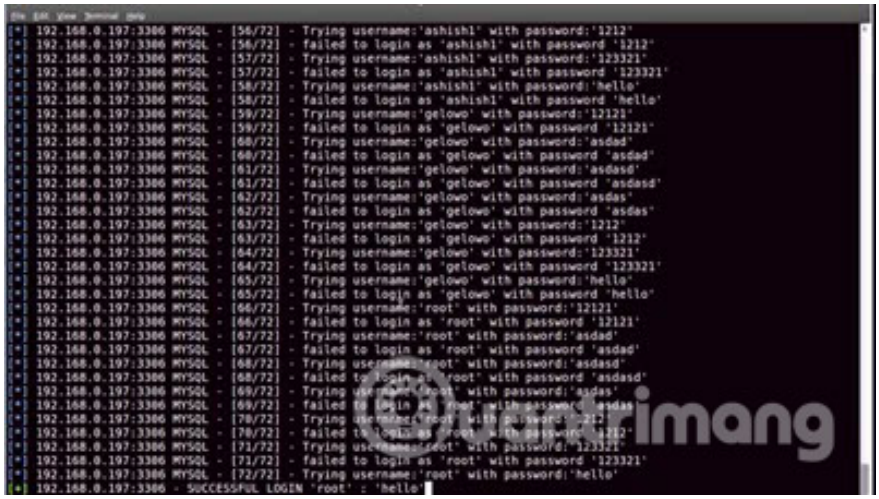
There are many methods used by hackers to access computers, computer networks, websites or online services. Making a Brute Force attack is one of those methods. It is one of the simplest methods, but takes time to hack a server or a normal computer. Brute force attack mechanism has its advantages. It can also be used to check network security and recover forgotten passwords. This article will help you understand what the Brute Force Attack definition is and consider the basic precautions.

## Learn about Brute Force attacks

1. What is Brute Force attack?
2. Speed ??of computer and problem to password in Brute Force attack
3. How to prevent and protect to avoid Brute Force attacks

## What is Brute Force attack?

Brute Force attack is a type of network attack, in which you have a software, which rotates different characters, combined to create a correct password. The simple Brute Force Attack password cracker software will use all possible combinations to find the password for the computer or network server. It is very simple and does not use any smart techniques. Because this method is mostly math-based, it takes less time to crack the password, using brute force applications instead of finding them manually. Saying this method is based on math because computers do very well maths and perform them in seconds, a lot faster than the human brain (takes longer to create combinations). .




Brute Force attacks are good or bad depending on who uses it. It may be that cyber criminals try to hack into a network server, or it may be used by a network administrator to see if their network is secure. Some computer users also use brute force applications to recover forgotten passwords.

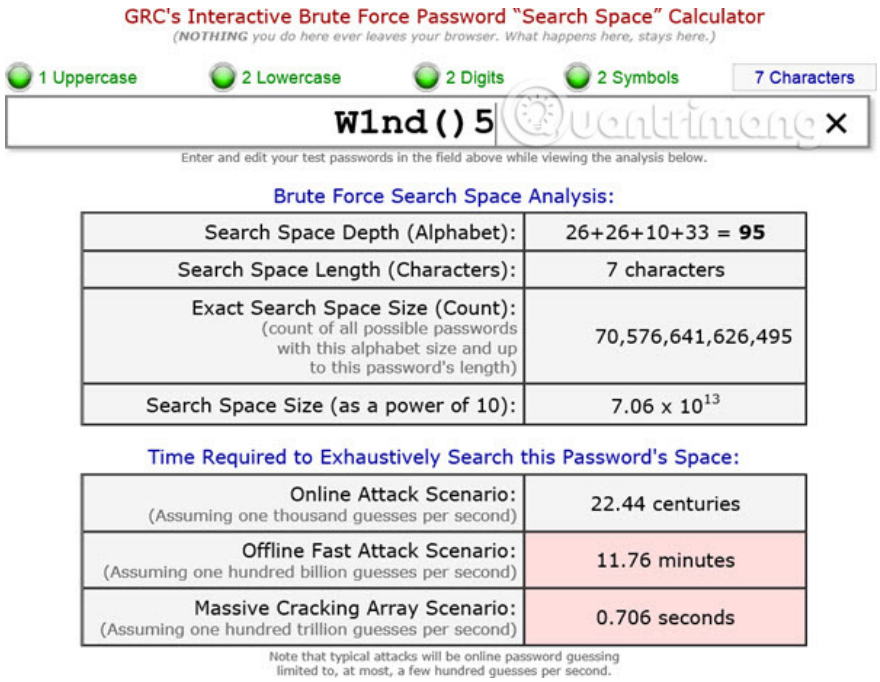
## Speed ??of computer and problem to password in Brute Force attack

If your password is using all the lower case letters and no special characters or digits, it only takes 2-10 minutes that a brute force attack can crack this password. Conversely, a password with a combination of both upper and lower case letters and a few digits (assuming 8 digits) will take more than 14-15 years to crack.

It also depends on the speed of the computer processor, as to how long to crack the network's password or log on normally to a standalone Windows computer.

Therefore, a strong password has a lot of meanings. To create a really strong password, you can use ASCII characters to create a stronger password. ASCII characters refer to all the characters available on the keyboard and more (you can view them by pressing ALT + numbers (from 0 to 255) on the Numpad). There are about 255 ASCII characters and each character has a code that is read by the machine and converted into binary (0 or 1), so that it can be used by the computer. For example, ASCII code gives a space of 32. When you enter a space, the computer reads it 32 and converts it to binary - it will be 10000. Characters 1, 0, 0, 0, 0, 0 stored in the form of ON, OFF, OFF, OFF, OFF, OFF in the memory of the computer. This has nothing to do with brute force, unless you use all ASCII characters. If you use special characters in the password, the total time needed to crack the password can be up to 100 years.

Brute Force Password Calculator (reference link: **https://www.grc.com/haystack.htm)** is where you can check how long it will take to crack a password. There are different options including lowercase, uppercase letters, numbers and all ASCII characters. Based on what you used in the password, select the options and click the **Calculate** button to see how hard the Brute attack will be to crack your computer or server password.




# How to prevent and protect to avoid Brute Force attacks

Since no special logic is applied in Brute Force attacks, except to try different combinations of characters used to generate passwords, precautions are very basic and relatively easy.

In addition to using security software and a fully updated Windows operating system, you should use a strong password with some of the following characteristics:

1. At least one uppercase letter
2. At least one digit
3. At least one special character
4. Password must be at least 8-10 characters
5. Include ASCII characters, if you want.

The longer the password, the longer it takes to crack it. If your password is like **'PA $$ w0rd', it** will take more than 100 years to crack it with existing brute force attack applications. Please do not use the proposed password in the example, because it is very easy to be broken, using some smart software, it is possible to synthesize the proposed passwords in related articles. to brute force attacks.

Free software **PassBox** is a handy little tool that will remember all your passwords and even create a strong password for your account. If not, you can use some free online password generators to create strong anonymous passwords. After doing that, check your new password with **Microsoft Password Checker - Microsoft Password Checker** . This password checker helps assess the password strength you entered.

If you are using WordPress website software, there are also many WordPress security plugins that automatically block brute force attacks. Using web firewalls like Sucuri or Cloudflare is another option you might consider. Another way to block brute-force attacks is to lock the accounts after a number of incorrect password attempts. **The Limit Logins WordPress plugin** is great for preventing brute force attacks on your blog. Other measures include allowing logging from only selected IP addresses, changing the default login URL to something else and

using Captcha to enhance your WordPress blog security.

See more:

1. What is Social Engineering? How to prevent Social Engineering?
2. What is Spear Phishing?
3. What is Office 365 Attack Simulator? How to use it?

You finished reading the article "**Learn about Brute Force attack**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

---