

How to stop brute force attempt ?

Author:
A+ Hosting

Created On: 06 May 2008 09:30 PM

keywords: hacking, brute force attempt, remote desktop, terminal service, ssh

>>>Preventing Brute force attack

> Overview

Blocking and preventing brute force attacks is one of the main things you want to do on your web server to add a layer of security. While someone might not be targeting your site or server specifically, they will have automated tools that will try to guess random usernames and passwords that are common against your system. They are essentially forcing their way to user only authorized areas of a system, such as FTP accounts, e-mail accounts, databases, script based administration areas and root or any shell access are most common attempts. They will try multiple login attempts, guessing usernames and passwords, trying to force their way onto your machine.

> How the brute force attack works

Hackers can try to get into your system using a few different methods.

1) Manual login attempts, they will try to type in a few usernames and passwords

2) Dictionary based attacks, automated scripts and programs will try guessing thousands of usernames and passwords from a dictionary file, sometimes a file for usernames and another file for passwords.

3) Generated logins, a cracking program will generate random usernames set by the user. They could generate numbers only, a combination of numbers and letters or other combinations.

> Signs of a brute force attempt

You can easily spot a brute force attempt by checking your servers log files. You will see a series of failed login attempts for the service they are trying to break into.

```
# pico /var/log/secure
```

```
or
```

```
# tail -f /var/log/secure
```

Check for failed login attempts such as:

Apr 11 19:02:10 fox proftpd[6950]: yourserver (usersip[usersip]) - USER theusername (Login failed): Incorrect password.

> How to prevent a brute force attack

There are a few main ways to stop a brute force attack we'll cover;

- 1) restricting the amount of login attempts that a user can perform
- 2) banning a users IP after multiple failed login attempts
- 3) keep a close eye on your log files for suspicious login attempts

>> If you have windows server then you can stop the brute force attempt by changing the port number of Terminal server / Remote desktop.

Default terminal service port is 3389, you can change it to any other port like 3399

This way when you will try to connect with remote desktop you will have to provide the port number along with the IP address like this

```
192.168.1.1:3399
```

>> If you have Linux server then you can stop the brute force attempt by changing the port number of ssh service.

Default ssh port is 22, you can change it for any other port like 222 or 10222 etc

This way when you will try to connect with ssh, you will have to provide the port number along with IP address like this

```
ssh root@192.168.1.1 -p 10222
```

You can find in our Knowledge for how to change the Remote desktop port and ssh port.

> Report Attackers

Instead of simply blocking the IP and ignoring the user you can also report the attacker to the IP source upstream provider, such as an ISP.

Lookup their IP: Go to DNSStuff.com and enter their IP the in IP Whois Lookup tool.

It will give you information about the ISP, including company and website. Go to their website and look for an abuse section, such as abuse@company.com

Compose an email including the attackers IP, time, any log snippets and other relevant information.

> Summing Up Brute Force Logins and Hack Attempts

Brute force attacks are more and more common these days as hacking tools are widely available

for script kiddies to play with. Arming yourself with knowledge and tools to deal with such attacks can give you peace of mind knowing your system is relatively protected but it will never be 100% foolproof safe.