Why Bruteforce?

Bruteforce is a simple and popular attack on a system. It checks a user’s password with a list of words in an attempt to crack it. While it is very simple it is powerful if not mitigated. Bruteforce allows hackers to obtain easy passwords like 123456 or password.

Steps to set up environment:

1. Step by step of how you set up the environment

Server:

1. In the Server Manager, go to the Dashboard section.

2. Select Add roles and features.

a. Select Role-based or feature-based installation.

b. Select your server in the list.

c. Select Active Directory Domain Services.

d. Click through until you start the installation and then keep the wizard open as it installs everything.

3. Click the link to Promote this server to a domain controller.

4. Go through the AD DS Installation Wizard:

a. Select Add a new forest.

b. Set the Root domain name to be: comp3550.private

c. For the Forest functional level and Domain functional level, choose Windows Server 2012 R2 or Windows Server 2016, depending on which version of Windows Server you’re using.

d. Choose a password for the Directory Services Restore Mode account.

e. Ignore the warning about DNS delegation.

f. Don't change the NetBIOS domain name.

g. Select the default locations for the various folders

h. After it runs prerequisite checks, click Install.

5. After installation is complete (takes ~5 minutes) the server will reboot.

1. Step by step of how you conducted the attack. Elaborate on all the numbers you see during the attack (network traffic, etc)

* The script pulls information from libraries and creates a connection to the network
* Once connected to the network, the attack script then obtains the client IP address and connects. Once connected, the attack begins
* When when running the script make sure python command works
* Make sure the wordlist is in the directory running the script.

Mitigation Techniques

So with brute force attacks, there is no single way to stop it. However there is a large variety of pre-emptive techniques and rules that can be deployed in order to mitigate one from happening or to make it so difficult that the attacker backs out. Below we will go into detail on each method.

**Account lockout after failed attempts**

Account lockouts with progressive delays lock an account only for a set amount of time after a designated number of unsuccessful login attempts. This means that automated brute force attack tools will not be as useful. Additionally, admins will not have to deal with unlocking several hundred accounts every 10 minutes or so.

**Make the root user inaccessible via SSH**

SSH brute force attempts are often carried out on the root user of a server. Make sure to make the root user inaccessible via SSH by editing the sshd\_config file. Set the ‘DenyUsers root’ and ‘PermitRootLogin no’ options.

**Modify the default port**

Most automated SSH attacks are attempted on the default port 22. So, running sshd on a different port could prove to be a useful way of dealing with brute force attacks. To switch to a non-standard port, edit the port line in your sshd\_config file.

**Use CAPTCHA**

Tools such as CAPTCHA render automated bots ineffective. That single requirement to enter a word, or the number of a specific item on a generated image is highly effective against bots. Even though hackers have started using optical character recognition tools to get past this safety mechanism.

**Limit logins to a specific IP address or range**

If you allow access only from a designated IP address or range, brute force attackers will need to work hard to overcome that obstacle and forcefully gain access. You can set this up by scoping a remote access port to a static IP address. If you don’t have a static IP address, you can configure a VPN instead.

**Employ 2-factor authentication**

Two-factor authentication is considered by many to be the first line of defense against brute force attacks. Implementing such a solution greatly reduces the risk of a potential data breach. The great thing about 2FA is that password alone is not enough. Even if an attacker cracks the password, they would have to have access to your smartphone or email client. Very persistent attackers might try to overcome that obstacle, but most will turn around and search for an easier target.

**Use Unique Login URLs**

Create unique login URLs for different user groups. This will not stop a brute force attack, but introducing that additional variable makes things a bit more challenging and time-consuming for an attacker.

**Monitor the server logs**

Analyzing log files diligently may also help. Log files are essential for maintaining a system. Log management applications, such as Logwatch, can help perform daily check-ups and can auto-generate daily reports.