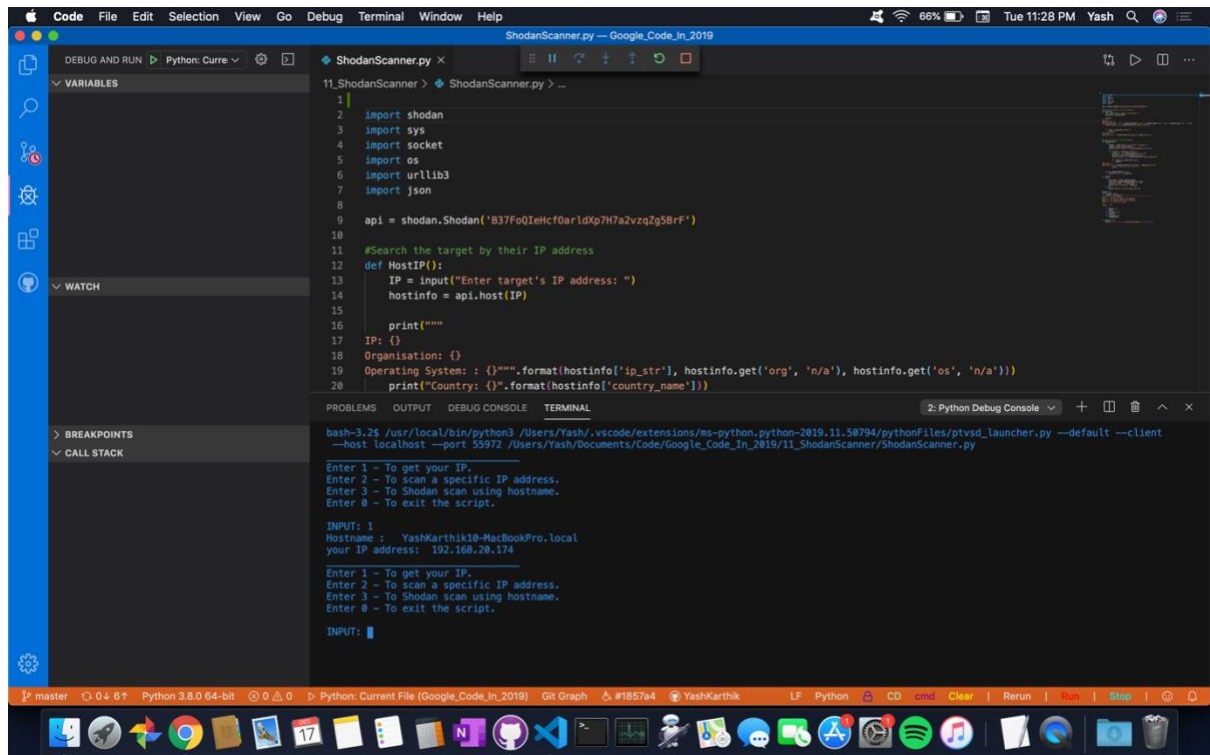


Shodan API Attacks

There were various attacks I performed on the site 'hackthissite.org' and its relatives.

Part 1:

Simple enough I found my devices IP address.



The screenshot shows the VS Code editor with a file named 'ShodanScanner.py' open. The script is a Python program that uses the Shodan API to search for information about a target IP address. The code is as follows:

```
1 import shodan
2 import sys
3 import socket
4 import os
5 import urllib3
6 import json
7
8 api = shodan.Shodan('B37FoQIeIcf0arldKp7H7a2vzqZg58rF')
9
10 #Search the target by their IP address
11
12 def HostIP():
13     IP = input("Enter target's IP address: ")
14     hostinfo = api.host(IP)
15
16     print("""
17 IP: {}
18 Organisation: {}
19 Operating System: : {}""".format(hostinfo['ip_str'], hostinfo.get('org', 'n/a'), hostinfo.get('os', 'n/a')))
20     print("Country: {}".format(hostinfo['country_name']))
```

The terminal output shows the script being run in a bash shell. The user enters '1' to get their IP, and the script outputs the following information:

```
bash-3.2$ /usr/local/bin/python3 /Users/Yash/.vscode/extensions/ms-python.python-2019.11.50794/pythonFiles/ptvsd_launcher.py --default --client
--host localhost --port 55972 /Users/Yash/Documents/Code/Google_Code_In_2019/11_ShodanScanner/ShodanScanner.py

Enter 1 - To get your IP.
Enter 2 - To scan a specific IP address.
Enter 3 - To Shodan scan using hostname.
Enter 0 - To exit the script.

INPUT: 1
Hostname : YashKarthik10-MacBookPro.local
your IP address: 192.168.20.174

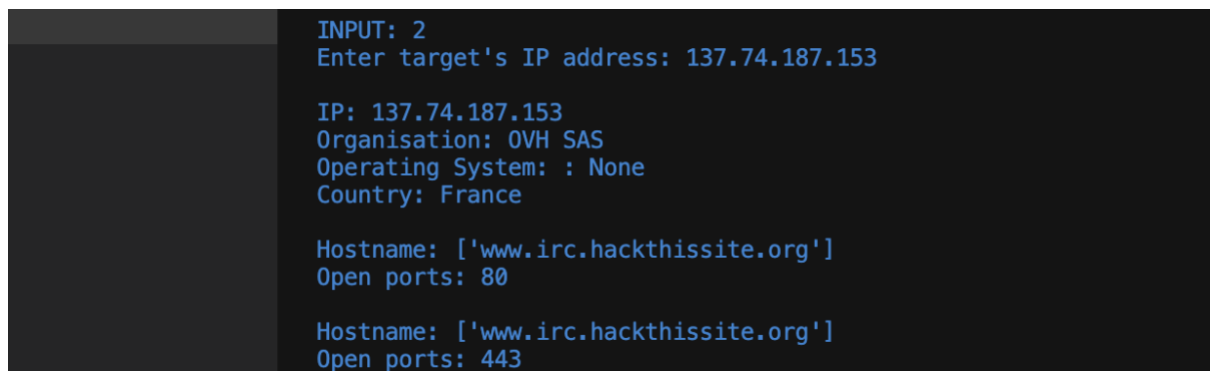
Enter 1 - To get your IP.
Enter 2 - To scan a specific IP address.
Enter 3 - To Shodan scan using hostname.
Enter 0 - To exit the script.

INPUT: 
```

I ran the script in my integrated terminal through VSCode.

Part 2:

Attacked one of the IP addresses of 'hackthissite' and returned information. Using IP address as user input.



The terminal output shows the script being run in a bash shell. The user enters '2' to scan a specific IP address, and the script outputs the following information:

```
INPUT: 2
Enter target's IP address: 137.74.187.153

IP: 137.74.187.153
Organisation: OVH SAS
Operating System: : None
Country: France

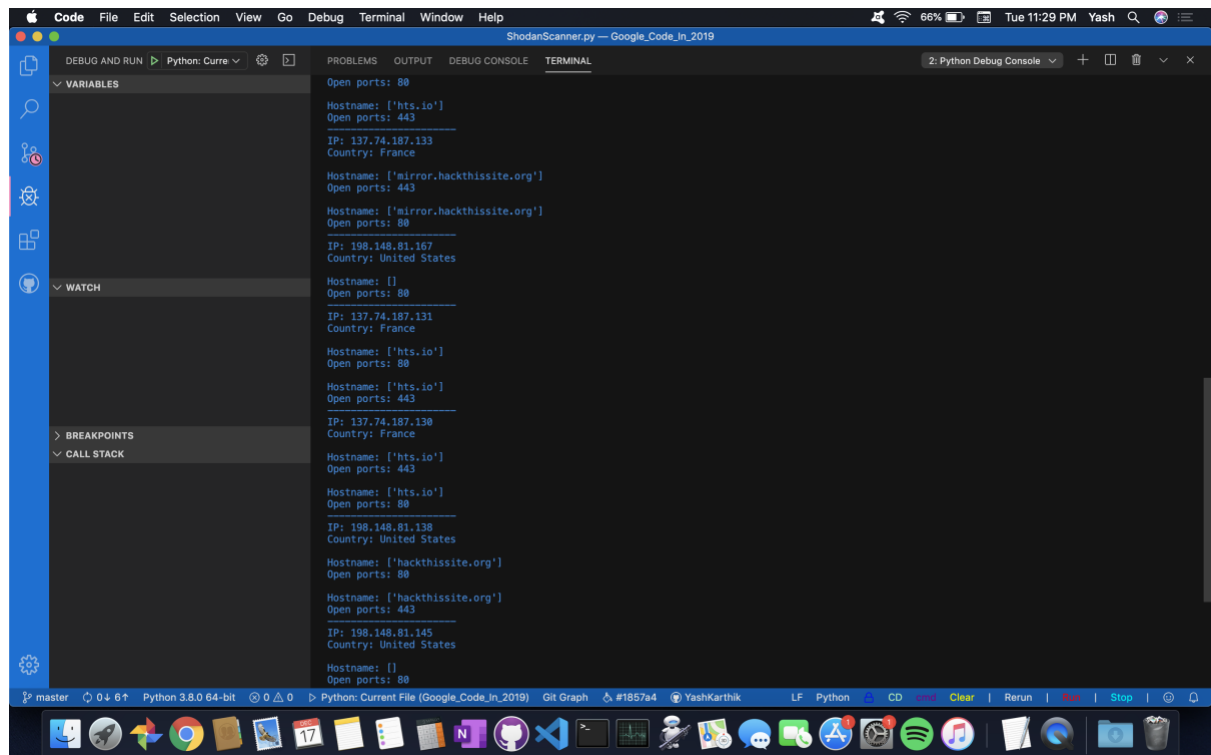
Hostname: ['www.irc.hackthissite.org']
Open ports: 80

Hostname: ['www.irc.hackthissite.org']
Open ports: 443
```

Continued running the script through VSCode.

Part 3:

Attacked the site 'hackthissite' using hostname as user input.



```
ShodanScanner.py — Google_Code_In_2019
DEBUG AND RUN Python: Current File (Google_Code_In_2019)
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 2: Python Debug Console
VARIABLES
WATCH
BREAKPOINTS
CALL STACK
Open ports: 80
Hostname: ['hts.io']
Open ports: 443
IP: 137.74.187.133
Country: France
Hostname: ['mirror.hackthissite.org']
Open ports: 443
Hostname: ['mirror.hackthissite.org']
Open ports: 80
IP: 198.148.81.167
Country: United States
Hostname: []
Open ports: 80
IP: 137.74.187.131
Country: France
Hostname: ['hts.io']
Open ports: 80
Hostname: ['hts.io']
Open ports: 443
IP: 137.74.187.130
Country: France
Hostname: ['hts.io']
Open ports: 443
Hostname: ['hts.io']
Open ports: 80
IP: 198.148.81.138
Country: United States
Hostname: ['hackthissite.org']
Open ports: 80
Hostname: ['hackthissite.org']
Open ports: 443
IP: 198.148.81.145
Country: United States
Hostname: []
Open ports: 80
```

Since I was running the script through VSCode I didn't use a separate command to perform the attacks.