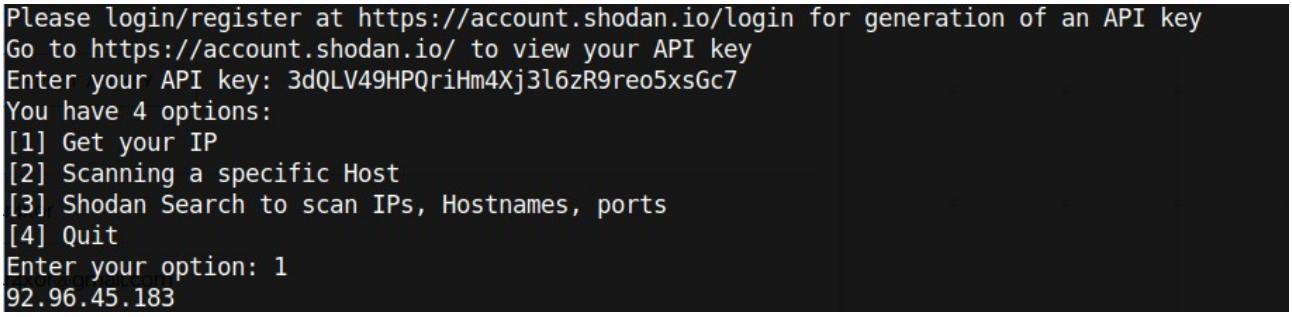
Create your own Shodan scanner for your terminal

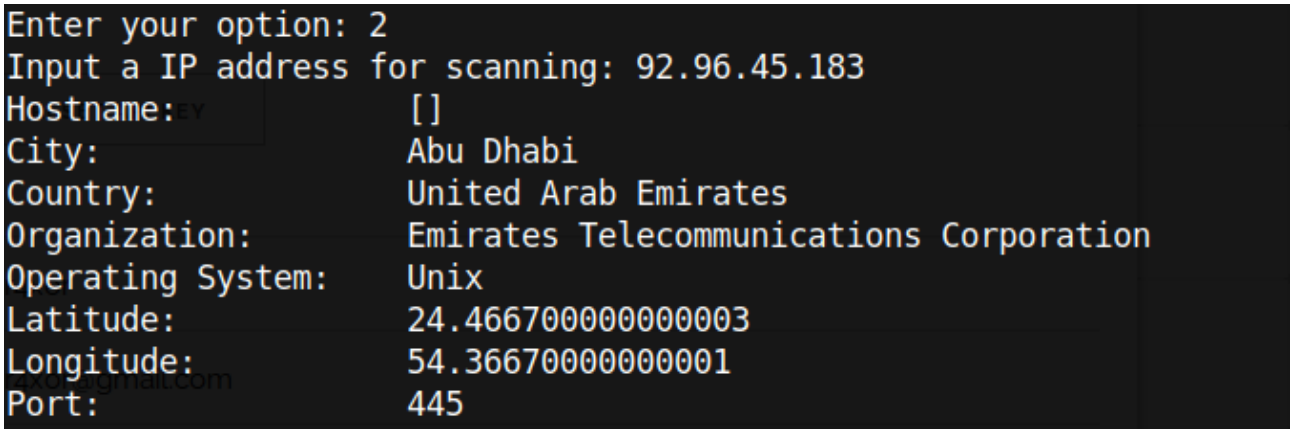
Attack 1: Get your IP



Code:

```
if option == 1:
        ip = api.tools.myip()
        print(ip)
```

Attack 2: Scanning a specific host



Code:

```
elif option == 2:
        host_ip = input("Input a IP address for scanning: ")
        scan = api.host(host_ip, history=True)
        print("Hostname: ", " "*9, scan['hostnames'])
        print("City: ", " "*13, scan["city"])
        print("Country: ", " "*10, scan["country_name"])
        print("Organization: ", " "*5, scan["org"])
        print("Operating System: ", " "*1, scan["os"])
        print("Latitude: ", " "*9, scan["latitude"])
        print("Longitude: "," "*8, scan["longitude"])
        print("Port: ", " "*13, scan["data"][0]["port"])
```

Attack 3: Shodan Search to scan IP, Hostnames, ports

```
Enter your option: 3
Query to be searched: fedora
+-----------------+------+-----------------------------------------------+
|        IP       | Port |                  Organization                 |
+-----------------+------+-----------------------------------------------+
|   121.201.0.37  | 9001 |             China Telecom Guangdong           |
|  212.142.253.59 |  80  |                  Euskaltel S.A.               |
|  173.0.186.241  |  80  |                  Techie Hosting               |
|   80.96.120.30  |  80  | Institutul National de Cercetare-Dezvoltare in inf |
|  137.122.89.28  |  80  |               University of Ottawa            |
|  217.13.199.48  |  80  |       Speedbone Internet & Connectivity GmbH  |
|  162.197.254.10 |  80  |              AT&T Internet Services           |
|  183.87.255.42  |  80  |               P4networks pvt ltd.             |
|  78.129.244.229 |  80  |              Iomart Hosting Limited           |
|  173.0.181.241  |  80  |                  Techie Hosting               |
|  41.65.116.133  | 143  |                  Etisalat Misr                |
|  45.251.113.120 | 110  |                    Superdata                  |
| 104.236.234.153 |  80  |                  Digital Ocean                |
|   94.32.67.60   |  80  |                   Tiscali SpA                 |
| 150.243.160.168 | 873  |              Truman State University          |
|   81.210.86.85  | 8080 |                     Netia SA                  |
|   52.87.67.102  |  80  |                    Amazon.com                 |
|   174.3.230.0   |  80  |               Shaw Communications             |
|  216.235.239.31 | 110  |            Kinex Networking Solutions         |
|  60.217.101.68  | 8090 |              China Unicom Shandong            |
|  129.110.131.21 |  80  |          University of Texas at Dallas        |
| 189.123.111.228 | 995  |                    NET Virtua                 |
|  204.8.224.243  | 8080 |              Beehive Broadband, LLC           |
| 180.131.125.196 |  80  |                     freebit                   |
|   195.83.197.3  | 993  |          Universite Toulouse 1 Capitole       |
|   93.87.71.26   |  80  |                  Telekom Srbija               |
|   69.61.92.132  |  80  |                  Cyber Wurx LLC               |
|  129.7.128.190  |  80  |               University of Houston           |
|   188.130.33.9  |  80  |  CTS Computers and Telecommunications Systems SAS |
|   45.79.68.47   |  80  |                     Linode                    |
|  35.177.148.63  |  80  |              Amazon Data Services UK          |
```

This image is not complete, but you get the idea :)

Code:

```
elif option ==3:
        search = input("Query to be searched: ")
        scan = api.search(search)
        x = PrettyTable()
        x.field_names = ["IP", "Port", "Organization"]
        for i in scan['matches']:
            a = i['ip_str']
            b = i['port']
            c = i['org']
            x.add_row([a,b,c])
        print(x)
```