15. API de shodan

Friday, October 9, 2020 4:31 PM

Shodan es un motor de búsqueda que se encarga de rastrear servidores y diversos tipos de dispositivos en Internet, extrayendo información útil sobre los servicios que se encuentran en ejecución en dichos objetivos.

Shodan no busca contenido web, sino que busca entre las cabeceras de las peticiones HTTP información sobre el servidor.

Shodan API key

Para usar su API requerimos una key, la cual podemos obtener al registrarnos en su sitio web: https://www.shodan.io/ y, para acceder a su documentación, podemos consultar: https://developer.shodan.io/.

Shodan y python

```
C:\WINDOWS\system32>pip install shodan
Collecting shodan
  Downloading shodan-1.23.1.tar.gz (49 kB)
     |                                | 49 kB 786 kB/s
```

```
>>> import shodan
>>> api = input("API key: ")
API key: sL4Vr0TrxYsCWk1N20hQHRJI[redacted]
>>> shodan = shodan.Shodan(api)
>>> buscar = input("termino a buscar: ")
termino a buscar: smtp
>>> resultados = shodan.search(buscar)
>>> type(resultados)
<class 'dict'>
>>> resultados
Squeezed text (8758 lines).
>>> resultados.keys()
dict_keys(['matches', 'total'])
>>> resultados['total']
305434
>>> type(resultados['matches'])
<class 'list'>
>>> len(resultados['matches'])
100
>>> resultados['matches'][0]
{'hash': -587287131, 'ip': 1653575716, 'isp': 'QuadraNet', 'transport': 'tcp', 'data': '421
Too many concurrent SMTP connections; please try again later.\r\n', 'asn': 'AS8100', 'port':
25, 'hostnames': [], 'location': {'city': 'Los Angeles', 'region_code': 'CA', 'area_code': N
one, 'longitude': -118.2641, 'country_code3': None, 'latitude': 34.0494, 'postal_code': None
, 'dma_code': 803, 'country_code': 'US', 'country_name': 'United States'}, 'timestamp': '202
0-10-09T21:41:13.052792', 'domains': [], 'org': 'QuadraNet', 'os': None, '_shodan': {'crawle
r': '82488cbcb7dd25da13f728d04775390417d9ee4e', 'ptr': True, 'id': '2f684eec-68b5-4e25-9e5e-
8e2ba96a8fcb', 'module': 'smtp', 'options': {}}, 'ip_str': '98.143.144.36'}
```

Buscando servidores FTP

FTP es un protocolo usado para transferir archivos, el cual tiene un servidor que permite almacenar ahí archivos para que los clientes se conecten y descarguen archivos.

En algunas ocasiones, los administradores de dichos servidores no los configuran correctamente, lo que implica que el servidor no requiere usuario y password para ingresar.

```
import shodan
sites = []
api_key = "sL4Vr0TrxYsCWk1N20hQ[redacted]
objShodan = shodan.Shodan(api_key)
resultados = objShodan.search("port: 21 Anonymous user logged in")
print("Numéro de hosts encontrados: ", len(resultados['matches']))
for match in resultados['matches']:
    if match['ip_str'] is not None:
```

```
        print(match['ip_str'])
        sites.append(match['ip_str'])
```

Ln: 11 Col

Python 3.8.5 Shell

File Edit Shell Debug Options Window Help

```
= RESTART: C:/Users/marle/Downloads/book-attachment-3744/CODIGO_PYTHON/TEMA4/SHODAN/serverFTP.py
Numéro de hosts encontrados:  100
173.254.19.104
193.230.8.54
50.87.68.33
162.243.172.155
50.87.195.231
69.195.121.209
24.173.231.190
69.195.114.111
51.89.95.111
49.50.96.104
209.59.131.194
50.87.169.139
134.119.112.239
67.20.92.20
46.252.28.22
```

OJO: El que aparezcan las IP no implica que directamente podamos ingresar al sistema FTP, pero si nos indica una posible vulnerabilidad en ese servidor.