

Shodan Command Sheet

To register for a free account: <https://www.shodan.io/>

- Quick and easy and will be required for the presentation.

IMPORTANT: First make sure you are running your system as “root”

Set up install and initialization:

Shodan install

```
pip install shodan
```

Shodan initialization

```
shodan init (API Key)
```

Command Line Interface (CLI) Commands:

count: Returns the number of results for a search query.

```
shodan count microsoft iis 6.0
```

download: this command is what you should be using most often. It lets you save the results and process them afterwards using the parse command.

```
shodan download microsoft-data microsoft iis 6.0
```

parse: to analyze a file that was generated using the download command. It lets you filter out the fields that you're interested in, convert the JSON to a CSV and is friendly for pipe-ing to other scripts

```
shodan parse --fields ip_string,port,org --separator , microsoft-data.json.gz
```

host: See information about the host such as where it's located, what ports are open and which organization owns the IP.

```
shodan host 189.201.128.250
```

myip: Returns your Internet-facing IP address

```
shodan myip
```

search: This command lets you search Shodan and view the results in a terminal-friendly way. By default it will display the IP, port, hostnames and data. You can use the **--fields** parameter to print whichever banner fields you're interested in.

```
shodan search --fields ip_string,port,org,hostnames microsoft iis 6.0
```

References/Additional Reading

Complete Guide to Shodan: <https://leanpub.com/shodan>

Shodan – Search Engine For Hackers – Beginner Guide: <https://hsploit.com/shodan-search-engine-for-hackers-beginner-guide/>