

Forum:[Hack Forums](#)

Thread: [Shodan Cheat Sheet for Penetration Testing](#)

#AfterDark - August 21, 2024, 5:26 pm

Before I start nmap and light up my targets firewall like a Christmas tree, I tend to go with the route of passive-recon. Here is a tool I often use.

Shodan is a search engine for Internet-connected devices. It can be used to discover which of your devices are connected to the Internet, where they are located, and who is using them.

Also on a side note: If you attend a CyberSecurity related college you can get a student acct for free with access to the API.

Website: <https://shodan.io/>

Here's how to use Shodan for penetration testing:

Basic Commands

Search for devices using a simple query

Code shodan search apache

Count the number of results for a query

Code shodan count microsoft iis 6.0

Searching by Filters

Use filters to refine your searches:

Code shodan search city:"Las Vegas" apache - Country -

shodan search country:"US" camera - Geo (latitude/longitude) -

shodan search geo:"50.3,8.25" - Hostname -

shodan search hostname:"example.com" - Net (network range) -

shodan search net:192.168.0.0/24 - OS (operating system) -

shodan search os:"windows 7" - Port - shodan search port:80

Advanced Search Techniques

Combine filters

Code shodan search country:"DE" port:21 "anonymous ftp"

Search for vulnerabilities

Code shodan search vuln:CVE-2024-36840

Using Shodan to Monitor Specific Systems or Assets

Set up alerts for specific termsCode shodan alert create "Name of Alert" "port:22 country:US"

List all your created alertsCode shodan alert list

Remove an alertCode shodan alert remove [ALERT ID]

Command-line Interface (CLI) Features

Download search resultsCode shodan download myresults apache

View downloaded dataCode shodan parse --fields ip_str,port,org,hostnames myresults.json.gz

Generate a report from downloaded dataCode shodan stats --facets port:top10 myresults.json.gz

Reconnaissance on Companies for Bug Bounties

Identify technology footprintCode shodan search org:"Example Company"

Find exposed databasesCode shodan search org:"Example Company" product:"MongoDB"

Locate vulnerable systemsCode shodan search org:"Example Company" vuln:cve-2022-0001

Monitor for new devicesCode shodan alert create "New Devices at Example Company"
"org:'Example Company'"

This cheat sheet provides a foundation for using Shodan in penetration testing and security assessments, with specific strategies for conducting company-specific reconnaissance for bug bounties. I utilize it quite frequently during my recons. The shodan API is prty neat too and I would recomend checking that out as well.

ham_flavred_licorice - September 20, 2024, 9:55 pm

New to this but def gonna check this out. Thank you

utk_1310 - October 28, 2024, 12:02 pm

Thank You! Very helpful resource.

Big Dong - November 2, 2024, 4:53 pm

Thank you for sharing - this is really great information!

jellyhat - November 4, 2024, 3:52 am

great share, shodan is very handy if you know how to use it, thanks and waiting for next part ;)

m0narch - November 10, 2024, 11:22 am

Any chance you got one for FOFA?

#AfterDark - November 12, 2024, 7:21 pm

(Nov 10, 2024 12:22 PM)m0narch Wrote: [\[CITE\]](#) Any chance you got one for FOFA?
Sorry I do not, I ussuly rely on shodan mostly. The api is prty neat.

Havent used FOFA to be honest. any good?

m0narch - November 18, 2024, 8:08 am

(Nov 12, 2024 08:21 PM)#AfterDark Wrote: [\[CITE\]](#) Sorry I do not, I usually rely on Shodan mostly. The api is pretty neat.

Havent used FOFA to be honest. any good?

It can filter out honeypot IPs and also has several more options for querying as well as better pricing for users who don't want to spend \$\$\$ - \$\$\$\$ per month for whatever they're using the service for. If you need unlimited results a month though... Shodan would be your best bet then. But FOFA is definitely better in terms of cheaper for consumers who don't want to go broke to get results. I think you still get 100,000 results a month the \$25/month plan. Though it's not as good as Shodan if you're trying to get 1,000,000+ results a month.