Shodan Query Lab

An Internet connection is necessary, this is a homework assignment. Take the usual precautions (re: patches, firewalls, least privilege, etc.) before venturing onto the Internet.

Clicking on links Shodan provides is not advised.

Additional information:

Find/Read: schearer-shodan.pdf

Title: SHODAN-for-Penetration-Testers

The Shodan database is a reasonable subset of the Internet.

Shodan Query Lab

The Tool: http://www.shodanhq.com/

Click on ‘Learn More’ and **read** the User Guide

Start with a simple search

Observe search results, refine via optional search parameters, including:

- **country: 2-letter country code**
- hostname: full or partial host name
- net: IP range using CIDR notation (ex: 18.7.7.0/24)
- port: 21, 22, 23 or 80

- FireFox add-in’s are available
- Most of the search functions can be used w/o registering at the site
- Registration provides additional features, is free

Shodan Queries

Example: http://www.shodanhq.com/?q=ADSL+port%3A80 (as a URL)

- q=ADSL+port:80 (as above but using Shodan’s form for entry)
- q=cisco-IOS (q=cisco+ios hostname:some.domain)
- q=IIS+4.0 q=IIS+6.0 q=IIS+5.0 ref: http://milw0rm.com/exploits/9541
- q=Fuji+xerox
- q=JetDirect
- q=port:23+“list+of+built-in+commands”
- q=port:80+iisstart.html
- q=Server: SQ-WEBCAM
- q=“Anonymous+access+allowed”
- q=“X-Powered-By:+PHP”
- q=Default+Password
- q=vFTPd+1.31 ref: http://www.exploit-db.com/exploits/11293
- q=PowerDNS ref: http://www.securityfocus.com/bid/37650
- q=nnCoection
- q=Cneonction

Shown here is a way to make searches via an absolute query. When searching from the site page omit the 'q='.

Shodan Queries

More sample queries

- http://www.shodanhq.com/?q=xerox+port%3A80
- http://www.shodanhq.com/?q=DD-WRT
- magicjack
- EIG embedded web server (Smart Meter)
- TRMB 401 (Trimble GPS receivers)

- Similar to many of the google hacking searches, most of the queries have a 'half-life' once they become known.

Shodan Query Lab

The lab exercise is to explore Shodan. Begin with the queries provided, try options, then combine and explore. Look at the results provided and consider the potential. Note the geolocation and summary numbers provided. The queries listed are there for a reason, you don't need to try all of them. Some may no longer be useful. Start by picking one and think about what the query could reveal. What do the results show? Several queries + results are provided. Google for Shodan queries and other material. GIYF.

Teamwork may yield synergy. Spend at least 30 minutes using Shodan.

- Objective:

  Turn in .5 to one page - on two things you learned from using Shodan that interested you, and why. Your response can be site specific, broad, abstract, technical, philosophical, etc.

- Optional Objectives (extra credit):
  - Create an interesting Shodan query specific to UOP (or similar, e.g. a narrow search local to the area).