Censys Search Cheat Sheet

by himajedi via cheatography.com/196419/cs/41272/

IP Addresses and Subnets

Single IP (*supports IPv4 and IPv6*)	8.8.8.8 or ip:8.8.8.8
Subnet by CIDR	ip: "23.0.0.0/8"
Subnet by IP Range	ip: [1.12.0.0 to 1.15.255.255]
Hostname	dns.names:"*.zip"
Autonomous System # (ASN)	autonomous_system.asn:16509
Autonomous System Name	autonomous_system.name:"AMAZON-02"
IPv6 hosts	ip: "2001::/3" or labels:ipv6

Ports, Protocols, and Software

Port	services.port:22 services.port:{20,21,22}
Service / Protocol	services.service_name:SSH
Transport protocol	services.transport_protocol:TCP
Software by product and/or vendor	services: (software.vendor:"Apache" AND software.product:"HTTPD")
Software by URI / CPE	services.software.cpe =`cpe:2.3:o:mikrotik:routeros:*:*:*:*:*:*:*:*`
Banner grab	services.banner:"HTTP/"
Device type	services.software: (other.key:"Device" and other.value:"Router")
Number of open ports on host	service_count: [1 to 20]

Geography

Country	location.country:"United States"
City	location.city:"Ann Arbor"
State	location.province:"Michigan"
GPS Coordinates	(location.coordinates.latitude=41.85003 AND location.coordinates.longitude=-87.65005)

Pro tip: Use Map To Censys to draw a box over the geographic area of interest and click “Open in Search” to see hosts in the area

Labels

search by label	labels:`<la bel -na me>`

Labels provide broad context about a host or service. **Some useful host labels:** c2, login-page, open-dir, ics, network.device, cryptocurrency, managed-file-transfer, ipv6, tarpit, honeypot.

Handy Censys Search CLI JQ filters

List of IP addresses	'.[].ip'
Banners	'.[] | .ip as $ip | .services[] | [$ip, .transport_protocol, .port, .service_name, .banner]'

Usage: `censys search <qu ery> | jq <fi lte r>`

Web Entities (HTTP/S)

HTML Title	services.http.response.html_title:"dashboard"
Response Body - plaintext or hash	services.http.response.body:"login" or services.http.response.body_hashes:*
Status code	services.http.response.status_code=200
Server header	services.http.response.headers: (key: `Server` and value.headers: `nginx`)
Certificate Issuer	services.tls.certificates.leaf_data.issuer.organization:"Let's Encrypt"
Certificate Subject Common Name	services.tls.certificates.leaf_data.subject.common_name:`*.hero kua pp.com`
TLS version (*Highest negotiated version*)	services.tls.version_selected:"TLSv1_1"
Favicon MD5 Hash	services.http.response.favicons.md5_hash:*
Favicon Shodan Hash (mmh3)	services.http.response.favicons.shodan_hash:*

Use Case Examples	
Hacked web servers	services: (service_name:"HTTP" and http.response.html_title:"hacked by")
Hosts serving login pages with port 22 open	services.port:22 and labels:`login-page`
Servers in Russia running remote access protocols	location.country:"Russia" and labels:`remote -access`
Filter out hosts with 100+ ports open	services.truncated: false
Compromised MikroTik routers	services.service_name: MIKROTIK_BW and "HACKED"
Filter out honeypots and noisy hosts	not labels:{'honeypot', 'tarpit', 'truncated'}
RDP running on nonstandard ports	services: (service_name="RDP" and NOT port=3389)

Pro tip: Get more results by including virtual hosts -- click the gear icon and toggle **Virtual Hosts: `INCLUDE`**

Certificates	
Unexpired certificates for a specific domain	labels=`unexpired` and names: censys.io
Self-signed certificates observed in Censys host scans	ever_seen_in_scan: true and labels: "self-signed"
Trusted certs from a specific CA expiring on specific day	parsed.issuer.organization: "Let's Encrypt" and labels: "trusted" and parsed.validity_period.not_after: 2023-10-13

Learn more about the data collected in our certificates dataset: https://search.censys.io/search/definitions?resource=certificates