Ethical Hacking and Countermeasures
Shodan Cheat Sheet

Shodan
Source: https://www.shodan.io

Shodan is a search engine for Internet-connected devices. It is a great resource to provide passive reconnaissance on a target. It also provides a public API that allows other tools to access all the Shodan's data

1. General Filters

Filter	Description
after	Only show results after the given date (dd/mm/yyyy) string
asn	Autonomous system number string
before	Only show results before the given date (dd/mm/yyyy) string
category	Available categories: ICS, malware string
city	Name of the city string Example: cisco city:"New York"
country	The 2-letter country code string Example: webcamxp country:"US"
geo	Accepts between 2 and 4 parameters. If 2 parameters: latitude, longitude. If 3 parameters: latitude, longitude, range If 4 parameters: top left latitude, top left longitude, bottom right latitude, bottom right longitude Example: Webcamxp geo:" -50.81,201.80"
hash	Hash of the data property integer
has_ipv6	True/ False boolean
has_screenshot	True/ False boolean
hostname	The full hostname for the device string
ip	Alias for net filter string
isp	ISP managing the netblock string
net	Network range in CIDR notation (ex. 199.4.1.0/24) string
org	The organization assigned the netblock string
os	Operating system string
port	Port number for the service integer Example: https port:443
postal	Postal code (US-only) string
product	Name of the software/ product providing the banner string
region	Name of the region/ state string
state	Alias for region string
version	Version for the product string
vuln	CVE ID for a vulnerability string Example: vuln:cve-2014-0160

2. HTTP Filters

Filter	Description
http.component	Name of web technology used on the website
http.component_category	Category of web components used on the website
http.html	HTML of web banners
http.html_hash	Hash of the website HTML
http.status	Response status code
http.title	Title for the web banners website Example : title:"+tm01+" has_Screenshot:true

3. NTP Filters

Filter	Description
ntp.ip	Domain Brute Force Enumeration
ntp.ip_count	Number of IPs returned by initial monlist
ntp.more	True/ False; whether there are more IP addresses to be gathered from monlist
ntp.port	Port used by IP addresses in monlist

4. SSL Filters

Filter	Description
has_ssl	True / False
ssl	Search all SSL data
ssl.alpn	Application layer protocols such as HTTP/2 ("h2")
ssl.chain_count	Number of certificates in the chain
ssl.version	Possible values: SSLv2, SSLv3, TLSv1,TLSv1.1, TLSv1.2
ssl.cert.alg	Certificate algorithm
ssl.cert.expired	True / False
ssl.cert.extension	Names of extensions in the certificate
ssl.cert.serial	Serial number as an integer or hexadecimal string
ssl.cert.pubkey.bits	Number of bits in the public key
ssl.cert.pubkey.type	Public key type
ssl.cipher.version	SSL version of the preferred cipher
ssl.cipher.bits	Number of bits in the preferred cipher
ssl.cipher.name	Name of the preferred cipher

5. Telnet Filters

Filter	Description
telnet.option	Search all the options
telnet.do	The server requests the client do support these options
telnet.dont	The server requests the client to not support these options
telnet.will	The server supports these options
telnet.wont	The server does not support these options

6. Shodan Search Filters Examples

Filter	Description
voIP	For footprinting VoIP
VPN	For footprinting VPN
linux upnp avtech	For exploiting cams
netcam	For exploiting netcam
"default password"	For Default Passwords
iis source:ExploitDB	To find exploits for various os, servers, platforms, applications etc present on ExploitDB or Metasploit
netgear port:80	To find Netgear devices
Android Webcam Server-Authenticate	To find android webcam server
port:8333	To find Bitcoin server
Server:Thin-3.2.11-3.1.10-3 .0.19-2.3.15	Ruby on Rails Vulnerable Server(CVE-2013-0156 and CVE-2013-0155)
Jetty 3.1.8(Windows 2000 5.0 x86)"200 OK"	DNSSEC zone walk with standard enumeration
port:5353	To find DNS service
iRidium	To search for vulnerable ICS systems
port:502	To Search for Modbus enabled ICS/SCADA systems:
"Schneider Electric"	Search for SCADA systems using PLC name
TM221ME16R	To detect Schneider Electric TM221 PLCs connected to the Internet
SCADA Country:"US"	Search for SCADA systems using geolocation
port:20000	To Search for ICS-specific protocol DNP3