# OPEN SOURCE TOOLS AVAILABLE TO ASSESS RISKS TO INTERNET FACING ICS

## Search Engines

Search engines on the Internet today are powerful software tools that crawl and categorize massive amounts of information. Search engines like Google, Bing, etc., continue to increase the speed at which they can "crawl" the Internet and the types of data they can consume and categorize. Today these search engines consume and create metadata on web pages, various document files, videos, and images among others.

### "Google Hacking"

"Google Hacking" is the common term for using a search engine (Google, Bing, etc.) with certain search modifiers to narrow the scope of the data returned. Narrowing the data returned allows for more detailed analysis and an increased chance of finding valuable information. This valuable data can then be used to find sensitive information about an entity, aid in finding weak or otherwise exploitable devices, or increase the ability for an adversary to gain more access.

### Search Engine Resources

There are many resources available to assist in advanced search engine use; just Google it. Most of the search commands listed here will work across various search engines; however, if one does not work, there may be a slight syntax difference required by that search engine. Many of the commands can be combined together to maximize your searching potential.

### Commands and Descriptions

| Operator | Purpose |
|---|---|
| site: | Searches only a specific site for matching content. |
| filetype: | Searches for files with the matching file type. |
| intitle: | Searches the page title for the text specified. |
| allintitle: | Searches the page title for all the text terms provided. |
| inurl: | Searches within the URL for matching text. |
| allinurl: | Searches with the URL for all the matching text terms. |
| allintext: | Searches the content of the page for all the matching text terms provided. |
| link: | Searches for sites that point to the link site. |
| cache: | Searches for cached versions of a web page. (Google Only) |
| + or - | Forces a search engine to include or exclude the given search term. |

NCCIC

National Cybersecurity and Communications Integration Center

## Shodan

Shodan (www.shodan.io) has become one of many popular search engines that specialize in searching for electronic devices connected to the Internet. Shodan searches the entire Internet address space and captures information on each device it finds. This information can include IP addresses, ports, banner messages, location, images from web cams, devices supporting remote desktop, etc. Shodan includes the capability to search its database of devices to find specific devices including servers, desktop and laptop computers, and critical infrastructure to include PLCs, HMIs, etc.

### Shodan Resources

Similar to traditional search engines, Shodan has a number of search commands that allow for the filtering of data. Shodan has a number of additional offerings that allow for easy mapping of data found, including an API for integration with custom applications, an image search tool, a Maltego add-on, and several others. Many of the Shodan features can be used free of charge while others do require purchase on either a one time or recurring basis.

### Shodan Filters

Filters are search modifiers in Shodan that allow for narrowing down the search dataset to find specific devices. Many of them can be used together to increase the searching capability.

| Operator | Purpose |
|---|---|
| Port: | Filters based on port provided. |
| Country: | Searches for a specific country, using a 2-letter code. Ex. US. |
| Net: | Searches a network block using CIDR notation. |
| Hostname: | Searches for matching Hostnames. |
| OS: | Searches based on the provided operating system. |
| City: | Searches a specific city. |
| Geo: | Searches specific coordinates. |
| Before/After: | Searches within a timeframe. |
| Product: | Finds specific product(s). |
| Version: | Displays certain version(s). |

## About ICS-CERT

The Industrial Control Systems Cybersecurity Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors.

www.ics-cert.us-cert.gov

## About NCCIC

The National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.

http://www.dhs.gov/national-cybersecurity-communications-integration-center