PIVOTS X PAYLOADS

SIMULATE A FULL-SCALE HIGH-VALUE PENETRATION TEST

SANS

www.sans.org/boardgame

# RECONNAISSANCE


**Contributors: Shodan**
JOSHUA WRIGHT @joswr1ght
JEFF MCJUNKIN @jeffmcjunkin

**Contributors: Google Dorks**
MIKE MURR @mikemurr
JOSHUA BARONE @tygarsai


## Shodan.io

***The search engine for security***

Shodan is the world's first search engine for Internet-connected devices.

https://www.shodan.io

**Shodan Search Operators:**
To perform more advanced searches using Shodan, apply search operators. Search operators are only available to registered users. It's free to create an account, which will also give you an API key for use with Shodan's command-line tool.

Once you are logged in, you can apply additional search modifiers to focus your search.

| | |
|---|---|
| **title:** | Search the content scraped from the HTML tag |
| **html:** | Search the full HTML content of the returned page |
| **product:** | Search the name of the software or product identified in the banner |
| **net:** | Search a given netblock (example: 204.51.94.79/18) |
| **version:** | Search the version of the product |
| **port:** | Search for a specific port or ports |
| **os:** | Search for a specific operating system name |
| **country:** | Search for results in a given country (2-letter code) |
| **city:** | Search for results in a given city |

Some filters allow multiple values, such as "postal:97201,97202".

## Google DORKS!

*Google dorking is a computer hacking technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites use.*

### Advanced Operators

There are many similar advanced operators that can be used to exploit insecure websites:

site:

site:sans.org site:www.sans.org

Restricts the search to a specific domain

site:sans.org -site:www.sans.org

Can also be combined with not operator to leave out specific sub-domains

PEN TEST EXAMPLE:

site:target.tgt “at least” “characters long” password

Search target.tgt for password policies (useful for password guessing)

site:target.tgt “employee directory”

Search target.tgt for an employee directory (useful for social engineering)

“@target.tgt” “Password1”

Search for password dumps containing email addresses from target.tgt

intitle:

Looks for keywords in the title of a page

PEN TEST EXAMPLE:

intitle:”Index Of”

This example looks for default configurations where directory listing is turned on, which can leak sensitive data, or data that can be used for other attacks

intitle:”admin”

Use to look for possible unlisted administration panel pages

inurl:

This looks for keywords that appear in the url

PEN TEST EXAMPLE:

inurl:admin

This looks for possible unlisted administration panel pages

filetype:

Looks for files with specific extensions

PEN TEST EXAMPLE:

filetype:xlsx

Look for Excel spreadsheets that might be exposing sensitive data (also xls, doc, docx, etc.)