Recently, there is a lot of buzz about the SHODAN search engine. It has even been called 'the scariest search engine on the internet'. Being used by white hat and black hat hackers alike to find vulnerable systems on the internet, it's essential for Penetration Tester's to try this unique search engine.

SHODAN is the Google for Hackers. It is known as the Scariest Search engine on the web, exposing loads of routers, servers, webcams, SCADA systems, and other network devices. Here we explore the capabilities of SHODAN.

Basically, SHODAN grabs banners from online devices on the internet. It interrogates ports and stores resulting banners. These Banners are then indexed for searching. So sometimes we may see some devices listed in SHODAN searches that are no longer present. This is because they may have been indexed a while ago and do not exist now.

Figure 1. SHODAN Main Page

Figure 2. The SHODAN Search
Based on the information revealed in the banners, hackers decide how to proceed with the attack. Attacks vary a lot, ranging from trying default passwords for particular devices to triggering specific vulnerabilities. However, the role of SHODAN ends at 'exposing online devices'. How one exploits the vulnerabilities in those devices is up to him/her. Typically the banners reside on port 80 but they may be on other ports as well.

SHODAN search is not exactly your friendly Google search. In order to get the maximum out of it, it’s recommended that you have an understanding of 'Banner Grabbing'. 'Banners' are welcome screens that reveal important information about the software version number and other system information.

Searching in SHODAN

The search query along with the filters and Boolean operators can be entered right into the SHODAN search bar. A simple search with a filter looks like pictured on Figure 2.

Boolean operator like +, – and | can be used in SHODAN to add or remove certain terms from the SHODAN search. Result of this search is displayed on Figure 3.

The search terms are marked in Red and we have a list of Webcams on Internet running on SQ-Webcam software.

The 'Search Directory' in SHODAN is a good place to begin exploring SHODAN. It provides a glimpse into what other people are looking for on SHODAN and can provide clues to what we could be looking for. It lists 'Popular searches', 'Popular tags' and 'Recently Added' SHODAN searches.

Refining SHODAN Search with Filters

Shodan offers various filters to aid our search. The common ones are mentioned in the table below:

<table>
<thead>
<tr>
<th>Filter</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country</td>
<td>Search devices located in a given Country</td>
</tr>
<tr>
<td>City</td>
<td>Search devices located in a given City</td>
</tr>
<tr>
<td>Geo</td>
<td>Search for devices in given latitude/longitude</td>
</tr>
<tr>
<td>Hostname</td>
<td>Search for a given value in hostname</td>
</tr>
<tr>
<td>Net</td>
<td>Search specific IP address or subnet</td>
</tr>
<tr>
<td>Port</td>
<td>Search for specific ports (21, 23, 80 etc.)</td>
</tr>
<tr>
<td>OS</td>
<td>Search for specific Operating Systems</td>
</tr>
</tbody>
</table>

Apart from these, some other add-on Filters are available. Together, these filters can be used in combinations to narrow down the results.

Sample Attack Scenario

Penetration Tester is looking for vulnerable 'ubnt' devices on the internet. A simple 'ubnt' search in SHODAN, reveals a lot of devices displaying a banner similar to the one shown on Figure 4.

'401 Unauthorized' code tells us that we would require a password to login. A quick Google search shows us the default username:password combination for 'ubnt' devices is 'ubnt':'ubnt'.

A hacker can then easily create a script that tries such default username:password combinations
one by one on each of these devices displayed by SHODAN search engine.

According to ICS-CERT “some of the identified systems continue to use default user names and passwords and/or common vendor accounts for remote access into these systems. These default/common accounts can in many cases be easily found in online documentation and/or online default password repositories”.

After the devices are exposed, hacker could look for the online documentation of the particular device and try to locate the default factory set username:password combo. After retrieving this combination, it’s simply a matter of time before hacker stumbles upon one of the devices in the list which is using a default setting.

**Exploiting Webcams with SHODAN**

These days the most popular SHODAN search seems to be the one for webcams. Many Hackers are searching for “SERVER: SQ-WEBCAM”. These webcam servers are usually configured to use default username:password combinations and they provide the hacker with access not only to view various channels on the webcam server but also to change configuration. Figure 5 presents a webcam revealed by SHODAN that was using defaults which resulted in access to complete control over the webcam remotely over the Internet.

**Gaining access to SCADA systems using SHODAN**

A Popular Tag searched in SHODAN is SCADA (short for Supervisory Control And Data Acquisition). These are computer controlled industrial systems. SHODAN exposes these SCADA systems and if they are vulnerable, Hackers can control important industrial processes (see Figure 6).

For the developers out there, SHODAN provides proper API documentation. Libraries are available for Python, Pert and Ruby. SHODAN is now integrated with many other popular tools like Foca, Maltego, PenTBox and even the nmap scripting engine.

---

**Figure 5. Exploiting a Webcam remotely over the Internet using SHODAN search results**

**Figure 6. A SCADA system accessible over the Internet revealed by SHODAN**

**Figure 7. Setting options for the SHODAN search module**

**Figure 8. SHODAN search results**
SHODAN and Metasploit

Pen testers who work closely with the Metasploit framework, seldom like to leave the comforts of 'msfconsole'. A module for 'shodan search' is available for Metasploit which lets the user set 'query' (see Figure 7) and search for online devices from within the Metasploit framework (see Figure 8).

Who uses SHODAN?

- Security Researchers – The massive amount of data provided by SHODAN can be used as a training set that facilitates research.
- The Government – Government can use SHODAN to identify important systems like SCADA and Power plants. If vulnerability is found in these systems then they contact the Network Administrators to hopefully get a shutdown before a malicious hacker gets to it.
- Curious People – There is a lot of people accessing SHODAN everyday just to see what is out there. They may try to look for open webcams just to have a glance.
- Hackers – They look for vulnerable devices over the Internet and exploit them for personal gain.

Protection Against Shodan

Both White Hat and Black Hat Hackers are continuously searching for vulnerable devices over SHODAN. White Hat Hackers are looking to patch such systems and Black Hats would 'own' such devices and use them later for malicious purposes. Protection against such exposure is essential.

Here are some recommendations...

- Change the system defaults – The importance of this cannot be stressed enough. Devices using defaults are easiest targets for hackers since they take little to no effort to break into.
- Put Devices behind a Network Firewall – Systems should not be exposed to tampering over the internet. A firewall should stand between important systems (like SCADA) and the internet.
- Implement Lockout Policies – While attempting to Brute force devices, hackers would try to authenticate as an authorized user a number of times. Lock out Policies ensure that devices lock out after a fixed number of attempts. This foils the Brute Force attempts.
- Remote access only over VPN – VPN is a secure way of remotely accessing devices over the internet. Devices should only be available for remote access over the VPN channel.
- Customize Banners – SHODAN search depends on Banner Grabbing. Make sure that your Banners are not giving out any useful information to potential attackers over the Internet.

Summary

This is what SHODAN’s founder John Matherly has to say about SHODAN “It’s not Google, it’s not easy. It took a while for people to get a hang of searching on SHODAN and now they are able to find all sorts of interesting devices on SHODAN. You are actually not afraid of SHODAN, you’re afraid of what SHODAN is able to find. For example Power plants, the problem is not that SHODAN search revealed a power plant, the problem is that someone put a power plant control over the Internet without authentication.”

SHODAN can be an aid to both white hat and black hat hackers. Its job is simply to reveal what is out there. Whether this information is used for Securing devices or penetrating them for malicious purposes, depends on an individual. SHODAN is definitely not the enemy; it provides a glimpse into how devices are lining up over the Internet for remote access. SHODAN acts like a warning to vulnerable devices and the warning should be heeded before it is too late.

PRANSHU BAJPAI

Pranshu Bajpai is a Computer Security Professional and White Hat Hacker. He is completing his Master’s in Information Security from the Indian Institute of Information Technology. Currently he is also working as a Penetration Tester on a Counter-Hacking Project in a Security Firm in Delhi, India.

On the Web