Searching Shodan For Fun And Profit

Sajal Verma
SEARCHING SHODAN FOR FUN AND PROFIT

Author: Sajal Verma   @sajalpentest (sajalverma007786@gmail.com)

Abstract:

This paper act as a guide for penetration testers and security folks who want to use Shodan and helps them to understand how it can be used it for security auditing purposes. This paper also outlines the procedure and explains the methods to find various vulnerable services and devices located on the internet. It helps to explain the basic filters that could be used by Shodan and its integration with other tools .It can be mainly used for reconnaissance phase of penetration testing.

Introduction:

Shodan is basically a search engine which helps to find (routers, switches, Scada etc.) mainly vulnerable systems on the internet .It is widely known as Google for hackers. It was launched in 2009 by computer programmer John Matherly. It is mainly a search engine of service banners in which metadata (data about data) is sent from the server to client. Shodan currently probes for 50+ ports.

What devices can Shodan really find:

1) Servers
2) Routers
3) Switches
4) Printers on public ip
5) Webcams
6) Gas station pumps
7) Voip phones And all Scada devices  

Working of Shodan:

1) User searches for a particular item.
2) Shodan probes for ports and captures the resulting banners.
3) Now, Shodan indexes the captured banners.
4) After indexing,it displays the results.

Difference between Shodan and google:
In Google, the google crawler/spider crawls for data on the web pages and then creates an index of web content and then displays the results according to the page rank which in turn depends on a number of factors. Shodan mainly looks for ports and then grabs the resulting banners and indexes them. And finally, it displays the results. It does not index web content (the key point) like Google and thus it is a search engine of banners.

**Figure 1. Shodan search working**

1. User search
2. Probes for ports and captures resulting banners
3. Indexes the captured banners
4. Displays results

**Figure 2. Google search working**

1. User search
2. Google crawler crawls for data on web pages
3. Indexes the web content
4. Displays results according to page rank
Basic filters:

City: The ‘city’ filter is used to find devices that are located in that particular city.
Eg: iis city: New York

Country: The ‘country’ filter is used to find devices running in that particular country.
Eg: iis country: United States

Port: The ‘port’ filter narrows the search by searching for specified ports.
Eg: https port: 443

Os: The ‘os’ filter is used to find specific operating systems.
Eg: microsoft-iis os: ”windows 2003"

Geo: The ‘geo’ filter according to certain longitudes and latitudes that are within a given radius. Only 2 3 parameters are allowed and 3 parameter by default is the radius which is 5 km.
Eg: apache geo: 42.9693, -74.1224

Net: The ‘net’ filter is used to find devices according to certain ip address and subnet mask
Eg: iis net: 216.0.0.0/16

Hostname: The ‘hostname’ filter always searches host containing a particular hostname.
Eg: Akamai hostname:.com

After and Before: The ‘after’ and ‘before’ filter helps you to devices after and before a particular date. The format allowed is
dd/mm/yyyy dd-mm-yy
Eg: apache before: 1/01/2014

nginx after: 1/01/2014

Note: Most of the filters will work when you are logged in.

Shodan’s integration with other tools:

1) Integration with Maltego

Requirements: Download Maltego from
and Shodan maltego entities from https://static.Shodan.io/downloads/Shodan-maltego-entities.mtz

Usage:

i) After installing maltego, select ‘Manage Entities’ in the ‘Manage tab’ and select ‘import’.

ii) Select ‘transforms’ and then ‘advanced’

iii) Now we have to add the Shodan seed by putting https://cetas.paterva.com/TDS/runner/showseed/Shodan

iv) Finally we get a screen, the transforms and entities have been successfully installed.

It includes:

5 Transforms namely:
i) searchShodan
ii) searchShodanByDomain
iii) searchShodanByNetblock
iv) toShodanHost v) searchExploits

2 Entities namely:
i) Service
ii) Exploit

Here is a screen shot of the transform (searchShodanByDomain) performed on google.com

Note:
You can perform Shodan transforms in maltego when you have the API keys and you will get the API keys by logging into your Shodan account.

2) Integration with Metasploit

Usage:
i) Open Metasploit framework in Kali/Backtrack Box
ii.) Type `show auxiliary` in the console

```bash
msf > show auxiliary

Auxiliary
---------

Name                  Rank   Description                                           Disclosure Date
admin/ncat/nat_password reset   normal  Cross-Site Request Forgery Password Reset Vulnerability                     2007-08-15
admin/backupexec.exploit         normal  Verifying Backup Exec Windows Remote File Access                      2007-08-15
admin/backupexec.registry        normal  Verifying Backup Exec Server Registry Access                       2007-08-15
admin/cisco/cisco_secure_acs.bypass normal  Cisco Secure ACS Version 5.1.0.44.5 or 5.2.0.26.2 Unauthorized Password Change        2005-08-23
admin/cisco/wsn3000.ftp.bypass   normal  Cisco WSN3000 FTP Unauthorized Administrative Access                  2004-08-04
admin/direct/dldap2.exe          normal  J2EE D2D-LDAP2 Command Execution Vulnerabilities                        2002-01-29
admin/directory/directory_cookie  normal  Novell eDirectory Decryptable Session Cookie                        2002-01-29
admin/directory/directory_httpd   normal  Novell eDirectory Unauthenticated File Access                        2002-01-29
admin/ezweb/webdavmanager.exe    normal  EPC Application Device Manager Arbitrary Command Execution              2008-05-27
admin/ezweb/webdavmanager_repo   normal  EPC Application Library Manager Arbitrary Command Execution             2008-05-27

msf >
```

iii) Using the module `auxiliary/gather/Shodansearch`

```bash
msf > use auxiliary/gather/shodan_search
msf auxiliary(shodan_search) >

root@sjal: ~ [root@sjal ~]
```

iv) Now, we will see the parameters required by the auxiliary by using `show options`.

```bash
msf auxiliary(shodan_search) > show options
```
v.) We need to set query to IIS to search for IIS servers and the API key which we get when we log into our Shodan account. Now we execute it by the Run command.
Basically the auxiliary/gather/Shodan_search module queries the Shodan API to query the database to search for the first 50 IP addresses. The limit of 50 IP address can be increased to 10,000 IP addresses by getting unlimited API keys by purchasing it from our Shodan account.

Components of Shodan:

1) Exploits: Shodan Exploits can be used to find exploits for various os, servers, platforms, applications etc present on ExploitDB or Metasploit.

2) Maps: Shodan maps is a paid service and you need to pay for it before using. We can see the Shodan results on a map in a easy and convenient manner. It has three kind of map views namely Satellite, Street View (Light) and Street View (Dark). It can show up to 1000 results on the screen at a time.
3) **Scanhubs**: Shodan Scanhubs can be used to create an to use to create a search of raw networks scans. Scanhubs supports tools like Nmap and Masscan. To use Scanhub, we have to set the tool(nmap/masscan) to give its output in XML format and then upload it to the Scanhub repository to get the results. Unfortunately, this is also a paid component of Shodan.

**Some Test Cases:**

1) **Netgear devices**:

2) **Webcam**:

3) **Bitcoin server**:
4) Ruby on Rails Vulnerable Server (CVE-2013-0156 and CVE-2013-0155):

5) Windfarms:

6) DNS service:
Some additional cheat sheet links:

http://www.Shodanhq.com/?q=bitcoin-mining-proxy (Bitcoin proxy mining)
http://www.Shodanhq.com/search?q=port%3A11 (Systat)
http://www.Shodanhq.com/search?q=port%3A8089+splunkd (Splunk servers on tcp/8089)
http://www.Shodanhq.com/search?q=port%3A17 (Search for quote of the day)
http://www.Shodanhq.com/search?q=port%3A5632 (Vnc)
http://www.Shodanhq.com/search?q=port%3A1434 ((MS-SQL (1434))
http://www.Shodanhq.com/search?q=OpenSSL%2F1.0.1 (Servers running OpenSSL/1.0.1)
http://www.Shodanhq.com/search?q=port%3A79 (Finger protocol)
http://www.Shodanhq.com/?q=telemetry+gateway (Telemetry gateway)
**References:**


http://www.rapid7.com/db/modules/auxiliary/gather/Shodan_search


http://www.slideshare.net/theprez98/Shodan-for-penetration-testers-defcon-18