Lab – Shodan Search

1. Objectives

Part 1: Obtain Access to Shodan’s Free Features

Part 2: Investigate Connected IoT Devices

1. Background / Scenario

**Warning**: Do not attempt to login to any device you find on the Shodan search engine. Doing so violates your ethical hacking agreement.

In this lab, you will use the Shodan search engine to gain an understanding of why security should be the focus of any IoT implementation.

Shodan has servers located around the world that continually crawl the Internet looking for connected devices. It can find specific devices and device types. This data can then be searched. Some of the more popular searches include terms such as "webcam", "default passwords", "routers", "video games," and more.

Shodan is a favorite tool used by researchers, security professionals, large enterprises, and computer emergency response teams (CERTs).

* Researchers can use Shodan to data mine information about what devices are connected, where they are connected, and what services are exposed.
* Security professionals can use Shodan as part of a penetration testing plan to discover devices that need to be hardened to prevent potential attacks.
* Large enterprises employ security professionals who should be aware of tools like Shodan for determining the current risk profile of the enterprise’s connected devices.
* CERTs can use Shodan to quickly generate reports about an emerging attack on connected devices.

Shodan is also a tool used by nefarious individuals and groups commonly referred to as threat actors. Shodan can accelerate a threat actor’s reconnaissance of Internet connected devices. Like all the tools in this course, you must use it responsibly according to your organization’s ethical hacking policies.

1. Required Resources

* Device with Internet access.
* SANS Penetration Testing article, “[Getting the Most Out of Shodan Searches](https://pen-testing.sans.org/blog/2015/12/08/effective-shodan-searches)”

1. Obtain Access to Shodan’s Free Features

In this part of the lab, you will navigate to the Shodan search engine and sign up for an account.

* + - 1. Open a web browser and navigate to the Shodan [website](https://www.shodan.io/) at https://www.shodan.io/.
      2. Create an account in one of two ways:
         1. If you click **Create a Free Account**, you will be directed to a page where you can fill in a form to create an account on Shodan.
         2. If you click **Login or Register**, you will be directed to a page where you can sign in with one of several other accounts that you may have, including Google or Facebook.
      3. After successfully logging in, you will see your account page, as shown below. Click the **Shodan** link to return to the homepage.

At the top of the Account page, there are 4 links: Shodan, Developer, Book, More..
The second line: SHODAN, Account, Logout

1. Investigate Connected IoT Devices

In this part, you will gain familiarity with using Shodan’s features to search for Internet-connected devices.

* + 1. Use the basic features of the Shodan search engine.

From the main page, you can type keywords in the search field to get a list of results.

* + - 1. Type **cisco** as the keyword and press **Enter**. How many results did you get for your search?

#### R: 6,872,612 results.

**Note:** Not every device that is found by Shodan is insecure. Shodan simply finds devices that are accessible from the Internet according to a set of search criteria.

* + - 1. Look at other information on the left side of the web page. Your search result is broken down into various categories. Each entry in a category is a clickable link that will refine your search.

How many results, if any, are there for the Windows XP operating system?

R: There is none using windows XP, but quite a few using windows server and other types.

* + - 1. Although Microsoft stopped supporting Windows XP in April 2014, it continues to release patches for it because there are so many end devices still using the operating system. Use an Internet search to discover the well-known 2017 cyberattack that targeted older Windows operating systems.

What was the attack called, what did it target, and what did it do?

R: The attack was called “WannaCry”, targeted Microsoft SMBv1 and did a Remote Code Execution on the target.

From your research, you should have noted that this attack targeted unpatched systems. Prior to the attack, Microsoft had released patches that addressed the vulnerabilities. The systems that were affected by the attack were ones that had not downloaded and applied the patches. Unpatched software is a primary attack vector for threat actors. Any connected device is vulnerable to this type of attack. In the IoT landscape, patching devices becomes even more important as tools such as Shodan can quickly reveal your device’s information, including potential vulnerabilities, to the world.

**Note**: Not all devices discovered by Shodan are vulnerable. Shodan results consist of Internet-connected devices and information about those devices. This information may or may not reveal potential vulnerabilities.

* + - 1. On the right side, the main section of your search shows the devices that match your search. Find an entry that looks interesting to you and fill in the information below.

IP address: 85.138.201.192

Hostname: a85-138-201-192.cpe.**netcabo.pt**

ISP: NOS COMUNICACOES S.A.

Date the entry was added: 2023-11-02 T16:51:36

Country: Portugal

* + - 1. Your entry will also show some banner information. You may see the beginnings of an SSH banner or an HTTP banner. Click **Details** for more information about your entry. You should see several open ports. If not, try a different entry. List the information you found below.

City and Country: Bangkok , Thailand

Ports open: 22, 23, 80, 161, 443, 4786

Services running: Cisco IOS

Key types: ssh-rsa

* + - 1. Return to the Shodan homepage and click **Explore**. What are some of the Top Voted results?

R: webcam, cam, router, ftp, iot, password, ...

One of the Top Voted results for you may have been **default password**. If so, click **default password** to see the results. If not, in the search field, type the keywords “default password,” with the quotes, and press **Enter**. You will see several results that show default passwords embedded in the banners for devices. Hopefully, the owners of these devices have changed the default password. However, this highlights how easy it can be to login to a device if appropriate security measures are not implemented.

**Warning**: Do not attempt to login to any device you find on the Shodan search engine. Doing so violates your ethical hacking agreement.

* + - 1. In the search field, type the keyword “webcam” with the quotes and press Enter. What is your count for Total Results?

R: 7298 results.

* + - 1. In the search field, type the keyword “refrigerator” with the quotes and press Enter. What is your count for Total Results?

R: 152 results.

* + 1. Use keywords together with search operators to filter your search.

You may have noticed that you can only get two pages of results with your free account access. However, even with a paid account you would not want to click through the pages that list thousands or millions of results. Instead, you can combine keywords and search operators to filter your results.

Shodan searches for the services running on a device. It then collects banner information for each service. For example, here is the banner information for the SNMP service running on a Cisco device found with the Shodan search:

Cisco Internetwork Operating System Software

IOS (tm) 7200 Software (UBR7200-IK9SU2-M), Version 12.3(23)BC10, RELEASE SOFTWARE (fc1)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2011 by cisco Systems, Inc.

A search for just "cisco" most likely reveals one to two million results for you. That information may be helpful to you. However, if you are interested in more specific information, you will want to filter your search using filter names and values from the banner information.

For example, if you are interested in seeing how many Cisco 7200 routers in the United States are running the SNMP service, you would enter the following search phrase.

country:US product:"Cisco 7200 Router" port:161

**Note**: Shodan searches use the two letter (alpha-2) country code based on the International Standards Organization’s 3166 publication (ISO 3166-1993).

Create your own searches to find the following:

* + - 1. Minecraft is a popular video game where players can set up their own servers for others to access online. Use an Internet search to find the following information.

What is the common port number used by Minecraft servers? 25565

What is the ISO 3166 alpha-2 code for South Africa? ZA

What Shodan search phrase can you use to discover how many Minecraft servers are currently online in South Africa?

R: country:ZA product:"Minecraft Server" port:25565.

How many Minecraft servers are currently online in South Africa? 306 servers.

* + - 1. Moxa is a supplier of devices that connect industrial equipment to the Internet. How many Moxa devices are running the Telnet service in Brazil?

Search phrase: country:BR product:"MOXA" port:23

Total results: 23

* + - 1. Use an Internet search or review Shodan help pages and tutorials to discover how you can filter your searches based on a range of IP addresses.
      2. Mr. Robot is an American drama television series that chronicles the adventures of a cybersecurity engineer. In the series, the protagonist uses the Shodan search engine to research a fictional corporation. Use an Internet search to find the search string that was used to discover E Corp’s web server.

What string was used?

R: Org: “Evil Corp”

Does the string work on the Shodan search engine? Yes

What IP address was returned by the search? 192.251.68.223

What is the URL for the IP address? http://y7hzuwep[.]bxjyb2jvda[.]net/

* + - 1. There are many home devices connected and controlled using IoT. Apply the methods previously used to search for “garage door” in the state of Michigan in the United States. What was the search string you used?

R: "garage door" country:US state:MI

How many results were returned?

R: None.

What was the top city listed with the most connected garage doors?

R: Madison

What are the potential risks of someone having access to this information?

R: Being able to mess with our personal iot devices. In this example open our garage door.