Name: Ronit Singh **CDAD-UH 1037 CYBERWARFARE** **Date:** 25 October, 2021

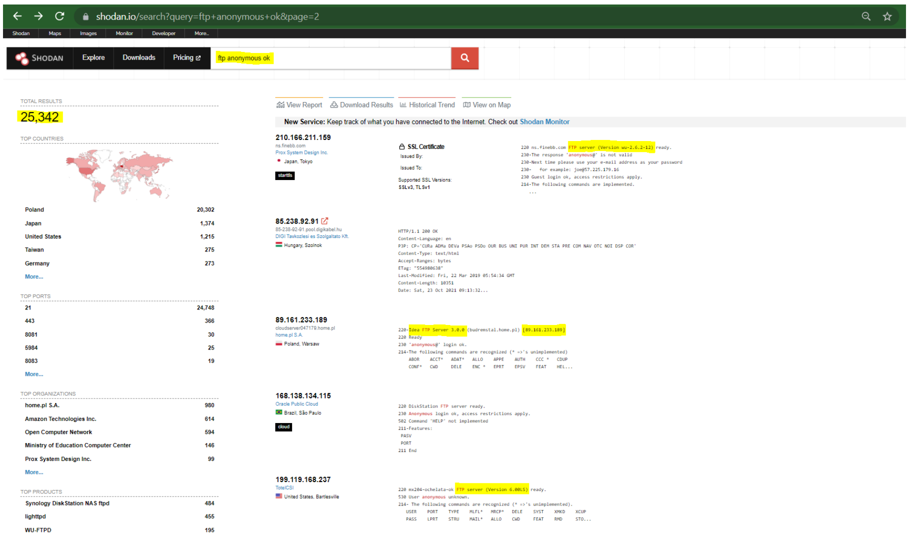
"Diving Deep into FTP Server Searches on Shodan and Ethics Surrounding it"

Abstract

Shodan, a search engine for devices connected to the internet, holds huge potential and impact in the world of cybersecurity due to its capability to retrieve and display information about devices in an instant, usually hidden to the public eye. In this report, I'll be considering FTP (File Transfer Protocol) Servers and showing how easy it can be for any determined hacker to exploit and gain information from any part of the world at any time. I'll also explain Shodan's popularity among malicious hackers as well as ethical hackers, and how they use it for their own intended purposes, while also touching on the topic of ethical or legal issues and policies concerning this search engine.

Part 1:

The FTP Servers (software applications which use a standard communication protocol FTP and enable the transfer of files from one computer to another) can be searched by typing the following **'ftp anonymous ok'** in Shodan's search box. The term 'anonymous ok' refers to the server's ability to accept guest or anonymous login from external sources. The screenshot below shows the results of the search containing as many as 25,342 results.



New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

TOTAL RESULTS

25,342

TOP COUNTRIES

Poland	20,302
Japan	1,374
United States	1,215
Taiwan	275
Germany	273
More...	

TOP PORTS

21	24,748
443	366
8081	30
5984	25
8083	19
More...	

TOP ORGANIZATIONS

home.pl S.A.	980
Amazon Technologies Inc.	614
Open Computer Network	594
Ministry of Education Computer Center	146
Prox System Design Inc.	99
More...	

TOP PRODUCTS

Synology DiskStation NAS ftpd	484
lighttpd	455
WU-FTPD	195

210.166.211.159
ns.finebb.com
Prox System Design Inc.
Japan, Tokyo
starttls

SSL Certificate
Issued By:
Issued To:
Supported SSL Versions:
SSLv3, TLSv1

```
220 ns.finebb.com FTP server (Version wu-2.6.2-12) ready.
230-The response 'anonymous@' is not valid
230-Next time please use your e-mail address as your password
230-   for example: joe@57.225.179.16
230 Guest login ok, access restrictions apply.
214-The following commands are implemented.
  ...
```

85.238.92.91
85-238-92-91.pool.digikabel.hu
DIGI Tavkozlesi es Szolgaltato Kft.
Hungary, Szolnok

```
HTTP/1.1 200 OK
Content-Language: en
P3P: CP='CURa ADMa DEVa PSAo PSDo OUR BUS UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR'
Content-Type: text/html
Accept-Ranges: bytes
ETag: "554980638"
Last-Modified: Fri, 22 Mar 2019 05:54:34 GMT
Content-Length: 10351
Date: Sat, 23 Oct 2021 09:13:32...
```

89.161.233.189
cloudserver047179.home.pl
home.pl S.A.
Poland, Warsaw

```
220-Idea FTP Server 3.0.0 (budremstal.home.pl) [89.161.233.189]
220 Ready
230 'anonymous@' login ok.
214-The following commands are recognized (* =>'s unimplemented)
    ABOR    ACCT*   ADAT*   ALLO    APPE    AUTH    CCC *   CDUP
    CONF*   CWD     DELE    ENC *   EPRT    EPSV    FEAT    HEL...
```

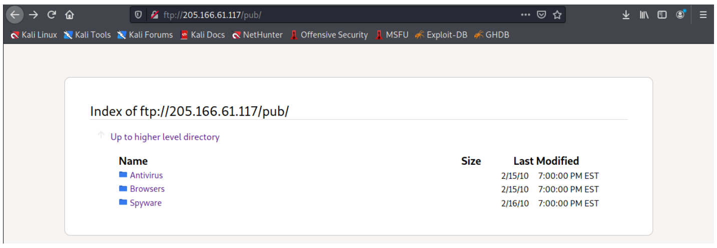
168.138.134.115
Oracle Public Cloud
Brazil, São Paulo
cloud

```
220 DiskStation FTP server ready.
230 Anonymous login ok, access restrictions apply.
502 Command 'HELP' not implemented
211-Features:
 PASV
 PORT
211 End
```

199.119.168.237
TotelCSI
United States, Bartlesville

```
220 mx204-ochelata-ok FTP server (Version 6.00LS) ready.
530 User anonymous unknown.
214- The following commands are recognized (* =>'s unimplemented).
   USER    PORT    TYPE    MLFL*   MRCP*   DELE    SYST    XMKD    XCUP
   PASS    LPRT    STRU    MAIL*   ALLO    CWD     FEAT    RMD     STO...
```

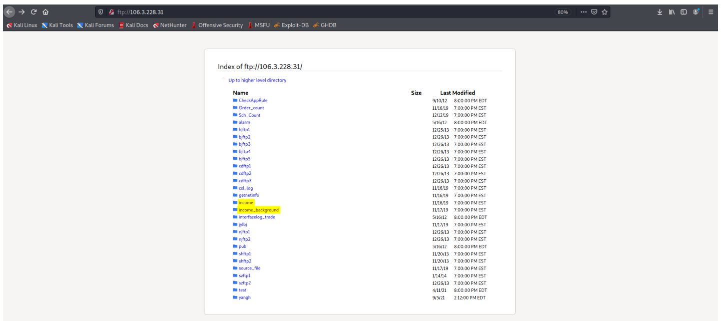
The highlighted texts (banners) indicate the specific versions and IP addresses of the servers which can be critical information to hackers. This is so due to the specific vulnerabilities present in them that hackers can know by searching **"vulnerabilities in <specific ftp version>"** on Google. Moreover, the FTP server information displayed (banners) can be used in the process of passive reconnaissance (gathering information without actively attacking). As an instance, I noticed a critical sentence in one of the banners i.e. "Next time please use your e-mail address as your password, for example: joe@57.225.179.16". This is error information disclosure which could give an idea to the hacker about other registered users' email and password and could result in brute force attacks to gain entry. The countries, ports, top organizations, and top products can further be used as filters in search results and can help hackers narrow down to find specific vulnerable targets. To take a look into what these particular FTP servers contain, one can type the URL in the following format in the search bar - **ftp://<ip address>**. I performed some searches in this way and could see several files and folders stored in them (screenshots below).



Index of ftp://205.166.61.117/pub/

Up to higher level directory

Name	Size	Last Modified
Antivirus		2/15/10 7:00:00 PM EST
Browsers		2/15/10 7:00:00 PM EST
Spyware		2/16/10 7:00:00 PM EST

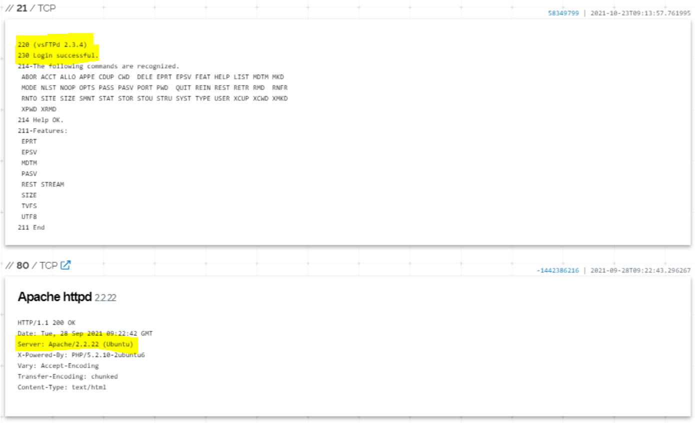


Index of ftp://106.3.228.31/

Up to higher level directory

Name	Size	Last Modified
CheckAppRule		9/10/12 8:00:00 PM EDT
Order_count		11/16/19 7:00:00 PM EST
Sch_Count		12/12/19 7:00:00 PM EST
alarm		5/16/12 8:00:00 PM EDT
bjftp1		12/25/13 7:00:00 PM EST
bjftp2		12/26/13 7:00:00 PM EST
bjftp3		12/26/13 7:00:00 PM EST
bjftp4		12/26/13 7:00:00 PM EST
bjftp5		12/26/13 7:00:00 PM EST
cdftp1		12/26/13 7:00:00 PM EST
cdftp2		12/26/13 7:00:00 PM EST
cdftp3		12/26/13 7:00:00 PM EST
csl_log		11/16/19 7:00:00 PM EST
getnetinfo		11/16/19 7:00:00 PM EST
income		11/16/19 7:00:00 PM EST
income_background		11/17/19 7:00:00 PM EST
interfacelog_trade		5/16/12 8:00:00 PM EDT
jylbj		11/17/19 7:00:00 PM EST
njftp1		12/26/13 7:00:00 PM EST
njftp2		12/26/13 7:00:00 PM EST
pub		5/16/12 8:00:00 PM EDT
shftp1		11/20/13 7:00:00 PM EST
shftp2		11/20/13 7:00:00 PM EST
source_file		11/17/19 7:00:00 PM EST
szftp1		1/14/14 7:00:00 PM EST
szftp2		12/26/13 7:00:00 PM EST
test		4/11/21 8:00:00 PM EDT
yangh		9/5/21 2:12:00 PM EDT

I was especially intrigued by a folder named "Spyware" which contained three .exe files. In another search, two folders, namely income and income_background, caught my attention. I could open each one of them and could see various log files. Moreover, the 'Last Modified' column can give an idea to the hacker about the company's or server's activeness. These can be extremely useful and valuable information depending on the situation and objectives. Moreover, when clicked on the IP address (displayed in bold) in Shodan's search page, one can view further information about that particular FTP server such as common vulnerabilities associated with it, country, city, organization, open ports, TCP responses of each open port, version, serial number, type of encryption algorithm used, and such. During my research, I came across a vulnerable FTP server i.e. **Vsftpd 2.3.4**, which has a backdoor command execution vulnerability. Searching this term on Shodan results in 2,784 results, with the United States being in the top. Some of these servers show 'login successful' while others show 'login incorrect'. Clicking on the particular server displays more information (such as server name, version, Operating System etc.) as highlighted. This information can be used during exploitation via an automated tool called 'Metasploit' which would perform the specific vulnerability's exploitation as specified.


// 21 / TCP

58349799 | 2021-10-23T09:13:57.761995

```
220 (vsFTPd 2.3.4)
230 Login successful.
214-The following commands are recognized.
 ABOR ACCT ALLO APPE CDUP CWD  DELE EPRT EPSV FEAT HELP LIST MDTM MKD
 MODE NLST NOOP OPTS PASS PASV PORT PWD  QUIT REIN REST RETR RMD  RNFR
 RNTO SITE SIZE SMNT STAT STOR STOU STRU SYST TYPE USER XCUP XCWD XMKD
 XPWD XRMD
214 Help OK.
211-Features:
 EPRT
 EPSV
 MDTM
 PASV
 REST STREAM
 SIZE
 TVFS
 UTF8
211 End
```

// 80 / TCP

-1442386216 | 2021-09-28T09:22:43.296267

Apache httpd 2.2.22

```
HTTP/1.1 200 OK
Date: Tue, 28 Sep 2021 09:22:42 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.2.10-2ubuntu6
Vary: Accept-Encoding
Transfer-Encoding: chunked
Content-Type: text/html
```

Part 2:

During the recent years, usage of IoT devices has been rapidly increasing but their security mechanisms have not been adequate. There have been attacks on IoT devices on a huge scale, such as the Mirai botnet attack. Hence, Shodan's information gathering capability across all the internet-connected devices is extremely useful for penetration testers and ethical hackers to point out weaknesses and vulnerabilities in them and also gain information required to perform further test attacks. Likewise, Shodan has made it easier for attackers to find vulnerable IoT devices and exploit them, thus alerting companies as well as the public.

Shodan can be useful to both the attacker as well as the defender. For the attacker, Shodan can be useful in the passive reconnaissance phase to gain critical information such as server name, version number, location, IP address, encryption algorithms, open ports, direct links to login pages, and such. These can then be extended to active reconnaissance, which eventually can be used to carry out effective attacks. Moreover, due to the availability of various search filters, attackers can easily find targets they are looking for in a matter of keystrokes. As for the defenders, the above capabilities are what helps the defenders as well. They can find the vulnerabilities in devices being used in their organization and secure them immediately. They can search for devices using outdated systems or OS and update them, as well as find unnecessarily open ports and close them. Hence, Shodan can be extremely useful for organizations hiring ethical hackers to test their devices' security because ethical hackers use similar methods that malicious hackers do.

Regarding CNN's statement of Shodan being the scariest search engine on the internet, I would say that it is dangerous in the hands of a hacker who knows what he's doing. As for the general population, the information would make little to no sense, but they are the ones who are being targeted by hackers. Shodan's capabilities to find vulnerable devices in a matter of keystrokes enhance the hacker's capabilities in a way and their reach as well. During my research, I came to know that Shodan has implemented measures to limit user's search abilities depending on the edition of Shodan, with 50 being the maximum for registered users and 10 for non-logged in users. Moreover, if the user requires more searches, Shodan requires them to let them know the reason or purpose for it. However, these limitations have only reduced the frequency of attacks leaving the impact of these attacks the same. Attackers can easily search devices with default usernames and passwords, access unprotected cameras around the world, routers, get direct access to ICS systems etc. In today's world, IoT devices are trending, but security is not keeping up pace with it. I believe awareness among the general public will force companies to focus more on the security aspect of these devices and in turn reduce the malicious impact of Shodan. That said, it's quite true that Shodan is dangerous and scary, but one can use this same technology to find loopholes and fix them for good!

Part 3:

Shodan is a legal search engine, but depending on its usage it can risk arising legal and ethical issues as well. It is legal due to the fact that the mechanism which it uses i.e. port scanning "is not a violation of the Abuse Act" (Ethical Hackers Academy). This is precisely because scanning does not do any direct harm. However, if it is used for purposes that aim to harm the victim's device or system or even steal data **without his/her consent**, it can be considered illegal and unethical. While browsing on Shodan, there is a fine line between using it for the good and the bad, because the information gained from the searches can be either used to make systems more secure or instead the same information can be used to gain unauthorized access. For example, malicious hackers and ethical hackers can use the same information and methods to try to break into the system, but the latter will have the written authority and specific set of guidelines to do so from the organization. As for the hackers, depending on the extent of the damage done, the attacker can either be arrested or asked to pay for the damage. On the other hand, individual hackers with good intentions might try to gain access to a system in order to test their skills, point out vulnerabilities, and disclose and inform them to the concerned authority. Although in this scenario, the intentions are good, it is unethical because they are doing it without the authority's permission.

As a cybersecurity policy maker in today's world, I would restrict the use of Shodan to anyone below the age of 16 or 18 because children are more likely to be tempted to try out things out of curiosity without thinking twice and without taking into consideration the security and law aspects. Moreover, due to Shodan's easy search interface, and the ease of access and availability of video tutorials and other resources, it has become comparatively easy to hack into any system that is not adequately protected. Shodan shouldn't be allowed to be accessed in its entirety by anyone because any kind of information about the devices can be extremely critical during the reconnaissance phase. Intelligent and malicious hackers can connect the dots with determined efforts and defeat the whole purpose of the search engine. My recommendation would be to only allow academic and security professionals and companies to use Shodan based on a verification process. Other individuals will need to go through a separate verification process stating their identity, purpose, and reason to use the search engine. This would leave the malicious hackers because they don't belong to any of the above categories. I would want to allow the students to use it because Shodan's capabilities will, without a doubt, help in their cybersecurity learning process. Moreover, universities have begun teaching the ethics surrounding cybersecurity, so there is relatively less fear of students using it for the wrong purpose.