

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



**BÁO CÁO BÀI THỰC HÀNH  
THỰC TẬP CƠ SỞ**

**Bài 14: Phát hiện lỗ hổng với công cụ tìm kiếm**

**Họ và tên: Nguyễn Huy Quang**

**Mã sinh viên: B20DCAT144**

**Giảng viên: Nguyễn Hoa Cương**

*Hà Nội – 2023*

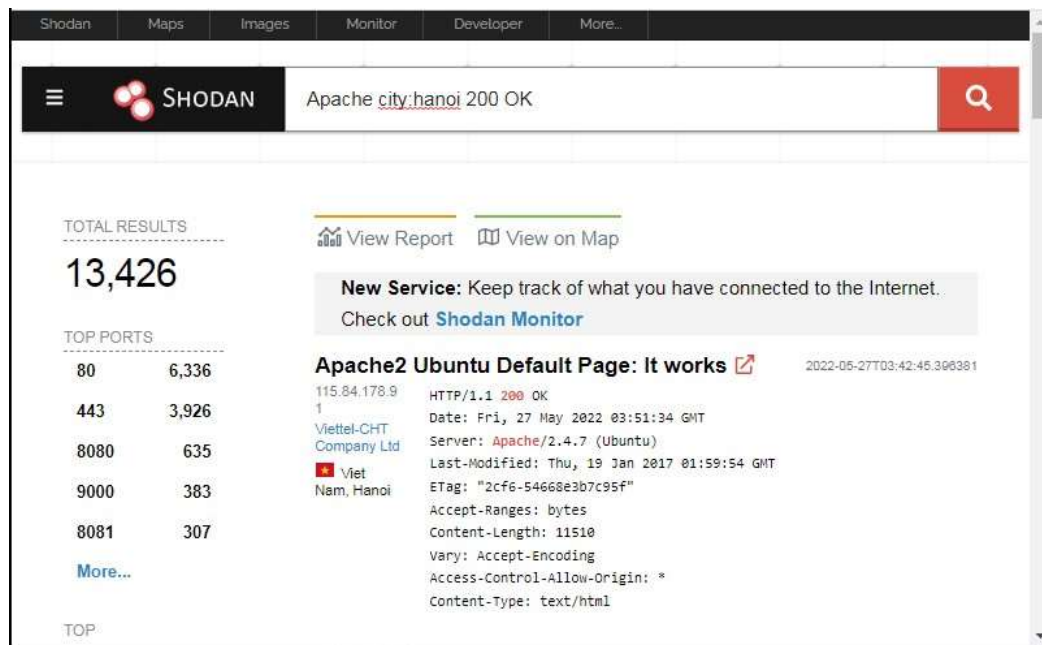
## MỤC LỤC

<b>I</b>	<b>Tìm hiểu lý thuyết .....</b>	<b>2</b>
1.	Shodan .....	2
2.	Google Hacking và sự ảnh hưởng của nó tới quyền riêng tư .....	4
<b>II</b>	<b>Nội dung thực hành .....</b>	<b>4</b>
1.	Thử nghiệm với Shodan .....	4
1.1.	Tìm hiểu và thử nghiệm các bộ lọc trong danh sách: <a href="https://beta.shodan.io/search/filters">https://beta.shodan.io/search/filters</a> .....	5
1.2.	Tìm hiểu và thử nghiệm các ví dụ trong danh sách: <a href="https://beta.shodan.io/search/examples">https://beta.shodan.io/search/examples</a> .....	6
1.3.	Tìm hiểu và thử nghiệm các ví dụ trong danh sách: <a href="https://help.shodan.io/the-basics/search-query-fundamentals">https://help.shodan.io/the-basics/search-query-fundamentals</a> .....	8
1.4.	Tìm hiểu và thử nghiệm các ví dụ trong danh sách: <a href="https://www.yeahhub.com/shodan-search-examples/">https://www.yeahhub.com/shodan-search-examples/</a> .....	9
1.5.	Tìm hiểu và thử nghiệm các ví dụ trong danh sách: <a href="https://www.yeahhub.com/find-vulnerable-webcams-shodan-metasploit-framework/">https://www.yeahhub.com/find-vulnerable-webcams-shodan-metasploit-framework/</a> .....	12
2.	Thử nghiệm với Google Hacking Database .....	15
<b>III</b>	<b>Tài liệu tham khảo .....</b>	<b>25</b>

## I. Tìm hiểu lý thuyết

### 1. Shodan

- Shodan (<https://www.shodan.io>) là một công cụ tìm kiếm được thiết kế bởi nhà phát triển web John Matherly.
- Shodan là một công cụ tìm kiếm khác nhiều so với các công cụ tìm kiếm nội dung như Google, Yahoo hoặc Bing.
- Shodan là một công cụ tìm kiếm để tìm các thiết bị trực tuyến trên internet như: máy tính, server, webcam, các thiết bị routers...
- Nó hoạt động bằng cách quét toàn bộ các các thiết bị trên internet có mở cổng public ra internet và thực hiện phân tích các dấu hiệu được phản hồi về từ các thiết bị.
- Sử dụng thông tin đó, Shodan có thể cho bạn biết những thứ như máy chủ web (và phiên bản) nào phổ biến nhất hoặc có bao nhiêu máy chủ FTP ẩn danh tồn tại ở một vị trí cụ thể, hay trả về danh sách các camera có thể truy cập trực tuyến qua internet.
- Nói chung, với shodan bạn có thể tìm kiếm bất cứ thiết bị nào trên internet miễn là chúng đang có kết nối internet và mở cổng public.
- Shodan được sử dụng hiệu quả trong việc kiểm thử bảo mật các thiết bị IOT (Internet Of Thing) qua việc phát hiện nhanh chóng các thiết bị đang trực tuyến và các thiết bị có tồn tại lỗ hổng bảo mật. Shodan hoạt động 24/7 nên dữ liệu của nó luôn được cập nhật một cách nhanh và chính xác nhất.
- Nguyên lý hoạt động của Shodan: Shodan (Sentient Hyper-Optimized Data Access Network) hoạt động theo thuật toán sau:
  - + Tạo một địa chỉ IPv4 (IPV4 là gì) một cách ngẫu nhiên.
  - + Chọn port (cổng dịch vụ) ngẫu nhiên và thực hiện gửi câu lệnh kiểm tra.
  - + Xem nội dung phản hồi của thiết bị (Service Banner) từ đó xác định xem đó là loại thiết bị gì và chạy cổng gì.
  - + Lặp lại quá trình trên nhưng với ip và port mới.
- Điều này giúp tạo ra sự ngẫu nhiên cũng như đảm bảo tránh gây ra lượng kết nối quá lớn tới một thiết bị một cách liên tục.
- Các cổng dịch vụ mà shodan thường xuyên rà quét: (Port 554 – Real Time Streaming Protocol, Port 5060 – SIP, Port 25 – SMTP, Port 161 – SNMP, Port 23 – Telnet, Port 993 – IMAP, Port 22 – SSH, Port 21 – FTP, Ports 8443, 443, 8080, and 80 – HTTPS/HTTP)
- Tìm kiếm từ khóa trên Shodan: Nhập từ khóa cần tìm kiếm vào search box của Shodan, ví dụ Apache city:hanoi 200 OK. Kết quả trả về là các máy chủ Apache public tại Hà Nội và kèm theo các thông tin sau:



- + Total Results: số lượng kết quả
- + Results map: bản đồ mật độ các khu vực trên thế giới có kết quả phù hợp
- + Top ports: Top các cổng dịch vụ đang mở
- + Top Operation System: Top các hệ điều hành sử dụng....
- + Top Countries: Top các nước sử dụng tương ứng...
- Tìm kiếm trên Shodan có phải là phạm pháp?
  - + Shodan là công cụ tìm kiếm nguy hiểm, đáng sợ nhất thế giới.
  - + Từ góc độ của người dùng, một công cụ tìm kiếm cung cấp những thông tin chi tiết và sâu và các thiết bị hay một số thông tin riêng tư.
  - + Tuy nhiên, Shodan hoàn toàn hợp pháp và không vi phạm luật. Về bản chất, shodan chỉ thu thập dữ liệu đã có sẵn trên internet và shodan chỉ đơn giản là báo cáo những gì nó tìm thấy.
- Ứng dụng của Shodan trong kiểm thử bảo mật: Pen Testing Ethics, Pen Testing Application và Pen Testing HTTP Status Code
  - + Đối với Pen Testing Ethics: Shodan được sử dụng để xem hoặc thay đổi cấu hình các thiết bị hay server mà không yêu cầu xác thực hoặc sử dụng tài khoản và mật khẩu mặc định, thay đổi cấu hình các thiết bị sử dụng chung hoặc lộ tài khoản/ mật khẩu.
  - + Đối với Pen Testing Application: Kiểm tra xâm nhập các ứng dụng trên thiết bị hay server sử dụng các yếu tố: mã code HTTP trả về, các thông tin banner, foot printing của dịch vụ, phiên bản của dịch vụ và các cổng dịch vụ đang mở.

- + Đối với Pen Testing HTTP Status Code: Tìm kiếm dựa trên phản hồi của server: 200 OK, 401 Unauthorized, 403 Forbidden...

## **2. Google Hacking và sự ảnh hưởng của nó tới quyền riêng tư**

- Hiện nay Google là công cụ tìm kiếm trên Internet được sử dụng nhiều nhất ở thời điểm hiện tại.
- Bằng cách sử dụng công cụ tìm kiếm Google, tội phạm mạng có thể thu được những thông tin có giá trị. Sau đó, dựa trên dữ liệu này, họ có thể thực hiện các cuộc tấn công và chuẩn bị cho chúng một cách hiệu quả hơn.
- Google Hacking có thể được định nghĩa là một kỹ thuật máy tính sử dụng các toán tử hoặc lệnh để lọc thông tin mà chúng tôi nhận được từ công cụ tìm kiếm Google. Nó cũng có thể được sử dụng để tìm các lỗ hổng bảo mật trong cấu hình và mã nguồn được sử dụng trên các trang web.
- Các toán tử cơ bản và quan trọng của GoogleHacking
  - + “”: Hiển thị kết quả chứa cụm từ chính xác mà người dùng đã viết.
  - + \*: Sử dụng như một ký tự đặc biệt, từ đơn.
  - + intitle hoặc allintitle: để nhận kết quả có chứa từ trong tiêu đề.
  - + inurl hoặc allinurl: hiển thị kết quả có chứa từ trong url.
  - + filetype: it được sử dụng để tìm kiếm các tệp bằng cách đặt phần mở rộng. Kết hợp với các từ khóa như chúng ta đã thấy trước đó, nó sẽ cải thiện kết quả tìm kiếm.
- Sự nguy hiểm của Google Hacking và ảnh hưởng của nó tới người dùng:
  - + Ngày nay IOT (Internet of Things) càng ngày càng phát triển, tự động hóa gia đình và nhiều hơn nữa được kết nối với Internet. Vấn đề mà họ gặp phải là chúng bị xử lý bởi những người không có đủ kiến thức hoặc các thiết bị này không được trang bị các biện pháp bảo mật cần thiết.
  - + Các hacker dễ dàng tìm thấy các lỗ hổng như mật khẩu , cấu hình và thiết bị do ít được cập nhật nên ngày càng trở nên không an toàn => sử dụng để tấn công vào camera, an ninh....
  - + Tìm kiếm các máy chủ lỗi thời và dễ bị tấn công.
  - + Thực hiện tìm kiếm thông người dùng và mật khẩu của các trang web, server và database.

## **II. Nội dung thực hành**

### **1. Thử nghiệm với Shodan**

- Vào website shodan, tiến hành tạo tài khoản và đăng nhập

Shodan Maps Images Monitor Developer More...

SHODAN Account

### Create Account

Username  
quangb20dcat144

Password  
\*\*\*\*\*

Confirm Password  
\*\*\*\*\*


Email  
huyquang880@gmail.com

- Giao diện của Shodan sau khi đăng nhập thành công

Shodan Maps Images Monitor Developer More...

SHODAN Search...

## Dashboard

 **Getting Started**

[What is Shodan?](#)

[Search Query](#)

**>\_ ASCII Videos**

[Setting up Real-Time Network Monitoring](#)

**</> Develo**

[How to \[Data wit](#)

```
cmd C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\NguyenHuyQuang>echo Quang-B20DCAT144
Quang-B20DCAT144

C:\Users\NguyenHuyQuang>
```

### 1.1. Tìm hiểu và thử nghiệm các bộ lọc trong danh sách:

<https://beta.shodan.io/search/filters>

- Tìm các web server chạy Apache tại thành phố Hà Nội, 200 OK thể hiện các website trả về response code 200

*Apache city:hanoi 200 OK*

The screenshot shows the Shodan search interface with the query 'Apache city:hanoi 200 OK'. The search results show 17,859 total results. A table of top ports is displayed:

Port	Count
80	7,651
443	5,725
8080	704
8081	366
9000	345

A sample result for IP 105.166.177.24 is shown, indicating it is a 'Page not found' response with status 200 OK. The server is identified as 'Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16'. A Windows command prompt window is overlaid on the screenshot, showing the command 'C:\Windows\system32\cmd.exe' and the output of a telnet connection to the IP.

- Tìm kiếm các thiết bị hoặc server đang mở cổng telnet 23 tại Việt Nam  
*port:23 country:vn*

The screenshot shows the Shodan search interface with the query 'port:23 country:vn'. The search results show 27,807 total results. A table of top cities is displayed:

City	Count
Hồ Chí Minh	6,622
Hanoi	5,387
Thanh Hóa	2,146
Vinh	1,048
Việt Trì	792

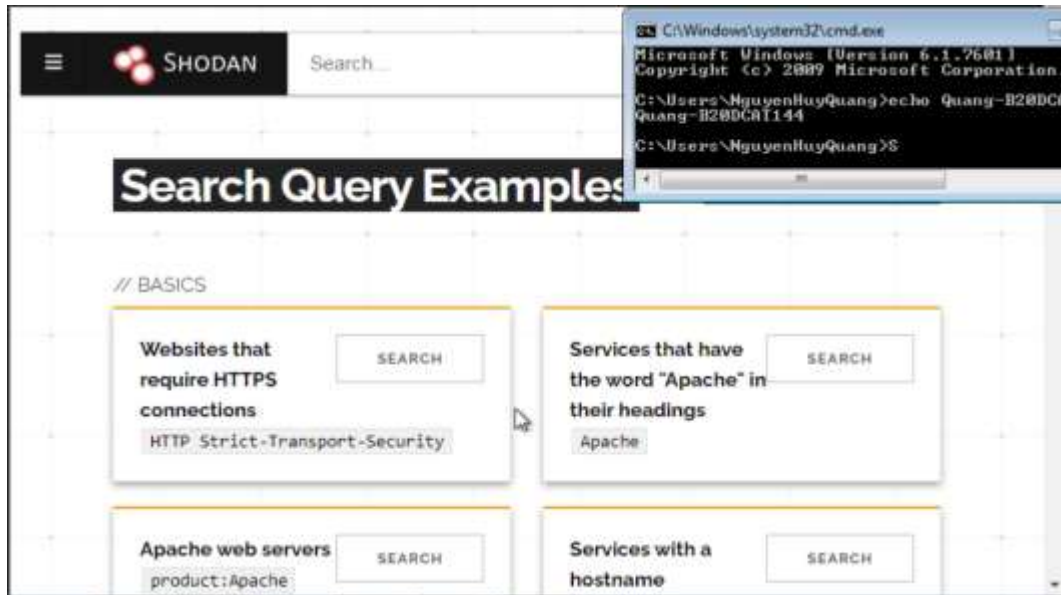
A sample result for IP 113.160.201.29 is shown, indicating it is a 'static.vnpt.vn' device. The device is identified as 'Vietnam Posts and Telecommunications Group'. A Windows command prompt window is overlaid on the screenshot, showing the command 'C:\Windows\system32\cmd.exe' and the output of a telnet connection to the IP.

### 1.2. Tìm hiểu và thử nghiệm các ví dụ trong danh sách:

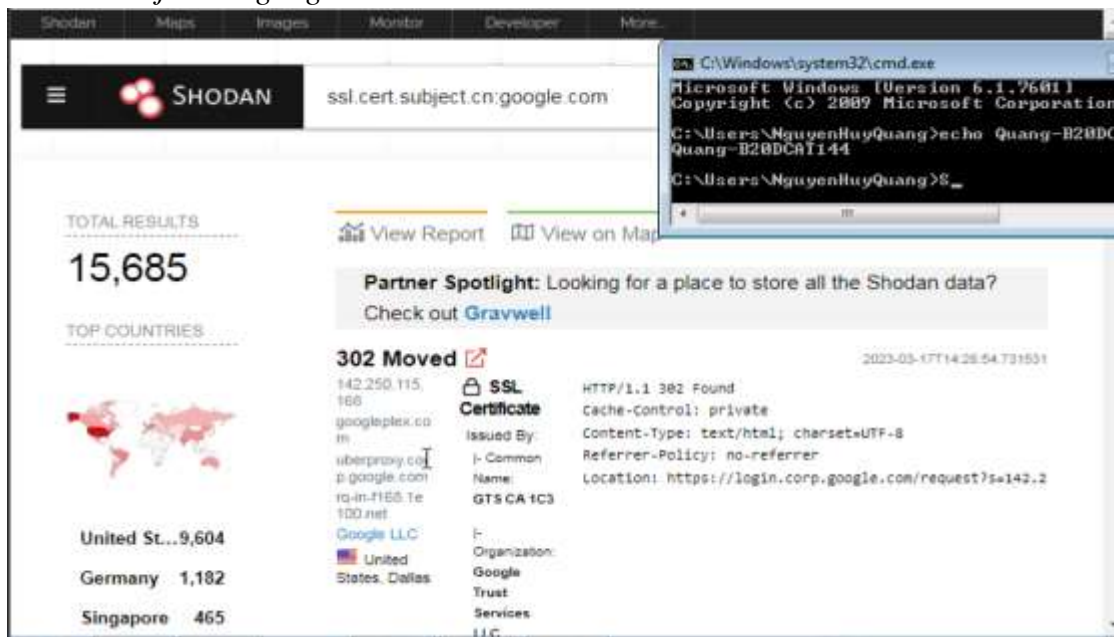
<https://beta.shodan.io/search/examples>

- Giao diện chính



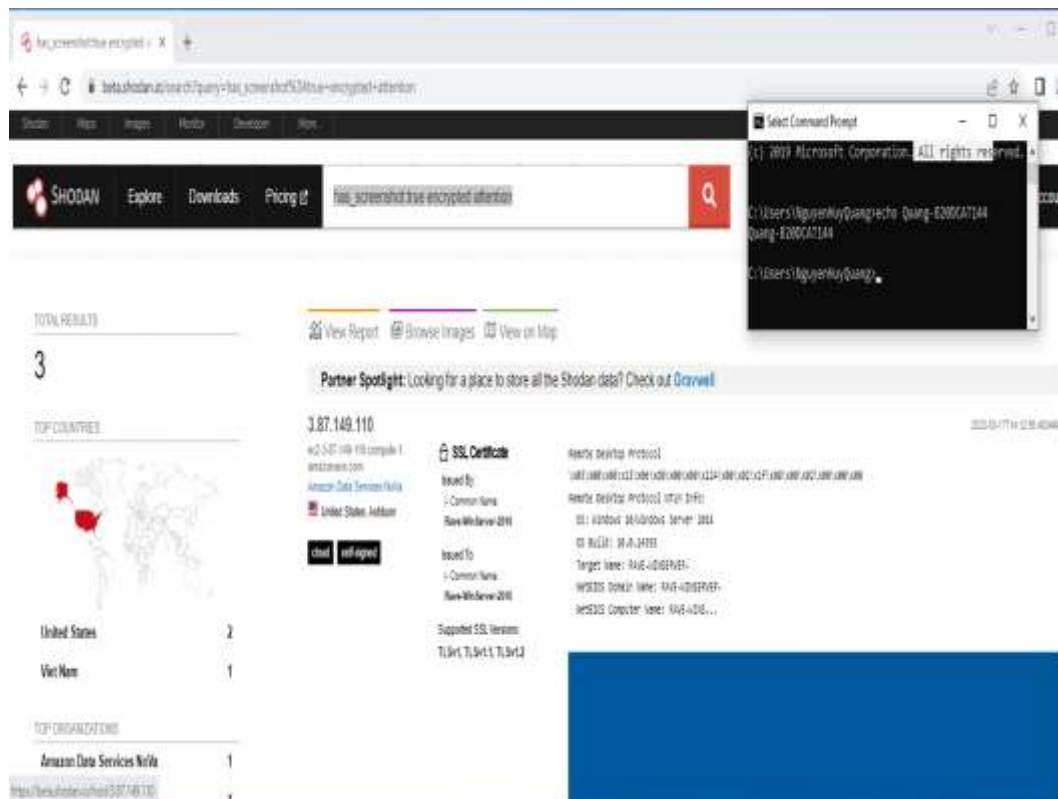


- Dịch vụ SSL đã được cấp chứng chỉ cho \*.google.com  
*ssl.cert.subject.cn:google.com*



- Các dịch vụ VNC công cộng ẩn sau các cổng web chung  
*has\_screenshot:true encrypted attention*

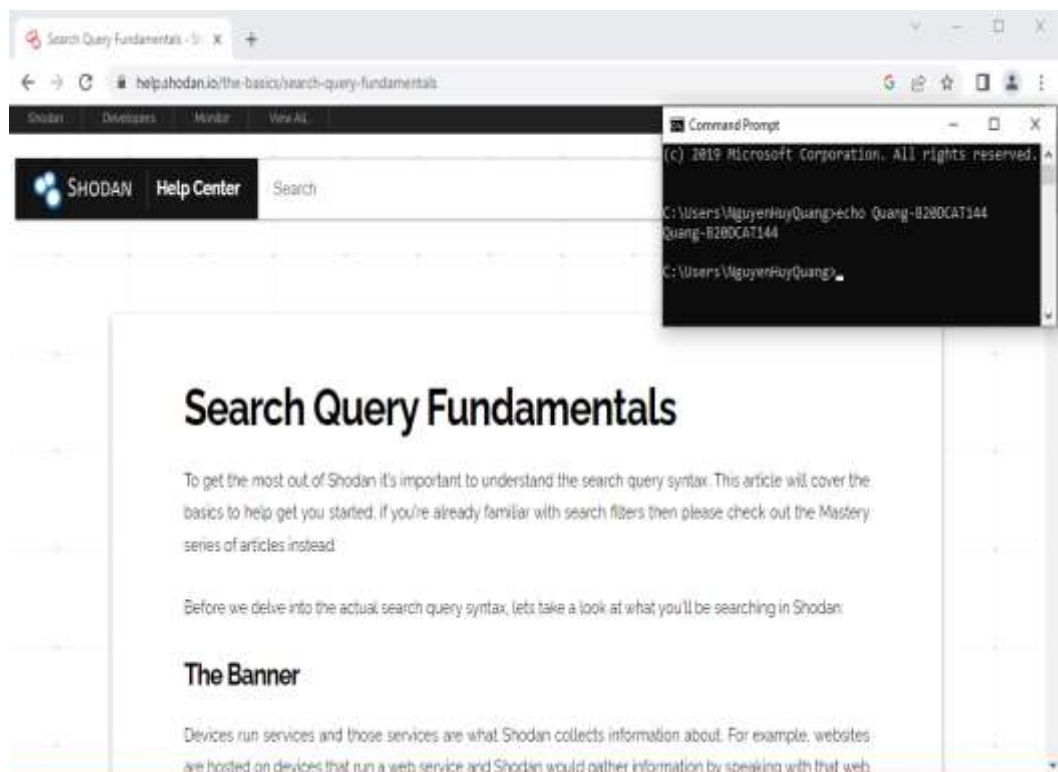




### 1.3. Tìm hiểu và thử nghiệm các ví dụ trong danh sách:

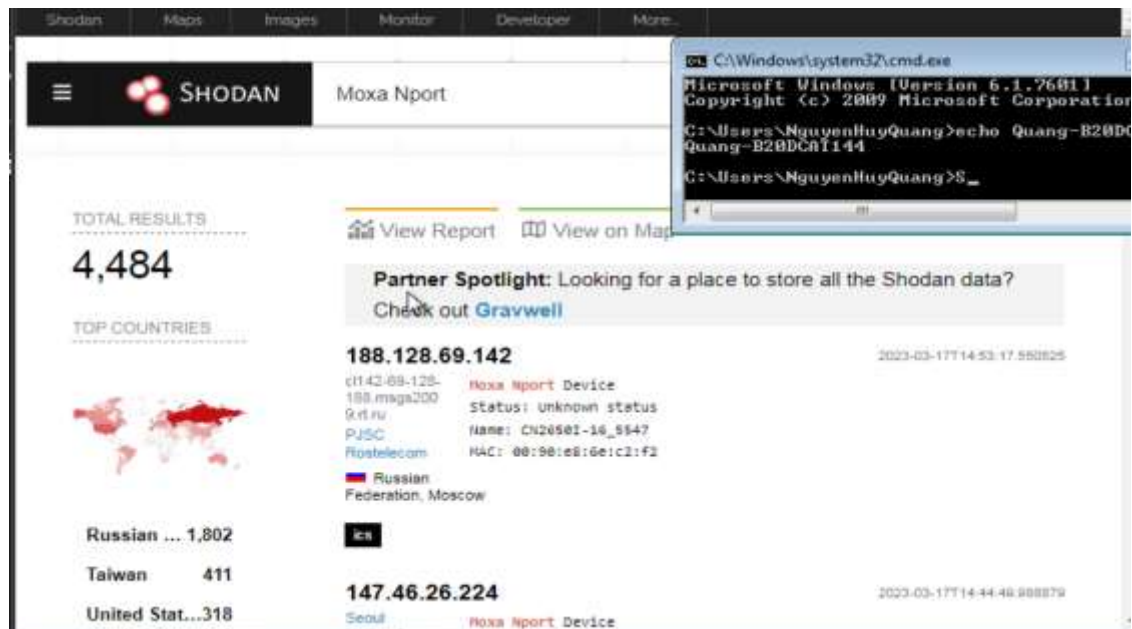
<https://help.shodan.io/the-basics/search-query-fundamentals>

- Giao diện chính:



### 1.4.

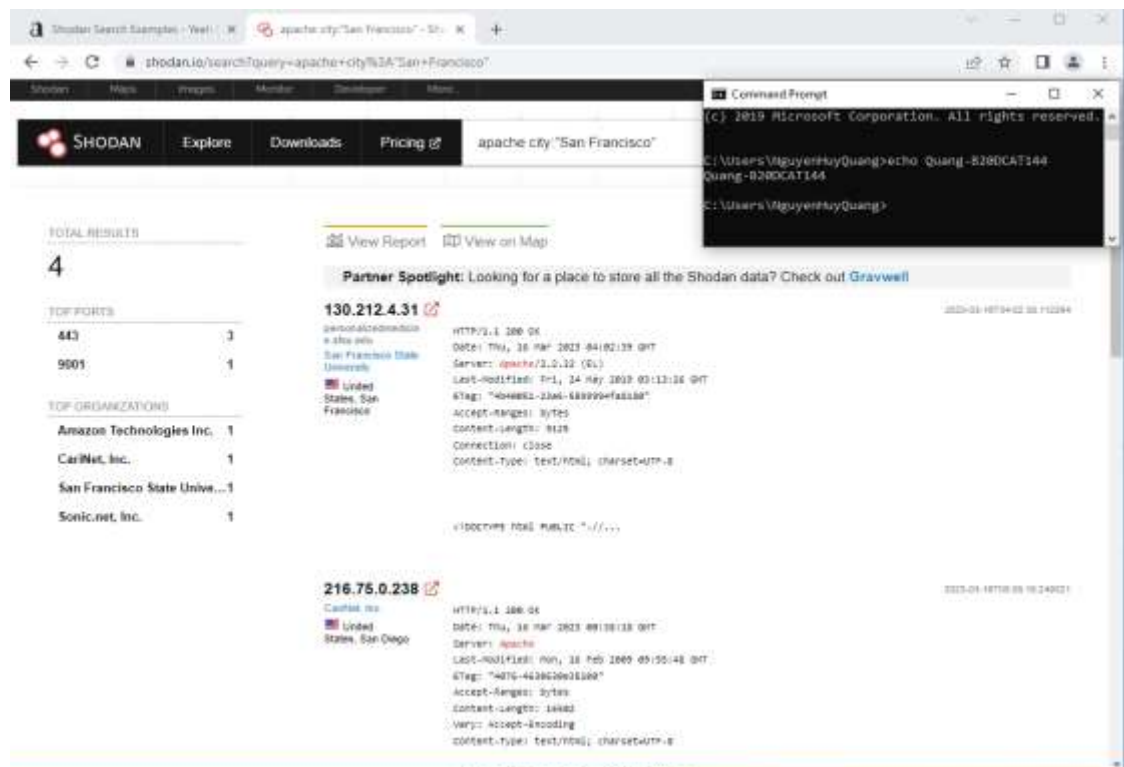
- Tìm kiếm thiết bị Moxa Nports



### 1.5. Tìm hiểu và thử nghiệm các ví dụ trong danh sách:

<https://www.yeahhub.com/shodan-search-examples/>

- Tìm kiếm Apache Server ở San Francisco  
*apache city: "San Francisco"*



- Tìm kiếm Nginx Server ở Australia  
*nginx country:"AU"*

The screenshot shows the Shodan search results for the query `nginx country:"AU"`. The page displays 373,773 total results. A list of top cities is shown: Sydney (285,106), Melbourne (41,889), Brisbane (20,569), Perth (9,235), and Adelaide (5,096). A detailed view of a specific result is shown, including an SSL Certificate for `ec2-52-84-159-96.ap-south-east-2.compute.amazonaws.com` issued by Amazon Technologies Inc. The certificate details include the common name, organization, location (Australia, Sydney), and the issuer (Amazon Technologies Inc.). The page also features a 'Partner Spotlight' for Gravwell and a 'View Report' button.

- Tìm kiếm Google Web Server (GWS)  
*"Server:gws" hostname:"google"*

The screenshot shows the Shodan search results for the query `"Server:gws" hostname:"google"`. The page displays 215 total results. A list of top countries is shown: United States (86), Chile (19), Netherlands (13), India (11), and United Kingdom (10). A detailed view of a specific result is shown, including an SSL Certificate for `171.217.213.106` issued by Google LLC. The certificate details include the common name, organization, location (United States, Des Moines), and the issuer (Google LLC). The page also features a 'Partner Spotlight' for Gravwell and a 'View Report' button.

## 1.1. Tìm hiểu và thử nghiệm các ví dụ trong danh sách:

<https://www.yeahhub.com/find-vulnerable-webcams-shodan-metasploit-framework/>

- Sử dụng công cụ metasploit framework để tìm webcam trên Shodan

```
(quangnh@Quang-B20DCAT144-Kali)-[~]
$ msfconsole

Metasploit

-=[ metasploit v6.2.26-dev ]-
+ -- --[ 2264 exploits - 1189 auxiliary - 404 post ]-
+ -- --[ 951 payloads - 45 encoders - 11 nops ]-
+ -- --[ 9 evasion ]-

Metasploit tip: View missing module options with show
missing
Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

- 
- Tìm kiếm các lỗ hổng liên quan tới shodan  
*search shodan*

```
quangnh@Quang-B20DCAT144-Kali: -
File Actions Edit View Help
msf6 > search shodan

Matching Modules:

#  Name                                     Disclosure Date  R
--  -
0  auxiliary/admin/http/hikvision_unauth_pwd_reset_cve_2017_7921  2017-09-23      n
normal Yes  Hikvision IP Camera Unauthenticated Password Change Via Improper Authentication Logic
1  auxiliary/scanner/http/influxdb_enum                                     n
normal No   InfluxDB Enum Utility
2  auxiliary/gather/shodan_honeyscore                                     n
normal No   Shodan Honeyscore Client
3  auxiliary/gather/shodan_host                                         n
normal No   Shodan Host Port
4  auxiliary/gather/shodan_search                                       n
normal No   Shodan Search
5  auxiliary/scanner/http/smt_ipmi_49152_exposure                       2014-06-19      n
normal No   Supermicro Onboard IPMI Port 49152 Sensitive File Exposure
6  auxiliary/gather/hikvision_info_disclosure_cve_2017_7921           2017-09-23      n
normal Yes  Unauthenticated information disclosure such as configuration, credentials and camera snapshots of a vulnerable Hikvision IP Camera

Interact with a module by name or index. For example info 6, use 6 or use auxiliary/gather/hikvision_info_disclosure_cve_2017_7921

msf6 > 
```



- Khai báo sử dụng modul tấn công  
*use auxiliary/gather/shodan\_search*

```

quangnh@Quang-B20DCAT144-Kali -
File Actions Edit View Help
 4 auxiliary/gather/shodan_search n
ormal No Shodan Search
 5 auxiliary/scanner/http/smt_ipmi_49152_exposure 2014-06-19 n
ormal No Supermicro Onboard IPMI Port 49152 Sensitive File Exposure
 6 auxiliary/gather/hikvision_info_disclosure_cve_2017_7921 2017-09-23 n
ormal Yes Unauthenticated information disclosure such as configuration, credentials
and camera snapshots of a vulnerable Hikvision IP Camera

Interact with a module by name or index. For example info 6, use 6 or use auxiliary/gat
her/hikvision_info_disclosure_cve_2017_7921

msf6 > use 4
msf6 auxiliary(gather/shodan_search) > show options

Module options (auxiliary/gather/shodan_search):

  Name          Current Setting  Required  Description
  ---          -
  DATABASE      false           no        Add search results to the database
  MAXPAGE       1               yes       Max amount of pages to collect
  OUTFILE       no              no        A filename to store the list of IPs
  QUERY         yes             yes       Keywords you want to search for
  REGEX         .*              yes       Regex search for a specific IP/City/Coun
try/Hostname
  SHODAN_APIKEY yes            yes       The SHODAN API key

View the full module info with the info, or info -d command.
msf6 auxiliary(gather/shodan_search) >

```

- Chạy lệnh “show option” để xem các thông tin về mô đun đang sử dụng.

```

quangnh@Quang-B20DCAT144-Kali -
File Actions Edit View Help
 4 auxiliary/gather/shodan_search n
ormal No Shodan Search
 5 auxiliary/scanner/http/smt_ipmi_49152_exposure 2014-06-19 n
ormal No Supermicro Onboard IPMI Port 49152 Sensitive File Exposure
 6 auxiliary/gather/hikvision_info_disclosure_cve_2017_7921 2017-09-23 n
ormal Yes Unauthenticated information disclosure such as configuration, credentials
and camera snapshots of a vulnerable Hikvision IP Camera

Interact with a module by name or index. For example info 6, use 6 or use auxiliary/gat
her/hikvision_info_disclosure_cve_2017_7921

msf6 > use 4
msf6 auxiliary(gather/shodan_search) > show options

Module options (auxiliary/gather/shodan_search):

  Name          Current Setting  Required  Description
  ---          -
  DATABASE      false           no        Add search results to the database
  MAXPAGE       1               yes       Max amount of pages to collect
  OUTFILE       no              no        A filename to store the list of IPs
  QUERY         yes             yes       Keywords you want to search for
  REGEX         .*              yes       Regex search for a specific IP/City/Coun
try/Hostname
  SHODAN_APIKEY yes            yes       The SHODAN API key

View the full module info with the info, or info -d command.
msf6 auxiliary(gather/shodan_search) >

```

- Mở Shodan, vào phần Account, lấy API Key



- Vào lại metasploit, thiết lập API Key  
set SHODAN\_APIKEY <api\_key>

```
msf6 auxiliary(gather/shodan_search) > set SHODAN_APIKEY LJR5DCgQ9TjIDHAYHfGuiRBL6gtGKWCw
SHODAN_APIKEY => LJR5DCgQ9TjIDHAYHfGuiRBL6gtGKWCw
```

- Thiết lập Query tìm kiếm  
set QUERY "webcamxp"

```
msf6 auxiliary(gather/shodan_search) > set QUERY "webcamxp"
QUERY => webcamxp
```

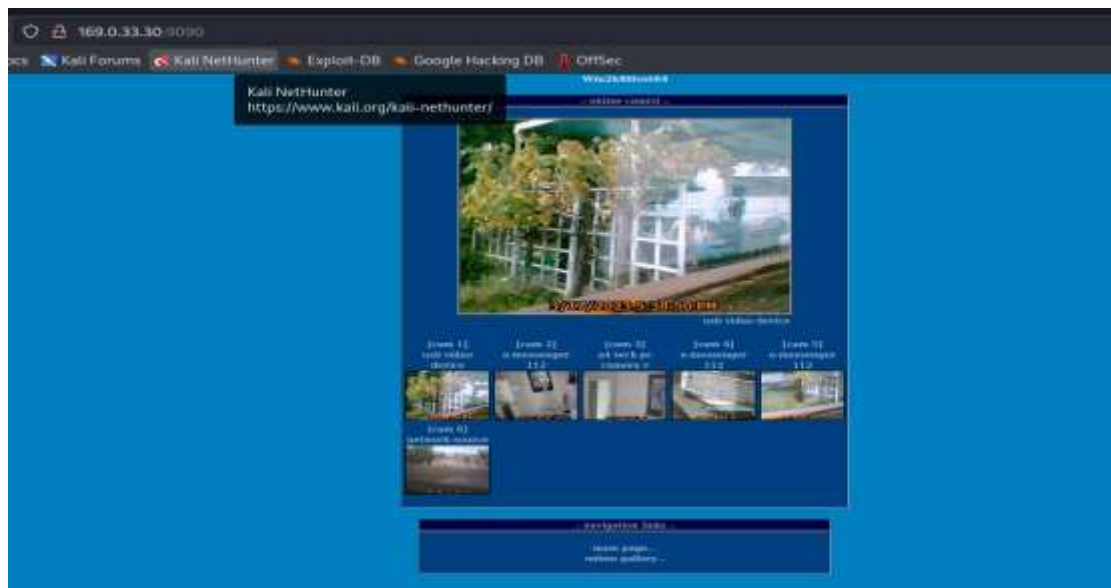
- Thực thi tấn công bằng lệnh "run"

```
quangnh@Quang-B20DCAT144-Kali: ~
File Actions Edit View Help
[*] Unknown datastore option: SHODAN_APTKEY. Did you mean SHODAN_APIKEY?
msf6 auxiliary(gather/shodan_search) > set SHODAN_APIKEY LJR5DCgQ9TjIDHAYHfGuiRBL6gtGKWCw
SHODAN_APIKEY => LJR5DCgQ9TjIDHAYHfGuiRBL6gtGKWCw
msf6 auxiliary(gather/shodan_search) > set QUERY "webcamxp"
QUERY => "webcamxp"
msf6 auxiliary(gather/shodan_search) > run
[*] Total: 203 on 3 pages. Showing: 1 page(s)
[*] Collecting data, please wait...

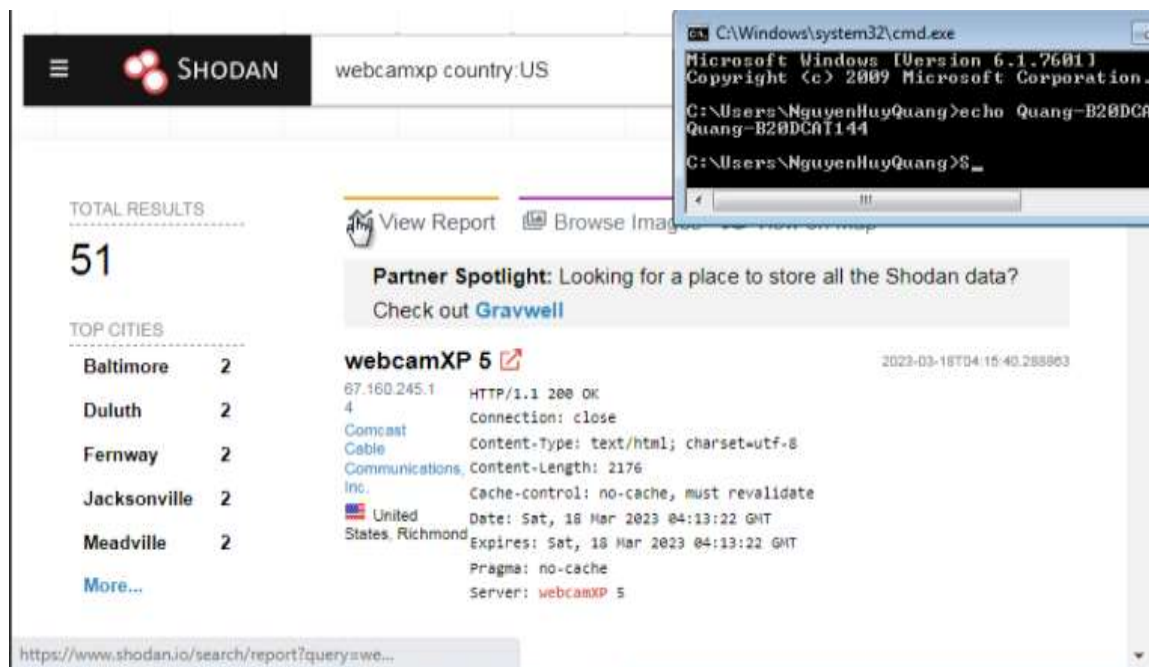
Search Results
```

IP:Port	City	Country	Hostname
104.177.153.145:8080	Jacksonville	United States	104-177-153-145.1ightspeed.jcvlfl.sbcglobal.net
107.13.2.109:8080	Brogden	United States	mta-107-13-2-109.nc.FF.com
108.48.26.47:8080	Gainesville	United States	pool-108-48-26-47.washdc.fios.verizon.net
109.192.213.146:888	Aalen	Germany	ip-109-192-213-146.um38.pools.vodafone-1p.de
109.233.191.130:8080	Novi Pazar	Serbia	ip-109-233-191-130.orientelekom.rs
109.233.191.228:8090	Belgrade	Serbia	ip-109-233-191-228.orientelekom.rs
114.32.131.232:1000	Taipei	Taiwan	114-32-131-232.hinet-ip.hinet.net
115.22.130.117:5000	Busan	Korea, Republic of	
138.123.62.124:8080	Wilmington	United States	s-a228-01.dtcc.ed

- Tiến hành truy cập vào bất kỳ 1 webcam nào đó



- Mở shodan, sử dụng thanh tìm kiếm của shodan để tìm webcam webcamxp country:US



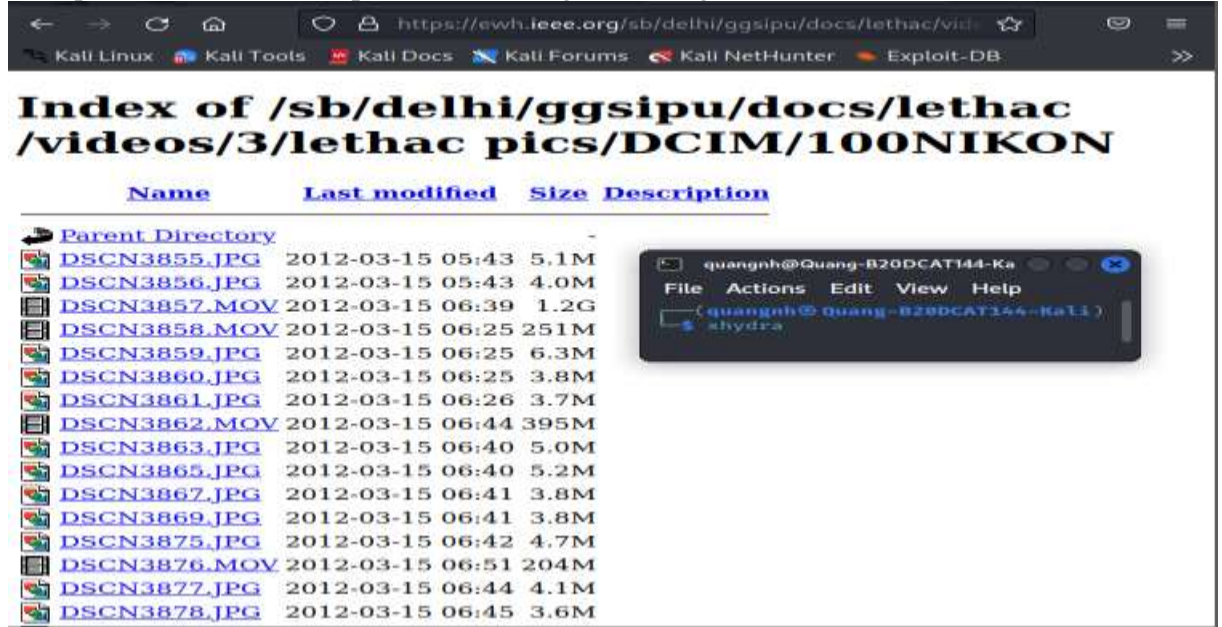
## 2. Thử nghiệm với Google Hacking Database

- Truy cập vào website [www.exploit-db.com/google-hacking-database](http://www.exploit-db.com/google-hacking-database)





Kết quả trả về 1 bộ sưu tập ảnh mà mọi người không biết ở đó



Name	Last modified	Size	Description
Parent Directory	-	-	-
DSCN3855.JPG	2012-03-15 05:43	5.1M	
DSCN3856.JPG	2012-03-15 05:43	4.0M	
DSCN3857.MOV	2012-03-15 06:39	1.2G	
DSCN3858.MOV	2012-03-15 06:25	251M	
DSCN3859.JPG	2012-03-15 06:25	6.3M	
DSCN3860.JPG	2012-03-15 06:25	3.8M	
DSCN3861.JPG	2012-03-15 06:26	3.7M	
DSCN3862.MOV	2012-03-15 06:44	395M	
DSCN3863.JPG	2012-03-15 06:40	5.0M	
DSCN3865.JPG	2012-03-15 06:40	5.2M	
DSCN3867.JPG	2012-03-15 06:41	3.8M	
DSCN3869.JPG	2012-03-15 06:41	3.8M	
DSCN3875.JPG	2012-03-15 06:42	4.7M	
DSCN3876.MOV	2012-03-15 06:51	204M	
DSCN3877.JPG	2012-03-15 06:44	4.1M	
DSCN3878.JPG	2012-03-15 06:45	3.6M	

- Tìm hiểu lệnh (còn gọi là Google dork) tại [www.exploit-db.com/ghdb/6322](http://www.exploit-db.com/ghdb/6322) để tìm các từ khóa SSH



intitle:"index of" "id\_rsa.pub"

**GHDB-ID:** 6322

**Author:** SID JOSHI

**Published:** 2020-06-22

**Google Dork Description:** intitle:"index of" "id\_rsa.pub"

**Google Search:** intitle:"index of" "id\_rsa.pub"

```
# Dork: intitle:"index of" "id_rsa.pub"
# Author: Sid Joshi
# Result of this dorks contains Sensitive Direc
# POC in attachment
# Thanks!
```


Tìm kiếm truy vấn intitle: "index of""id\_rsa.pub"

Click vào 1 kết quả để xem

## Index of /apiAgro/puphpet/files/dot/ssh

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">id_rsa</a>	2015-11-02 17:20	1.6K	
<a href="#">id_rsa.ppk</a>	2015-11-02 17:20	1.4K	
<a href="#">id_rsa.pub</a>	2015-11-02 17:20	392	
<a href="#">insecure_private_key</a>	2015-11-02 17:20	1.6K	
<a href="#">root_id_rsa</a>	2015-11-02 17:20	1.6K	
<a href="#">root_id_rsa.ppk</a>	2015-11-02 17:20	1.4K	
<a href="#">root_id_rsa.pub</a>	2015-11-02 17:20	392	

Apache/2.4.10 (Debian) Server at 164.177.30.131 Port 80



- Tìm hiểu Google dork tại [www.exploit-db.com/ghdb/6412](http://www.exploit-db.com/ghdb/6412) tìm log có tên người dùng và mật khẩu, có thể có các mục như địa chỉ email, URL những thông tin đăng nhập này được sử dụng.....

## allintext:username,password filetype:log

**GHDB-ID:**  
6412


Published: 2020-07-16

**Google Dork Description:**  
allintext:username,password filetype:log

Google Search: allintext:username,password filetype:log

← →

allintext:username,password filetype:log



Tìm kiếm truy vấn allintext:username,password filetype:log  
Click vào một dòng để xem kết quả

```
Firefox (1.x->3.x) Passwords:

serv - http://fr-fr.facebook.com
email      : roi_de_la_casse@hotmail.com
pass      : zzqqh9qy

serv - http://fr.youtube.com
username   : Sargerans
password   : zzqqh9qy

serv - http://snowtigers.net
username   : Maxter
password   : WOW071789788

serv - https://login.facebook.com
email      : roi_de_la_casse@hotmail.com
pass      : zzqqh9qy

serv - http://hostarea.org
login      : Sargeran
pass      : zzqqh9qy

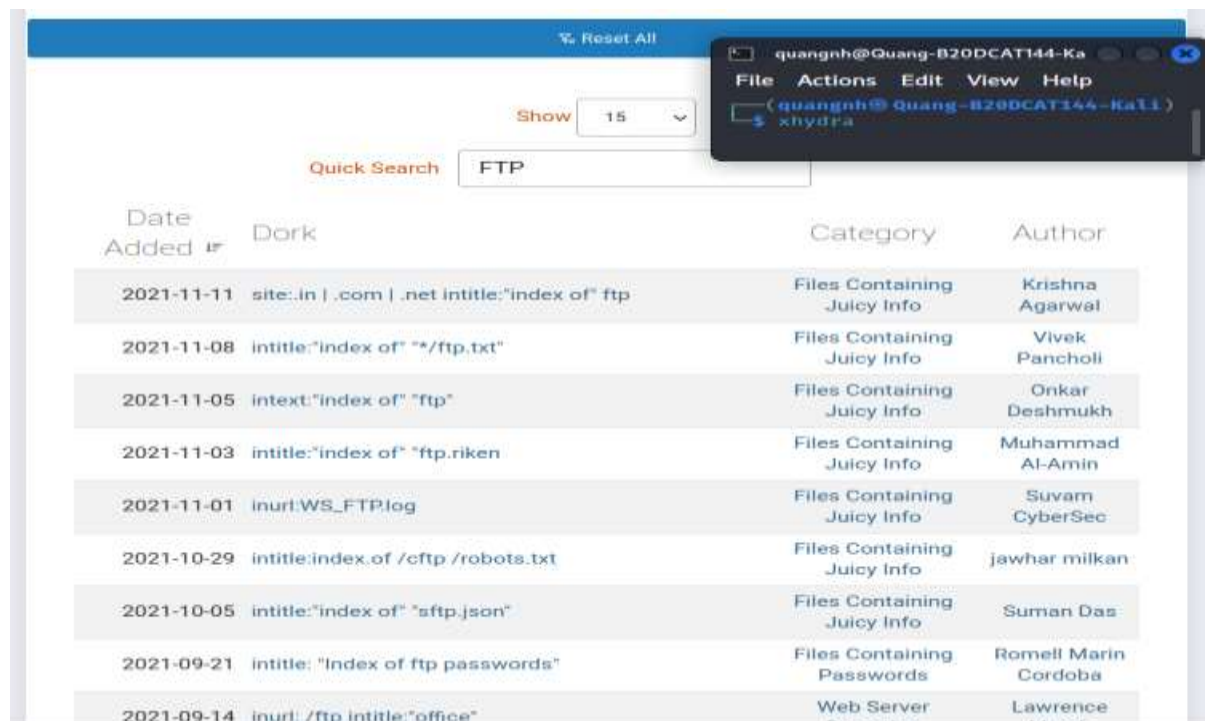
serv - http://www.facebook.com
email      : roi_de_la_casse@hotmail.com
pass      : zzqqh9qy

serv - http://www.forumactif.com
password2   : zzqqh9qy

serv - http://pubggoogle.forumactif.net
username    : Admin
password    : zzqqh9qy

serv - https://www.google.com
Email       : Sargeran@hotmail.com
Passwd      : zzqqh9qy
```

- Quay lại GHDB ([www.exploit-db.com/google-hacking-database](http://www.exploit-db.com/google-hacking-database)) và trong hộp văn bản Tìm kiếm nhanh ở bên phải, nhập FTP. Xuất hiện rất nhiều Google dorks liên quan đến Giao thức truyền tệp (FTP).



Date Added	Dork	Category	Author
2021-11-11	site:.in   .com   .net intitle:"index of" ftp	Files Containing Juicy Info	Krishna Agarwal
2021-11-08	intitle:"index of" "*/ftp.txt"	Files Containing Juicy Info	Vivek Pancholi
2021-11-05	intext:"index of" "ftp"	Files Containing Juicy Info	Onkar Deshmukh
2021-11-03	intitle:"index of" "ftp.riken"	Files Containing Juicy Info	Muhammad Al-Amin
2021-11-01	inurl:WS_FTP.log	Files Containing Juicy Info	Suvam CyberSec
2021-10-29	intitle:index.of /cftp /robots.txt	Files Containing Juicy Info	jawhar milkan
2021-10-05	intitle:"index of" "sftp.json"	Files Containing Juicy Info	Suman Das
2021-09-21	intitle: "Index of ftp passwords"	Files Containing Passwords	Romell Marin Cordoba
2021-09-14	inurl: /ftp intitle:"office"	Web Server Detection	Lawrence Meech

Chọn một mục bất kỳ





Tìm kiếm truy vấn

Click vào để xem kết quả



## Index of /net

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">OpenSSL/</a>	2023-03-18 14:41	-	
<a href="#">ProFTPD/</a>	2023-03-18 02:45	-	
<a href="#">apache/</a>	2023-03-18 13:32	-	
<a href="#">postfix-release/</a>	2023-02-05 03:00	-	
<a href="#">postfix/</a>	2017-06-29 22:16	-	

- Tìm kiếm với một số loại google dork khác
- Xem thư mục liên quan tới “/cftp /robot.txt”



# Index of /

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <a href="#">mirrors/</a>	2021-03-17 10:05	-	
 <a href="#">robots.txt</a>	2017-10-31 12:40	64	

```
quangnh@Quang-B20DCAT144-Ka
File Actions Edit View Help
(quangnh@Quang-B20DCAT144-Kali
[~]
$ echo Quang-B20DCAT144
```

Xem log của máy chủ FTP



The screenshot shows the Exploit Database search results for the query 'inurl:WS\_FTP.log'. The results page includes the following information:

- GHDB-ID:** 7547
- Author:** SUVAM CYBERSEC
- Published:** 2021-11-01
- Google Dork Description:** inurl:WS\_FTP.log
- Google Search:** inurl:WS\_FTP.log

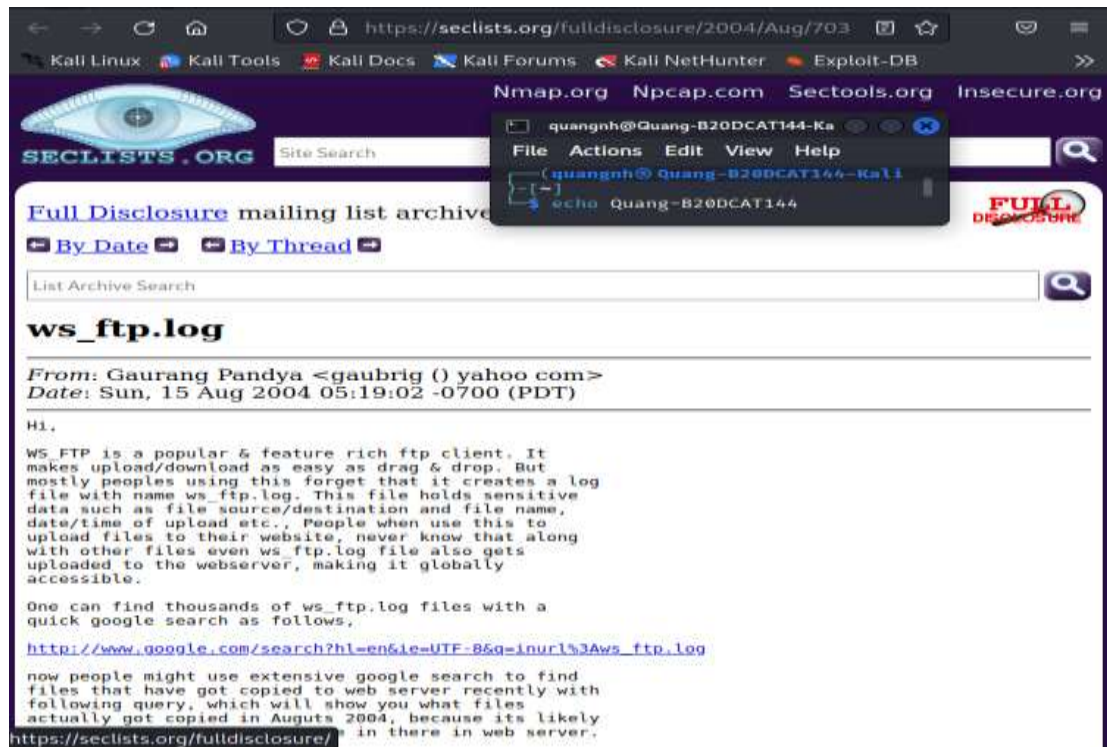
At the bottom, there is a summary of the search results:

```
# Google Dork: inurl:WS_FTP.log
# Files Containing Juicy Info
# Date: 31/10/2021
```



The screenshot shows a vulnerability report from Acunetix. The report title is 'WS\_FTP log file found'. The report includes the following sections:

- Description:** WS\_FTP is a popular FTP client. This application creates a log file named WS\_FTP.LOG. This file contains sensitive data such as file source/destination and file name, date/time of upload etc.
- Remediation:** Remove this file from your website or change its permissions to remove access.
- References:** ws\_ftp.log
- Related Vulnerabilities:** MongoDB HTTP status interface, WordPress Plugin HTML5 MP3 Player with Playlist Free Information Disclosure (2.6), WordPress Plugin Slack-Chat Information Disclosure (1.5.5)



Những nguy hiểm của google dork:

- + Kẻ tấn công có thể thực hiện tìm kiếm các máy chủ lỗi thời và dễ bị tấn công, thực hiện tìm kiếm thông tin người dùng và mật khẩu các trang web, server và database, các log của các server, các tài liệu mật như thông tin tài khoản và mật khẩu của người dùng, các tài liệu mật của các cơ quan, tổ chức, chính phủ, quân đội.... để thực hiện cho mục đích xấu.

### III. Tài liệu tham khảo

- [Google Hacking và sự ảnh hưởng của nó tới quyền riêng tư \(viblo.asia\)](#)
- [Shodan - Công cụ tìm kiếm cho kiểm thử bảo mật \(viblo.asia\)](#)