

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**  
**KHOAN AN TOÀN THÔNG TIN**

---



**BÁO CÁO THỰC HÀNH**

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

**Họ và tên: VũThành Long**

**Mã sinh viên: B21DCAT012**

**Nhóm: 06**

**Môn học: Thực tập cơ sở**

**Giảng viên giảng dạy: Nguyễn Hoa Cường**

**Hà Nội, 2024**

I. Mục đích:.....	2
II. Nội dung thực hành:.....	2
2.1 Tìm hiểu lý thuyết:.....	2
2.2. Các bước thực hiện :.....	3
2.2.1. Thử nghiệm với Shoban: .....	3
III. Tài liệu tham khảo.....	20

# I. Mục đích:

Bài thực hành này giúp sinh viên hiểu được mối đe dọa đến từ các công cụ tìm kiếm bao gồm Shodan và Google.

## II. Nội dung thực hành:

### 2.1 Tìm hiểu lý thuyết:

- **Tìm hiểu về công cụ Shodan:**

- Shodan(Sentient Hyper-Optimized Data Access Network), là một công cụ tìm kiếm giống như Google, nhưng thay vì tìm kiếm các trang web, nó tìm kiếm các thiết bị kết nối Internet từ các bộ định tuyến và máy chủ, đến các thiết bị Internet of Things (IoT), như máy cảm ứng nhiệt, TV thông minh, đến các hệ thống phức tạp chi phối một loạt các ngành công nghiệp, bao gồm năng lượng, năng lượng và giao thông vận tải. Shodan có thể tìm thấy bất cứ thứ gì kết nối trực tiếp với internet và nếu các thiết bị đó tồn tại lỗ hổng, Shodan có thể nói với tin tặc mọi thứ họ cần biết để tấn công vào mạng lưới của thiết bị đó.
- Shodan (Sentient Hyper-Optimized Data Access Network) hoạt động theo thuật toán sau:
  - Tạo một địa chỉ IPv4 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 cổ.
  - Lặp lại quá trình trên nhưng với ip và port mới.
- Shodan thu thập dữ liệu trên web của các thiết bị sử dụng mạng máy tính và máy chủ toàn cầu. Shodan có thể cung cấp tất cả các loại thông tin nó nhận được, một số thông tin phổ biến như: Tên thiết bị, địa chỉ IP, cổng mạng, nhà mạng, vị trí địa lý,... Một số thiết bị sử dụng tên đăng nhập và mật khẩu mặc định, mã hiệu thiết bị, phiên bản phần mềm, tất cả đều có thể được khai thác bởi tin tặc. Ngoài các tìm kiếm cơ bản, shodan cung cấp các bộ lọc (filter) để lọc thông tin một cách chính xác và "thông minh"

- **Tìm hiểu về Google Hack:**

- Google Hacking (Google Dorking), là một kỹ thuật thu thập thông tin được sử dụng bởi kẻ tấn công tận dụng các kỹ thuật tìm kiếm nâng cao của Google. Các truy vấn tìm kiếm của Google Hacking có thể được sử dụng để xác định các lỗ hổng bảo mật trong các ứng dụng web, thu thập thông tin cho các mục tiêu tùy ý hoặc riêng lẻ, khám phá các thông báo lỗi tiết lộ thông tin nhạy cảm, khám phá các tệp có chứa thông tin xác thực và dữ liệu nhạy cảm khác.
- Chuỗi tìm kiếm nâng cao được tạo ra bởi kẻ tấn công có thể đang tìm kiếm phiên bản chứa lỗ hổng của ứng dụng web hoặc loại tệp cụ thể (.pwd, .sql ...). Tìm kiếm cũng có thể được giới hạn ở các trang trên một trang web cụ thể hoặc nó có

thể tìm kiếm thông tin cụ thể trên tất cả các trang web, đưa ra một danh sách các trang web có chứa thông tin.

- Chẳng hạn, truy vấn tìm kiếm sau đây sẽ liệt kê các tệp SQL (filetype: sql) có sẵn đã được Google lập chỉ mục trên các trang web nơi danh sách thư mục được bật (Intitle: "Index of").

## 2.2. Các bước thực hiện :

### 2.2.1. Thử nghiệm với Shoban:

#### a. Các bước thực hiện:

Vào website shodan và tạo tài khoản, đăng nhập sử dụng

-Ta thử tìm kiếm 1 bộ lọc là: city:" san francisco" sẽ cho ra kết quả là các website, các cổng dịch vụ, các tổ chức, các hệ điều hành đang chạy trên phạm vi của Hoa Kỳ và thành phố sanfrancisco

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Downloads | Pricing | city:"san francisco" | Account

TOTAL RESULTS  
8,319,174

TOP COUNTRIES

United States 8,276,186  
Argentina 18,918  
Dominican Re... 13,787  
Peru 5,951  
Mexico 2,842  
More...

TOP PORTS

80 987,879  
443 969,391

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

Home - Safe&#039;N&#039;Clear, Inc. | The Communic... 2024-05-14T08:29:55.181775

162.159.136.54  
safenclear.com  
Cloudflare, Inc.  
United States, San Francisco  
cdn

SSL Certificate  
Issued By: Common Name: GTS CA 1P5  
Issued To: Common Name: safenclear

HTTP/1.1 200 OK  
Date: Tue, 14 May 2024 08:25:12 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
Connection: keep-alive  
CF-Ray: 88397f0cdeb090d-LAX  
CF-Cache-Status: DYNAMIC  
Cache-Control: no-cache  
Link: <https://cdn-kejhd.nitrocdn.com>; rel=preconnect, <https://

File Actions Edit View Help  
(kali@ B21AT012-LongVT-Kali-Internal)-[~]  
\$ echo B21DCAT012  
B21DCAT012  
(kali@ B21AT012-LongVT-Kali-Internal)-[~]  
\$ date  
Tue May 14 04:25:54 AM EDT 2024

-Xem chi tiết 1 địa chỉ IP, ta sẽ thấy rõ hơn về các thông tin như hostname, domain, dịch vụ, quốc gia, thành phố, tổ chức và chi tiết các lỗ hổng.

**162.159.136.54** Regular View > Raw Data OpenMapTiles Satellite MapTiler OpenStreetMap contributors

// TAGS: **cdn** // LAST SEEN: 2024-05-14

### General Information

Hostnames: **cloudways.cloud**  
**digacore.com**

Domains: **CLOUDWAYS.CLOUD**  
**DIGACORE.COM**

Country: **United States**

City: **San Francisco**

Organization: **Cloudflare, Inc.**

ISP: **Cloudflare, Inc.**

ASN: **AS13335**

### Open Ports

80 443 2082 2083 2086 2087

8080 8443 8880

// 80 / TCP -968759734 | 2024-05-14T08:21:18.549852

HTTP/1.1 301 Moved Permanently  
Date: Tue, 14 May 2024 08:21:17 GMT  
Content-Type: text/html  
Transfer-Encoding: chunked

kali@B21AT012-LongVT-Kali-Internal: ~

File Actions Edit View Help

```
(kali@B21AT012-LongVT-Kali-Internal)-[~]
$ echo B21DCAT012
B21DCAT012

(kali@B21AT012-LongVT-Kali-Internal)-[~]
$ date
Tue May 14 04:25:54 AM EDT 2024
```

-Sử dụng bộ lọc port để tìm kiếm hai cổng 21 và 22: port:21,22

Shodan Maps Images Monitor Developer More...

SHODAN Explore Downloads Pricing port:21,22 Account

TOTAL RESULTS: **150,212**

TOP COUNTRIES

Partner Spotlight: Looking for a Splunk alternative to store all the Shodan data? Check out [Gravwell](#)

**64.182.213.88** 2024-05-14T08:29:36.773076

CoreSpace, Inc. 220 manhattanclub2.propagation.net FTP server (Version wu-2.6.2(1) Sun Aug 24 11 230 Guest login ok, access restrictions apply.  
214-The following commands are recognized (\* => 's' unimplemented).  
USER PORT STOR MSAM\* RNT0 NLST MKD CDUP  
PASS PA...

**PaperCut Login** 2024-05-14T08:26:45.995323

13.40.100.55 HTTP/1.1 200 OK  
Date: Tue, 14 May 2024 08:26:22 GMT  
Server: nginx  
Content-Type: text/html  
X-Frame-Options: DENY  
X-Content-Type-Options: nosniff  
X-XSS-Protection: 1; mode=block  
Expires: Tue, 14 May 2024 08:26:22 GMT  
Cache-Control: max-age=3600  
Set-Cookie: ...

United States 51,668  
Hong Kong 42,181  
China 10,782  
Germany 5,969  
France 3,669  
More...

TOP ORGANIZATIONS

Unified Layer 7,734  
DXTL HK 4,341

kali@B21AT012-LongVT-Kali-Internal: ~

File Actions Edit View Help

```
(kali@B21AT012-LongVT-Kali-Internal)-[~]
$ echo B21DCAT012
B21DCAT012

(kali@B21AT012-LongVT-Kali-Internal)-[~]
$ date
Tue May 14 04:25:54 AM EDT 2024
```

Sử dụng bộ lọc port để tìm kiếm hai cổng 21, 22 và country để tìm kiếm tại Việt Nam: port:21,22 country:"VN"

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Downloads | Pricing | port:21,22 country:"VN" | Search | Account

TOTAL RESULTS: 950

TOP CITIES:

- Ho Chi Minh City: 430
- Hanoi: 321
- Thuận An: 20
- Biên Hòa: 16
- Đà Nẵng: 9

More...

TOP ORGANIZATIONS:

- Viettel Group: 147
- Vietnam Posts and Telecommunications: 68
- Super Online Data: 47
- GMO-Z.com: 36
- FPT Telecom Company: 24

More...

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB

118.69.168.77

2024-05-14T07:35:39.263055

FPT Telecom

SSL Certificate

Issued By: FPT Telecom

Name: Viet Nam, Ho Chi Minh City

Issued To: localhost

Organization: none

Supported Versions: TLSv1.2

Tags: starttls, self-signed

171.238.239.116

kali@B21AT012-LongVT-Kali-Internal: ~

File Actions Edit View Help

(kali@B21AT012-LongVT-Kali-Internal)-[~]

\$ echo B21DCAT012

B21DCAT012

(kali@B21AT012-LongVT-Kali-Internal)-[~]

\$ date

Tue May 14 04:25:54 AM EDT 2024

Xem chi tiết các thông tin của địa chỉ: 118.69.168.77

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Downloads | Pricing | port:21,22 country:"VN" | Search | Account

TOTAL RESULTS: 950

TOP CITIES:

- Ho Chi Minh City: 430
- Hanoi: 321
- Thuận An: 20
- Biên Hòa: 16
- Đà Nẵng: 9

More...

TOP ORGANIZATIONS:

- Viettel Group: 147
- Vietnam Posts and Telecommunications: 68
- Super Online Data: 47
- GMO-Z.com: 36
- FPT Telecom Company: 24

More...

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB

118.69.168.77

2024-05-14T07:35:39.263055

FPT Telecom

SSL Certificate

Issued By: FPT Telecom

Name: Viet Nam, Ho Chi Minh City

Issued To: localhost

Organization: none

Supported Versions: TLSv1.2

Tags: starttls, self-signed

171.238.239.116

kali@B21AT012-LongVT-Kali-Internal: ~

File Actions Edit View Help

(kali@B21AT012-LongVT-Kali-Internal)-[~]

\$ echo B21DCAT012

B21DCAT012

(kali@B21AT012-LongVT-Kali-Internal)-[~]

\$ date

Tue May 14 04:25:54 AM EDT 2024

Sử dụng bộ lọc product để tìm kiếm: “product: Apache”

Shodan

Maps

Images

Monitor

Developer

More...

SHODAN

Explore

Downloads

Pricing

product:Apache

Q

Account

TOTAL RESULTS

15,729,597

TOP COUNTRIES

United States	5,061,136
Germany	1,527,093
Japan	1,505,484
France	729,183
China	719,566
More...	

View Report

Browse Images

View on Map

Product Spotlight: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

301 Moved Permanently

209.10.40.136

gracernote.com

web.glob.gracernote.com

Gracernote

United States, San Jose

SSL Certificate

Issued By:

Common Name:

Name:

GlobalSign RSA OV SSL CA 2018

Organization:

GlobalSign nv-sa

Issued To:

Common Name:

\*.gracernote.com

Organization:

GRACENOTE INC.

Supported SSL Versions:

TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 301 Moved Permanently

Date: Tue, 14 May 2024 08:31:02 GMT

Server: Apache

Location: http://www.gracernote.com/

Content-Length: 233

Content-Type: text/html; charset=iso-8859-1

X-Varnish: 545489805

Age: 0

Via: 1.1 varnish-v4

Connection: keep-alive

2024-05-14T08:35:45.844956

Xem cụ thể một địa chỉ IP

San Jose

Cupertino

209.10.40.136

Regular View

Raw Data

OpenMapTiles Satellite MapTiler OpenStreetMap contributors

General Information

Hostnames

gracernote.com

web.glob.gracernote.com

Domains

GRACENOTE.COM

Country

United States

City

San Jose

Organization

Gracernote

ISP

Quality Technology Services, LLC

ASN

AS40913

Open Ports

80

443

80 / TCP

1285199853 | 2024-05-14T08:35:10.564907

Apache httpd

HTTP/1.1 307 Temporary Redirect

Date: Tue, 14 May 2024 07:10:54 GMT

Server: Apache

X-XSS-Protection: 1; mode=block

X-Content-Type-Options: nosniff

6

Organization

Gracernote

ISP

Quality Technology Services, LLC

ASN

AS40913

```

server: Apache
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Referrer-Policy: no-referrer-when-downgrade
X-Safe-Redirect-Manager: true
X-Safe-Redirect-ID: 22462
Location: https://www.nielsen.com/solutions/content-metadata/
Content-Length: 0
Content-Type: text/html
X-Varnish: 585433898 586744419
Age: 5045
Via: 1.1 varnish-v4
Connection: keep-alive

```

kali@B21AT012-LongVT-Kali-Internal: ~

File Actions Edit View Help

(kali@B21AT012-LongVT-Kali-Internal)-[~

\$ echo B21DCAT012

B21DCAT012

(kali@B21AT012-LongVT-Kali-Internal)-[~

\$ date

Tue May 14 04:25:54 AM EDT 2024

(kali@B21AT012-LongVT-Kali-Internal)-[~

\$

// 443 / TCP

470582980 | 2024-05-14T08:35:45.844956

Apache httpd

HTTP/1.1 301 Moved Permanently

Date: Tue, 14 May 2024 08:31:02 GMT

Server: Apache

Location: http://www.gracernote.com/

Content-Length: 233

Content-Type: text/html; charset=iso-8859-1

X-Varnish: 545489805

Age: 0

Via: 1.1 varnish-v4

Connection: keep-alive

Sử dụng bộ lọc hostname để tìm kiếm các hostname của google và facebook

Shodan

Maps

Images

Monitor

Developer

More...

SHODAN

Explore

Downloads

Pricing

hostname:google.com,facebook.com

Q

Account

TOTAL RESULTS

172,358

TOP COUNTRIES

United States	139,838
Brazil	3,740
Russian Feder...	2,611
India	2,245
Germany	1,146

View Report

Browse Images

View on Map

Product Spotlight: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

104.133.128.200

2024-05-14T08:31:26.363732

ncc-poc-104-133-128-200.corp.google.com

Google LLC

United States, Mountain View

104.133.128.193

No data returned

ncc-poc-104-133-128-193.corp.google.com

Google LLC

United States, Mountain View

104.133.128.178

No data returned

ncc-poc-104-133-128-178.corp.google.com

Google LLC

United States, Mountain View

kali@B21AT012-LongVT-Kali-Internal: ~

File Actions Edit View Help

(kali@B21AT012-LongVT-Kali-Internal)-[~

\$ echo B21DCAT012

B21DCAT012

(kali@B21AT012-LongVT-Kali-Internal)-[~

\$ date

Tue May 14 04:25:54 AM EDT 2024

(kali@B21AT012-LongVT-Kali-Internal)-[~

\$

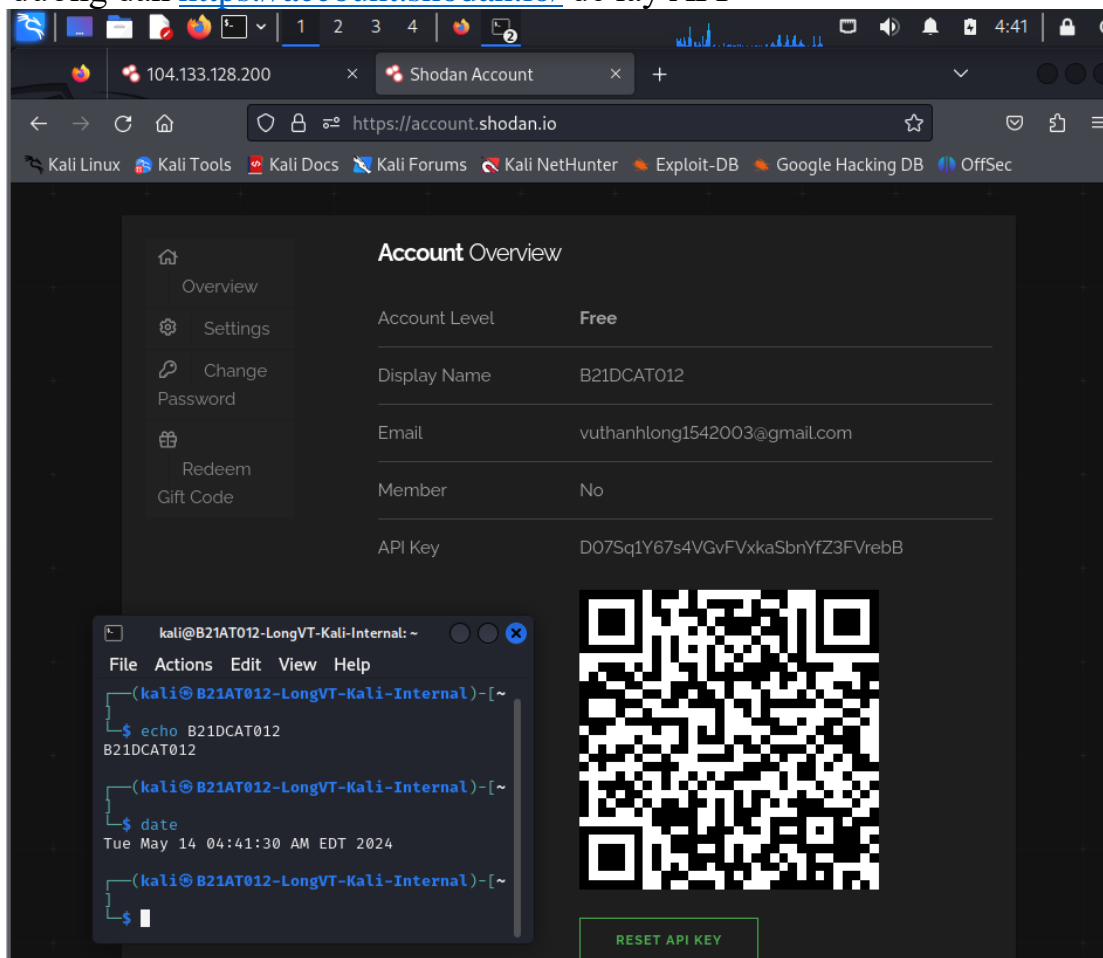




Khai báo sử dụng mô đun tấn công: use auxiliary/gather/shodan\_search

```
kali@B21AT012-LongVT-Kali-Internal: ~  
File Actions Edit View Help  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > search shodan  
  
Matching Modules  
  
# Name                                     Disclosure Date  
---  
0 auxiliary/admin/http/hikvision_unauth_pwd_reset_cve_2017_7921 2017-09-23  
normal Yes Hikvision IP Camera Unauthenticated Password Change Via Impro-  
per Authentication Logic  
1 auxiliary/scanner/http/influxdb_enum 2016-07-01  
normal No InfluxDB Enum Utility  
2 auxiliary/gather/prometheus_api_gather 2016-07-01  
normal No Prometheus API Information Gather  
3 auxiliary/gather/shodan_honeyscore  
normal No Shodan Honeyscore Client  
4 auxiliary/gather/shodan_host  
normal No Shodan Host Port  
5 auxiliary/gather/shodan_search  
normal No Shodan Search  
6 auxiliary/scanner/http/smt_ipmi_49152_exposure 2014-06-19  
normal No Supermicro Onboard IPMI Port 49152 Sensitive File Exposure  
7 auxiliary/gather/hikvision_info_disclosure_cve_2017_7921 2017-09-23  
normal Yes Unauthenticated information disclosure such as configuration,  
credentials and camera snapshots of a vulnerable Hikvision IP Camera
```

Ấn vào đường dẫn <https://account.shodan.io/> để lấy API



Đặt truy vấn muốn tìm kiếm là webcamxp

Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng

```
kali@B21AT012-LongVT-Kali-Internal: ~  
File Actions Edit View Help  
credentials and camera snapshots of a vulnerable Hikvision IP Camera  
  
Interact with a module by name or index. For example info 7, use 7 or use auxiliary/gather/hikvision_info_disclosure_cve_2017_7921  
  
msf6 > use auxiliary/gather/shodan_search  
msf6 auxiliary(gather/shodan_search) > set SHODAN_APIKEY D07Sq1Y67s4VGvFVxkaSbnYfZ3FVrebB  
SHODAN_APIKEY => D07Sq1Y67s4VGvFVxkaSbnYfZ3FVrebB  
msf6 auxiliary(gather/shodan_search) > set QUERY webcamxp  
QUERY => webcamxp  
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       | A filename to store the list of IPs                  |
| QUERY         | webcamxp                         | yes      | Keywords you want to search for                      |
| REGEX         | .*                               | yes      | Regex search for a specific IP/City/Country/Hostname |
| SHODAN_APIKEY | D07Sq1Y67s4VGvFVxkaSbnYfZ3FVrebB | yes      | The SHODAN API key                                   |

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

Chạy lệnh “run” để tìm kiếm

Do account là account thường nên phần key yêu cầu không đáp ứng được cho nên khi run hệ thống thông báo quyền access cao hơn. Mong thầy thông cảm ạ

```
kali@B21AT012-LongVT-Kali-Internal: ~  
File Actions Edit View Help  
ry/gather/hikvision_info_disclosure_cve_2017_7921  
  
msf6 > use auxiliary/gather/shodan_search  
msf6 auxiliary(gather/shodan_search) > set SHODAN_APIKEY D07Sq1Y67s4VGvFVxkaSbnYfZ3FVrebB  
SHODAN_APIKEY => D07Sq1Y67s4VGvFVxkaSbnYfZ3FVrebB  
msf6 auxiliary(gather/shodan_search) > set QUERY webcamxp  
QUERY => webcamxp  
msf6 auxiliary(gather/shodan_search) > show options  
  
Module options (auxiliary/gather/shodan_search):  

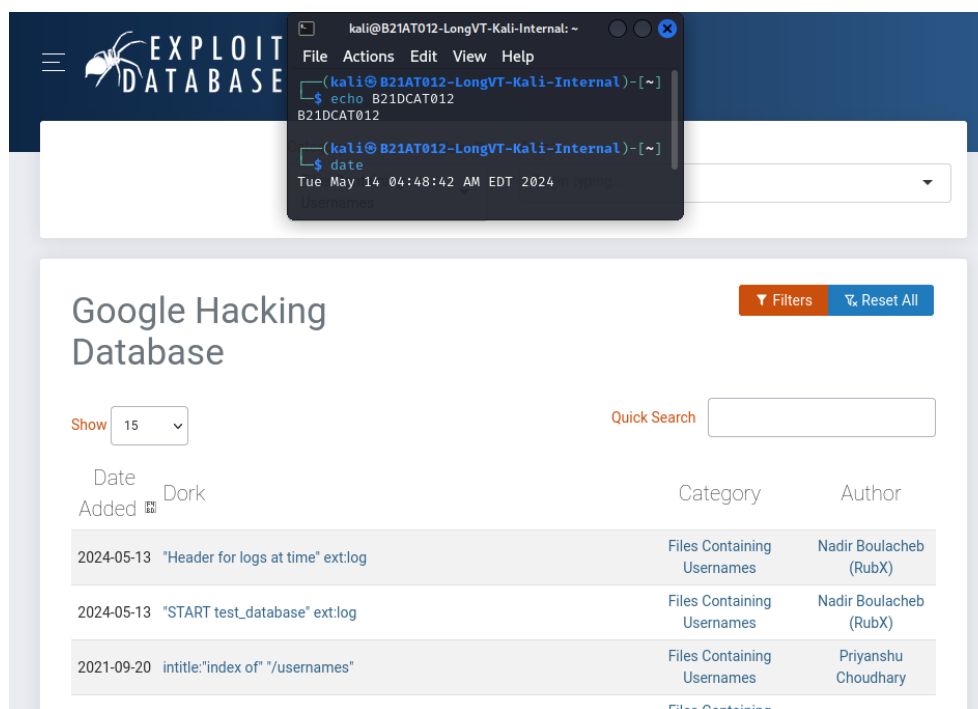

| Name          | Current Setting                  | Required | Description                                          |
|---------------|----------------------------------|----------|------------------------------------------------------|
| DATABASE      | false                            | no       | Add search results to the database                   |
| MAXPAGE       | 1                                | yes      | Max amount of pages to collect                       |
| OUTFILE       |                                  | no       | A filename to store the list of IPs                  |
| QUERY         | webcamxp                         | yes      | Keywords you want to search for                      |
| REGEX         | .*                               | yes      | Regex search for a specific IP/City/Country/Hostname |
| SHODAN_APIKEY | D07Sq1Y67s4VGvFVxkaSbnYfZ3FVrebB | yes      | The SHODAN API key                                   |

  
View the full module info with the info, or info -d command.  
msf6 auxiliary(gather/shodan_search) > run  
  
[-] No results. Error: Requires membership or higher to access  
[*] Auxiliary module execution completed  
msf6 auxiliary(gather/shodan_search) > 
```

Thử nghiệm với Google Hacking Database

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

Nhấn vào nút Filters đầu bên phải của trang và mũi tên xổ menu để khai thác các mục. Các mục ở đây bao gồm Footholds, Files Containing Usernames, Sensitive Directories, Web Server Detection, và các thứ khác

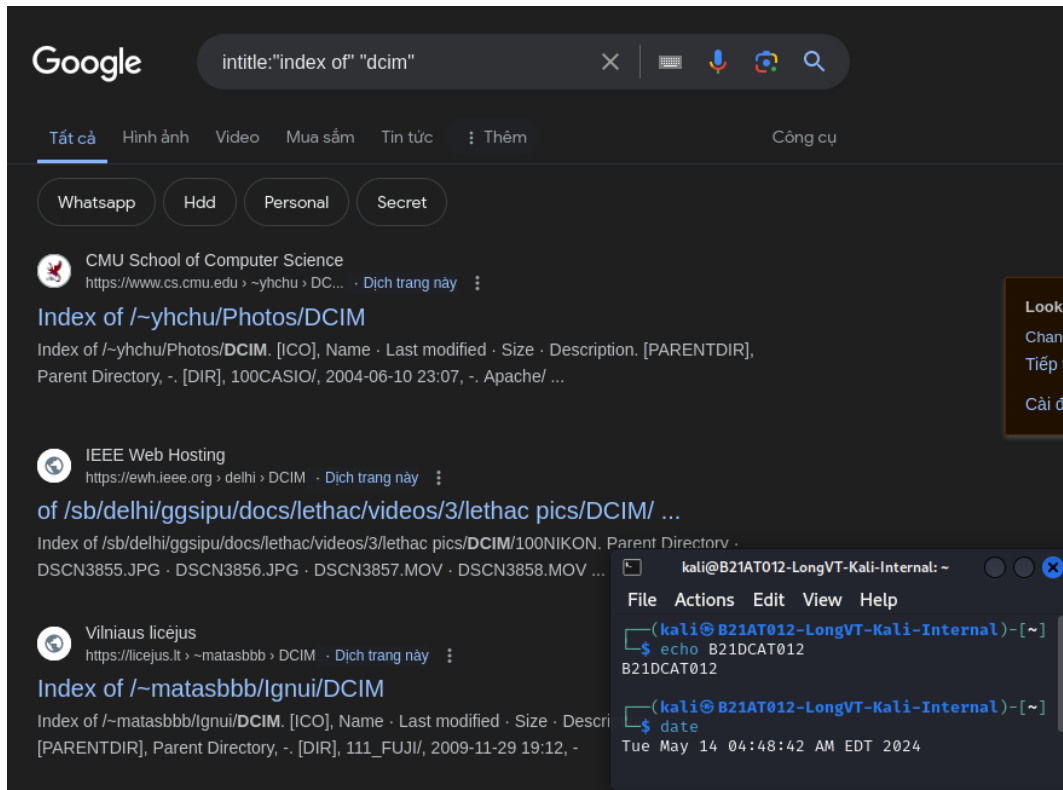


Ta chọn Vulnerable Servers và hiện ra trang thông tin có liên quan bao gồm thông tin tác giả, mô tả về tìm kiếm và các thông tin khác.



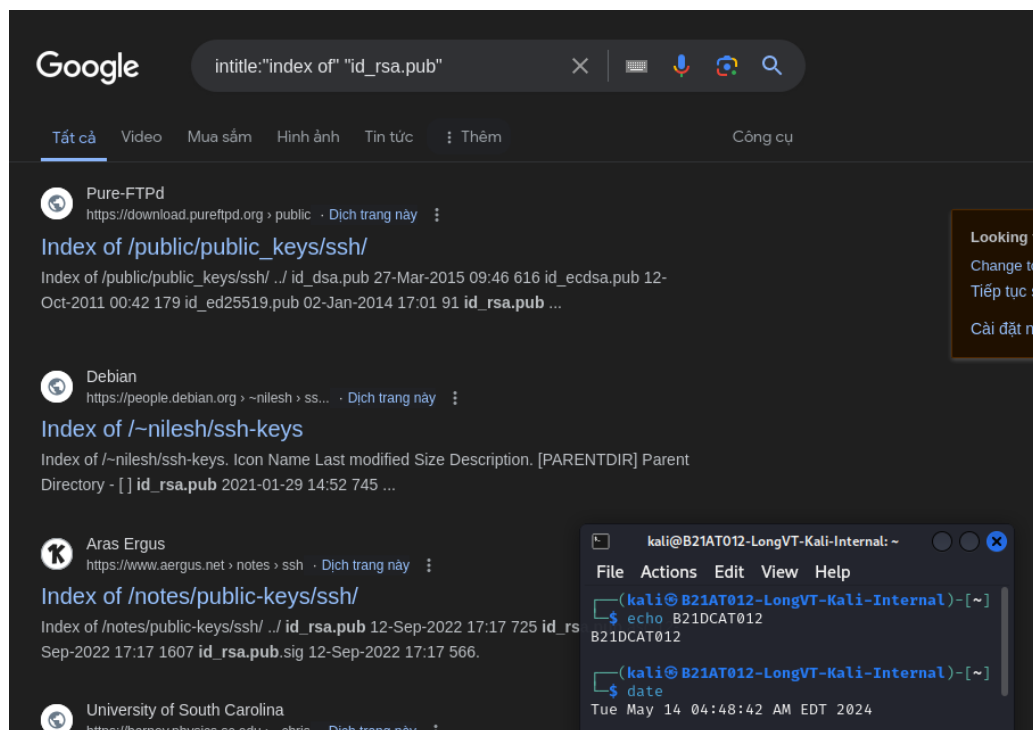
-Thử nghiệm với truy vấn tìm kiếm intitle: “Index of” “DCIM”, Google sẽ trả về kết quả của các bộ sưu tập ảnh mà mọi người không biết ở đó.  
 +intitle: tìm kiếm trong phần title của trang web

+DCIM: Là thư mục gốc lưu tất cả các ảnh mà bạn đã chụp trên các máy ảnh và điện thoại



**Google dork** - một chức năng mà google cung cấp để việc tìm kiếm hiệu quả hơn.

Kết quả của dorks này chứa các Thư mục nhạy cảm với các khóa ssh



## Index of /public/public\_keys/ssh/

<a href="#">../</a>		
<a href="#">id_dsa.pub</a>	27-Mar-2015 09:46	616
<a href="#">id_ecdsa.pub</a>	12-Oct-2011 00:42	179
<a href="#">id_ed25519.pub</a>	02-Jan-2014 17:01	91
<a href="#">id_rsa.pub</a>	27-Mar-2015 11:05	742

```
kali@B21AT012-LongVT-Kali-Internal: ~  
File Actions Edit View Help  
(kali@B21AT012-LongVT-Kali-Internal)-[~]  
$ echo B21DCAT012  
B21DCAT012  
(kali@B21AT012-LongVT-Kali-Internal)-[~]  
$ date  
Tue May 14 04:48:42 AM EDT 2024
```

## Index of /public/public\_keys/ssh/

<a href="#">../</a>	27-Mar-2015 09:46	616
<a href="#">id_dsa.pub</a>	12-Oct-2011 00:42	179
<a href="#">id_ecdsa.pub</a>		
<a href="#">id_ed25519.pub</a>		
<a href="#">id_rsa.pub</a>		

```
kali@B21AT012-LongVT-Kali-Internal: ~/Downloads  
File Actions Edit View Help  
(kali@B21AT012-LongVT-Kali-Internal)-[~/Downloads]  
$ cat id_rsa.pub  
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDDIrnZeP0eMeQ2KXJCPmw3jdfhh5QnbZu6sRCgh8MReeqZcKTU1KnXaMZ/m4pu  
4jeXp+RAnpNhdNTy8f2CXCmP/GHfNDN1thpNk4+5qkAkMBZLxRHP6n2n5A6W0pw8NW3VV9YeH4AtdCIq0tc+15oAmcR3vBx4wZrFV  
LWH3DLS88hsgftAvtGUFOn1r4oEj7CB6o7XcnB1L8yVCMERJLRu4Kk48QvSRU/5JD4r+4NeMbieMa7jpjIpiQ/iCych5CPd1Tjp0S  
hkWQp3eqzPQ8yst6YieiViYy5MzUDGZvLn3yVtMWyPtKrsunocCvpcts81k/cghq0Ns+9nWqa/smpZw8GbXFOPUZeu7wnlOQFkghI  
TALep9Qupm/hbTMOZHxomi4n3xuby3C/istFrqIIiEcBCT9i/UWGOVXX13k3M3yQtgA+u2i2zaeNpHj2zM/r6Ilt3NP5RPuRxnryL  
ujcMvQF4LWSEhB5OZFjUSCnbuQCK0sd1CsMaprmuv2EK0LS3mma55AA7HCIUdMfoAq7uWQdolkdvc7xjw770L8QfaKGztjzmsfTF9  
gFH5HJxwQZDYzf+epH0p7ThhxuRUz0QszYZf06DbPt0y/F19nK0fckFs6CoXX5pu0fLLDrhVSSljt2AbIt03NOZXW5OMT4IBGWwFN  
gyc9lnHjPI+KCRQ= fdenis@crypto.sx  
(kali@B21AT012-LongVT-Kali-Internal)-[~/Downloads]  
$
```

-Tìm log có tên người dùng và mật khẩu, địa chỉ e-mail, URL mà những thông tin đăng nhập này được sử dụng



Google allintext:username,password filetype:log X

Hình ảnh Video Admin Invalid Mua sắm TOTOLINK Godsteam PPP > Tất cả bộ lọc

**Free**  
http://remikaing.free.fr > ... > Dịch trang này

**http://remikaing.free.fr/PC-DE-SARGERAN-mC:%5CUser...**  
... username : Sargerans password : zzqgh9qy ----- serv -  
http://snowtigers.net username : Maxter password : WOW071789788 ...

**GitHub**  
https://github.com > SSH-worm > blob > Dịch trang này

**SSH-worm/worm.log at master**  
... username: admin password: admin INFO:root:Failed... INFO:root:Trying with username:  
admin password: password INFO:root:Failed... INFO:root:Trying with ...

**GitHub**  
https://github.com > blob > develop > c... > Dịch trang này

**cheese.log - ZHYI-source/zy-express-sequelize-mysql**  
... username:"周义","password":"123456","nickName":"MK","verificationCode":  
{"data":{"id":1,"username":"周义","password":"123456","nickName":"MK ...

**FreeAccount.biz**  
https://freeaccount.biz > accounts > us... > Dịch trang này

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

```
serv - http://fr-fr.facebook.com
email      : roi_de_la_casse@hotmail.com
pass       : zzqgh9qy
-----

serv - http://fr.youtube.com
username   : Sargerans
password   : zzqgh9qy
-----

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

serv - https://login.facebook.com
email      : roi_de_la_casse@hotmail.com
pass       : zzqgh9qy
-----

serv - http://hostarea.org
login      : Sargeran
pass       : zzqgh9qy
-----

serv - http://www.facebook.com
email      : roi_de_la_casse@hotmail.com
pass       : zzqgh9qy
-----

serv - http://www.forumactif.com
:
password2  : zzqgh9qy
-----

serv - http://pubgoogle.forumactif.net
username   : Admin
password   : zzqgh9qy
-----
```

**kali@B21AT012-LongVT-Kali-Internal: ~**

File Actions Edit View Help

```
(kali@B21AT012-LongVT-Kali-Internal)-[~]
$ echo B21DCAT012
B21DCAT012

(kali@B21AT012-LongVT-Kali-Internal)-[~]
$ date
Tue May 14 04:48:42 AM EDT 2024
```

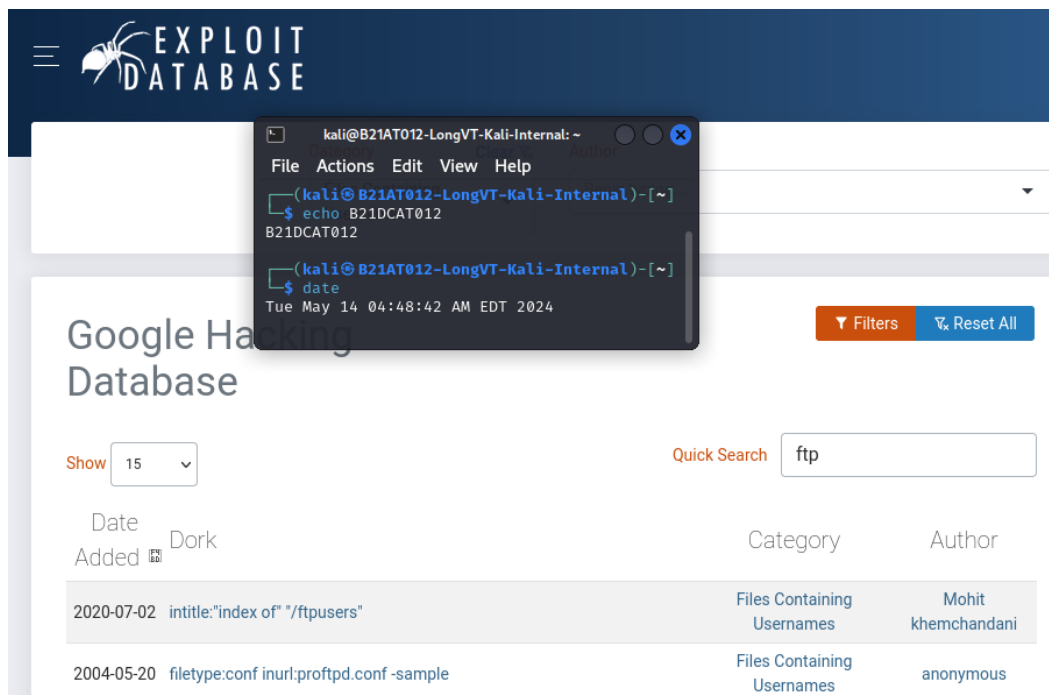
**kali@B21AT012-LongVT-Kali-Internal: ~**

File Actions Edit View Help

```
(kali@B21AT012-LongVT-Kali-Internal)-[~]
$ echo B21DCAT012
B21DCAT012

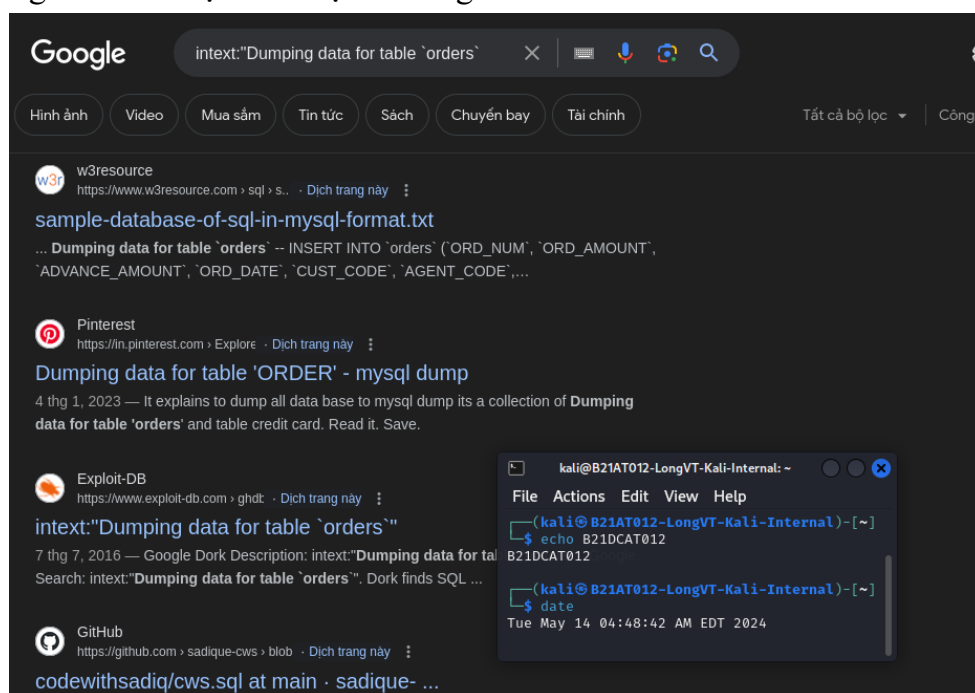
(kali@B21AT012-LongVT-Kali-Internal)-[~]
$ date
Tue May 14 04:48:42 AM EDT 2024
```

- 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).



Chọn 5 Google dork, mỗi loại thuộc một danh mục khác nhau và giải thích cách chúng có thể có nguy hiểm như thế nào. Theo tùy chọn, hãy nhấp vào siêu liên kết cho các dork thực tế của Google để xem kết quả nào được trả về

- Google dork "intext:"Dumping data for table `orders`"" được dùng để tìm nội dung cơ sở dữ liệu của một số trang web:



Nhấp vào một liên kết, ta thu được thông tin và nội dung của cơ sở dữ liệu dưới đây.



```
-- phpMyAdmin SQL Dump
-- version 3.3.9
-- http://www.phpmyadmin.net
--
-- Host: localhost
-- Generation Time: Feb 08, 2014 at 06:53 AM
-- Server version: 5.1.36
-- PHP Version: 5.3.0

SET SQL_MODE="NO_AUTO_VALUE_ON_ZERO";

--
-- Database: `sample`
--

--
-- Table structure for table `agents`
--

CREATE TABLE IF NOT EXISTS `agents` (
  `AGENT_CODE` varchar(6) NOT NULL DEFAULT '',
  `AGENT_NAME` varchar(40) DEFAULT NULL,
  `WORKING_AREA` varchar(35) DEFAULT NULL,
  `COMMISSION` decimal(10,2) DEFAULT NULL,
  `PHONE_NO` varchar(15) DEFAULT NULL,
  `COUNTRY` varchar(25) DEFAULT NULL,
  PRIMARY KEY (`AGENT_CODE`)
) ENGINE=MyISAM DEFAULT CHARSET=latin1;

--
-- Dumping data for table `agents`
--

INSERT INTO `agents` (`AGENT_CODE`, `AGENT_NAME`, `WORKING_AREA`, `COMMISSION`, `PHONE_NO`, `COUNTRY`) VALUES
('A007', 'Ramasundar', 'Bangalore', '0.15', '077-25814763', 'IN'),
('A003', 'Alex', 'London', '0.13', '075-12458969', 'IN'),
('A008', 'Alford', 'New York', '0.12', '044-25874365', 'IN'),
('A011', 'Ravi Kumar', 'Bangalore', '0.15', '077-45625874', 'IN'),
('A010', 'Santakumar', 'Chennai', '0.14', '007-22388644', 'IN'),
('A012', 'Lucida', 'San Jose', '0.12', '044-52981425', 'IN'),
('A005', 'Anderson', 'Brisban', '0.13', '045-21447739', 'IN'),
('A001', 'Subbarao', 'Bangalore', '0.14', '077-12346674', 'IN');
```

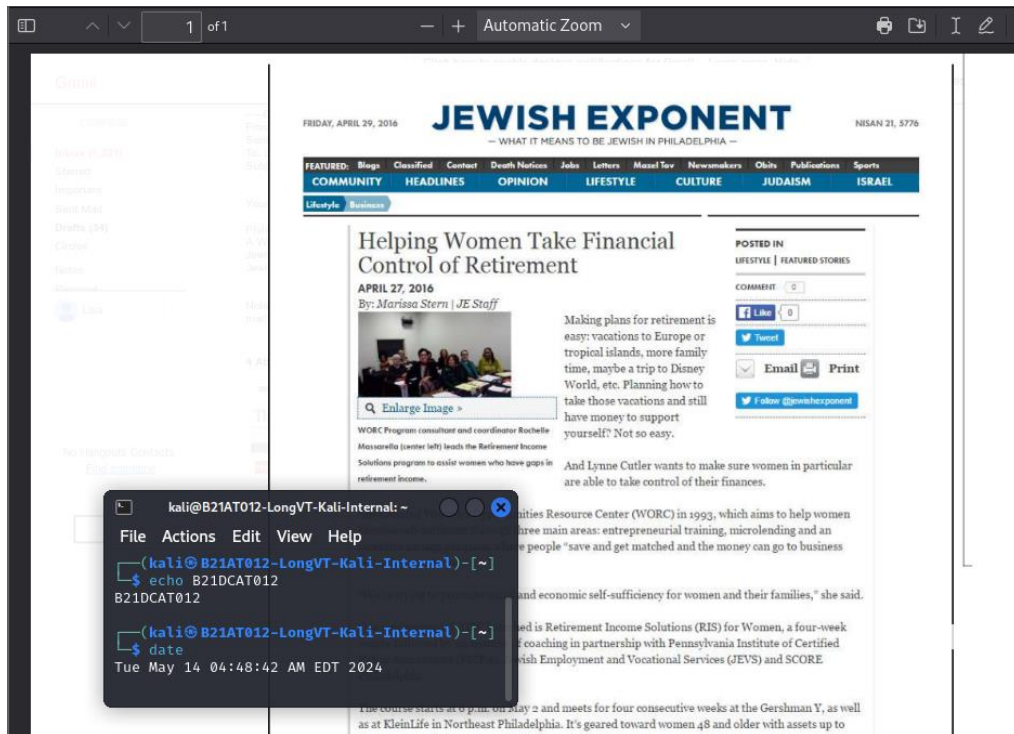
- Google dork “mail/u/0 filetype:pdf” được dùng để tìm các văn bản tài liệu định dạng pdf gửi từ Email.

Google search results for "mail/u/0 filetype:pdf".

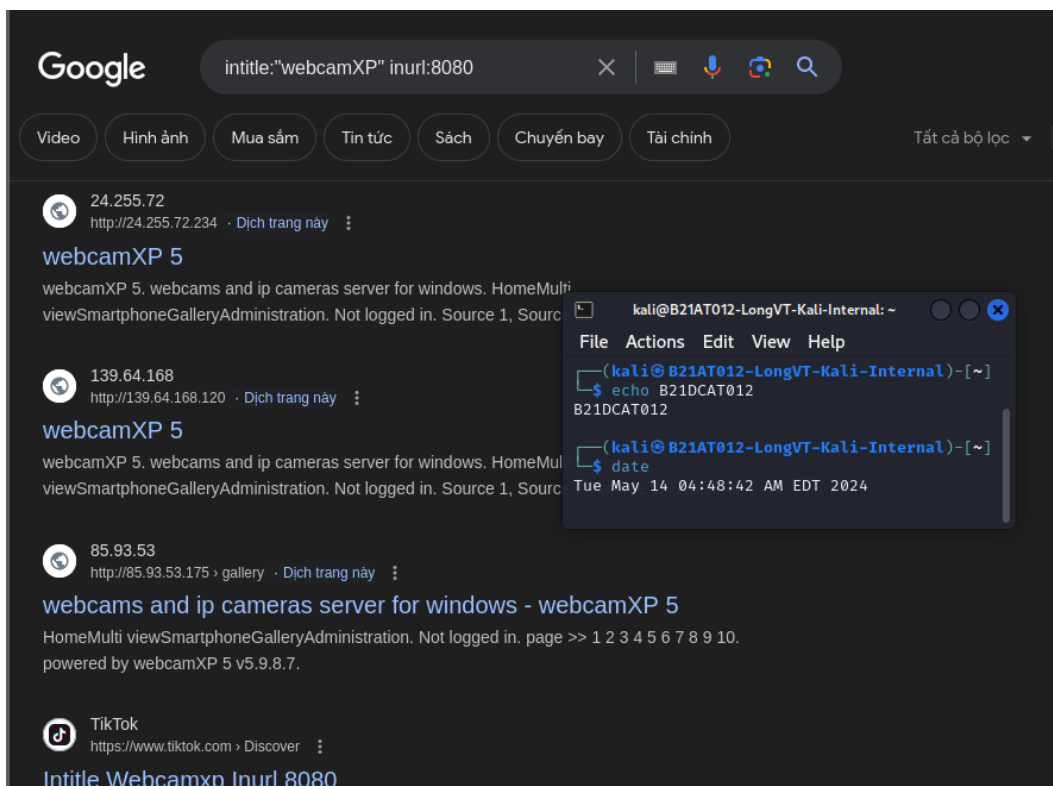
Results include:

- worc-pa.com: <https://www.worc-pa.com/docs/PDF>
- Gmail: <https://mail.google.com/mail/u/0/#inbox/155fa8c60dabb50f?projector=1.1/1> (1,221). Starred. Important. Sent Mail. Drafts (34). Circles. Notes. 1 trang
- Phường Mộ Lao |: <http://molao.hadong.hanoi.gov.vn/default/files/PDF>
- b2.pdf: <https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox?projector=1.1/1>
- mৎস্য অধিদপ্তর: [https://fisheries.portal.gov.bd/files/office\\_order/PDF](https://fisheries.portal.gov.bd/files/office_order/PDF)
- 2023-03-01-07-18-9259da67c1662825f57a0a05b67934e6.pdf: <https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox?projector=1.1/1> 1 thg 3, 2023 — 1 trang

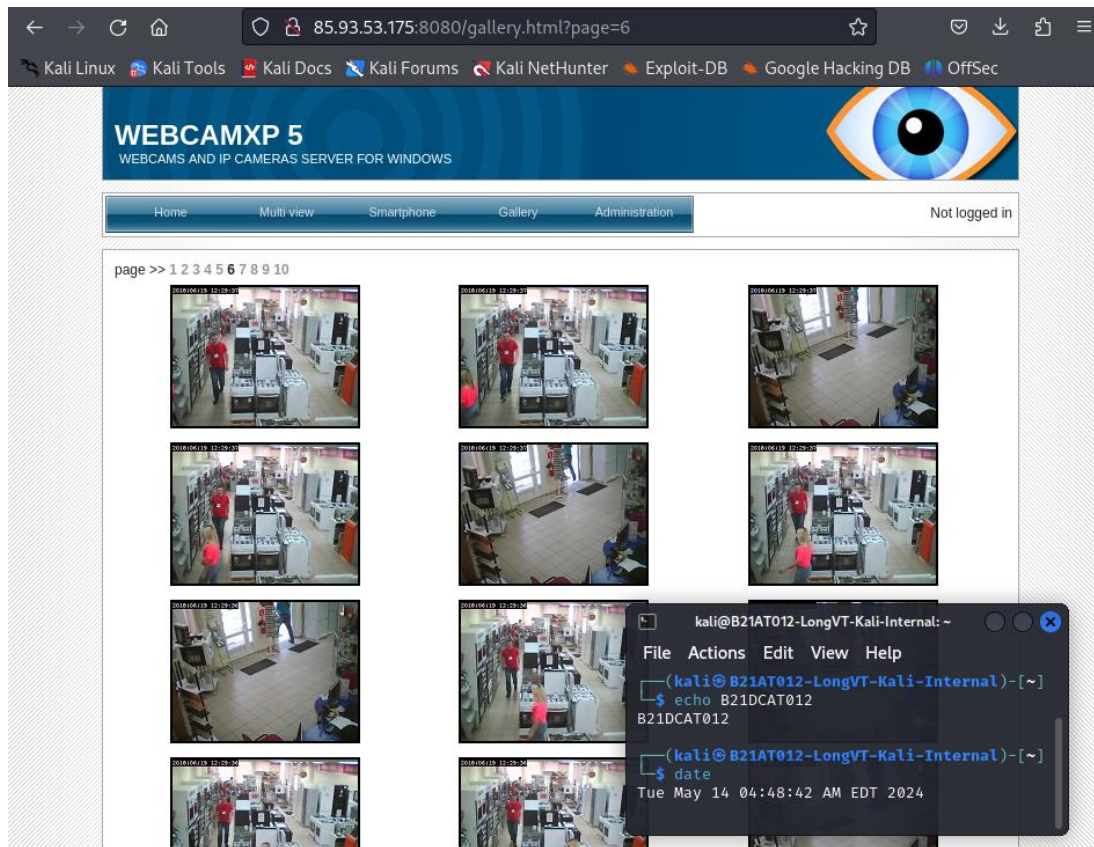
Nhấp vào một liên kết và nhận được văn bản dưới đây.



- Google dork “intitle:”webcamXP” inurl:8080” được dùng để tìm các dịch vụ camera webcamXP được công khai hoặc sử dụng tên người dùng và mật khẩu dễ nhận biết:

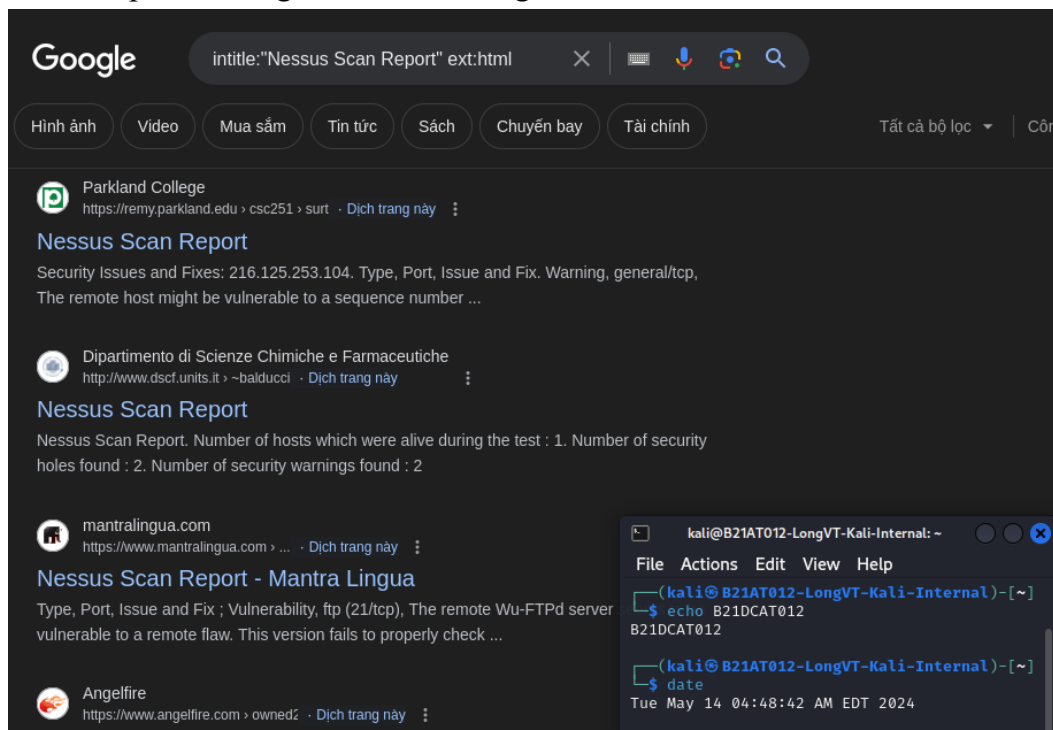


Nhấp vào liên kết và thu được các hình ảnh webcam gửi về.



*Webcam đang hoạt động*

- Google dork “intitle:”Nessus Scan Report” ext:html” được dùng để tìm các báo cáo dò quét lỗ hổng bảo mật sử dụng Nessus:



Nhấp vào liên kết và nhận được báo cáo chứa các lỗ hổng bảo mật.

Nessus Scan Report	
This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.	

Scan Details	
Hosts which were alive and responding during test	1
Number of security holes found	0
Number of security warnings found	3

Host List	
Host(s)	Possible Issue
216.125.253.104	Security warning(s) found

[ return to top ]

Analysis of Host		
Address of Host	Port/Service	Issue regarding Port
216.125.253.104	general/tcp	Security warning(s) found
216.125.253.104	ssh (22/tcp)	Security warning(s) found
216.125.253.104	general/udp	Security notes found

Security Issues		
Type	Port	Issue and Fix
Warning	general/tcp	<p>The remote host might be vulnerable to a sequence number approximation bug, which may allow an attacker to send spoofed RST packets to the remote host and close established connections.</p> <p>This may cause problems for some dedicated services (BGP, a VPN over TCP, etc...).</p> <p>Solution : See <a href="http://www.securityfocus.com/bid/10183/solution/">http://www.securityfocus.com/bid/10183/solution/</a></p>

```
kali@B21AT012-LongVT-Kali-Internal: ~
File Actions Edit View Help
(kali@B21AT012-LongVT-Kali-Internal)-[~]
$ echo B21DCAT012
B21DCAT012
(kali@B21AT012-LongVT-Kali-Internal)-[~]
$ date
Tue May 14 04:48:42 AM EDT 2024
```

- Google dork “inurl:adm/login.jsp.bak” được dùng để tìm các trang đăng nhập quản trị website từ đó sử dụng các phương thức tấn công để chiếm quyền điều khiển:

Google search results for "inurl:adm/login.jsp.bak". The results show several pages with login forms, including "203.105.227", "175.96.48", "203.105.230", and "203.105.229". Each result includes the URL, a brief description of the page, and a "Dịch trang này" link. An inset terminal window shows a Kali Linux command prompt with the command "echo B21DCAT012" and the output "B21DCAT012", and the command "date" showing the time "Tue May 14 04:48:42 AM EDT 2024".

### **III. Tài liệu tham khảo**

- <https://money.cnn.com/gallery/technology/security/2013/05/01/shodan-most-dangerous-internet-searches/index.html>
- Principles of Computer Security: CompTIA Security+ and Beyond