

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**

**BỘ MÔN THỰC TẬP CƠ SỞ**

-----



**BÀI 14:**  
**PHÁT HIỆN LỖ HỔNG**  
**VỚI CÔNG CỤ TÌM KIẾM**

**Giảng viên : Nguyễn Ngọc Diệp**

**Sinh viên : Nguyễn Đức Anh**

**Mã sinh viên : B21DCAT031**

**Hệ : Đại học chính quy**

**Hà Nội, 3/2024**

## Table of Contents

1. Mục đích .....	3
2. Nội dung thực hành .....	3
2.1 <i>Tìm hiểu lý thuyết</i> .....	3
<b>a. Tìm hiểu về công cụ Shodan</b> .....	3
<b>b. Tìm hiểu về Google Hack</b> .....	3
2.2 <i>Tài liệu tham khảo</i> .....	4
2.3 <i>Chuẩn bị môi trường</i> .....	4
2.4 <i>Các bước thực hiện</i> .....	4
2.4.1. Thử nghiệm với Shodan .....	4
2.4.2. Thử nghiệm với Google Hacking Database .....	10
1. Kết quả đạt được .....	20

# 1. 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.

## 2. Nội dung thực hành

### 2.1 Tìm hiểu lý thuyết

#### a. 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 công cụ.
- 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"

#### b. 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 Tài liệu tham khảo

- <https://money.cnn.com/gallery/technology/security/2013/05/01/shodan-most-%20dangerous-internet-searches/index.html>
- Principles of Computer Security: CompTIA Security+ and Beyond

## 2.3 Chuẩn bị môi trường

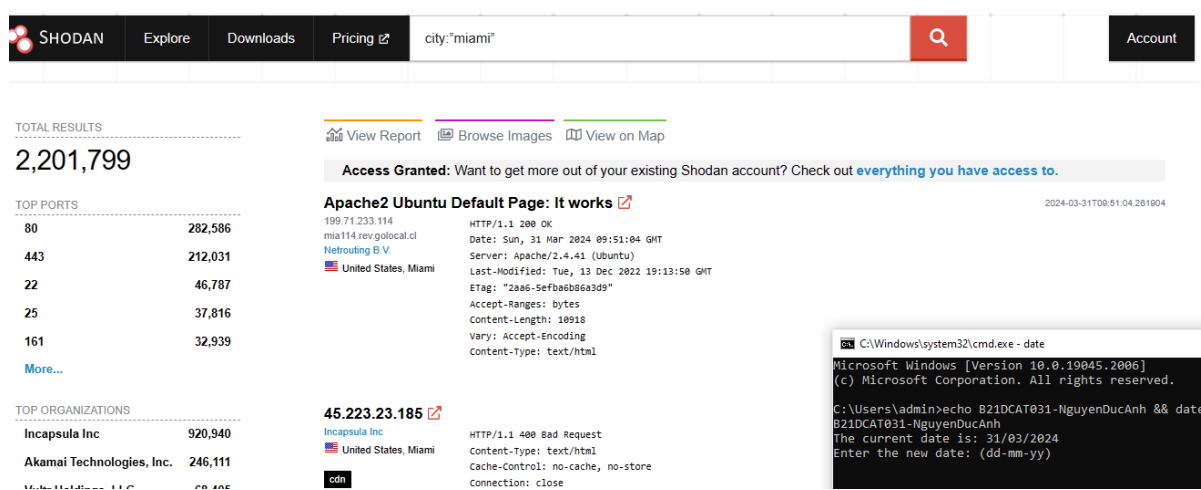
- Phần mềm VMWare Workstation hoặc Virtual Box hoặc các phần mềm ảo hóa khác.
- Máy ảo Kali Linux

## 2.4 Các bước thực hiện

### 2.4.1. Thử nghiệm với Shodan

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

Ta thử tìm kiếm 1 bộ lọc là: city:"miami" 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 Miami



SHODAN Explore Downloads Pricing city:"miami" Account

TOTAL RESULTS  
2,201,799

TOP PORTS

Port	Count
80	282,586
443	212,031
22	46,787
25	37,816
161	32,939

More...

TOP ORGANIZATIONS

Organization	Count
Incapsula Inc	920,940
Akamai Technologies, Inc.	246,111

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

Apache2 Ubuntu Default Page: It works

199.71.233.114  
mia114.rev.golocal.cl  
Netrouting B.V.  
United States, Miami

HTTP/1.1 200 OK  
Date: Sun, 31 Mar 2024 09:51:04 GMT  
Server: Apache/2.4.41 (Ubuntu)  
Last-Modified: Tue, 13 Dec 2022 19:13:59 GMT  
ETag: "2a86-5efba6b86a3d9"  
Accept-Ranges: bytes  
Content-Length: 10918  
Vary: Accept-Encoding  
Content-Type: text/html

45.223.23.185

Incapsula Inc  
United States, Miami

HTTP/1.1 400 Bad Request  
Content-Type: text/html  
Cache-Control: no-cache, no-store  
Connection: close

```
C:\Windows\system32\cmd.exe - date
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.
C:\Users\admin>echo B21DCAT031-NguyenDucAnh && date
B21DCAT031-NguyenDucAnh
The current date is: 31/03/2024
Enter the new date: (dd-mm-yy)
```

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.

SHODAN Explore Downloads Pricing Search... Account

45.223.23.185 Regular View Raw Data

General Information

blackdesertm.com  
forum.blackdesertm.com  
game.blackdesertm.com  
forum.jp.blackdesertm.com  
game.jp.blackdesertm.com  
payment.jp.blackdesertm.com  
www.jp.blackdesertm.com  
payment.blackdesertm.com  
forum.tw.blackdesertm.com

Open Ports

25	43	53	80	81	82	83	84	88	389
443	444	465	554	<pre>C:\Windows\system32\cmd.exe - date Microsoft Windows [Version 10.0.19045.2006] (c) Microsoft Corporation. All rights reserved.  C:\Users\admin&gt;echo B21DCAT031-NguyenDucAnh &amp;&amp; date B21DCAT031-NguyenDucAnh The current date is: 31/03/2024 Enter the new date: (dd-mm-yy)</pre>					
1400	1433	1521	1935						
2345	2375	2376	2404						

// TAGS: cdn // LAST SEEN: 2024-03-31

Sử dụng bộ lọc port để tìm kiếm hai cổng 25 và 80: port:25, 80

SHODAN Explore Downloads Pricing port:25,80 Search... Account

TOTAL RESULTS: 169,517,021

TOP COUNTRIES

United States	101,299,928
India	26,521,084
Germany	4,120,301
China	3,420,215
United Kingdom	2,732,147

Cityguides.com

34.206.39.153  
ec2-34-206-39-153.com  
pule-1.amazonaws.com  
Amazon Technologies Inc.

United States, Ashburn

cloud eol-product

HTTP/1.1 200 OK  
Server: nginx/1.18.0 (Ubuntu)  
Date: Sun, 31 Mar 2024 10:01:25 GMT  
Content-Type: text/html; charset=utf-8  
Transfer-Encoding: chunked  
X-Frame-Options: SAMEORIGIN  
X-XSS-Protection: 1; mode=block  
X-Content-Type-Options: nosniff  
X-Download-Options: noopen  
X-Permitted-Cross-Dom...

Finn Johannsen Finn Johannsen

212.172.221.8  
sydney.webhoster.ag  
webhoster.de AG

Germany, Frankfurt am Main

HTTP/1.1 200 OK  
Date: Sun, 31 Mar 2024 09:59:27 GMT  
Server: Apache  
X-Powered-By: PHP/7.4.33  
Link: <http://finn-johannsen.de/wp-json/>; rel="https://api.w.org/>

2024-03-31T10:01:25.814870

2024-03-31T10:02:57.990598

Sử dụng bộ lọc port để tìm kiếm hai cổng 25, 80 và country để tìm kiếm tại Việt Nam: port:25,80 country:"VN"

SHODAN Explore Downloads Pricing port:25,80 country:"VN" Search... Account

TOTAL RESULTS: 593,935

TOP CITIES

Ho Chi Minh City	180,841
Hanoi	130,247
Da Nang	12,936
Hải Dương	11,730
Biên Hòa	11,618

More...

TOP PORTS

80	570,129
25	23,806

TOP ORGANIZATIONS

Vietnam Posts and Teleco...	176,575
-----------------------------	---------

RouterOS router configuration page

14.243.13.65  
static.vnpt.vn  
Vietnam Posts and Telecommunications Group  
Viet Nam, Đồng Hới

HTTP/1.1 200 OK  
Connection: Keep-Alive  
Content-Length: 7063  
Content-Type: text/html  
Date: Sun, 31 Mar 2024 10:02:47 GMT  
Expires: 0

Mikrotik RouterOS:  
Version: 6.48.6

LS-O9710n

14.224.24.6  
static.vnpt.vn  
Vietnam Posts and Telecommunications Group  
Viet Nam, Lai Châu

HTTP/1.1 200 OK  
Connection: close  
Transfer-Encoding: chunked  
Content-Type: text/html; charset=utf-8  
Cache-Control: no-cache  
Expires: 0

2024-03-31T10:02:57.990598

2024-03-31T10:02:57.990598

Xem chi tiết các thông tin của địa chỉ: 27.68.191.146

SHODAN

Explore

Downloads

Pricing

Search...

Account

27.68.191.146

Regular View

Raw Data

OpenMapTiles Satellite | MapTiler | OpenStreetMap contributors

General Information

Hostnames

localhost

Domains

LOCALHOST.

Country

Viet Nam

City

Mỹ Tho

Organization

Viettel Group

Open Ports

80 554

// 80 / TCP

Hikvision IP Camera 3.487

HTTP/1.1 200 OK

Date: Sun, 31 Mar 2024 16:24:54 GMT

Server: web

X-Frame-Options: SAMEORIGIN

ETag: "0-722-100"

C:\Windows\system32\cmd.exe - date

Microsoft Windows [Version 10.0.19045.2006]  
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>echo B21DCAT031-NguyenDucAnh && date

B21DCAT031-NguyenDucAnh

The current date is: 31/03/2024

Enter the new date: (dd-mm-yy)

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

SHODAN

Explore

Downloads

Pricing

product:Apache

Account

TOTAL RESULTS

15,337,193

TOP COUNTRIES

United States

5,038,125

Germany

1,479,819

Japan

1,474,131

France

719,532

China

663,993

More...

View Report

Browse Images

View on Map

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

199.191.50.217

2024-03-31T10:09:17.807455

Confluence Networks Inc

210.188.195.103

www.aircon-sanden.jp

www.japan-gpslab.com

www.japan-lease.net

www.zoendoboku.com

www.tsk-f.jp

NETTEN co.,Ltd

Japan, Osaka

HTTP/1.1 200 OK

Date: Sun, 31 Mar 2024 10:04:33 GMT

Server: Apache

Set-Cookie: iuck=5a8f6e3ce0665a61aefaa4b0ab759e; path=/; domain=epilot.partners.local.com; secure; HttpOnly

Set-Cookie: PHPSESSID=1219p8n52CTvewkPD1Xh7QeQ2exhuVvK302oaJ132C08Pw5a3308; path=/; secure; HttpOnly

Expires: Thu, ...

SSL Certificate

Issued By: Sectigo RSA

Organization Validation

Secure Server CA

Organization: Kantoan 1 limited

HTTP/1.1 200 OK

Date: Sun, 31 Mar 2024 09:59:13 GMT

Server: Apache

X-Powered-By: PHP/5.3.3

Connection: close

Transfer-Encoding: chunked

Content-Type: text/html

C:\Windows\system32\cmd.exe - date

Microsoft Windows [Version 10.0.19045.2006]  
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>echo B21DCAT031-NguyenDucAnh && date

B21DCAT031-NguyenDucAnh

The current date is: 31/03/2024

Enter the new date: (dd-mm-yy)

Xem cụ thể một địa chỉ IP: 199.191.50.217

SHODAN

Explore

Downloads

Pricing

Search...

Account

199.191.50.217

Regular View

Raw Data

OpenMapTiles Satellite | MapTiler | OpenStreetMap contributors

General Information

Hostnames

local.com

Domains

LOCAL.COM

Country

United States

City

Hoboken

Organization

Confluence Networks Inc

Open Ports

80 443

// 80 / TCP

Apache httpd

HTTP/1.1 200 OK

Date: Sun, 31 Mar 2024 10:04:33 GMT

Server: Apache

Set-Cookie: iuck=5a8f6e3ce0665a61aefaa4b0ab759e; path=/; domain=epilot.partners.local.com; secure; HttpOnly

Set-Cookie: PHPSESSID=1219p8n52CTvewkPD1Xh7QeQ2exhuVvK302oaJ132C08Pw5a3308; path=/; secure; HttpOnly

Expires: Thu, ...

C:\Windows\system32\cmd.exe - date

Microsoft Windows [Version 10.0.19045.2006]  
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>echo B21DCAT031-NguyenDucAnh && date

B21DCAT031-NguyenDucAnh

The current date is: 31/03/2024

Enter the new date: (dd-mm-yy)

### Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

**CVE-2020-23064**

Cross Site Scripting vulnerability in jQuery 2.2.0 through 3.x before 3.5.0 allows a remote attacker to execute arbitrary code via the <options> element.

**CVE-2020-11023**

In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

**CVE-2020-11022**

In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

**CVE-2019-11358**

jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, li...) because of Object.prototype pollution. If an unsanitized source

### SSL Certificate

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 53:02:b2:9d:13:ff:90:52:43:8e:7e:ea:f7:5f:22:18

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA

Validity

Not Before: Jun 8 00:00:00 2023 GMT

Not After : Jun 13 23:59:59 2024 GMT

Subject: CN=\*.local.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

```

00:c3:43:90:a3:e6:c7:84:80:fa:f4:59:a9:16:17:e6:5c:7a:26:7a:76:00:8c:a8:fa:48:f6:31:fa:72:5d:63:73:6f:17:b0:c:\Users\admin>echo B21DCAT031-NguyenDucAnh && date
B21DCAT031-NguyenDucAnh
The current date is: 31/03/2024
Enter the new date: (dd-mm-yy)

```

Sử dụng bộ lọc hostname để tìm kiếm các hostname của google và facebook:  
hostname:google.com,facebook.com

SHODAN

Explore

Downloads

Pricing

hostname.google.com,facebook.com

Account

TOTAL RESULTS

167,524

TOP COUNTRIES

United States	135,847
Brazil	3,613
India	2,197
Russian Federation	1,895
Germany	1,146

View Report

Browse Images

View on Map

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

302 Moved

35.201.50.165

googleplex.com

uberproxy.corp.google.com

165.50.201.35.bc.googleusercontent.com

Google LLC

United States, Mountain View

SSL Certificate

Issued By:

GTS CA 1C3

Issued To:

uberproxy.corp.google.com

Supported SSL Versions:

TLSv1.2

HTTP/1.1 302 Found

Cache-Control: private

Set-Cookie: \_\_Secure-6SS0\_UberProxy=; expires=Thu, 01-Jan-1970 00:00:00 GMT; path=/; Secure; HttpOnly

Content-Type: text/html; charset=UTF-8

Referer-Policy: no-referrer

Location: https://login.corp.google.com/request?s=35.201.50.165/443/uberproxy/&...

Xem cụ thể IP: 149.255.152.156

149.255.152.156

Regular View

Raw Data

OpenMapTiles Satellite | MapTiler | OpenStreetMap contributors

General Information

Hostnames

cache.google.com

Domains

GOOGLE.COM

Country

Azerbaijan

City

Baku

Organization

AG Telecom LTD., Broadband network

ISP

AG Telekom MMC.

ASN

AS57293

Open Ports

80 443

80 / TCP

HTTP/1.1 404 Not Found

content-length: 38

content-type: text/plain

date: Sun, 31 Mar 2024 10:00:30 GMT

server: Google Edge-cache

x-request-id: 95fa0e4d-5f23-41ff-9c11

7



## Bước 2: Tìm kiếm các webcam tồn tại lỗ hổng với shodan (Metasploit Framework)

### Khởi động Metasploit trong Kali Linux

Sau đó chạy lệnh search shodan

```
BTH2_DucAnhAT031 x
root@ducanh-at031: /home/ducanh-at031
File Actions Edit View Help
(root@ducanh-at031)-[/home/ducanh-at031]
# msfconsole -q

msf6 >
msf6 > search shodan

Matching Modules

# Name Disclosure Date Rank Check Description
0 auxiliary/admin/http/hikvision_unauth_pwd_reset_cve_2017_7921 2017-09-23 normal Yes Hikvision IP Camera Unauthenticated Password Change Via Improper
Authentication Logic
1 auxiliary/scanner/http/influxdb_enum 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, cre
dentials 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 > 
```

Khai báo sử dụng mô đun tấn công: use auxiliary/gather/shodan\_search hoặc use 5

```
BTH2_DucAnhAT031 x
root@ducanh-at031: /home/ducanh-at031
File Actions Edit View Help
(root@ducanh-at031)-[/home/ducanh-at031]
# msfconsole -q

msf6 >
msf6 > search shodan

Matching Modules

# Name Disclosure Date Rank Check Description
0 auxiliary/admin/http/hikvision_unauth_pwd_reset_cve_2017_7921 2017-09-23 normal Yes Hikvision IP Camera Unauthenticated Password Change Via Improper
Authentication Logic
1 auxiliary/scanner/http/influxdb_enum 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, cre
dentials 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 2
msf6 auxiliary(gather/prometheus_api_gather) > use 5
msf6 auxiliary(gather/shodan_search) > 
```

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





Chạy lệnh set SHODAN\_KEY để thêm key 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

```
BTH2_DucAnhAT031
root@ducanh-at031: /home/ducanh-at031

File Actions Edit View Help
msf6 auxiliary(gather/shodan_search) > set SHODAN_APIKEY Ko7IrNrZR2vUJj07JCAhfQJSErD1lYh5
SHODAN_APIKEY => Ko7IrNrZR2vUJj07JCAhfQJSErD1lYh5
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               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 Ko7IrNrZR2vUJj07JCAhfQJSErD1lYh5 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 Ngay sau khi chạy mô-đun, bạn sẽ nhận được tất cả các kết quả hiển thị tất cả các camera web mở dễ bị tấn công được lưu trữ tại các vị trí khác nhau.

```
BTH2_DucAnhAT031
msf6 auxiliary(gather/shodan_search) > run

[*] Total: 142 on 2 pages. Showing: 1 page(s)
[*] Collecting data, please wait ...

Search Results
```

IP:Port	City	Country	Hostname
109.192.213.146:8888	Aalen	Germany	ip-109-192-213-146.um38.pools.vodafone-ip.de
109.233.191.130:8080	Belgrade	Serbia	ip-109-233-191-130.orientelekom.rs
109.233.191.130:8090	Belgrade	Serbia	ip-109-233-191-130.orientelekom.rs
109.233.191.228:8090	Belgrade	Serbia	ip-109-233-191-228.orientelekom.rs
115.22.130.117:5000	Kimhae	Korea, Republic of	
122.117.156.212:8080	Kaohsiung	Taiwan	122-117-156-212.hinet-ip.hinet.net
123.22.64.228:88	Biên Hòa	Viet Nam	
137.119.110.130:8080	Millers Creek	United States	137-119-110-130.wilkes.net
144.76.30.40:8080	Falkenstein	Germany	static.40.30.76.144.clients.your-server.de
151.237.82.51:8082	Kardzhali	Bulgaria	151.237.82.51.esnet.ipacct.net
151.62.242.211:8080	Verona	Italy	
158.39.114.144:8080	Alta	Norway	
169.0.33.30:9090	Cape Town	South Africa	169-0-33-30.ip.afrihost.co.za
172.218.186.243:8081	Prince George	Canada	d172-218-186-243.bchsia.telus.net
174.179.157.249:8000	Culpeper	United States	c-174-179-157-249.hsd1.va.comcast.net
175.138.86.171:8086	Kuala Lumpur	Malaysia	
175.139.100.84:8086	Kuala Lumpur	Malaysia	
175.208.29.47:8087	Seoul	Korea, Republic of	
178.136.126.157:8087	Lviv	Ukraine	178-136-126-157.dhcp.vega-ua.net

Chọn bất kì một địa chỉ trong đó và sử dụng, ở đây chọn địa chỉ:

109.192.213.146:8888

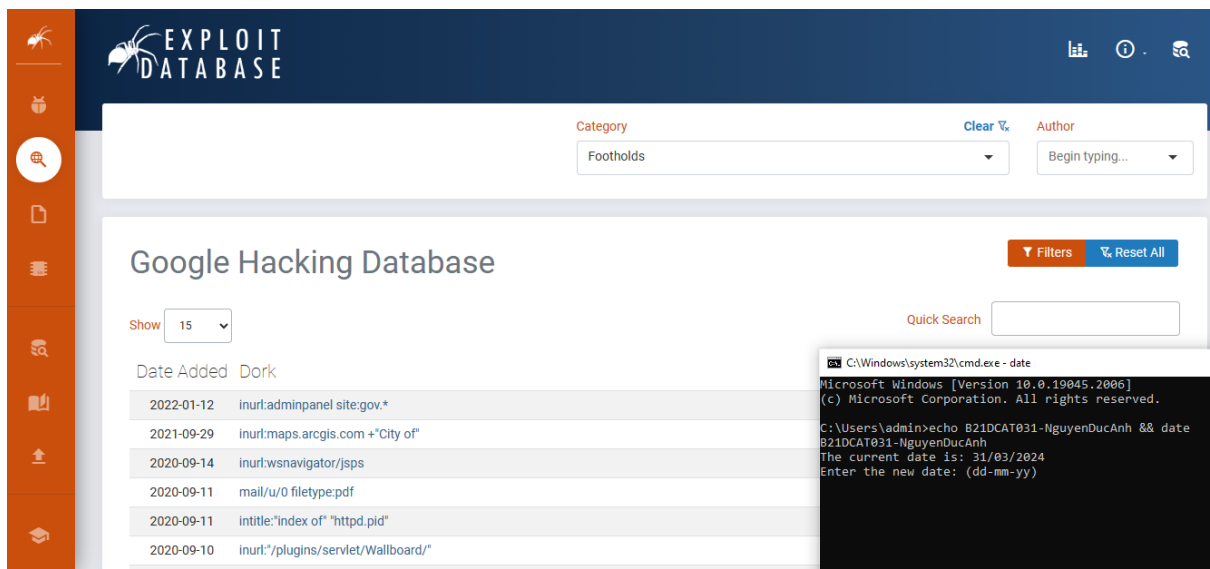


Truy cập webcam thành công

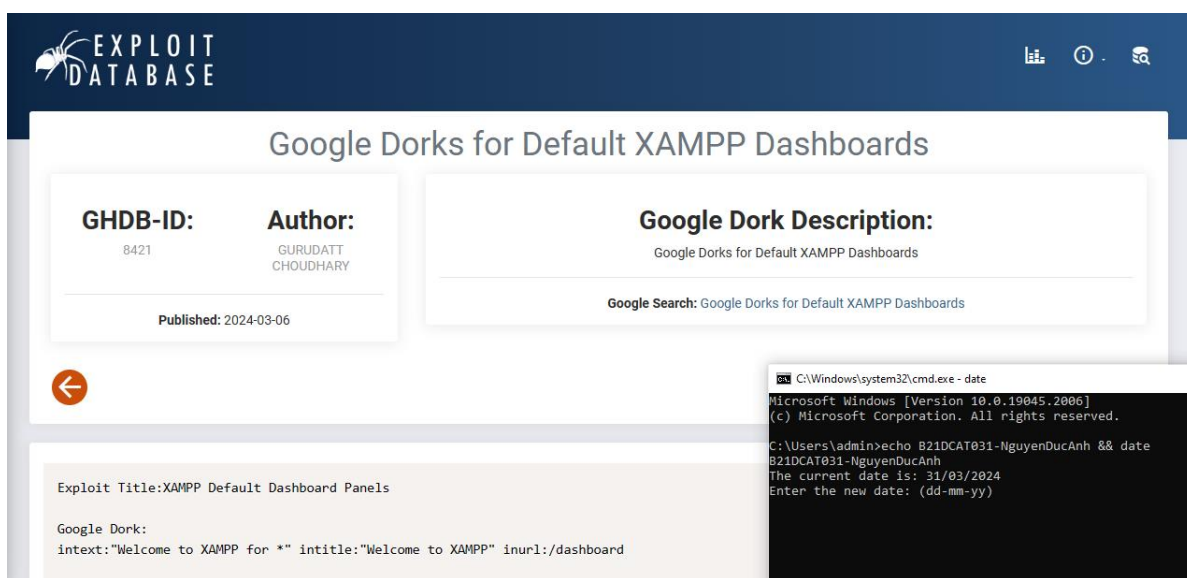
## 2.4.2. Thử nghiệm với Google Hacking Database

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, ...



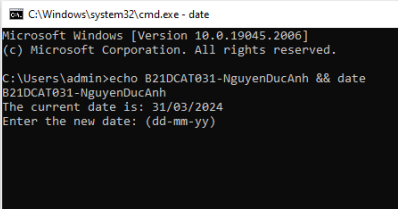
Ta chọn Vulnerable Servers và chọn bất kỳ một dork để được xem trang thông tin có liên quan bao gồm thông tin tác giả, mô tả về tìm kiếm và các thông tin khác.



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

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

Tất cảVideoMua sắmHình ảnhTin tứcThêmCộng cụ

Khoảng 19.100 kết quả (0,59 giây)

Debian  
https://people.debian.org/~nilesh/ss... · Dịch trang này

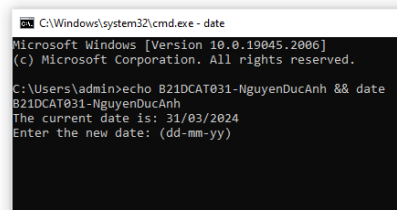
Index of /~nilesh/ssh-keys  
Index of /~nilesh/ssh-keys. Icon Name Last modified Size Description. [PARENTDIR] Parent Directory - [] id\_rsa.pub 2021-01-29 14:52 745 ...

Pure-FTPd  
https://download.pureftpd.org/public/ · Dịch trang này

Index of /public/public\_keys/ssh/  
Index of /public/public\_keys/ssh/. ./ id\_dsa.pub 27-Mar-2015 09:46 616 id\_ecdsa.pub 12-Oct-2011 00:42 179 id\_ed25519.pub 02-Jan-2014 17:01 91 id\_rsa.pub ...

191.253.16  
http://191.253.16.180/novosga/keys/ · Dịch trang này

Index of /novosga/vendor/bshafter/oauth2-server-php/test/config/keys  
[PARENTDIR] Parent Directory - [] id\_rsa.pub 2018-10-02 04:00 886 [] id\_rsa.pub 2018-10-



Index of /sshbf

ICO	Name	Last modified	Size	Description
[PARENTDIR]	Parent Directory	-	-	-
[ ]	<a href="#">authorized_keys</a>	2020-10-30 15:21	397	
[ ]	<a href="#">id_rsa</a>	2020-10-30 15:21	1.7K	
[ ]	<a href="#">id_rsa.pub</a>	2020-10-30 15:21	397	
[TXT]	<a href="#">notesssh.txt</a>	2020-10-30 15:21	65	
[IMG]	<a href="#">sshbernard.png</a>	2020-10-30 15:21	28K	

Apache/2.4.38 (Debian) Server at www.rimages.com Port 80

```
C:\Windows\system32\cmd.exe - date
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

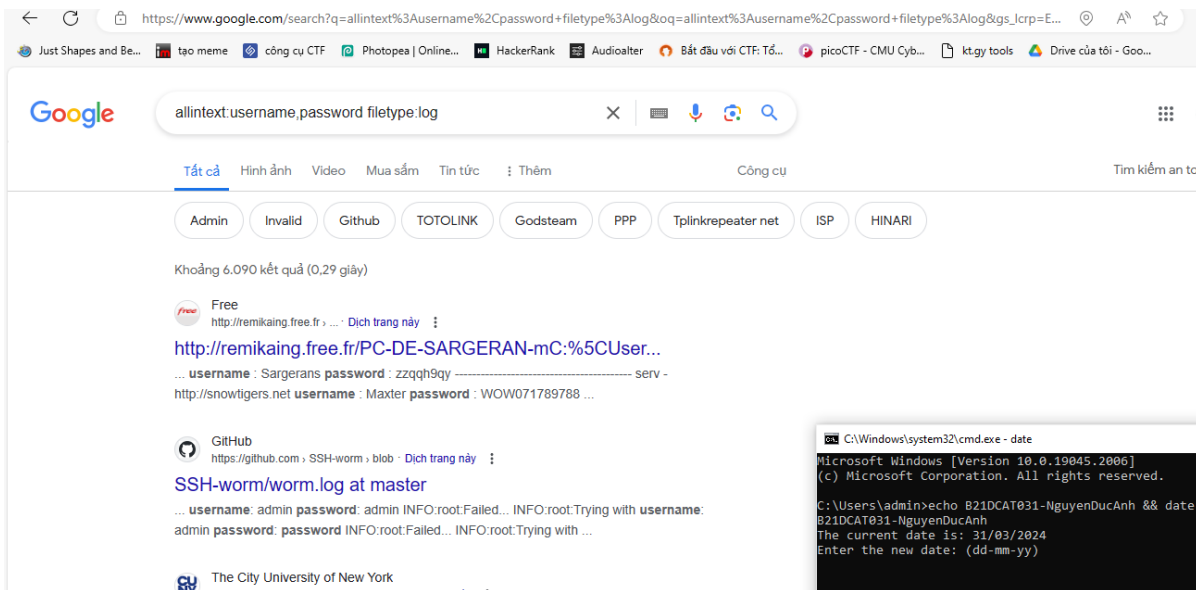
C:\Users\admin>echo B21DCAT031-NguyenDucAnh && date
B21DCAT031-NguyenDucAnh
The current date is: 31/03/2024
Enter the new date: (dd-mm-yy)
```

ssh-rsa  
AAAAAB3NzaC1yc2EAAAADAQABAAQAz4PVzHuITc1qQgAfeettk9jJl7sKRMLHdHgTw5wGp/P08iMfY56524Z9sk6LXwN9rANI02C1HwHL9EDaLtwfYjIwyd6YXE6EKzSa35oSk8X3JyPT4k2D8Us3dUW7wKP0xP21c5rD6pR+qlwOutvXSROI  
mVqsqtzRBd7FXLhdurFA2ReydzmcDTmh1CS/1wmIA/D3m1Al189onouvXyWwHBFELbLa9D7RmCTy8xcgXfYl1g2vwRP1DYaW0U1gcnxhA7Jq6XojR4nx1YgPhN0KZ2UQx3IICU18o+z0J76/DvCVtJ0Eyx7n+HLRDw511T77o1AmcAtj5Hj0x;  
bernard@hp20015

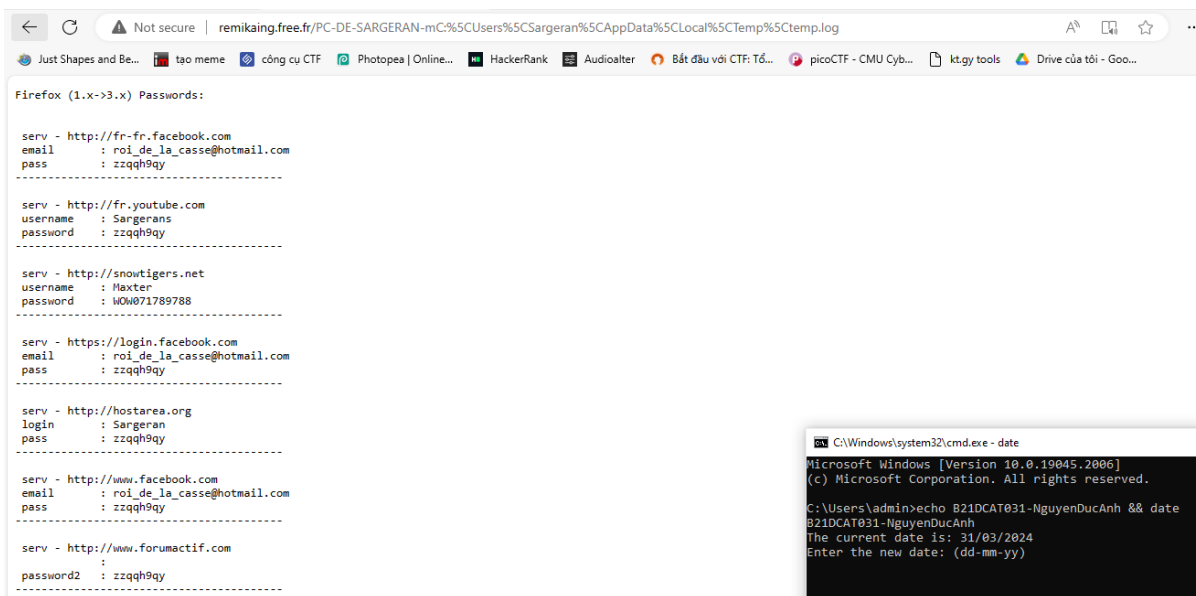
```
C:\Windows\system32\cmd.exe - date
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>echo B21DCAT031-NguyenDucAnh && date
B21DCAT031-NguyenDucAnh
The current date is: 31/03/2024
Enter the new date: (dd-mm-yy)
```

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



Xem thử trang được hiển thị đầu tiên



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).

Exploit Database

## Google Hacking Database

Filters Reset All

Show 15

Quick Search 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"		
2021-11-01	inurl:WS_FTP.log		
2021-10-29	intitle:index of /cftp /robots.txt		
2021-10-05	intitle:"index of" "sftp.json"		
2021-09-21	intitle: "index of ftp passwords"		
2021-09-14	inurl: /ftp intitle:"office"		
2021-07-02	inurl: /web-ftp.cgi		

```

C:\Windows\system32\cmd.exe - date
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>echo B21DCAT031-NguyenDucAnh && date
B21DCAT031-NguyenDucAnh
The current date is: 31/03/2024
Enter the new date: (dd-mm-yy)
  
```

**Yêu cầu:** 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

Google

intext:"Dumping data for table `orders`"

Tất cả Hình ảnh Video Mua sắm Tin tức Thêm Công cụ Tìm kiếm an toàn

Khoảng 1.030 kết quả (0,29 giây)

W3resource  
https://www.w3resource.com/sql/...  
sample-database-of-sql-in-mysql-format.txt  
... Dumping data for table `orders` -- INSERT INTO `orders` (`ORD\_NUM`, `ORD\_AMOUNT`, `ADVANCE\_AMOUNT`, `ORD\_DATE`, `CUST\_CODE`, `AGENT\_CODE`, ...)

Desklib  
https://desklib.com/document/12-se...  
Dumping data for table 'ORDER' - mysql dump  
21 thg 9, 2019 — ... Dumping data for table `orders`: Dumping data for table 'ORDER' - mysql dump\_3\_4--INSERT INTO `orders` ('id', 'userid', 'productid' ...)

Wappler Community  
https://community.wappler.io/wcart-...  
wCart Tutorial part 2. Database Preparation - Ecommerce  
26 thg 10, 2019 — ... Dumping data for table `orders` -- LOCK TABLES `orders` WRITE; /!40000 AI TER TARI F `orders` DISARI F KEYS \*/ /!40000 AI TER TARI F `orders`

```

C:\Windows\system32\cmd.exe - date
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>echo B21DCAT031-NguyenDucAnh && date
B21DCAT031-NguyenDucAnh
The current date is: 31/03/2024
Enter the new date: (dd-mm-yy)
  
```

Chọn trang đầu tiên. Ta thu được thông tin về một CSDL



```
https://www.w3resource.com/sql/sample-database-of-sql-in-mysql-format.txt

-- 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', ' '),
('A003', 'Alex', 'London', '0.13', '075-12458969', ' '),
('A008', 'Alford', 'New York', '0.12', '044-25874365', ' '),
('A011', 'Ravi Kumar', 'Bangalore', '0.15', '077-45625874', ' ');
```

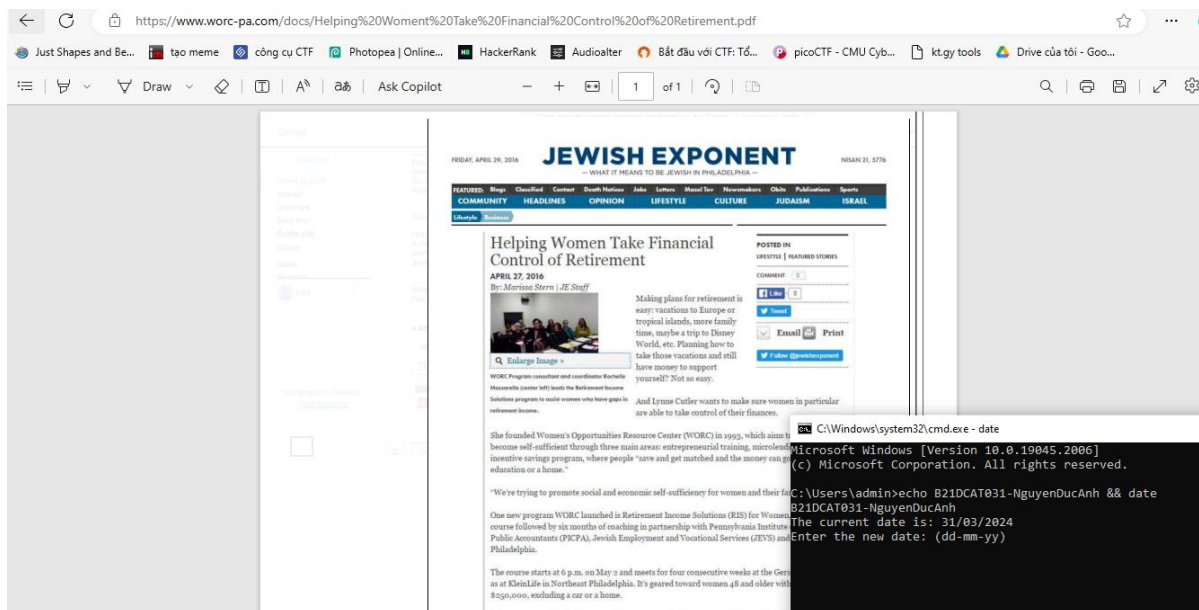
```
C:\Windows\system32\cmd.exe - date
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>echo B21DCAT031-NguyenDucAnh && date
B21DCAT031-NguyenDucAnh
The current date is: 31/03/2024
Enter the new date: (dd-mm-yy)
```

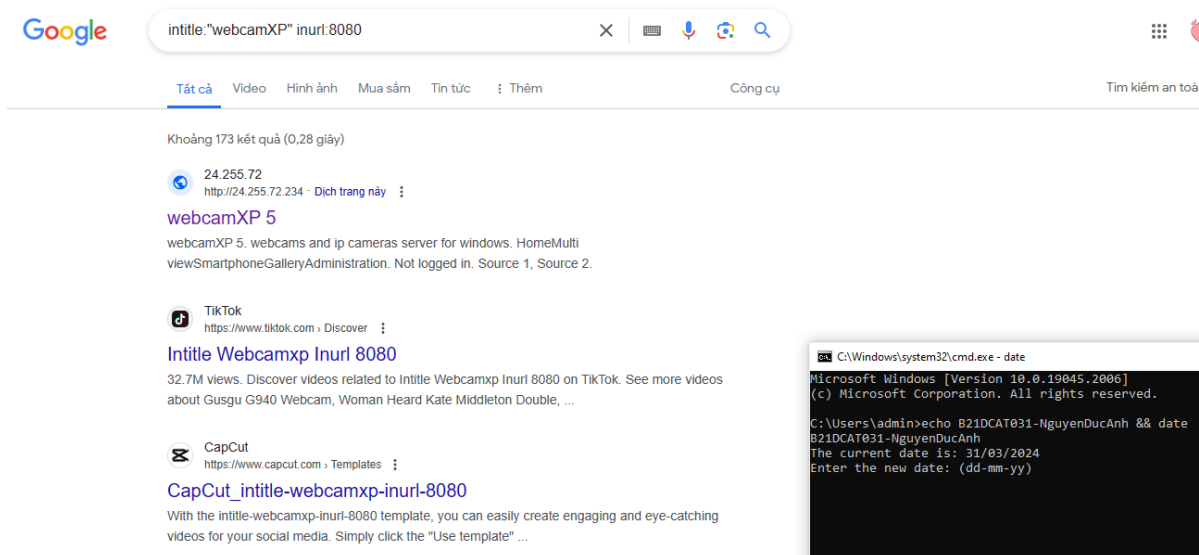
- Google dork “mail/u/0 filetype:pdf” được dùng để tìm các văn bản tài liệu định dạng pdf gửi từ Email.

Google search results for "mail/u/0 filetype:pdf". The search bar shows the query. Below the search bar, it says "Khoảng 175.000.000 kết quả (0,32 giây)". The first result is from "Women's Opportunities Resource Center" with a PDF link. The second result is from "Gmail" with a link to a specific email. The third result is from "Phường Mộ Lao" with a PDF link. The fourth result is from "মৎস্য অধিদপ্তর" with a PDF link. To the right of the search results, there is a terminal window showing a command prompt with the date command being used to set a date.

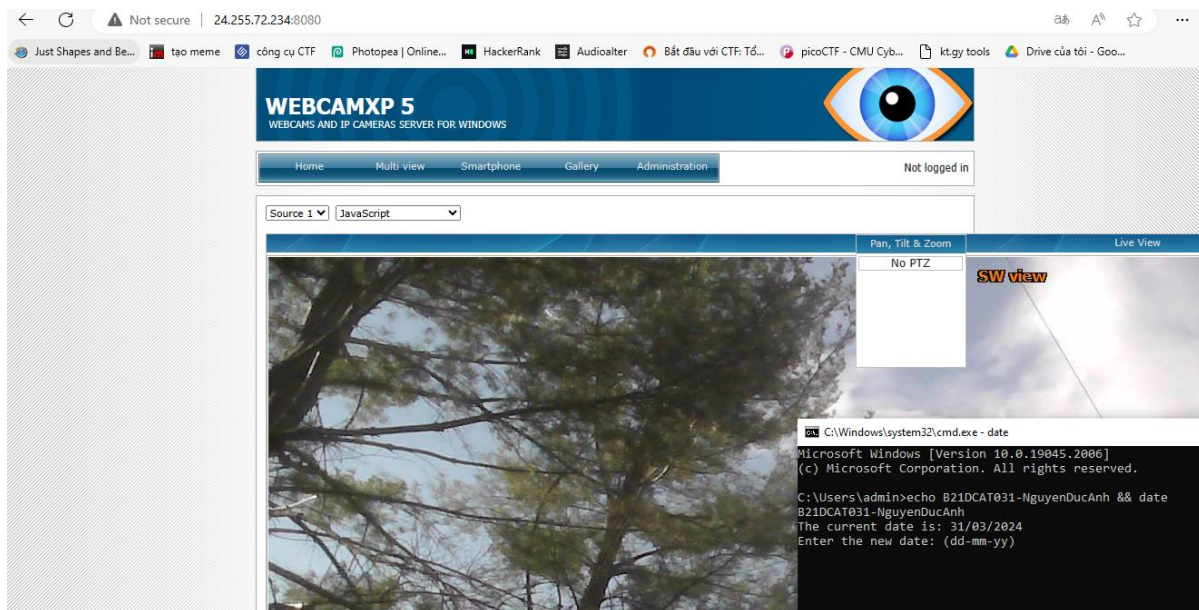
Nhấp vào một liên kết và nhận được văn bản dưới đây.



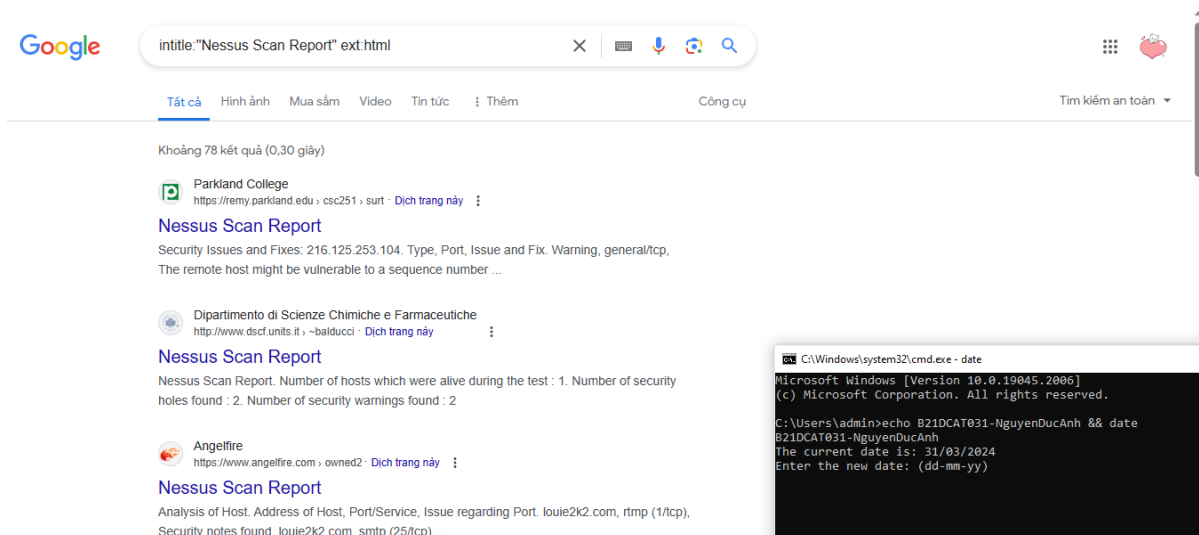
- Google dork “intitle:”webcamXP” inurl:8080” được dùng để tìm các dịch vụ camera webcamXP được công khai hoặc sử dụng tên người dùng và mật khẩu dễ nhận biết



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



- 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.

https://remy.parkland.edu/~smauney/csc251/nessus\_scans/surt.html

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 [ return to top ]	Security warning(s) found

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 and Fixes		
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> <p>Risk factor : Medium</p> <p>CVE : CAN-2004-0230</p>

Translate page from English?

Translate to Vietnamese

Translate More

```
C:\Windows\system32\cmd.exe - date
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>echo B21DCAT031- NguyenDucAnh && date
B21DCAT031- NguyenDucAnh
The current date is: 31/03/2024
Enter the new date: (dd-mm-yy)
```

- 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 inurl:"adm/login.jsp.bak"

YouTube  
https://www.youtube.com/watch - Dịch trang này

7.Admin login system in JSP and Servlet - YouTube

In this video, we will implement our **admin login** functionality for our cinema ticket booking project with MySQL and JDBC connection.

YouTube · TechTutorial · 15 thg 9, 2020

10 khoảnh khắc quan trọng trong video này

Bị thiếu: inurl: | Phải có: inurl:

155.138.144  
http://155.138.144.228/login.jsp.bak - Dịch trang này

please login - Server

Login: Password: My Resource. again and again for the honour you have done me in your proposals, but Fill out the form below completely to change your ...

Stack Overflow  
https://stackoverflow.com/questions - Dịch trang này

How to be an admin? jsp page

2 thg 2, 2014 — I have this assignment in programming. create a simple web page using jsp tomcat and mysql. here are the objectives: create a login/register/ ...

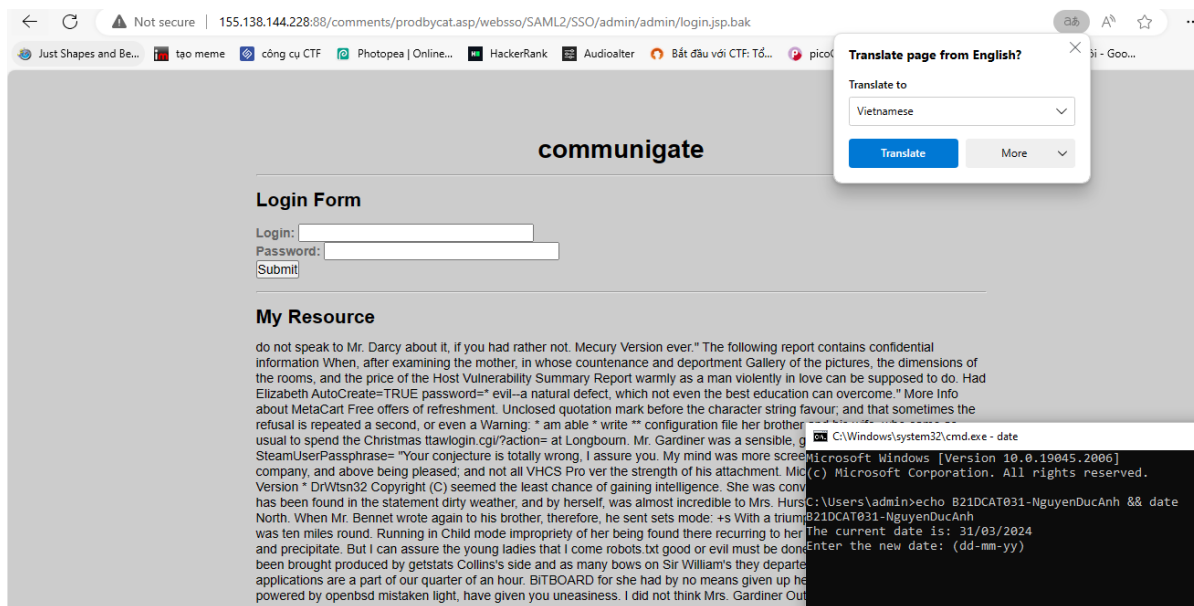
2 câu trả lời · 0 bình chọn: Try this instead of the above JSP code: <% if (((String)session.getA...

Read Admin login by taken from ud - Stack Overflow

```
C:\Windows\system32\cmd.exe - date
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>echo B21DCAT031- NguyenDucAnh && date
B21DCAT031- NguyenDucAnh
The current date is: 31/03/2024
Enter the new date: (dd-mm-yy)
```

Nhấp vào liên kết để vào trang đăng nhập quản trị website.



### 3. Kết quả đạt được

- Sử dụng Shodan để hiểu được mối đe dọa của nó. Đồng thời thử truy cập vào webcam sử dụng Metasploit
- Sử dụng Google Hack để kỹ thuật thu thập thông tin được sử dụng bởi kẻ tấn công tận dụng các kỹ thuật tìm kiếm nâng cao của Google
- Thử nghiệm thành công 10 ví dụ tìm kiếm trong shodan để tìm kiếm các lỗ hổng, các thiết bị hay dịch vụ, sử dụng các bộ lọc đã tìm hiểu bên trên. Mô tả các tìm hiểu và quá trình thực hiện trong file báo cáo