

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: THỰC TẬP CƠ SỞ
MÃ HỌC PHẦN: INT13147

BÀI THỰC HÀNH 3.4
PHÁT HIỆN LỖ HỔNG VỚI CÔNG CỤ TÌM KIẾM

Sinh viên thực hiện:

B22DCAT206 PHẠM ĐỨC NAM

Giảng viên hướng dẫn: **Đỗ Xuân Chợt**

HỌC KỲ 2 NĂM HỌC 2024-2025

Mục lục

1.	Mục đích.....	3
2.	Nội dung thực hành	3
2.1.	Cơ sở lý thuyết	3
2.1.1.	Shodan.....	3
2.1.2.	Google Hacking.....	6
2.2.	Các bước thực hiện.....	8
2.2.1.	Shodan.....	8
2.2.2.	Google Hacking.....	14
3.	Kết luận	25
4.	Tài liệu tham khảo	25

Danh mục hình ảnh

Hướng tiếp cận.....	6
Tìm kiếm tên module, khai báo module sử dụng.....	13
Thiết lập các cấu hình cần thiết.....	13
Kết quả.....	14
1 banner.....	15
Kết quả trả về.....	16
Kết quả trả về.....	17
Kết quả trả về.....	18
Kết quả trả về.....	19

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. Cơ sở lý thuyết

2.1.1. Shodan

Shodan là gì?

Shodan (<https://www.shodan.io/>), được phát triển bởi John Matherly (<http://twitter.com/achillela>) là một công cụ tìm kiếm độc đáo, khác biệt với các công cụ như Google, Bing hay Yahoo. Thay vì thu thập nội dung từ các trang web, Shodan tập trung vào việc quét các thiết bị kết nối Internet, như máy chủ, webcam, máy in, bộ định tuyến và các hệ thống thông minh khác. Nó hoạt động liên tục, thu thập dữ liệu từ khoảng 500 triệu thiết bị và dịch vụ mỗi tháng. Shodan cho phép người dùng phát hiện các thiết bị như camera an ninh, đèn giao thông, hệ thống sưởi, hoặc thậm chí các hệ thống điều khiển phức tạp như nhà máy điện hạt nhân hay công viên giải trí. Điều đáng lo ngại là nhiều thiết bị được Shodan phát hiện thiếu các biện pháp bảo mật, sử dụng mật khẩu mặc định như “admin”/“1234” hoặc thậm chí không có mật khẩu. Theo HD Moore, Giám đốc Bảo mật của Rapid7, gần một nửa các thiết bị kết nối Internet có thể bị truy cập dễ dàng do bảo mật yếu.

Không sử dụng cơ chế “cần lướt, sục sạo mạng web để tìm kiếm các website” như Google, Shodan chỉ tập trung thăm dò các kênh sau của mạng Internet. Nói cách khác, nó giống như một Google “đen tối”, chuyên cần quét máy chủ, webcam, máy in, routers và tất cả những thứ khác, miễn là chúng có kết nối với mạng Internet.

Shodan hoạt động 24/7 và thu thập thông tin từ khoảng 500 triệu thiết bị, dịch vụ mỗi tháng.

Bạn sẽ thực sự ngỡ ngàng với những gì mình tìm thấy sau khi thực hiện một thao tác tìm kiếm đơn giản trên Shodan. Vô số đèn giao thông, camera an ninh, các thiết bị tự động trong nhà hay các hệ thống sưởi nhiệt thông minh đều kết nối với Internet và có thể dễ dàng định vị giống như bóc kẹo.

Sau một thời gian dùng quen, bạn có thể tìm thấy hệ thống điều khiển của cả một công viên nước, một trạm xăng, dàn tủ ướp lạnh rượu vang của khách sạn. Các nhà nguyên cứu bảo mật thậm chí còn có thể định vị hệ thống điều khiển và kiểm soát nhà mạng điện hạt nhân hay các lò gia tốc hạt thông qua Shodan.

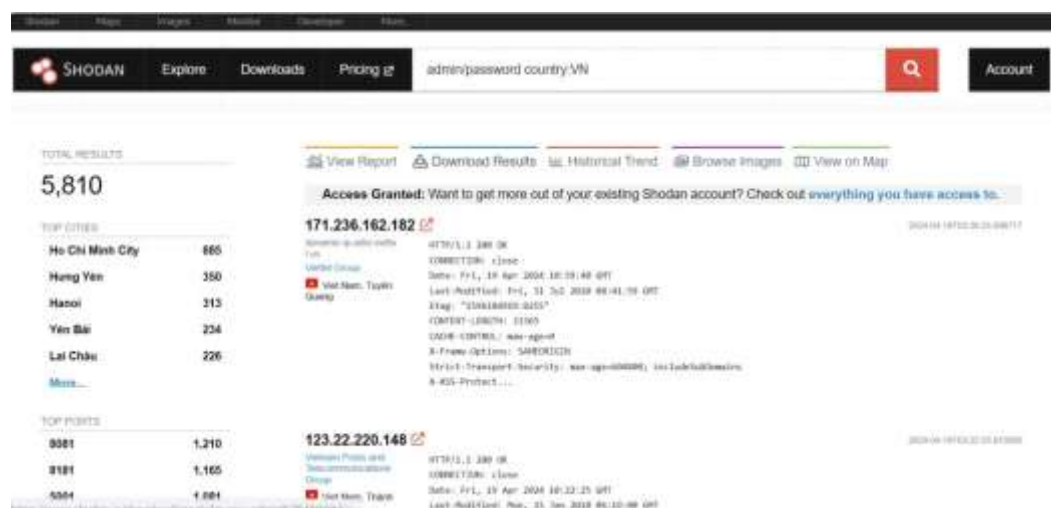
Điều thực sự đáng nói về khả năng tìm kiếm thông tin của Shodan – cũng như tác nhân khiến cho nó trở nên thực sự đáng sợ – là rất hiếm những thiết bị mà Shodan có thể sục sạo được trang bị các hàng rào bảo mật.

“Bạn có thể đăng nhập vào khoảng một nửa mạng Internet với mật khẩu mặc định”, ông HD Moore, Giám đốc Bảo mật của Rapid 7 bình luận. “Đó là một sự thất bại kinh hoàng nhưng chưa được thừa nhận của giới bảo mật”.

Chỉ một từ khóa tìm kiếm “mật khẩu mặc định” sẽ tiết lộ vô số các thiết bị điều khiển hệ thống, máy in, máy chủ dùng “admin” làm username và “1234” làm mật khẩu chính. Nhiều hệ thống nối mạng thậm chí còn chả có mật khẩu – tất cả những gì bạn cần là một trình duyệt web để có thể kết nối chúng.

❖ Hướng dẫn tìm kiếm

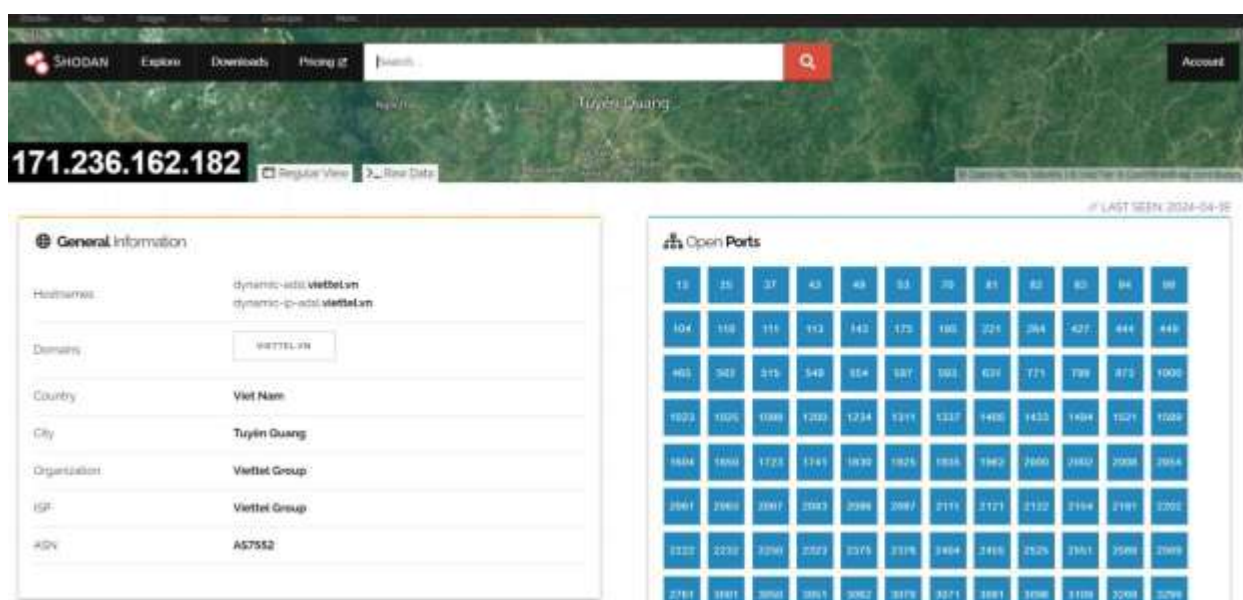
Nhập từ khóa cần tìm kiếm vào ô searchbox trên shodan. Ví dụ với từ khóa: admin/password



Kết quả trả về các máy chủ apache public, đồng thời cho bạn rất nhiều các thông tin liên quan:

- Total results: Số lượng kết quả
- Results map: Bản đồ mật độ các khu vực trên thế giới có kết quả phù hợp
- Top countries : Top các nước có số lượng tương ứng
- Top operating systems: Top các hệ điều hành sử dụng
- Top services (Ports): Top các cổng dịch vụ mở ...

Khi vào một địa chỉ IP các bạn có thêm các thông tin như: cổng đang mở, dịch vụ đang chạy, các lỗ hổng (CVE) của dịch vụ..



Để kết quả tìm kiếm chính xác hơn, các bạn có thể sử dụng thêm dấu "", kết hợp các toán tử + để có thể có nhiều hơn hoặc - để lọc bớt các kết quả không mong muốn. Ví dụ: Apache + os:windows

❖ Tìm kiếm shodan có được coi là phạm pháp?

Shodan được CNN Business gọi là “công cụ tìm kiếm đáng sợ nhất”. Tuy nhiên, nó hoàn toàn hợp pháp, chỉ thu thập dữ liệu công khai trên Internet và báo cáo kết quả. Shodan không xâm nhập hệ thống mà chỉ hiển thị thông tin sẵn có, tương tự như một công cụ lập chỉ mục.

❖ Tìm kiếm hiệu quả hơn với shodan

Ngoài các tìm kiếm cơ bản, để sử dụng hiệu quả shodan hơn các bạn cần biết sử dụng kết hợp các bộ lọc (filter) một cách chính xác và "thông minh". Sau đây là các bộ lọc mà các bạn có thể sử dụng kết hợp:

Các bộ lọc

Cấu trúc sử dụng filter: *filtername:value*

- **city**: Tìm kiếm các thiết bị trong một thành phố cụ thể sử dụng mã thành phố (Ví dụ: hanoi,..)
- **country**: Tìm kiếm các thiết bị trong một quốc gia cụ thể sử dụng mã quốc gia (Ví dụ: vn, us,..)
- **hostname**: Tìm kiếm theo hostname hay domain (Ví dụ: goole, edu.vn,...)
- **net**: Tìm kiếm bằng địa chỉ IP hoặc CIDR (Classless Inter-Domain Routing)
- **os**: Tìm kiếm theo hệ điều hành
- **port**: Tìm kiếm theo port cụ thể được mở
- **before/after**: Tìm kiếm trong một khoảng thời gian ...

❖ Ứng dụng shodan trong kiểm thử bảo mật Pen Testing:

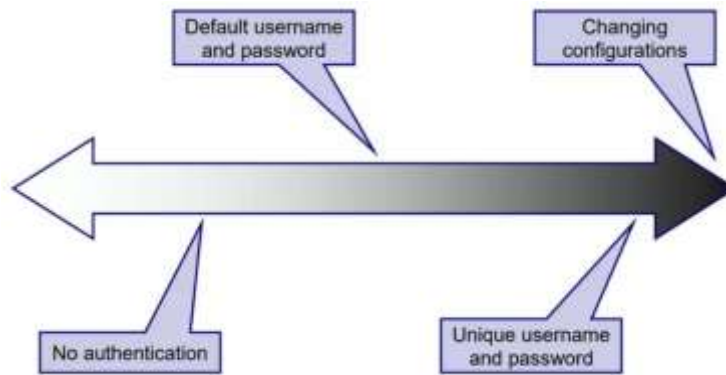
Ethics

- Sử dụng shodan để xem hoặc thay đổi cấu hình các thiết bị hay server mà không yêu cầu xác thực
- Sử dụng shodan để xem hoặc thay đổi cấu hình các thiết bị hay server sử dụng tài khoản và

mật khẩu mặc định

- Sử dụng shodan để xem hoặc thay đổi cấu hình của các thiết bị sử dụng chung tài khoản mật khẩu

- Sử dụng shodan để xem hoặc thay đổi cấu hình của các thiết bị bị lộ tài khoản và mật khẩu (trong cấu hình hoặc file...)



Hướng tiếp cận

Pen Testing Applications

- Tìm kiếm để kiểm tra xâm nhập các ứng dụng trên thiết bị hay server sử dụng các yếu tố
 - o Mã code HTTP trả về
 - o Các thông tin banner, foot printing của dịch vụ
 - o Phiên bản của dịch vụ
 - o Các cổng dịch vụ đang mở

Pen Testing: HTTP Status Codes

Tìm kiếm dựa theo phản hồi từ phía server

Status Code	Description
200 OK	Request succeeded
401 Unauthorized	Request requires authentication
403 Forbidden	Request is denied regardless of authentication

2.1.2. Google Hacking Một số khái niệm cần biết

- **Google Hacking Database (GHDB):** Đây là một cơ sở dữ liệu chứa các chuỗi truy vấn (dorks) được sử dụng để tìm kiếm các lỗ hổng bảo mật trên các trang web sử dụng Google.

GHDB cung cấp các dorks đã được phân loại và được cập nhật

thường xuyên, giúp người dùng tìm kiếm và khám phá các lỗ hổng bảo mật trên trang web một cách hiệu quả.

- **Google Dorks:** Google Dorks là các chuỗi truy vấn đặc biệt được sử dụng để tìm kiếm thông tin cụ thể trên Google. Bằng cách sử dụng Google Dorks, người dùng có thể tìm kiếm các tài liệu, thông tin bảo mật, thông tin người dùng, tệp đính kèm và nhiều nội dung khác mà không thể tìm thấy thông qua việc tìm kiếm thông thường.
- **Google Advanced Search:** Google Advanced Search là tính năng đặc biệt của Google cho phép người dùng tìm kiếm chính xác và rõ ràng hơn bằng cách sử dụng các tiêu chí tìm kiếm nâng cao. Với Google Advanced Search, người dùng có thể tìm kiếm đoạn văn bản cụ thể, loại tệp tin, ngôn ngữ, thời gian và vị trí, giúp lọc kết quả tìm kiếm theo yêu cầu cụ thể.
- **Google Alerts:** Google Alerts là dịch vụ của Google cho phép người dùng theo dõi các từ khóa, cụm từ hoặc tên thương hiệu trên mạng. Khi có thông tin mới liên quan đến từ khóa được theo dõi xuất hiện trên trang web, tin tức hoặc diễn đàn, người dùng sẽ nhận được thông báo qua email. Điều này giúp người dùng duy trì sự cập nhật với các tin tức và thông tin mới nhất về từ khóa quan tâm.

Có những loại thông tin nào được lưu trữ trong Google Hacking Database?

Google Hacking Database (GHD) là một tập hợp các mẫu truy vấn tìm kiếm và quy tắc để tìm kiếm các lỗ hổng bảo mật, thông tin nhạy cảm và các thông tin khác trên internet. GHD được duy trì và cập nhật bởi các chuyên gia bảo mật và là công cụ hữu ích cho người dùng muốn kiểm tra tính bảo mật của hệ thống mạng.

Trong Google Hacking Database, có nhiều loại thông tin được lưu trữ như:

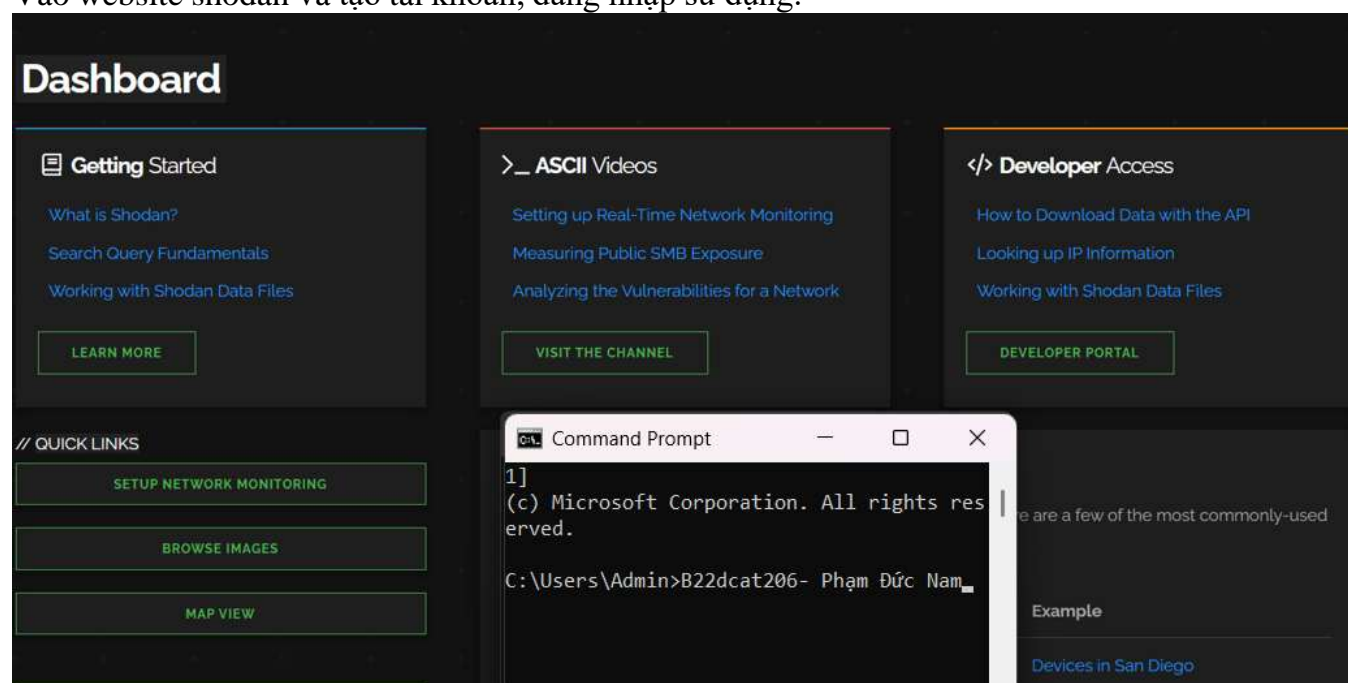
- Lỗ hổng bảo mật: GHD cung cấp một danh sách các truy vấn tìm kiếm để tìm kiếm các hệ thống có lỗ hổng bảo mật. Ví dụ, `"inurl:admin"` sẽ tìm kiếm các trang web có đường dẫn chứa từ `"admin"`, có thể là các trang quản trị hệ thống mà không được bảo mật đầy đủ.
- Thông tin nhạy cảm: GHD cũng cung cấp các truy vấn để tìm kiếm thông tin nhạy cảm như thông tin tài khoản, mật khẩu, tài liệu quan trọng, email và tệp tin lưu trữ. Ví dụ, `"filetype:pdf site:google.com confidential"` sẽ tìm kiếm các tệp tin PDF có từ khóa `"confidential"` trên trang web `"google.com"`.
- Các công cụ và ứng dụng hệ thống: GHD cung cấp truy vấn để tìm kiếm các công cụ và ứng dụng đang chạy trên các máy chủ và hệ thống mạng. Ví dụ, `"intitle:index of" "Apache/2.2.14 (Ubuntu)"` sẽ tìm kiếm các trang web chạy trên máy chủ Apache/2.2.14 (Ubuntu).
- Cấu hình mạng: GHD cung cấp các truy vấn để tìm kiếm thông tin về cấu hình mạng như các địa chỉ IP, DNS, địa chỉ email hoặc các tệp tin cấu hình mạng. Ví dụ, `"intitle:index.of etc"` sẽ tìm kiếm các tệp tin cấu hình trong thư mục `/etc` trên các trang web.

Lưu ý rằng việc sử dụng Google Hacking Database để tìm kiếm thông tin nhạy cảm hoặc tấn công vào hệ thống mà không được sự cho phép là vi phạm pháp luật và không được khuyến khích. Việc sử dụng GHD nên tuân theo các quy tắc đạo đức và tuân thủ pháp luật bảo mật thông tin.

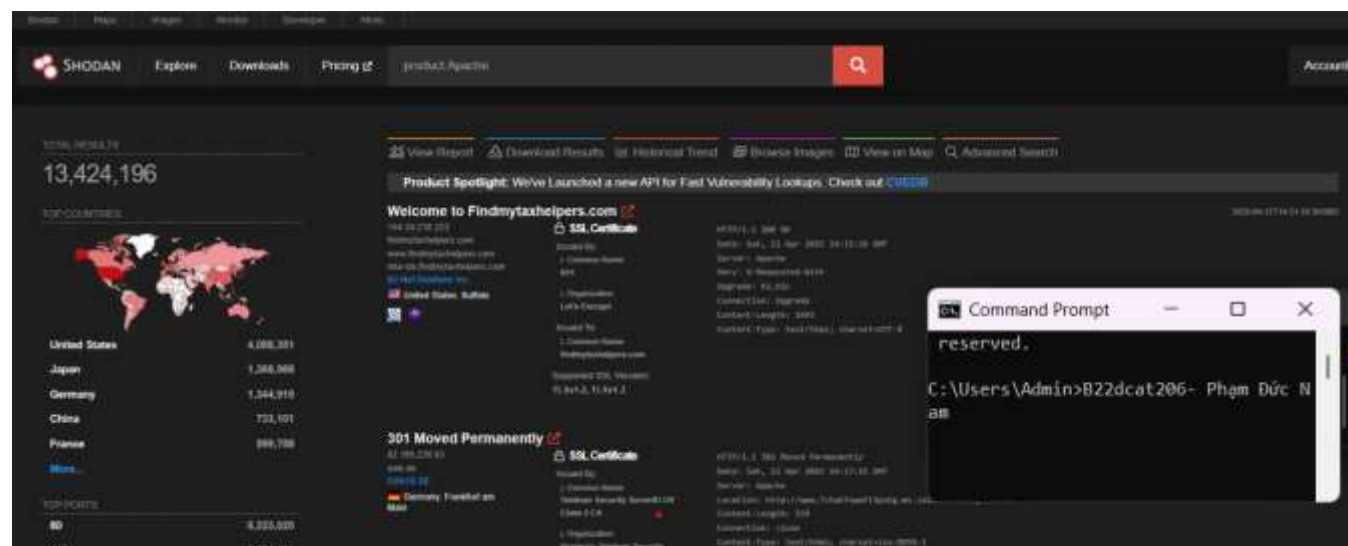
2.2. Các bước thực hiện

2.2.1. Shodan

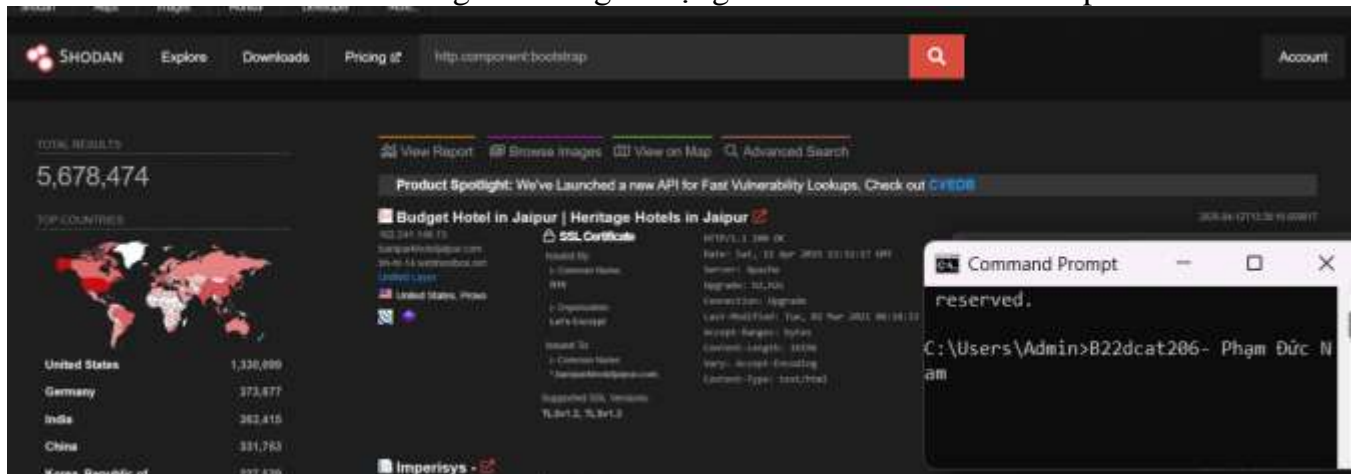
Vào website shodan và tạo tài khoản, đăng nhập sử dụng:



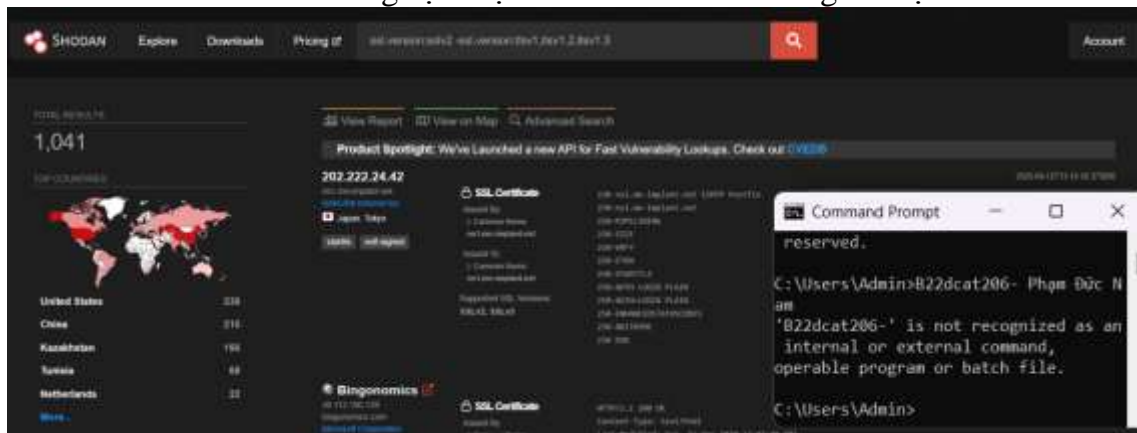
1. Basic: Tìm kiếm các web Apache server



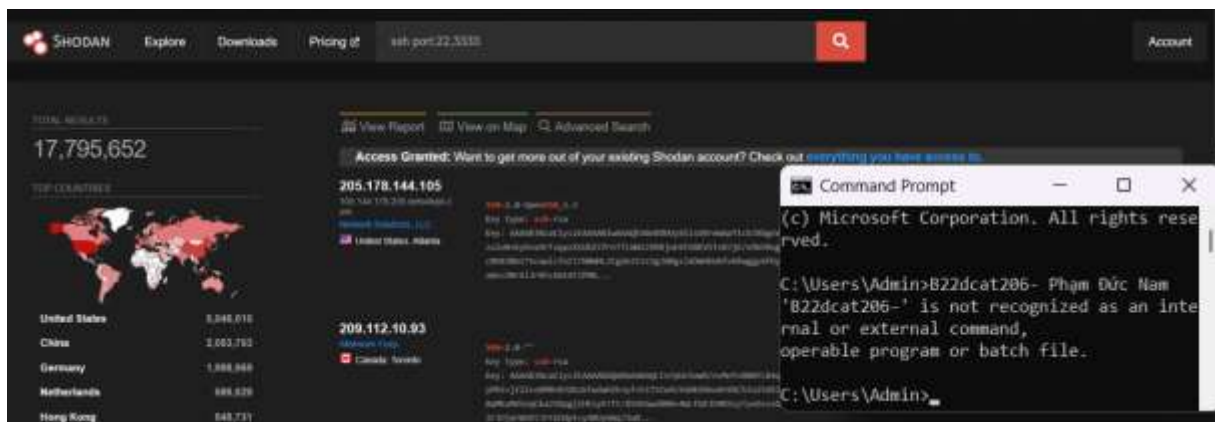
2. HTTP Filter: Tìm kiếm Các trang web đang sử dụng framework CSS Bootstrap



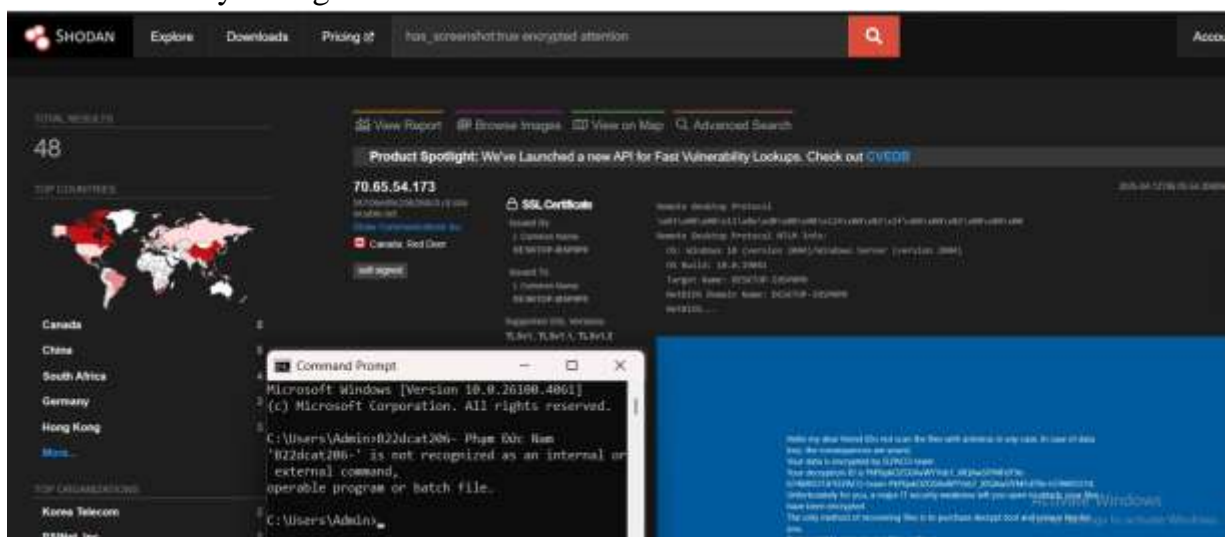
3. SSL Filter: Tìm kiếm những dịch vụ hỗ trợ SSLv2 và không hỗ trợ TLS



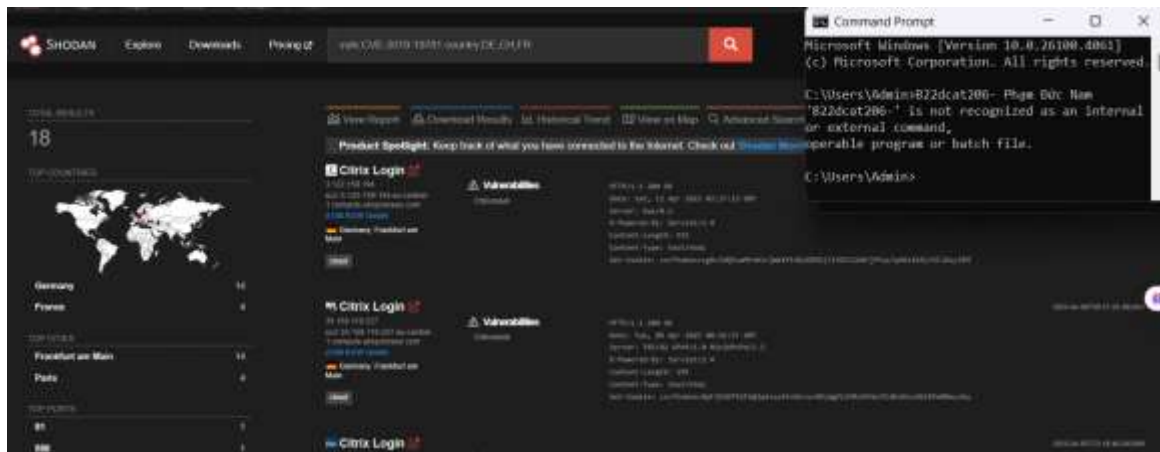
4. SSH Filter: Tìm kiếm SSH trên cổng 22 hoặc 3333



5. Screenshot Filter: Tìm kiếm OCR trong máy tính từ xa xem có bị nhiễm ransomware hay không



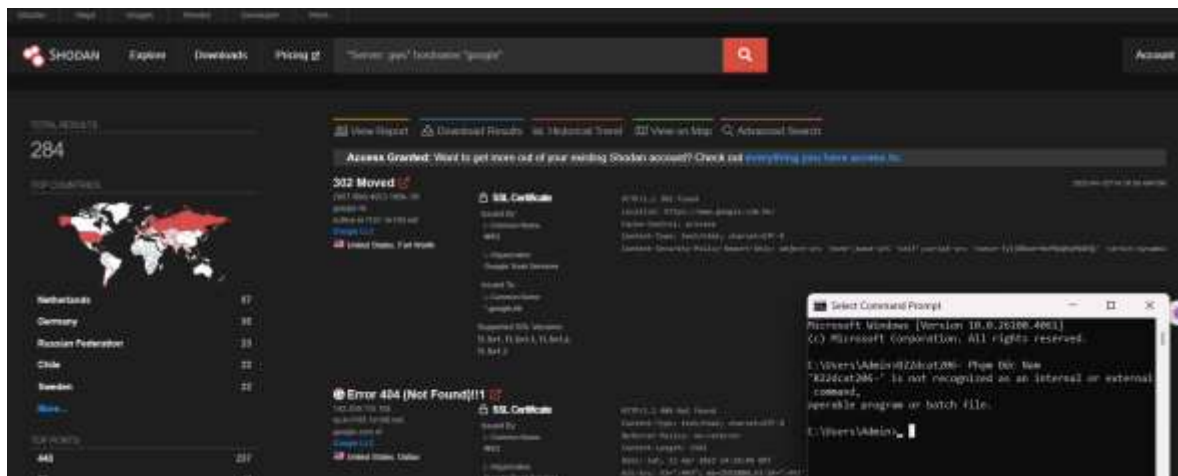
6. RESTRICTED FILTER: Tìm kiếm Các thiết bị Citrix ở Đức, Thụy Sĩ hoặc Pháp để bị tấn công bởi CVE-2019-19781



7. Tìm kiếm với mã CVE-ID



8. Tìm kiếm máy chủ GWS (Google Web Server)



9. Tìm kiếm từ khóa “Default Password”



10. Tìm các webcam dễ bị tổn thương bằng Shodan [Metasploit Framework]


```

    =[ metasploit v6.4.56-dev ]
    --=[ 2505 exploits - 1291 auxiliary - 431 post ]
    --=[ 1610 payloads - 49 encoders - 13 nops ]
    --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

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 AP
Information Gather
3  auxiliary/gather/shodan_honeyscore .               normal No    Shodan Honeys
Core Client
4  auxiliary/gather/shodan_host .               normal No    Shodan Host P
rt
5  auxiliary/gather/shodan_search .               normal No    Shodan Search
6  auxiliary/scanner/http/smt_ipmi_49152_exposure 2014-06-19      normal No    Supermicro On
board IPMI Port 49152 Sensitive File Exposure
7  auxiliary/gather/hikvision_info_disclosure_cve_2017_7921 2017-09-23      normal Yes   Unauthenticat
d information disclosure such as configuration, credentials and camera snapshots of a vulnerable Hikvision IP Came
ra
8  \ action: Automatic . . . Dump all info
Information
9  \ action: Configuration . . . Dump camera h
rdware and software configuration
10 \ action: Credentials . . . Dump all cred
ntials and passwords
11 \ action: Snapshot . . . Take a camera
Snapshot

Interact with a module by name or index. For example info 11, use 11 or use auxiliary/gather/hikvision_info_disclos
ure_cve_2017_7921
After interacting with a module you can manually set a ACTION with set ACTION 'Snapshot'

```

Tìm kiếm tên module, khai báo module sử dụng

```

msf6 auxiliary(gather/shodan_search) > set SHODAN_APIKEY j9AWHh1WbUTZd6qhuugwcUnWsAmBdAmo
SHODAN_APIKEY => j9AWHh1WbUTZd6qhuugwcUnWsAmBdAmo
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 j9AWHh1WbUTZd6qhuugwcUnWsAmBdAmo yes       The SHODAN API key

View the full module info with the info, or info -d command.

msf6 auxiliary(gather/shodan_search) > run
[-] Auxiliary failed: JSON::ParserError invalid ASCII control character in string:
[-] Call stack:
[-] /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/json-2.10.2/lib/json/common.rb:248:in `parse'
[-] /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/json-2.10.2/lib/json/common.rb:248:in `parse'
[-] /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/active-support-7.0.8.7/lib/active_support/json/de
coding.rb:23:in `decode'
[-] /usr/share/metasploit-framework/modules/auxiliary/gather/shodan_search.rb:80:in `shodan_query'
[-] /usr/share/metasploit-framework/modules/auxiliary/gather/shodan_search.rb:125:in `run'
[*] Auxiliary module execution completed
msf6 auxiliary(gather/shodan_search) > run
[*] Total: 151 on 2 pages. Showing: 1 page(s)
[*] Collecting data, please wait...

```

Thiết lập các cấu hình cần thiết

```

File Actions Edit View Help
[+] /usr/share/metasploit-framework/modules/auxiliary/gather/shodan_search.rb:125:in `run'
[*] Auxiliary module execution completed
msf6 auxiliary(gather/shodan_search) > run
[*] Total: 151 on 2 pages. Showing: 1 page(s)
[*] Collecting data, please wait...

Search Results

IP:Port      City          Country          Hostname
-----
1.213.178.190:20000 Seoul        Korea, Republic of
104.229.232.108:8080 Herkimer     United States    syn-104-229-232-108.res.spectrum.com
108.28.226.199:8080 Gainesville United States    pool-108-28-226-199.washdc.fios.verizon.net
109.233.191.130:8080 Belgrade     Serbia          ip-109-233-191-130.oriontelekom.rs
109.233.191.130:8090 Belgrade     Serbia          ip-109-233-191-130.oriontelekom.rs
109.233.191.226:8080 Belgrade     Serbia          ip-109-233-191-226.oriontelekom.rs
115.22.130.117:5000 Busan        Korea, Republic of
118.122.8.155:4640 Chengdu      China
121.121.139.88:8080 Puchong      Malaysia
122.117.156.212:8080 Kaohsiung    Taiwan          122-117-156-212.hinet-ip.hinet.net
137.119.110.130:8080 Millers Creek United States    137-119-110-130.wilkes.net
139.64.168.120:8080 Logan        United States
14.52.200.16:8081 Seoul        Korea, Republic of
160.119.231.105:9090 Johannesburg South Africa
175.208.29.47:8087 Jeongeup     Korea, Republic of
178.164.140.165:8888 Gdöllő       Hungary         178-164-140-165.pool.digikabel.hu
183.100.82.122:8080 Pyeongtaek   Korea, Republic of
184.57.102.6:5400 Erie         United States    syn-184-057-102-006.res.spectrum.com
184.57.102.6:5432 Erie         United States    syn-184-057-102-006.res.spectrum.com
184.57.102.6:5600 Erie         United States    syn-184-057-102-006.res.spectrum.com
184.57.102.6:5800 Erie         United States    syn-184-057-102-006.res.spectrum.com
184.57.102.6:6500 Erie         United States    syn-184-057-102-006.res.spectrum.com
184.57.102.6:6565 Erie         United States    syn-184-057-102-006.res.spectrum.com
184.57.102.6:7070 Erie         United States    syn-184-057-102-006.res.spectrum.com
184.57.102.6:8585 Erie         United States    syn-184-057-102-006.res.spectrum.com
184.57.102.6:8800 Erie         United States    syn-184-057-102-006.res.spectrum.com
184.57.102.6:9090 Erie         United States    syn-184-057-102-006.res.spectrum.com
184.57.102.6:9550 Erie         United States    syn-184-057-102-006.res.spectrum.com
189.146.122.65:8870 Mexico City  Mexico          dsl-189-146-122-65-dyn.prod-infinet.com.mx
194.193.220.137:18007 Sydney      Australia       194-193-220-137.tpgi.com.au
194.193.220.137:18007 Zurich      Switzerland

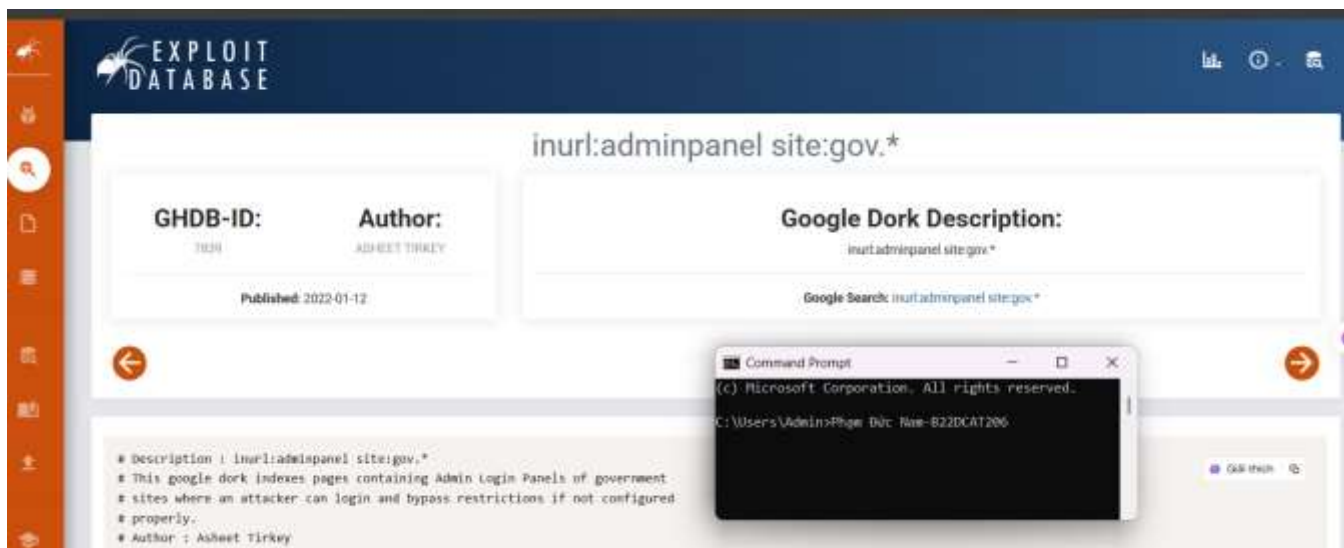
```

Kết quả

2.2.2. Google Hacking

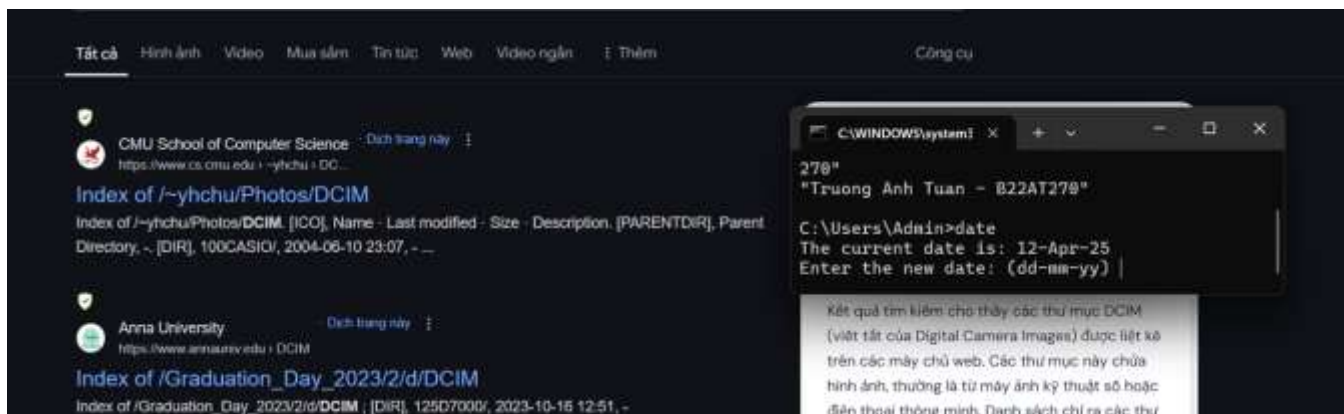
Vào website www.exploit-db.com/google-hacking-database, sử dụng Filters. Nhấn vào nút Filters đầu bên phải của trang và mũi tên xổ menu để khai thác các mục. Các mục ở đây bao gồm Footholds, Files Containing Usernames, Sensitive Directories, Web Server Detection, và các thứ khác. Chọn mục Footholds để hiện ra trang thông tin có liên quan bao gồm thông tin tác giả, mô tả về tìm kiếm và các thông tin khác:

[illegible]



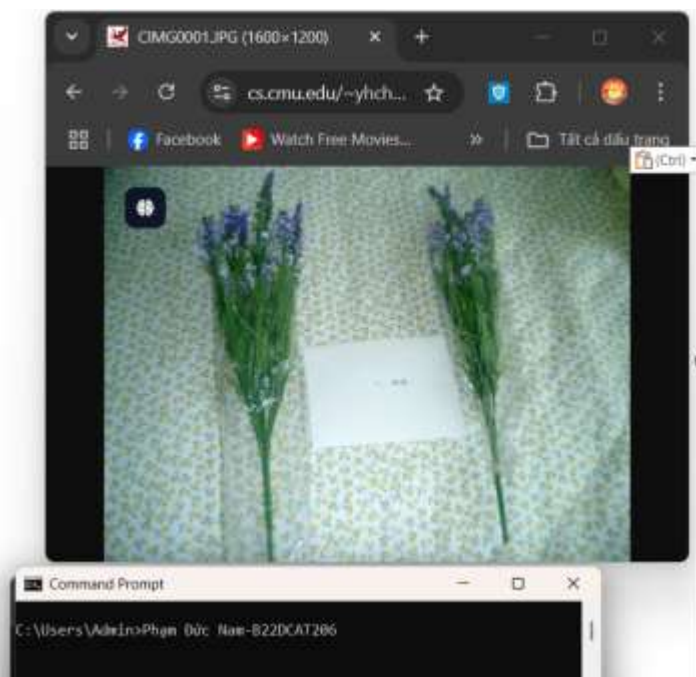
1 banner

Thử nghiệm với ví dụ tại <http://www.exploit-db.com/ghdb/4057>, trong đó từ khóa `intitle` tìm kiếm những từ ở trong tiêu đề của trang web, DCIM là tên thư mục thường sử dụng để lưu ảnh:



Name	Last modified	Size	Description
Parent Directory	-	-	-
CIMG0001.JPG	2002-01-10 11:45	555K	
CIMG0002.JPG	2002-01-12 14:51	537K	
CIMG0003.JPG	2002-01-12 14:52	541K	
CIMG0004.JPG	2002-01-12 14:52	537K	
CIMG0005.JPG	2002-01-12 14:52	556K	
CIMG0006.JPG	2002-01-12 14:53	551K	
CIMG0007.JPG	2002-01-12 14:53	566K	
CIMG0008.JPG	2002-01-12 14:54	543K	
CIMG0009.JPG	2002-01-15 14:18	557K	
CIMG0010.JPG	2002-01-15 14:19	533K	
CIMG0011.JPG	2002-01-15 14:19	526K	
CIMG0012.JPG	2002-01-15 19:11	594K	
CIMG0013.JPG	2002-01-15 19:11	578K	
CIMG0014.JPG	2002-01-15 19:12	593K	
CIMG0015.JPG	2002-01-15 19:13	591K	

Apache/2.4.18 (Ubuntu) Server at www.cs.cmu.edu Port 443



Kết quả trả về

Thử nghiệm câu lệnh tại <https://www.exploit-db.com/ghdb/6322>, kết quả trả về các thư mục và tập tin nhạy cảm có chứa khóa ssh:

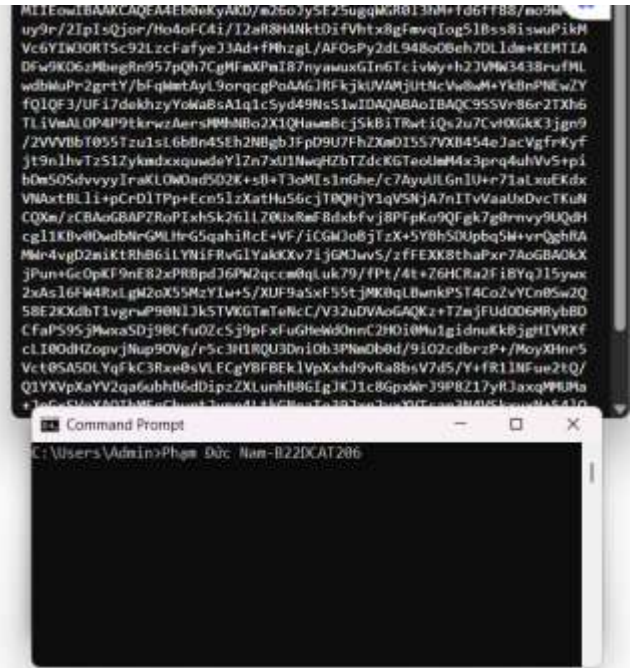
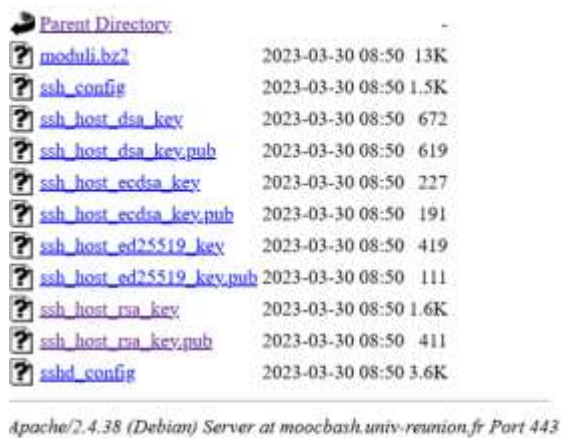
Google search results for `intitle:index of id_rsa.pub`. The top result is from Debian, titled "Index of /~nilesh/ssh-keys". The search results also show a link to "Exploit-DB" and "Pure-FTPd".

Command Prompt output:

```
C:\Users\Adelin>Phạm Đức Nam-B22DCAT206
```

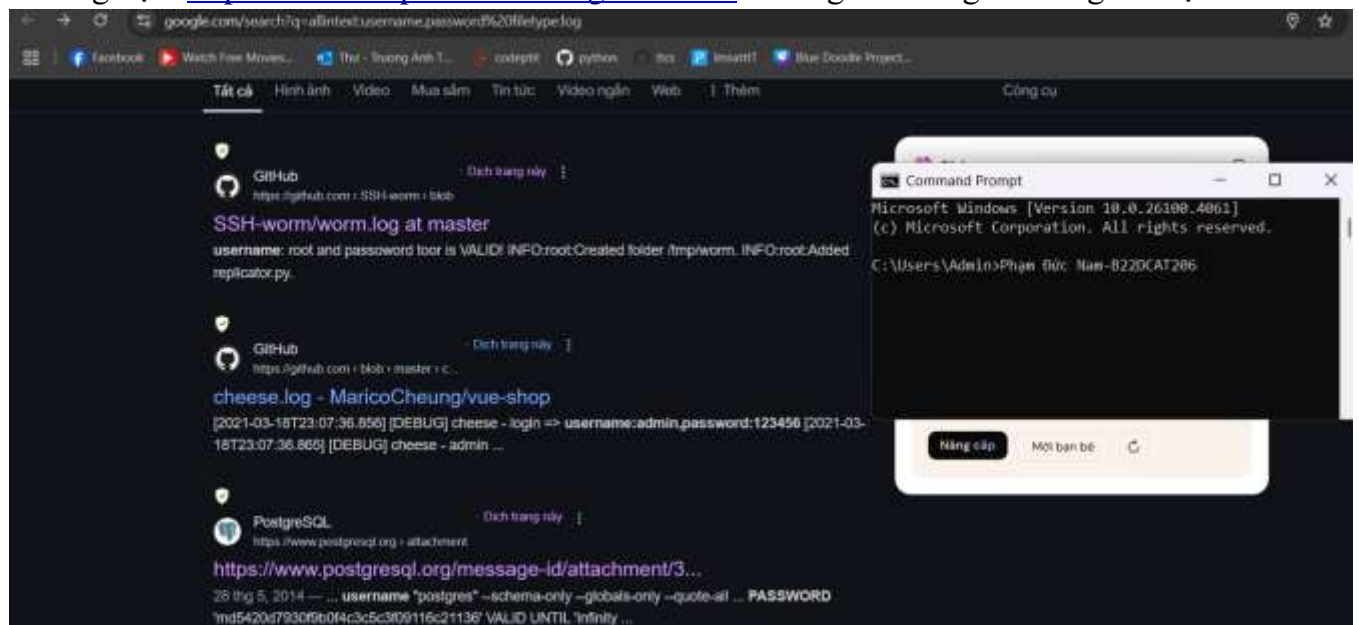
Text overlay on the right side of the image:

mục được liệt kê (index of) và chứa các tập tin id_rsa.pub. Những tập tin này là các khóa public SSH. Việc lộ thông tin này có thể cho phép truy cập trái phép vào các hệ thống nếu khóa private tương ứng không được bảo mật. Các tìm kiếm sử dụng "Google Dork" để xác định các trang web này, tập trung vào việc tìm kiếm các trang web bị cấu hình sai hoặc chưa được bảo mật đúng cách. Bạn cần hết sức cẩn thận với các trang web hiển thị...



Kết quả trả về

Thử nghiệm <https://www.exploit-db.com/ghdb/6412> tìm log có tên người dùng và mật khẩu



```
-----
pg_upgrade run on Wed May 20 08:03:08 2014
-----

pg_upgrade run on Wed May 20 08:03:55 2014
-----

command: "/usr/lib/postgresql/9.3/bin/pg_dumpall" --port 50432 --username "postgres" --schema-only --globals-only --quote-all-identifiers --binary-upgrade -f pg_upgrade_dump_globals.sql >>
"pg_upgrade_utility.log" 2>&1

command: "/usr/lib/postgresql/9.3/bin/vacuumdb" --host "/tmp/toto" --port 50432 --username "postgres" --all --analyze >> "pg_upgrade_utility.log" 2>&1
vacuumdb: limpiando la base de datos postgres
vacuumdb: limpiando la base de datos template1

command: "/usr/lib/postgresql/9.3/bin/vacuumdb" --host "/tmp/toto" --port 50432 --username "postgres" --all --freeze >> "pg_upgrade_utility.log" 2>&1
vacuumdb: limpiando la base de datos postgres
vacuumdb: limpiando la base de datos template1

command: cp -Rf "/mnt/datos/pg_log" "/mnt/datos/datos_9.3/main/pg_log" >> "pg_upgrade_utility.log" 2>&1

command: "/usr/lib/postgresql/9.3/bin/pg_resetlog" -f -s 767620816 "/mnt/datos/datos_9.3/main" >> "pg_upgrade_utility.log" 2>&1
B11Cura de transacciones reiniciada

command: "/usr/lib/postgresql/9.3/bin/pg_resetlog" -w 24527,24526 "/mnt/datos/datos_9.3/main" >> "pg_upgrade_utility.log" 2>&1
B11Cura de transacciones reiniciada

command: "/usr/lib/postgresql/9.3/bin/pg_resetlog" -i 00000000000000000000000000000000 "/mnt/datos/datos_9.3/main" >> "pg_upgrade_utility.log" 2>&1
B11Cura de transacciones reiniciada
```

Kết quả trả về

Quay lại GHDB (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):

15

Date Added	Dork
2024-07-04	intext:"proftpd.com" "index of"
2021-11-11	site:in com net intitle:"index of" ftp
2021-11-08	intitle:"index of" "/ftp.txt"
2021-11-05	intext:"index of" "ftp"
2021-11-03	intitle:"index of" "ftp.rtfm"
2021-11-01	intext:WS_FTPlog
2021-10-29	intitle:index.of /cftp /robots.txt
2021-10-08	intitle:"index of" "sftp.json"
2021-09-21	intitle:"index of ftp passwords"
2021-09-14	intext:/ftp intitle:"office"
2021-07-02	intext:/web-ftp.cgi
2021-04-19	intitle:"index of" ws_ftp.ini
2021-03-16	intext:ftp-intext(http https) intext:"@gmail.com" intext:subject fwi3confidentialimportantGANDcyv
2021-01-05	intext:ftp.*.* "ComputerName" + "intended" UnattendedMode"
2020-10-26	site:sftp.*/* intext:"login" intitle:"server login"

Select Command Prompt

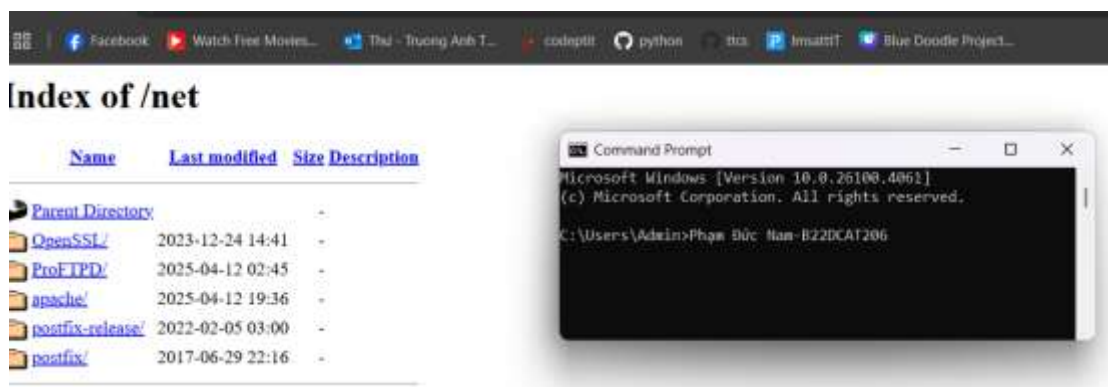
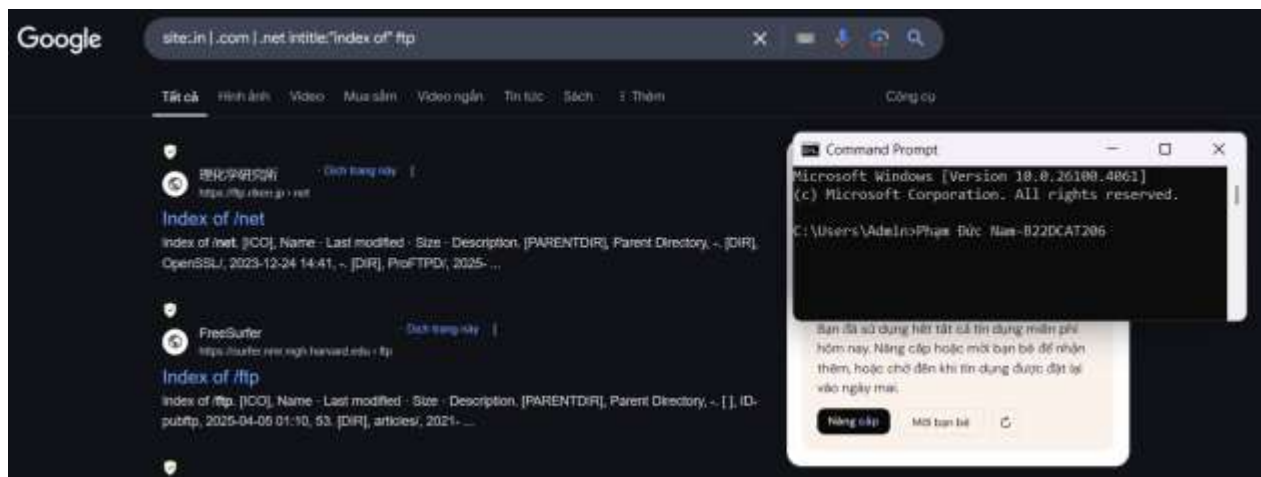
C:\Users\Admin>Phạm Đức Nam-B220CAT206

Quick Search

FTP

Category	Author
Files Containing Juicy Info	Fernando Mengali
Files Containing Juicy Info	Kishra Agarwal
Files Containing Juicy Info	Vivek Parshetti
Files Containing Juicy Info	Orkay Doshmukh
Files Containing Juicy Info	Muhammad Al-Amin
Files Containing Juicy Info	Suham CyberSec
Files Containing Juicy Info	Jawhar milan
Files Containing Juicy Info	Suman Das
Files Containing Passwords	Romeo Marin Cordoba
Web Server Detection	Lawrence March
Pages Containing Login Portals	Alexandros Pappas
Files Containing Juicy Info	Aman Srivastav
Files Containing Juicy Info	Agno
Files Containing Juicy Info	Alexandros Pappas
Pages Containing Login Portals	Alexandros Pappas

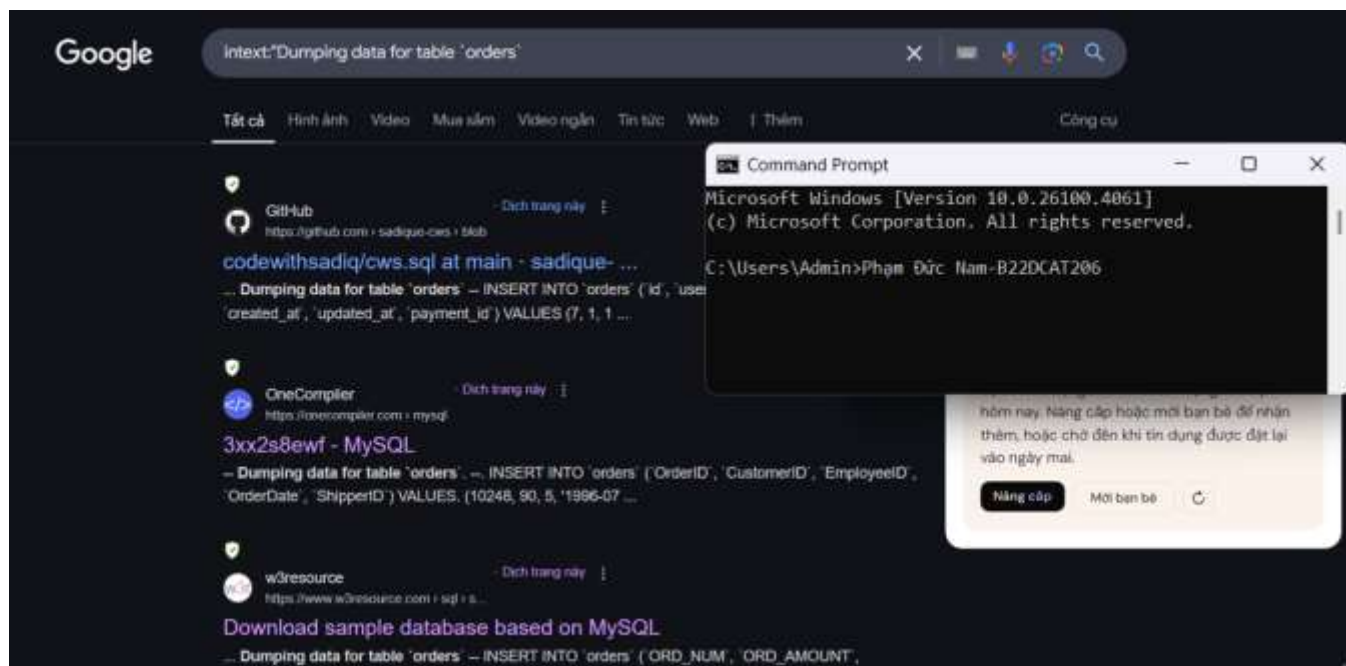
Thử nghiệm <https://www.exploit-db.com/ghdb/7772> chỉ ra các thư mục hoặc tệp index trên các máy chủ FTP. Các tệp index thường chứa danh sách các tệp và thư mục trên máy chủ, có thể cung cấp thông tin về nội dung của máy chủ và thường được sử dụng để quản lý nội dung hoặc chia sẻ tệp.



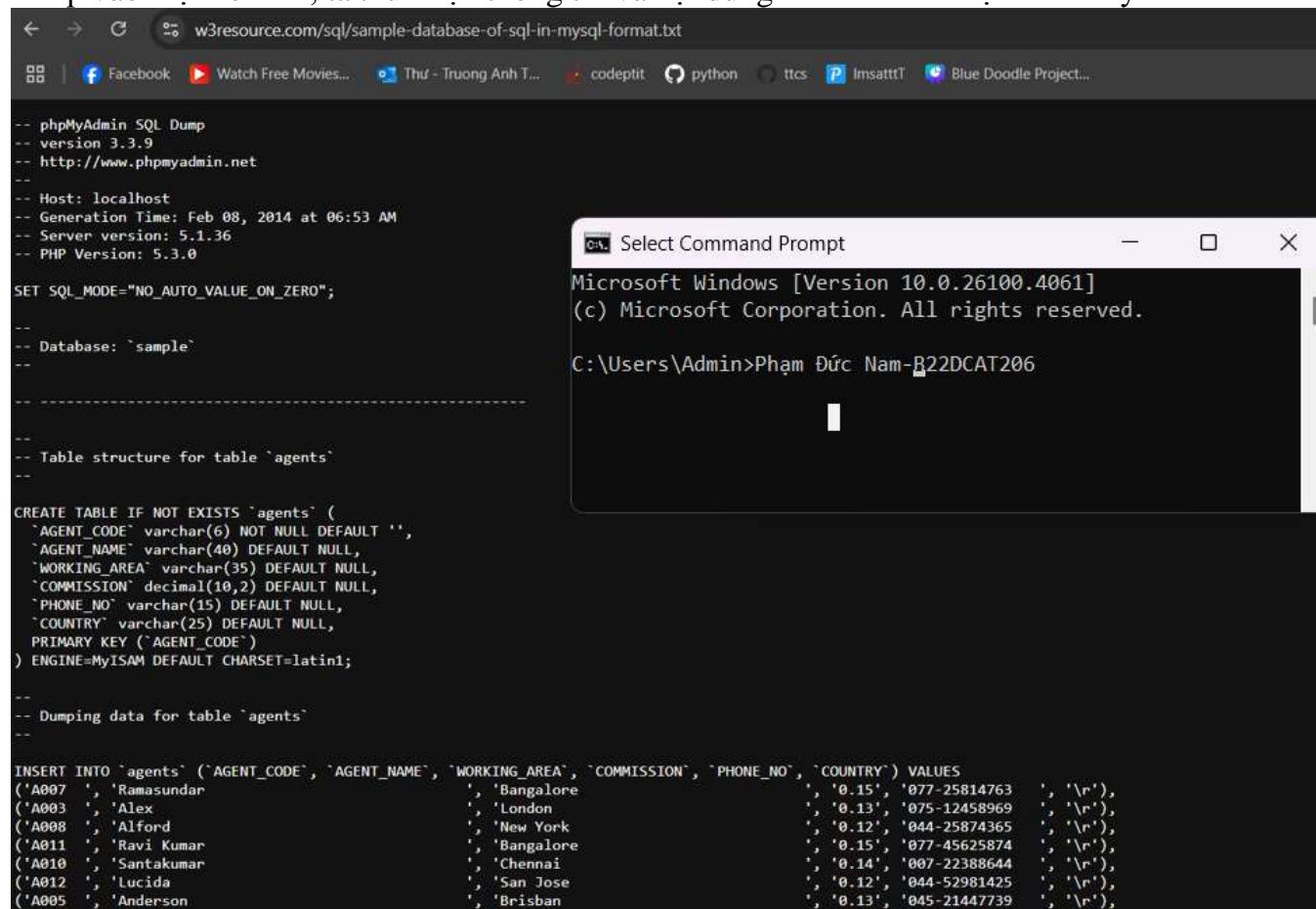
Kết quả trả về

Thực hành tìm hiểu trên 5 câu lệnh Google dork:

1. 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:



The screenshot shows a web browser window displaying a SQL dump file from w3resource.com. The dump is for a database named 'sample' and contains the structure and data for a table named 'agents'. The table has columns for agent code, name, working area, commission, phone number, and country. A Windows Command Prompt window is overlaid on the browser, showing the user's name 'Phạm Đức Nam' and a session ID 'B22DCAT206'.

```
-- 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`
--

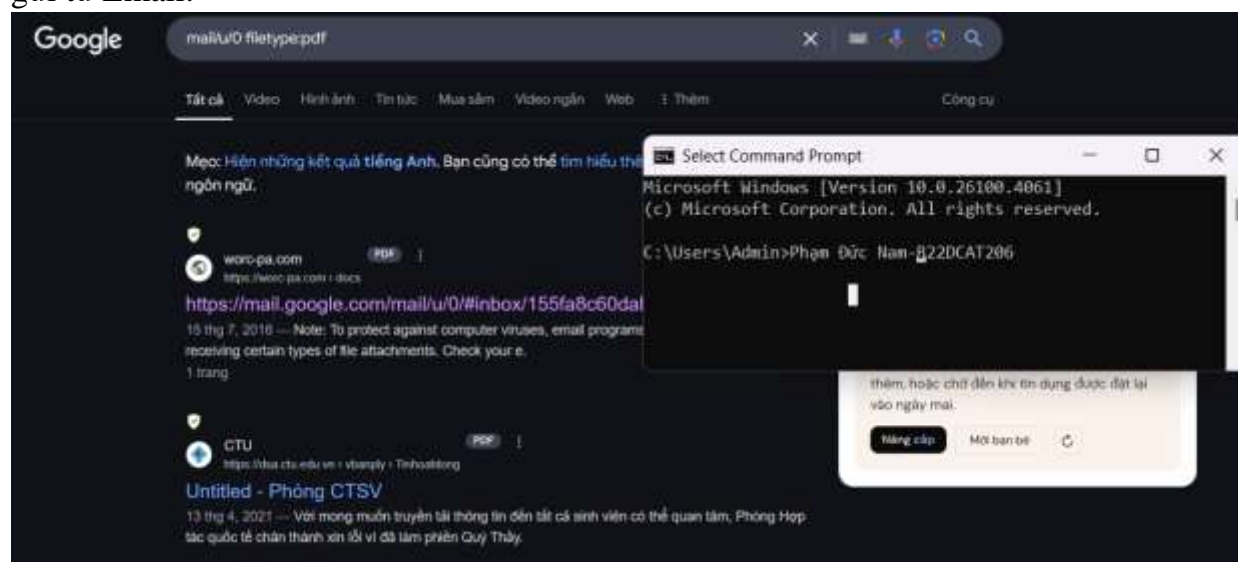
--
-- Table structure for table `agents`
--

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;

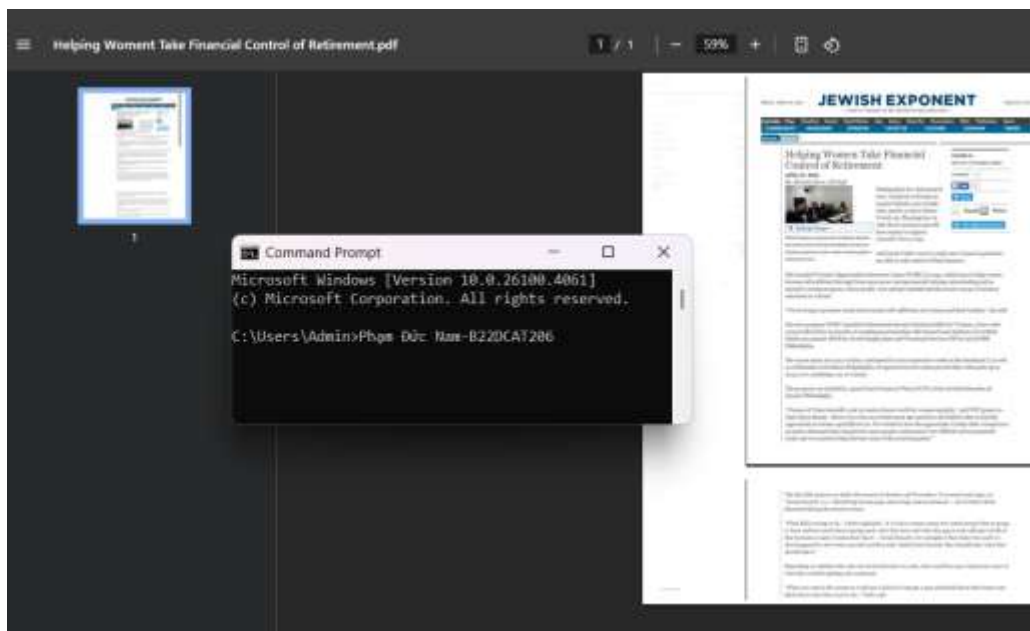
--
-- Dumping data for table `agents`
--

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

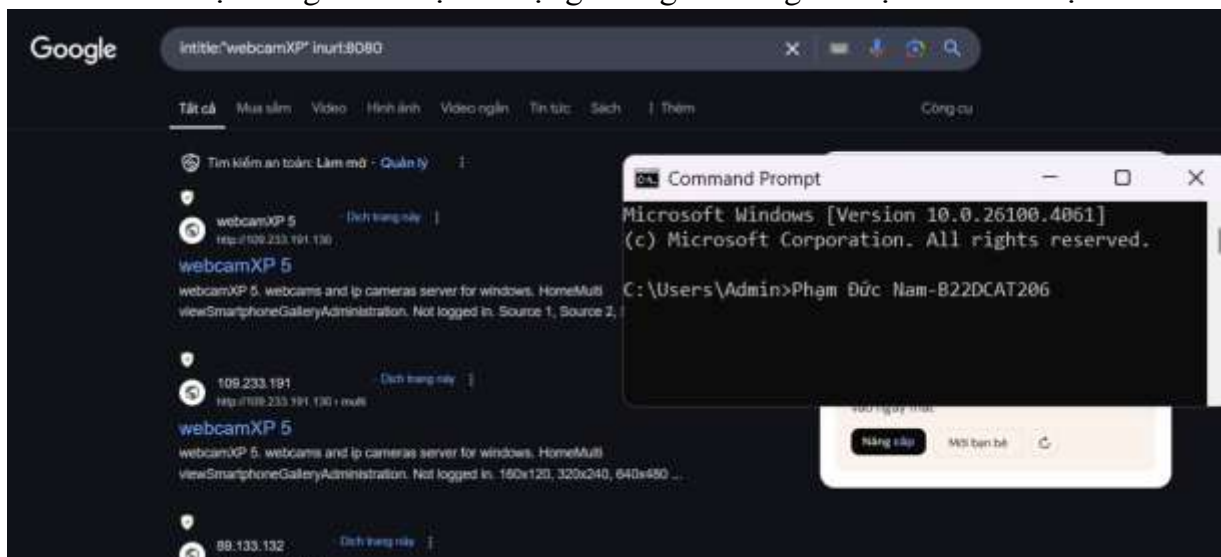
- Google dork “mail/u/0 filetype:pdf” được dùng để tìm các văn bản tài liệu định dạng pdf gửi từ Email:



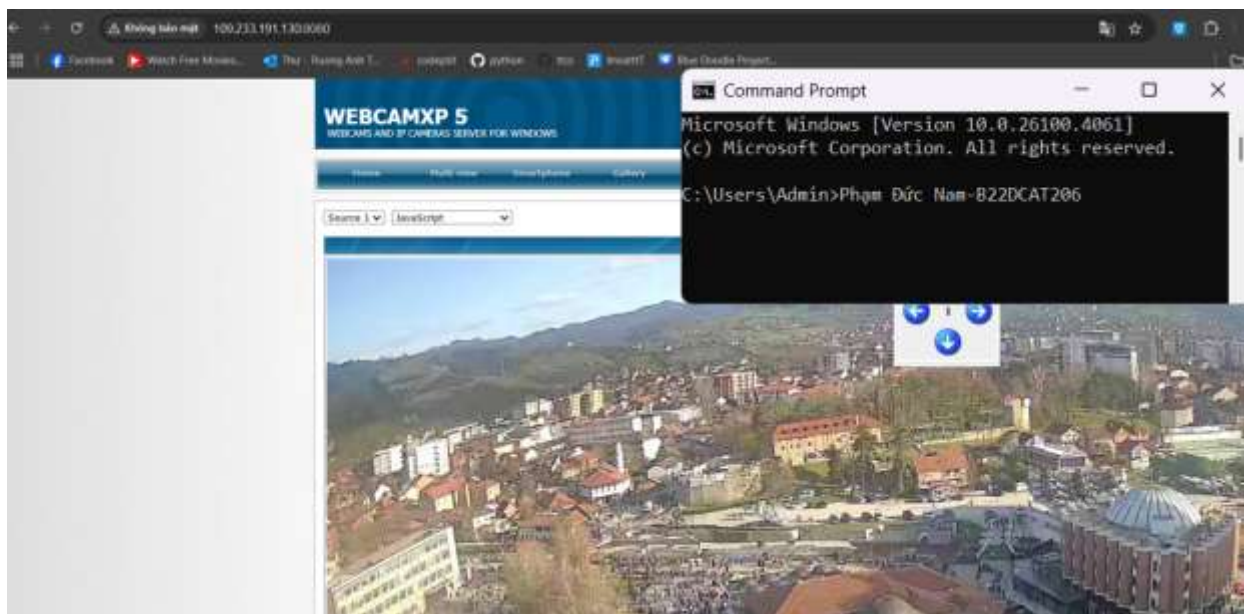
Nhấp vào một liên kết và nhận được văn bản dưới đây:



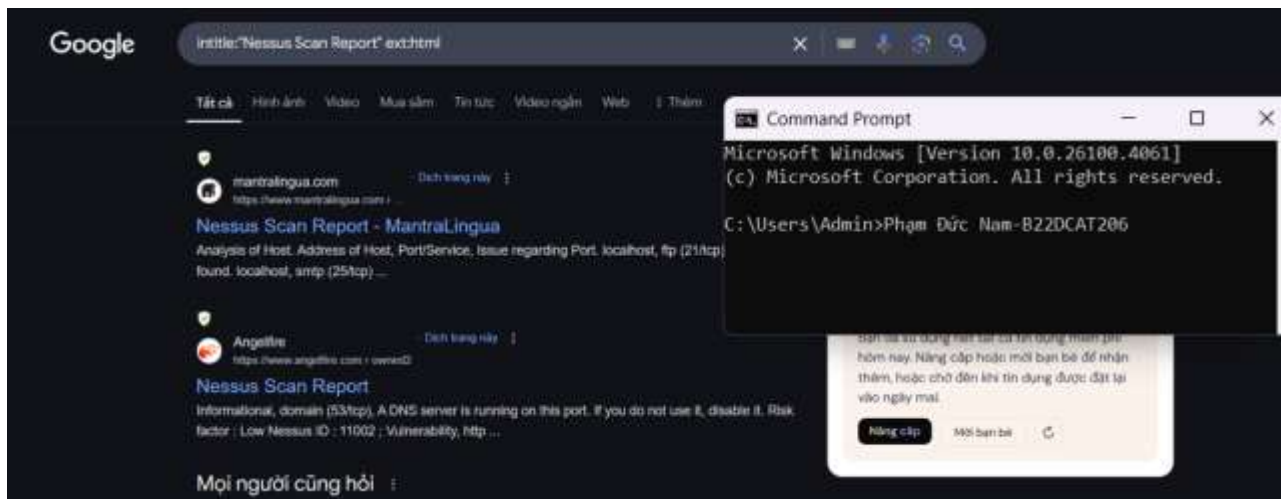
- Google dork “intitle:”webcamXP” inurl:8080” được dùng để tìm các dịch vụ camera webcamXP được công khai hoặc sử dụng tên người dùng và mật khẩu để nhận biết:



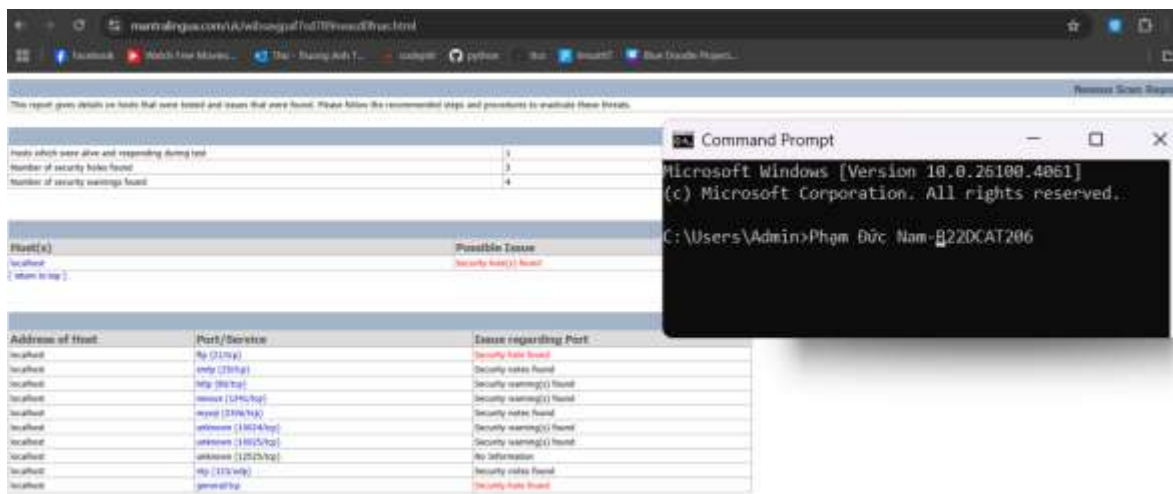
Nhấp vào liên kết và thu được các hình ảnh webcam gửi về:



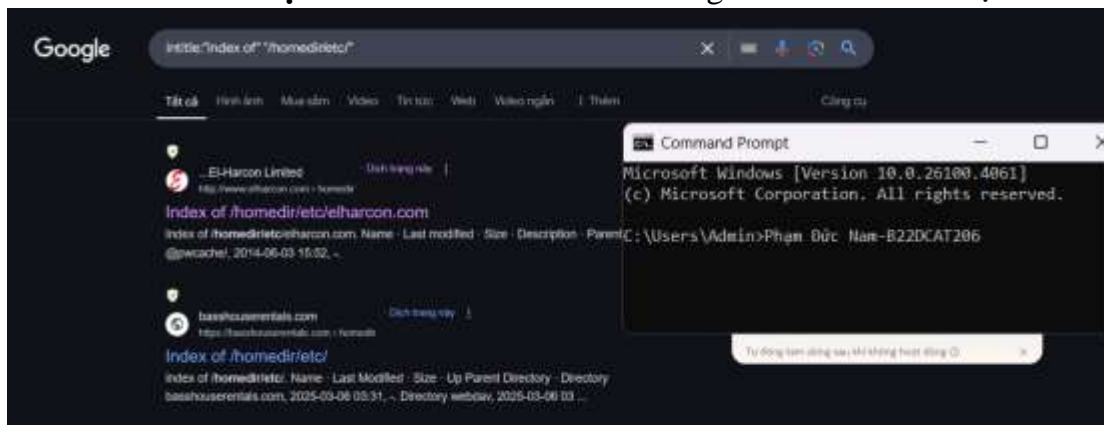
- Google dork “intitle:”Nessus Scan Report” ext:html” được dùng để tìm các báo cáo dò quét lỗ hổng bảo mật sử dụng Nessus:

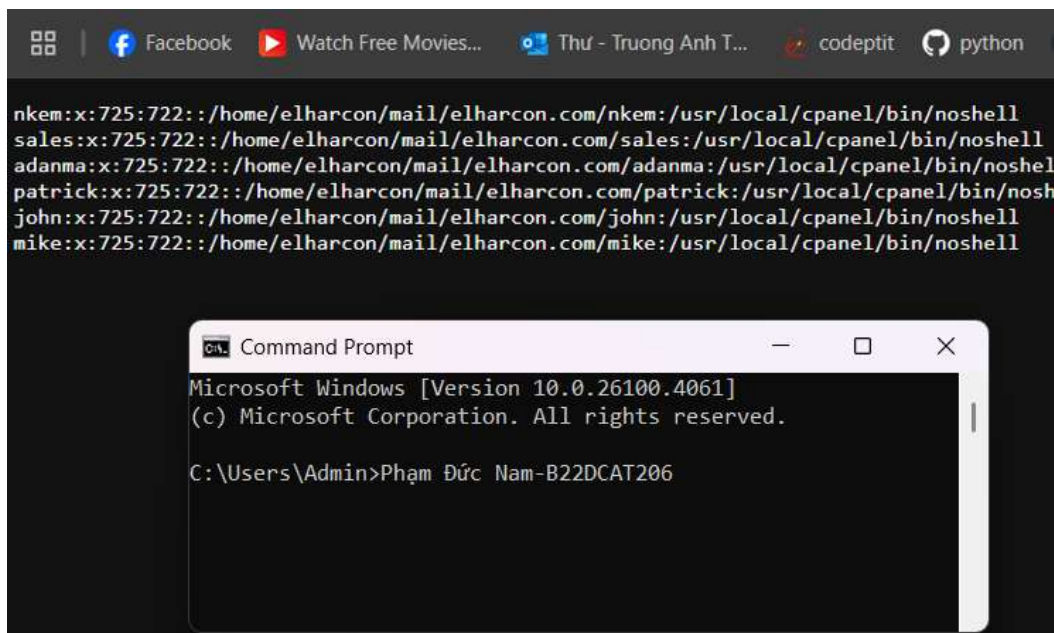


Nhấp vào liên kết và nhận được báo cáo chứa các lỗ hổng bảo mật:

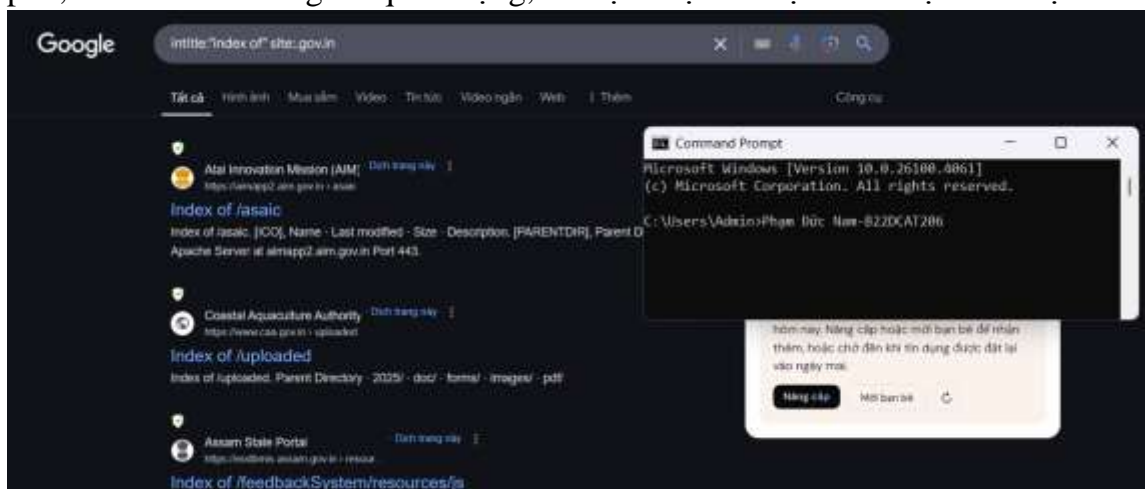


5. Google dork “intitle:index of” “/homedir/etc/” ” được dùng để tìm các thư mục web công khai (directory listing) có chứa đường dẫn giống như /homedir/etc/ – nơi thường có file cấu hình server hoặc tài khoản trên các host dùng cPanel/WHM hoặc shared hosting.



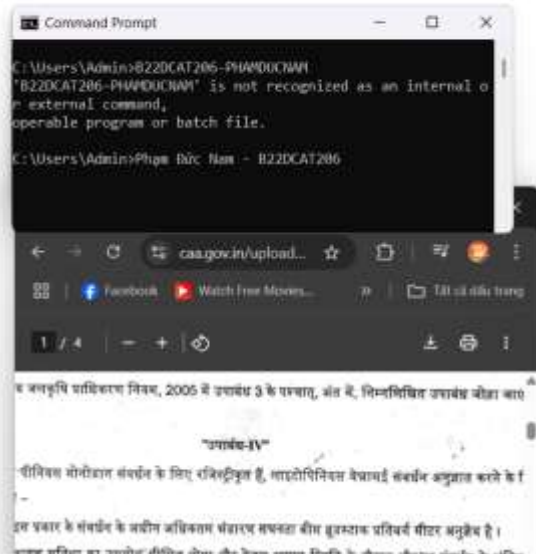


6. Google dork “intitle:”index of” site:.gov.in” nhằm mục đích tìm kiếm các trang có tiêu đề chứa "index of" trên các trang web thuộc tên miền .gov.in của chính phủ Ấn Độ. Điều này có thể dẫn đến việc phát hiện các thư mục hoặc tệp index trên các trang web chính phủ, có thể chứa thông tin quan trọng, tài liệu hoặc dữ liệu cần được bảo mật.



Nhấp vào liên kết để vào xem kết quả tìm kiếm:

- [Parent Directory](#)
- [100E.pdf](#)
- [1244E.pdf](#)
- [1573E.pdf](#)
- [18 - update_upload_2010_12_09 - final.pdf](#)
- [2013-2014.pdf](#)
- [2014-2015.pdf](#)
- [2873E.pdf](#)
- [2967E.pdf](#)
- [54th meeting_ag_12112020.pdf](#)
- [59th Meeting of CAA.pdf](#)
- [64E.pdf](#)
- [667E.pdf](#)
- [9-4-2008.pdf](#)
- [AFAoIngnts-07-02-2018.pdf](#)
- [AFAoIngnts-07-07-2017.pdf](#)
- [AFAoIngnts-19-02-2018.pdf](#)
- [AFAoIngnts-9-04-2018.pdf](#)
- [AFAoIngnts-10th-23-07-2018.pdf](#)
- [AFAoIngnts-11th-31-07-2018.pdf](#)
- [AFAoIngnts-12th-09-08-2018.pdf](#)
- [AFAoIngnts-13th-2018-11-02.pdf](#)
- [AFAoIngnts-14th-2018-11-02.pdf](#)
- [AFAoIngnts-15th-2019-03-15.pdf](#)
- [AFAoIngnts-16th-2019-03-18.pdf](#)
- [AFAoIngnts-17th-2019-10-18.pdf](#)
- [AFAoIngnts-17th-2019-11-13.pdf](#)
- [AFAoIngnts-17th-2019-11-16.pdf](#)



3. Kết luận

- Lý thuyết về Shodan, Google Hacking
- 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.
- Thử nghiệm thành công 10 ví dụ Google hacking như đã tìm hiểu bên trên.

4. Tài liệu tham khảo

- Shodan: [shodan là gì, hướng dẫn sử dụng shodan](#)
- Google Hacking: [Kiến thức về Google Hacking](#)
- Tìm hiểu về shodan và google hack
<https://money.cnn.com/gallery/technology/security/2013/05/01/shoda-dangerous-internet-searches/index.html>
- Principles of Computer Security: CompTIA Security+ and Beyond