

**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 HỒNG VỚI CÔNG CỤ TÌM KIẾM**

Sinh viên thực hiện:

B22DCAT199 Đỗ Duy Nam

Giảng viên hướng dẫn: TS.Đinh Trường Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

MỤC LỤC	2
DANH MỤC CÁC HÌNH VẼ.....	3
CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH	4
1.1 Mục đích.....	4
1.2 Tìm hiểu lý thuyết	4
1.2.1 Shodan.....	4
1.2.2 Google Hacking.....	5
1.3 Kết chương	7
CHƯƠNG 2. NỘI DUNG THỰC HÀNH	8
2.1 Shodan.....	8
2.2 Google Hacking.....	15
2.3 Kết chương	27
KẾT LUẬN	28
TÀI LIỆU THAM KHẢO	29

DANH MỤC CÁC HÌNH VẼ

Hình 1 Tạo tài khoản shodan.....	8
Hình 2 Các web Apache Server	9
Hình 3 Các trang web đang sử dụng framework CSS Bootstrap	9
Hình 4 Những dịch vụ hỗ trợ SSLv2 và không hỗ trợ TLS	10
Hình 5 SSH trên cổng 22 hoặc 3333	10
Hình 6 Screenshot Filter.....	11
Hình 7 Restricted Filter	11
Hình 8 CVE-2014-0160	12
Hình 9 Các máy chủ Google Web Server	12
Hình 10 Từ khóa “default password”	13
Hình 11 Sử dụng Metasploit Framework	13
Hình 12 Tìm kiếm tên module, khai báo module sử dụng	14
Hình 13 Thiết lập các cấu hình cần thiết	14
Hình 14 Kết quả thu được	15
Hình 15 Giao diện web của Google Hacking Database	15
Hình 16 Mục Footholds.....	16
Hình 17 Xem bất kì 1 thông tin liên quan	16
Hình 18 Thông tin liên quan tới ví dụ	17
Hình 19 Kết quả tìm được	18
Hình 20 Thông tin liên quan tới ví dụ	19
Hình 21 Kết quả tìm được	20
Hình 22 Thông tin liên quan tới ví dụ	21
Hình 23 Kết quả tìm được	22
Hình 24 Các Google dorks liên quan đến giao thức truyền tệp FTP.....	22
Hình 25 Kết quả tìm được	23
Hình 26 Kết quả tìm được	24
Hình 27 Kết quả tìm được	25
Hình 28 Kết quả tìm được	26
Hình 29 Kết quả tìm được	27

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

1.1 Mục đích

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

1.2 Tìm hiểu lý thuyết

1.2.1 Shodan

Shodan là một công cụ tìm kiếm đặc biệt được thiết kế để khám phá các thiết bị kết nối internet, chẳng hạn như máy chủ, camera, router, và các thiết bị IoT (Internet of Things). Không giống như các công cụ tìm kiếm thông thường như Google, Shodan không tìm kiếm nội dung web mà tập trung vào việc lập chỉ mục các giao thức mạng, địa chỉ IP, và thông tin kỹ thuật của các thiết bị trực tuyến.

Người dùng có thể sử dụng Shodan để tìm kiếm các thiết bị cụ thể (ví dụ: webcam, máy chủ chạy phần mềm nhất định) bằng cách nhập các truy vấn như "port:80 os:Windows" hoặc "webcamxp country:US". Nó thường được sử dụng bởi các nhà nghiên cứu bảo mật để kiểm tra lỗ hổng, nhưng cũng có thể bị lạm dụng nếu rơi vào tay kẻ xấu.

Cách hoạt động của Shodan

Shodan hoạt động bằng cách quét liên tục toàn bộ không gian địa chỉ IP công cộng trên internet (IPv4 và một phần IPv6). Nó gửi các yêu cầu đến các cổng mạng (ports) phổ biến như 80 (HTTP), 443 (HTTPS), 21 (FTP), 22 (SSH), v.v., để kiểm tra xem có thiết bị nào đang lắng nghe tại đó không. Khi nhận được phản hồi, Shodan thu thập thông tin từ các thiết bị này, bao gồm:

- Banner: Một đoạn thông tin mà thiết bị trả về, thường chứa dữ liệu như phiên bản phần mềm (ví dụ: Apache 2.4.7), hệ điều hành, hoặc thông điệp chào mừng.
- Địa chỉ IP và vị trí: Shodan gắn thẻ địa lý (geotag) dựa trên cơ sở dữ liệu địa chỉ IP để xác định vị trí gần đúng của thiết bị (quốc gia, thành phố).
- Cổng mở: Danh sách các cổng đang hoạt động trên thiết bị.
- Giao thức: Loại giao thức mà thiết bị sử dụng (HTTP, FTP, SSH, Telnet, v.v.).

Shodan không "xâm nhập" vào thiết bị mà chỉ ghi lại những gì thiết bị công khai trả về khi được hỏi. Dữ liệu này sau đó được lập chỉ mục và lưu trữ trên cơ sở dữ liệu của Shodan, cho phép người dùng tìm kiếm thông qua giao diện web hoặc API.

Quá trình quét của Shodan diễn ra tự động và liên tục, với hàng triệu thiết bị được kiểm tra mỗi ngày. Nó giống như một "máy quét radar" không lồ cho internet.

Ứng dụng của Shodan

- Bảo mật mạng

- Kiểm tra lỗ hổng: Các chuyên gia bảo mật dùng Shodan để tìm các thiết bị hoặc máy chủ dễ bị tấn công trong tổ chức của họ, ví dụ: máy chủ chạy phần mềm lỗi thời hoặc để cổng mặc định mở (như port 23 Telnet không bảo mật).
- Giám sát thiết bị: Doanh nghiệp có thể kiểm tra xem thiết bị nào của họ vô tình lộ ra trên internet công cộng, chẳng hạn như camera giám sát hoặc máy in không được bảo vệ bằng mật khẩu.
- Nghiên cứu bảo mật: Các nhà nghiên cứu sử dụng Shodan để phân tích xu hướng bảo mật, như số lượng thiết bị IoT không an toàn hoặc mức độ phổ biến của một lỗ hổng cụ thể.
- Kiểm tra hệ thống công cộng
 - Quản lý hạ tầng: Các công ty có thể dùng Shodan để đảm bảo rằng hệ thống của họ không vô tình để lộ thông tin nhạy cảm (ví dụ: cơ sở dữ liệu không mã hóa).
 - Phát hiện thiết bị giả mạo: Tìm các thiết bị bất thường xuất hiện trên mạng mà không được phép.
 - Ứng dụng trong tấn công mạng (mặt tiêu cực)
 - Tìm mục tiêu: Tin tặc có thể dùng Shodan để xác định các thiết bị dễ tấn công, như camera IP không mật khẩu, máy chủ chạy phần mềm cũ, hoặc hệ thống điều khiển công nghiệp (SCADA) tiếp xúc trực tuyến.
 - Khám phá hệ thống điều khiển: Một số hệ thống quan trọng (như đèn giao thông, nhà máy điện) từng bị phát hiện qua Shodan do cấu hình sai.
- Nghiên cứu và giáo dục
 - Phân tích xu hướng công nghệ: Các nhà nghiên cứu có thể dùng Shodan để xem phần mềm nào phổ biến nhất trên internet hoặc quốc gia nào có nhiều thiết bị IoT nhất.
 - Đào tạo: Sinh viên ngành an ninh mạng thường dùng Shodan để học về cách các hệ thống kết nối và cách bảo vệ chúng.

1.2.2 Google Hacking

Google Hacking là một kỹ thuật sử dụng các tính năng tìm kiếm nâng cao của Google để tìm kiếm thông tin nhạy cảm, lỗ hổng bảo mật hoặc dữ liệu không được bảo vệ trên internet. Nó thường được thực hiện bằng cách sử dụng các toán tử tìm kiếm đặc biệt (gọi là "Google Dorks") để lọc và truy vấn chính xác hơn, thay vì chỉ nhập từ khóa thông thường. Kỹ thuật này tận dụng khả năng lập chỉ mục mạnh mẽ của Google để phát hiện các trang web, tệp, hoặc thiết bị có cấu hình sai, từ đó lộ ra thông tin như mật khẩu, tên người dùng, tệp cấu hình, hoặc thậm chí các thiết bị kết nối internet như camera giám sát.

Google Hacking có thể được sử dụng cho mục đích hợp pháp, chẳng hạn như kiểm tra bảo mật (ethical hacking) để phát hiện lỗ hổng và cảnh báo quản trị viên, nhưng cũng có thể

bị tội phạm mạng lợi dụng để thu thập dữ liệu nhạy cảm phục vụ các cuộc tấn công. Vì vậy, nó vừa là công cụ hữu ích vừa tiềm ẩn rủi ro tùy thuộc vào cách sử dụng.

Cách hoạt động của Google Hacking

Google Hacking hoạt động dựa trên việc khai thác các tính năng tìm kiếm nâng cao của Google thông qua các toán tử tìm kiếm (search operators) và sự hiểu biết về cách Google lập chỉ mục các trang web. Dưới đây là cách nó vận hành chi tiết:

- Sử dụng Google Dorks:
 - Google Dorks là các chuỗi truy vấn được xây dựng cẩn thận bằng cách kết hợp từ khóa với toán tử tìm kiếm để nhắm mục tiêu thông tin cụ thể. Ví dụ:
 - `inurl:login` - Tìm các trang có từ "login" trong URL, thường dẫn đến các trang đăng nhập không được bảo vệ.
 - `filetype:sql site:*.edu | site:*.org -inurl:(signup | login)` - Tìm các tệp cơ sở dữ liệu SQL trên các trang giáo dục hoặc tổ chức, loại trừ các trang đăng ký hoặc đăng nhập.
- Khai thác lập chỉ mục của Google:
 - Google liên tục thu thập dữ liệu từ internet và lưu trữ trong cơ sở dữ liệu của nó. Các trang web hoặc tệp không được cấu hình đúng (ví dụ: không có tệp robots.txt để chặn)
- Phân tích phản hồi:
 - Google không trực tiếp hiển thị nội dung nhạy cảm, nhưng các quản trị viên web đôi khi để lộ thông tin do cấu hình sai, như danh sách thư mục (directory listing) hoặc tệp nhạy cảm (PDF, Excel, SQL dump) mà không có bảo mật.
- Kiểm tra kết quả:
 - Người dùng nhập truy vấn vào Google, kiểm tra kết quả, và tinh chỉnh truy vấn để có được thông tin chính xác hơn. Ví dụ, tìm camera IP bằng truy vấn: `inurl:(axis | webcam | camera)`.

Ứng dụng của Google Hacking

- Ứng dụng hợp pháp
 - Kiểm tra bảo mật (Penetration Testing):
 - Các chuyên gia bảo mật sử dụng Google Hacking để phát hiện lỗ hổng trên hệ thống của khách hàng, như tệp cấu hình lộ ra ngoài (`filetype:conf inurl:(config)`), trang quản trị không bảo vệ (`inurl:admin`), hoặc thông tin nhạy cảm trên trang web của họ.
 - Nghiên cứu và thu thập thông tin (OSINT):

- Các nhà báo, nhà nghiên cứu, hoặc cơ quan thực thi pháp luật dùng Google Hacking để tìm thông tin công khai, như tài liệu chính phủ (filetype:pdf site:*.gov) hoặc hồ sơ công ty.
- Kiểm tra rò rỉ dữ liệu:
 - Doanh nghiệp có thể tìm kiếm xem dữ liệu nội bộ của họ có bị lộ không, ví dụ: site:pastebin.com "companyname" password.
- Ứng dụng bất hợp pháp
 - Tấn công mạng:
 - Tin tặc dùng Google Hacking để tìm các máy chủ dễ bị tấn công (như inurl:(phpmyadmin | webmin)), thông tin đăng nhập bị lộ (filetype:txt "username:password"), hoặc các trang lỗi SQL injection (inurl:(id= | page=)).
 - Khai thác dữ liệu cá nhân:
 - Tìm kiếm danh sách email, số điện thoại, hoặc thông tin cá nhân từ các tệp không được bảo vệ (filetype:xls "email" "phone").
 - Truy cập thiết bị IoT:
 - Tìm camera giám sát, máy in, hoặc thiết bị khác không có bảo mật (inurl:(viewerframe | webcamxp)).

1.3 Kết chương

Chương này đã tìm hiểu cơ bản về Shoban và Google Hacking, hiểu được cách hoạt động cũng như là ứng dụng của chúng.

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

2.1 Shodan

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

The image shows a 'Create Account' form for Shodan. The form has fields for Username (B22DCAT199), Password (masked with dots), Confirm Password (masked with dots), and Email (doduynam1308@gmail.com). There is a checkbox for 'Subscribe to the newsletter' which is checked. Below the form is a green 'CREATE' button. To the right of the form is a 'CONTACT US' section with the email support@shodan.io and social media icons for LinkedIn, Messenger, Twitter, and Facebook. At the bottom right, it says 'Shodan ® - All rights reserved'.

Create Account

Username
B22DCAT199

Password
.....

Confirm Password
.....

Email
doduynam1308@gmail.com

☒ Subscribe to the newsletter

By creating an account you are agreeing to our [Privacy Policy](#) and [Terms of Use](#)

CREATE

Command Prompt

Microsoft Windows [Version 10.0.26100.3775]
(c) Microsoft Corporation. All rights reserved.

C:\Users\doduy>date
The current date is: 12/04/2025
Enter the new date: (dd-mm-yy)

C:\Users\doduy>echo DoDuyNam_B22DCAT199
DoDuyNam_B22DCAT199

C:\Users\doduy>

// CONTACT US
support@shodan.io

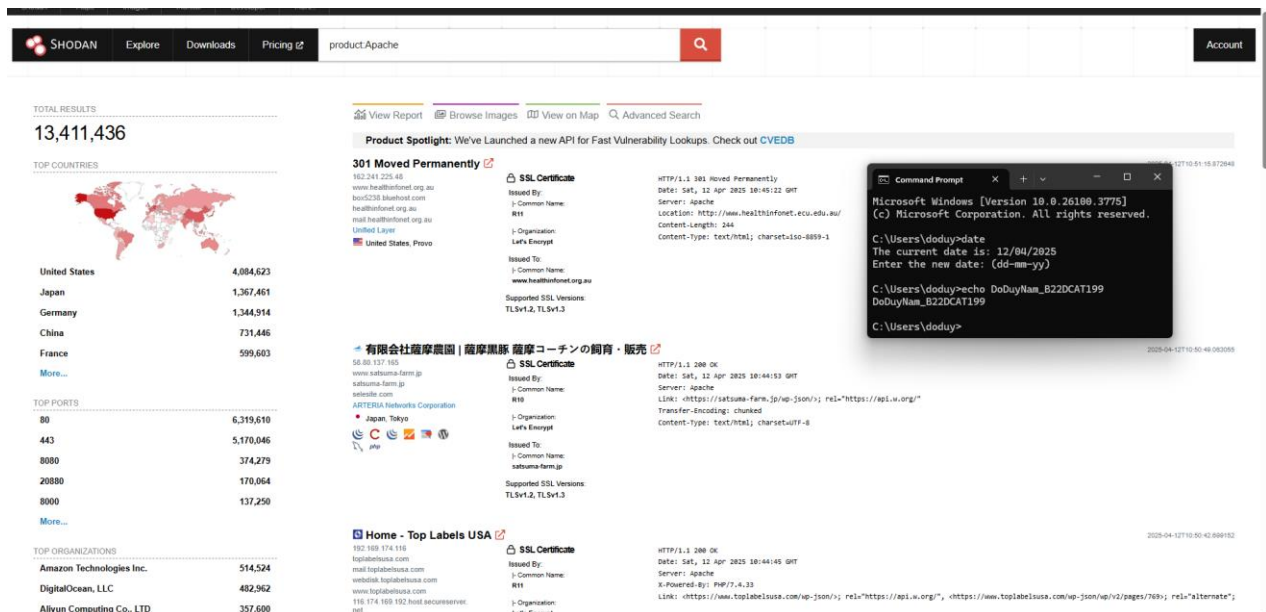
[in](#) [m](#) [t](#) [f](#)

Shodan ® - All rights reserved

Hình 1 Tạo tài khoản shodan

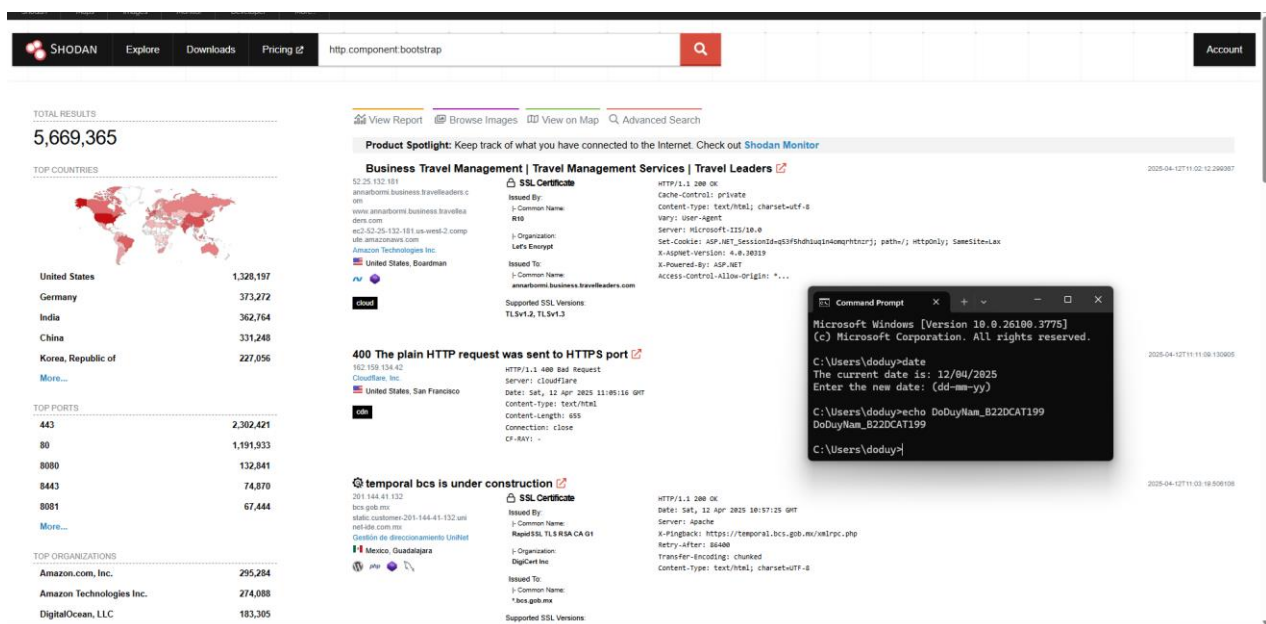
Tìm hiểu và thử nghiệm các bộ lọc trong danh sách

- Basic: Tìm kiếm các web Apache Server



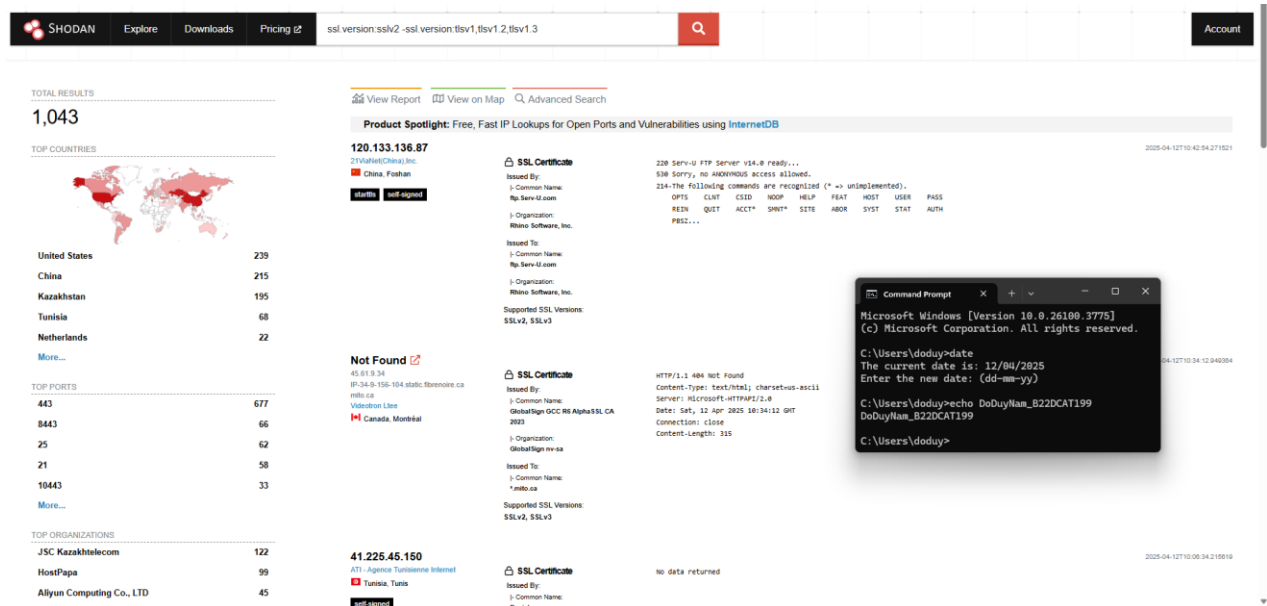
Hình 2 Các web Apache Server

- HTTP Filter: Tìm kiếm các trang web đang sử dụng framework CSS Bootstrap



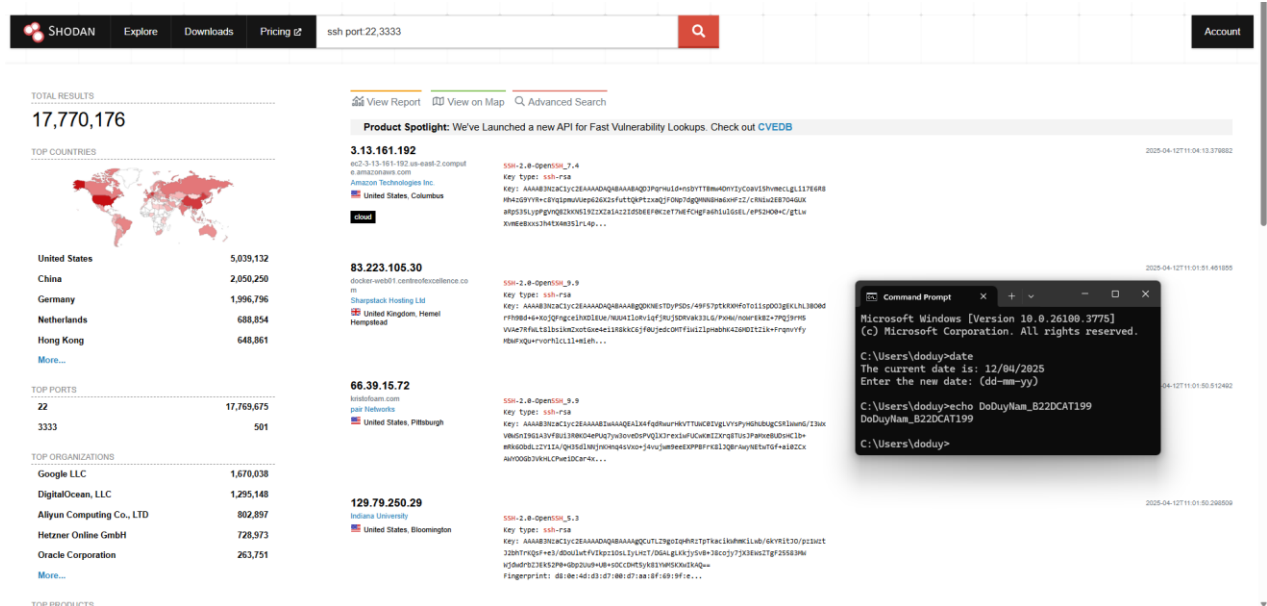
Hình 3 Các trang web đang sử dụng framework CSS Bootstrap

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



Hình 4 Những dịch vụ hỗ trợ SSLv2 và không hỗ trợ TLS

- SSH Filter: Tìm kiếm SSH trên cổng 22 hoặc 3333



Hình 5 SSH trên cổng 22 hoặc 3333

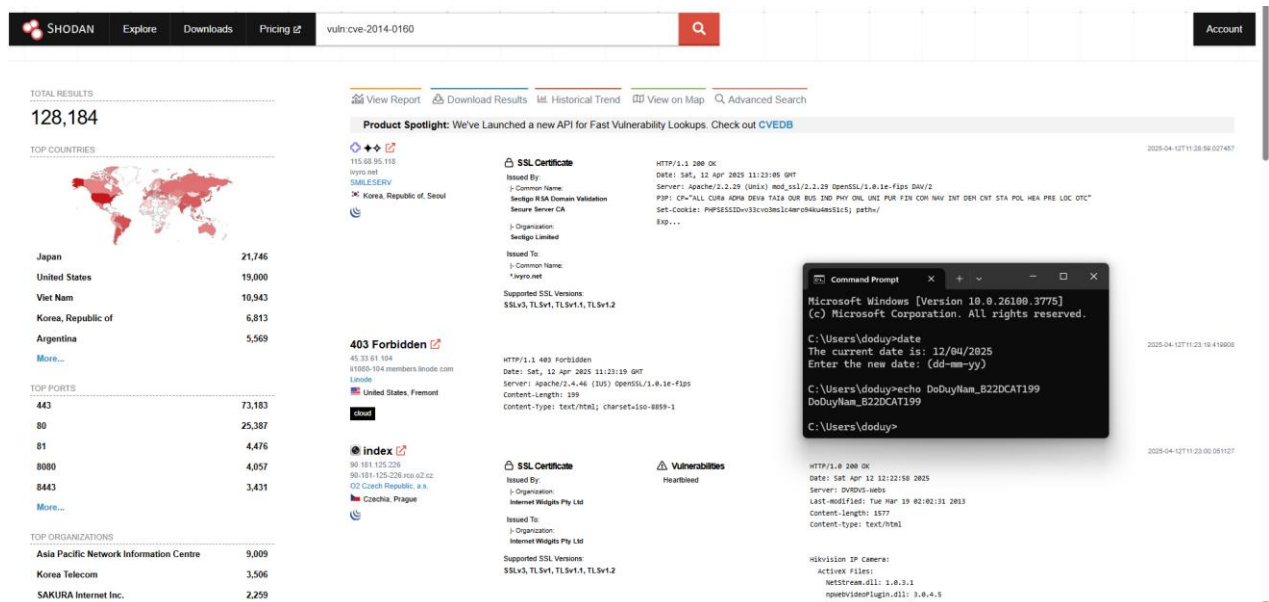
- Screenshot Filter: Tìm kiếm OCR trong máy tính từ xa xem có bị nhiễm ransomware hay không

Hình 6 Screenshot Filter

- Resstricted Filter: Tìm kiếm các thiết bị Citrix ở Đức, Thụy Sĩ hoặc Pháp để bị tấn công bởi CVE-2019-19781.

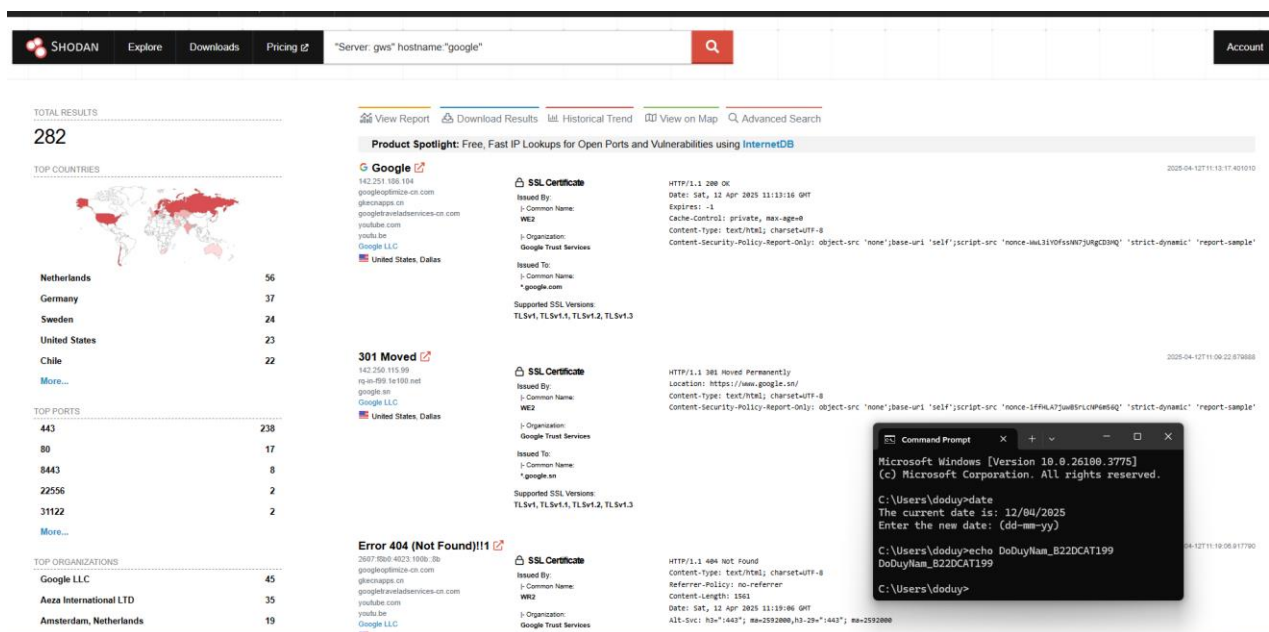
Hình 7 Resstricted Filter

- Tìm kiếm với mã CVE-ID



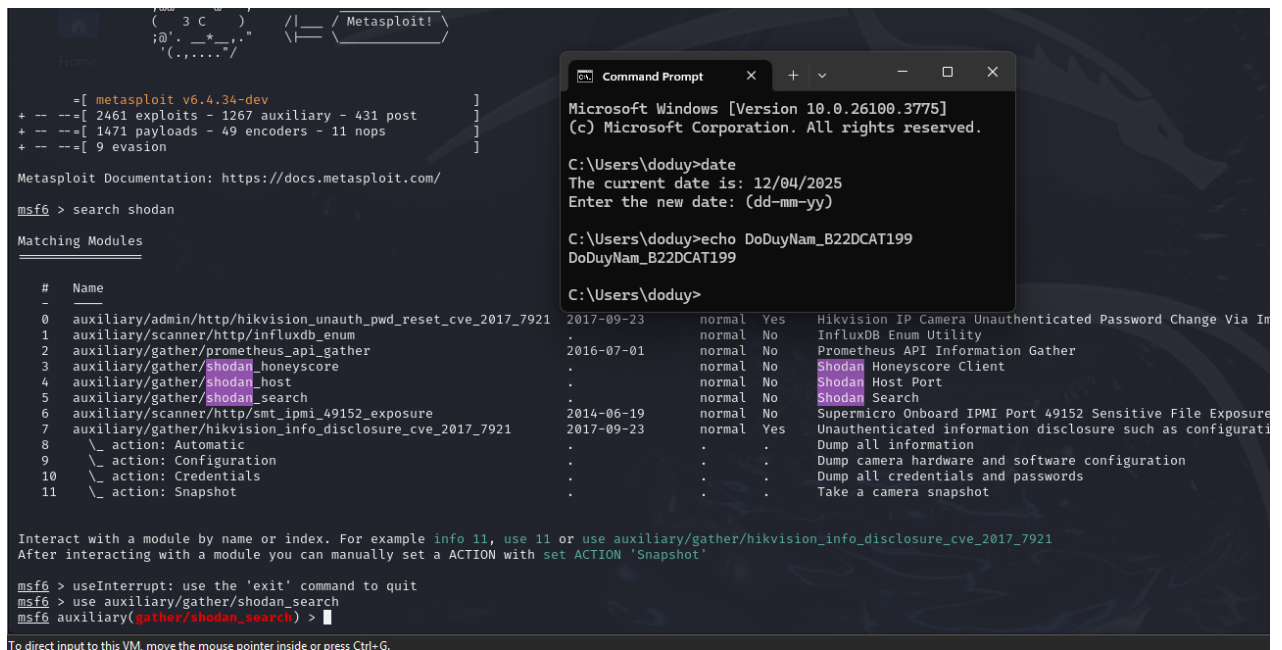
Hình 8 CVE-2014-0160

- Tìm kiếm máy chủ GWS (Google Web Server)

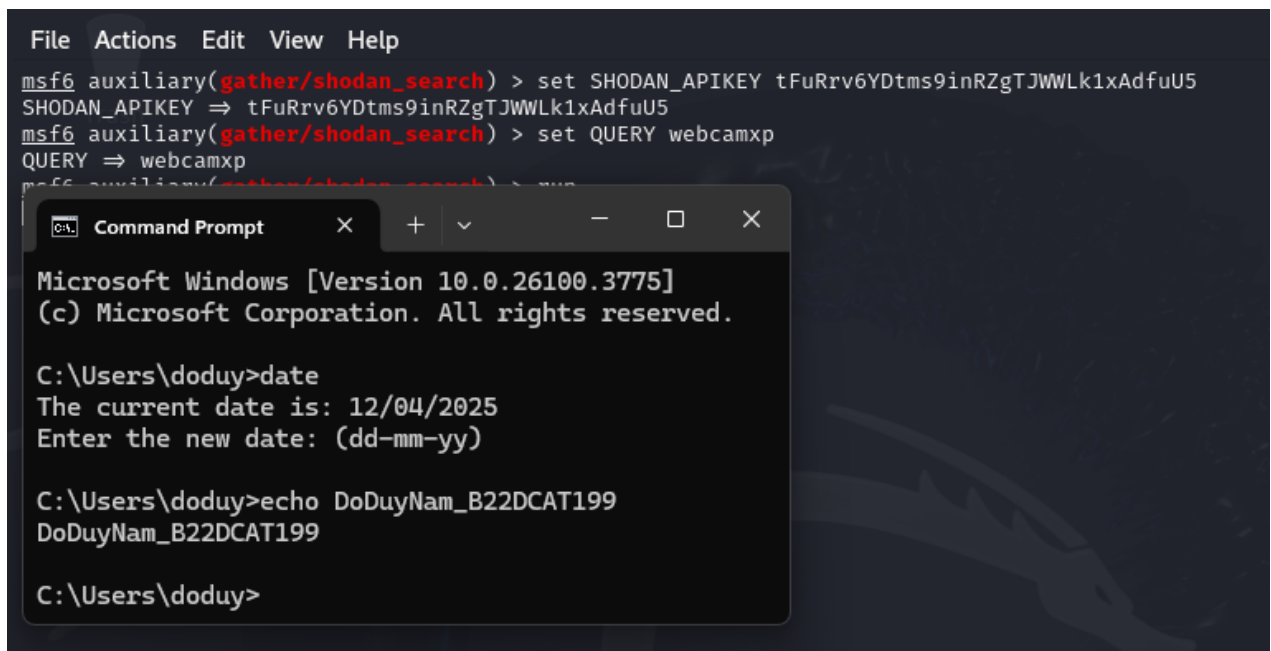


Hình 9 Các máy chủ Google Web Server

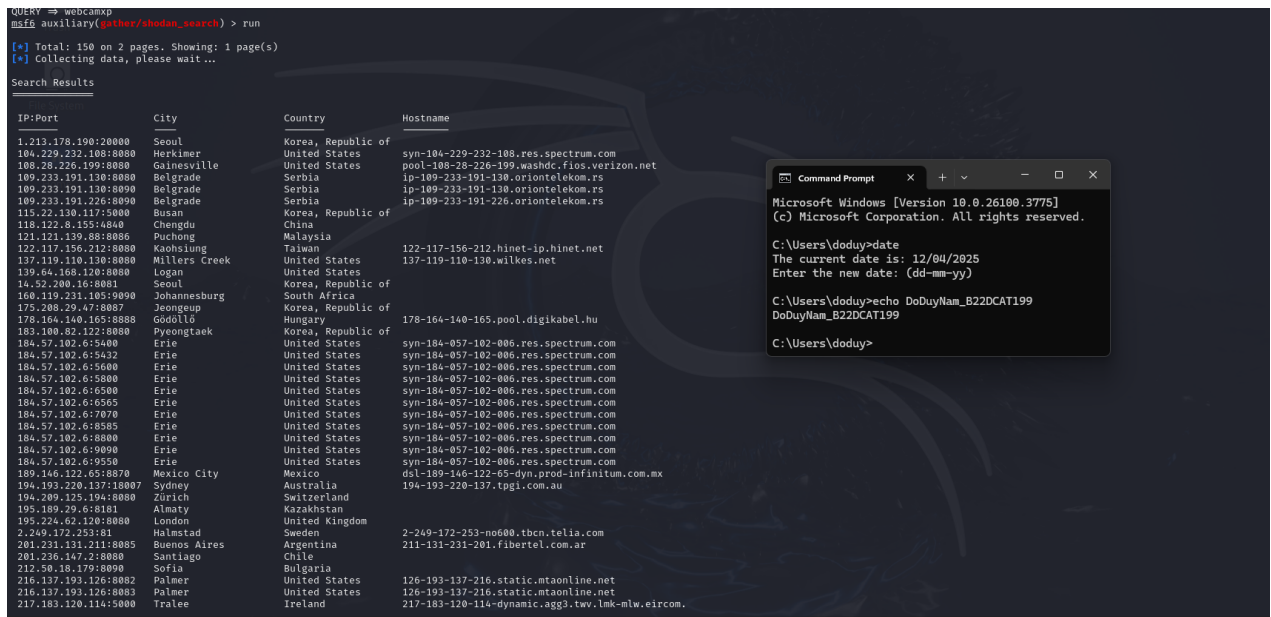
- Tìm kiếm từ khóa “Default Password”



Hình 12 Tìm kiếm tên module, khai báo module sử dụng



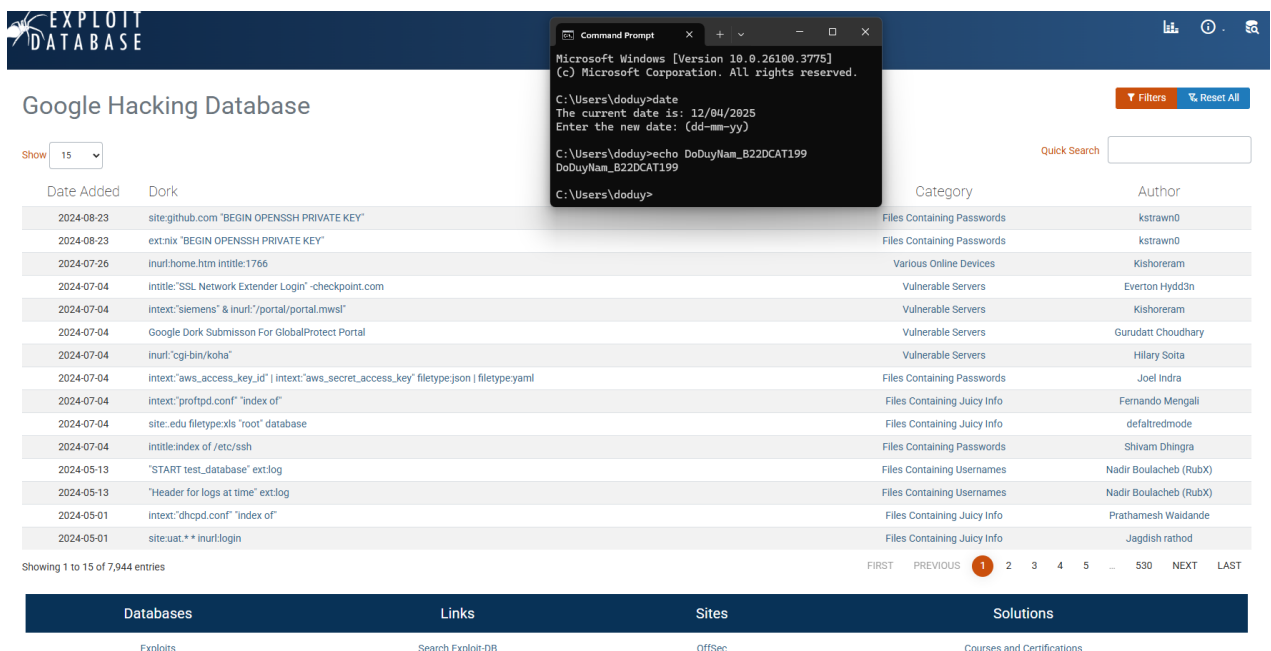
Hình 13 Thiết lập các cấu hình cần thiết



Hình 14 Kết quả thu được

2.2 Google Hacking

- Vào website www.exploit-db.com/google-hacking-database.



Hình 15 Giao diện web của 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. Chọn một mục 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.

Date Added	Dork	Category	Author
2022-01-12	inurl:adminpanel site:gov.*	Footholds	Asheet Tirkey
2021-09-29	inurl:maps.arcgis.com + "City of"	Footholds	Edmond Major
2020-09-14	inurl:wanavigator/jsp	Footholds	Javier Bernardo
2020-09-11	mail/u/0 filetype:pdf	Footholds	AjithKumar
2020-09-11	intitle:"index of" "httpd.pid"	Footholds	Navaneeth Shyam
2020-09-10	inurl:"/plugins/servlet/Wallboard/"	Footholds	Pratik Khalane
2020-09-01	inurl:/Dashboard.xhtml intitle:"Dashboard"	Footholds	Alexandros Pappas
2020-08-31	inurl:/app/kibana "Kibana" -discuss -ipaddress -git	Footholds	Adithya Chandra
2020-08-27	inurl:CTCWebService	Footholds	Javier Bernardo
2020-07-21	intitle:"index of" +jmx-console	Footholds	Tanmay Bhattacharjee
2020-07-09	intitle:"index of/" +htdocs	Footholds	Tanmay Bhattacharjee
2020-07-08	intitle:"index of/" +htaccess	Footholds	Priyanka Prasad
2020-07-02	intitle:"index of" "nginx.log"	Footholds	Emmanuel Karunya
2020-07-01	"radius-server key" ext:cfg OR ext:log OR ext:txt	Footholds	Alexandros Pappas
2020-06-22	inurl:"/arcgis/rest/services"	Footholds	Tolga Kayaş

Hình 16 Mục Footholds

- Chọn bất kì để xem các thông tin liên quan.

GHDB-ID: 7839
Author: ASHEET TIRKEY
Published: 2022-01-12

Google Dork Description:
inurl:adminpanel site:gov.*
Google Search: inurl:adminpanel site:gov.*

Description: inurl:adminpanel site:gov.*
This google dork indexes pages containing Admin Login Panels of government
sites where an attacker can login and bypass restrictions if not configured properly.
Author : Asheet Tirkey
Date : 11th Jan 2022

Databases	Links	Sites	Solutions
Exploits	Search Exploit-DB	OffSec	Courses and Certifications
Google Hacking	Submit Entry	Kali Linux	Learn Subscriptions
Papers	SearchSploit Manual	VulnHub	OffSec Cyber Range
Shellcodes	Exploit Statistics		Proving Grounds

Hình 17 Xem bất kì 1 thông tin liên quan

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

EXPLOIT DATABASE

intitle:"Index of" "DCIM"

GHDB-ID:
4057

Author:
ANONYMOUS

Published: 2015-08-19

Google Dork Description:
intitle:"Index of" "DCIM"

Google Search: intitle:"Index of" "DCIM"

A lot of Camera Photos Dump.

Have Fun!

Rootkit.

Command Prompt

Microsoft Windows [Version 10.0.26100.3775]
 (c) Microsoft Corporation. All rights reserved.
 C:\Users\doduy>date
 The current date is: 12/04/2025
 Enter the new date: (dd-mm-yy)
 C:\Users\doduy>echo DoDuyNam_B22DCAT199
 DoDuyNam_B22DCAT199
 C:\Users\doduy>

Databases

[Exploits](#)
[Google Hacking](#)
[Papers](#)
[Shellcodes](#)

Links

[Search Exploit-DB](#)
[Submit Entry](#)
[SearchSploit Manual](#)
[Exploit Statistics](#)

Solutions

[OffSec](#)
[Kali Linux](#)
[VulnHub](#)

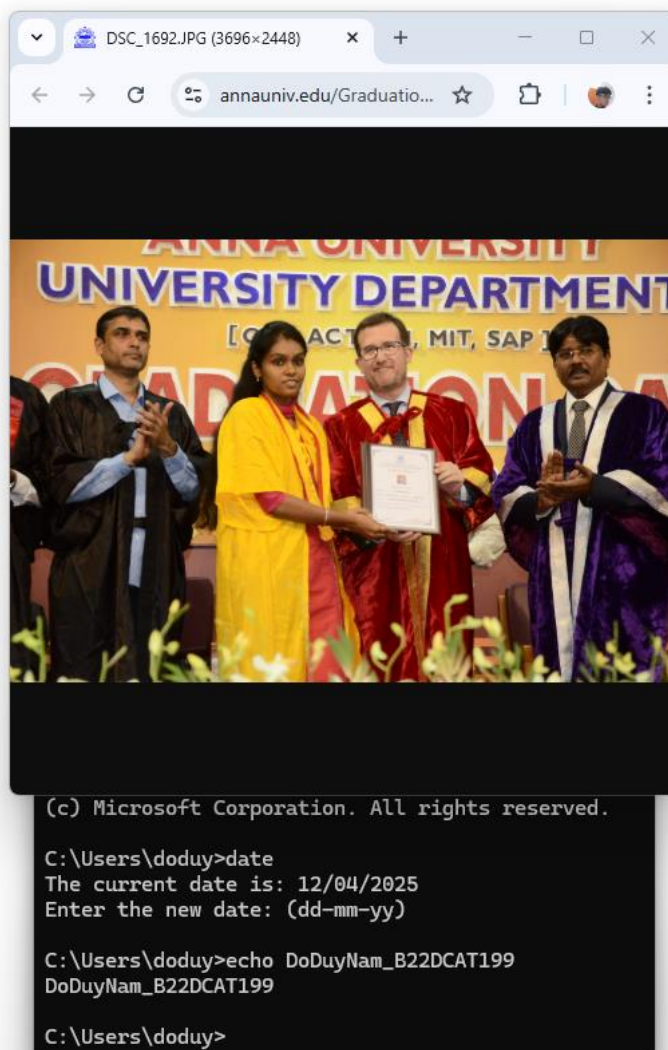
[Courses and Certifications](#)
[Learn Subscriptions](#)
[OffSec Cyber Range](#)
[Proving Grounds](#)
[Penetration Testing Services](#)

Hình 18 Thông tin liên quan tới ví dụ

- Thử với 1 truy vấn tìm kiếm bất kỳ.

Index of /Graduation_Day_2023/2/d/DCIM/125D7000

Name	Last modified	Size	Description
Parent Directory			
DSC_1692.JPG	2023-10-02 10:23	4.8M	
DSC_1693.JPG	2023-10-02 10:23	4.9M	
DSC_1694.JPG	2023-10-02 10:23	4.7M	
DSC_1695.JPG	2023-10-02 10:24	4.7M	
DSC_1696.JPG	2023-10-02 10:24	4.6M	
DSC_1697.JPG	2023-10-02 10:24	4.7M	
DSC_1698.JPG	2023-10-02 10:24	4.7M	
DSC_1699.JPG	2023-10-02 10:24	4.8M	
DSC_1700.JPG	2023-10-02 10:25	4.8M	
DSC_1701.JPG	2023-10-02 10:25	4.8M	
DSC_1702.JPG	2023-10-02 10:25	4.6M	
DSC_1703.JPG	2023-10-02 10:25	4.6M	
DSC_1704.JPG	2023-10-02 10:25	4.6M	
DSC_1705.JPG	2023-10-02 10:26	5.0M	
DSC_1706.JPG	2023-10-02 10:27	5.0M	
DSC_1707.JPG	2023-10-02 10:27	5.1M	
DSC_1708.JPG	2023-10-02 10:27	4.8M	
DSC_1709.JPG	2023-10-02 10:28	5.1M	
DSC_1710.JPG	2023-10-02 10:28	5.0M	
DSC_1711.JPG	2023-10-02 10:29	5.0M	
DSC_1712.JPG	2023-10-02 10:29	4.7M	
DSC_1713.JPG	2023-10-02 10:29	4.9M	
DSC_1714.JPG	2023-10-02 10:30	4.9M	
DSC_1715.JPG	2023-10-02 10:30	4.9M	
DSC_1716.JPG	2023-10-02 10:30	5.2M	
DSC_1717.JPG	2023-10-02 10:30	5.1M	
DSC_1718.JPG	2023-10-02 10:30	4.7M	
DSC_1719.JPG	2023-10-02 10:30	5.0M	
DSC_1720.JPG	2023-10-02 10:44	4.7M	
DSC_1721.JPG	2023-10-02 10:44	4.7M	
DSC_1722.JPG	2023-10-02 10:44	5.0M	



Hình 19 Kết quả tìm được

Thử nghiệm câu lệnh tại www.exploit-db.com/ghdb/6322 để tìm các khóa SSH.

EXPLOIT
DATABASE

intitle:"index of" "id_rsa.pub"

GHDB-
ID:
6322

Author:
SID JOSHI

Published: 2020-06-22

Google Dork Description:
intitle:"index of" "id_rsa.pub"

Google Search: intitle:"index of" "id_rsa.pub"

←

Command Prompt

Microsoft Windows [Version 10.0.26100.3775]
(c) Microsoft Corporation. All rights reserved.

C:\Users\doduy>date
The current date is: 12/04/2025
Enter the new date: (dd-mm-yy)

C:\Users\doduy>echo DoDuyNam_B22DCAT199
DoDuyNam_B22DCAT199

C:\Users\doduy>

→

Dork: intitle:"index of" "id_rsa.pub"

Author: Sid Joshi

Result of this dork

POC in attachment

Thanks!

Hình 20 Thông tin liên quan tới ví dụ

19

```

-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,12E5E0B1787119B9C04F5CD350C0369E

wLoNn3hYdZvguD1mnLTi+izJWw9tWORY7tX34JqVqUgJ0g8UyWv8t2nkEcsvI6Q0
XY64jJ9gVCwXCE+jJlLG0ClPfQ3kQel+5ETqYstvxhxZDrN+mrikLraGG3nFxHIA
71gL45HT+B/shGQcpXAZf0Qgve7MHY4ndN1n10EDGEJoxZ5ZXa/F5V5+uQ05jYmK
uMeDi6h6yga0F9zLn7uu1mKF6LhvkigkSG7nXe2KkecwTs/pXxVaffckPXH7fVvy
T79I3QS40LaMt375sKGUOEXSxb1iSAd9bTSM45MSg3GB/16AYnc2fSeIsSu24NCe
5eTdGkZGdLZhFmF8ZaoijYisxRlvRwPrYno+VZ5GhoevLwnkdGJ4jH96iqpiQYA
KREEEH9WSoG+u6SMkiJ06TFa7MiakHMS+buRtKQb2VTEcc613sXsLXw9cGd4Q4Cz
gs/VXQXIbY1/vNT8mYQLDXvtJ5KDj7VNqqpQweOvxN0CPkRLc02eLl81W+uI0sia
wgIoPrMdDY24FEcFv21HKUloxLP1gzVarhaaXxmyTfUZ6HW2Pqe27tXvXi++cLYy
egfwz0DIDRCCZ/PuQR5uqHYmC9nr3UBlj4rniuBYn9o1wlgEtrSVKmioc537qfcc
VjuEy5eh0JxRjkyDsMCh/MaCcu8dud7AB2MdNaqpTDGLtCgZHVDMZJ6K7XY+Ljsz
m4MSB6NoNo9VjTdhwaTNIa3s49njTH+1wrRHVX8jFFjPpL1zS91tBosVRwZagSc0
s2zcHjAh7UIhg4Imh375YU7rXgp9iHjvF18QdXt1IIq+jV/WaSzD3VvV3Et6tnc
17o9SCcrLJ1QvjEYnjAa/6gHGKugdaJREIfXclUT+7bt91U1IUU670052eSLzSfk
PMgTLuEYiTG93Pdfm51H5jCdX2mgh9TZY1q64NqQYpF0eZRzSvz1snFsx13FDmgA
4D92c9q+MD02C4PpQy4P+nJa2REzI+NaI8jjB0CLhZzYaUVQ2mAqwEz3DcHRDaIX
IpHtzEQA4jEVQ/ELCmp3pUjc7+K+GouPU2cD8UVhFfsOoNP300dtshIXmIT7nCTQ
9bNk87kd0c5FSd2qeAot5dCZBRhTqPOdG+cU8jPFiraybjr9S/nb7GLw6cYM8kkF
7Ihnp5nm2o0g6t2LCThrGdLx8D2LDY7v19wxfaMi9kYBKbt40G0eBfWQHUCvgw2S
qK3j3098Qamfd6gFAL7Qy3AO/32+NQ1tQJ9/ktqebj/ZcwbVLo+3UUCjVJtWmpOg
NDqjtSRjzjYDc8ldlrIXF9mpytTjQXYaPZLJBQuzgG8c11+G58CwbVoHDkkoIiXW
rNE89RrnX2CREHf1K/uewz9CeLzzYr9h1xvyVP0tYSsOS722A4x2DwYSMvyxVJC7
2YXmt6ePAhs+cgs2AXBTeVEGnuZrKt0QvBLAX2LsLLxHzoEz3dw84gXQXxu61C0v
rTIwVAQEJfCmClgkT807zuwq8onVGdEzXZR1Qo2P9f9ST42ZU65Jmdyanb1X8D1
I48IHdRUCVo/YM6hmXoWfNu49wHvVew9hpDsmHAXjkGJKzM3hUuZ8XRm1Kx9cp
-----END RSA PRIVATE KEY-----

```

```

Microsoft Windows [Version 10.0.26100.3775]
(c) Microsoft Corporation. All rights reserved.

C:\Users\doduy>date
The current date is: 12/04/2025
Enter the new date: (dd-mm-yy)

C:\Users\doduy>echo DoDuyNam_B22DCAT199
DoDuyNam_B22DCAT199

C:\Users\doduy>

```

Hình 21 Kết quả tìm được

- Thử nghiệm www.exploit-db.com/ghdb/6412 tìm log có tên người dùng và mật khẩu, có thể có các mục khác như địa chỉ e-mail, URL mà những thông tin đăng nhập này được sử dụng, v.v.

allintext:username,password filetype:log

**GHDB-
ID:**

6412

Author:

ISA GHOJARIA

Published: 2020-07-16

Google Dork Description:

allintext:username,password filetype:log

Google Search: allintext:username,password filetype:log



allintext:username,pa

```
Command Prompt
Microsoft Windows [Version 10.0.26100.3775]
(c) Microsoft Corporation. All rights reserved.

C:\Users\doduy>date
The current date is: 12/04/2025
Enter the new date: (dd-mm-yy)

C:\Users\doduy>echo DoDuyNam_B22DCAT199
DoDuyNam_B22DCAT199

C:\Users\doduy>
```



Databases ▾

Hình 22 Thông tin liên quan tới ví dụ

Free accounts to username.log

100%	Login	<script>alert('xss')</script>		
	Password	<script>alert('xss')</script>		

Votes: 10

95%	Login	01609503489		
	Password	764112		

Votes: 20

90%	Login	admin		
	Password	<script>alert('xss')</script>		

Votes: 30

88%	Login	deepak		
	Password	321		

Votes: 106

87%	Login	Trish10mae		
	Password	Chey2210		

Votes: 39

87%	Login	Usman		
	Password	1234567		

Command Prompt

Microsoft Windows [Version 10.0.26100.3775]
(c) Microsoft Corporation. All rights reserved.

C:\Users\doduy>date
The current date is: 12/04/2025
Enter the new date: (dd-mm-yy)

C:\Users\doduy>echo DoDuyNam_B22DCAT199
DoDuyNam_B22DCAT199

C:\Users\doduy>

Hình 23 Kết quả tìm được

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).

Google Hacking Database

Show 15

Date Added	Dork	Category	Author
2024-07-04	intext:"proftpd.conf" "index of"	Files Containing Juicy Info	Fernando Mengali
2021-11-11	site:in .com .net intitle:"index of" ftp	Files Containing Juicy Info	Krishna Agarwal
2021-11-08	intitle:"index of" "*/ftp.txt"	Files Containing Juicy Info	Vivek Pancholi
2021-11-05	intext:"index of" "ftp"	Files Containing Juicy Info	Onkar Deshmukh
2021-11-03	intitle:"index of" "ftp.riken"	Files Containing Juicy Info	Muhammad Al-Amin
2021-11-01	inurl:WS_FTPlog	Files Containing Juicy Info	Suram CyberSec
2021-10-29	intitle-index of /cftp /robots.txt	Files Containing Juicy Info	Jawhar milan
2021-10-05	intitle:"index of" "sftp.json"	Files Containing Juicy Info	Suman Das
2021-09-21	intitle:"index of ftp passwords"	Files Containing Passwords	Romell Marin Cordoba
2021-09-14	inurl:/ftp intitle:"office"	Web Server Detection	Lawrence March
2021-07-02	inurl:/web-ftp.cgi	Pages Containing Login Portals	Alexandros Pappas
2021-04-19	intitle:"index of" ws_ftp.ini	Files Containing Juicy Info	Aman Srivastav
2021-03-16	inurl:ftp-inurl:(http https) intext:"@gmail.com" intext:subject fwd confidential important CARD cvv	Files Containing Juicy Info	Algo
2021-01-05	site:ftp.*.*.* "ComputerName=" + "Unattended" UnattendedMode	Files Containing Juicy Info	Alexandros Pappas
2020-10-26	site:sftp.*.*.* intext:"login" intitle:"server login"	Pages Containing Login Portals	Alexandros Pappas

Showing 1 to 15 of 89 entries (filtered from 7,944 total entries)

Command Prompt

Microsoft Windows [Version 10.0.26100.3775]
(c) Microsoft Corporation. All rights reserved.

C:\Users\doduy>date
The current date is: 12/04/2025
Enter the new date: (dd-mm-yy)

C:\Users\doduy>echo DoDuyNam_B22DCAT199
DoDuyNam_B22DCAT199

C:\Users\doduy>

Filters

Reset All

Quick Search

FTP

Databases

Exploits

Links

Search Exploit-DB

Sites

OffSec

Solutions

Courses and Certifications

Hình 24 Các Google dorks liên quan đến giao thức truyền tệp FTP

- Chọn 5 Google dork, mỗi loại thuộc một danh mục khác nhau.

+*Google Dork: intext:"proftpd.conf" "index of"* dùng để tìm kiếm các file cấu hình ProFTPD đang được công khai trên internet.

```

ServerName                "FTP"
ServerIdent                on "FTP Server ready."
ServerAdmin               root@localhost
DefaultServer              on
VRootEngine                on
DefaultRoot                ~ !adm
AuthPAMConfig              proftpd
AuthOrder                  mod_auth_pam.c* mod_auth_unix.c
UseReverseDNS              off
User                       nobody
Group                      nobody
MaxInstances               20
UseSendfile                off
LogFormat                  default "%h %l %u %t \"%r\" %s %b"
LogFormat                  auth      "%v [%P] %h %t \"%r\" %s"
ListOptions                -a
RequireValidShell          off
PassivePorts               12000 12100

<Global>
  Umask                     002
  IdentLookups              off
  AllowOverwrite            yes
  <Limit ALL SITE_CHMOD>
    AllowAll
  </Limit>
</Global>

```

```

Microsoft Windows [Version 10.0.26100.3775]
(c) Microsoft Corporation. All rights reserved.

C:\Users\doduy>date
The current date is: 12/04/2025
Enter the new date: (dd-mm-yy)

C:\Users\doduy>echo DoDuyNam_B22DCAT199
DoDuyNam_B22DCAT199

































C:\Users\doduy>

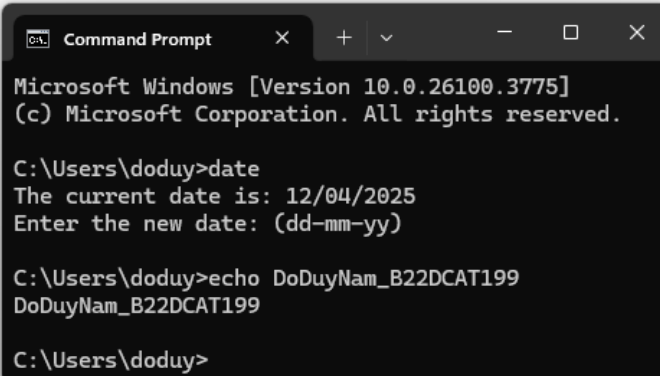
```

Hình 25 Kết quả tìm được

+ *Google Dork: site:.in / .com / .net intitle:"index of" ftp* dùng để tìm các thư mục FTP hoặc file liên quan đến FTP (như file cấu hình, nhật ký, tài liệu...) được lộ ra công khai trên web.

Index of /ubuntu/dists

Name	Last modified	Size
 Parent Directory		-
 bionic-backports/	2025-04-08 03:35	-
 bionic-proposed/	2025-04-11 01:12	-
 bionic-security/	2025-04-08 03:33	-
 bionic-updates/	2025-04-08 03:35	-
 bionic/	2018-04-26 23:38	-
 devel-backports/	2025-04-08 03:16	-
 devel-proposed/	2025-04-12 11:51	-
 devel-security/	2025-04-08 03:16	-
 devel-updates/	2025-04-08 03:16	-
 devel/	2025-04-12 11:51	-
 focal-backports/	2025-04-08 03:31	-
 focal-proposed/	2025-04-11 18:04	-
 focal-security/	2025-04-10 21:09	-
 focal-updates/	2025-04-12 11:59	-
 focal/	2020-04-23 17:34	-
 jammy-backports/	2025-04-08 03:24	-
 jammy-proposed/	2025-04-12 11:56	-
 jammy-security/	2025-04-12 11:54	-
 jammy-updates/	2025-04-12 11:56	-
 jammy/	2022-04-21 17:16	-
 noble-backports/	2025-04-08 03:19	-
 noble-proposed/	2025-04-12 11:52	-
 noble-security/	2025-04-11 17:55	-
 noble-updates/	2025-04-12 11:52	-
 noble/	2024-04-25 15:11	-
 oracular-backports/	2025-04-08 03:17	-
 oracular-proposed/	2025-04-12 11:51	-
 oracular-security/	2025-04-11 17:54	-
 oracular-updates/	2025-04-11 17:54	-
 oracular/	2024-10-11 10:22	-
 plucky-backports/	2025-04-08 03:16	-



```

Microsoft Windows [Version 10.0.26100.3775]
(c) Microsoft Corporation. All rights reserved.

C:\Users\doduy>date
The current date is: 12/04/2025
Enter the new date: (dd-mm-yy)

C:\Users\doduy>echo DoDuyNam_B22DCAT199
DoDuyNam_B22DCAT199

C:\Users\doduy>
  
```

Hình 26 Kết quả tìm được

+Google Dork: `intitle:"index of" "*/ftp.txt"` dùng để tìm file cụ thể có tên ftp.txt được lưu trữ trong thư mục web cho phép liệt kê (directory listing).

Copyright 1992 by Urban A. LeJeune

Anonymous File Transfer Protocol (FTP)

Files may be transferred via Internet using anonymous file transfer protocol (FTP) from those institutions making files available using this method. The are called anonymous ftp because you do not need an account to transfer files from systems allowing this type of transfer. Additionally, you will always log on using "anonymous" as your identification. You password should be you full internet address, unless you are instructed otherwise.

Let us assume that an archie search has produced the following listing of an archived file at Tohoku University in Japan.

Host akiu.gw.tohoku.ac.jp (130.34.8.9)
Last updated 00:18 10 Mar 1992

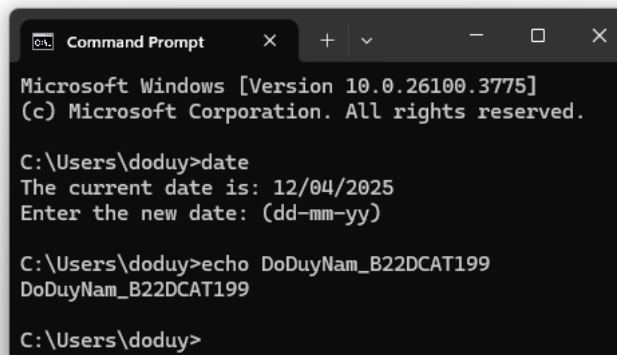
```
Location: /pub/mac  
FILE      rw-r--r--      405 Apr  4 1991  README.txt
```

The host name is the internet location location of the file. Since many locations are not recognizable by the letter listings ftping using the numbers tends to be fail-safe, although more tedious. The last update entry describes when this institution was searched for archie inclusion, not the creation date of the file. The update is rarely over thirty days old. The location is the directory path for the specified file. The file line has information about the specific file. The first group of letters related to file specifics and are of no read concern, there is information about the file such as read-only and other system information. The next group of numbers is the actual file size in bytes followed by the date when it was added to the data base. The last item is the actual file name. It is important to note that most archive data bases are stored on computers using the Unix operating system. On these machines case counts. If you see mixed case you know you are looking at a UNIX configuration. To be on the safe side always request files using the case as shown.

The following is the VAX sequence that fetched the file listed above using FTP. Remember that the "\$" is the actual VAX prompt. The parts starting with "!!!" are my added comments. The FPT prompt at the illustrated installation is "*". Other prompts, including ftp>, may be encountered. Netiquette (net etiquette) requires that you include your full internet address when ask for the password unless specifically instructed otherwise. Some systems may instruct you to enter "guest", or something else, as a password.

When issuing the get command include the full pathname. You may alternatively issue a series of change directory, cd, commands. The second parameter is the name you would like the file to have on your receiving directory. If the second parameter is omitted the file will be copied with the same name as the original file.

```
$ ftp 130.34.8.9 !!! domain from archie listing  
vax003 Wollongong FTP User Process (Version 5.2-05)
```



```
Microsoft Windows [Version 10.0.26100.3775]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\doduy>date  
The current date is: 12/04/2025  
Enter the new date: (dd-mm-yy)  
  
C:\Users\doduy>echo DoDuyNam_B22DCAT199  
DoDuyNam_B22DCAT199  
  
C:\Users\doduy>
```

Hình 27 Kết quả tìm được



















+Google Dork: `intitle:"index of" "ftp.riken` dùng để tìm các thư mục web đang công khai (directory listing) mà trong nội dung có chứa từ khóa "ftp.riken" – thường nhằm truy tìm các mirror site hoặc file được đồng bộ từ máy chủ FTP của RIKEN (một viện nghiên cứu lớn của Nhật Bản).

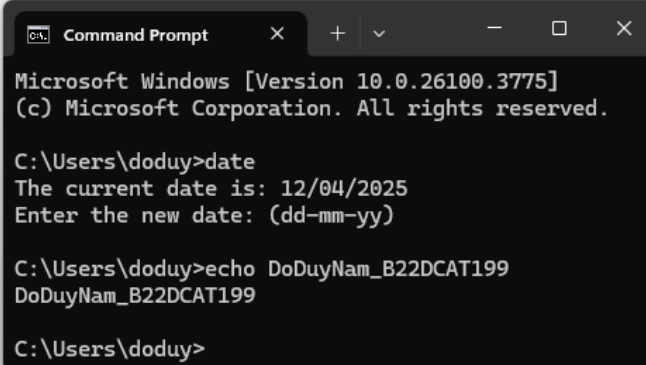
Welcome to ftp.riken.jp

ftp.riken.jp is an unsupported ftp/http/https/rsync service of RIKEN Nishina Center for research support.
Use entirely at your own risk - no warranty is expressed or implied.
Complaints and questions should be sent to ftp-adm a.t. ml.riken.jp

N.B.

- The number of simultaneous connection is limited.
- Do NOT use HTTP/FTP acceleration softwares and methods, such as the divided download (Axel etc.).
Your connections may be disconnected when you use them.
- <https://ftp.riken.jp> (TLS) in test.

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 CTAN/	2020-03-31 22:01	-	
 FreeBSD/	2025-04-12 21:16	-	
 GNU/	2025-04-12 06:12	-	
 Lecture/	2010-12-27 23:31	-	
 Linux/	2024-11-19 23:09	-	
 NetBSD/	2024-11-30 15:41	-	
 OpenBSD/	2025-04-12 14:19	-	
 X11/	2025-04-12 06:15	-	
 cernlib/	2024-05-21 16:47	-	
 iris/	2015-02-22 08:10	-	
 lang/	2008-07-07 15:26	-	
 net/	2021-07-05 14:52	-	
 office/	2019-08-14 17:10	-	
 pc/	2021-07-05 15:06	-	
 pub/	2024-11-19 01:30	-	
 sagemath/	2022-05-17 18:10	-	
 tex-archive/	2020-03-31 22:01	-	
 welcome.msg	2024-11-19 01:25	224	



```
Command Prompt
Microsoft Windows [Version 10.0.26100.3775]
(c) Microsoft Corporation. All rights reserved.

C:\Users\doduy>date
The current date is: 12/04/2025
Enter the new date: (dd-mm-yy)




C:\Users\doduy>echo DoDuyNam_B22DCAT199
DoDuyNam_B22DCAT199

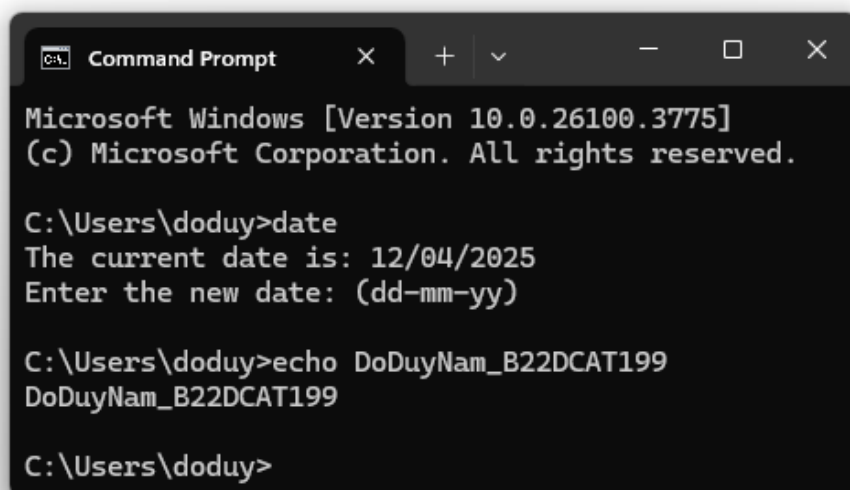
C:\Users\doduy>
```

Hình 28 Kết quả tìm được

+ Google Dork: `intitle:"index of" "sftp.json"` dùng để tìm các file có tên sftp.json được lộ ra trong các thư mục web có bật directory listing (Apache, nginx, v.v.), với tiêu đề "Index of".

Index of /.vscode

Name	Last modified	Size	Description
 Parent Directory		-	
 settings.json	2020-12-18 11:26	38	
 sftp.json	2020-12-18 11:26	254	



```
C:\> Command Prompt
Microsoft Windows [Version 10.0.26100.3775]
(c) Microsoft Corporation. All rights reserved.

C:\Users\doduy>date
The current date is: 12/04/2025
Enter the new date: (dd-mm-yy)

C:\Users\doduy>echo DoDuyNam_B22DCAT199
DoDuyNam_B22DCAT199

C:\Users\doduy>
```

Hình 29 Kết quả tìm được

2.3 Kết chương

Ở chương này đã thực hiện thành công các ví dụ tìm kiếm trong shodan để tìm kiếm các lỗ hổng, các thiết bị hay dịch vụ đồng thời cũng thực hiện thành công các ví dụ trong Google Hacking.

KẾT LUẬN

- Tìm hiểu về Shodan và Google Hacking.
- Thử nghiệm thành công các ví dụ tìm kiếm trong Shodan để tìm kiếm lỗ hổng, thiết bị và dịch vụ.
- Thử nghiệm thành công các ví dụ trong Google Hacking.

TÀI LIỆU THAM KHẢO

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