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

Môn: Thực tập cơ sở

BÀI BÁO THỰC TẬP CƠ SỞ

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

Họ và tên giảng viên:	TS.Đinh Trường Duy
Họ và tên:	Nguyễn Quốc Khánh
Mã sinh viên:	B20DCAT103
Lớp:	D20CQAT03-B
Số điện thoại:	0964137761

Hà Nội 2023

1.1 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.

1.2 Nội dung thực hành

1. Tìm hiểu lý thuyết

Tìm hiểu về shodan và google hack. Tài liệu tham khảo:

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

a. Shodan

Shodan là một công cụ tìm kiếm trên internet cho các thiết bị kết nối mạng như máy tính, camera, máy in, router, v.v. Shodan có thể cung cấp nhiều thông tin về các thiết bị này như địa chỉ IP, hệ điều hành, phiên bản phần mềm, vị trí địa lý, v.v. Shodan có thể được sử dụng cho nhiều mục đích khác nhau như nghiên cứu, giáo dục, bảo mật, phát hiện lỗ hổng, v.v. Shodan cũng có thể được sử dụng cho các mục đích xấu như tấn công, đột nhập, đánh cắp dữ liệu, v.v.

Shodan là một công cụ tìm kiếm Internet, hoạt động bằng cách quét các địa chỉ IP trên Internet và lưu trữ thông tin về các thiết bị và hệ thống được kết nối trên đó. Shodan sử dụng một loạt các công cụ và kỹ thuật để tìm kiếm các thiết bị, bao gồm:

- Scanning: Shodan sử dụng kỹ thuật quét để tìm kiếm các thiết bị và hệ thống trên mạng. Nó có thể quét các cổng mạng khác nhau để xác định các dịch vụ đang chạy trên một thiết bị cụ thể.
- Banner grabbing: Shodan sử dụng kỹ thuật banner grabbing để lấy thông tin từ các banner HTTP và các thông điệp trả về từ các dịch vụ trên một thiết bị. Các thông tin này cung cấp cho Shodan thông tin chi tiết về thiết bị và các dịch vụ đang chạy trên đó.
- Các công cụ phân tích: Shodan sử dụng các công cụ phân tích để xác định các lỗ hổng bảo mật và các thông tin khác liên quan đến các thiết bị và hệ thống trên mạng. –

Sau khi Shodan đã tìm thấy các thiết bị và hệ thống trên mạng, nó sẽ lưu trữ thông tin về chúng trong một cơ sở dữ liệu lớn và cung cấp cho người dùng truy cập

thông tin này thông qua giao diện tìm kiếm và API. Người dùng có thể tìm kiếm các thiết bị và hệ thống trên mạng bằng cách sử dụng các tiêu chí như địa chỉ IP, tên miền, dịch vụ và các thông tin khác liên quan đến các thiết bị và hệ thống trên mạng

b. Google hacking

Google Hacking là một kỹ thuật máy tính sử dụng các toán tử hoặc lệnh để lọc thông tin mà chúng ta nhận được từ công cụ tìm kiếm Google, có thể được sử dụng để tìm các lỗ hổng bảo mật trong cấu hình và mã nguồn được sử dụng trên các trang web, cũng có thể được sử dụng để thực hiện các vụ tấn công, bằng cách khai thác thông tin nhạy cảm hoặc ẩn trên mạng.

Google Hacking sử dụng các toán tử nâng cao của Google để tìm kiếm chính xác hơn và giới hạn phạm vi tìm kiếm. Google Hacking yêu cầu kiến thức cơ bản về cách hoạt động của Google và cách sử dụng các cú pháp tìm kiếm đặc biệt. 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.

Các kỹ thuật Google hacking thường bao gồm việc sử dụng các từ khóa đặc biệt để tìm kiếm các thông tin như tên đăng nhập và mật khẩu, các tập tin không được bảo mật, thông tin về hệ thống, tên miền và các thông tin khác liên quan đến các trang web và hệ thống trên mạng. Các từ khóa đặc biệt này thường được sử dụng để tìm kiếm các tài liệu nhạy cảm trên các trang web và các hệ thống trên mạng.

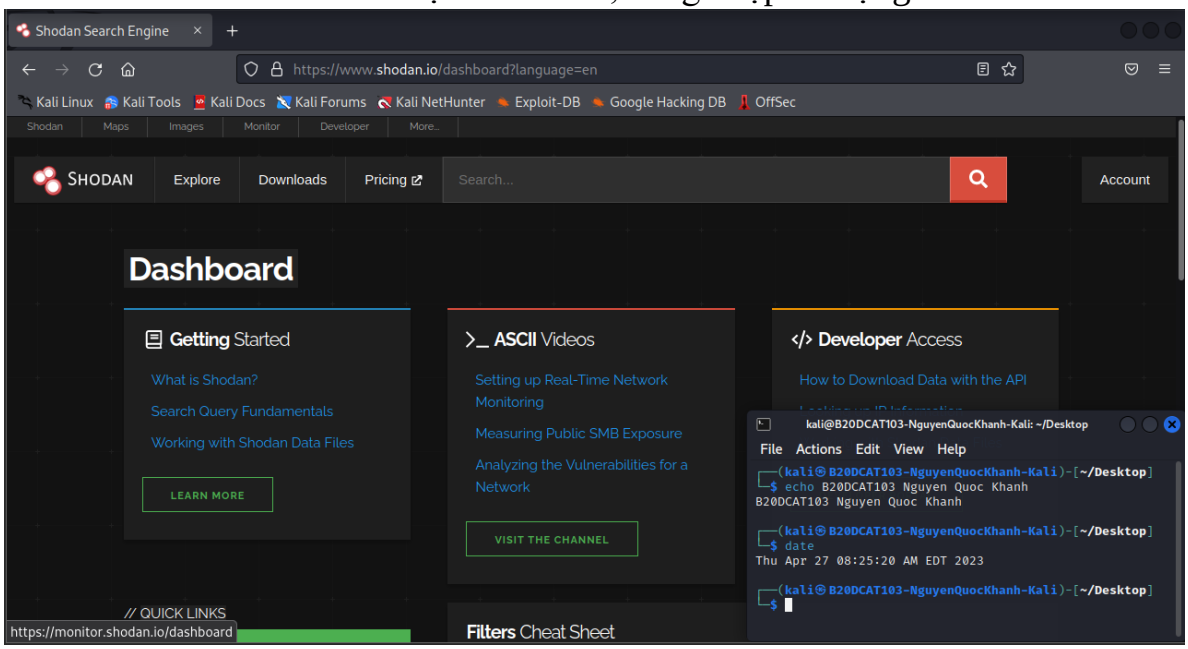
Các từ khóa đặc biệt này được sử dụng để giới hạn kết quả tìm kiếm của Google theo các tiêu chí cụ thể, ví dụ như tìm kiếm các tập tin không được bảo mật trên một trang web cụ thể, tìm kiếm thông tin về tên đăng nhập và mật khẩu, tìm kiếm thông tin về hệ thống và các thông tin khác liên quan đến các trang web và hệ thống trên mạng.

2. Thực hành

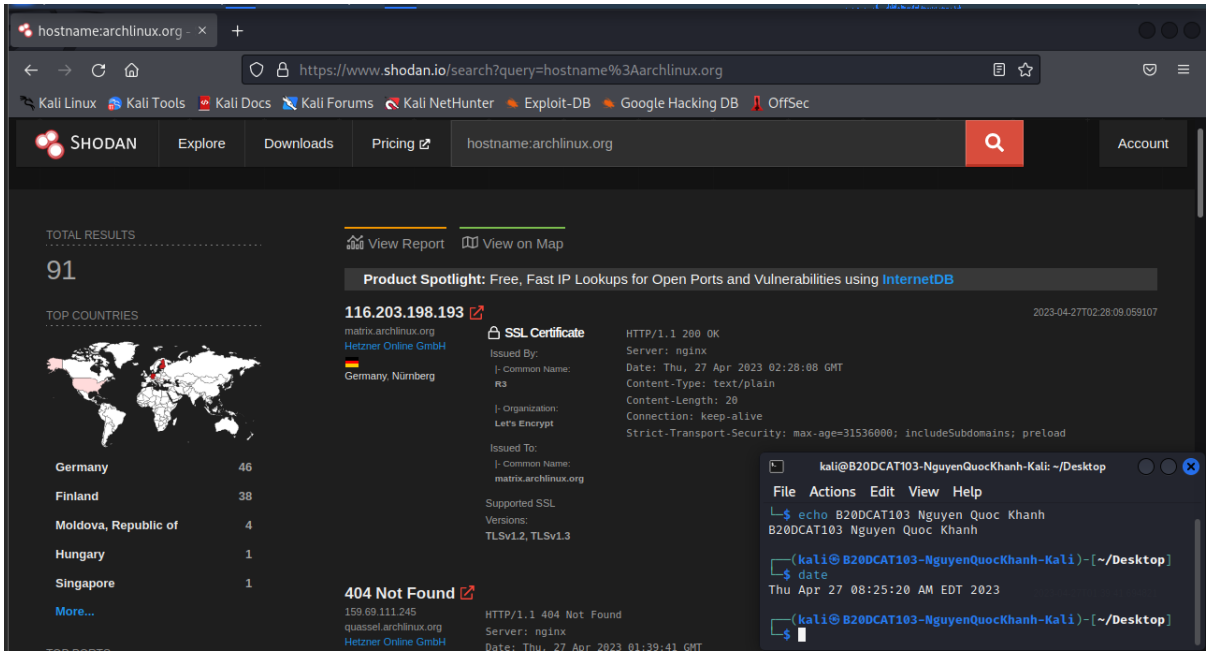
a. Thử nghiệm với Shodan

Các bước thực hiện:

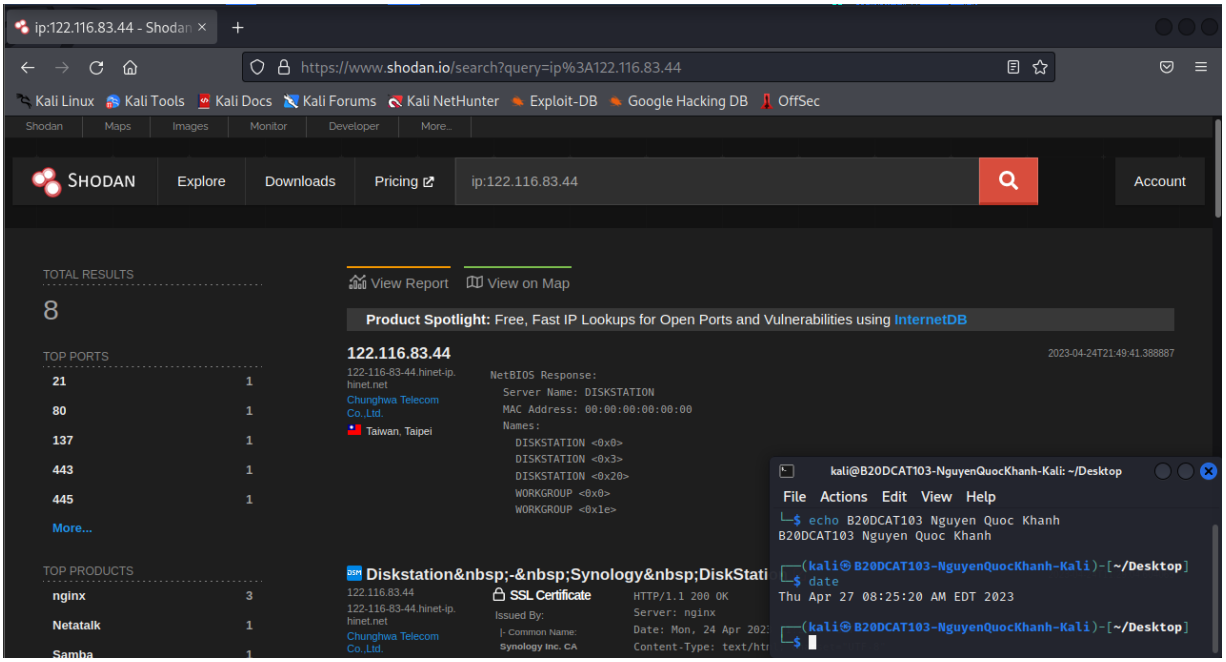
- Vào website shodan và tạo tài khoản, đăng nhập sử dụng.



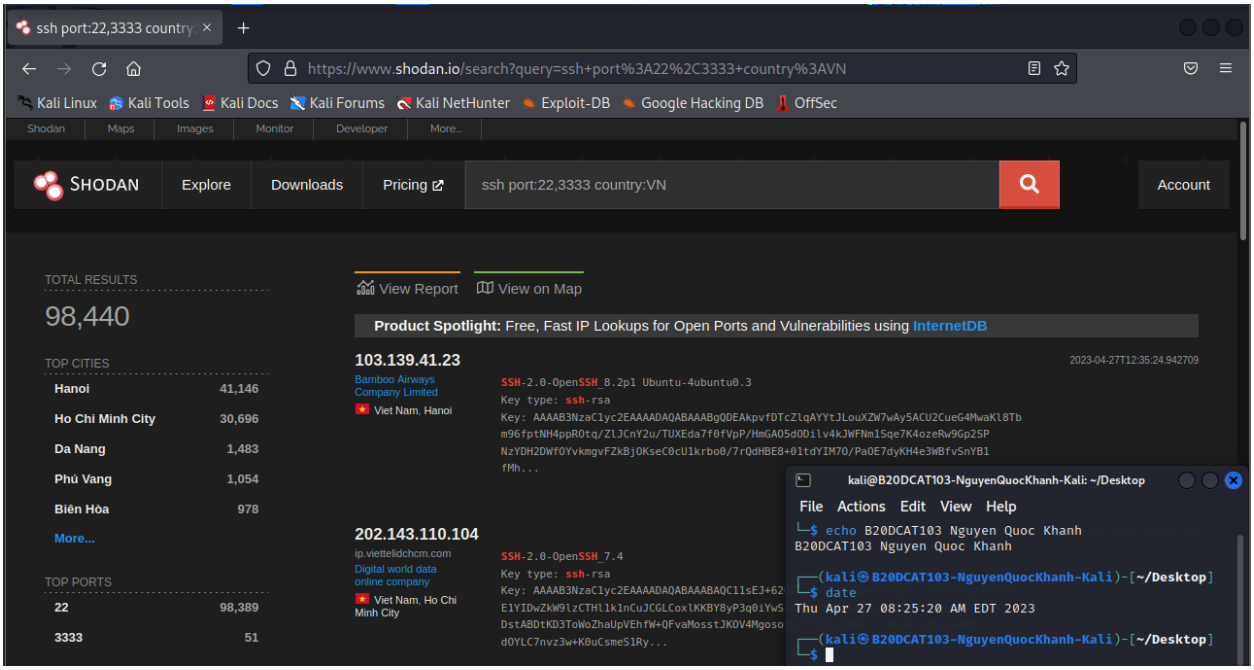
- Sử dụng shodan để tìm kiếm thông tin về trang web archlinux.org:



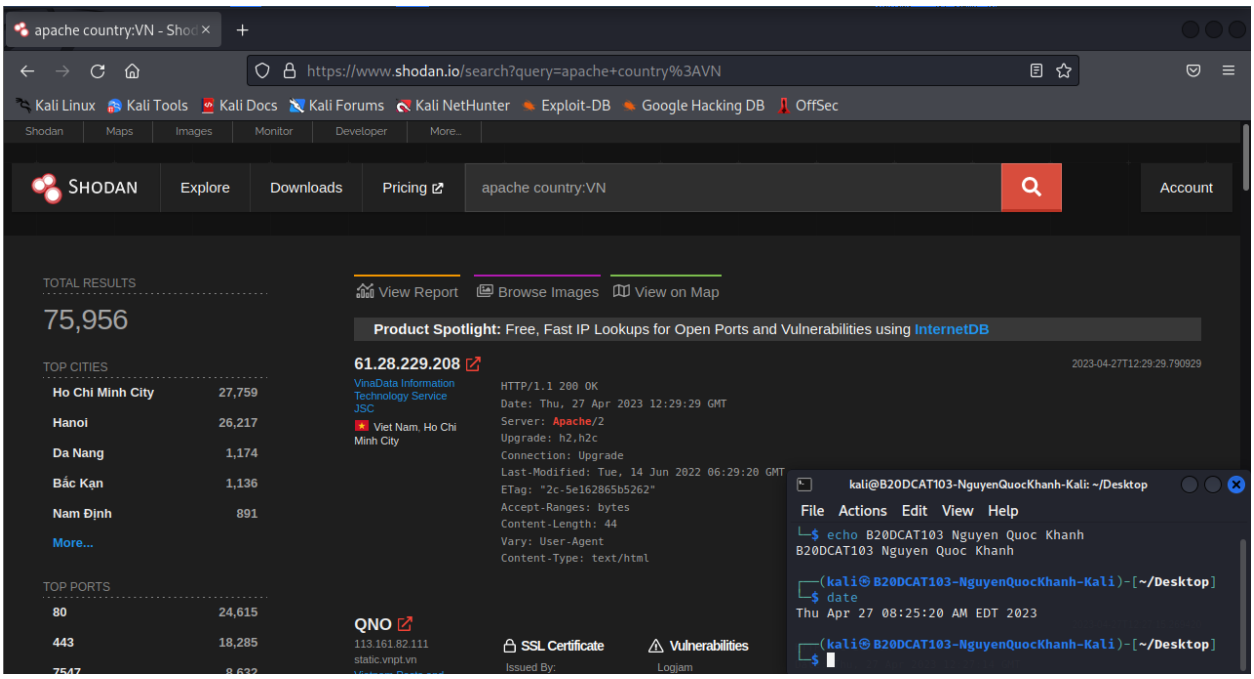
- Sử dụng shodan để tìm kiếm thông tin địa chỉ IP 122.116.83.44:



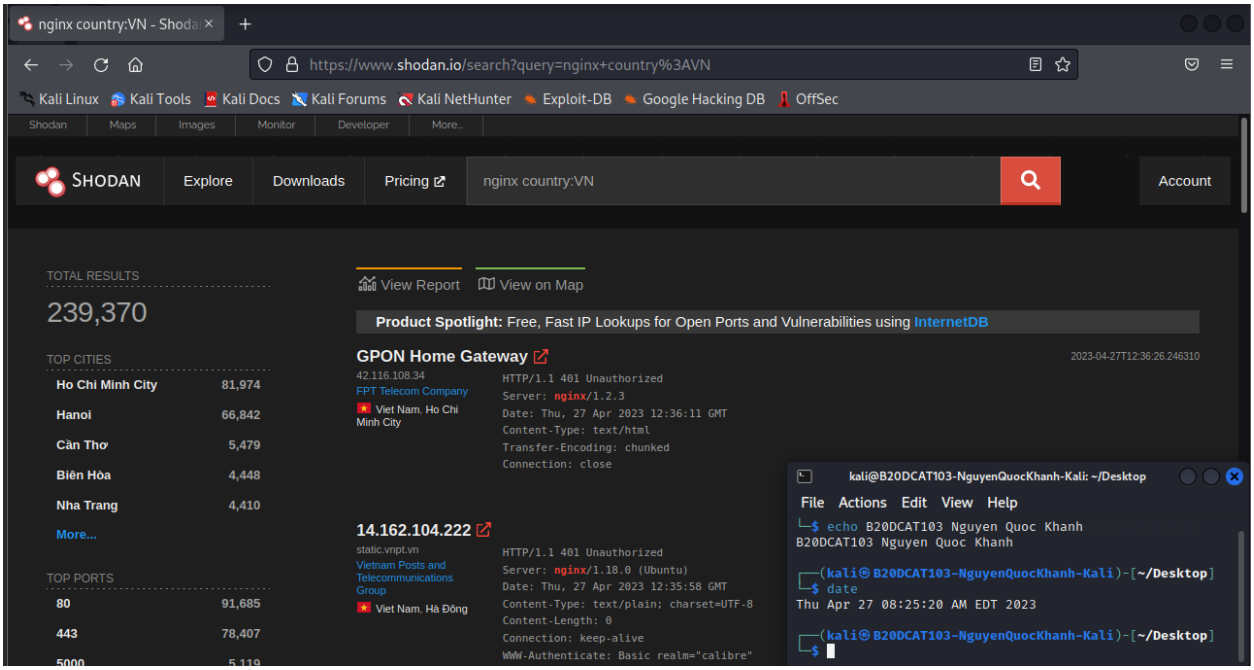
- Sử dụng shodan để tìm kiếm thông tin các dịch vụ ssh trên cổng 22 và 3333 tại Việt Nam:



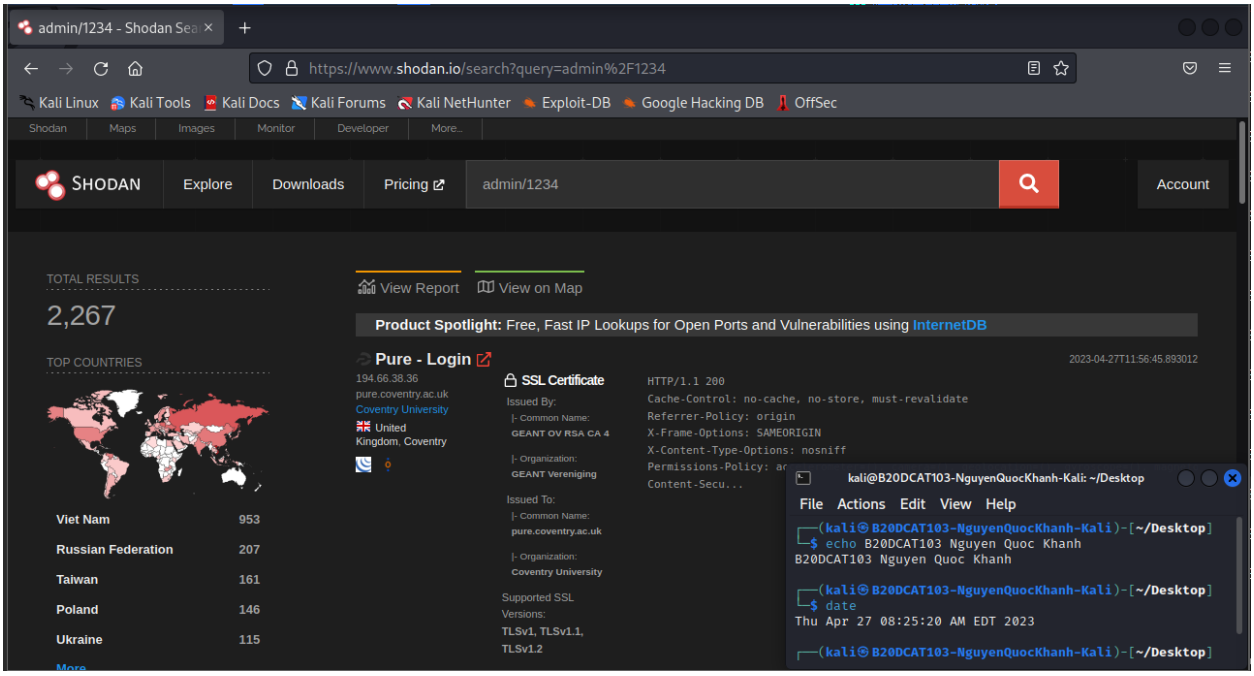
- Sử dụng shodan để tìm kiếm thông tin các máy chủ sử dụng apache tại Việt Nam:



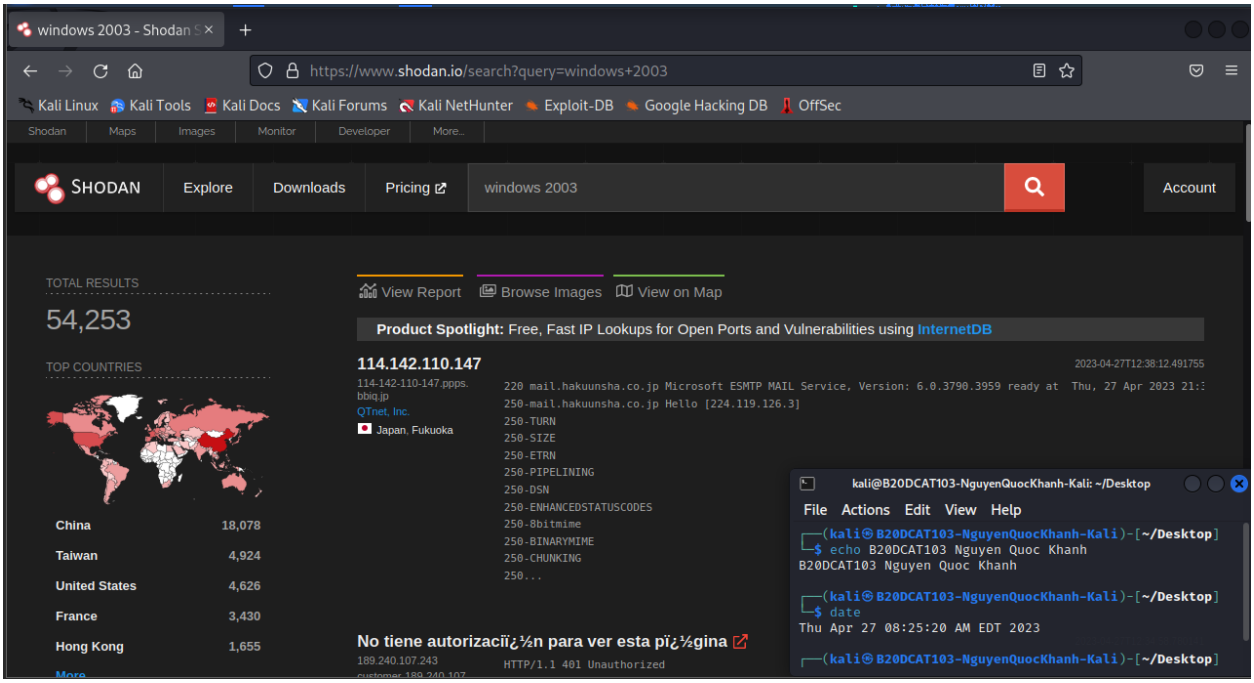
- Sử dụng shodan để tìm kiếm thông tin các máy chủ sử dụng nginx tại Việt Nam:



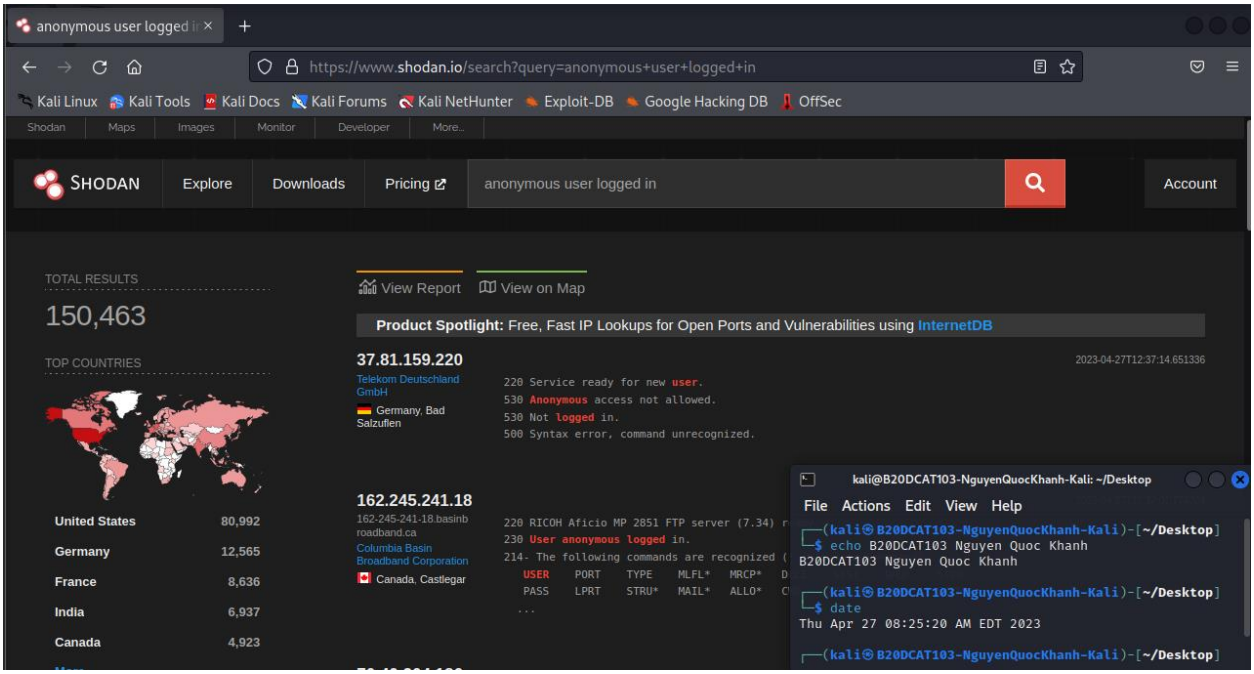
- Sử dụng shodan để tìm kiếm thông tin các máy có thành phần sử dụng tên người dùng là admin và mật khẩu mặc định 1234:



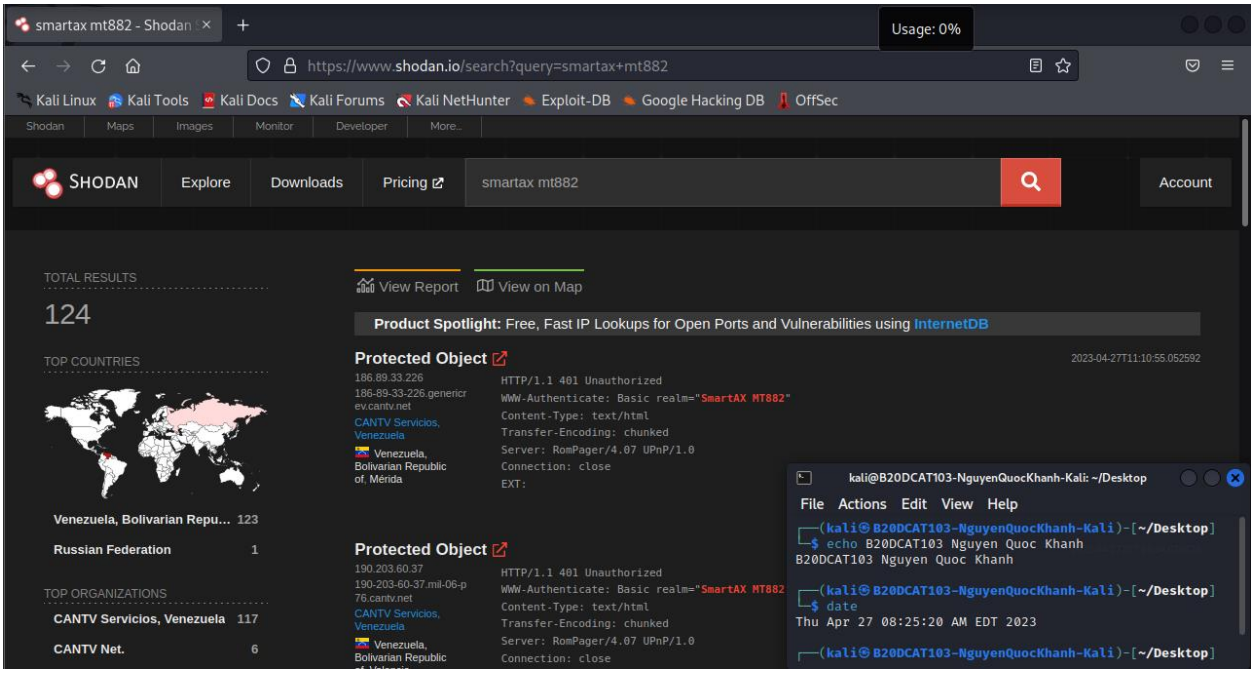
- Sử dụng shodan để tìm kiếm thông tin các máy chủ có hệ điều hành Windows 2003:



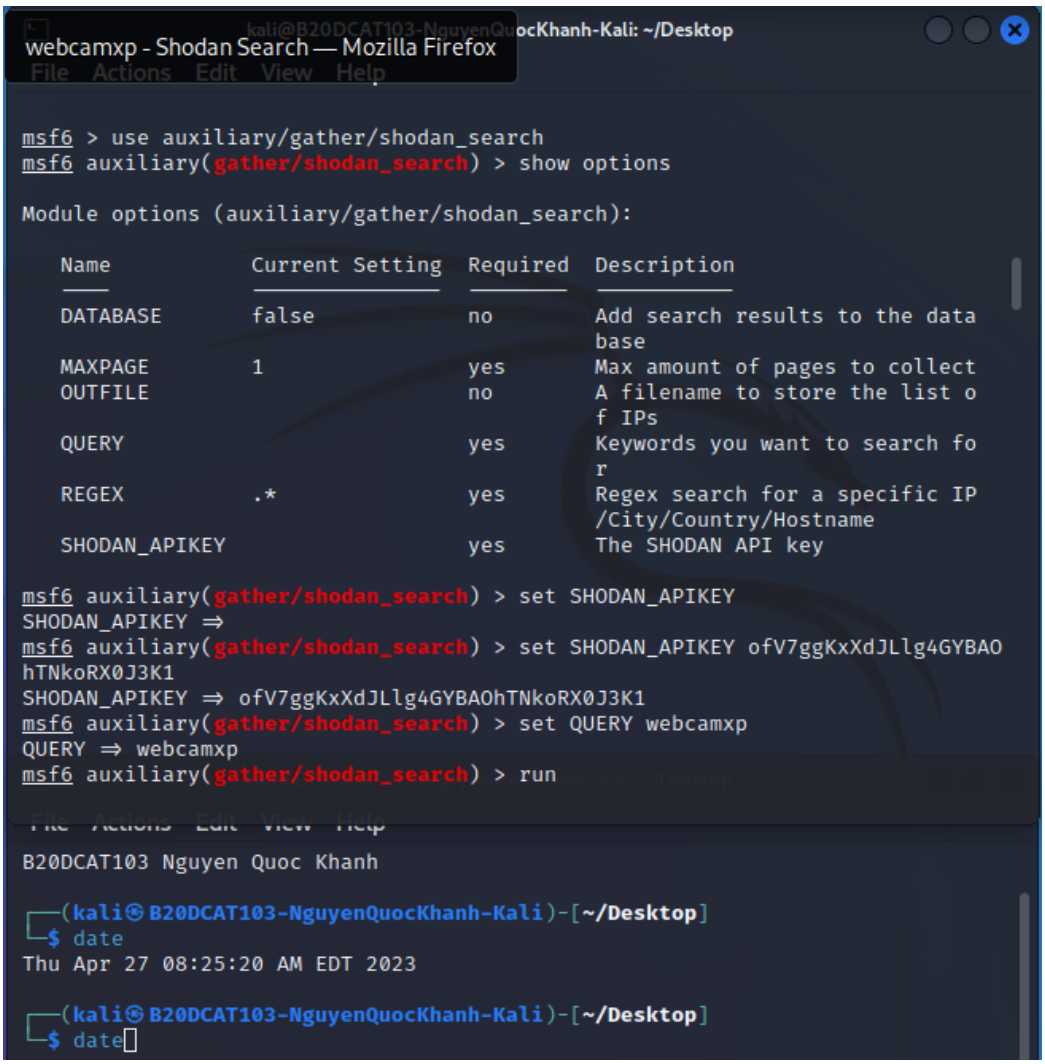
- Sử dụng shodan để tìm kiếm thông tin các dịch vụ FTP cho phép mọi người dùng có thể đăng nhập:

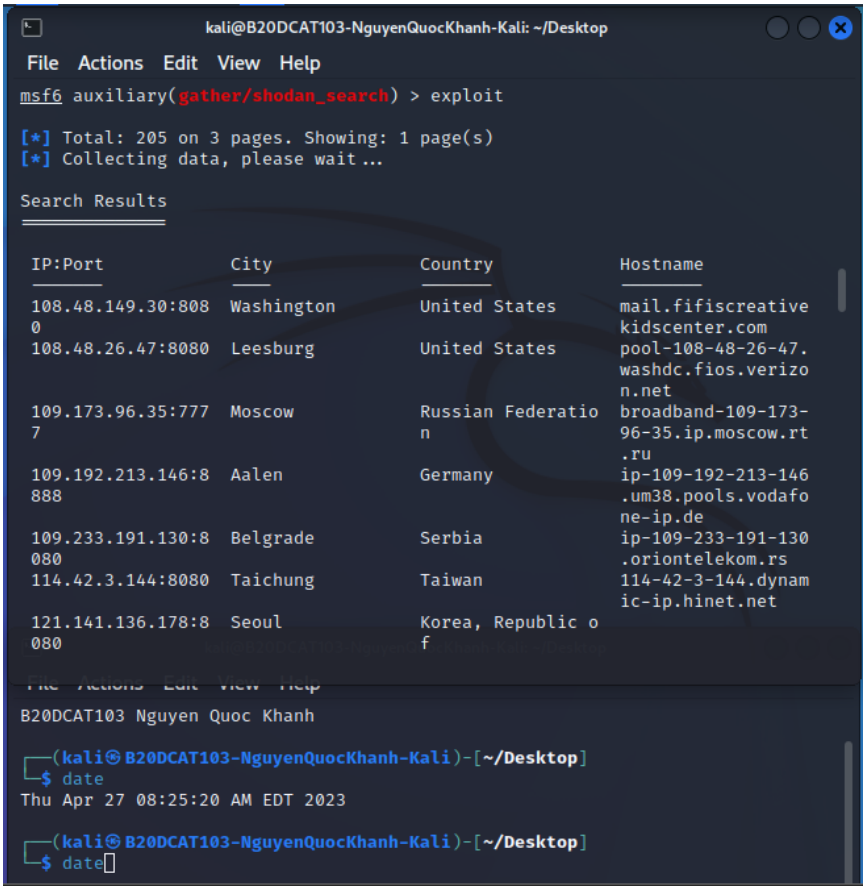


- Sử dụng shodan để tìm kiếm thông tin các máy sử dụng router số hiệu SmartAX MT882:



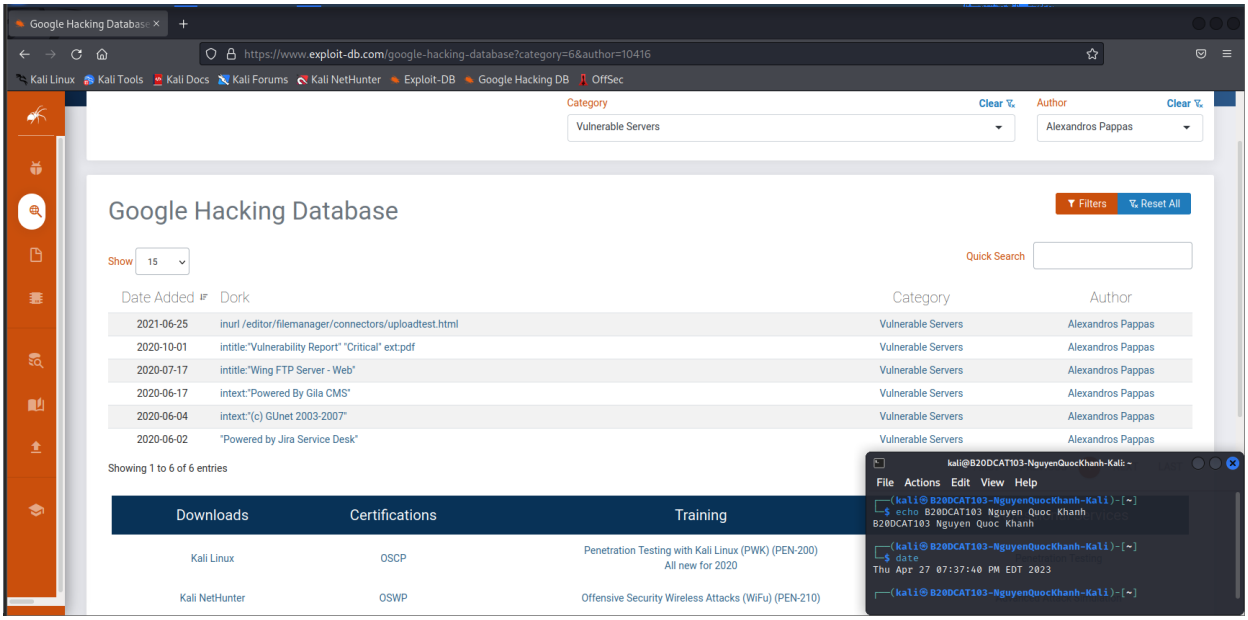
- Sử dụng shodan từ Metasploit Framework để tìm kiếm thông tin các máy sử dụng phần mềm webcamxp:



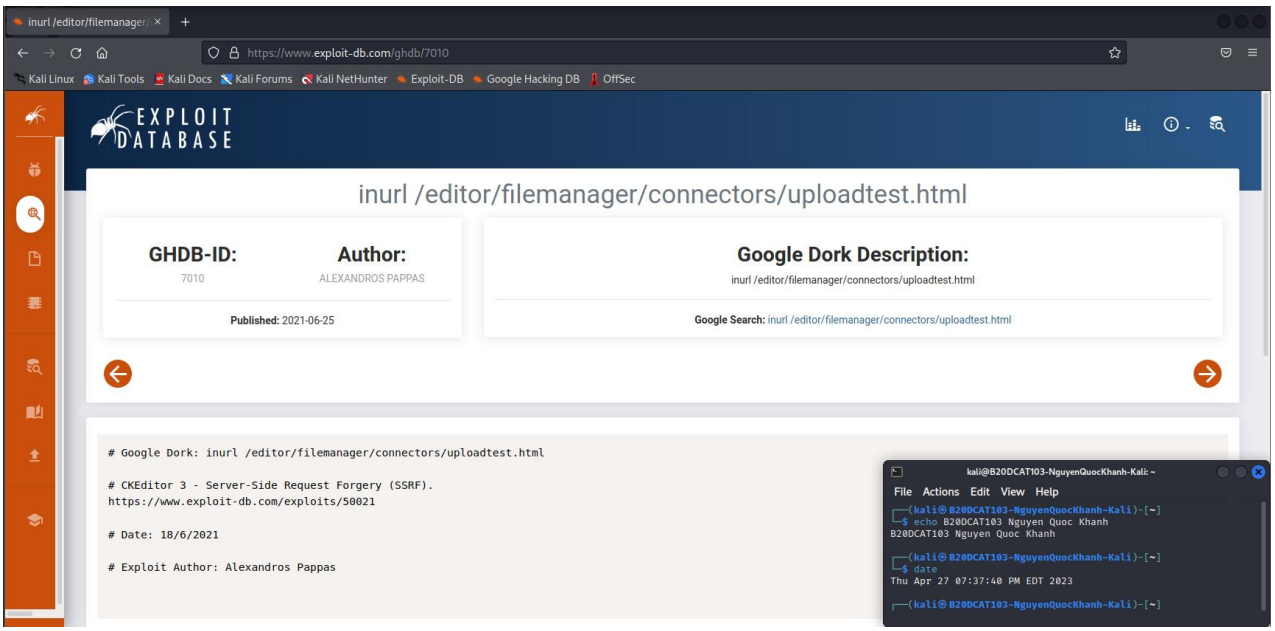


b. Thử nghiệm với Google Hacking

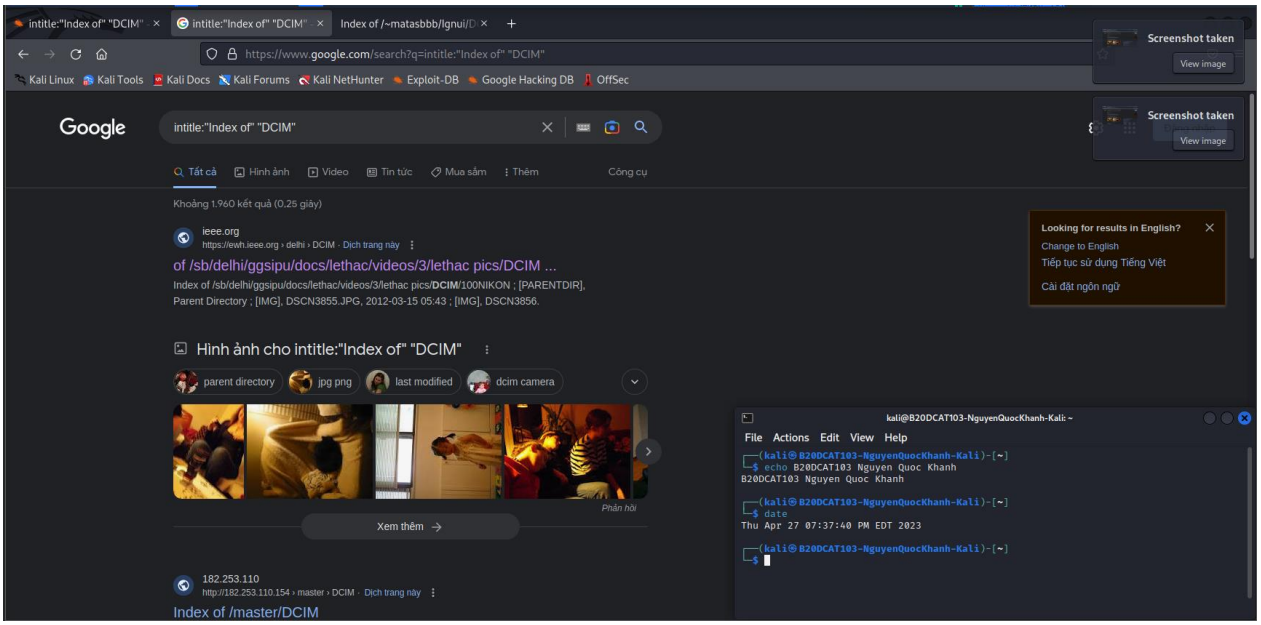
- Vào website www.exploit-db.com/google-hacking-database, sử dụng Filters



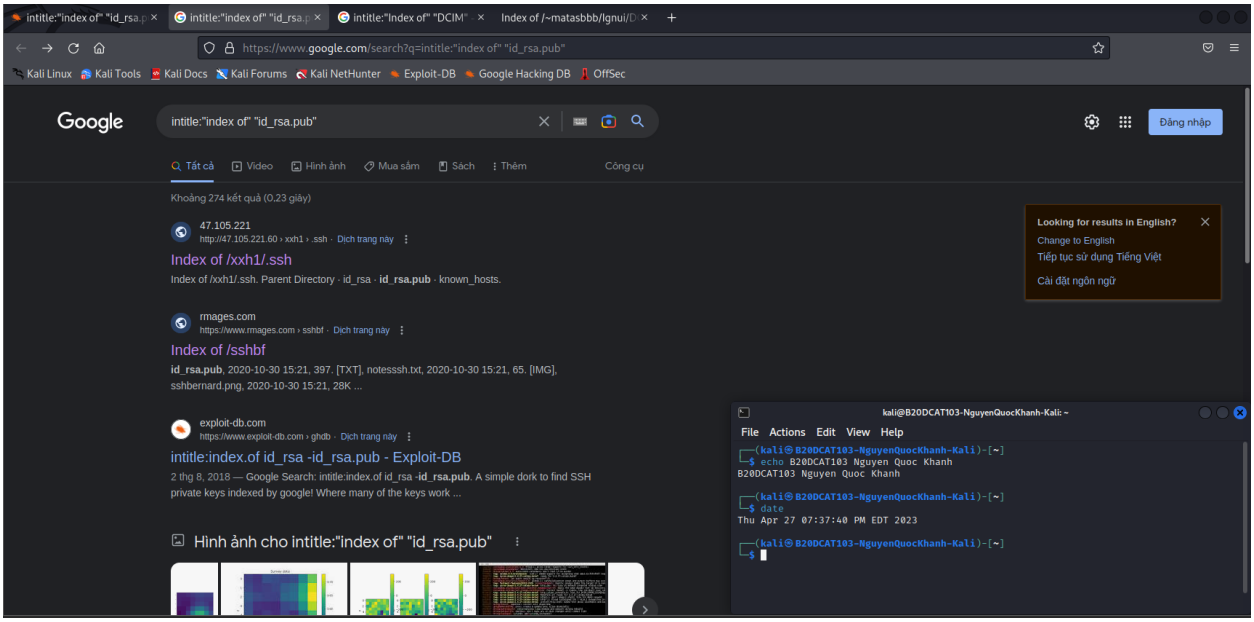
- Chọn một mục để hiện ra trang thông tin có liên quan bao gồm thông tin tác giả, mô tả về tìm kiếm và các thông tin khác:

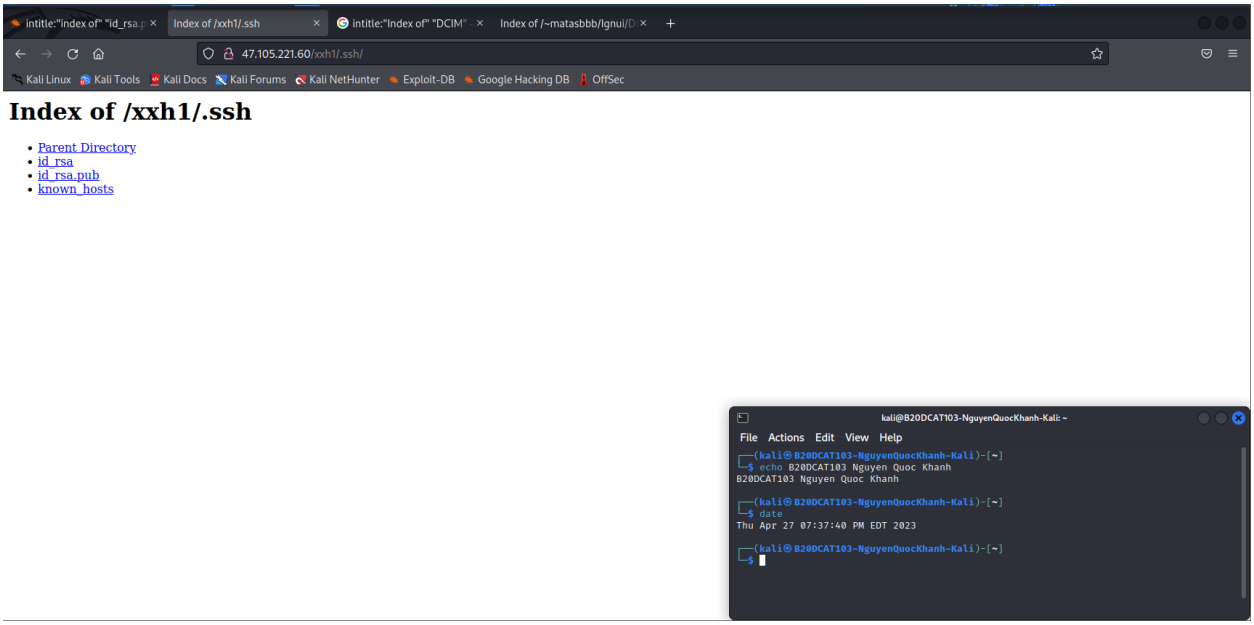


- Thử nghiệm với ví dụ tại http://www.exploit-db.com/ghdb/4057, trong đó từ khóa intitle tìm kiếm những từ ở trong tiêu đề của trang web, DCIM là tên thư mục thường sử dụng để lưu ảnh

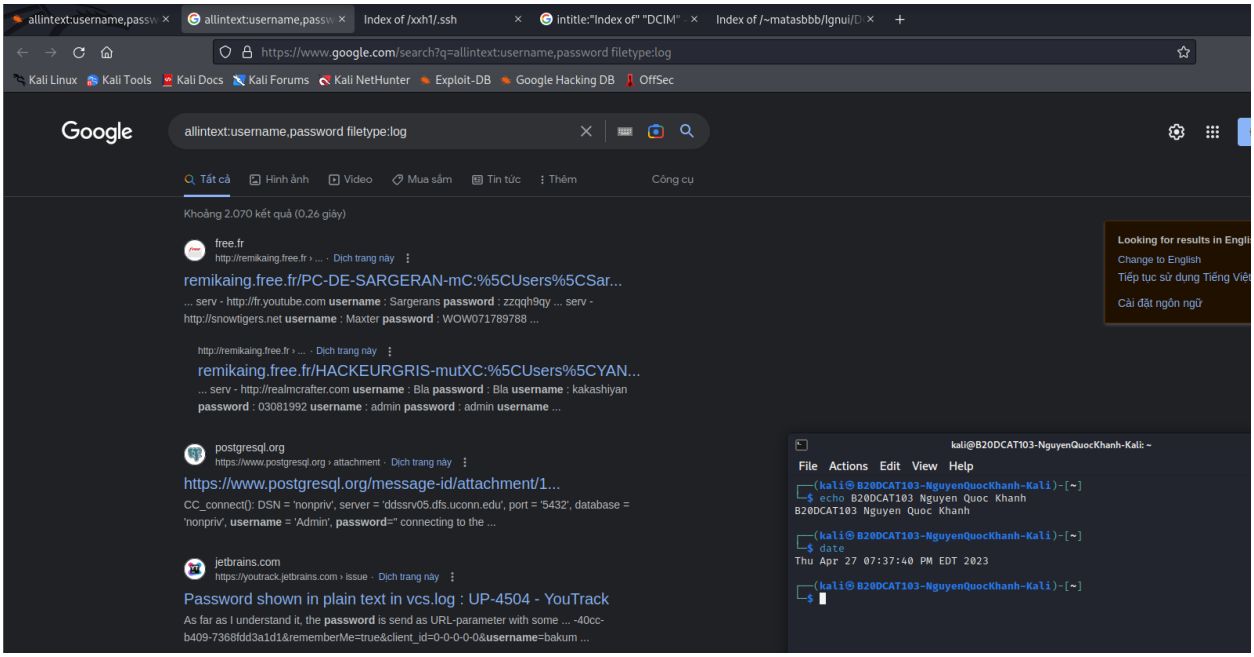


- Thử nghiệm câu lệnh tại https://www.exploit-db.com/ghdb/6322, kết quả trả về các thư mục và tập tin nhạy cảm có chứa khóa ssh:

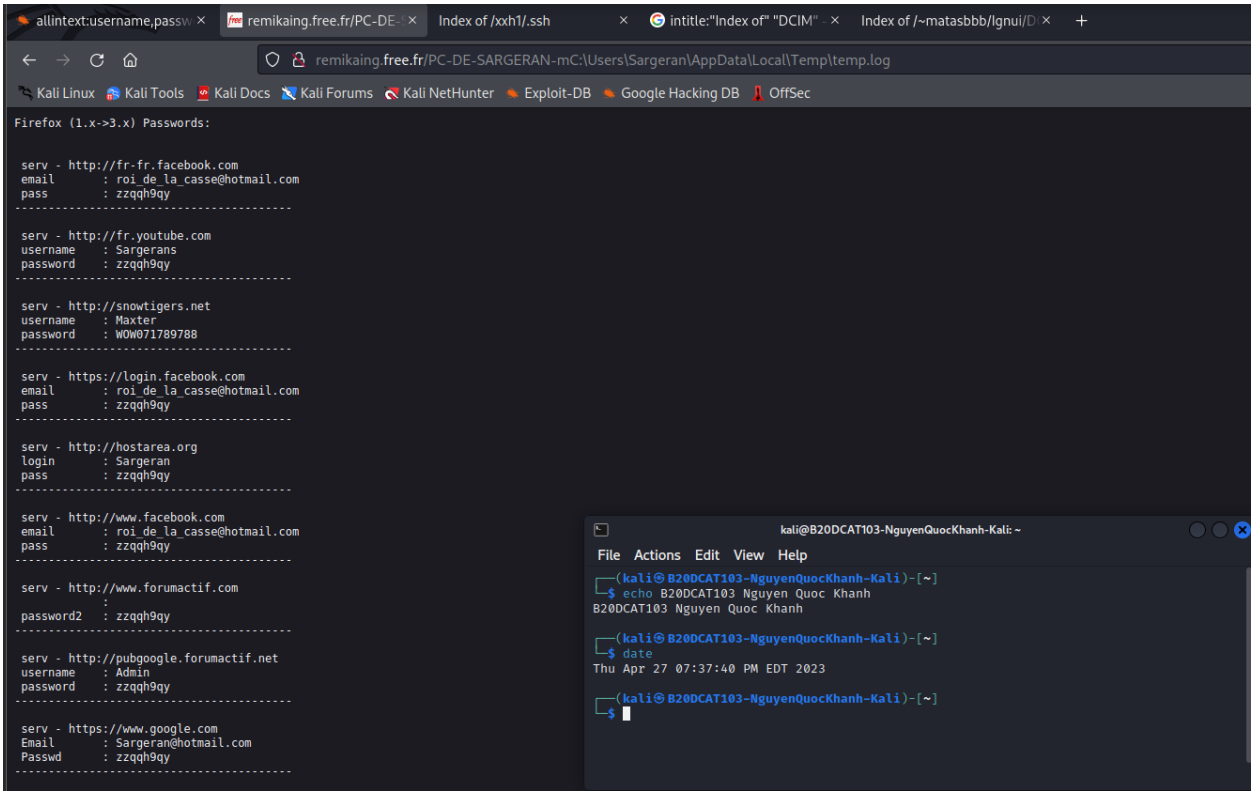




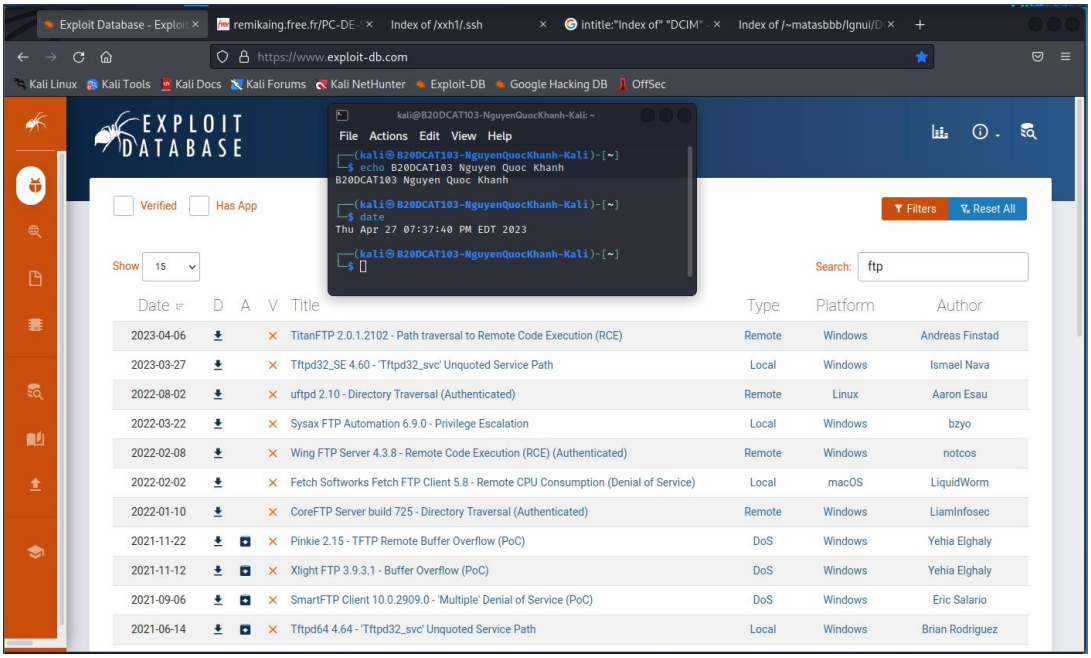
- Thử nghiệm lệnh tại www.exploit-db.com/ghdb/6412:



- Tìm được log có tên người dùng và mật khẩu:

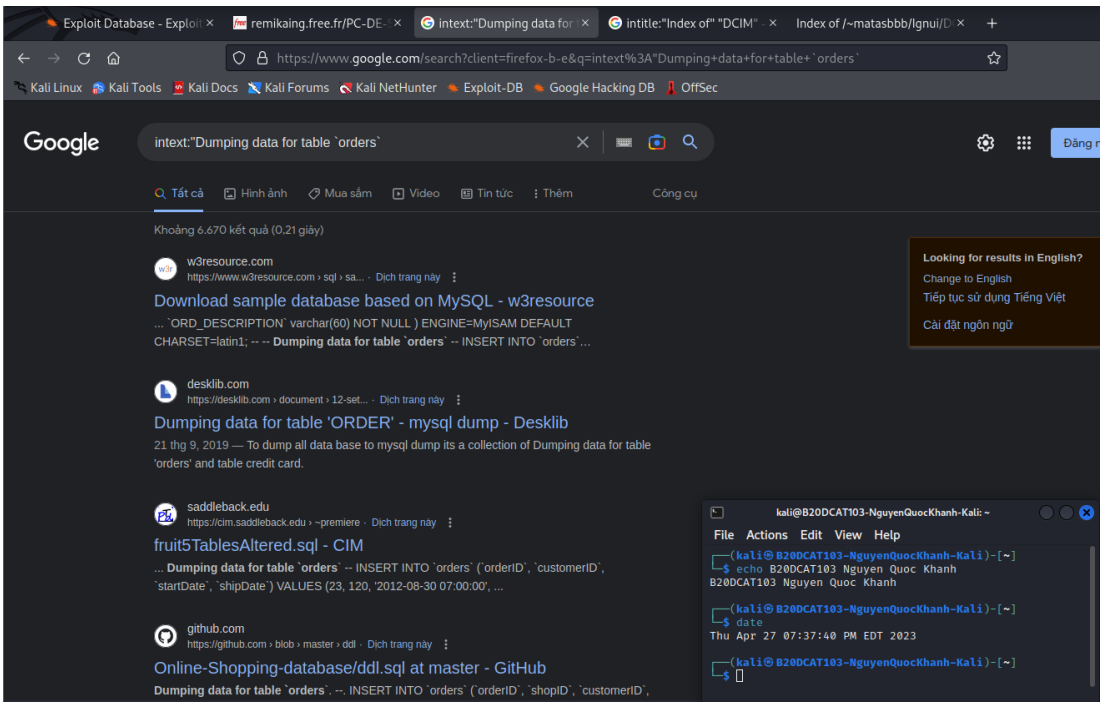


- Quay lại GHDB (www.exploit-db.com/google-hacking-database) và trong hộp văn bản Tìm kiếm nhanh ở bên phải, nhập FTP. Xuất hiện rất nhiều Google dorks liên quan đến Giao thức truyền tệp (FTP):

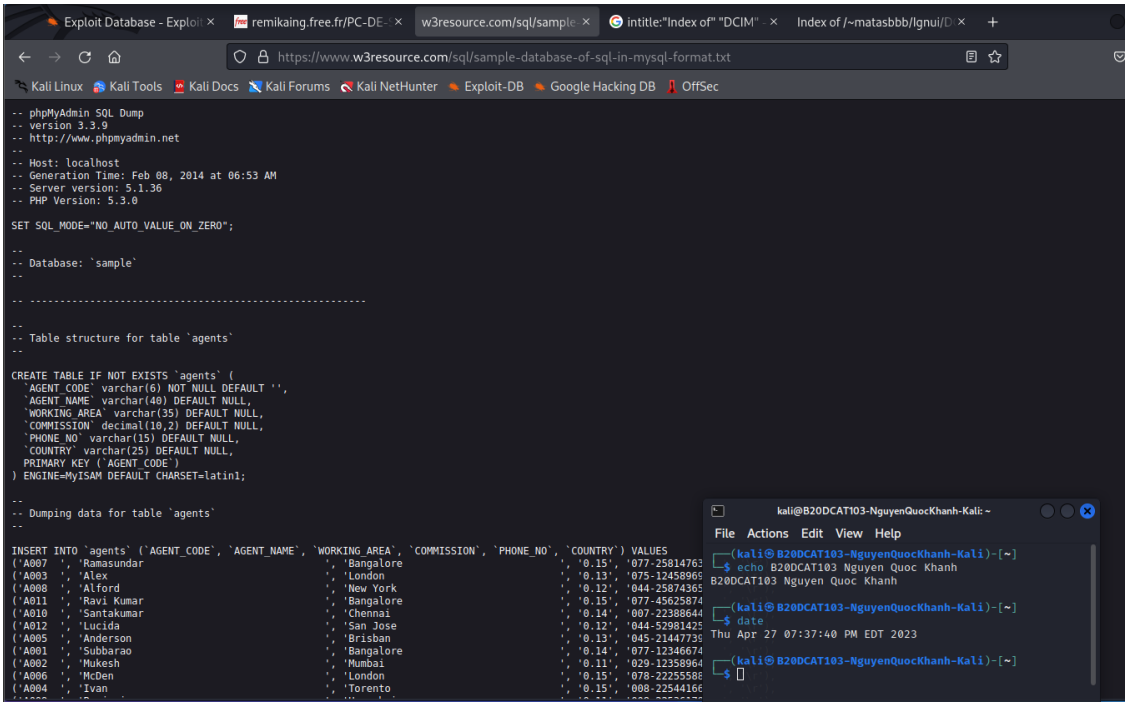


Thực hành tìm hiểu trên năm câu lệnh Google dork:

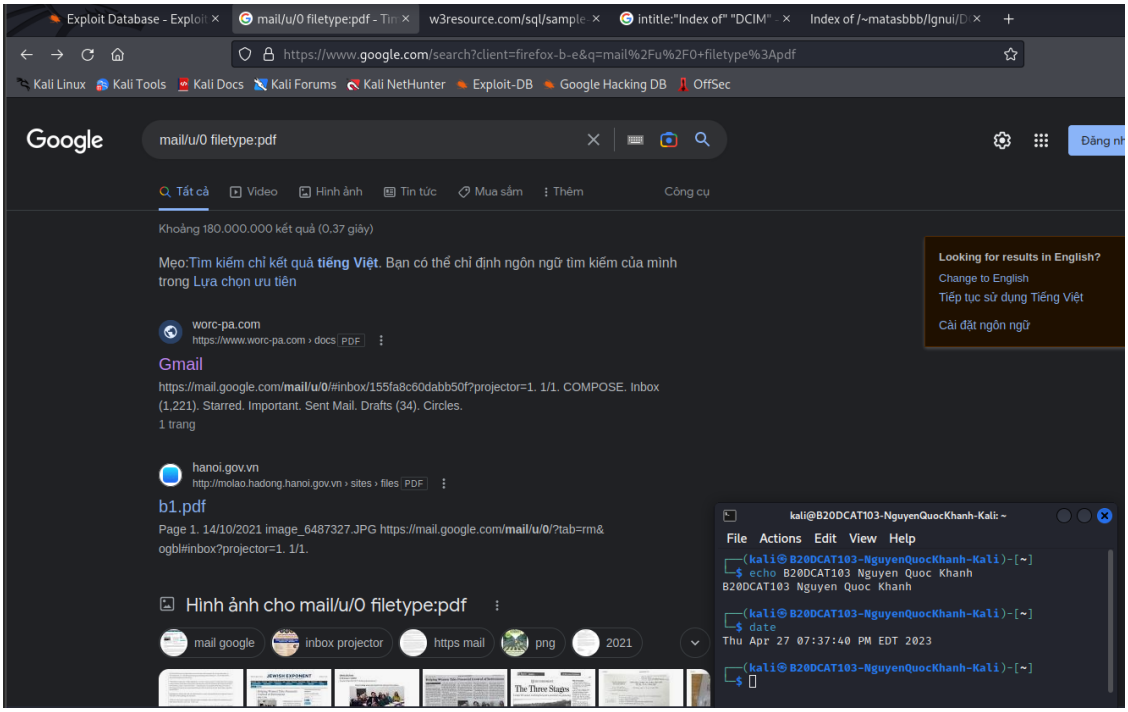
- Google dork “intext:"Dumping data for table `orders`"” được dùng để tìm nội dung cơ sở dữ liệu của một số trang web:



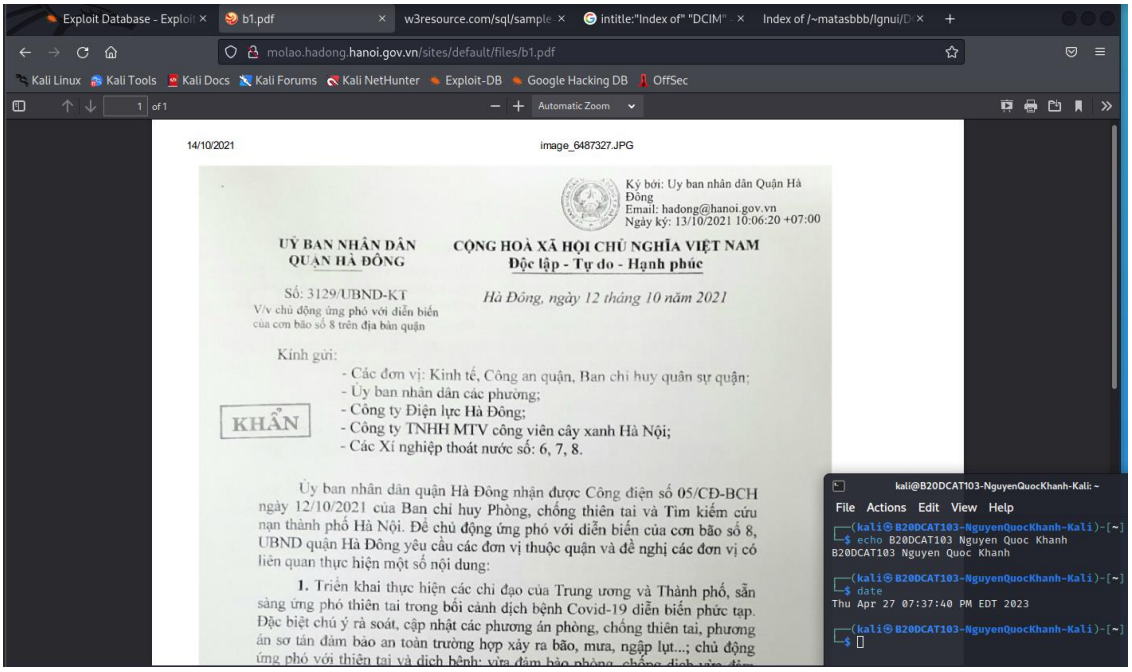
- Nhấp vào một liên kết, ta thu được thông tin và nội dung của cơ sở dữ liệu dưới đây:



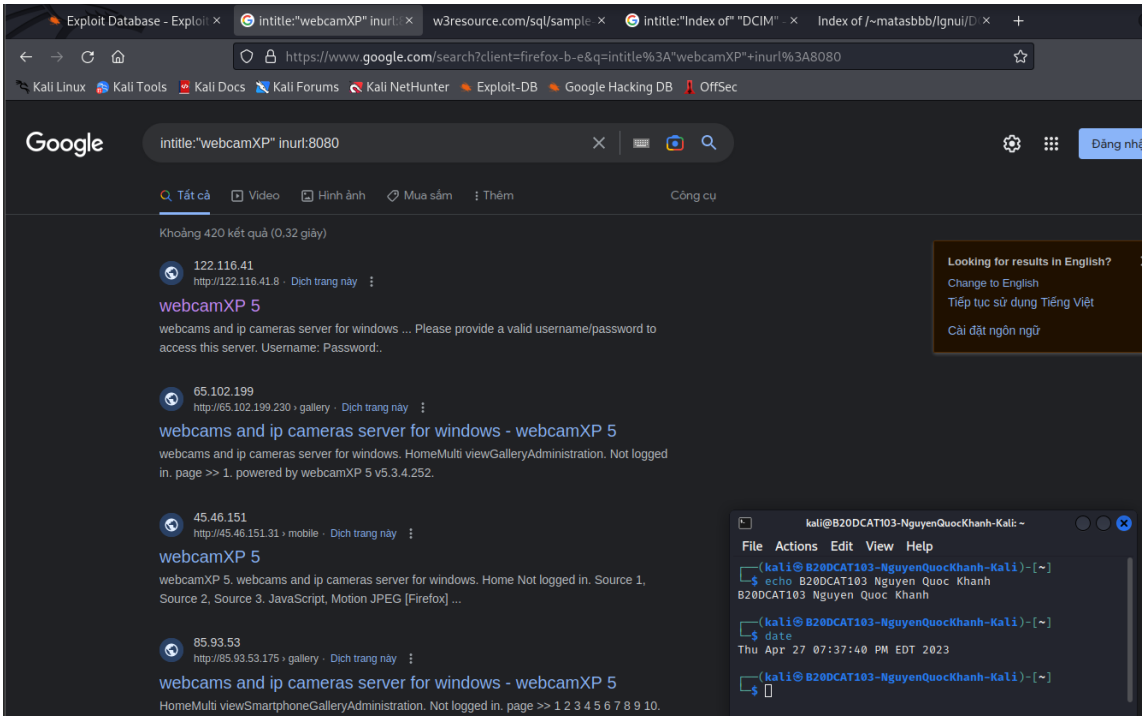
- Google dork “mail/u/0 filetype:pdf” được dùng để tìm các văn bản tài liệu định dạng pdf gửi từ Email:



- 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 dễ nhận biết:



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