HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOAN AN TOÀN THÔNG TIN

BÁO CÁO THỰC HÀNH

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

Họ và tên: VũThành Long

Mã sinh viên: B21DCAT012

Nhóm: 06

Môn học: Thực tập cơ sở

Giảng viên giảng dạy: Nguyễn Hoa Cương

Hà Nội, 2024

I. Mục đích:

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

II. Nội dung thực hành:

2.1 Tìm hiểu lý thuyết:

- **Tìm hiểu về công cụ Shodan:**
  - Shodan(Sentient Hyper-Optimized Data Access Network), là một công cụ tìm kiếm giống như Google, nhưng thay vì tìm kiếm các trang web, nó tìm kiếm các thiết bị kết nối Internet từ các bộ định tuyến và máy chủ, đến các thiết bị Internet of Things (IoT), như máy cảm ứng nhiệt, TV thông minh, đến các hệ thống phức tạp chi phối một loạt các ngành công nghiệp, bao gồm năng lượng, năng lượng và giao thông vận tải. Shodan có thể tìm thấy bất cứ thứ gì kết nối trực tiếp với internet và nếu các thiết bị đó tồn tại lỗ hổng, Shodan có thể nói với tin tặc mọi thứ họ cần biết để tấn công vào mạng lưới của thiết bị đó.
  - Shodan (Sentient Hyper-Optimized Data Access Network) hoạt động theo thuật toán sau:
    - Tạo một địa chỉ IPv4 một cách ngẫu nhiên.
    - Chọn port (cổng dịch vụ) ngẫu nhiên và thực hiện gửi câu lệnh kiểm tra.
    - Xem nội dung phản hồi của thiết bị (Service Banner) từ đó xác định xem đó là loại thiết bị gì và chạy cổng cổ.
    - Lặp lại quá trình trên nhưng với ip và port mới.
  - Shodan thu thập dữ liệu trên web của các thiết bị sử dụng mạng máy tính và máy chủ toàn cầu. Shodan có thể cung cấp tất cả các loại thông tin nó nhận dạng, một số thông tin phổ biến như: Tên thiết bị, địa chỉ IP, cổng mạng, nhà mạng, vị trí địa lý,... Một số thiết bị sử dụng tên đăng nhập và mật khẩu mặc định, mã hiệu thiết bị, phiên bản phần mềm, tất cả đều có thể được khai thác bởi tin tặc. Ngoài các tìm kiếm cơ bản, shodan cung cấp các bộ lọc (filter) để lọc thông tin một cách chính xác và "thông minh"
- **Tìm hiểu về Google Hack:**
  - Google Hacking (Google Dorking), là một kỹ thuật thu thập thông tin được sử dụng bởi kẻ tấn công tận dụng các kỹ thuật tìm kiếm nâng cao của Google. Các truy vấn tìm kiếm của Google Hacking có thể được sử dụng để xác định các lỗ hổng bảo mật trong các ứng dụng web, thu thập thông tin cho các mục tiêu tùy ý hoặc riêng lẻ, khám phá các thông báo lỗi tiết lộ thông tin nhạy cảm, khám phá các tệp có chứa thông tin xác thực và dữ liệu nhạy cảm khác.
  - Chuỗi tìm kiếm nâng cao được tạo ra bởi kẻ tấn công có thể đang tìm kiếm phiên bản chứa lỗ hổng của ứng dụng web hoặc loại tệp cụ thể (.pwd, .sql ...). Tìm kiếm cũng có thể được giới hạn ở các trang trên một trang web cụ thể hoặc nó có

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

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

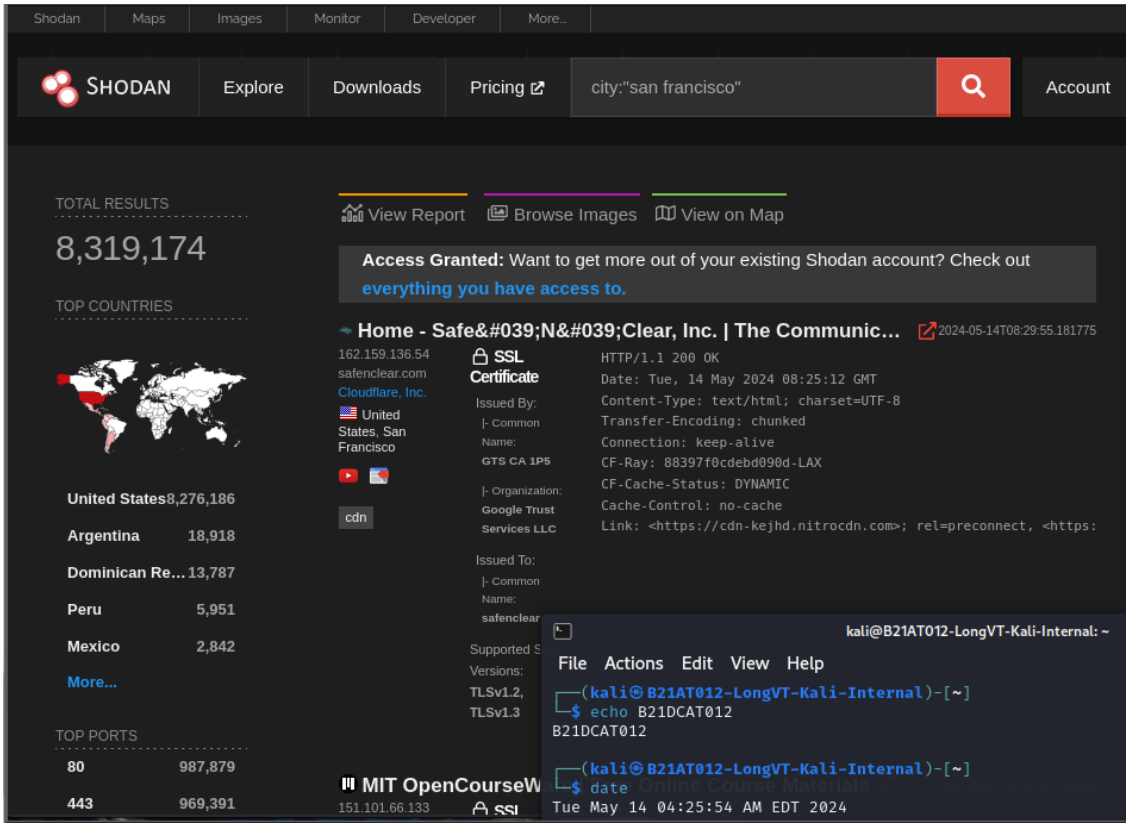
2.2. Các bước thực hiện :

2.2.1. Thử nghiệm với Shoban:

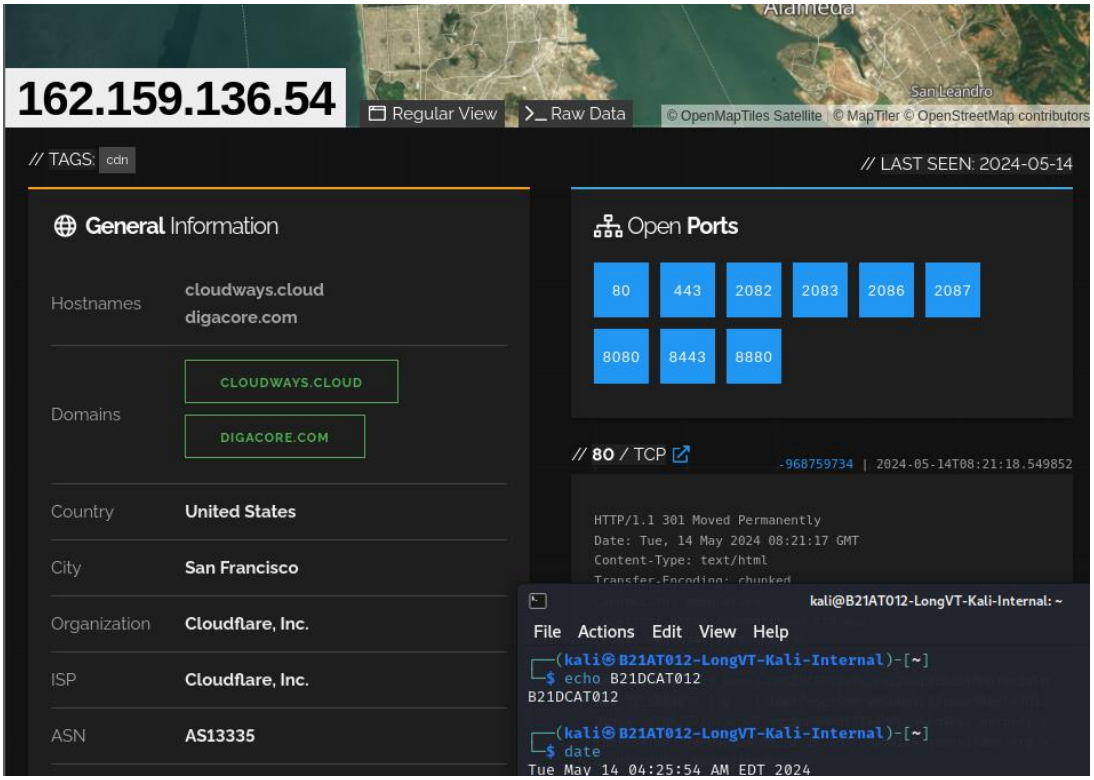
a. Các bước thực hiện:

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

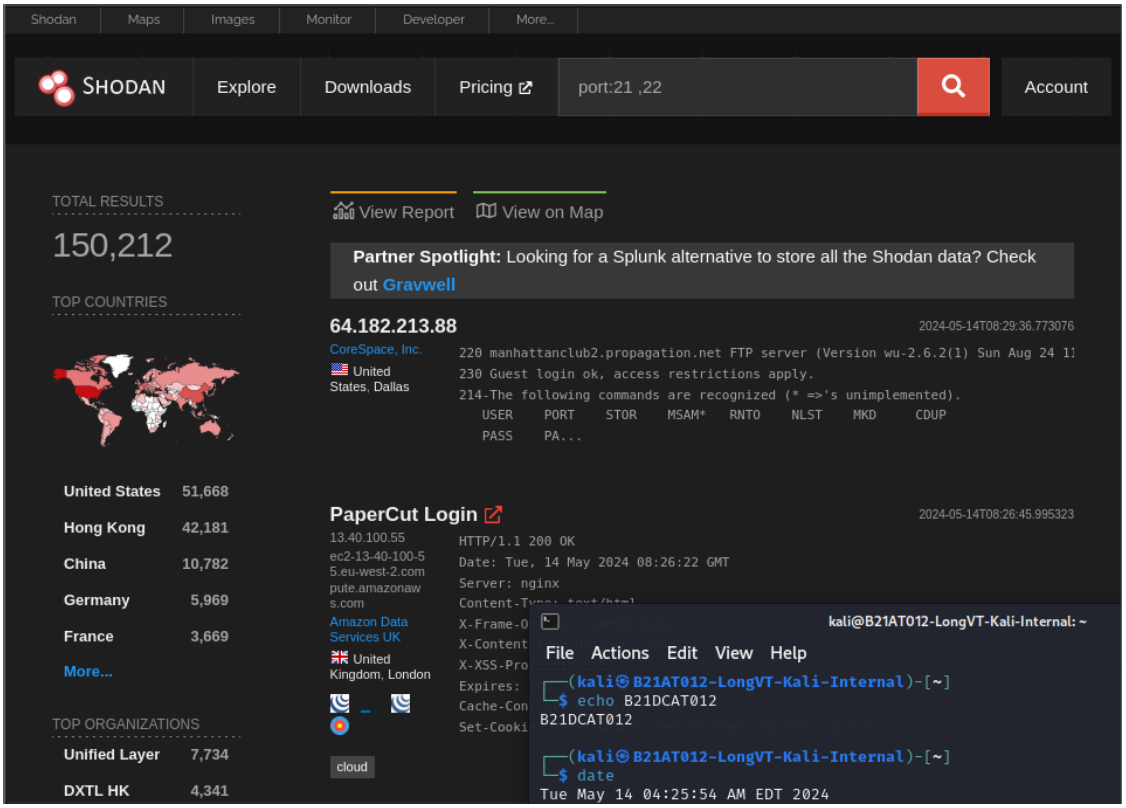
-Ta thử tìm kiếm 1 bộ lọc là: city:" san francisco" sẽ cho ra kết quả là các website, các cổng dịch vụ, các tổ chức, các hệ điều hành đang chạy trên phạm vi của Hoa Kỳ và thành phố sanfrancisco



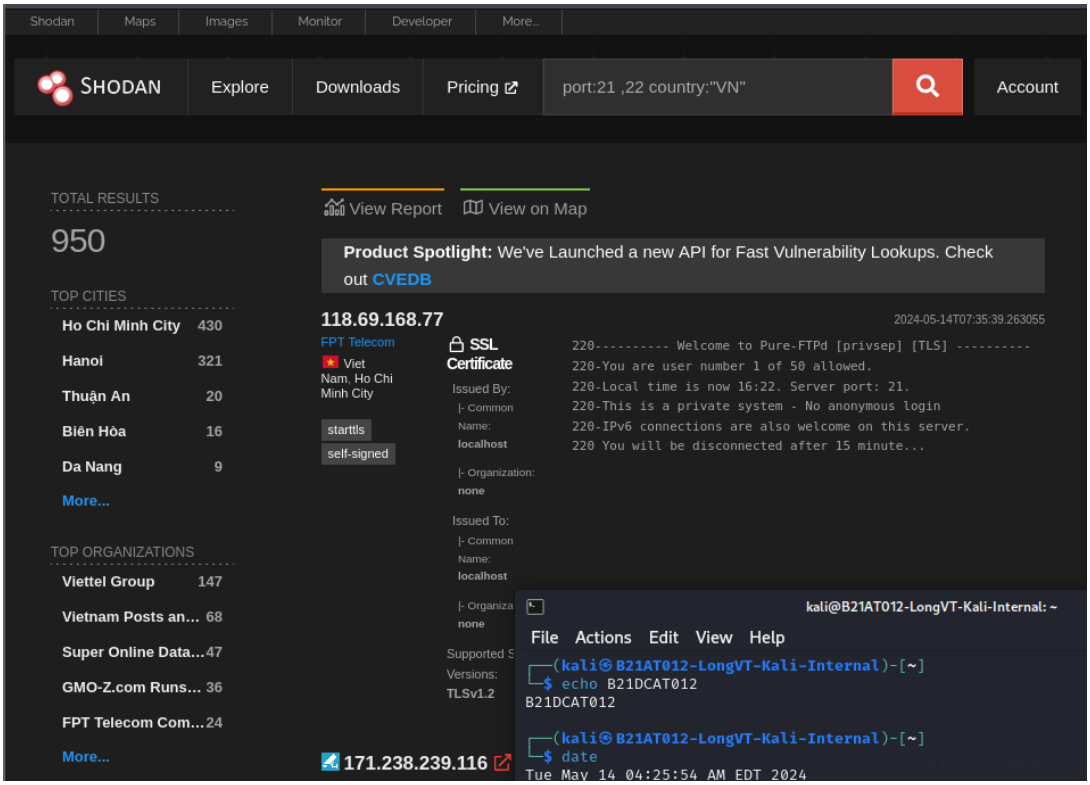
-Xem chi tiết 1 địa chỉ IP, ta sẽ thấy rõ hơn về các thông tin như hostname, domain, dịch vụ, quốc gia, thành phố, tổ chức và chi tiết các lỗ hổng.



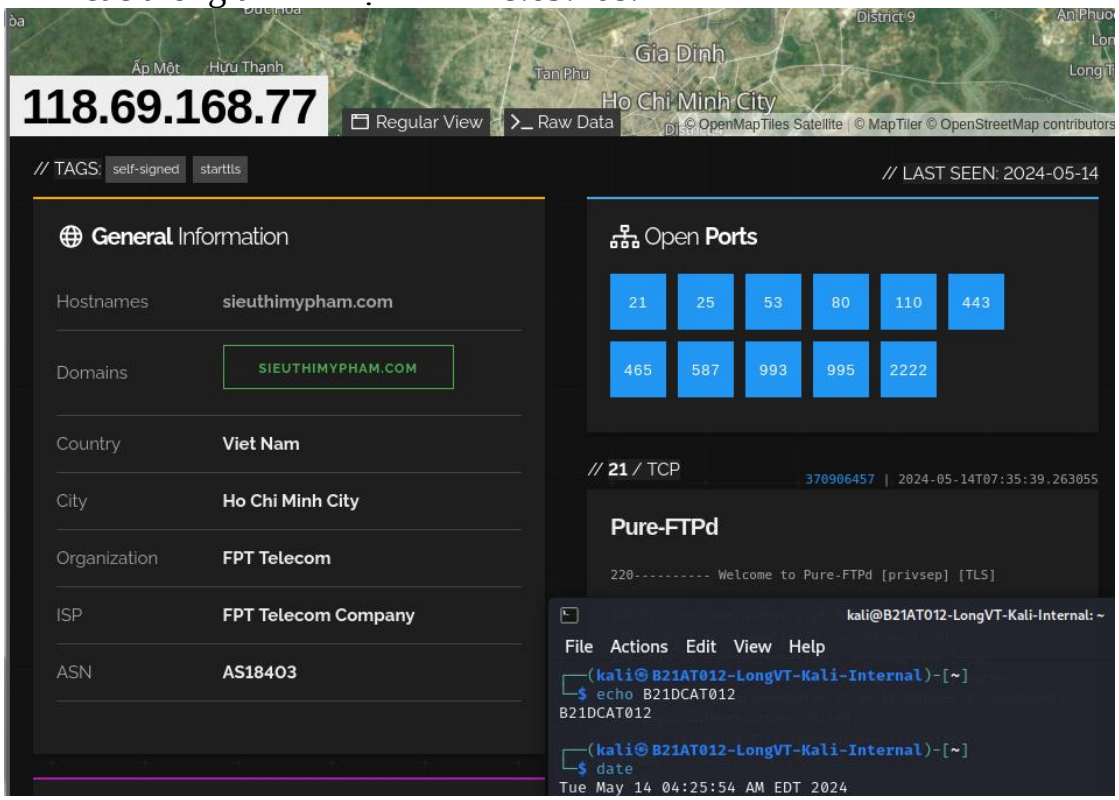
-Sử dụng bộ lọc port để tìm kiếm hai cổng 21 và 22: port:21,22



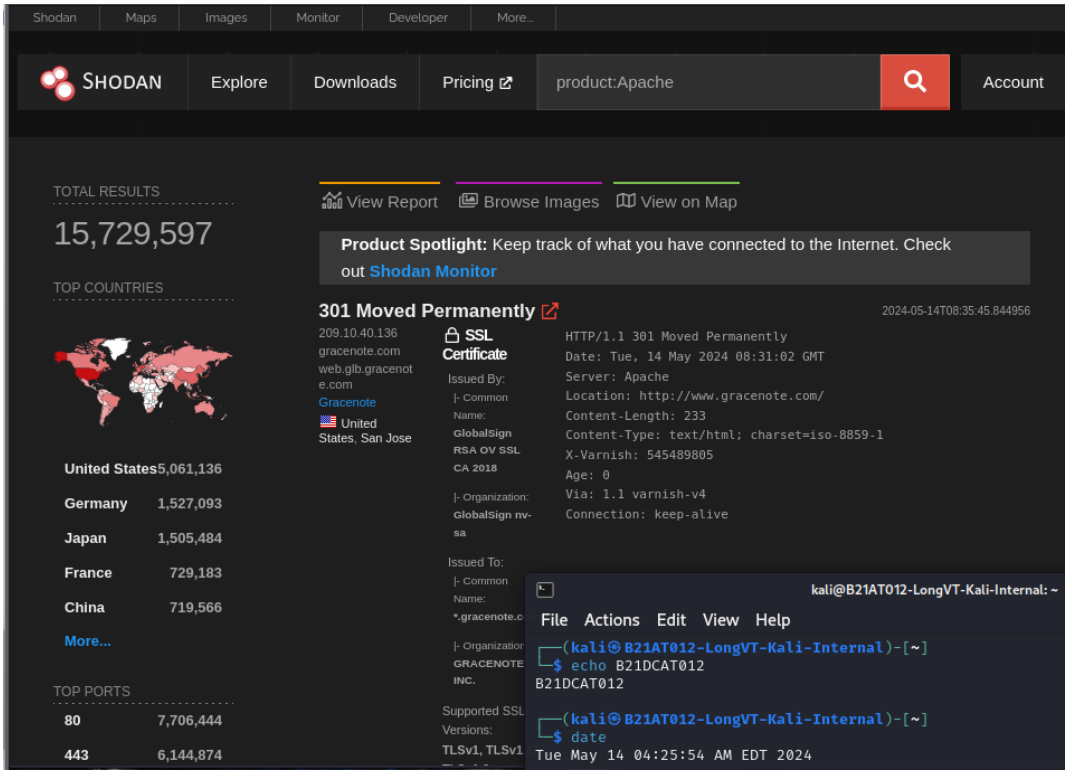
Sử dụng bộ lọc port để tìm kiếm hai cổng 21, 22 và country để tìm kiếm tại Việt Nam: port:21,22 country:"VN"



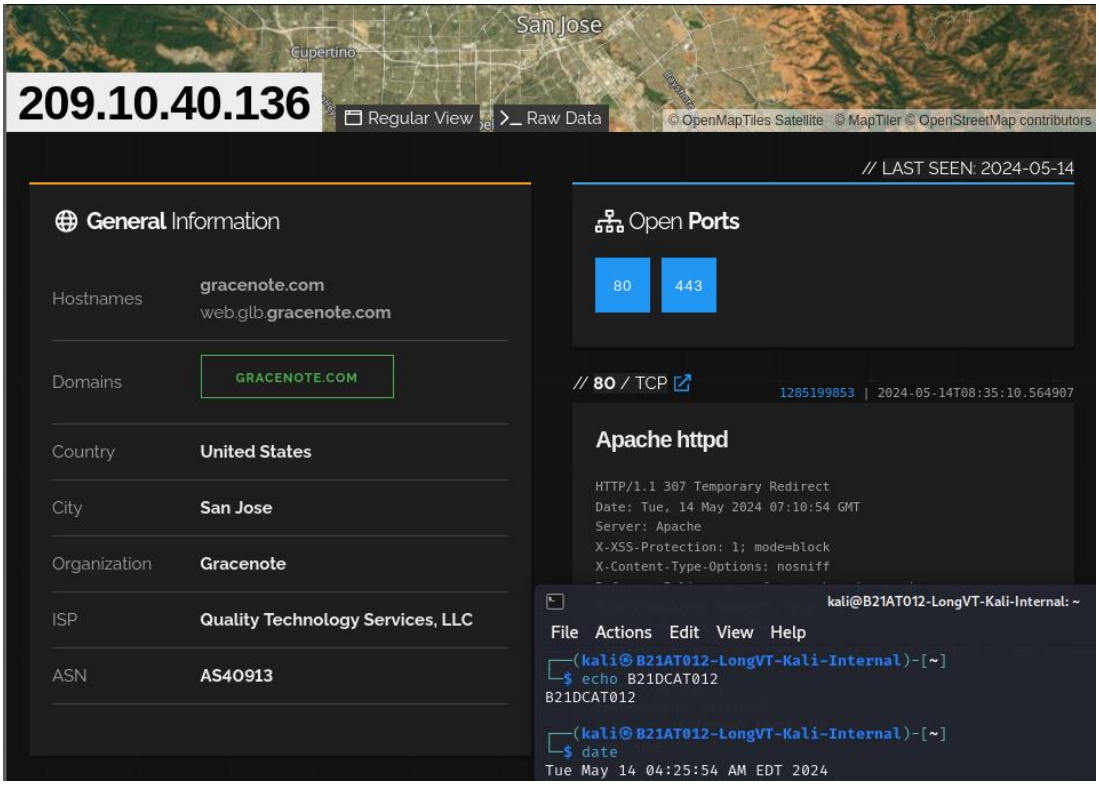
Xem chi tiết các thông tin của địa chỉ: 118.69.168.77

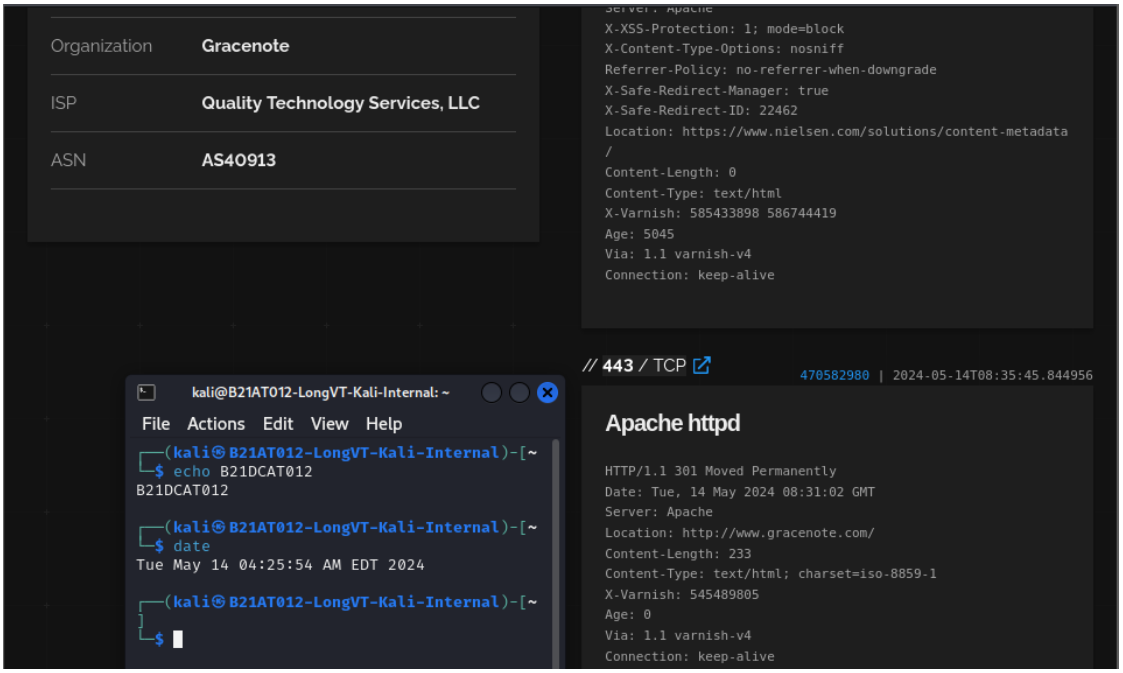


Sử dụng bộ lọc product để tim kiếm: “product: Apache”

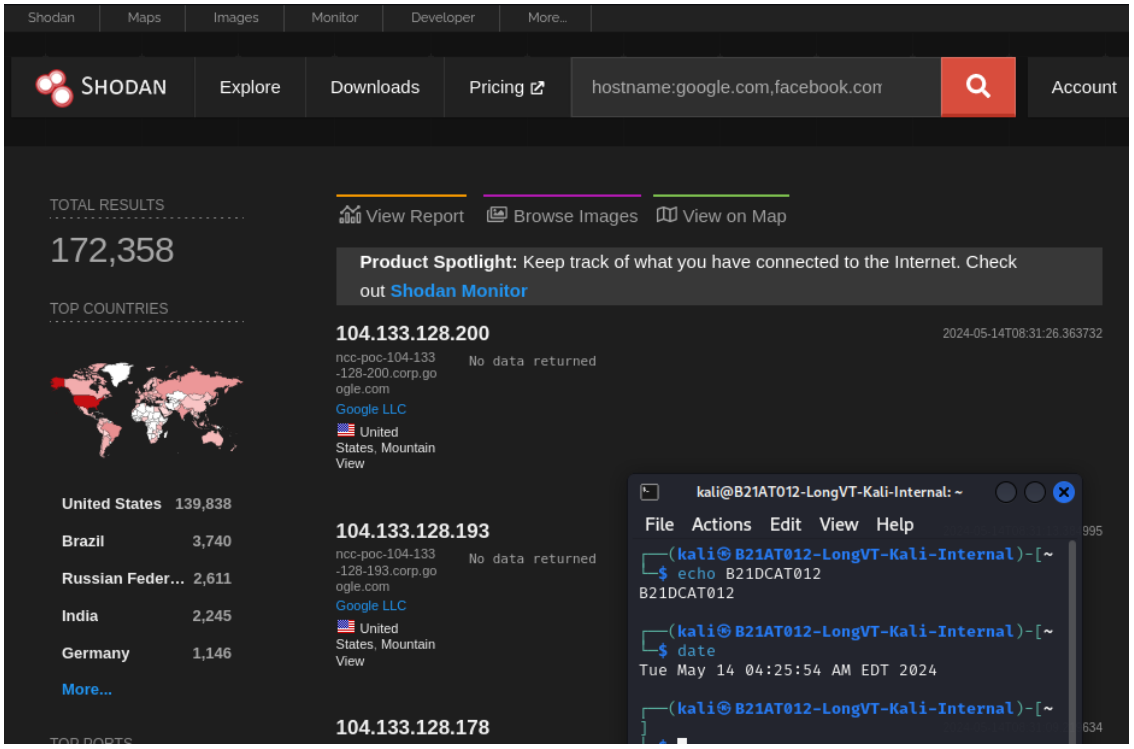


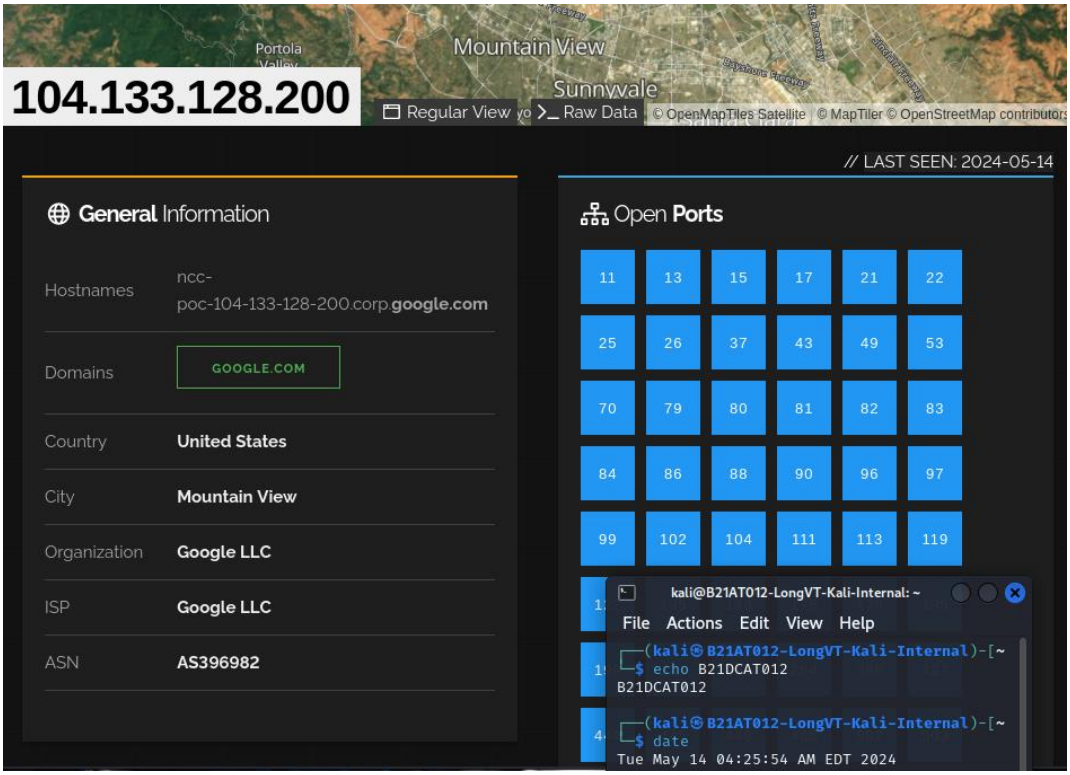
Xem cụ thể một địa chỉ IP



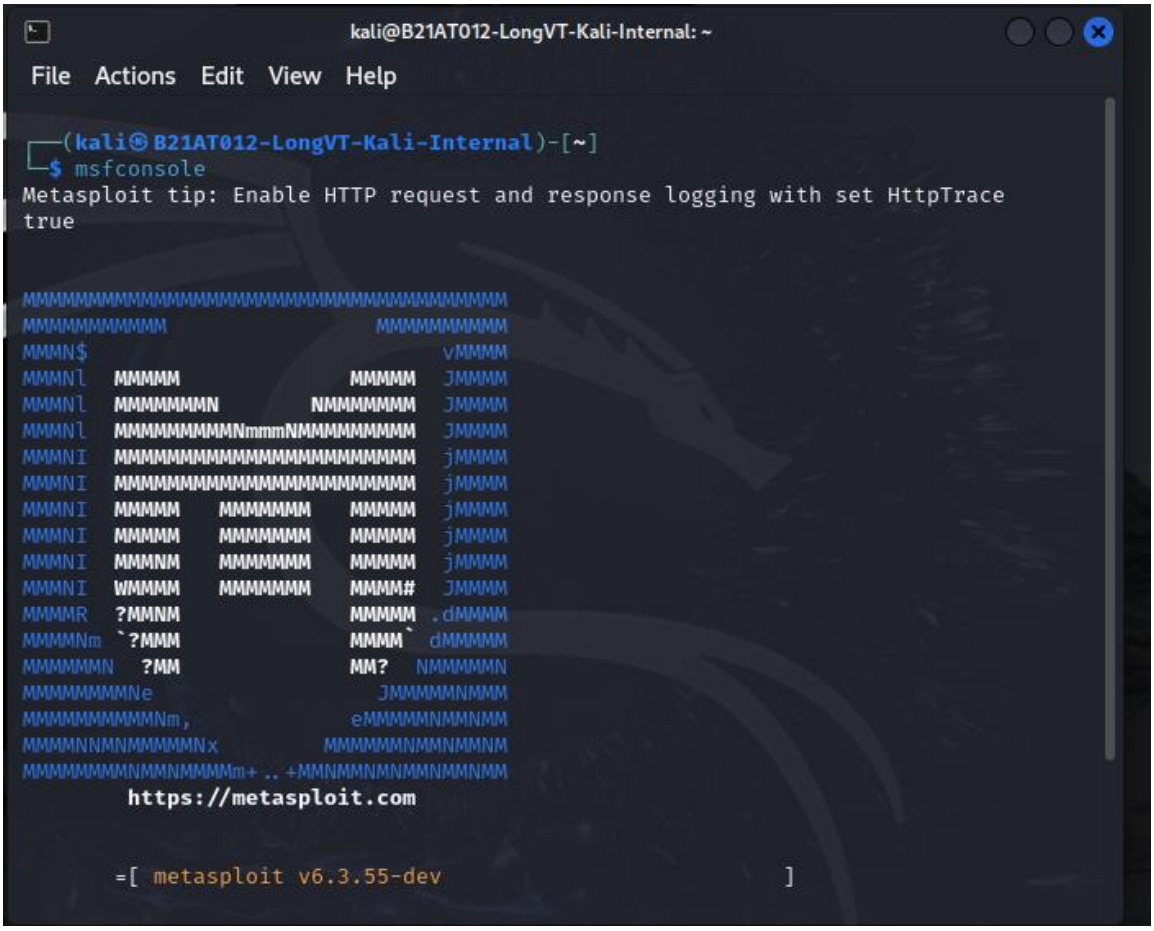


Sử dụng bộ lọc hostname để tìm kiếm các hostname của google và facebook



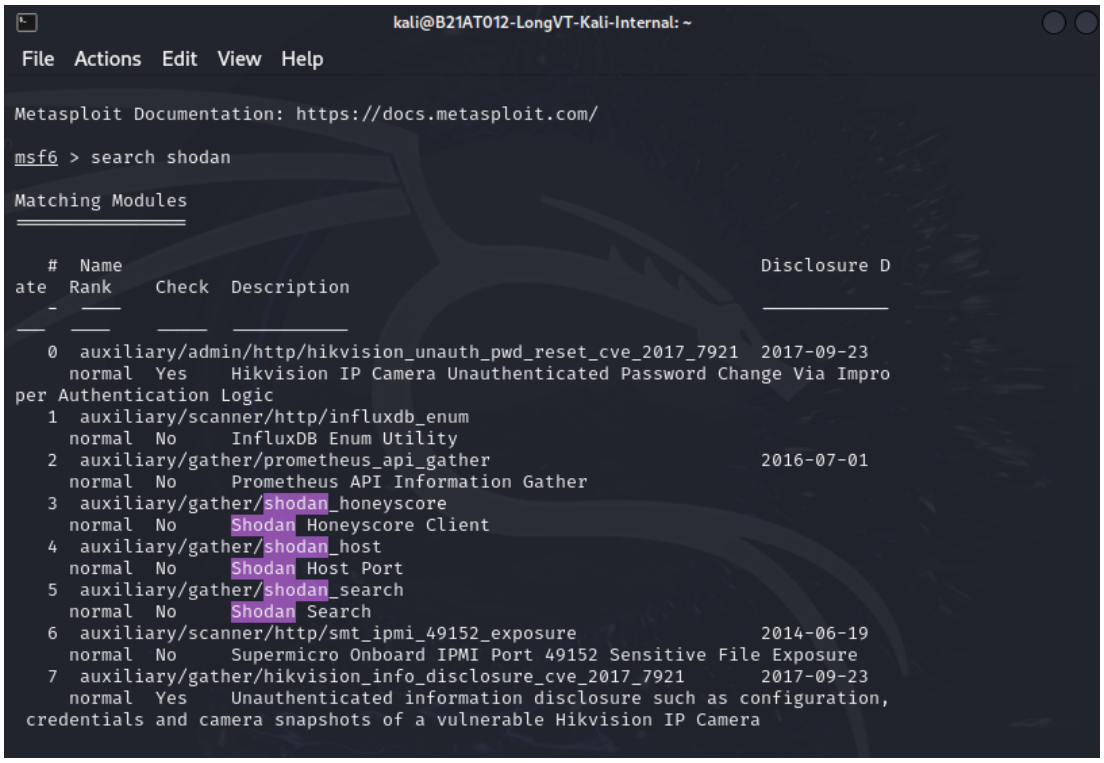


- Tìm kiếm các webcam tồn tại lỗ hổng với shodan (Metasploit Framework):
Khởi động metaspoilit trong kali linux

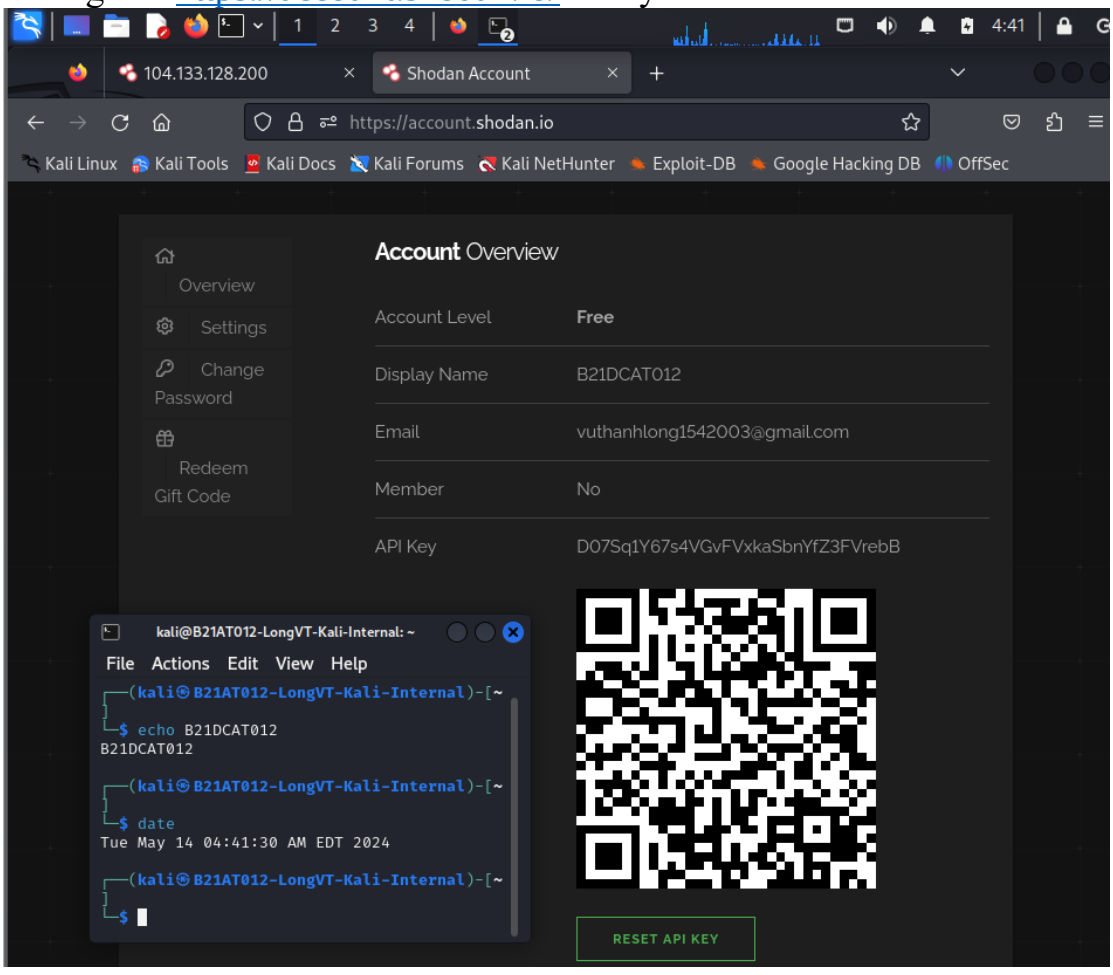


Tìm kiếm: search shodan

Khai báo sử dụng mô đun tấn công: use auxiliary/gather/shodan_search

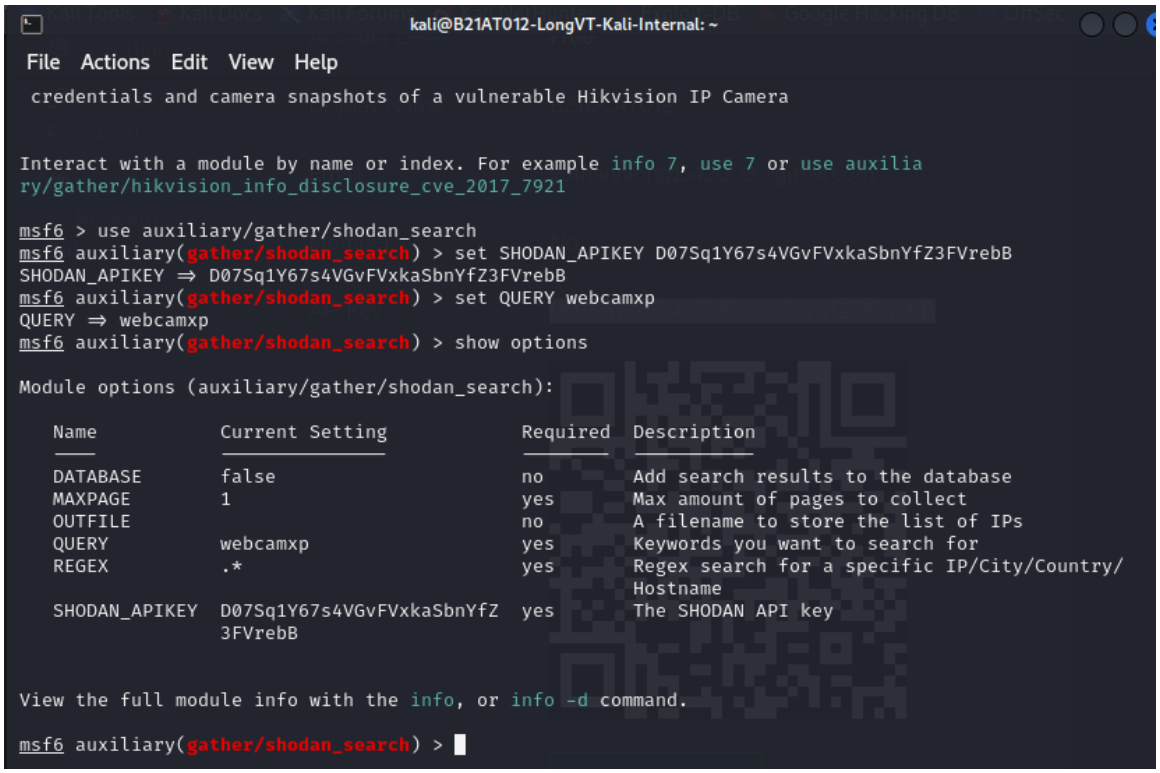


Ấn vào đường dẫn https://account.shodan.io/ để lấy API



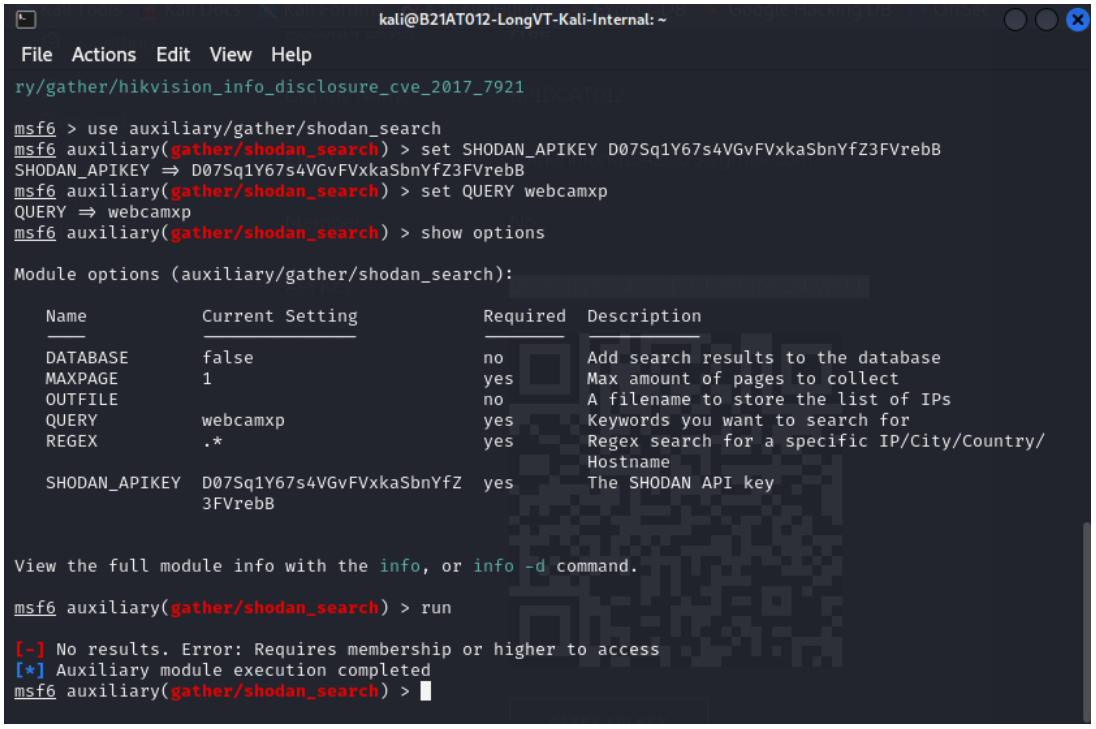
Đặt truy vấn muốn tìm kiếm là webcamxp

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



Chạy lệnh “run” để tìm kiếm

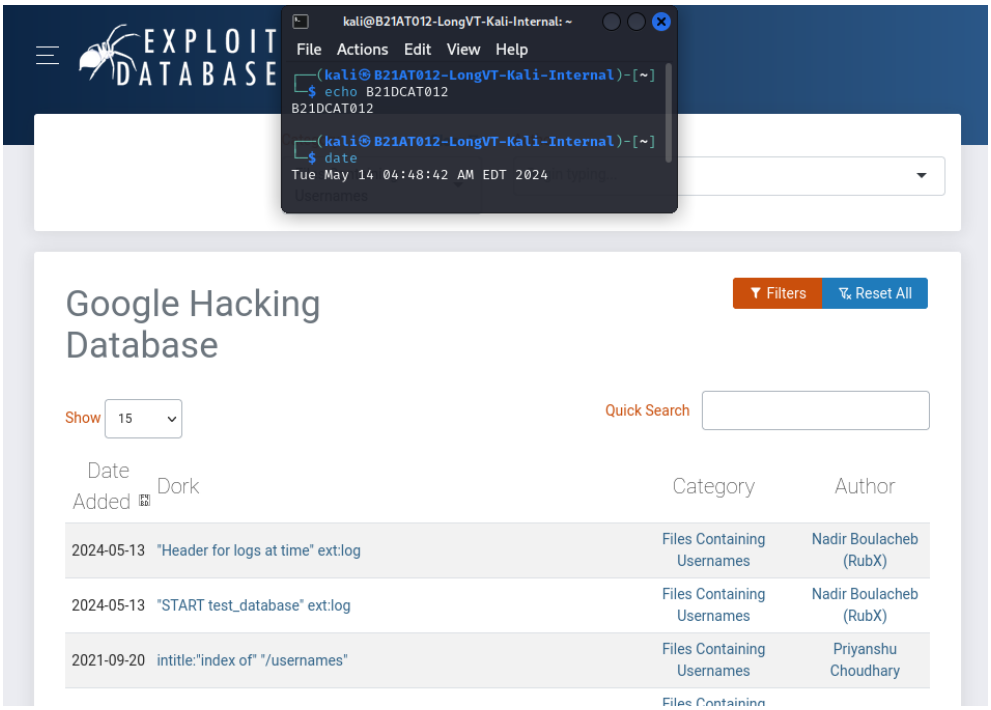
Do account là account thường nên phần key yêu cầu không đáp ứng được cho nên khi run hệ thống thông báo quyền access cao hơn. Mong thầy thông cảm ạ



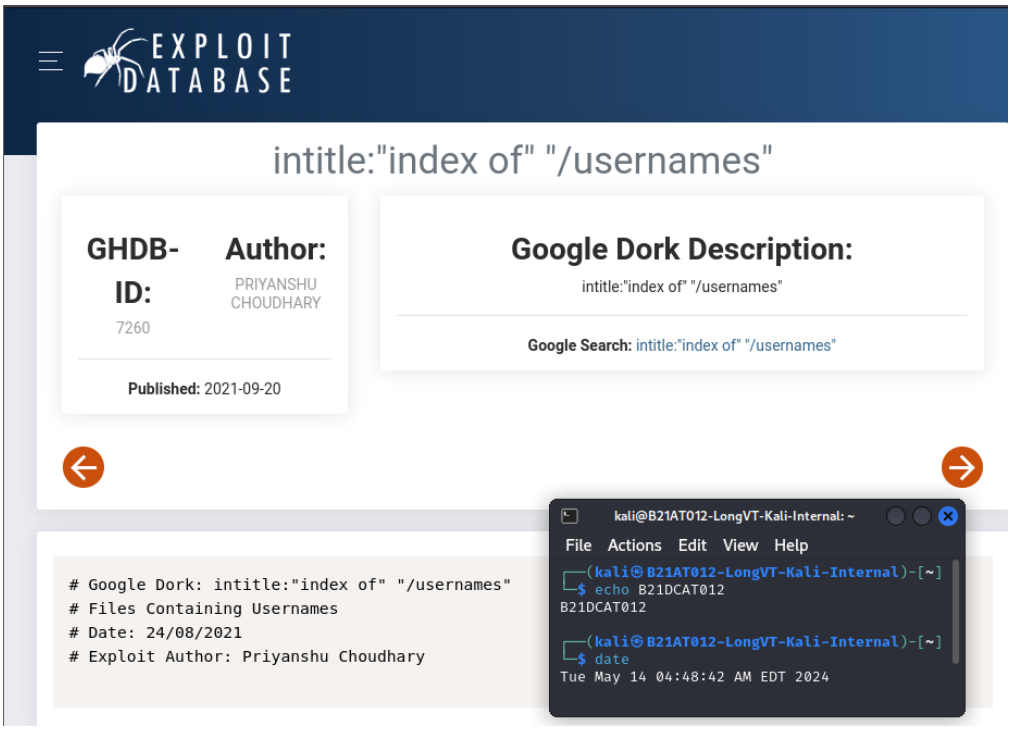
Thử nghiệm với Google Hacking Database

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

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

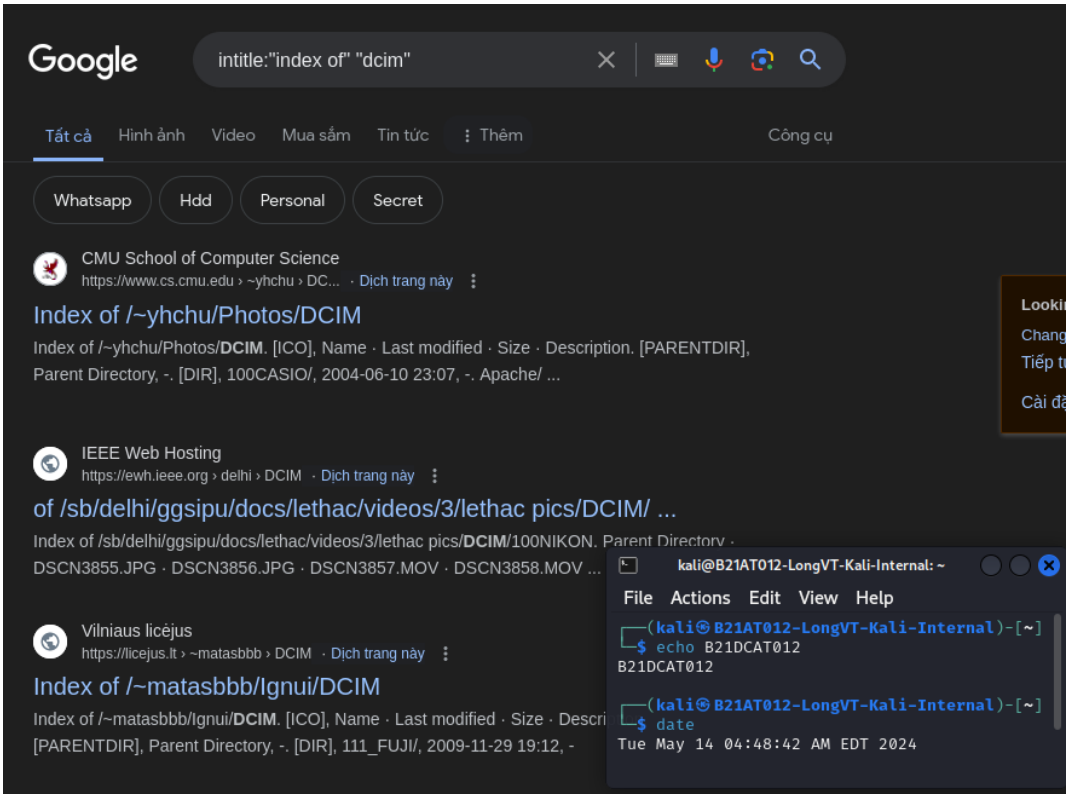


Ta chọn Vulnerable Servers và hiện ra trang thông tin có liên quan bao gồm thông tin tác giả, mô tả về tìm kiếm và các thông tin khác.



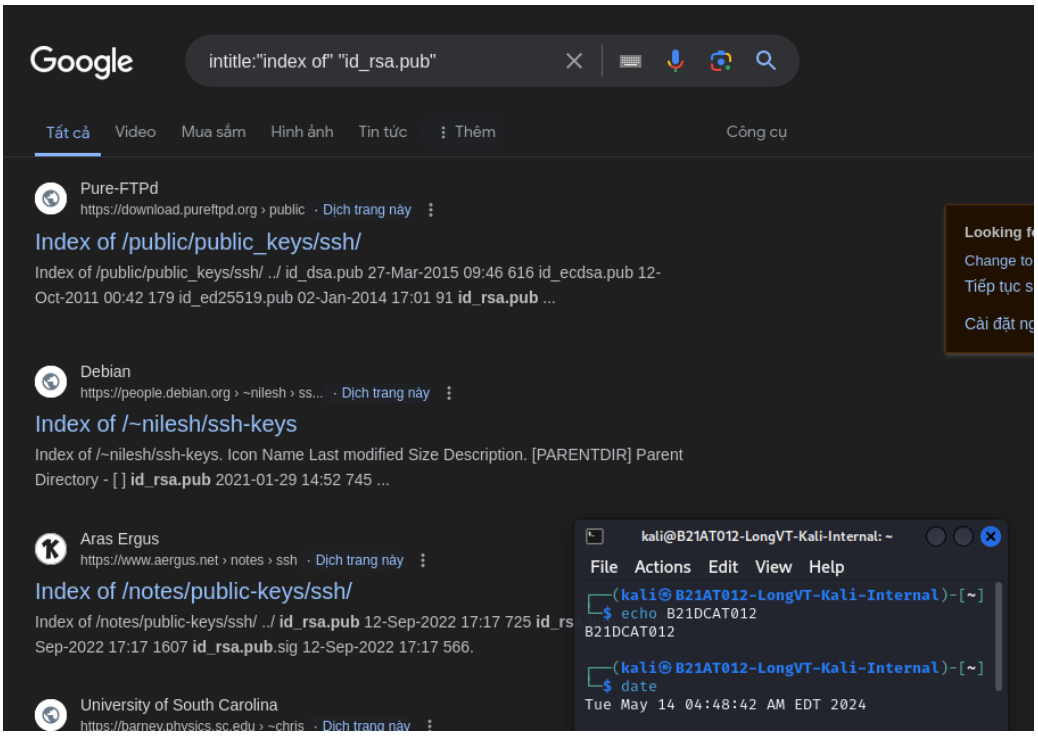
-Thử nghiệm với truy vấn tìm kiếm intitle: “Index of” “DCIM”, Google sẽ trả về kết quả của các bộ sưu tập ảnh mà mọi người không biết ở đó.
+intitle: tìm kiếm trong phần title của trang web

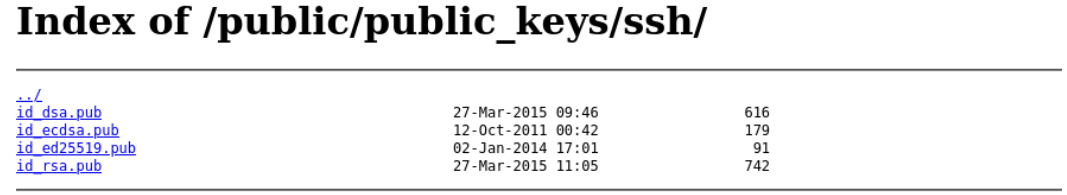
+DCIM: Là thư mục gốc lưu tất cả các ảnh mà bạn đã chụp trên các máy ảnh và điện thoại

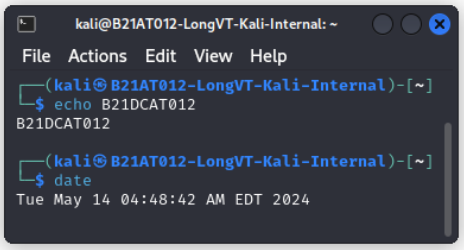


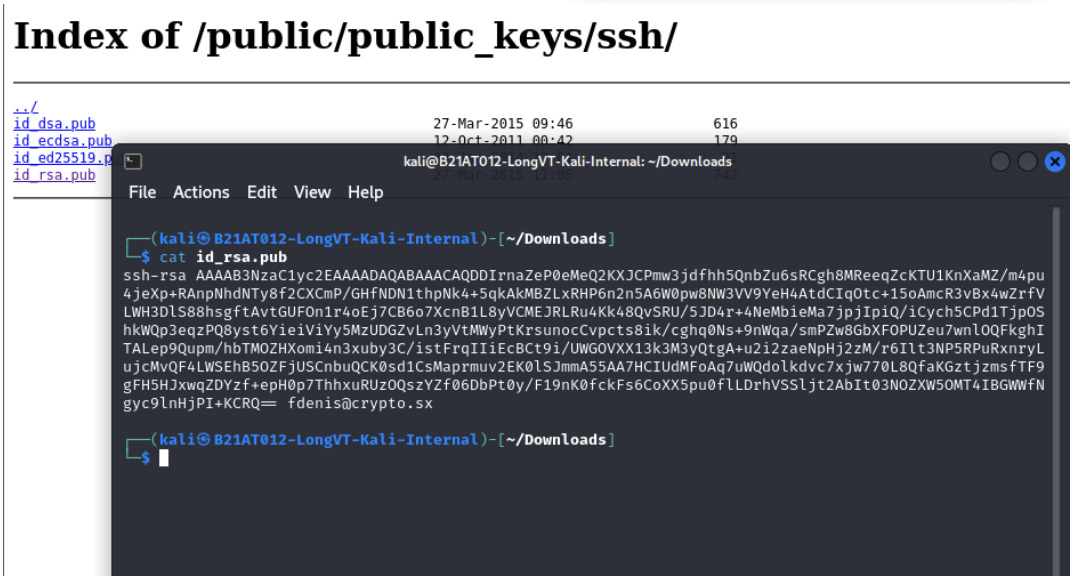
Google dork - một chức năng mà google cung cấp để việc tìm kiếm hiệu quả hơn.

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

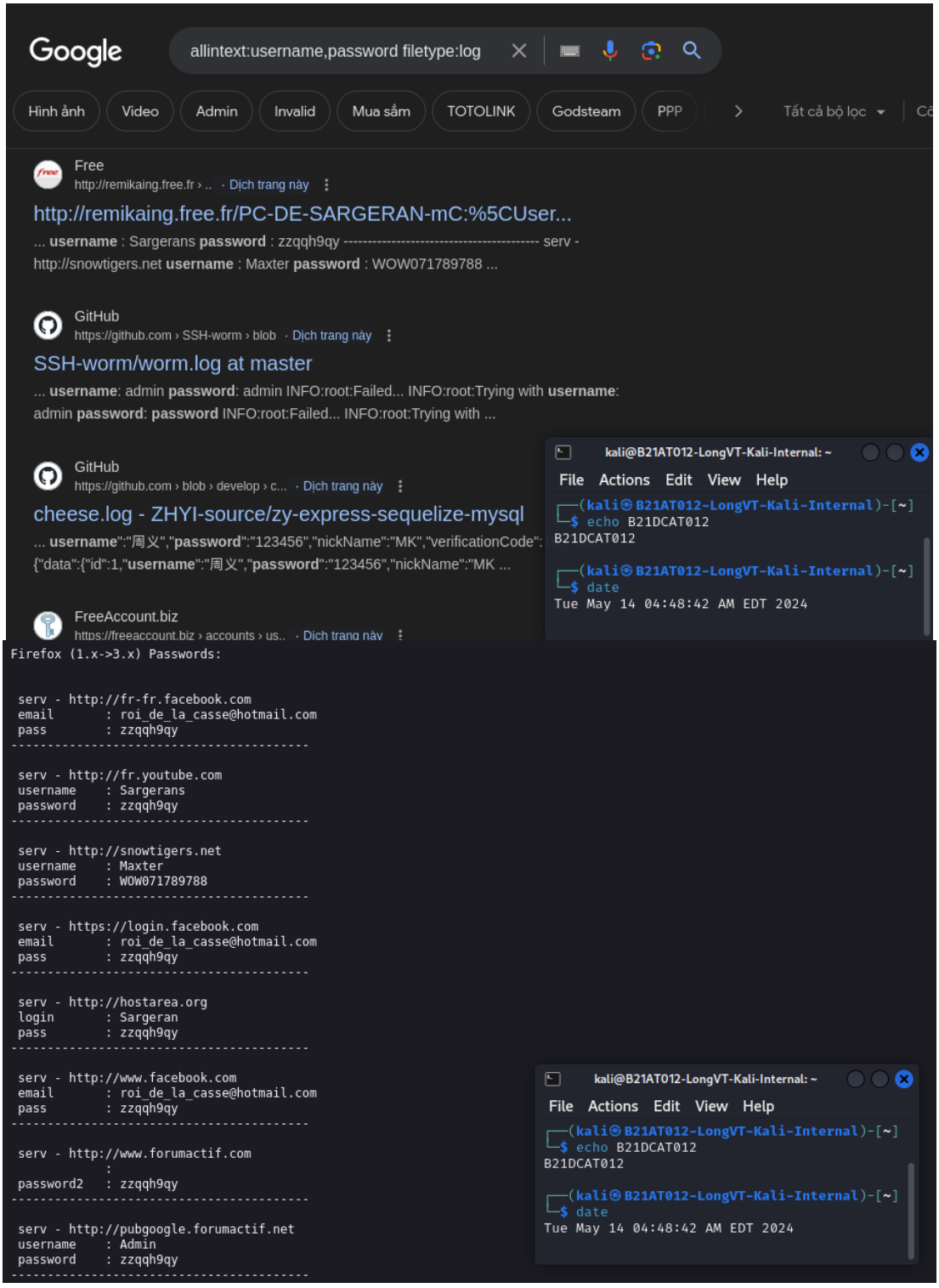




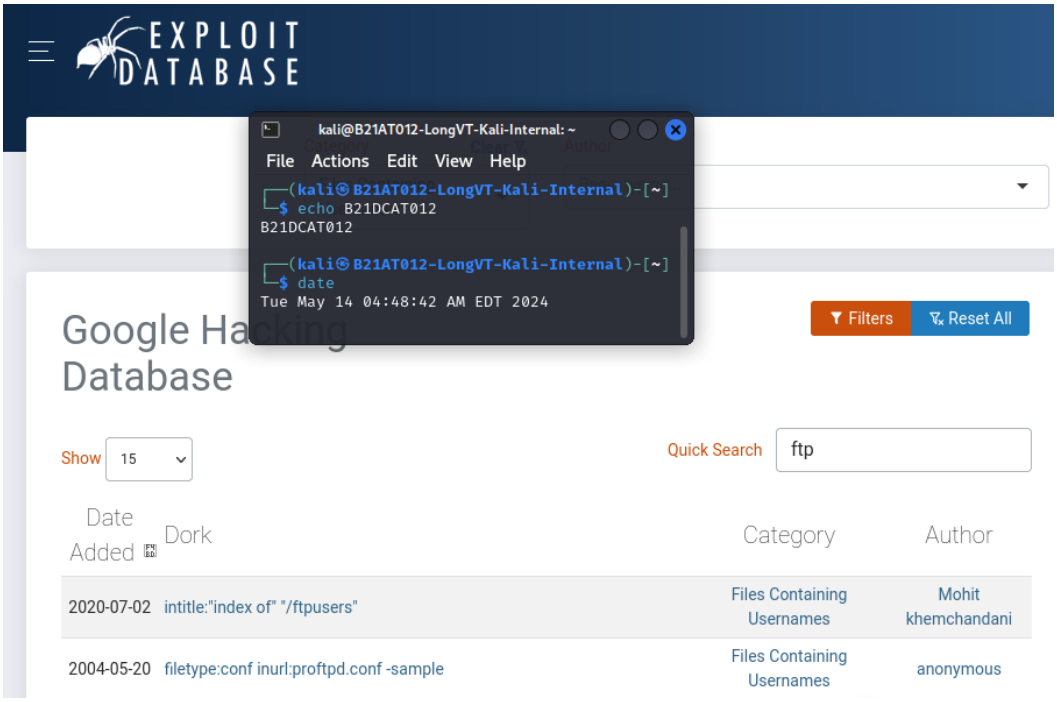




-Tìm log có tên người dùng và mật khẩu, ư địa chỉ e-mail, URL mà những thông tin đăng nhập này được sử dụng

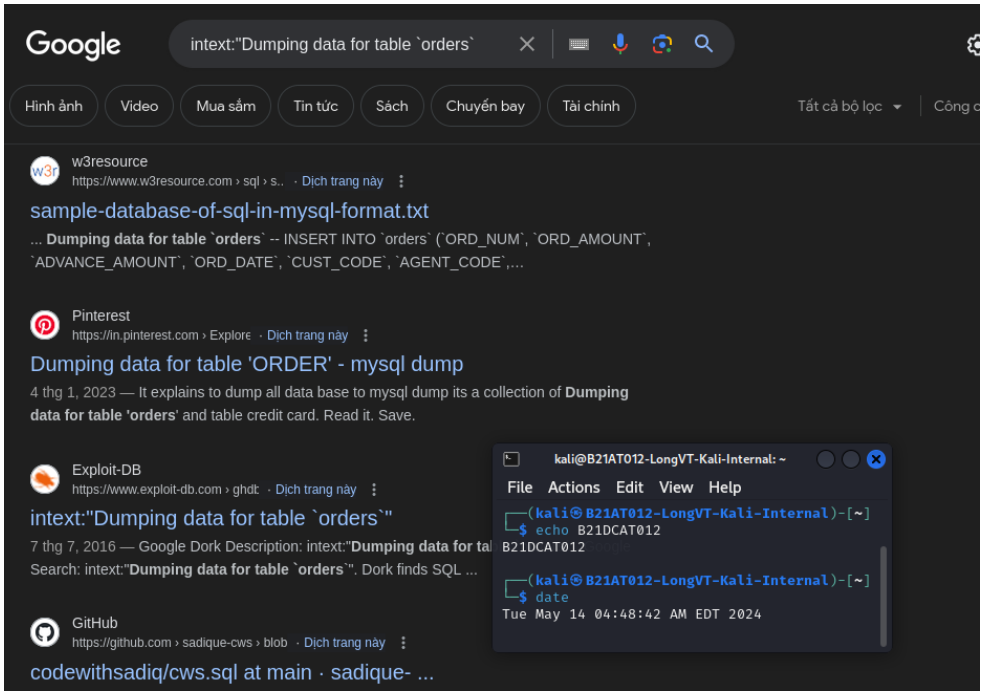


- Trong hộp văn bản Tìm kiếm nhanh ở bên phải, nhập FTP. Xuất hiện rất nhiều Google dorks liên quan đến Giao thức truyền tệp (FTP).

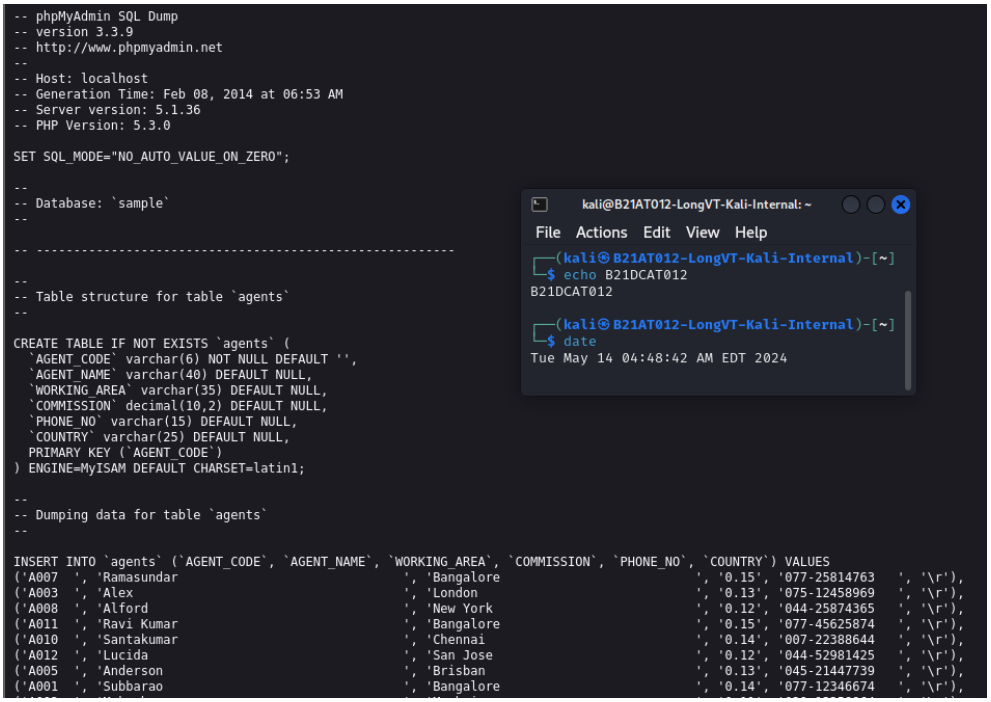


Chọn 5 Google dork, mỗi loại thuộc một danh mục khác nhau và giải thích cách chúng có thể có nguy hiểm như thế nào. Theo tùy chọn, hãy nhấp vào siêu liên kết cho các dork thực tế của Google để xem kết quả nào được trả về

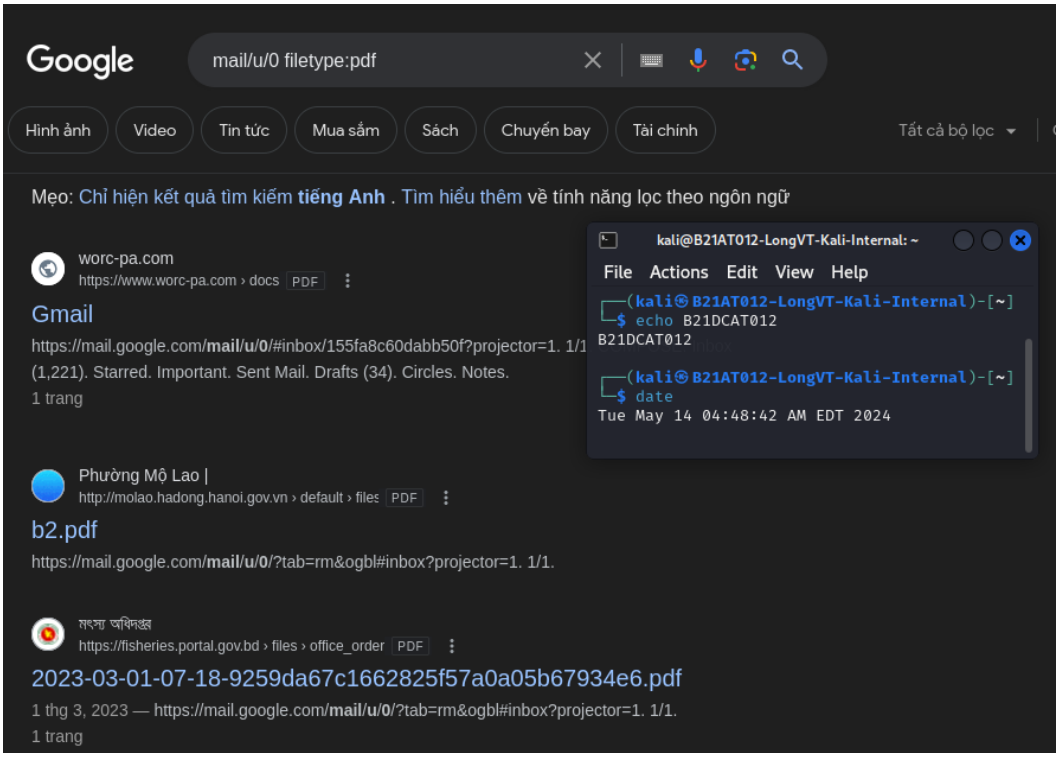
- Google dork “intext:"Dumping data for table `orders`"” được dùng để tìm nội dung cơ sở dữ liệu của một số trang web:



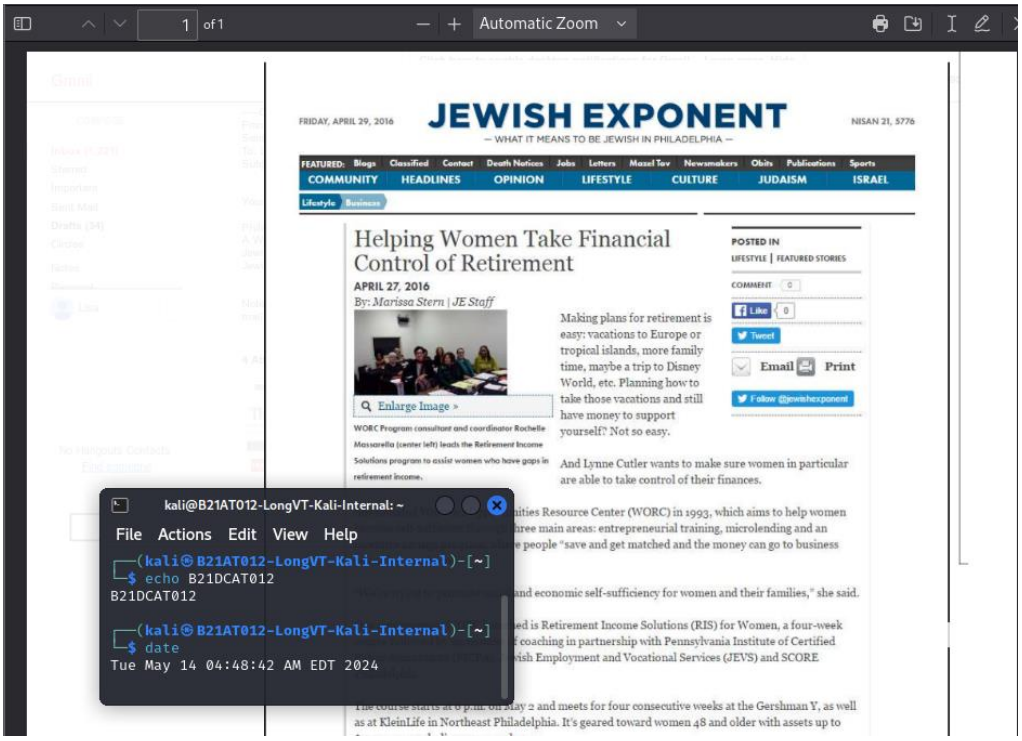
Nhấp vào một liên kết, ta thu được thông tin và nội dung của cơ sở dữ liệu dưới đây.



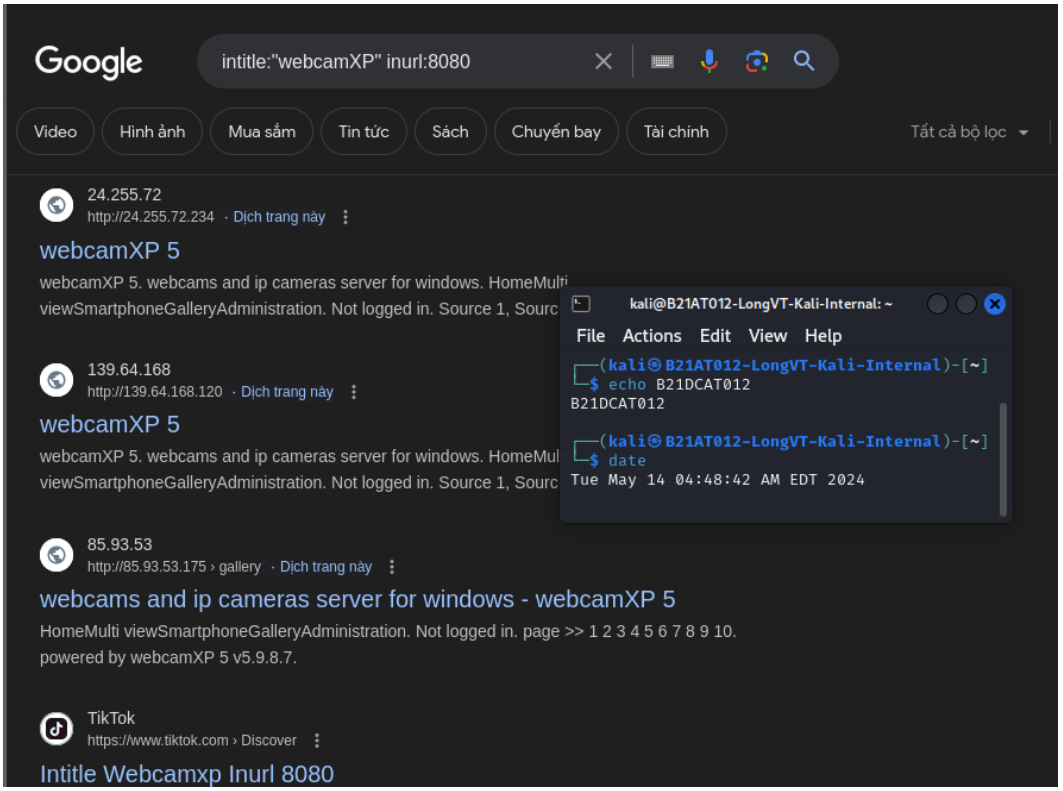
- Google dork “mail/u/0 filetype:pdf” được dùng để tìm các văn bản tài liệu định dạng pdf gửi từ Email.



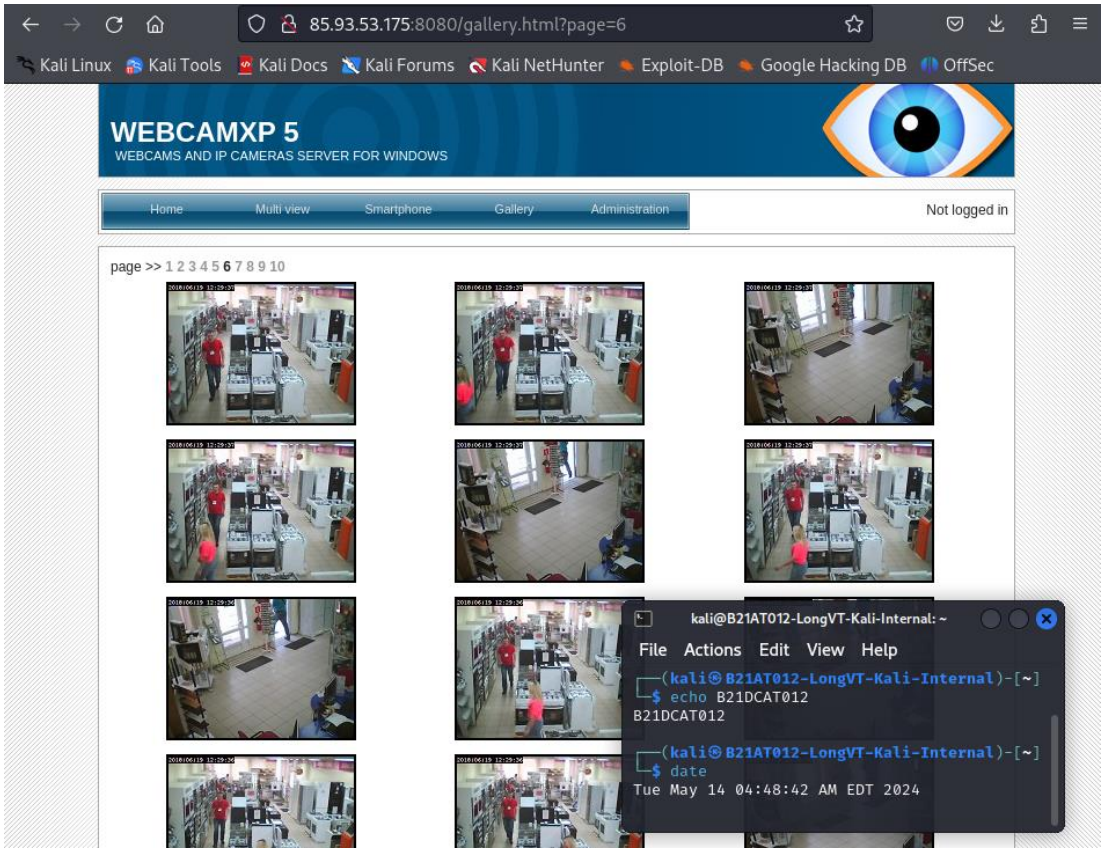
Nhấp vào một liên kết và nhận được văn bản dưới đây.



- 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:

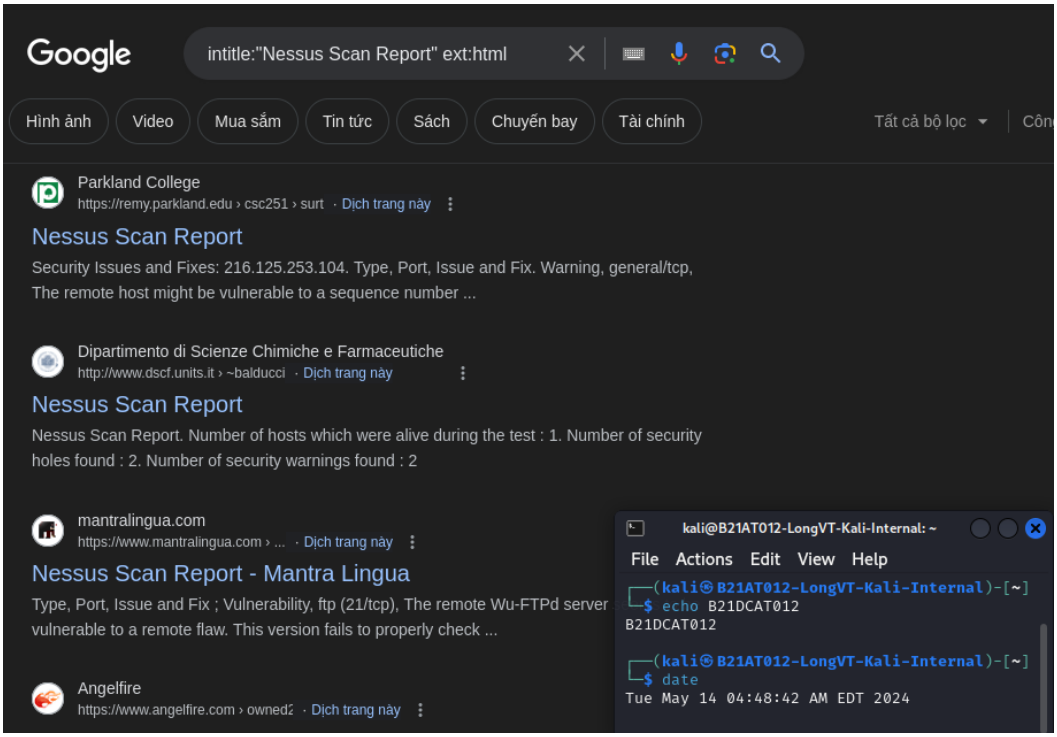


Nhấp vào liên kết và thu được các hình ảnh webcam gửi về.

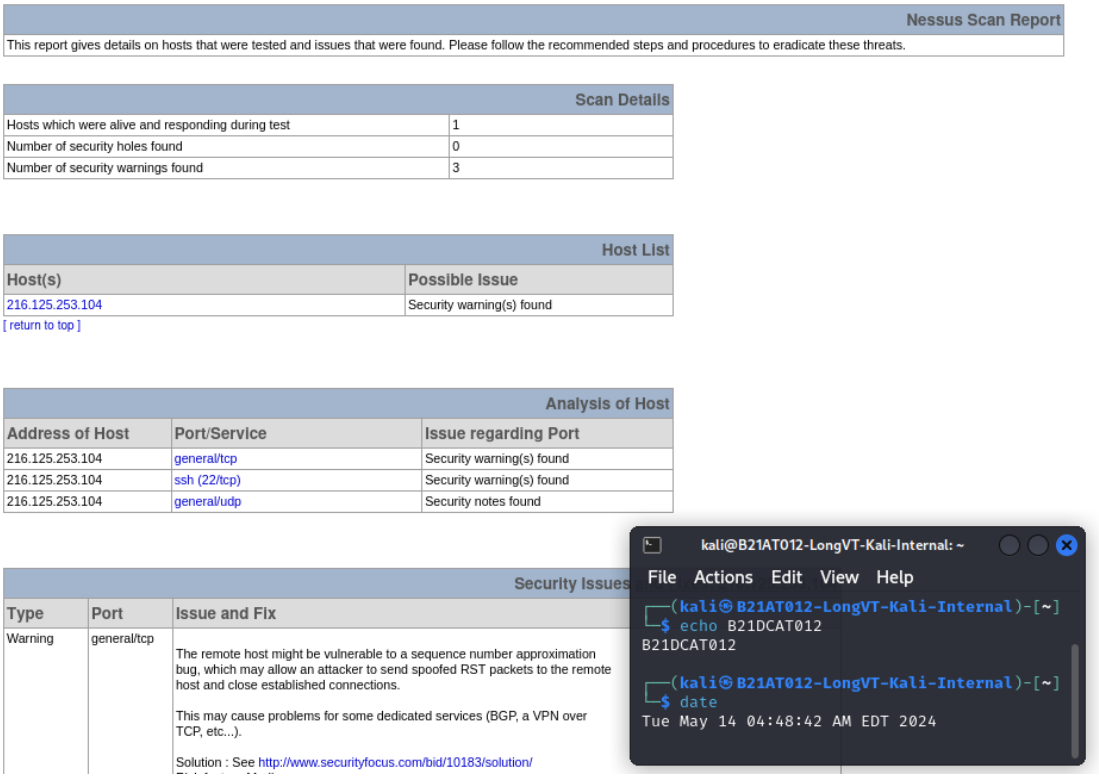


Webcam đang hoạt động

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



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



Nessus Scan Report

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

Scan Details

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

Host List

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

[return to top]

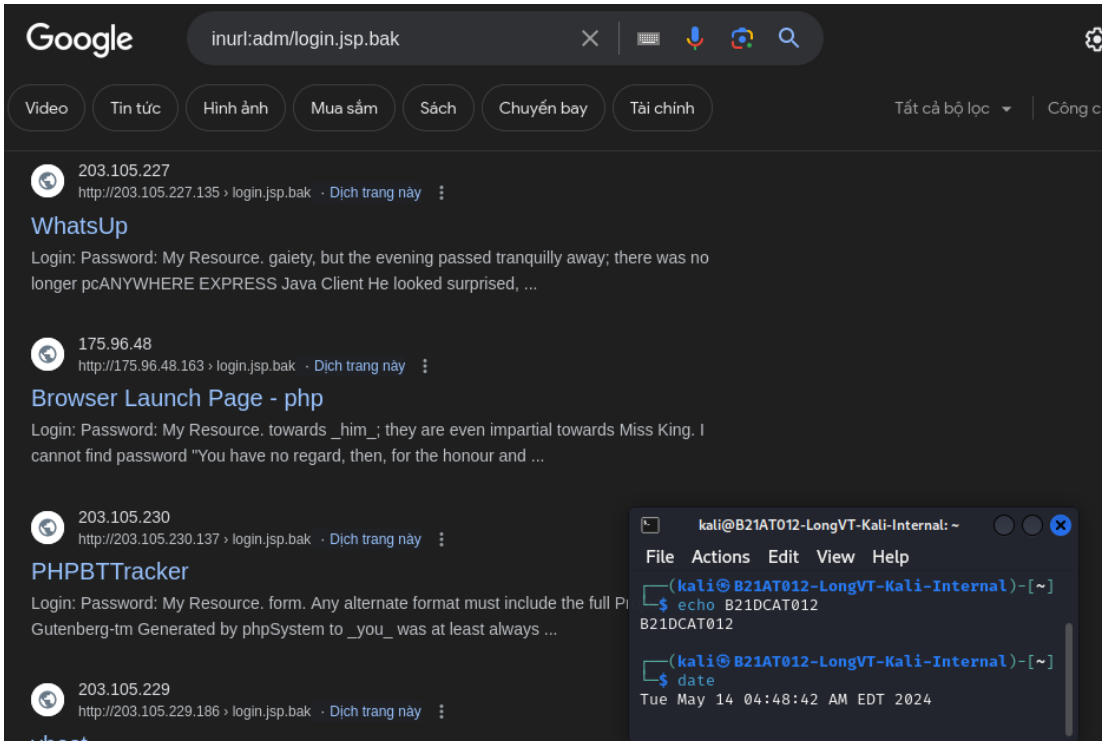
Analysis of Host

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

Security Issues

Type	Port	Issue and Fix
Warning	general/tcp	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. This may cause problems for some dedicated services (BGP, a VPN over TCP, etc...). Solution : See http://www.securityfocus.com/bid/10183/solution/

- 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:



III. Tài liệu tham khảo

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