MỤC LỤC

1. [Tìm hiểu lý thuyết 2](file:///C:\Users\Acer\Downloads\Bài-thực-hành-14_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark0)
   1. [Shodan 2](file:///C:\Users\Acer\Downloads\Bài-thực-hành-14_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark1)
   2. [Google Hacking và sự ảnh hưởng của nó tới quyền riêng tư 4](file:///C:\Users\Acer\Downloads\Bài-thực-hành-14_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark2)
2. [Nội dung thực hành 4](file:///C:\Users\Acer\Downloads\Bài-thực-hành-14_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark3)
   1. [Thử nghiệm với Shodan 4](file:///C:\Users\Acer\Downloads\Bài-thực-hành-14_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark4)
      1. [Tìm hiểu và thử nghiệm các bộ lọc trong danh sách: https:// beta.shodan.io/search/filters 5](file:///C:\Users\Acer\Downloads\Bài-thực-hành-14_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark5)
      2. [Tìm hiểu và thử nghiệm các ví dụ trong danh sách: https:// beta.shodan.io/search/examples 6](file:///C:\Users\Acer\Downloads\Bài-thực-hành-14_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark6)
      3. [Tìm hiểu và thử nghiệm các ví dụ trong danh sách: https://help.shodan.io/the -basics/search- query-fundamentals 8](file:///C:\Users\Acer\Downloads\Bài-thực-hành-14_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark7)
      4. [Tìm hiểu và thử nghiệm các ví dụ trong danh sách: https://](file:///C:\Users\Acer\Downloads\Bài-thực-hành-14_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark8)[www.ye ahhub.com/shodan](http://www.yeahhub.com/shodan)[-search- examples/ 9](file:///C:\Users\Acer\Downloads\Bài-thực-hành-14_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark8)
      5. [Tìm hiểu và thử nghiệm các ví dụ trong danh sách: https://](file:///C:\Users\Acer\Downloads\Bài-thực-hành-14_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark9)[www.ye ahhub.com/find-vulnerable-](http://www.yeahhub.com/find-vulnerable-) [webcams-shodan-metasploit-framework/ 12](file:///C:\Users\Acer\Downloads\Bài-thực-hành-14_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark9)
   2. [Thử nghiệm với Google Hacking Database 15](file:///C:\Users\Acer\Downloads\Bài-thực-hành-14_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark10)
3. [Tài liệu tham khảo 25](file:///C:\Users\Acer\Downloads\Bài-thực-hành-14_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark11)

# Tìm hiểu lý thuyết

# Shodan

* + - Shodan ([https://www.shodan.io)](https://www.shodan.io/) là một công cụ tìm kiếm được thiết kế bởi nhà phát triển web John Matherly.
    - Shodan là một công cụ tìm kiếm khác nhiều so với các công cụ tìm kiếm nội dung như Google, Yahoo hoặc Bing.
    - Shodan là một công cụ tìm kiếm để tìm các thiết bị trực tuyến trên internet

như: máy tính, server, webcam, các thiết bị routers…

* + - Nó hoạt động bằng cách quét toàn bộ các các thiết bị trên internet có mở cổng public ra internet và thực hiện phân tích các dấu hiệu được phản hồi về từ các thiết bị.
    - Sử dụng thông tin đó, Shodan có thể cho bạn biết những thứ như máy chủ web (và phiên bản) nào phổ biến nhất hoặc có bao nhiêu máy chủ FTP ẩn danh tồn tại ở một vị trí cụ thể, hay trả về danh sách các camera có thể truy cập trực tuyến qua internet.
    - Nói chung, với shodan bạn có thể tìm kiếm bất cứ thiết bị nào trên internet miễn là chúng đang có kết nối internet và mở cổng public.
    - Shodan được sử dụng hiệu quả trong việc kiểm thử bảo mật các thiết bị IOT (Internet Of Thing) qua việc phát hiện nhanh chóng các thiết bị đang trực tuyến và các thiết bị có tồn tại lỗ hổng bảo mật. Shodan hoạt động 24/7 nên dữ liệu của nó luôn được cập nhật một cách nhanh và chính xác nhất.
    - Nguyên lý hoạt động của Shodan: Shodan (Sentient Hyper-Optimized Data Access Network) hoạt động theo thuật toán sau:
      * Tạo một địa chỉ IPv4 (IPV4 là gì) 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 gì.
      * Lặp lại quá trình trên nhưng với ip và port mới.
    - Điều này giúp tạo ra sự ngẫu nhiên cũng như đảm bảo tránh gây ra lượng kết nối quá lớn tới một thiết bị một cách liên tục.
    - Các cổng dịch vụ mà shodan thường xuyên rà quét: (Port 554 – Real Time Streaming Protocol, Port 5060 – SIP, Port 25 – SMTP, Port 161 – SNMP, Port 23 – Telnet, Port 993 – IMAP, Port 22 – SSH, Port 21 – FTP, Ports 8443, 443,

8080, and 80 – HTTPS/HTTP)

* + - Tìm kiếm từ khóa trên Shodan: Nhập từ khóa cần tìm kiếm vào search box của Shodan, ví dụ Apache city:hanoi 200 OK. Kết quả trả về là các máy chủ Apache public tại Hà Nội và kèm theo các thông tin sau:

A screenshot of a computer

Description automatically generated

* + - * Total Results: số lượng kết quả
      * Results map: bản đồ mật độ các khu vực trên thế giới có kết quả phù hợp
      * Top ports: Top các cổng dịch vụ đang mở
      * Top Operation System: Top các hệ điều hành sử dụng….
      * Top Countries: Top các nước sử dụng tương ứng…
    - Tìm kiếm trên Shodan có phải là phạm pháp?
      * Shodan là công cụ tìm kiếm nguy hiểm, đáng sợ nhất thế giới.
      * Từ góc độ của người dùng, một công cụ tìm kiếm cung cấp những thông chi tiết và sâu và các thiết bị hay một số thông tin riêng tư.
      * Tuy nhiên, Shodan hoàn toàn hợp pháp và không vi phạm luật. Về bản chất, shodan chỉ thu thập dữ liệu đã có sẵn trên internet và shodan chỉ đơn giản là báo cáo những gì nó tìm thấy.
    - Ứng dụng của Shodan trong kiểm thử bảo mật: Pen Testing Ethics, Pen Testing Application và Pen Testing HTTP Status Code
      * Đối với Pen Testing Ethics: Shodan được sử dụng để xem hoặc thay đổi cấu hình các thiết bị hay server mà không yêu cầu xác thực hoặc sử dụng tài khoản và mật khẩu mặc định, thay đổi cáu hình các thiết bị sử dụng chung hoặc lộ tài khoản/ mật khẩu.
      * Đối với Pen Testing Application: Kiểm tra xâm nhập các ứng dụng trên thiết bị hay server sử dụng các yếu tố: mã code HTTP trả về, các thông tin banner, foot printing của dịch vụ, phiên bản của dịch vụ và các cổng dịch vụ đang mở.
      * Đối với Pen Testing HTTP Status Code: Tìm kiếm dựa trên phản hồi của server: 200 OK, 401 Unauthorized, 403 Forbidden…

# Google Hacking và sự ảnh hưởng của nó tới quyền riêng tư

* + - Hiện nay Google là công cụ tìm kiếm trên Internet được sử dụng nhiều nhất ở thời điểm hiện tại.
    - Bằng cách sử dụng công cụ tìm kiếm Google, tội phạm mạng có thể thu được những thông tin có giá trị. Sau đó, dựa trên dữ liệu này, họ có thể thực hiện các cuộc tấn công và chuẩn bị cho chúng một cách hiệu quả hơn.
    - Google Hacking có thể được định nghĩa là một kỹ thuật máy tính sử dụng các toán tử hoặc lệnh để lọc thông tin mà chúng tôi nhận được từ công cụ tìm kiếm Google. Nó cũng 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.
    - Các toán tử cơ bản và quan trọng của Google Hacking
      * “”: Hiển thị kết quả chứa cụm từ chính xác mà người dùng đã viết.
      * \*: Sử dụng như một ký tự đặc biệt, từ đơn.
      * intitle hoặc allintitle: để nhận kết quả có chứa từ trong tiêu đề.
      * inurl hoặc allinurl: hiển thị kết quả có chứa từ trong url.
      * filetype: it được sử dụng để tìm kiếm các tệp bằng cách đặt phần mở rộng. Kết hợp với các từ khóa như chúng ta đã thấy trước đó, nó sẽ cải thiện kết quả tìm kiếm.
    - Sự nguy hiểm của Google Hacking và ảnh hưởng của nó tới người dùng:
      * Ngày nay IOT (Internet of Things) càng ngày càng phát triển, tự động hóa gia đình và nhiều hơn nữa được kết nối với Internet. Vấn đề mà họ gặp phải là chúng bị xử lý bởi những người không có đủ kiến thức hoặc các thiết bị này không được trang bị các biện pháp bảo mật cần thiết.
      * Các hacker dễ dàng tìm thấy các lỗ hổng như mật khẩu , cấu hình và thiết bị do ít được cập nhật nên ngày càng trở nên không an toàn => sử dụng để tấn công vào camera, an ninh….
      * Tìm kiếm các máy chủ lỗi thời và dễ bị tấn công.
      * Thực hiện tìm kiếm thông người dùng và mật khẩu của các trang web, server và database.

# Nội dung thực hành

# Thử nghiệm với Shodan

* + - Vào website shodan, tiến hành tạo tài khoản và đăng nhập

A screenshot of a computer

Description automatically generated

* + - Giao diện của Shodan sau khi đăng nhập thành công
    - A screenshot of a computer

      Description automatically generated with medium confidence

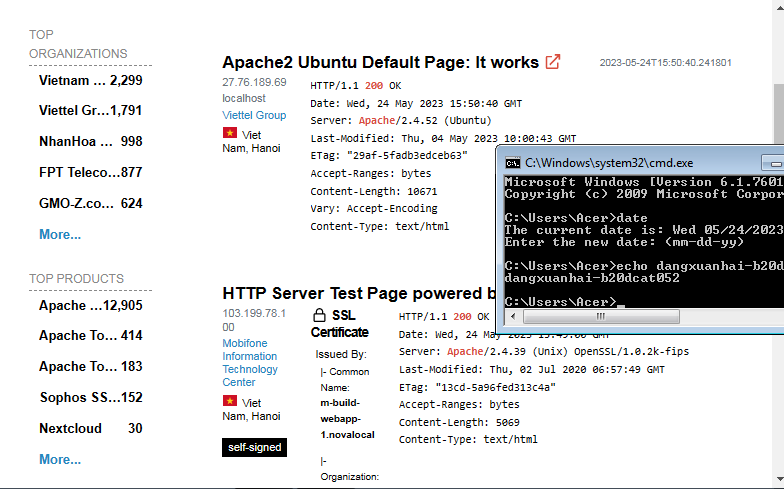
# Tìm hiểu và thử nghiệm các bộ lọc trong danh sách:<https://beta.shodan.io/search/filters>

* + - Tìm các web server chạy Apache tại thành phố Hà Nội, 200 OK thể hiện các website trả về response code 200

*Apache city:hanoi 200 OK*

A screenshot of a computer

Description automatically generated



* + - Tìm kiếm các thiết bị hoặc server đang mở cổng telnet 23 tại Việt Nam

*port:23 country:vn*

*A screenshot of a computer

Description automatically generated*

# Tìm hiểu và thử nghiệm các ví dụ trong danh sách:<https://beta.shodan.io/search/examples>

* + - Giao diện chính

A screenshot of a computer

Description automatically generated with medium confidence

* + - Dịch vụ SSL đã được cấp chứng chỉ cho \*.google.com

*ssl.cert.subject.cn:google.com*

*A screenshot of a computer

Description automatically generated with medium confidence*

*A picture containing text, screenshot, software, web page

Description automatically generated*

* + - Tìm kiếm các máy tính từ xa bị nhiếm ransomware và có tính năng nhận dạng ký tự quang học (OCR)

*has\_screenshot:true encrypted attention*

A screenshot of a computer

Description automatically generated with medium confidence

# Tìm hiểu và thử nghiệm các ví dụ trong danh sách:<https://help.shodan.io/the-basics/search-query-fundamentals>

* + - Giao diện chính:

# A screenshot of a computer Description automatically generated

* + - Tìm kiếm thiết bị Moxa Nports

A screenshot of a computer

Description automatically generated

# Tìm hiểu và thử nghiệm các ví dụ trong danh sách:<https://www.yeahhub.com/shodan-search-examples/>

* + - Tìm kiếm Apache Server ở San Francisco

*apache city:”San Francisco”*

A picture containing text, screenshot, software, web page

Description automatically generated

* + - Tìm kiếm Nginx Server ở Australia

*nginx country:”AU”*

*A screenshot of a computer

Description automatically generated*

* + - Tìm kiếm Google Web Server (GWS)

*“Server:gws” hostname:”google”*

A screenshot of a computer

Description automatically generated with medium confidence

# Tìm hiểu và thử nghiệm các ví dụ trong danh sách: [https://www.yeahhub.com/find-vulnerable-webcams-shodan-metasploit- framework/](https://www.yeahhub.com/find-vulnerable-webcams-shodan-metasploit-framework/)

* + - Sử dụng công cụ metasploit framework để tìm webcam trên Shodan
    - A screenshot of a computer

      Description automatically generated
    - Tìm kiếm các lỗ hổng liên quan tới shodan

*search shodan*

*A screenshot of a computer

Description automatically generated*

* + - Khai báo sử dụng modun tấn công

*use auxiliary/gather/shodan\_search*

A screenshot of a computer

Description automatically generated with medium confidence

* + - Chạy lệnh “show option” để xem các thông tin về mô đun đang sử dụng.

A screenshot of a computer

Description automatically generated

* + - Mở Shodan, vào phần Account, lấy API Key

A picture containing text, screenshot, font, number

Description automatically generated

* + - Vào lại metasploit, thiết lập API Key set SHODAN\_APIKEY <api\_key>

A screenshot of a computer

Description automatically generated with medium confidence

* + - Thiết lập Query tìm kiếm

*set QUERY “webcamxp”*

*A screenshot of a computer

Description automatically generated with medium confidence*

* + - Thực thi tấn công bằng lệnh “run”

A screenshot of a computer

Description automatically generated

* + - Tiến hành truy cập vào bất kỳ 1 webcam nào đó

A screenshot of a computer

Description automatically generated with medium confidence

A screen shot of a computer

Description automatically generated with medium confidence

* + - Mở shodan, sử dụng thanh tìm kiếm của shodan để tìm webcam webcamxp country:US

A screenshot of a computer

Description automatically generated with medium confidence

# Thử nghiệm với Google Hacking Database

* + - Truy cập vào website [www.exploit-db.com/google-hacking-database](http://www.exploit-db.com/google-hacking-database)

A screenshot of a computer

Description automatically generated with medium confidence

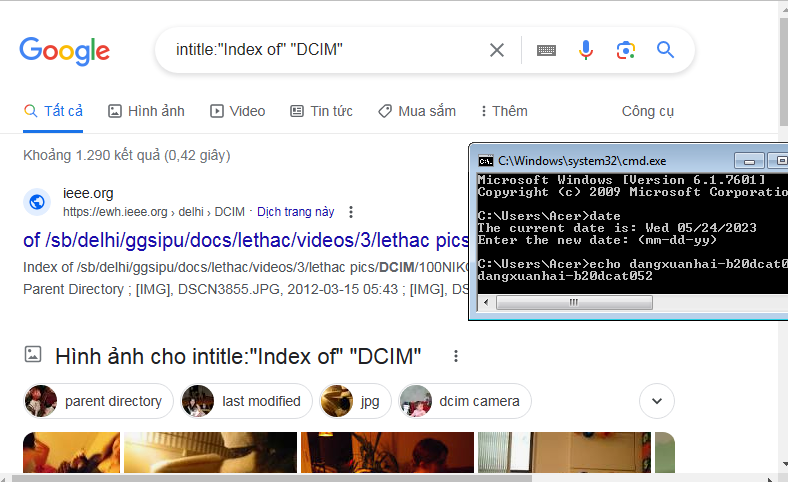
* + - Tại nút Filters bên trái bao gồm các mục Footholds, File Containing Usernames, Sensitive Directory, Web Server Detection…
    - Chọn một mục bất kỳ để hiện ra trang thông tin liên quan bao gồm thông tin tác giả, mô tả về tìm kiếm và các thông tin khác.

A screenshot of a computer

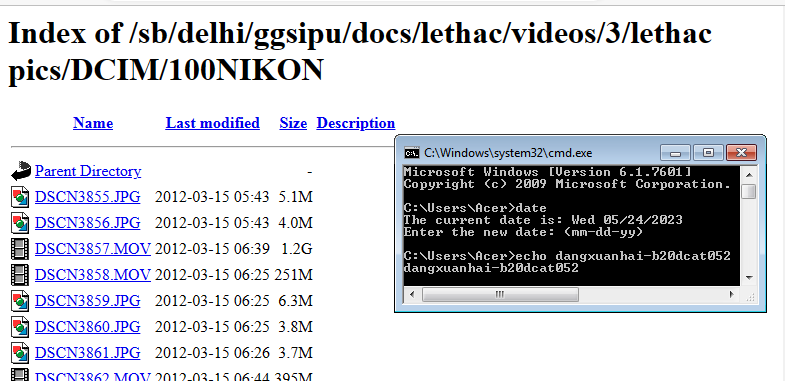
Description automatically generated with medium confidence

* + - Tiến hành thử nghiệm với một ví dụ: [www.exploit-db.com/ghdb/4057](http://www.exploit-db.com/ghdb/4057)
    - A screenshot of a computer

      Description automatically generated
    - Tìm kiếm với truy vấn intitle:”Index of” “DCIM”
      * Từ khóa intitle: giúp google giới hạn kết quả tìm kiếm về những trang có chứa từ khóa đó trong tiêu đề.
      * DCIM (Digital Camera Image) là tên thư mục trong Quy tắc thiết kế cho hệ thống tệp máy ảnh, là một phần của hệ thống tệp máy ảnh kỹ thuật số.



Kết quả trả về 1 bộ sưu tập ảnh mà mọi người không biết ở đó



* + - Tìm hiểu lệnh (còn gọi là Google dork) tại [www.exploit-db.com/ghdb/6322](http://www.exploit-db.com/ghdb/6322) để tìm các từ khóa SSH

A computer screen shot of a computer screen

Description automatically generated with low confidence

Tìm kiếm truy vấn intitle: “index of””id\_rsa.pub”

A screenshot of a computer

Description automatically generated

Click vào 1 kết quả để xem A picture containing text, screenshot, software, web page

Description automatically generated

* + - Tìm hiểu Google dork tại [www.exploit-db.com/ghdb/6412](http://www.exploit-db.com/ghdb/6412) tìm log có tên người dùng và mật khẩu, có thể có các mục như địa chỉ email, URL những thông tin đăng nhập này được sử dụng…..

A screenshot of a computer

Description automatically generated

Tìm kiếm truy vấn allintext:username,password filetype:log

A picture containing text, electronics, screenshot, software

Description automatically generated

Click vào một dòng để xem kết quả

A screenshot of a computer

Description automatically generated

* + - Quay lại GHDB ([www.exploit-db.com/google-hac](http://www.exploit-db.com/google-hac)king-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).

A screenshot of a computer

Description automatically generated with medium confidence

Chọn một mục bất kỳ

A picture containing text, screenshot, software, web page

Description automatically generated

Tìm kiếm truy vấn

A picture containing text, electronics, screenshot, software

Description automatically generated

Click vào để xem kết quả

A screenshot of a computer

Description automatically generated with medium confidence

* + - Tìm kiếm với một số loại google dork khác Xem thư mục liên quan tới “mysql”

A screenshot of a computer

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated with medium confidence

A picture containing text, font, software, web page

Description automatically generated

Xem log của máy chủ FTP

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated with medium confidence

` \

Những nguy hiểm của google dork:

* + - * Kẻ tấn công có thể thực hiện tìm kiếm các máy chủ lỗi thời và dễ bị tấn công, thực hiện tìm kiếm thông tin người dùng và mật khẩu các trang web, server và database, các log của các server, các tài liệu mật như thông tin tài khoản và mật khẩu của người dùng, các tài liệu mật của các cơ quan, tổ chức, chính phủ, quân đội…. để thực hiện cho mục đích xấu.

# Tài liệu tham khảo

* + - [Google Hacking và sự ảnh hưởng của nó tới quyền riêng tư (viblo.asia)](https://viblo.asia/p/google-hacking-va-su-anh-huong-cua-no-toi-quyen-rieng-tu-4dbZNRkgZYM)
    - [Shodan - Công cụ tìm kiếm cho kiểm thử bảo mật (viblo.asia)](https://viblo.asia/p/shodan-cong-cu-tim-kiem-cho-kiem-thu-bao-mat-924lJJD0lPM)