BÁO CÁO THỰC HÀNH

**Môn học: An toàn Mạng**

**Kỳ báo cáo: Buổi 02 (Session 02)**

**Tên chủ đề: Thu thập thông tin**

*GVHD: Nghi Hoàng Khoa*

*Ngày báo cáo: 31/10/2023*

**Nhóm: 07 (ghi số thứ tự nhóm)**

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT140.O11.ANTN.1

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Phạm Ngọc Thơ | 21522641 | 21522641@gm.uit.edu.vn |
| 2 | Hà Thị Thu Hiền | 21522056 | 21522056@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Ở lớp: Câu 1 | 100% |
| 2 | Câu 2 | 100% |
| 3 | Câu 3 | 100% |
| 4 | Câu 4 | 100% |
| 5 | Câu 5 | 100% |
| 6 | Câu 6 | 100% |
| 7 | Câu 7 | 100% |
| 8 | Câu 23 | 100% |
| 9 | Câu 24 | 100% |
| 10 | Câu 30 | 100% |
| 11 | Về nhà: Câu 8 | 100% |
| 12 | Câu 9 | 100% |
| 13 | Câu 10 | 100% |
| 14 | Câu 11 | 100% |
| 15 | Câu 12 | 100% |
| 16 | Câu 13 | 100% |
| 17 | Câu 14 | 100% |
| 18 | Câu 15 | 100% |
| 19 | Câu 16 | 100% |
| 20 | Câu 17 | 100% |
| 21 | Câu18 | 100% |
| 22 | Câu 19 | 0% |
| 23 | Câu 20 | 0% |
| 24 | Câu 21 | 0% |
| 25 | Câu 22 | 0% |
| 26 | Câu 25 | 100% |
| 27 | Câu 26 | 100% |
| 28 | Câu 27 | 100% |
| 29 | Câu 28 | 100% |
| 30 | Câu 29 | 100% |
| 31 | Câu 31 | 100% |
| 32 | Câu 32 | 100% |
| 33 | Câu 33 | 100% |
| 34 | Câu 34 | 100% |
| 35 | Câu 35 | 100% |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

**Phần ở lớp:**

## Câu 1: Từ trang web của MegaCorp One, hãy mô tả một chút về lĩnh vực hoạt động của công ty?

Cty MegaCorp One hoạt động chủ yếu trong ngành công nghệ nano, cung cấp các sản phẩm có sử dụng công nghệ nano trong lĩnh vực y tế, điện tử và thương mại. Công nghệ nano được sử dụng trong y học để tái tạo tế bào cho đến các ứng dụng quân sự để chế tạo vũ khí thông minh.

Các dịch vụ mà MegaCorp One cung cấp bao gồm: tái tạo tế bào, bổ sung hệ thống miễn dịch, sửa chữa điều khiển máy vi mô, bộ xử lý nano,...

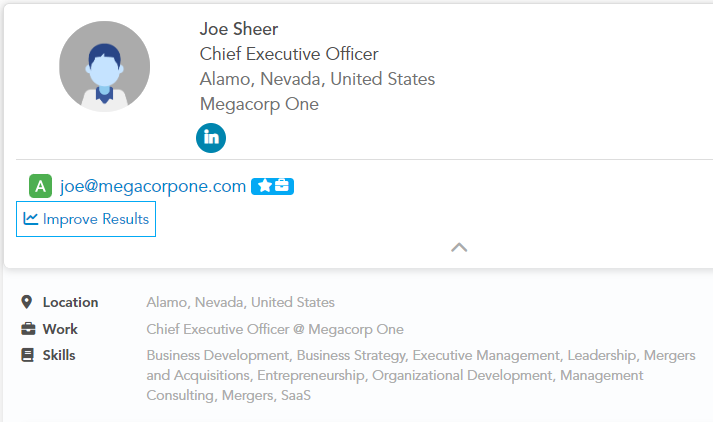
## Câu 2: Hãy liệt kê những thành viên đang làm việc cho MegaCorp One và một vài thông tin về những thành viên đó (địa chỉ email, chức vụ, tài khoản mạng xã hội)?

Tại trang thông tin của cty, hiển thị thông tin cơ bản của 4 nhân viên:

* Joe Sheer
* Địa chỉ email: [joe@megacorpone.com](mailto:joe@megacorpone.com)
* Chức vụ: Chief Exxecutive Officer
* Tài khoản mạng xã hội (twitter): <https://twitter.com/joe_sheer/>
* Tom Hudson
* Địa chỉ email: [thudson@megacorpone.com](mailto:thudson@megacorpone.com)
* Chức vụ: Web designer
* Tài khoản mạng xã hội (twitter): https://twitter.com/TomHudsonMCO
* Tanya Rivera
* Địa chỉ email: [trivera@megacorpone.com](mailto:trivera@megacorpone.com)
* Chức vụ: Senior Developer
* Tài khoản mạng xã hội (twitter): <https://twitter.com/TanyaRiveraMCO>
* Matt Smith
* Địa chỉ email: [msmith@megacorpone.com](mailto:msmith@megacorpone.com)
* Chức vụ: Marketing director
* Tài khoản mạng xã hội (twitter): <https://twitter.com/MattSmithMCO>

## Câu 3: Khi có được địa chỉ Email của các thành viên thuộc tổ chức, bạn có phát hiện ra được điều gì?

Sau khi có được email, có thể tìm thấy được thêm một số thông tin về các thành viên, thông qua RocketReach như chuyên môn, nơi sinh sống:



Đồng thời, từ email, có thể tra cứu để xem được nhiều thông tin hơn trên các nền tảng khác nhau.

## Câu 4: Sử dụng công cụ whois để xác định các name server của MegaCorp One

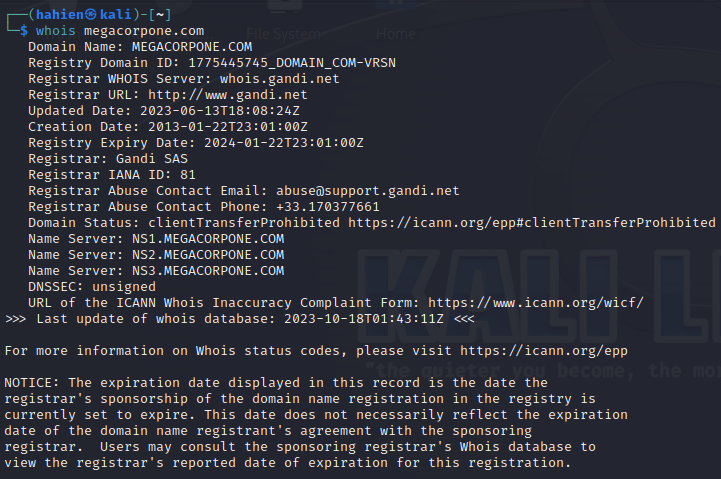
## Tài nguyên: gõ lệnh trên kali

* whois megacorpone.com

## Mô tả/mục tiêu: xác định các name server của MegaCorp One

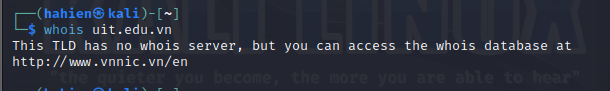
## Các bước thực hiện/ Phương pháp thực hiện (Ảnh chụp màn hình, có giải thích)

* Name server của MegaCorp One là:
  + NS1.MEGACORPONE.COM
  + NS2.MEGACORPONE.COM
  + NS3.MEGACORPONE.COM

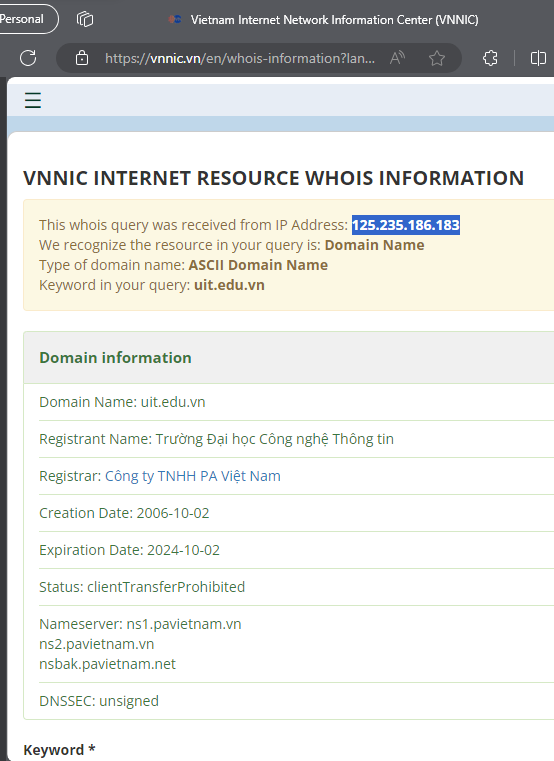


## Câu 5: **Sử dụng công cụ whois để tìm kiếm các thông tin của trường Đại học Công ng**hệ Thông tin (uit.edu.vn) có được không? Giải thích?

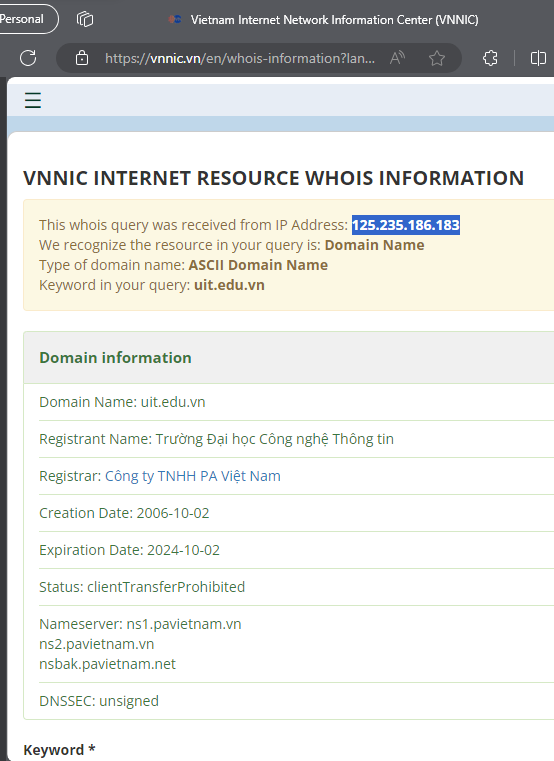
* Không thể sử dụng công cụ whois trực tiếp để tìm kiếm thông tin của trường Đại học Công nghệ Thông tin (uit.edu.vn) vì tên miền này sử dụng TLD (Top-Level Domain) mà không có máy chủ whois chính thức. Tuy nhiên, có thể truy cập cơ sở dữ liệu whois của tên miền này tại http://www.vnnic.vn/en để tìm kiếm thông tin liên quan đến nó.
* Ban đầu, khi ta gõ “whois uit.edu.vn” thì kali sẽ hiện thông báo như sau cho biết rằng TLD này không có máy chủ whois nhưng có thể truy cập qua cơ sở dữ liệu của whois.



* Tiếp đến ta truy cập vào <http://www.vnnic.vn/en> và tìm kiếm domain name là “uit.edu.vn”



## Câu 6: Thu thập thông tin về tên miền uit.edu.vn và hãy cho biết các thông tin như:



## a. Ngày đăng ký tên miền: 2/10/2006

## b. Ngày hết hạn tên miền: 2/10/2024

## c. Chủ sở hữu tên miền: Trường Đại học Công nghệ Thông tin

## d. Các name server của tên miền:

## - ns1.pavietnam.vn - ns2.pavietnam.vn - nsbak.pavietnam.net

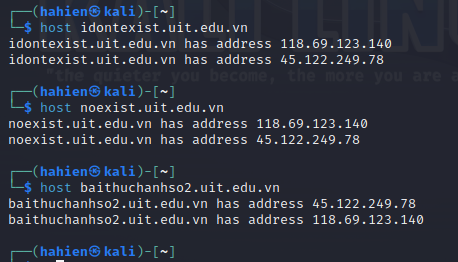
## Câu 7: Ai là Phó chủ tịch Pháp lý (Vice President of Legal) của MegaCorp One và địa chỉ email của họ là gì?

## Tài nguyên: tìm kiểm với “vice president email site:megacorpone.com”.

* Kết quả tên và email được tìm thấy như trên hình:



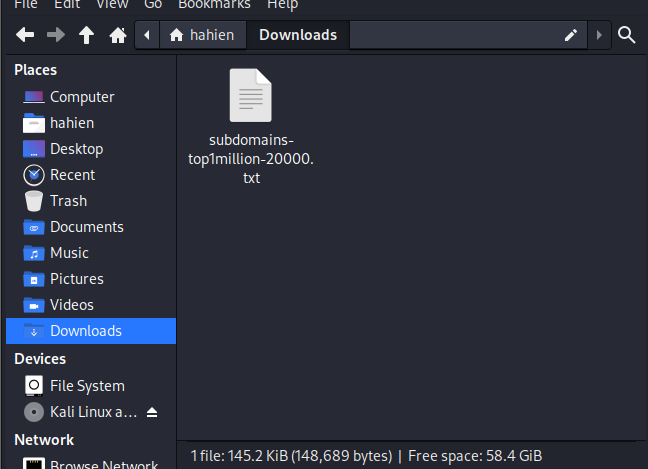
## Câu 23: Sử dụng lệnh host cho các hostname không tồn tại trong tên miền uit.edu.vn (idontexist, noexist, baithuchanhso2). Có nhận xét gì về kết quả trả về hay không? Giải thích?



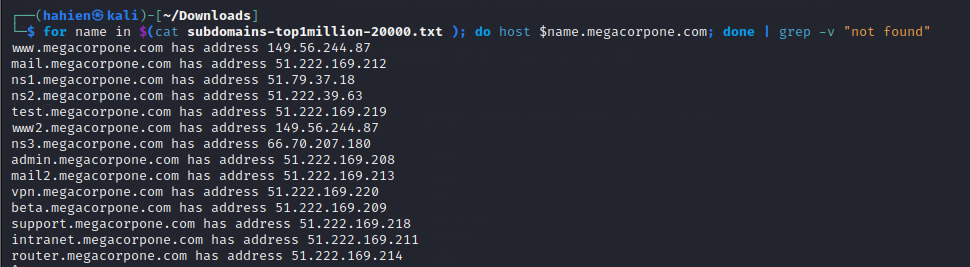
* Kết quả trả về khi sử dụng lệnh host cho các hostname không tồn tại trong tên miền uit.edu.vn (idontexist, noexist, baithuchanhso2) gây ngạc nhiên bởi việc nó trả về các địa chỉ IP. Lý giải:
  + **idontexist.uit.edu.vn và noexist.uit.edu.vn:**
    - Cả hai hostname này đều trả về hai địa chỉ IP: 118.69.123.140 và 45.122.249.78.
    - Điều này không phải là hiện tượng thực sự, mà là kết quả của một số tên miền mặc định trả về các địa chỉ IP không hợp lệ hoặc giả mạo. Có thể người quản trị hệ thống hoặc DNS server đã cấu hình tên miền này để tránh lộ thông tin thực sự hoặc để bắt đầu đầu tư tại các địa chỉ IP mà họ không muốn tiết lộ.
  + **baithuchanhso2.uit.edu.vn:**
    - Cũng giống như hai hostname trước, hostname này cũng trả về hai địa chỉ IP: 45.122.249.78 và 118.69.123.140.
    - Hiện tượng này có thể do cùng một lý do như ở trên, và việc xáo trộn hoặc ngẫu nhiên việc trả về địa chỉ IP cho các tên miền không tồn tại.

## Câu 24: Sử dụng wordlist thông dụng khác (rockyou, seclists) để tìm kiếm các hostname hợp lệ khác của megacorpone.com

* Tải seclist về:



* Chạy lệnh để xem kết quả:

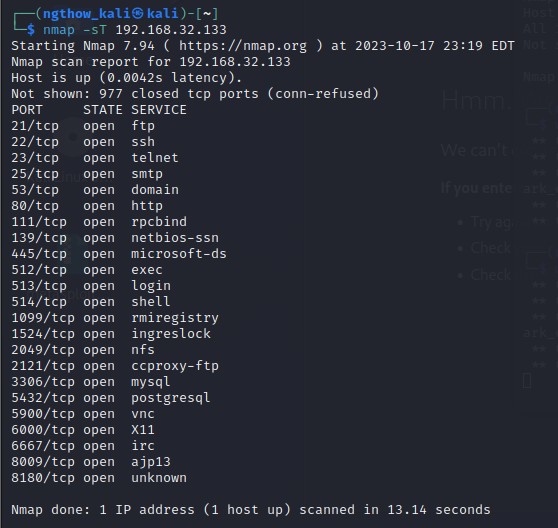


## Câu 30: Thực hiện bắt Wireshark để mô tả cách gói tin được gửi và nhận khi thực hiện TCP Connect Scan sử dụng Nmap.

* Kiểm tra địa chỉ IP để nmap đến:



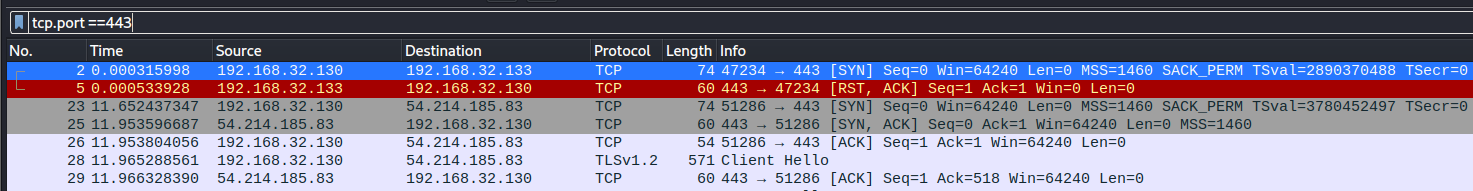
* Trên máy ảo, thực thi câu lệnh **nmap -sT 192.168.32.133**:



* Đồng thời, mở wireshark để bắt gói tin, tại port 80 được kết quả như sau:

Gói tin gửi đi với Seq=0, nhận được phản hồi ACK tức là nhận thành công gói tin. Do đó, có thể kết luận port 80 đang mở.

Tiếp tục xét tại port 443, kết quả như sau:

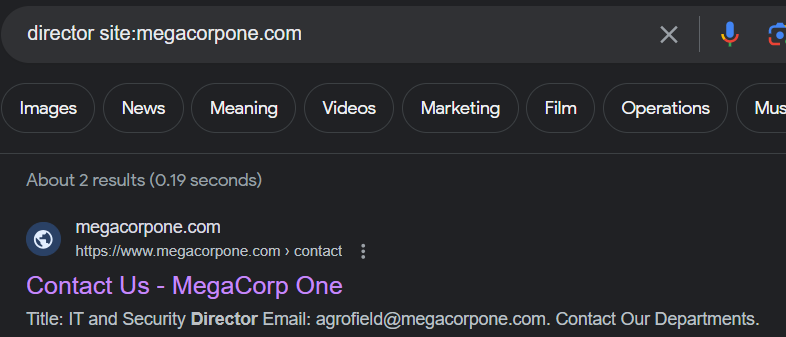


Phản hồi RST (reset) thể hiện máy chủ TCP đang bị đóng lại hoặc ngắt kết nối, tức là cổng 443 không được mở.

**Phần về nhà:**

**Câu 8: Bạn có thể tìm kiếm thêm các nhân viên khác của MegaCorp One mà không được liệt kê trên trang web** [**www.megacorpone.com**](http://www.megacorpone.com)**?**

Có thể, khi tìm kiếm với *director site:megacorpone.com****,***  kết quả hiển thị thông tin về IT and security Director - người không được liệt kê trên trang web:





**Câu 9: Liệt kê một vài từ khóa thường gặp trên Google và cho ví dụ? (Yêu cầu: ít nhất 5 từ khóa).**

Tùy thuộc vào xu hướng và mục đích của người dùng Google mà từ khóa thường gặp sẽ khác nhau. Tuy nhiên, một vài từ khóa có thể sẽ được tìm kiếm nhiều trên Google là:

* Tên các tài khoản mạng xã hội.

VD: Facebook, YouTube, Instagram…

* Công cụ dịch thuật:

VD: Google translate, …

* Thời tiết.

VD: Nhiệt độ hôm nay, dự báo thời tiết ngày XX/YY/2023, …

* Các trang thương mại điện tử:

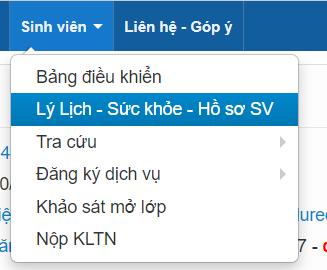
VD: Lazada, Shoppe, Taobao, Tiki, …

* How to: cách dùng phổ biến để tìm kiếm một sự hướng dẫn trên Google

VD: how to cook omelette, how to learn Python, ...

**Câu 10: Thực hiện tìm kiếm các tài liệu thú vị của Trường Đại học Công nghệ Thông tin mà được công bố trên Internet mà theo bạn là không nên được công bố?**

Những thông tin cá nhân như lý lịch, sức khỏe, hồ sơ của sinh viên, … là các thông tin không nên được công bố:



Mức độ công bố ở đây không phải với tất cả mọi người mà với 1 hoặc 1 nhóm người như giảng viên, các phòng ban có liên quan hoặc cán bộ cần thông tin để xét học bổng, thành tích cho sinh viên đó. Thông tin cá nhân chỉ sinh viên mới có quyền truy cập nhưng thực tế, vẫn có những tài khoản đặc quyền được truy xuất thông tin này.

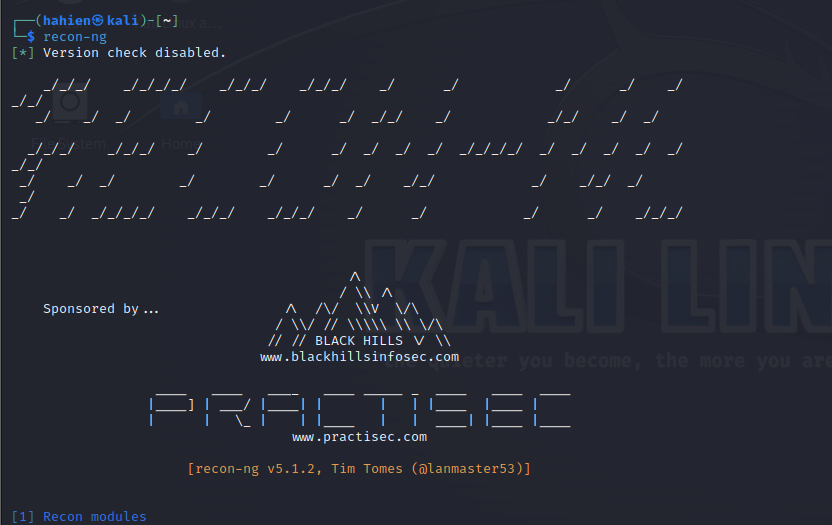
**Câu 11: Sử dụng Netcraft để xác định máy chủ ứng dụng (application server) đang chạy trên** [**www.megacorpone.com**](http://www.megacorpone.com)

Mở “site report” của trang [www.megacorpone.com](http://www.megacorpone.com) để tìm thông tin về máy chủ ứng dụng đang chạy, đó là Apache và Debian:

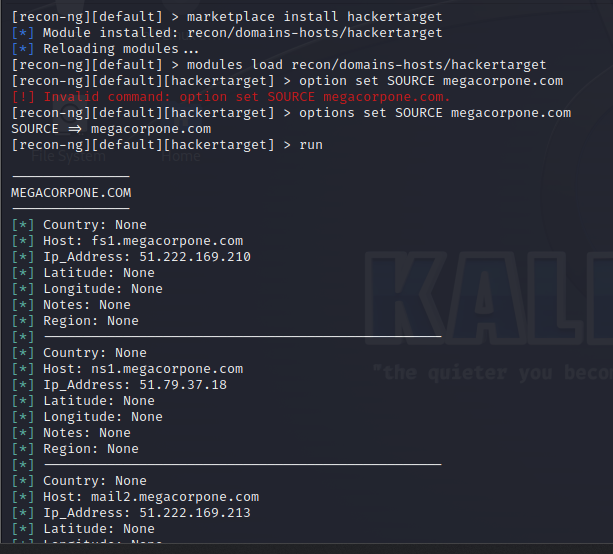


**Câu 12: Thực hiện sử dụng module có thể giúp phân giải tên miền ở Hình 20 thành địa chỉ IP tương ứng.**

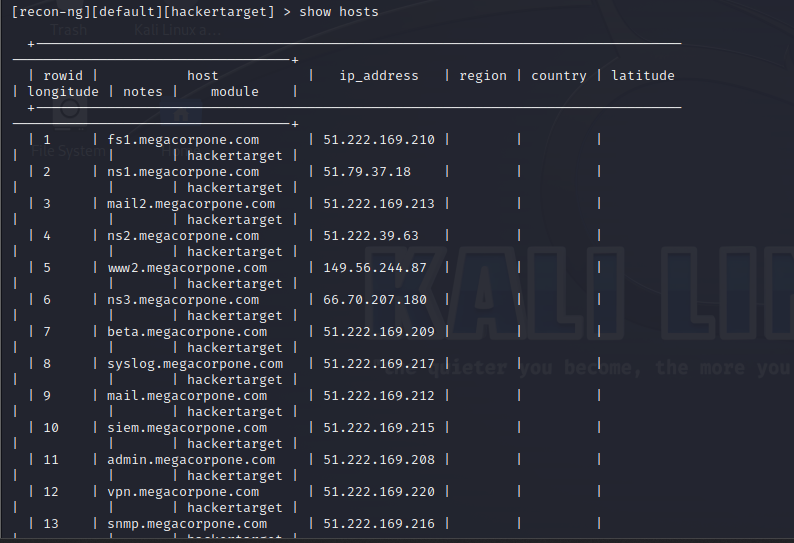
* Module có thể giúp phân giải tên miền: hackertaget.
* Thực hiện các bước khởi động recon-ng



* Install, download module hackertarget
* Load module
* Run

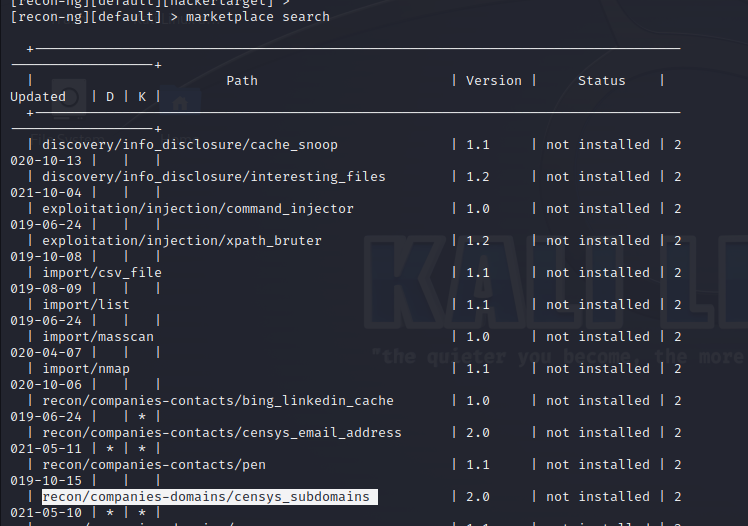


* Show hosts ta thấy được các địa chỉ IP của tên miền:

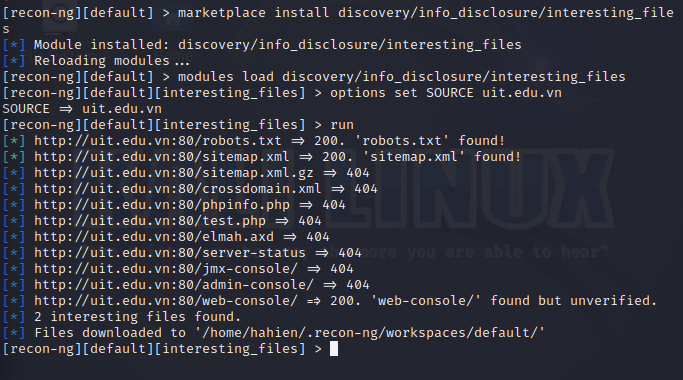


**Câu 13: Sử dụng một số module khác có trong recon-ng để thu thập thông tin về UIT nhiều nhất có thể.**

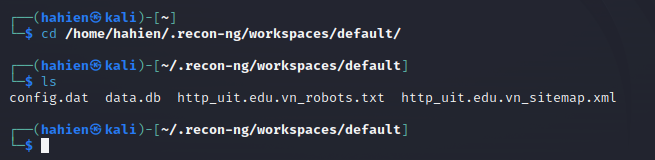
* Search các modules:

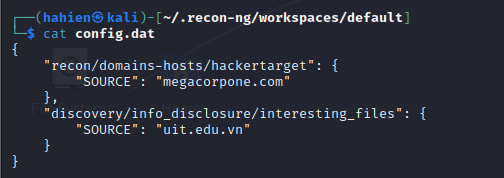


* Install modules “discovery/info\_disclosure/interesting\_files”: được sử dụng để tìm kiếm files quan trọng và tiềm ẩn.

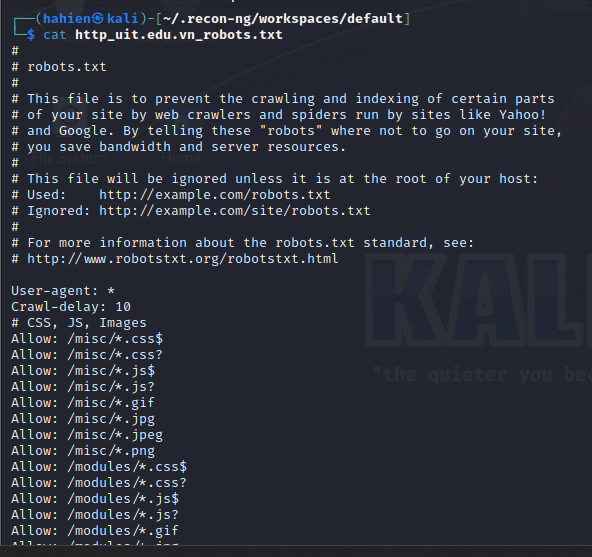
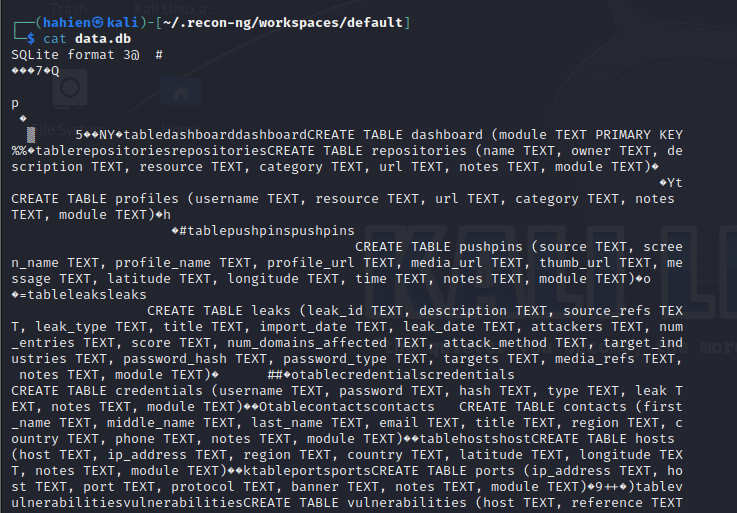


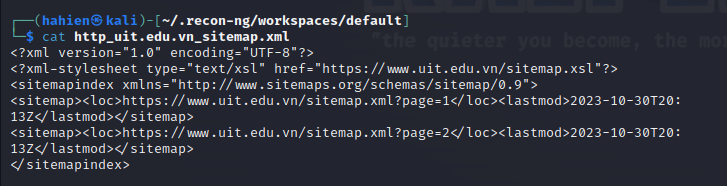
* Files download sẽ ở /home/hahien/.recon-ng/workspaces/default/





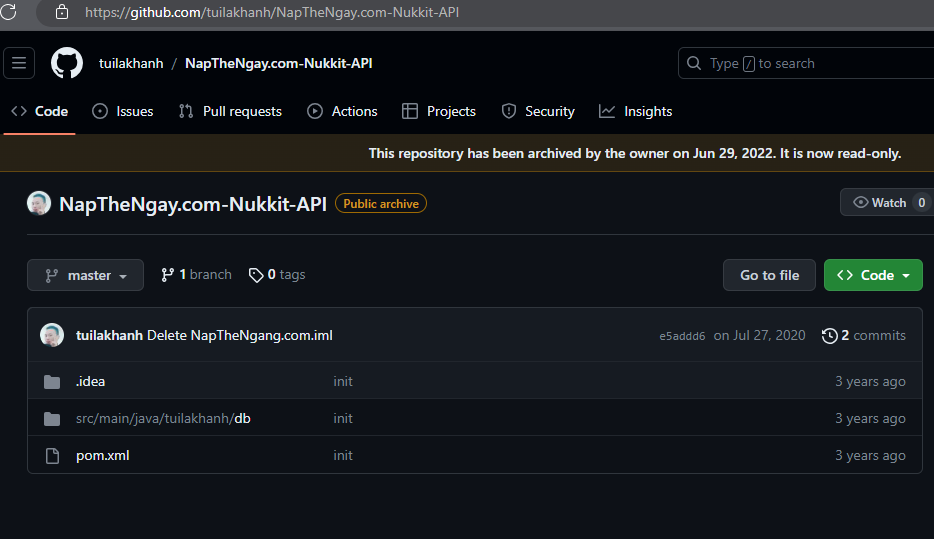
* Cuối cùng, ta xem thông tin từng files

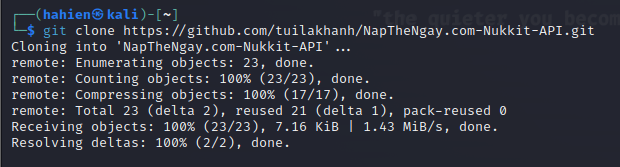




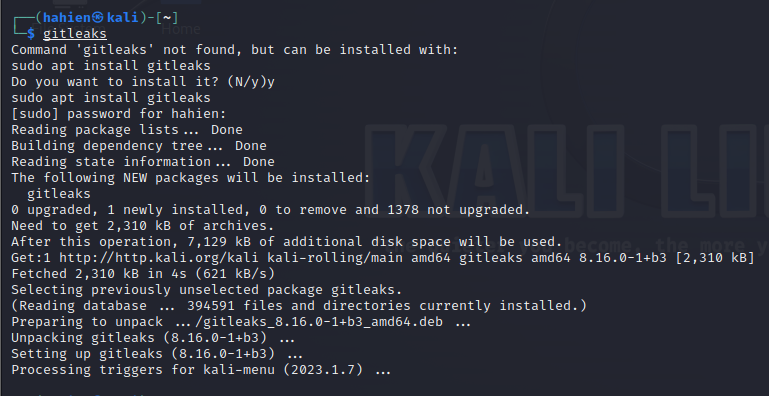
**Câu 14: Sử dụng 1 trong 2 công cụ Gitrob hoặc Gitleaks để tìm kiếm các thông tin nhạy cảm bị rò rỉ đối với các trường đại học thành viên trong ĐHQG.**

* Git clone project này <https://github.com/tuilakhanh/NapTheNgay.com-Nukkit-API.git> về.

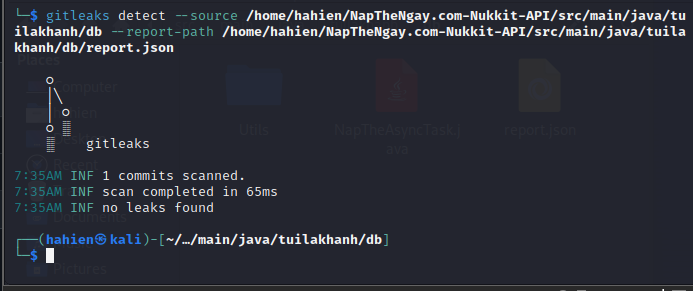


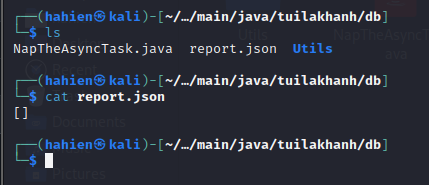


* Install gitleaks.

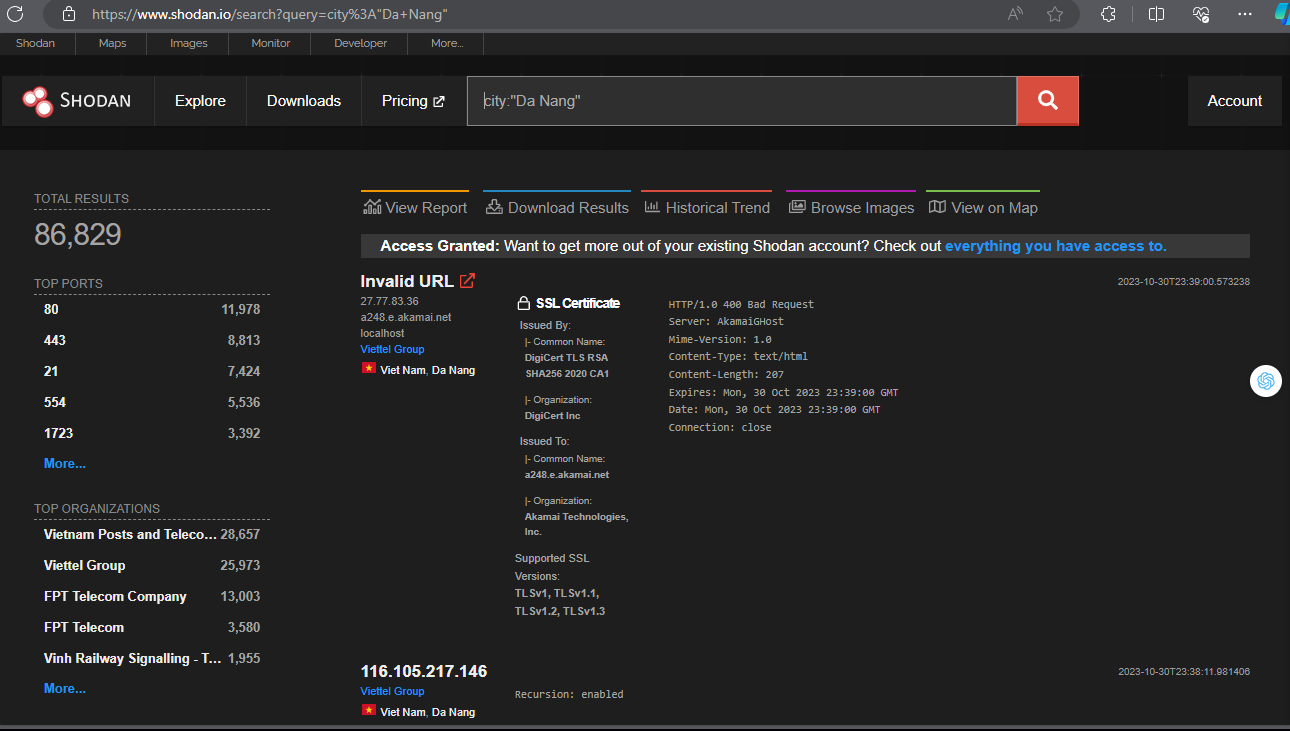


* Sử dụng gitleaks để tìm kiếm các thông tin nhạy cảm bị rò rỉ, nhưng trong đây chưa có lỗ hổng

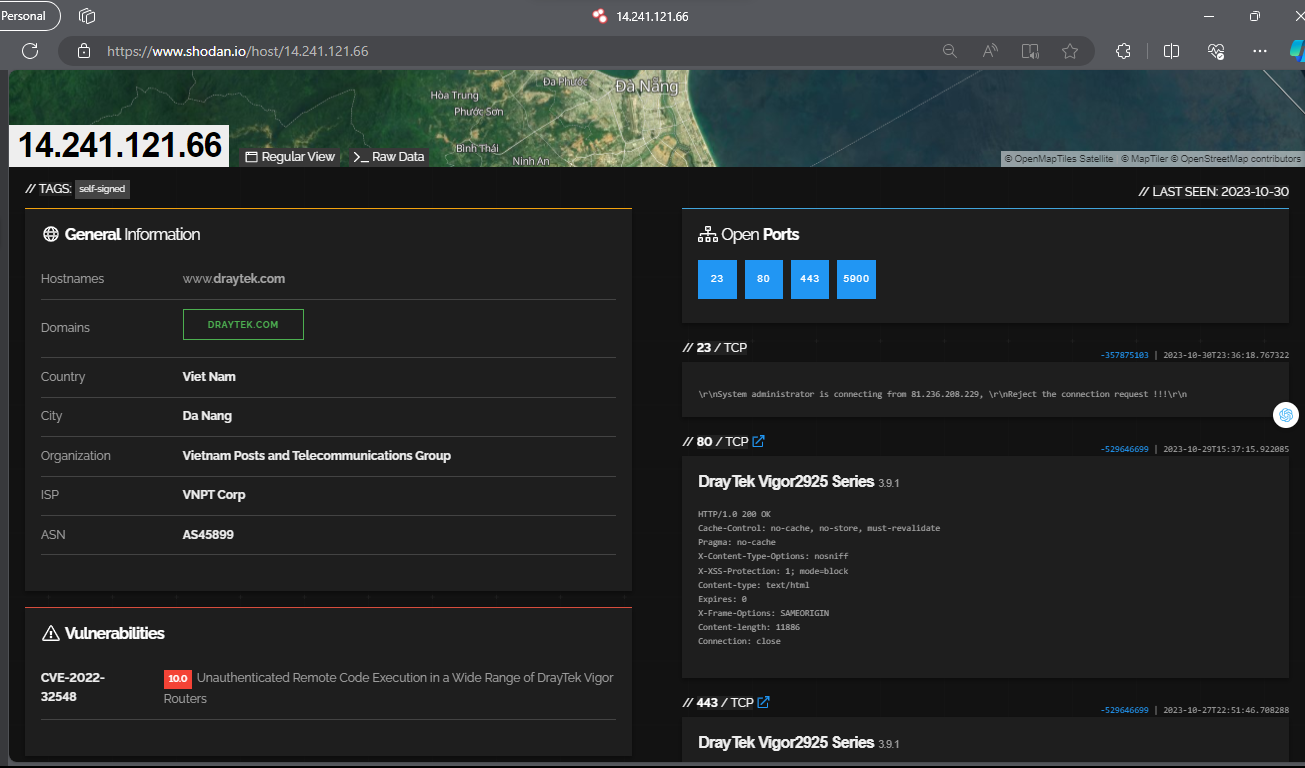




**Câu 15: Thực hiện tìm kiếm các lệnh khác trên Shodan mà có thể tiết lộ thêm nhiều thông tin thú vị về một đối tượng bất kỳ.**



* Bấm random vào 1 địa chỉ Ip, ta thấy Vulnerabilities



**Câu 16: So sánh kết quả tìm kiếm trên Shodan so với các search engine khác như Google, Bing…**

Shodan và các công cụ tìm kiếm khác như Google, Bing có mục đích và cách hoạt động khác nhau.

* Shodan:
* Shodan được thiết kế 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 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.

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.

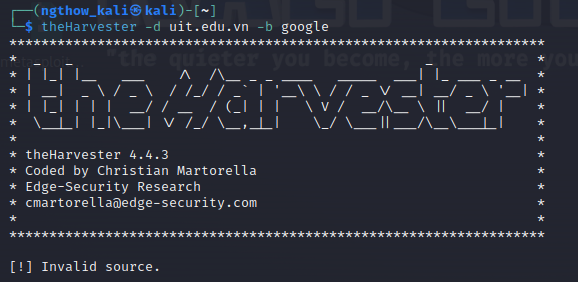
* Google và Bing:
* Google và Bing là công cụ tìm kiếm nội dung trên internet phổ biến nhất.
* Google có lượng tìm kiếm cao hơn so với Bing.

Đối với mua sắm và ngân hàng, Google không cung cấp nhiều tùy chọn. Mặt khác, Bing cung cấp rất nhiều dữ liệu cho các dịch vụ tài chính và bán lẻ.

Vì vậy, Shodan thường được sử dụng trong ngành công nghiệp an ninh mạng, trong khi Google và Bing thường được sử dụng để tìm kiếm thông tin phổ biến trên web. Mỗi công cụ có ưu điểm riêng của mình tùy thuộc vào mục đích sử dụng.

**Câu 17: Sử dụng công cụ theHarvester để lấy tìm kiếm các địa chỉ email của UIT.**

* Khi sử dụng lệnh tìm kiếm trên theHarvester với search engine là google, không hiển thị được kết quả:



Giải thích cho điều này, em sử dụng lệnh **theHarvester –h** nhằm xem những source mà tool sử dụng để lấy data, kết quả như sau:

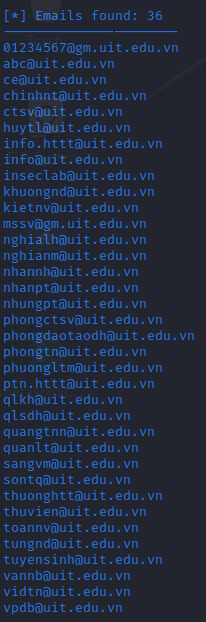


Vẫn hỗ trợ nhiều source nhưng không có google, do đó không thể lấy thông tin trực tiếp từ google. Có thể có cách khác để lấy gián tiếp, nhưng với yêu cầu bài toán này, em sẽ sử dụng **bing** để lấy các địa chỉ email của UIT vì em nghĩ nó vẫn đủ khả năng để lấy được thông tin em cần.

* Sau khi thực thi câu lệnh **theHarvester -d uit.edu.vn -b bing**:



**theHarvester** tìm được 36 emails:



**Câu 18: Sử dụng với nguồn tìm kiếm khác (-b). Theo bạn, kết quả của nguồn nào tốt hơn?**

* Em thực hiện tìm kiếm trên **yahoo**, kết quả hiển thị 21 emails được tìm thấy:
* So với kết quả tìm được từ **bing**, rõ ràng từ **bing** sẽ cho nhiều kết quả hơn **yahoo**.

**Câu 19:**

**Câu 20:**

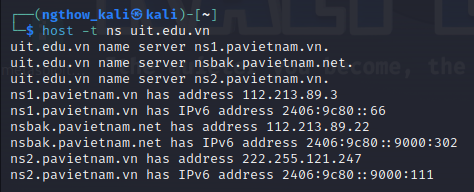
**Câu 21:**

**Câu 22:**

**Câu 25: Viết một chương trình Bash script để liệt kê danh sách các nameserver của các đơn vị thành viên thuộc Đại học Quốc Gia TP.HCM (hcmus.edu.vn, hcmussh.edu.vn, uit.edu.vn, hcmut.edu.vn, hcmiu.edu.vn, uel.edu.vn, hcmier.edu.vn, vnuhcm.edu.vn) và thực hiện zone transfer ứng với các nameserver đã tìm được.**

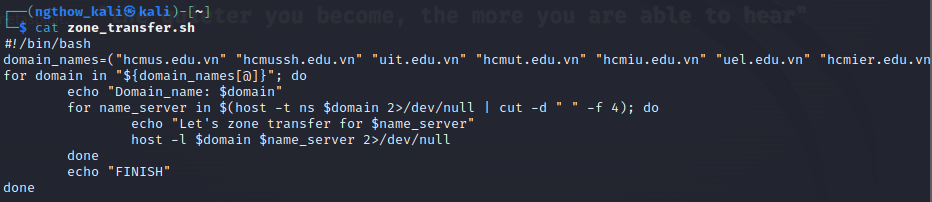
* Để tìm kiếm các nameserver của các đơn vị trường, ví dụ trường UIT, sử dụng lệnh:

**host -t ns uit,edu.vn**



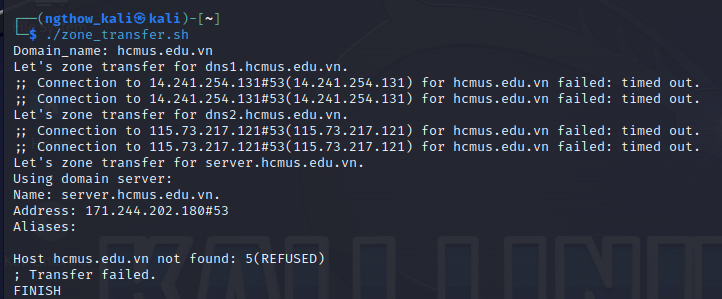
Nameserver sẽ là giá trị tại cột thứ 4 theo cách liệt kê trên.

* Viết chương trình như sau:



Giải thích:

* Trước tiên, tạo danh sách chứa tên các domain cần kiểm tra.
* **for name\_server in $(host -t ns $domain 2>/dev/null | cut -d " " -f 4); do:** chạy vòng lặp duyệt qua tất cả tên miền, chạy lệnh **host –t ns** để lấy nameservers của các trường, cụ thể lấy giá trị tại cột thứ 4 như đã giải thích phía trên.
* **host -l $domain $name\_server 2>/dev/null**: bắt đầu quá trình zone transfer.
* Kết quả:



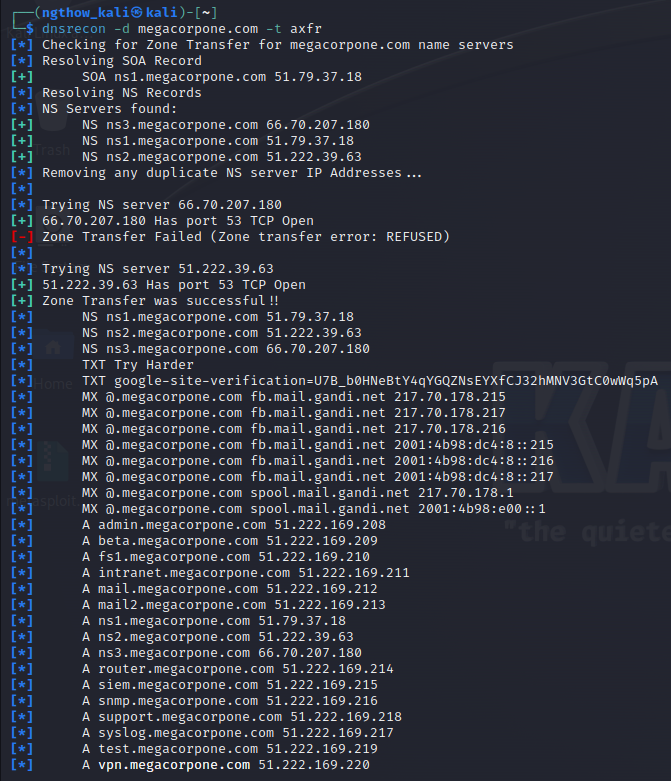
**Câu 26: Viết liệt kê danh sách các loại enumeration có thể được sử dụng cùng với tùy chọn -t.**

Một số loại enumeration có thể được sử dụng với tùy chọn -t là:

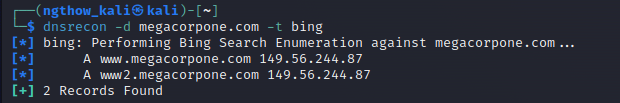
* std (standard): tìm kiếm các bản ghi DNS cơ bản như A, AAA, MX, txt, …
* brute: dùng để tấn công brute-force.
* rvl: ánh xạ IP sang tên miền, dùng để tìm kiếm tên miền dựa trên IP.
* axfr: zone transfer.
* srv (service record): cung cấp thông tin về dịch vụ cung cấp bởi máy chủ.
* bing: sử dụng bing để tìm thông tin liên quan đến tên miền bao gồm loại bản ghi DNS, các trang liên quan đến trang đang tìm.
* yandex: sử dụng yandex - là một công cụ tìm kiếm lớn của Nga.
* tld (top-level domain): cung cấp thông tin về loại tên miền (.com, .org, …).

**Câu 27: Cho một vài ví dụ sử dụng kết hợp các tùy chọn được DNSRecon hỗ trợ khác (ít nhất là 2 ví dụ)**

* Sử dụng kết hợp với tùy chọn **axfr:**



* Sử dụng kết hợp với tùy chọn **bing**:

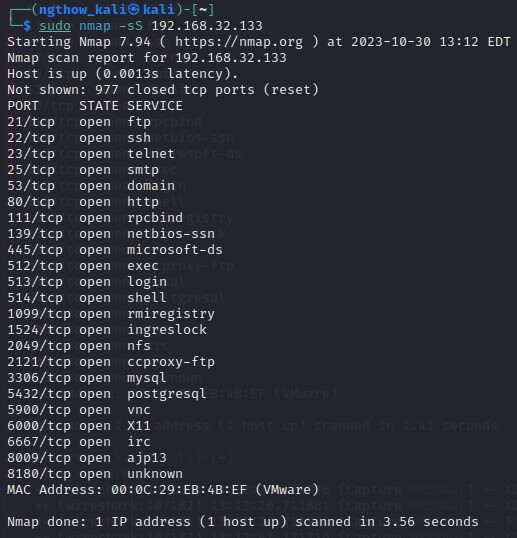


**Câu 28: So sánh 2 công cụ DNSEnum và DNSRecon? Công cụ nào dễ sử dụng hơn? Công cụ nào cho kết quả chính xác hơn? Công cụ nào hiển thị nhiều kết quả hơn?**

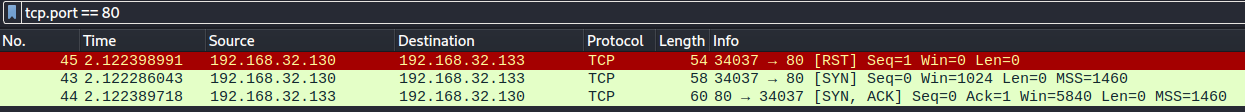
|  |  |  |
| --- | --- | --- |
|  | DNSEnum | DNSRecon |
| Sử dụng | Giao diện đơn giản, cung cấp những thông tin cơ bản nên dễ sử dụng hơn so với DNSRecon. | Giao diện dễ sử dụng và cung cấp nhiều options hơn, cung cấp nhiều tính năng mạnh mẽ. |
| Kết quả | Sẽ cung cấp chính xác kết quả kiểm tra DNS và zone transfer, nhưng đối với những phân tích sâu hơn về domain name sẽ có những giới hạn nhất định. | Đối với những phân tích sâu phức tạp sẽ cho những kết quả chính xác hơn so với DNSEnum vì phân tích được chi tiết và nhiều khía cạnh hơn. |
| Hiển thị | Hiển thị kết quả kiểm tra và các thông tin dưới dạng danh sách, nhìn sẽ trực quan và dễ hiểu hơn. Tuy nhiên chỉ hiển thị những thông tin cơ bản nên ít hơn so với DNSRecon. | Phạm vi mà DNSRecon thu thập rộng hơn nên sẽ hiển thị nhiều hơn tùy vào mục đích sử dụng. |

**Câu 29: Thực hiện bắt Wireshark để mô tả cách gói tin được gửi và nhận khi thực hiện SYN Scan sử dụng Nmap.**

* Thực thi câu lệnh **sudo nmap -sS 192.168.32.133** để thực hiện SYN scan, với địa chỉ IP 192.168.32.133 là địa chỉ IP của máy ảo Metasploitable2.

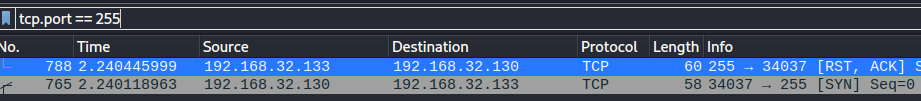


* Kết quả bắt wireshark:
* Tại port 80:



Gói tin 43 được gửi từ máy em đến máy Meta với cờ SYN để yêu cầu thiết lập kết nối. Gói tin 44 là gói tin Meta phản hồi với cờ SYN ACK tức là chấp nhận kết nối, lúc này port 80 đang mở. Sau đó, máy em gửi cờ RST yêu cầu ngắt kết nối.

* Tại port 255:



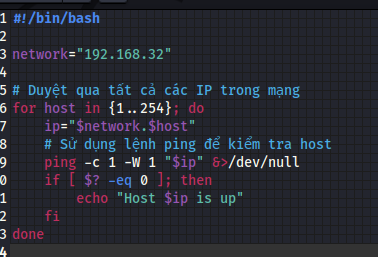
Gói tin thứ 765 gửi từ máy em đến Meta yêu cầu thiết lập kết nối. Meta phản hồi lại máy em bằng gói tin 788 với cờ RST ACK để đóng kết nối mà không gửi bất kỳ cờ SYN ACK nào, do đó, port 255 đang đóng.

**Câu 31: So sánh với sử dụng phương thức SYN Scan (số lượng gói tin được gửi, số lượng gói tin được nhận, thời gian quét, kết quả hiển thị…)**

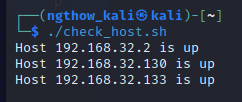
|  |  |  |
| --- | --- | --- |
|  | SYN scan | Connect scan |
| Số lượng gói tin được gửi | Chỉ gửi một gói tin SYN để yêu cầu kết nối. | Gửi nhiều gói tin hơn. |
| Số lượng gói tin được nhận | Chỉ cần nhận một gói tin SYN ACK để xác nhận cổng mở hay đóng, nên nhận ít hơn. | Nhận nhiều hơn. |
| Thời gian quét | Nhanh hơn do gửi ít gói tin. | Chậm hơn do phải thiết lập kết nối thực sự. |
| Kết quả hiển thị | Hiển thị port và trạng thái của port nhưng kết quả mang tính tương đối. | Tương tự SYN scan nhưng kết quả đáng tin cậy hơn (do có bắt tay 3 bước). |

**Câu 32: Thực hiện kiểm tra các host đang hoạt trong mạng bằng các ngôn ngữ lập trình khác (Bash script, Python, C/C++, Perl, …)**

* Viết bằng bash script:



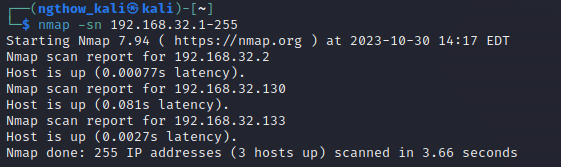
* Sau khi thực th, thu được kết quả:



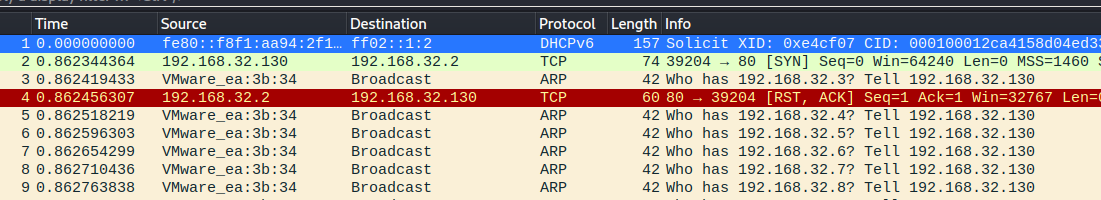
Có 3 host đang hoạt động trong mạng.

**Câu 33: Sử dụng Wireshark để phân tích gói tin khi sử dụng Nmap với tùy chọn -sn.**

* Lệnh nmap với -sn được dùng để quét mạng mà không quan tâm đến port. Nó sẽ chỉ ra các máy đang hoạt động trong dải IP nhưng không show port nào cụ thể đang được mở. -sn sẽ gửi các gói tin ICMP Echo Request (ping) đến các máy chủ hoặc máy mục tiêu để xem liệu chúng phản hồi hay không.
* Kết quả chạy lệnh, có 3 host đang hoạt động:



* Kết quả wireshark:



**Câu 34: Liệt kê các banner, dịch vụ đang chạy trên máy Metasploitable 2 (chỉ liệt kê các dịch vụ TCP).**

- Sử dụng lệnh **nmap -sS -sV -p- --open 192.168.32.133** để quét, trong đó:

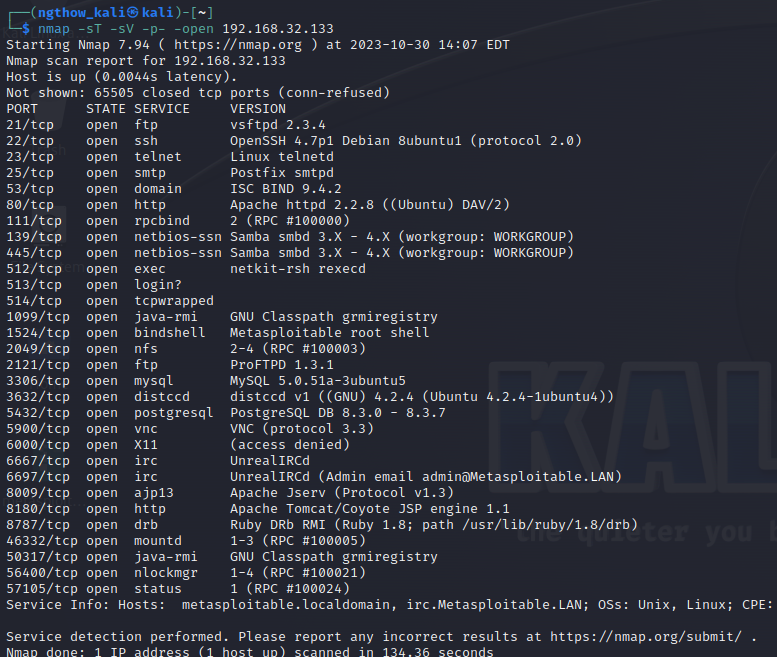
**-sS**: SYN scan để kiểm tra port.

**-sV**: Kiểm tra các banner của dịch vụ.

**-p**: quét tất cả các cổng từ 1 đến 65535.

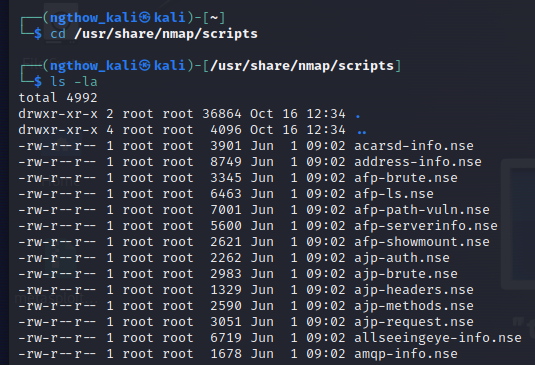
**--open**: liệt kê các cổng đang mở.

* Kết quả:

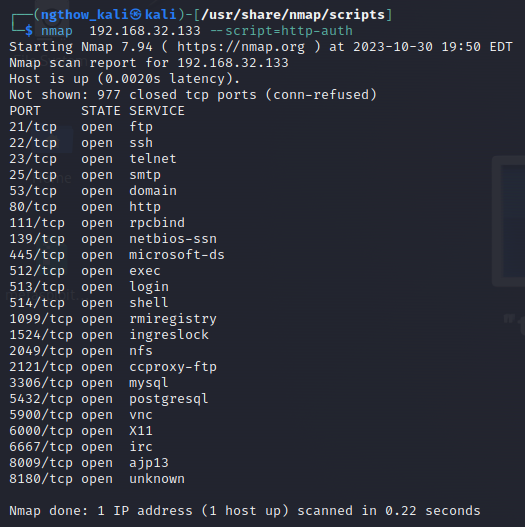


**Câu 35: Sử dụng thêm 2 NSE script (tự chọn) để quét máy mục tiêu (Metasploitable 2)**

* Để sử dụng được NSE script, cần di chuyển vào trong thư mục **/usr/share/nmap/scripts**. Em sẽ xem qua tổng quan xem thư mục có gì, tồn tại rất nhiều file NSE trong đây:



* Chọn 2 NSE script để thực thi: Máy mục tiêu là Metasploitable2 có địa chỉ IP là **192.168.32.133**:
* Sử dụng file **ssh-publickey-acceptance.nse** để kiểm tra xem máy chủ có chấp nhận cặp khóa công khai để đăng nhập thay vì sử dụng password hay không:
* Sử dụng **http-auth.nse** kiểm tra tính bảo mật của trang web:



---

***Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này***

# **YÊU CẦU CHUNG**

* Sinh viên tìm hiểu và thực hành theo hướng dẫn.
* Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
* Sinh viên báo cáo kết quả thực hiện và nộp bài.

**Báo cáo:**

* File .DOCX và .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
* Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
* Đặt tên theo định dạng: [Mã lớp]-SessionX\_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành đã đăng ký với GVHD-TH).

*Ví dụ: [*NT101.K11.ATCL*]-Session1\_Group3.*

* Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
* Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài Lab.
* Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá**: Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

* Chuẩn bị tốt.
* Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

*Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)