BÁO CÁO THỰC HÀNH

**Môn học: An toàn mạng máy tính**

**Lab 2: THU THẬP THÔNG TIN**

*GVHD: Đoàn Minh Trung*

1. **THÔNG TIN CHUNG:**

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

Lớp: NT140.O12.ATCL – N03

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Bùi Hoàng Trúc Anh | 21521817 | [21521817@gm.uit.edu.vn](mailto:21521817@gm.uit.edu.vn) |
| 2 | Lê Hoàng Oanh | 21521253 | 21521253@gm.uit.edu.vn |
| 3 | Nguyễn Ngọc Trà My | 21520353 | [21520353@gm.uit.edu.vn](mailto:21520353@gm.uit.edu.vn) |
| 4 | Huỳnh Minh Tân Tiến | 21521520 | 21521520@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | 1 - 13 | 100% |
| 2 | 15 | 100% |
| 3 | 17 | 100% |
| 4 | 21 | 100% |

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

BÁO CÁO CHI TIẾT

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

Các lĩnh vực của công ty gồm:

* + Cell Regeneration
  + Immune Systems Supplements
  + Micromachine Cyberisation Repair
  + Nanomite Based Weaponry Systems
  + Nanoprobe Based Entity Assimilation
  + Nanoprocessors
  + Perlin VanHook Chemical Dispersal

1. **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)?**

* Joe Sheer

Position: chief executive officer

Email: [joe@megacorpone.com](mailto:joe@megacorpone.com)

Twitter: @Joe\_Sheer

* Tom Hudson

Position: web designer

Email: [thudson@megacorpone.com](mailto:thudson@megacorpone.com)

Twitter: @TomHudsonMCO

* Tanya Rivera

Position: senior developer

Email: [trivera@megacorpone.com](mailto:trivera@megacorpone.com)

Twitter: @TanyaRiveraMCO

* Matt Smith

Position: marketing director

Email: [msmith@megacorpone.com](mailto:msmith@megacorpone.com)

Twitter: @MattSmithMCO

1. **Khi có được địa chỉ Email của các thành viên thuộc tổ chức, bạn có phát hiện ra được điều gì?**

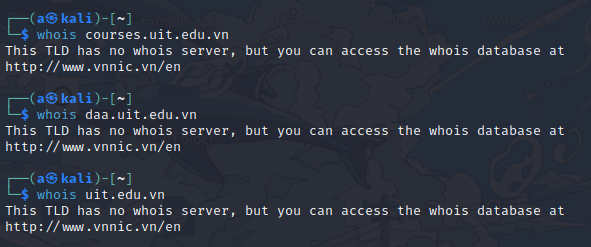
Các email đều có dạng [[name]@megacorpone.com](mailto:name]@megacorpone.com)

1. **Sử dụng công cụ whois để xác định các name server của MegaCorp One.**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Description automatically generated

1. **Sử dụng công cụ whois để tìm kiếm các thông tin của trường Đại học Công nghệ Thông tin (uit.edu.vn) có được không? Giải thích?**



Vấn đề xảy ra ở đây liên quan đến cách quản lý tên miền cho TLD ".edu.vn" và cách các TLD khác nhau xử lý thông tin whois.

Một số TLD có một máy chủ whois chung và cung cấp thông tin công khai về các tên miền dưới TLD đó thông qua giao thức whois. Tuy nhiên, không phải tất cả các TLD hoạt động theo cách này. Trong trường hợp của TLD ".edu.vn," thì hiển nhiên rằng nó không cung cấp máy chủ whois riêng và không hỗ trợ truy vấn whois thông qua giao thức truyền thống.

Thay vào đó, tên miền trong TLD ".edu.vn" cần được tra cứu thông qua cơ quan quản lý tên miền quốc gia của Việt Nam, là Trung tâm Thông tin Mạng Internet Việt Nam (VNNIC). VNNIC có một cơ sở dữ liệu whois riêng, và họ cung cấp các công cụ trực tuyến trên trang web của họ để tra cứu thông tin về tên miền trong TLD ".edu.vn."

Lý do chính là một số TLD, đặc biệt là các TLD quốc gia, không tuân theo các tiêu chuẩn whois quốc tế và thay vào đó có các quy tắc và quy định riêng. Điều này có thể tạo ra sự không nhất quán trong việc truy xuất thông tin whois giữa các loại TLD khác nhau.

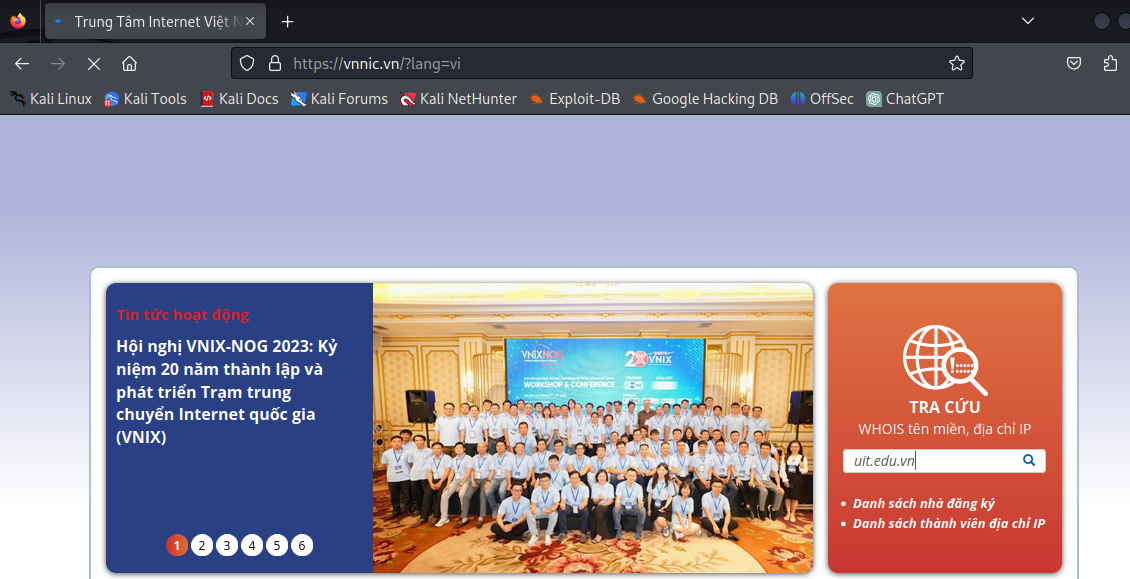
1. **Thu thập thông tin về tên miền uit.edu.vn và hãy cho biết các thông tin như:**

**a. Ngày đăng ký tên miền**

**b. Ngày hết hạn tên miền**

**c. Chủ sở hữu tên miền**

**d. Các name server của tên miền**



Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Description automatically generated

a. Ngày đăng ký tên miền: 2006-10-02

b. Ngày hết hạn tên miền: 2024-10-02

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

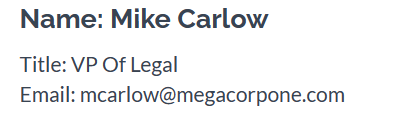
d. Các name server của tên miền

* ns1.pavietnam.vn
* ns2.pavietnam.vn
* nsbak.pavietnam.net

1. **Ai là Phó chủ tịch Pháp lý (Vice President of Legal) của MegaCorp One và địa chỉ email của họ là gì?**

Phó chủ tịch Pháp lý (Vice President of Legal) của MegaCorp One là Mike Carlow

Địa chỉ email: mcarlow@megacorpone.com



1. **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 tìm kiếm thêm các nhân viên khác tại trang: https://www.zoominfo.com/pic/megacorp-one/1160818919



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

* “site”: Tìm kiếm các trang web liên quan đến một chủ đề cụ thể.

VD: "site:example.com" sẽ tìm kiếm thông tin chỉ trên trang web example.com.

* “inurl”: Tìm kiếm các trang web có URL chứa từ khóa cụ thể.

VD: "inurl:admin" sẽ liệt kê các trang web có URL chứa từ "admin".

* "filetype": Tìm kiếm các tệp tin có định dạng cụ thể.

VD: "filetype:pdf" sẽ liệt kê các tệp tin PDF.

* "intext": Tìm kiếm các trang web có nội dung chứa từ khóa cụ thể.

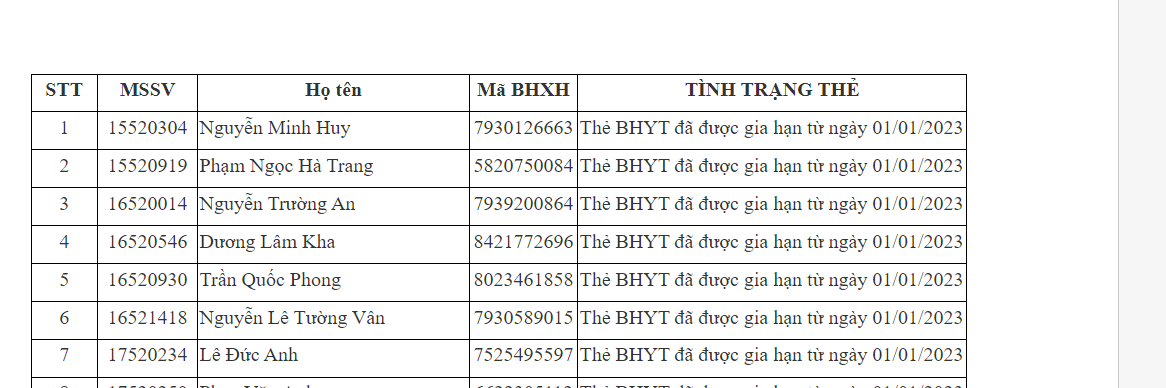
VD: "intext:password" sẽ liệt kê các trang web có nội dung chứa từ "password".

* "intitle": Tìm kiếm các trang web có tiêu đề chứa từ khóa cụ thể.

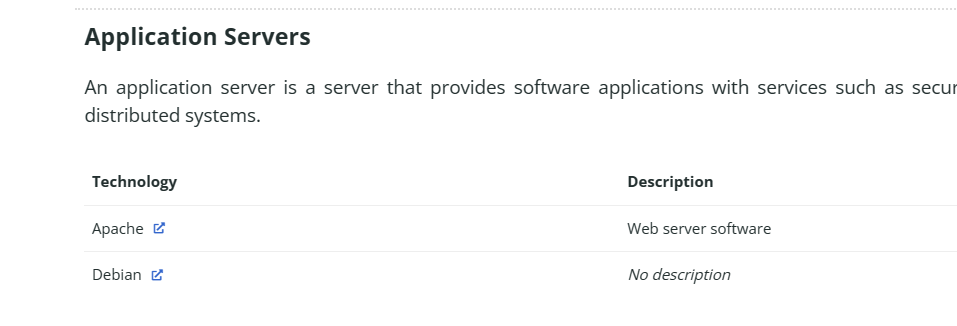
VD: "intitle:index of" sẽ liệt kê các trang có tiêu đề chứa cụm từ "index of".

1. **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?**

Danh sách các sinh viên mua bảo hiểm y tế: lộ mã bảo hiểm xã hội



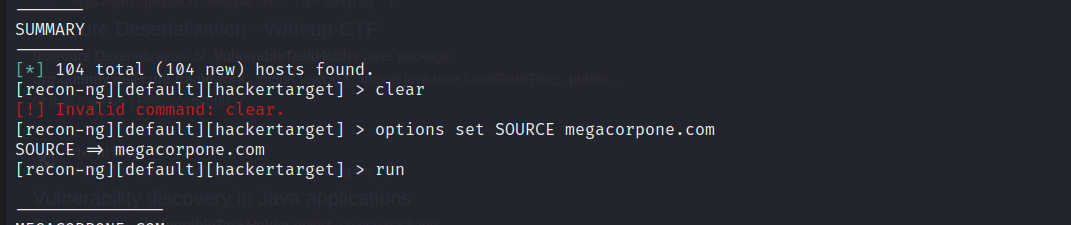
1. **Sử dụng Netcraft để xác định máy chủ ứng dụng (application server) đang chạy trên** [**www.megacorpone.com**](http://www.megacorpone.com)



Apache và Debian

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

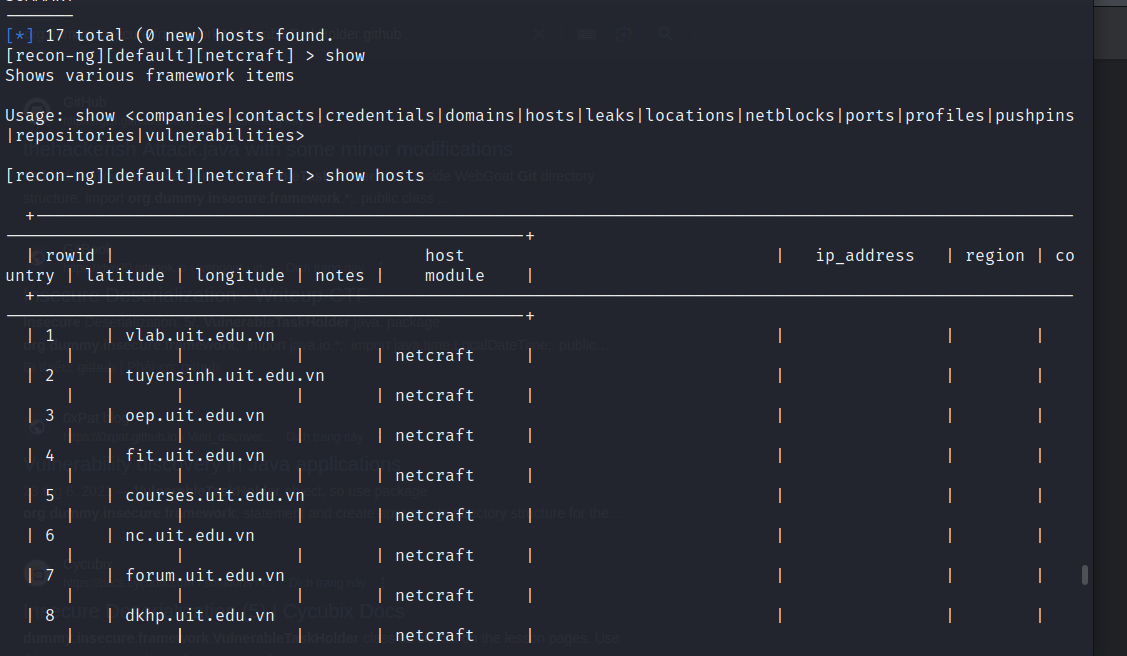
Dùng modules hackertarget



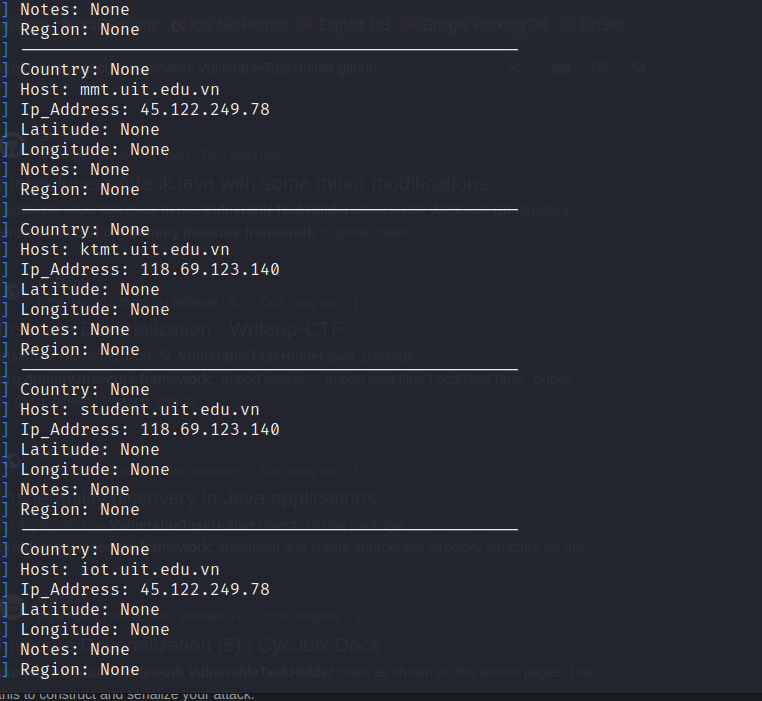


1. **Sử dụng một số module khác có trong recon-ng để thu thập thông tin về UIT nhiều nhất có thể**

Dùng netcraft để xác định có domain uit.edu.vn

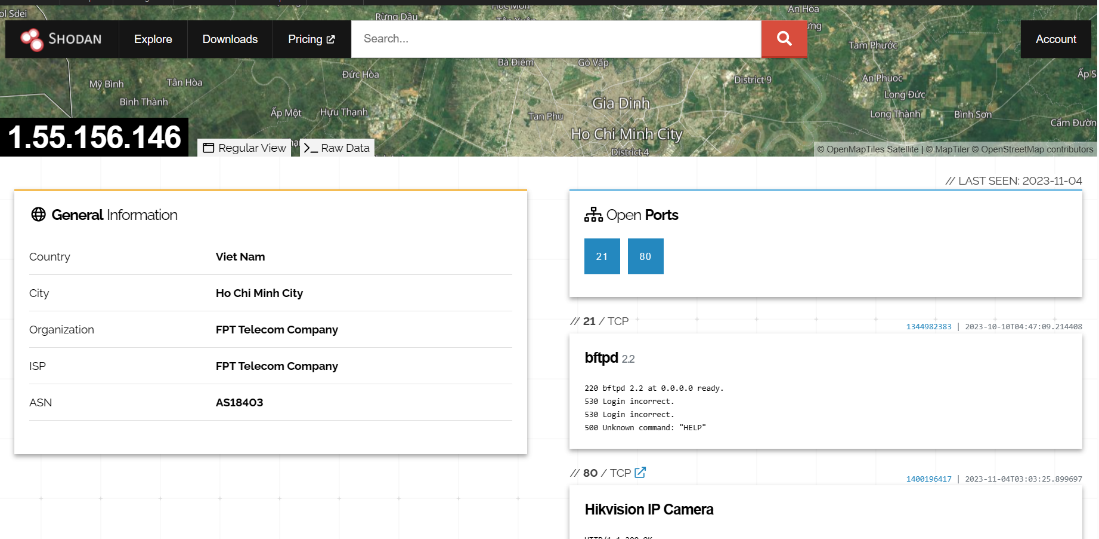


Dùng hacketarget để xác định ip của các domains uit.edu.vn



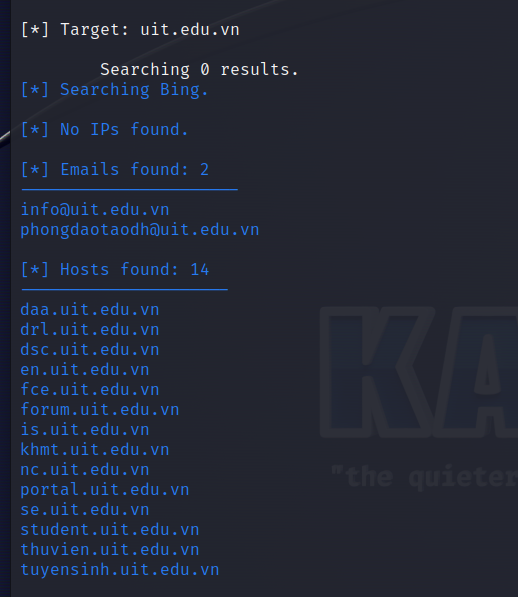
1. **Sử dụng 1 trong 2 công cụ Gitrob hoặc Gitleaks để tìm kiếm các thông tin nhạy cảm bị rò rỉ đối với các trường đại học thành viên trong ĐHQG**
2. **Thực hiện tìm kiếm các lệnh khác trên Shodan mà có thể tiết lộ thêm nhiều thông tin thú vị về một đối tượng bất kỳ.**

country:VN city:"Ho CHi Minh" product:"Hikvision IP Camera"  
Thông tin về ip hikvision IP camera của FPT



1. **So sánh kết quả tìm kiếm trên Shodan so với các search engine khác như Google, Bing…**
2. **Sử dụng công cụ theHarvester để lấy tìm kiếm các địa chỉ email của UIT**

TheHarvester –d uit.edu.vn -b bing

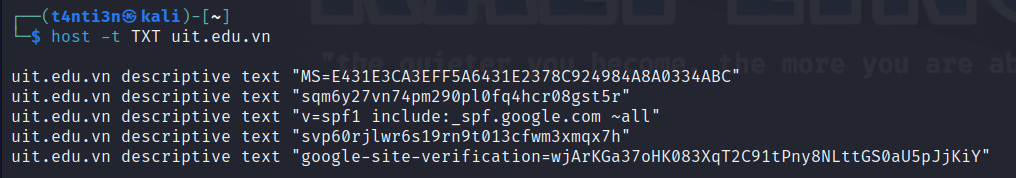


a. Ngoài các bản ghi kể trên, hãy liệt kê các bản ghi khác của DNS. b. Sử dụng lệnh host để tìm kiếm các bản ghi TXT, MX cho tên miền uit.edu.vn

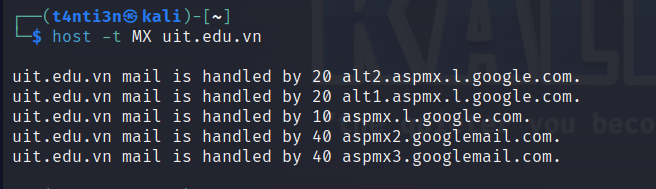
* a. **AAAA**: Bản ghi này được sử dụng để ánh xạ một tên miền đến một địa chỉ IPv6.
* **NS**: Bản ghi này xác định tên máy chủ DNS chịu trách nhiệm cho một tên miền cụ thể.
* **SOA**: Bản ghi này xác định thông tin về máy chủ DNS chính cho một tên miền cụ thể.
* **SRV**: Bản ghi này được sử dụng để xác định các máy chủ cung cấp một dịch vụ cụ thể trong một tên miền.
* **NAPTR**: Bản ghi này được sử dụng để ánh xạ các tên miền vào các URI (Uniform Resource Identifier) cho các dịch vụ VoIP (Voice over Internet Protocol) và SIP (Session Initiation Protocol).
* **CAA**: Bản ghi này được sử dụng để chỉ định các cơ quan chứng nhận có thể phát hành chứng chỉ cho một tên miền và tất cả các tên miền con của nó.

b.

Bản TXT của uit.edu.vn



Bản MX của uit.edu.vn

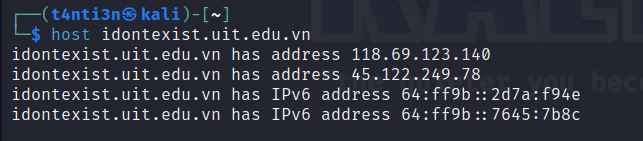


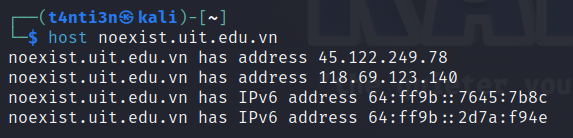
1. **Sử dụng với nguồn tìm kiếm khác (-b). Theo bạn, kết quả của nguồn nào tốt hơn?**
2. **Thực hiện tìm kiếm các địa chỉ Email của MegaCorp One sử dụng Maltego**
3. **Sử dụng công cụ Maltego cho UIT (tên miền: uit.edu.vn) và trả lời các câu hỏi sau:**

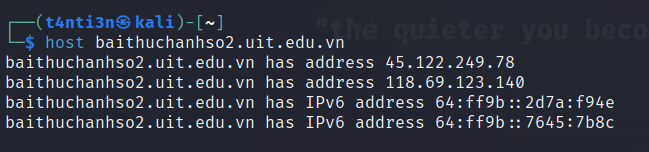
**a. Các bản ghi DNS.**

**b. Các website và địa chỉ IP tương ứng.**

1. **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?**







Các hotsname không tồn tại đều có cùng địa chỉ IP

1. **Sử dụng wordlist thông dụng khác (rockyou, seclists) để tìm kiếm các hostname hợp lệ khác của megacorpone.com**
2. **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.**
3. **Viết Liệt kê danh sách các loại enumeration có thể được sử dụng cùng với tùy chọn -t**
4. **Cho một vài ví dụ sử dụng kết hợp các tùy chọn được DNSRecon hỗ trợ khác (ít nhất là 2 ví dụ)**
5. **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?**
6. **Thực hiện bắt Wireshark để mô tả cách gói tin được gửi và nhận khi thực hiện SYN Scan sử dụng Nmap**
7. **Thực hiện bắt Wireshark để mô tả cách gói tin được gửi và nhận khi thực hiện TCP Connect Scan sử dụng Nmap.**
8. **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…)**
9. **Thực hiện kiểm tra các host đang hoạt trong mạng bằng các ngôn ngữ lập trình khác (Bash script, Python, C/C++, Perl, …)**
10. **Sử dụng Wireshark để phân tích gói tin khi sử dụng Nmap với tùy chọn -sn**
11. **Liệt kê các banner, dịch vụ đang chạy trên máy Metasploitable 2 (chỉ liệt kê các dịch vụ TCP).**
12. **Sử dụng thêm 2 NSE script (tự chọn) để quét máy mục tiêu (Metasploitable 2)**

---

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

# **YÊU CẦU CHUNG**

* Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, 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 nộp bài theo thời gian quy định trên course.

**Báo cáo:**

* File **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
* Đặt tên theo định dạng: **[Mã lớp]-AssignmentX\_NhomY** (trong đó X là Thứ tự Assignment, Y là số thứ tự nhóm đồ án theo danh sách đã đăng ký).

*Ví dụ: [NT521.O11.ATCL]-Assignment01\_Nhom03.pdf.*

* Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.

**Đánh giá**:

* Hoàn thành tốt yêu cầu được giao.
* Có nội dung mở rộng, ứng dụng.

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

**HẾT**