BÁO CÁO THỰC HÀNH

**Bài thực hành số xx: Tên bài thực hành**

**Môn học:** Nhập môn Mạng máy tính

**Lớp:** NT100.ATTT.2

**THÀNH VIÊN THỰC HIỆN (Nhóm xx):**

|  |  |  |
| --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** |
| 1 | Nguyễn Thị A | 20520001 |
| 2 | Phan Văn B | 20520002 |
|  |  |  |

|  |
| --- |
| **Điểm tự đánh giá** |
|  |

**ĐÁNH GIÁ KHÁC:**

|  |  |
| --- | --- |
| Tổng thời gian thực hiện |  |
| Phân chia công việc |  |
| Ý kiến *(nếu có)*  + Khó khăn  + Đề xuất, kiến nghị |  |

Phần bên dưới của báo cáo này là báo cáo chi tiết của nhóm thực hiện

MỤC LỤC

[**A.** BÁO CÁO CHI TIẾT 2](#_Toc117536750)

[1. Thu thập thông tin thụ động (Passive Information Gathering) 2](#_Toc117536751)

[2. Nội dung 2 13](#_Toc117536752)

[**B.** TÀI LIỆU THAM KHẢO 13](#_Toc117536753)

# BÁO CÁO CHI TIẾT

## Thu thập thông tin thụ động (Passive Information Gathering)

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

+ Là công ty chuyên về công nghệ nano

+ Chịu trách nhiệm về các tiêu chuẩn xác định nghành trong lĩnh vực y tế, điện tử, thương mại

+ Đánh giá các nhóm nhỏ làm việc trong dự án độc lập, khi 1 dự án xác định sẽ thành công họ sẽ thu hút nhân tài và cải tiến công nghệ để hướng tới mục tiêu chung của công ty

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)?

+ Joe Sheer: Giám đốc điều hành

* Mail: [joe@megacorpone.com](mailto:joe@megacorpone.com)
* Twitter: @Joe\_Sheer

+ Tom Hudson: Thiết kế web

* Mail: [thudson@megacorpone.com](mailto:thudson@megacorpone.com)
* Twitter: @TomHudsonMCO

+ Tanya Rivera: Senior dev

* Mail: [trivera@megacorpone.com](mailto:trivera@megacorpone.com)
* Twitter: @TanyaRiveraMCO

+Matt Smith: Giám đốc marketting

* Mail: [msmith@megacorpone.com](mailto:msmith@megacorpone.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?

+ Mail sẽ là tên đi kèm ký tự đầu tiên của tên @megacorpone.com

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

+ 3 name server

* 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 nghệ Thông tin (uit.edu.vn) có được không? Giải thích?

+ Không tìm kiếm được, vì nó không có trong whois server

Câu 6 : Thu thập thông tin về tên miền uit.edu.vn

+ Ngày đăng ký: 2/10/2006

+ Ngày hết hạn: 2/10/2023

+ Chủ sở hữu: công ty TNHH PA Việt Nam

+ Nameserver: ns1.pavietnam.vn, ns2.pavietnam.vn, bak.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?

+ Mike Carlow

* Mail: [mcarlow@megacorpone.com](mailto:mcarlow@megacorpone.com)

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)?

+ Jon Nelson: Pentest

+ Franco Zettiici: IT

+ Steve Wong: System AD



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

+ intile: giới hạn tìm kiếm với tiêu đề trang web

+ iurl: giới hạn tìm kiếm với url trang wb

+ intext: chỉ tìm kiếm nội dung bỏ qua url, liên kết, tiêu đề

+ inanchor: tìm kiếm văn bản trong liên kết của 1 trang, link anchor là mô tả văn bản của 1 liên kết

+ site: thu hẹp tìm kiếm theo một trang web hoặc 1 miền hoặc domain

+ link: Trả về danh sách các trang liên kết đến url được chỉ định

+ cache: tìm bản sao của trang mà google đã lập chỉ mục ngay cả khi trang đó không còn

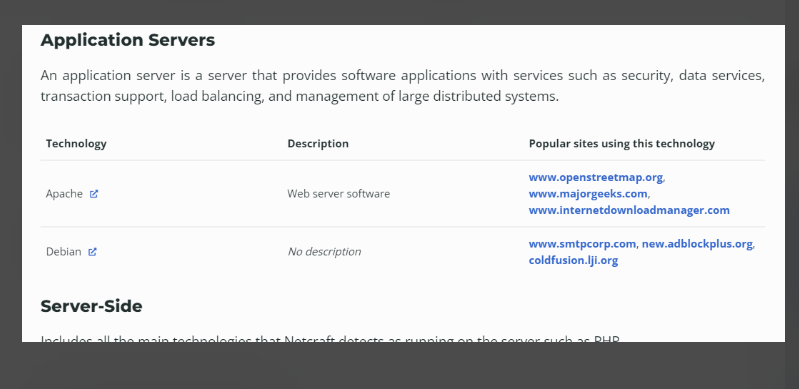
Câu 10: Thực hiện tìm kiếm các tài liệu thú vị của Trường Đại học Công nghệ Thông tin mà được công bố trên Internet mà theo bạn là không nên được công bố?

+ Hãy lên fanpage confession uit trên facebook sẽ có những thông tin thú vị cho người đọc

+ Link: <https://www.facebook.com/ConfessionUIT>

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

+ Máy chủ ứng dụng: apche



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

+ Ảnh có chứa văn bản

Mô tả được tạo tự động

Ảnh có chứa văn bản, màn hình, ảnh chụp màn hình, đen

Mô tả được tạo tự động

Ảnh có chứa văn bản

Mô tả được tạo tự động

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



+ Sử dụng module hackertarget

+ module to gather some subdomains

Ảnh có chứa văn bản

Mô tả được tạo tự động

Ảnh có chứa văn bản

Mô tả được tạo tự động

Ảnh có chứa văn bản

Mô tả được tạo tự động

Ảnh có chứa văn bản, thiết bị điện tử, máy tính

Mô tả được tạo tự động

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.

+ Dùng các bộ lọc

Ảnh có chứa văn bản

Mô tả được tạo tự động

Ảnh có chứa văn bản

Mô tả được tạo tự động

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

+ Kết quả tìm kiếm thông thường với shodan là các thiết bị kết nối internet như là web server, router, IoT

+ Các công cụ khác sẽ là file, text, hình ảnh, url

Câu 17, 18: Sử dụng công cụ theHarvester để lấy tìm kiếm các địa chỉ email của UIT, Sử dụng với nguồn tìm kiếm khác (-b). Theo bạn, kết quả của nguồn nào tốt hơn?

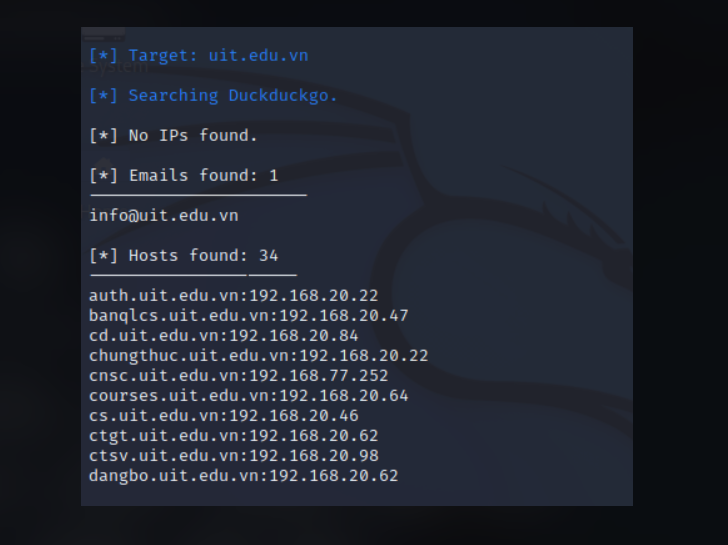
Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Nguồn bing cho 8 kết quả

Ảnh có chứa văn bản, màn hình, máy tính xách tay, ảnh chụp màn hình

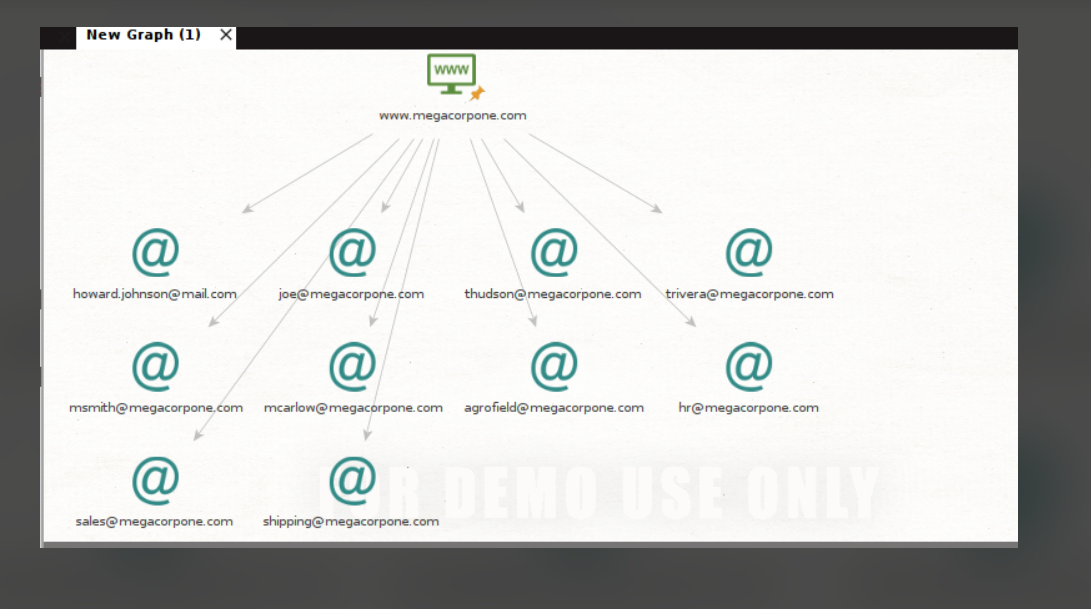
Mô tả được tạo tự động



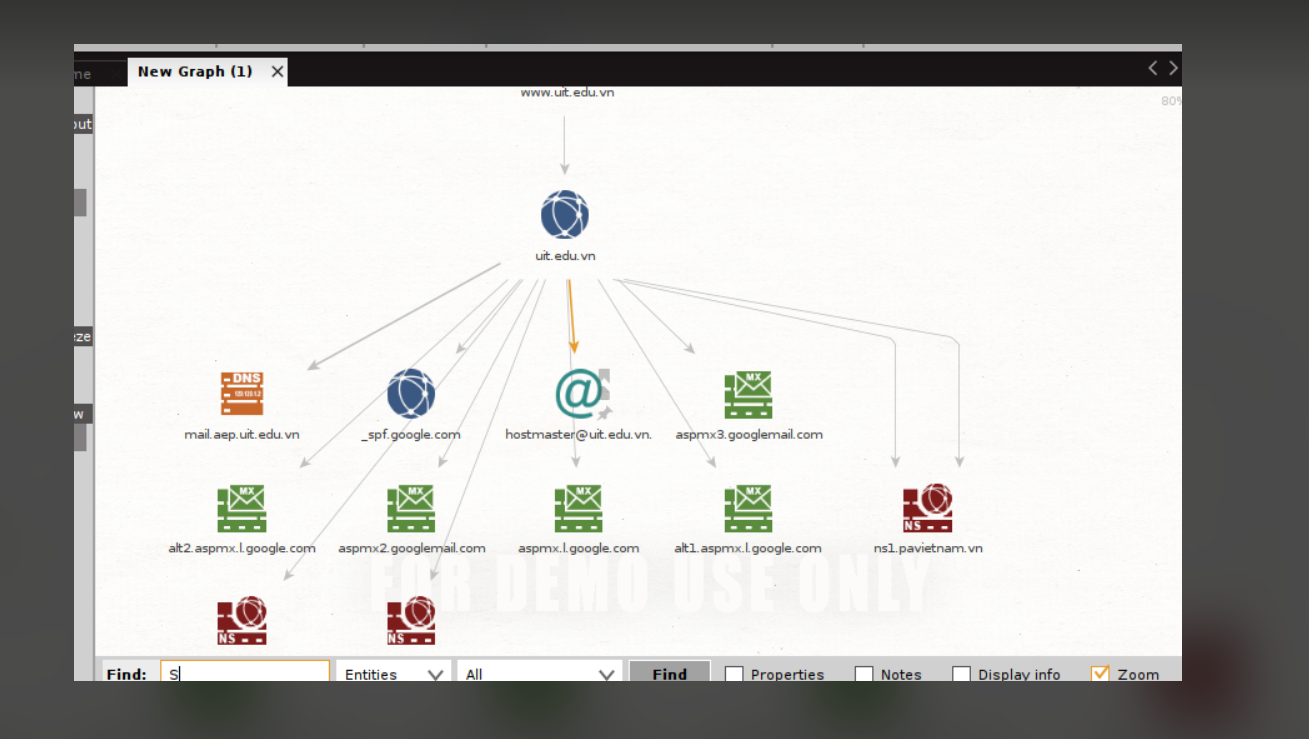
+ search engine duckduckgo có được 34 kết quả

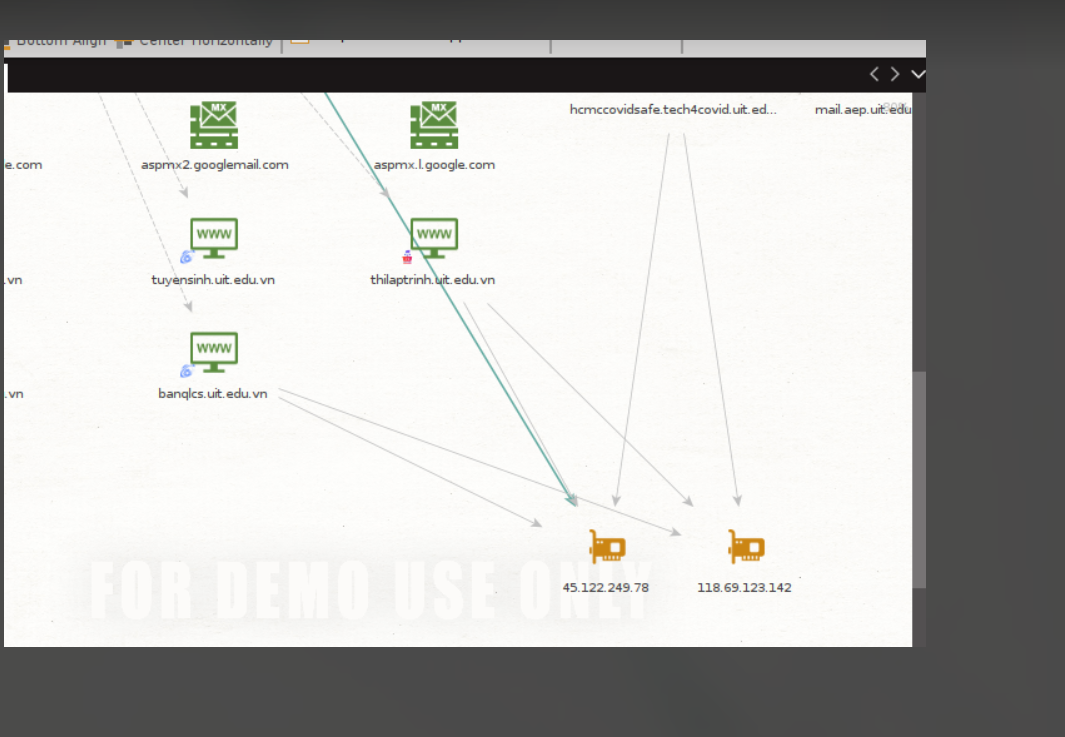
* Bing cho kết quả nhiều nhất
* Search bằng google thì do phiên bản mới nhất đang bị lỗi

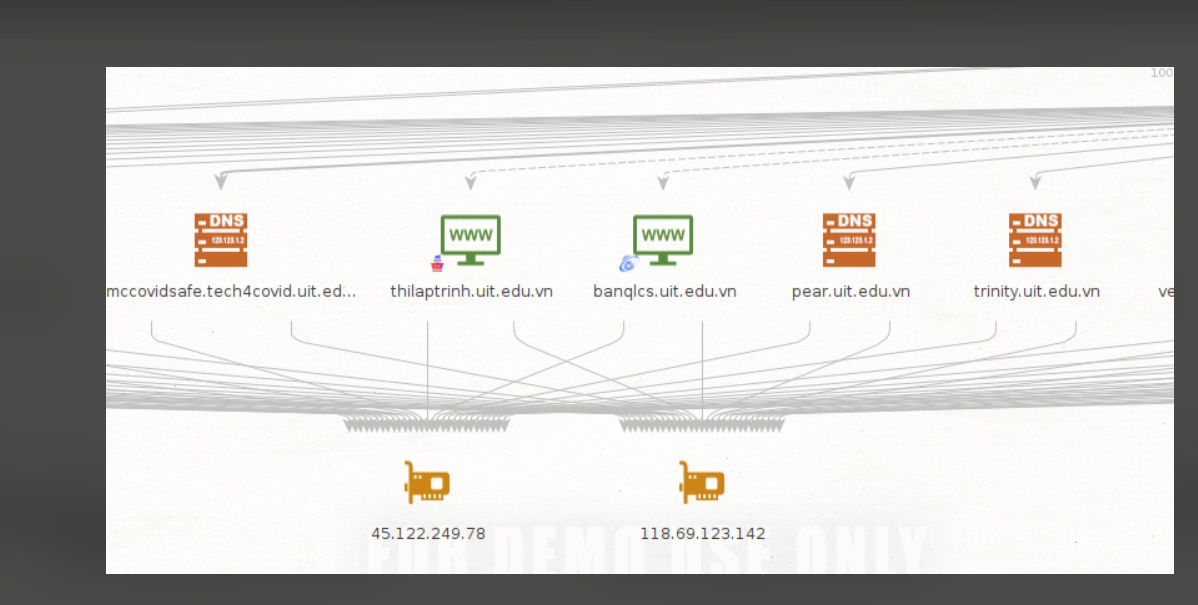
Câu 19: Thực hiện tìm kiếm các địa chỉ Email của MegaCorp One sử dụng Maltego



Câu 20: Sử dụng công cụ Maltego cho UIT (tên miền: uit.edu.vn) và trả lời các câu hỏi







## Thu thập thông tin chủ động (Active Information Gathering)

Ảnh có chứa văn bản

Mô tả được tạo tự động

1. SOA (Start of Authority)  
   Trong mỗi tập tin cơ sở dữ liệu DNS có một và chỉ một record SOA . Bao gồm các thông tin về domain trên DNS Server, thông tin về zone transfer.
2. Record AAAA  
   Có nhiệm vụ tương tự A nhưng là địa chỉ Ipv6.
3. Record SRV   
   Bản ghi SRV được sử dụng để xác định vị trí các dịch vụ đặc biệt trong 1 domain, ví dụ tên máy chủ và số cổng của các máy chủ cho các dịch vụ được chỉ định
4. Record DKIM   
   Là bản ghi dùng để xác thực người gửi bằng cách mã hóa một phần email gửi bằng một chuỗi ký tự, xem như là chữ ký.
5. Record SPF  
   Record SPF được tạo ra nhầm đảm bảo các máy chủ mail sẽ chấp nhận mail từ tên miền của khách hàng chỉ được gửi đi từ server của khách hàng. Sẽ giúp chống spam và giả mạo email.

* Text

  Description automatically generated
* Lệnh host tìm kiếm txt record.
* Text

  Description automatically generated
* Lệnh host tìm kiếm mx record.

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Graphical user interface, text

Description automatically generated

Có thể thấy rằng lệnh host cho các tên miền vẫn cho ra kết quả. Chứng tỏ DNS vẫn tồn tại các hostname này.

Thử tìm kiếm 2 địa chỉ IP trên thanh url của trình duyệt đều dẫn tới hostname uit.edu.vn.

Graphical user interface, text, application, Word

Description automatically generated

Text

Description automatically generated

Do danh sách quá dài nên em chỉ chụp 1 đoạn.

Text

Description automatically generated

Do không thể tìm ở đây nên em đã tìm ở trang web vnnic.vn và đây là danh sách:

Nameserver của UIT:

Text

Description automatically generated

Zone transfer

Graphical user interface, text, application, chat or text message

Description automatically generated

Nameserver của USSH, HCMIER và VNUHCM



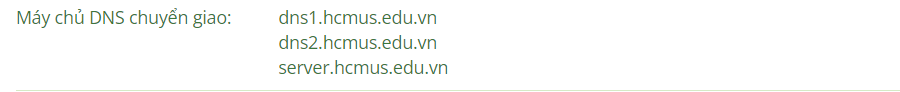
Zone transfer

Text

Description automatically generated

Tương tự với HCMIER và VNUHCM đều transfer failed.

Nameserver của HCMUS

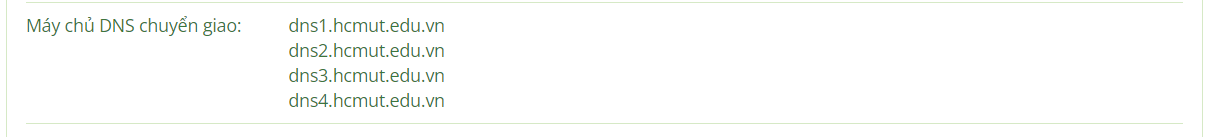


Zone transfer

Text

Description automatically generated

Nameserver của HCMUT



Zone transfer

Graphical user interface, text, application, chat or text message

Description automatically generated

Tương tự với hostname dns1 và dns2.

Nameserver của HCMIU



Text

Description automatically generated

Nameserver của UEL

Text

Description automatically generated

Tương tự với các trường hợp trên đều cho ra kết quả fail.

Graphical user interface, text, application

Description automatically generated

24.

-t axfr: Zone transfer.

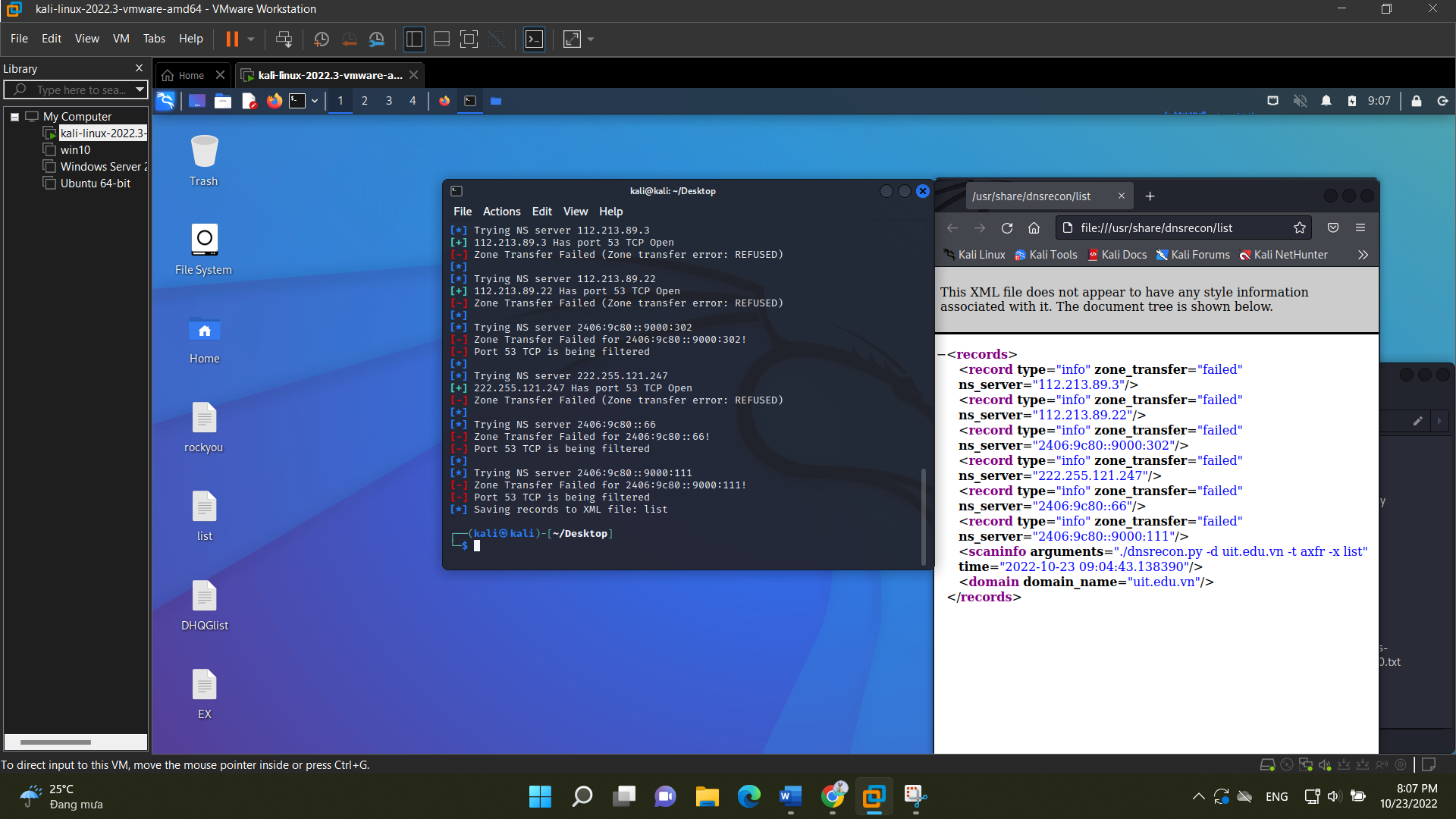
-t brt: brute force.

-t snoop: truy tìm bộ nhớ cache của DNS(Cache Snooping)

-t zonewalk: truy tìm các bản ghi nội bộ nếu zone không được cấu hình đúng cách.

25.

-x: lưu đầu ra vào 1 file.



-a: Thực hiện AXFR với kiểu liệt kê tiêu chuẩn.

A screenshot of a computer

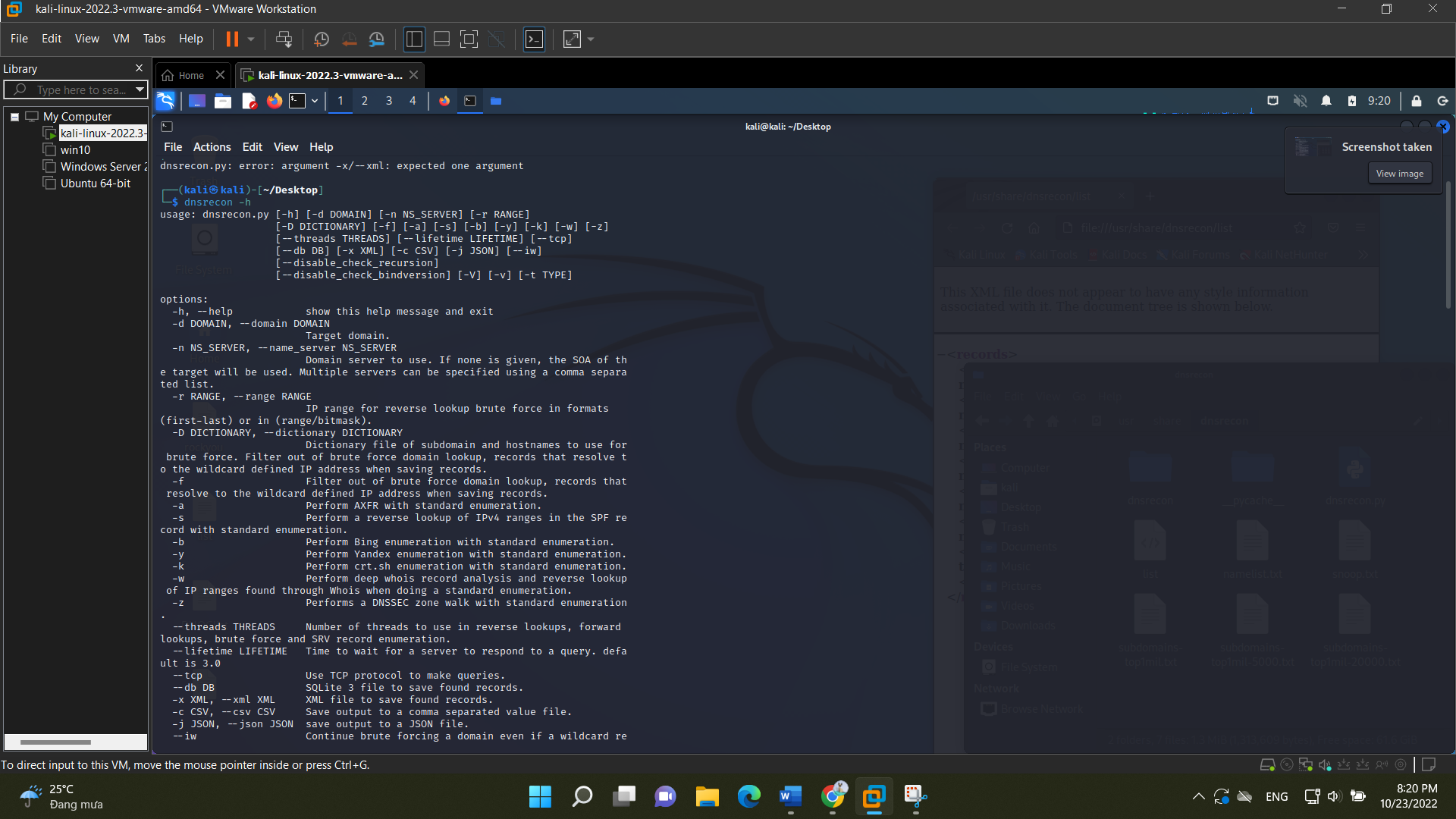
Description automatically generated with medium confidence

--lifetime: Thời gian chờ máy chủ phản hồi một truy vấn. mặc định là 3.0

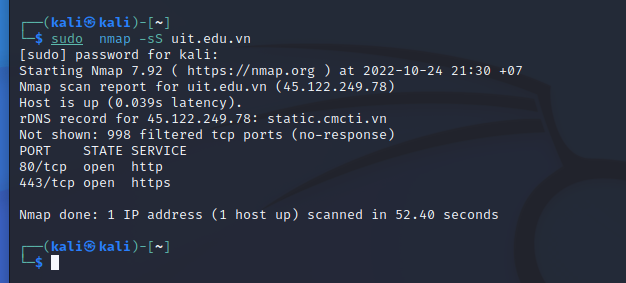
Text

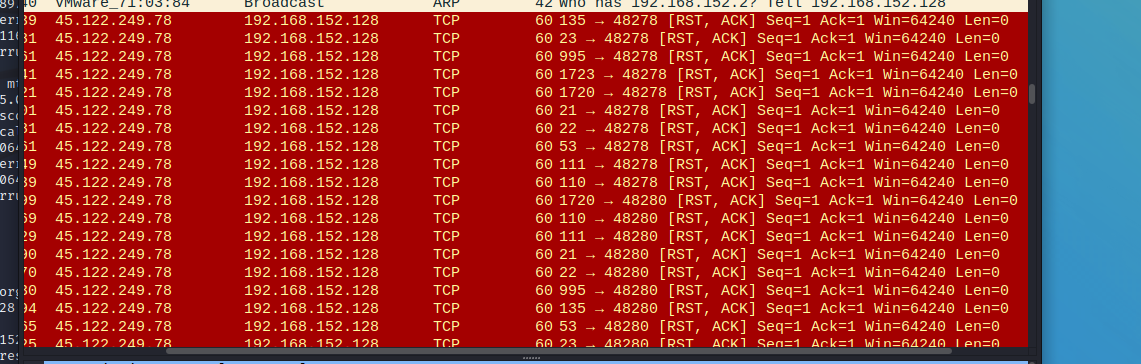
Description automatically generated

Dưới đây là các tùy chọn của dnsrecon

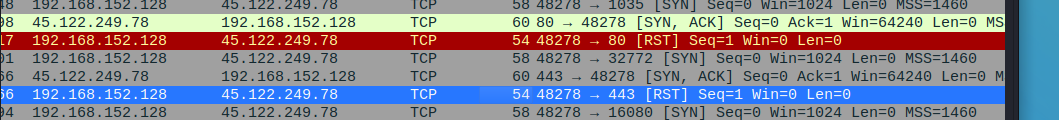


* Câu 27: .Thực hiện bắt Wireshark để mô tả cách gói tin được gửi và nhận khi thực hiện SYN Scan sử dụng Nmap



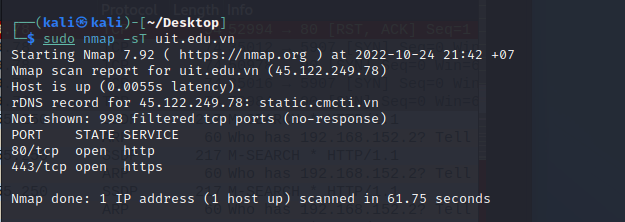


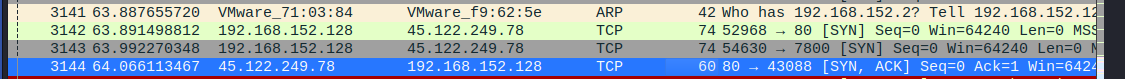
+ Ta thấy trong wire shark thì ip đích gửi trả kết quả lại cho máy tính những gói bị RST để có thể đóng kết nói trong quá trình bắt tay 3 bước nhưng không được



+ Máy ta bắt được 2 gói tin gửi tù máy cá nhân đến uit.edu.vn có port được mở là 80 và 443

* Câu 28: Thực hiện bắt Wireshark để mô tả cách gói tin được gửi và nhận khi thực hiện TCP Connect Scan sử dụng Nmap.





+ Ta thấy có gửi lại gói ACK để đóng kết nối

* Câu 29: 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…)

+ Với SYN Scan thì thời gian quét nhanh hơn vì số lượng gói tin được gửi đi ít hơn do không có gói ACK để hoàn tất quá trình bắt tay 3 bước

+ Còn với TCP Connect Scan thì ngược lại. Thời gian quét lâu hơn và số lương gói cũng nhiều hơn vì có gửi gói ACK để xác nhận hoàn tất quá trình bắt tay 3 bước

+ Thấy số lượng gói tin nhận thì TCP Connect scan cũng nhiều hơn do số gói gửi đi cũng nhiều hơn SYN Scan

* Câu 30: Thực hiện kiểm tra các host đang hoạt trong mạng bằng các ngôn ngữ lập trình khác (Bash script, Python, C/C++, Perl, …)

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Source code

Ảnh có chứa văn bản

Mô tả được tạo tự động

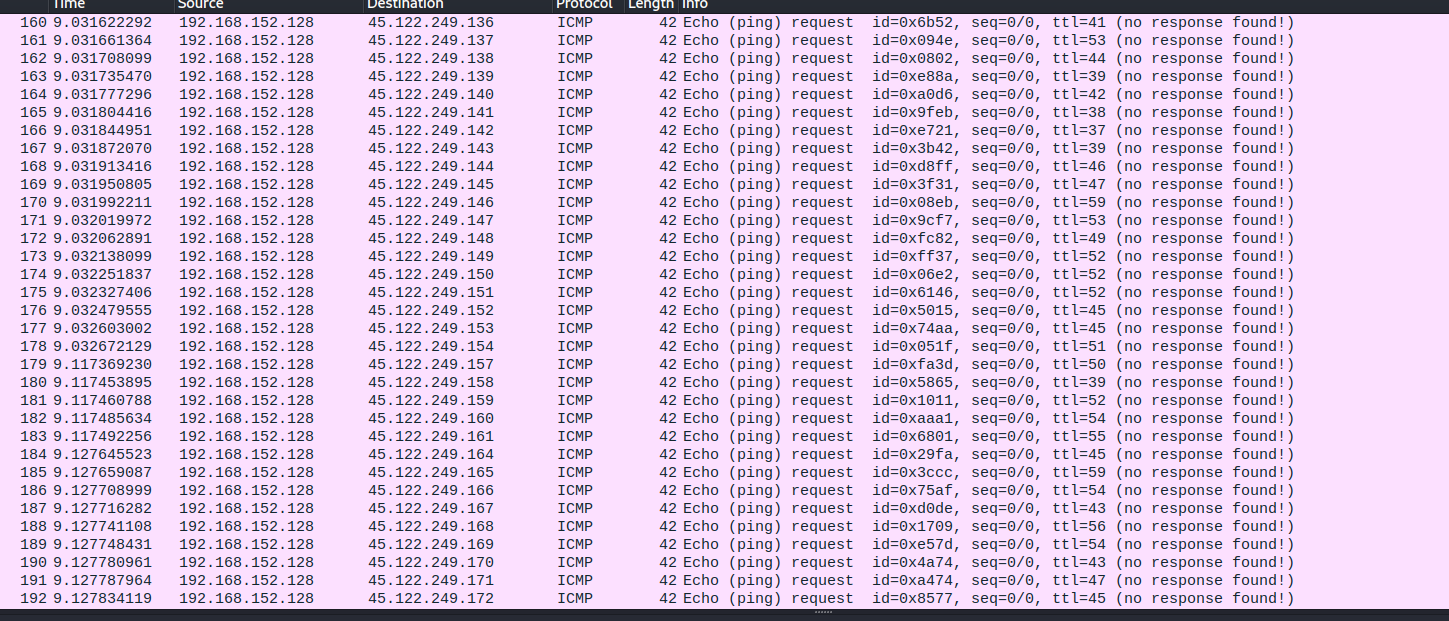
+ Kết quả ta quét được có host 192.152.1.1 và host 192.168.152.2 đang hoạt động

Ảnh có chứa văn bản

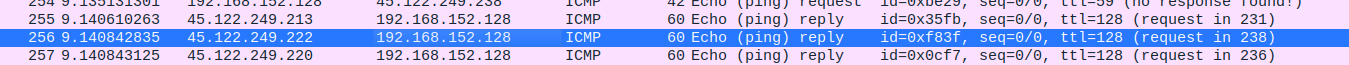
Mô tả được tạo tự động

+ So sánh với nmap sweep thì cũng tương tự nhưng ở trên chưa quét xong

* Câu 31: Sử dụng Wireshark để phân tích gói tin khi sử dụng Nmap với tùy chọn -sn



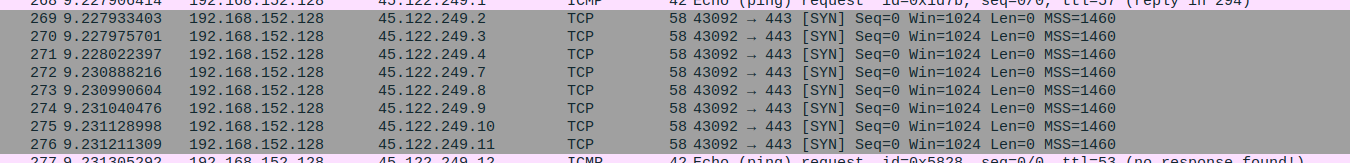
+ Ta thấy nó gửi 1 loạt gói tin ICMP request tới các host xem có host nào phản hồi



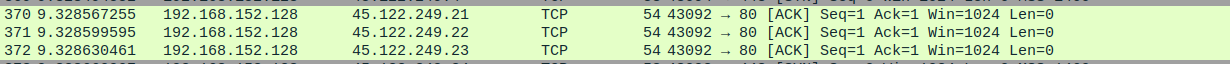
+ Có host 192.168.152.125 có gói reply ở vị trí 231, 238, 236



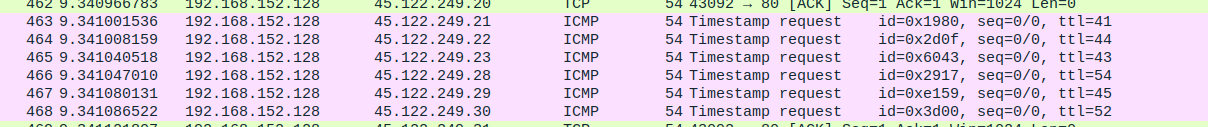
+ Gói ICMP reply



+ Ngoài ra nó còn gửi gói TCP Syn đến Port 443



+ Và gói tin TCP ACK đến port 80



+ Nó cũng gửi những gói ICMP timestamp request đến từng host để xác minh máy host có sẵn hay không

# TÀI LIỆU THAM KHẢO