BÁO CÁO THỰC HÀNH

Môn học: Nhập môn bảo đảm và an ninh thông tin

Lab 3:

GVHD: Đoàn Minh Trung

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: IE105.P13.CNVN

STT	Họ và tên	MSSV	Email
1	Hoàng Bảo Long	22520807	22520807@gm.uit.edu.vn
2	Đặng Trần Long	22520805	22520805@gm.uit.edu.vn
3	Nguyễn Duy Phương	22521165	22521165@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]2

STT	Công việc	Kết quả tự đánh giá
1	Bài tập 1-10	100%
2	Bài tập 10-20	90%
3	Bài tập 20-33	80%

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

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

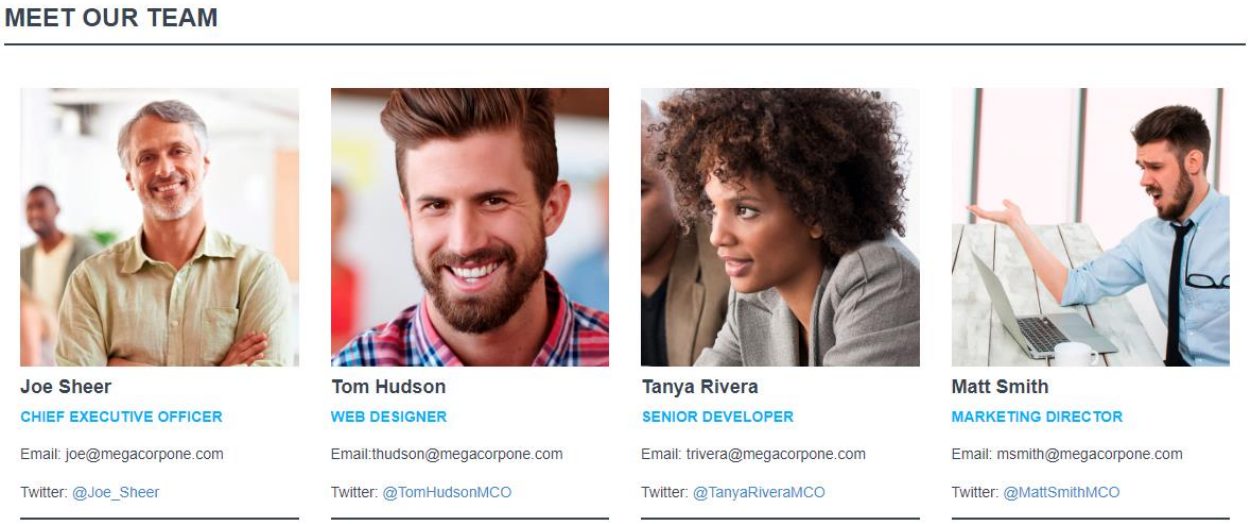
1. Từ trang web của MegaCorp One, hãy mô tả một chút về lĩnh vực hoạt động của công ty?

MegaCorp One chuyên về công nghệ nano tiên tiến, cung cấp các giải pháp đột phá trong các lĩnh vực y tế, điện tử và thương mại. Công nghệ của họ được ứng dụng trong y học nano để tái tạo tế bào và trong các ứng dụng quân sự như vũ khí thông minh.

- **Y học nano**: Tái tạo tế bào và điều trị bệnh bằng công nghệ tiên tiến.
- **Quân sự**: Phát triển vũ khí thông minh và thiết bị an ninh hiện đại.
- **Điện tử nano**: Sản xuất linh kiện nhỏ gọn, hiệu suất cao.
- **Năng lượng sạch**: Tối ưu hóa hệ thống năng lượng tái tạo.

Tầm nhìn của công ty là dẫn đầu toàn cầu trong ứng dụng công nghệ nano để cải thiện chất lượng cuộc sống và thúc đẩy các giải pháp bền vững. MegaCorp One hợp tác với các tổ chức lớn trong nghiên cứu và phát triển, hướng tới giải quyết các thách thức lớn của xã hội.

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)?

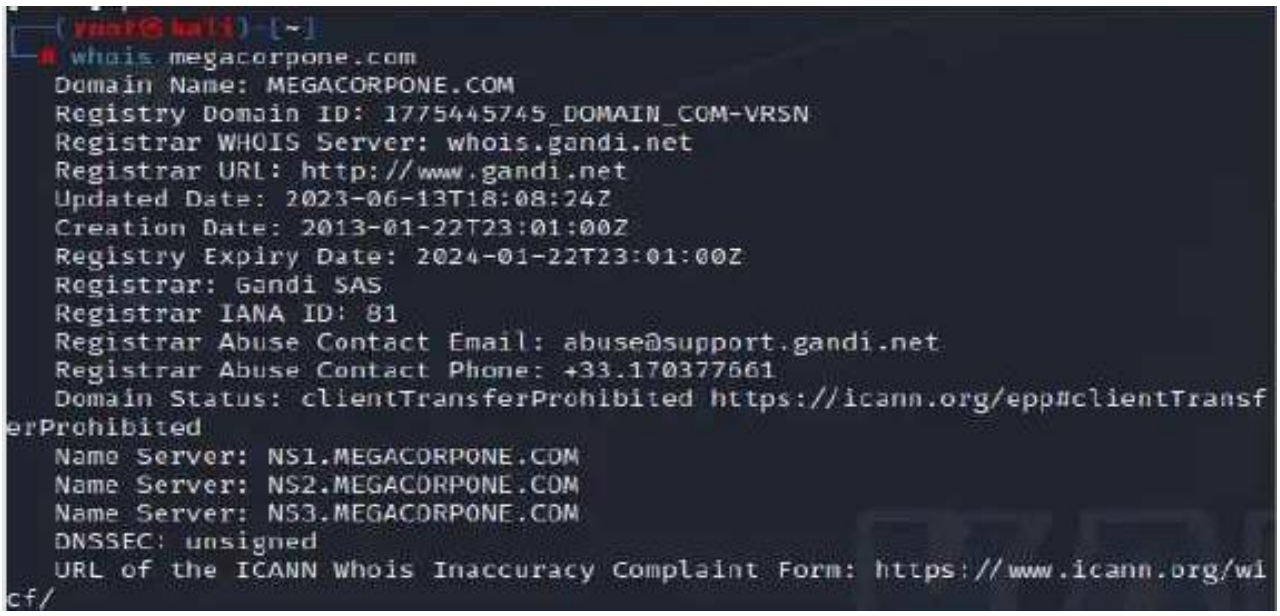


3. Khi có được địa chỉ Email của các thành viên thuộc tổ chức, bạn có phát hiện ra được điều gì?

Khi có được email của thành viên:

- **Phân tích bảo mật**:
    - Địa chỉ email có thể được sử dụng để xác định tổ chức thông qua các công cụ OSINT (Open Source Intelligence).
    - Có thể phát hiện các mối đe dọa tiềm năng nếu email bị lạm dụng trong các cuộc tấn công lừa đảo (phishing).
    - Email của MegaCorp One có thể là một mục tiêu để kiểm tra tính an toàn của hạ tầng tổ chức, từ đó đưa ra các biện pháp tăng cường bảo mật.

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



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?

Có thể sử dụng WHOIS để tra cứu thông tin tên miền uit.edu.vn, bao gồm ngày đăng ký, nhà cung cấp dịch vụ. Tuy nhiên, thông tin chi tiết như tên, địa chỉ, email chủ sở hữu thường bị ẩn do chính sách bảo mật của VNNIC hoặc dịch vụ ẩn thông tin.

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

b. Ngày hết hạn tên miền

c. Chủ sở hữu tên miền

d. Các name server của tên miền

VNNIC INTERNET RESOURCE WHOIS INFORMATION

This whois query was received from IP Address: **14.161.6.190**
We recognize the resource in your query is: **Domain Name**
Type of domain name: **ASCII Domain Name**
Keyword in your query: **uit.edu.vn**

Domain Information

Domain Name:	uit.edu.vn
Registrant Name:	Trường Đại học Công nghệ Thông tin
Registrar:	Công ty TNHH PA Việt Nam
Creation Date:	2006-10-02
Expiration Date:	2024-10-02
Status:	clientTransferProhibited
Nameserver:	ns1.pavietnam.vn ns2.pavietnam.vn nsbak.pavietnam.net
DNSSEC:	unsigned

7. 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 của MegaCorp one là Mike Carlow.
Địa chỉ email: mcarlow@megacorpone.com

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?

Các nhân viên khác: Stan Denvers, Mike Schneakins, Fred Ducasse, Handy Mckay.

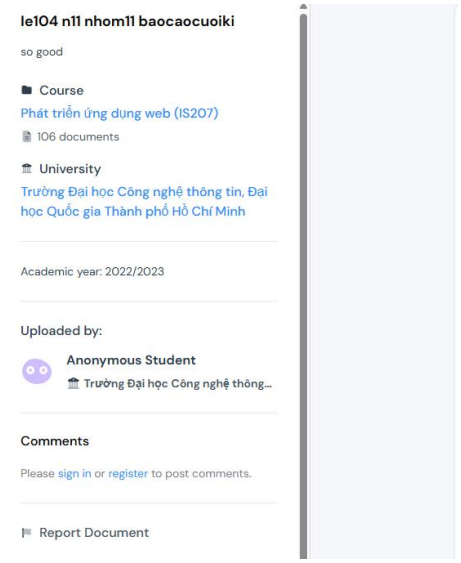
9. Liệt kê một vài từ khóa thường gặp trên Google và cho ví dụ? (Yêu cầu: ít nhất 5 từ khóa)

- "how to": Ví dụ: "How to make pizza" – Cách làm pizza.
- "best": Ví dụ: "Best smartphones 2024" – Những chiếc điện thoại tốt nhất năm 2024.

- "near me": Ví dụ: "Coffee shops near me" – Các quán cà phê gần tôi.
- "tutorial": Ví dụ: "Python tutorial for beginners" – Hướng dẫn Python cho người mới bắt đầu.
- "reviews": Ví dụ: "Laptop reviews" – Đánh giá laptop.

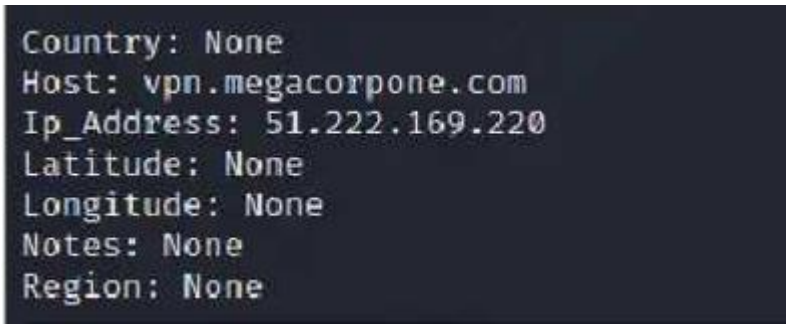
10. Thực hiện tìm kiếm các tài liệu thú vị của Trường Đại học Công nghệ Thông tin mà được công bố trên Internet mà theo bạn là không nên được công bố?

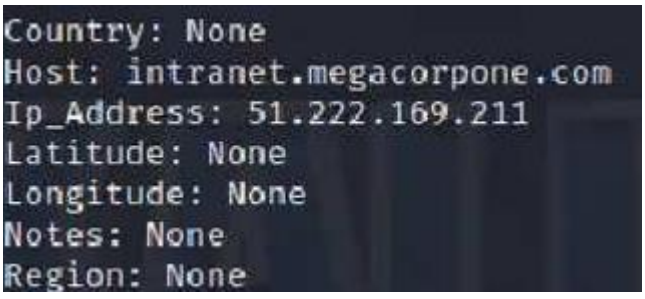
- Các tài liệu nội bộ như đề thi, báo cáo nghiên cứu, hoặc thông tin về nghiên cứu bảo mật có thể không nên công bố công khai nếu chứa thông tin nhạy cảm hoặc chưa được kiểm duyệt.
- Các tài liệu liên quan đến quy trình bảo mật thông tin của trường hoặc thông tin tài chính nội bộ cũng có thể bị rò rỉ nếu công bố mà không kiểm soát đúng mức.



11. Sử dụng Netcraft để xác định máy chủ ứng dụng (application server) đang chạy trên www.megacorpone.com

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



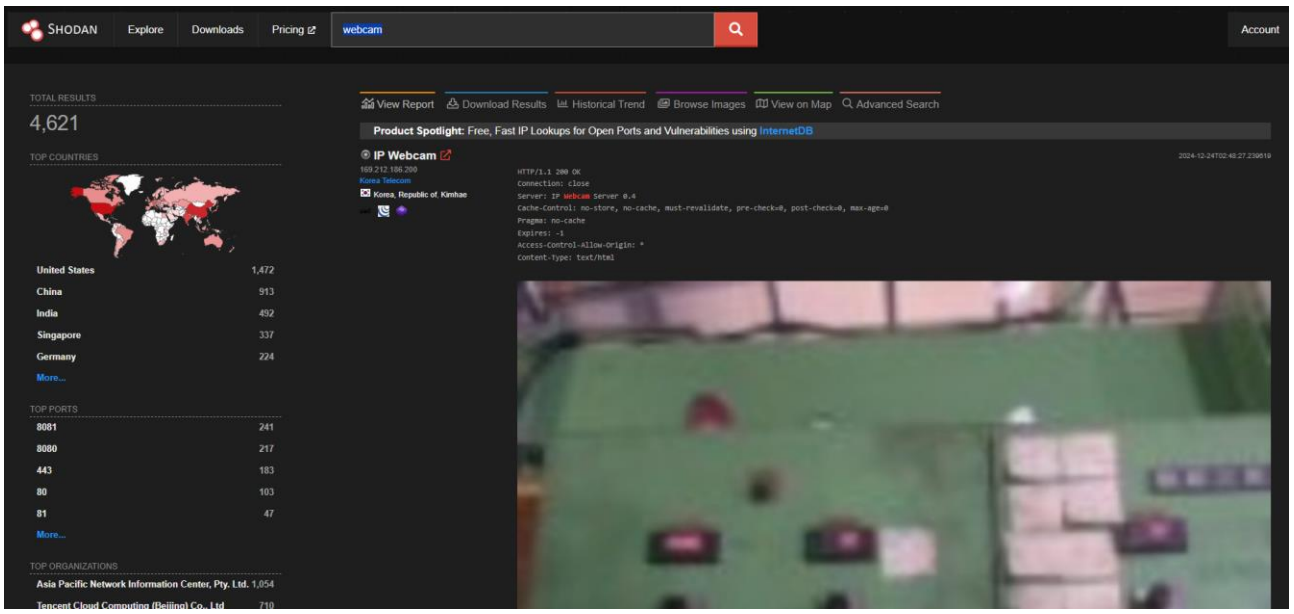


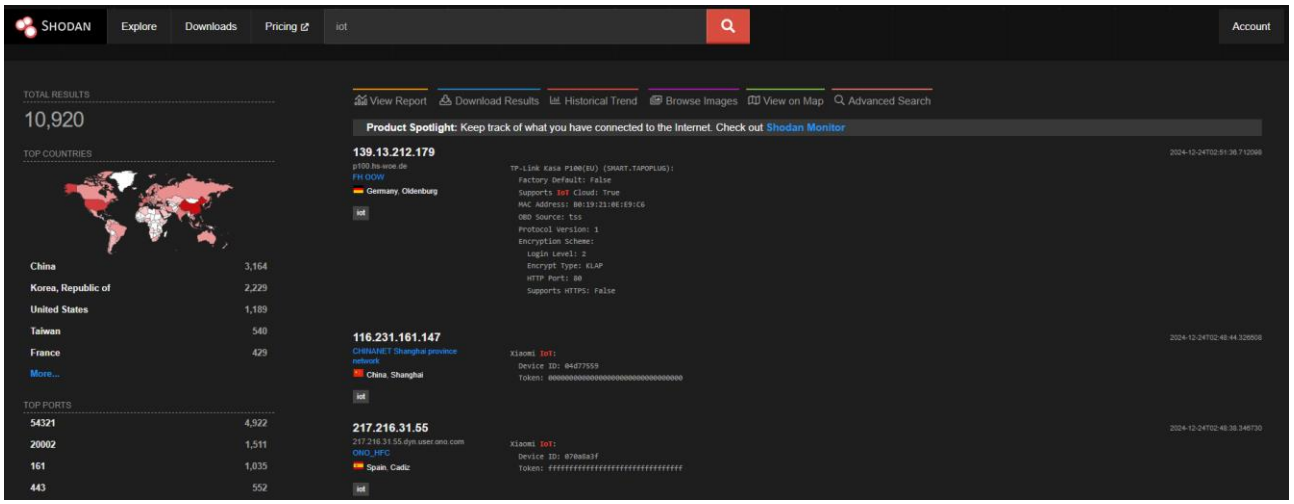
```
Country: None
Host: support.megacorpone.com
Ip_Address: 51.222.169.218
Latitude: None
Longitude: None
Notes: None
Region: None
```

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

```
| 27  | mx1.uit.edu.vn                                                  | 45.122.249.77 |  |  |
|     | hackertarget |
| 28  | mapr2022.uit.edu.vn                                             | 45.122.249.77 |  |  |
|     | hackertarget |
| 29  | a084742fa316491c8c78564efcbce9e0-68f6236f-vm-80.vlab2.uit.edu.vn | 45.122.249.76 |  |  |
|     | hackertarget |
| 30  | host2.uit.edu.vn                                                | 45.122.249.77 |  |  |
|     | hackertarget |
| 31  | mx2.uit.edu.vn                                                  | 45.122.249.77 |  |  |
|     | hackertarget |
| 32  | forum4.uit.edu.vn                                               | 45.122.249.77 |  |  |
|     | hackertarget |
| 33  | kse2015.uit.edu.vn                                              | 45.122.249.77 |  |  |
|     | hackertarget |
| 34  | sois2017.uit.edu.vn                                             | 45.122.249.77 |  |  |
|     | hackertarget |
| 35  | mapr2018.uit.edu.vn                                             | 45.122.249.77 |  |  |
|     | hackertarget |
|     | hackertarget |
| 212 | debian.uit.edu.vn                                               | 118.69.123.140 |  |  |
|     | hackertarget |
| 213 | congdoan.uit.edu.vn                                             | 118.69.123.140 |  |  |
|     | hackertarget |
| 214 | khcn.uit.edu.vn                                                 | 118.69.123.140 |  |  |
|     | hackertarget |
| 215 | qhdn.uit.edu.vn                                                 | 45.122.249.78 |  |  |
|     | hackertarget |
| 216 | en.uit.edu.vn                                                   | 45.122.249.78 |  |  |
|     | hackertarget |
| 217 | thuvien.uit.edu.vn                                              | 45.122.249.78 |  |  |
|     | hackertarget |
| 218 | www.thuvien.uit.edu.vn                                          | 118.69.123.140 |  |  |
|     | hackertarget |
| 219 | cybertrain.uit.edu.vn                                           | 118.69.123.140 |  |  |
|     | hackertarget |
| 220 | doantn.uit.edu.vn                                               | 118.69.123.140 |  |  |
|     | hackertarget |
| 221 | dangbo.uit.edu.vn                                               | 118.69.123.140 |  |  |
|     | hackertarget |
| 222 | huongnghiep.uit.edu.vn                                          | 118.69.123.140 |  |  |
|     | hackertarget |
| 223 | oep.uit.edu.vn                                                  | 45.122.249.78 |  |  |
```

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.





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

- Shodan:
  - Tìm kiếm các thiết bị kết nối Internet (máy chủ, camera, router, IoT, v.v.).
  - Hiển thị cổng dịch vụ mở, phiên bản phần mềm, và lỗ hổng bảo mật.
  - Chủ yếu dùng cho bảo mật mạng và phân tích các thiết bị trực tuyến.
- Google/Bing:

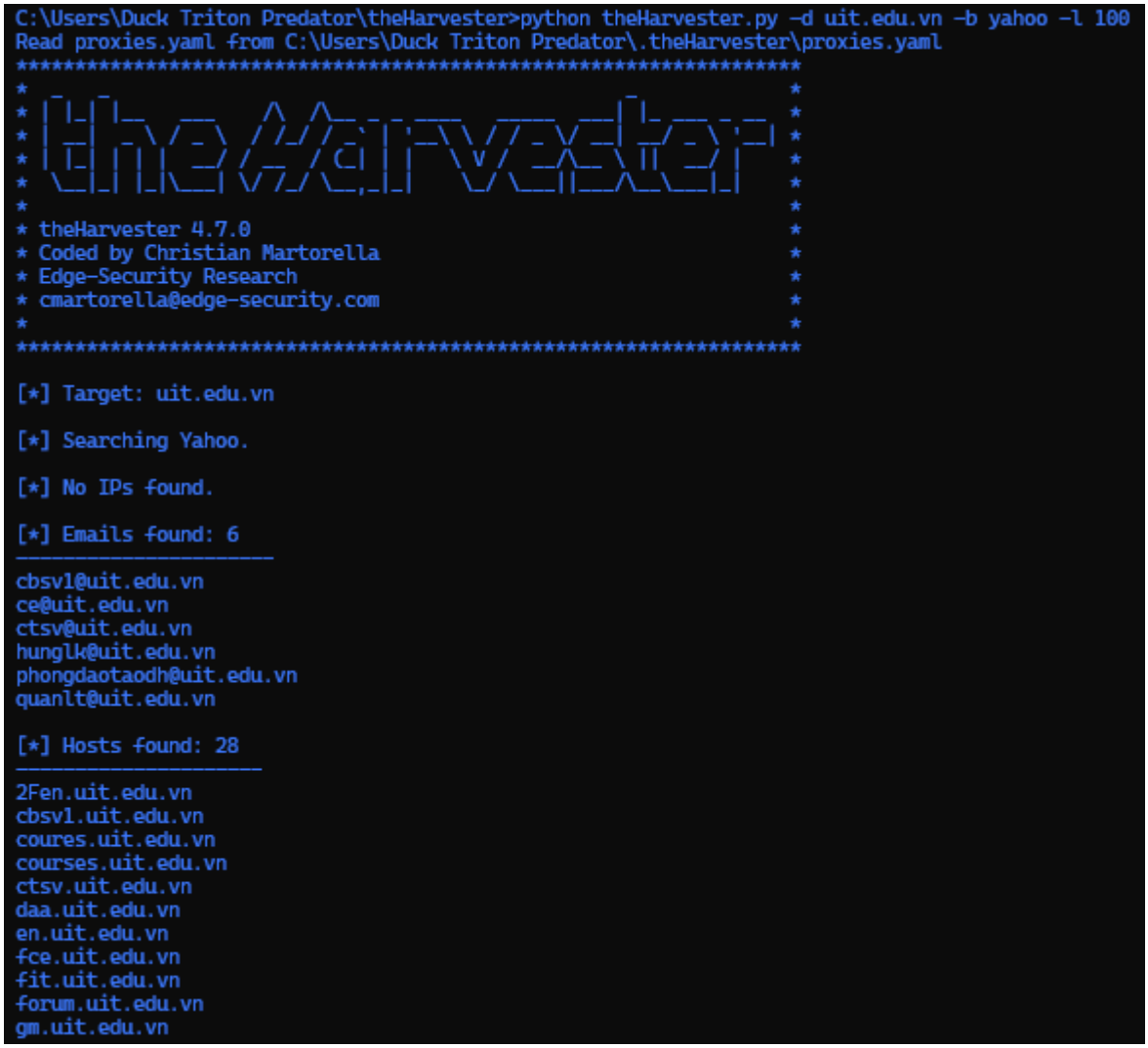
- Tìm kiếm nội dung web như bài viết, hình ảnh, video, sản phẩm.
- Không tìm kiếm thông tin về cổng dịch vụ mở hay các thiết bị kết nối.
- Dùng cho tìm kiếm thông tin trên web, không phải thiết bị mạng.

Kết luận: Shodan chuyên về thiết bị và bảo mật mạng, còn Google/Bing tập trung vào tìm kiếm thông tin web.

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

```
Created default api-keys.yaml at C:\Users\Duck Triton Predator\.theHarvester\api-keys.yaml
        Searching 0 results.
[*] Searching Bing.

[*] No IPs found.

[*] Emails found: 2
----------------------
info.httt@uit.edu.vn
phongdaotaodh@uit.edu.vn

[*] Hosts found: 13
---------------------
ctsv.uit.edu.vn
daa.uit.edu.vn
en.uit.edu.vn
fce.uit.edu.vn
forum.uit.edu.vn
httt.uit.edu.vn
i-english.uit.edu.vn
iot.uit.edu.vn
link.uit.edu.vn
oep.uit.edu.vn
sdh.uit.edu.vn
student.uit.edu.vn
tuyensinh.uit.edu.vn
```

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



1. Bing (-b bing)

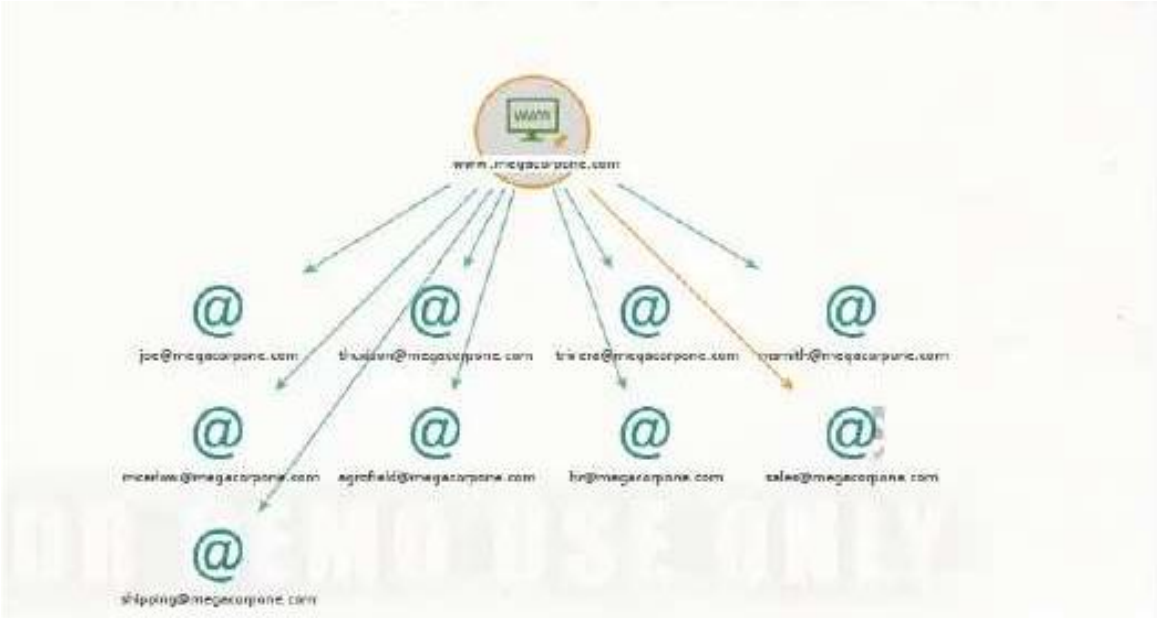
- Ưu điểm:
    - Bing cũng có khả năng tìm kiếm mạnh mẽ và thường ít bị hạn chế hơn Google.
    - Hỗ trợ tìm kiếm theo tên miền hoặc địa chỉ email rất tốt.
    - Kết quả có thể có một số thông tin mà Google không trả về, ví dụ như thông tin từ các website ít phổ biến hơn.
- Nhược điểm:
    - Không mạnh mẽ bằng Google trong việc tìm kiếm các tài liệu hoặc các email công khai.

2. Yahoo (-b yahoo)

- Ưu điểm:
    - Yahoo có khả năng tìm kiếm các thông tin cũ hơn, đôi khi có thể tìm thấy dữ liệu đã bị Google hoặc Bing bỏ qua.
- Nhược điểm:
    - Hiệu quả tìm kiếm có thể không mạnh mẽ bằng Google hay Bing.
    - Tương tác với Yahoo có thể không được tối ưu như các công cụ khác.

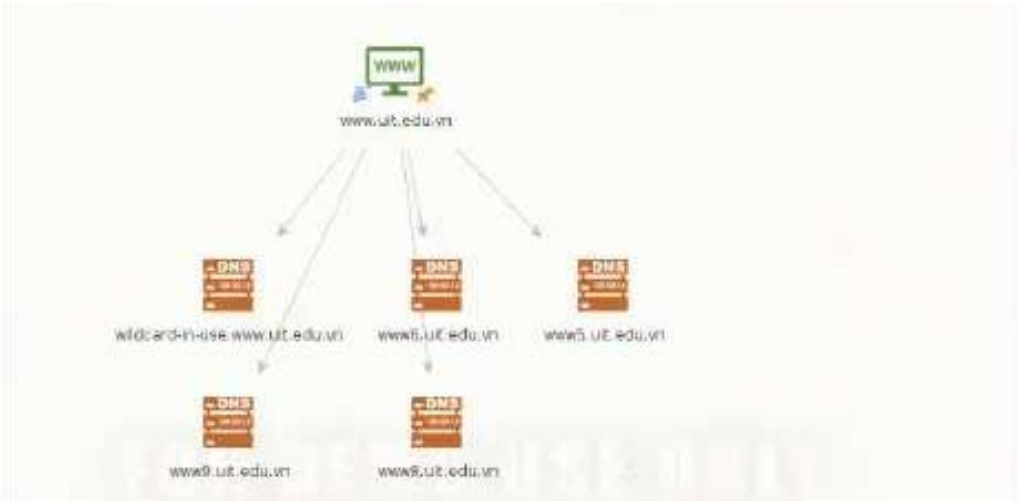
Kết quả đem lại trong việc tìm kiếm địa chỉ gmaile của Yahoo tốt hơn Bing do có thể tìm kiếm các thông cũ và dễ bị bỏ qua.

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



20. 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.

21. 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?

```
Host idontexist.uit.edu.vn not found: 3(NXDOMAIN)
```

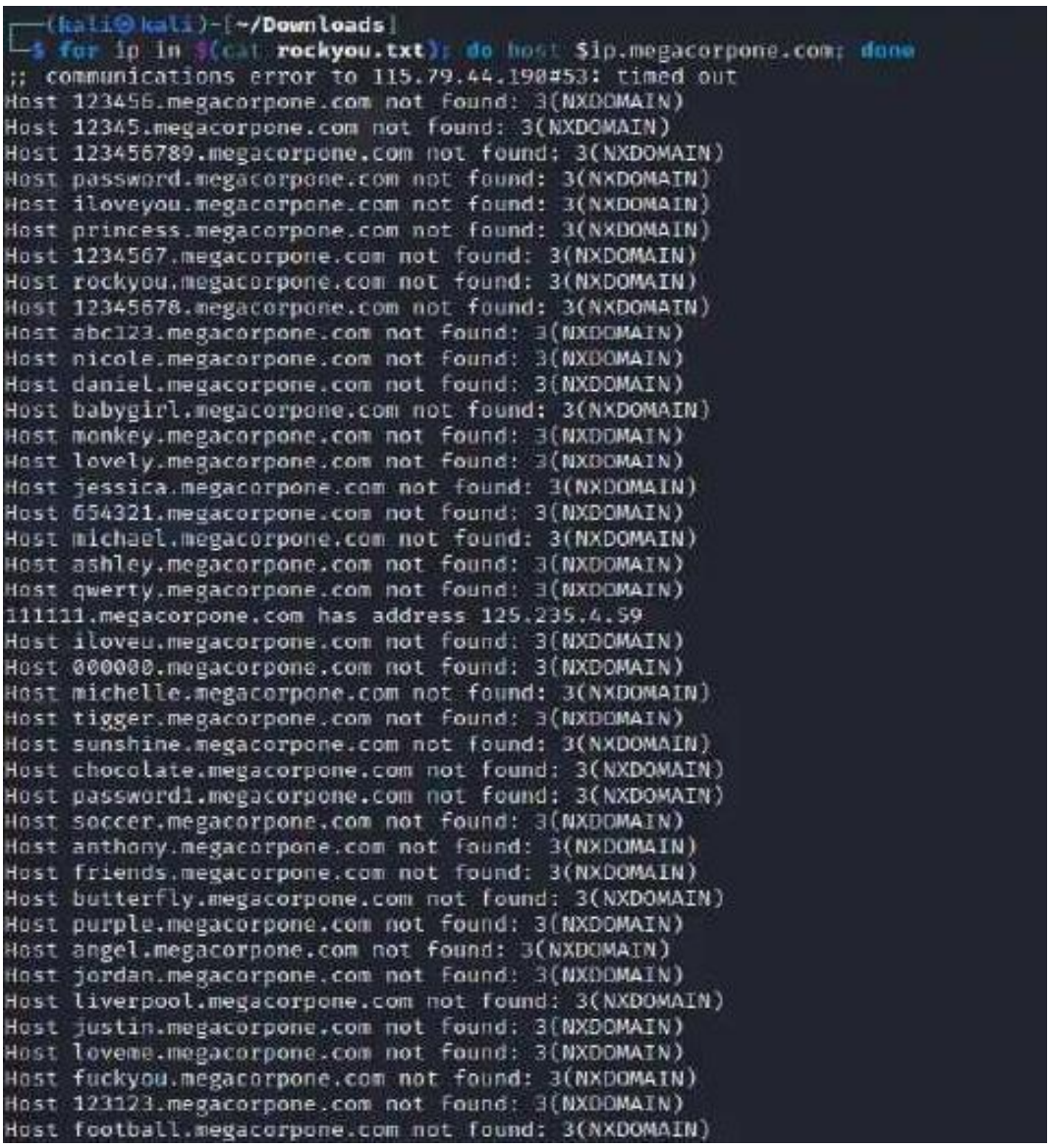
```
Host idontexist.uit.edu.vn not found: 3(NXDOMAIN)
```

```
Host noexist.uit.edu.vn not found: 3(NXDOMAIN)
```

Nhận xét về kết quả:

- NXDOMAIN: Kết quả trả về thông báo NXDOMAIN, điều này có nghĩa là hostname không tồn tại trong hệ thống DNS của tên miền uit.edu.vn.
- Không tìm thấy địa chỉ IP: Khi hostname không tồn tại trong DNS, không có địa chỉ IP được trả về. Điều này có thể chỉ ra rằng tên miền chưa được cấu hình hoặc không tồn tại trong cơ sở dữ liệu của DNS.
- Giải thích:
    - NXDOMAIN là một mã lỗi trả về từ DNS, chỉ ra rằng tên miền hoặc hostname không tồn tại. Đây là phản hồi chuẩn khi bạn yêu cầu DNS tra cứu một tên miền không được đăng ký hoặc không tồn tại trong cơ sở dữ liệu của DNS.

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



23. 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.

```
domains=("hcmus.edu.vn" "hcmussh.edu.vn" "uit.edu.vn" "hcmut.edu.vn" "hcmiu.edu.vn" "uel.edu.vn" "hcmier.edu.vn" "vnuhcm.edu.vn")

for domain in "${domains[@]}"; do
    echo "----------------------------------------------------"
    echo "Tìm nameservers của domain: $domain"

    ns=$(dig ns $domain +short)

    if [ -n "$ns" ]; then
        echo "Danh sách nameserver của $domain:"
        echo "$ns"

        for server in $ns; do
            echo "Thực hiện zone transfer với nameserver: $server"
            dig axfr $domain @$server
        done
    else
        echo "Không tìm thấy nameserver cho $domain"
    fi
    echo "----------------------------------------------------"
done
```

```
Thực hiện zone transfer với nameserver: ns1.hcmus.edu.vn
; <<>> DiG 9.10.6 <<>> axfr hcmus.edu.vn @ns1.hcmus.edu.vn
;; global options: +cmd
hcmus.edu.vn.         86400   IN      SOA     ns1.hcmus.edu.vn. admin.hcmus.edu.vn.
hcmus.edu.vn.         86400   IN      NS      ns1.hcmus.edu.vn.
hcmus.edu.vn.         86400   IN      NS      ns2.hcmus.edu.vn.
hcmus.edu.vn.         3600    IN      A       192.168.1.1
hcmus.edu.vn.         3600    IN      MX      10 mail.hcmus.edu.vn.
----------------------------------------------------
```

24. Viết Liệt kê danh sách các loại enumeration có thể được sử dụng cùng với tùy chọn nhất là 2 ví dụ) -t

-t domain: Tìm kiếm thông tin về tên miền.

- Ví dụ: theHarvester -d uit.edu.vn -b google -t domain

-t email: Liệt kê các địa chỉ email liên quan đến tên miền.

- Ví dụ: theHarvester -d uit.edu.vn -b google -t email

-t net: Tìm kiếm thông tin về mạng (IP, host).

- Ví dụ: theHarvester -d uit.edu.vn -b google -t net

-t whois: Tìm kiếm thông tin WHOIS về tên miền.

- Ví dụ: theHarvester -d uit.edu.vn -b google -t whois

-t subdomain: Tìm kiếm các subdomains của tên miền.

- Ví dụ: theHarvester -d uit.edu.vn -b google -t subdomain

25. Cho một vài ví dụ sử dụng kết hợp các tùy chọn được DNSRecon hỗ trợ khác (ít nhất là 2 ví dụ)

Ví dụ 1: Tìm DNS records và thực hiện Zone Transfer

dnsrecon -d uit.edu.vn -t axfr -t std

- -d uit.edu.vn: Tên miền cần kiểm tra.
- -t axfr: Thực hiện zone transfer (lấy toàn bộ bản ghi DNS).
- -t std: Lấy các bản ghi DNS chuẩn (A, MX, NS, CNAME, TXT, v.v.).

Ví dụ 2: Brute-force Subdomain và Tìm DNS Records

dnsrecon -d uit.edu.vn -t brt -t std

- -d uit.edu.vn: Tên miền cần kiểm tra.
- -t brt: Brute-force tìm kiếm subdomains.
- -t std: Lấy các bản ghi DNS chuẩn.

26. 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?

So sánh DNSEnum và DNSRecon:

- Dễ sử dụng:
    - DNSEnum: Đơn giản, dễ sử dụng cho các nhiệm vụ cơ bản như tìm kiếm DNS và brute-force subdomains.
    - DNSRecon: Phức tạp hơn nhưng cung cấp nhiều tính năng nâng cao, dễ sử dụng với người có kinh nghiệm.
- Kết quả chính xác:

- DNSEnum: Chính xác cho các tên miền hỗ trợ zone transfer và subdomain brute-forcing, nhưng có thể thiếu sót nếu không hỗ trợ.
- DNSRecon: Kết quả chính xác hơn nhờ nhiều phương pháp kiểm tra và phân tích DNS nâng cao.

- Kết quả hiển thị:
  - DNSEnum: Hiển thị ít kết quả, chủ yếu là bản ghi cơ bản.
  - DNSRecon: Hiển thị nhiều kết quả hơn và cung cấp thông tin chi tiết hơn (PTR, CNAME, reverse lookup).

a) Kết luận:

- DNSRecon mạnh mẽ hơn và cung cấp kết quả chính xác, chi tiết hơn, nhưng DNSEnum dễ sử dụng cho các tác vụ cơ bản.

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

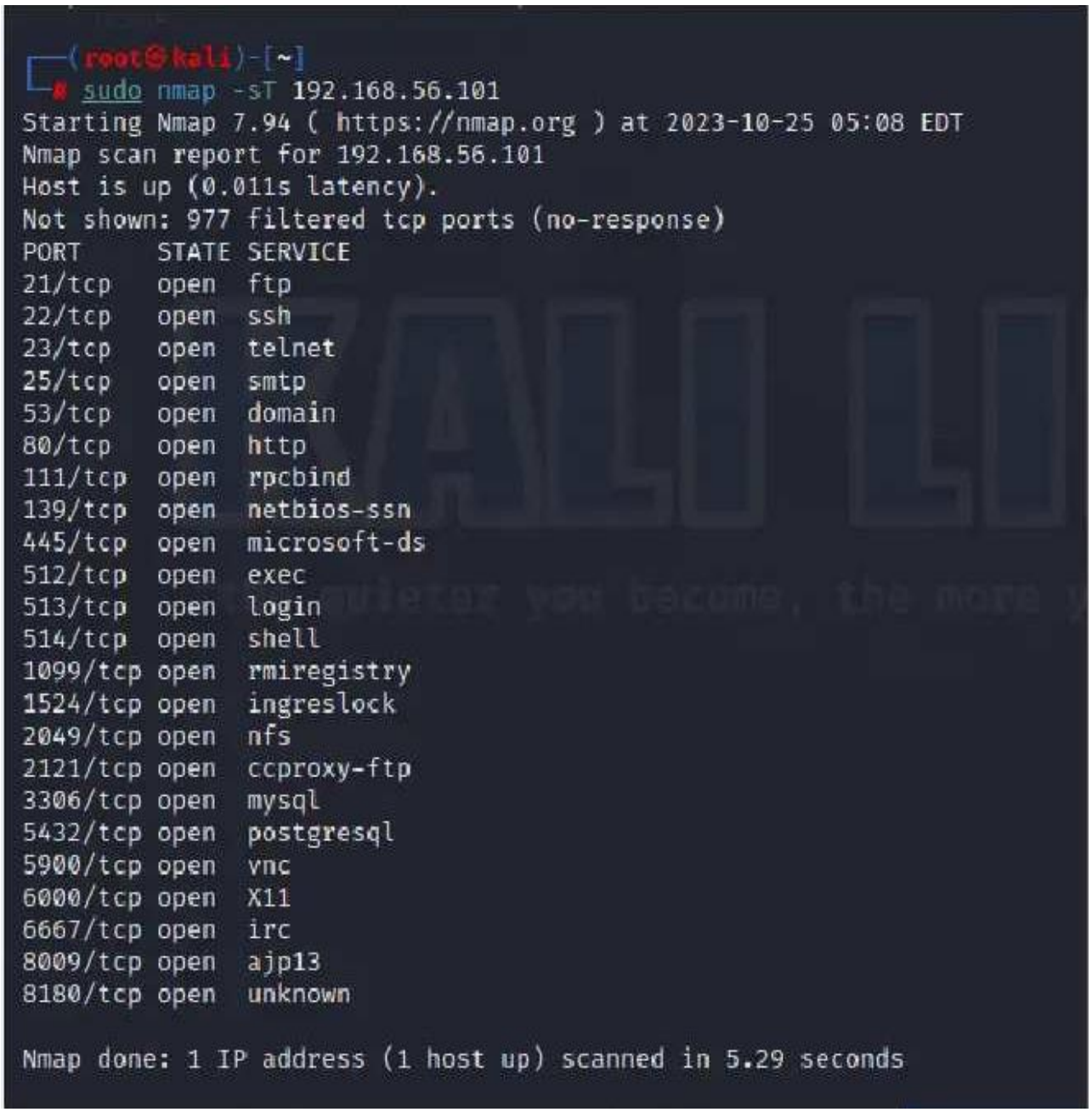
SYN Scan sử dụng Nmap

```
┌──(kali㉿kali)-[~]
└─$ sudo -i
[sudo] password for kali:
┌──(root㉿kali)-[~]
└─# sudo nmap -sS 192.168.56.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 05:07 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0081s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 11.27 seconds
┌──(root㉿kali)-[~]
└─#
```

Dùng Wireshark

2888 3.912078927	10.0.2.15	192.168.56.101	TCP	58 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2889 3.920507030	10.0.2.15	192.168.56.101	TCP	54 [ACK] Seq=1 Ack=1 Win=1024 Len=0

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



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…)

1. Số lượng gói tin

- SYN Scan: Gửi ít gói tin (chỉ SYN, nhận SYN-ACK/RST).
- TCP Connect Scan: Gửi nhiều gói tin hơn (thực hiện đầy đủ three-way handshake và gửi thêm FIN/RST).

2. Thời gian quét

- SYN Scan: Nhanh hơn vì không hoàn tất kết nối TCP.
- TCP Connect Scan: Chậm hơn do thực hiện kết nối đầy đủ.

3. Phát hiện bởi IDS/IPS

- SYN Scan: Khó bị phát hiện hơn vì không hoàn tất kết nối.
- TCP Connect Scan: Dễ bị phát hiện do tạo kết nối đầy đủ và ghi lại trong nhật ký.

4. Kết quả hiển thị

- Cả hai đều hiển thị trạng thái cổng: Open, Closed, Filtered.

5. Ưu, nhược điểm

- SYN Scan:
  - Ưu điểm: Nhanh, nhẹ, khó phát hiện.
  - Nhược điểm: Không hoạt động nếu tường lửa chặn gói SYN.
- TCP Connect Scan:
  - Ưu điểm: Không cần quyền root, hoạt động trên mọi mạng.
  - Nhược điểm: Chậm hơn, dễ bị phát hiện.

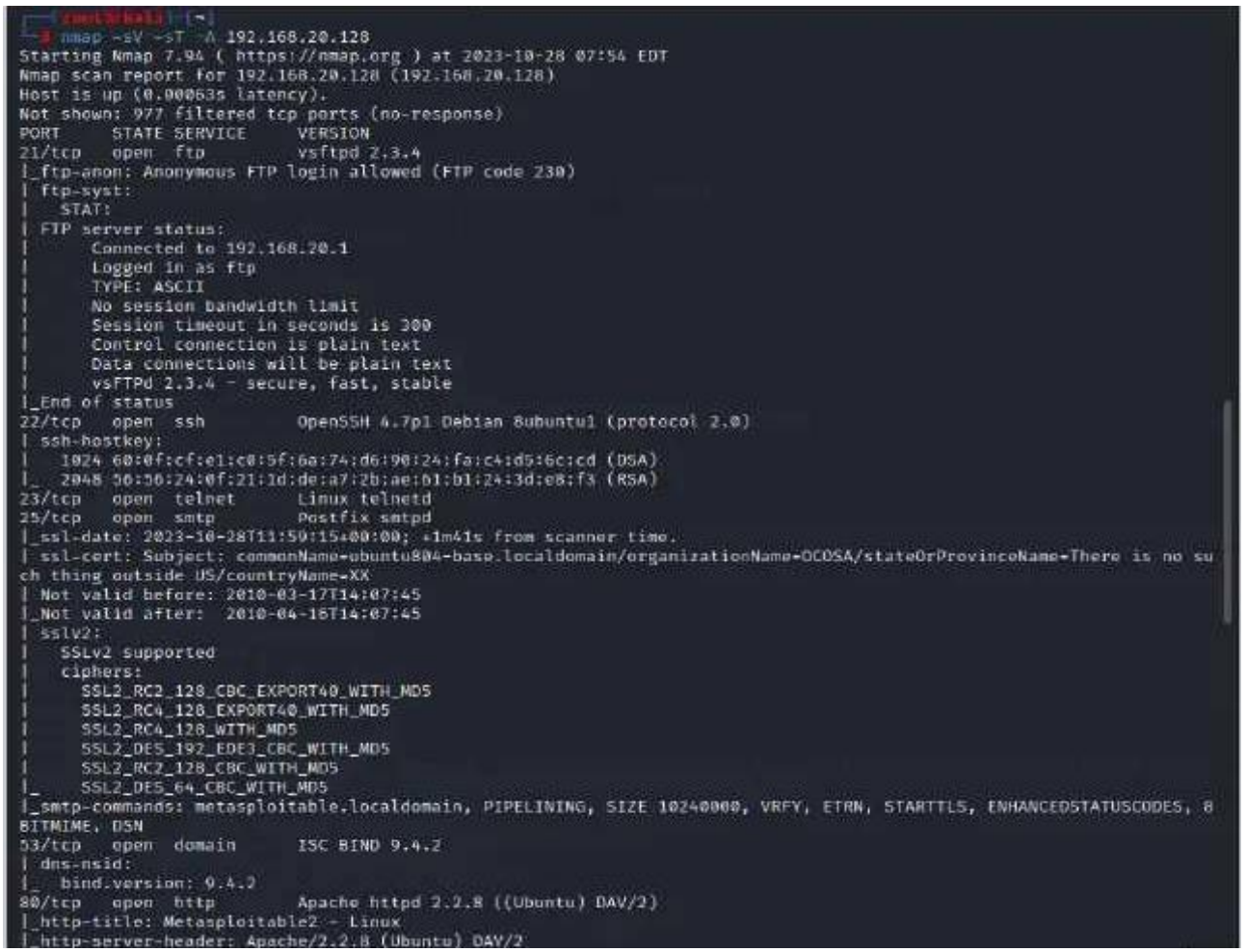
30. Thực hiện kiểm tra các host đang hoạt trong mạng bằng các ngôn ngữ lập trình khác (Bash script, Python, C/C++, Perl, …)

```c
int main() {
    char ip[16];
    char command[64];
    int subnet = 1;

    printf("Scanning active hosts in network 192.168.%d.0/24...\n", subnet);
    for (int i = 1; i <= 254; i++) {
        sprintf(ip, "192.168.%d.%d", subnet, i);
        sprintf(command, "ping -c 1 -W 1 %s > /dev/null 2>&1", ip);
        if (system(command) == 0) {
            printf("Host %s is up\n", ip);
        }
    }

    return 0;
}
```

```
Scanning active hosts in network 192.168.1.0/24...

Host 192.168.1.1 is up
Host 192.168.1.10 is up
Host 192.168.1.25 is up
Host 192.168.1.50 is up
Host 192.168.1.100 is up
Host 192.168.1.200 is up
```

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

32. Liệt kê các banner, dịch vụ đang chạy trên máy Metasploitable 2 (chỉ liệt kê các dịch vụ TCP).



```
nmap -sV -sT -A 192.168.20.128
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-28 07:54 EDT
Nmap scan report for 192.168.20.128 (192.168.20.128)
Host is up (0.00063s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.20.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2023-10-28T11:59:15+00:00; +1m41s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no su
ch thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8
BITMIME, DSN
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```

33. 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 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]-ExeX_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

  *Ví dụ: [*NT101.K11.ANTT*]-Exe01_Group03.*
- 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 nộp.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

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