

BÁO CÁO THỰC HÀNH

Môn học: Bảo mật Web và Ứng dụng

Lab 3: Reconnaissance

GVHD: Ngô Khánh Khoa

Nhóm: 6

1. THÔNG TIN CHUNG:

Lớp: NT213.P11.ANTT.2

STT	Họ và tên	MSSV	Email
1	Lại Quan Thiên	22521385	22521385@gm.uit.edu.vn
2	Mai Nguyễn Nam Phương	22521164	22521164@gm.uit.edu.vn
3	Hồ Diệp Huy	22520541	22520541@gm.uit.edu.vn
4	Nguyễn Phúc Nhi	22521041	22521041@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Nội dung	Tình Trạng	Thực hiện
1	Bài 1	100%	Quan Thiên
2	Bài 2	100%	Diệp Huy
3	Bài 3	100%	Phúc Nhi
4	Bài 4	100%	Nam Phương
5	Bài 5	100%	Diệp Huy
6	Bài 6	100%	Phúc Nhi
7	Bài 7	100%	Quan Thiên
8	Bài 8	100%	Nam Phương
9	Bài 9	100%	Diệp Huy
10	Bài 10	100%	Phúc Nhi
11	Bài 11	100%	Quan Thiên
12	Bài 12	100%	Phúc Nhi
13	Bài 13	100%	Nam Phương
14	Bài 14	100%	Quan Thiên

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

15	Bài 15	100%	Diệp Huy
16	Bài tập Luyện tập 6.1	100%	Phúc Nhi
17	Bài tập Luyện tập Try Hack Me	100%	Nam Phương
18	Bài tập Luyện tập Hack The Box	90%	Thiên, Huy

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

BÁO CÁO CHI TIẾT

Bài tập 1: Thực hiện lệnh WHOIS lookup với tên miền indriver.com.

- *Id của IANA của tên miền trên là gì?*
- *Tên miền trên được đăng ký khi nào?*
- *Registrar của tên miền trên?*
- *Công ty nào được sử dụng cho dịch vụ name server?*
- *Địa chỉ admin contact email cho tên miền trên?*

Trả lời:

```
(kali㉿thinnnlinux)-[~]
$ whois indriver.com
Domain Name: INDRIVER.COM
Registry Domain ID: 130600645_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: http://cscdbs.com
Updated Date: 2024-08-26T14:18:16Z
Creation Date: 2004-09-21T21:01:04Z
Registry Expiry Date: 2025-09-21T21:01:04Z
Registrar: CSC Corporate Domains, Inc.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: 8887802723
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS-1336.AWSDNS-39.ORG
Name Server: NS-1696.AWSDNS-20.CO.UK
Name Server: NS-294.AWSDNS-36.COM
Name Server: NS-621.AWSDNS-13.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-11-19T07:32:06Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability. VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
```

```

Domain Name: indriver.com
Registry Domain ID: 130600645_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectbrands.com
Updated Date: 2024-08-26T10:18:16Z
Creation Date: 2004-09-21T07:00:00Z
Registrar Registration Expiration Date: 2025-09-21T21:01:04Z
Registrar: CSC CORPORATE DOMAINS, INC.
Sponsoring Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887882723
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Domain Manager
Registrant Organization: SUOL INNOVATIONS LTD
Registrant Street: 41 Themistokli Dervi, Hawaii Tower, 1ST Floor, Office 106
Registrant City: Nicosia
Registrant State/Province: Nicosia
Registrant Postal Code: 1066
Registrant Country: CY
Registrant Phone: +357.22667730
Registrant Phone Ext:
Registrant Fax Ext:
Registrant Fax: +357.22667740
Registrant Email: domainmaster@indriver.com
Registry Admin ID:
Admin Name: Domain Manager
Admin Organization: SUOL INNOVATIONS LTD
Admin Street: 41 Themistokli Dervi, Hawaii Tower, 1ST Floor, Office 106
Admin City: Nicosia
Admin State/Province: Nicosia
Admin Postal Code: 1066
Admin Country: CY
Admin Phone: +357.22667730
Admin Phone Ext:
Admin Fax: +357.22667740
Admin Fax Ext:
Admin Email: domainmaster@indriver.com
Registry Tech ID:
Tech Name: Domain Manager
Tech Organization: SUOL INNOVATIONS LTD
Tech Street: 41 Themistokli Dervi, Hawaii Tower, 1ST Floor, Office 106
Tech City: Nicosia
Tech State/Province: Nicosia
Tech Postal Code: 1066
Tech Country: CY
Tech Phone: +357.22667730
Tech Phone Ext:
Tech Fax: +357.22667740
Tech Fax Ext:
Tech Email: domainmaster@indriver.com
Name Server: ns-294.awsdns-36.com
Name Server: ns-1696.awsdns-20.co.uk
Name Server: ns-1336.awsdns-39.org
Name Server: ns-621.awsdns-13.net
DNSSEC Unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-08-26T10:18:16Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

Corporation Service Company(c) (CSC) The Trusted Partner of More than 50% of the 100 Best Global Brands.

Contact us to learn more about our enterprise solutions for Global Domain Name Registration and Management, Trademark Research and Watching, Brand, Logo and Auction Monitoring, as well as SSL Certificate Services and DNS Hosting.

NOTICE: You are not authorized to access or query our WHOIS database through the use of high-volume, automated, electronic processes or for the purpose or purposes of using the data in any manner that violates these terms of use. The Data in the CSC WHOIS database is provided by CSC for information purposes only, and to assist persons in obtaining information about or related to a domain name registration record. CSC does not guarantee its accuracy. By submitting a WHOIS query, you agree to abide by the following terms of use: you agree that you may use this Data only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via direct mail, e-mail, telephone, or fax imile; or (2) enable high volume, automated, electronic processes that apply to CSC (or its computer systems). CSC reserves the right to terminate your access to the WHOIS database in its sole discretion for any violations by you of these terms of use. CSC reserves the right to modify these terms at any time.

Register your domain name at http://www.cscglobal.com
[kali㉿thinnnlinux: ~]
[kali㉿thinnnlinux: ~]
$ |

```

- Video thực hiện: <https://youtu.be/pWiM6hGhuPg>
 - ID của IANA của tên miền trên là gì? ID IANA của tên miền là: 299
 - Tên miền trên được đăng ký khi nào? Ngày đăng ký: 2004-09-21 (21 tháng 9 năm 2004).
 - Registrar của tên miền trên? Registrar: CSC Corporate Domains, Inc.
 - Công ty nào được sử dụng cho dịch vụ name server? Công ty: Amazon Web Services (AWS), thông qua các name server:
 - + ns-294.awsdns-36.com
 - + ns-1696.awsdns-20.co.uk
 - + ns-1336.awsdns-39.org
 - + ns-621.awsdns-13.net
 - Địa chỉ admin contact email cho tên miền trên?
- =>Admin contact email: domainmaster@indriver.com

Bài tập 2. So sánh kết quả khi thực hiện nslookup và dig với loại query là mx với tên miền indriver.com, thông tin nào được cung cấp thêm bởi lệnh DIG, ý nghĩa các thông tin đó như thế nào?

- Video thực hiện: <https://youtu.be/3X8jFgLfMLE>

```
hohuy@ubuntu:~$ nslookup -query=mx indriver.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
indriver.com    mail exchanger = 14 alt4.aspmx.l.google.com.
indriver.com    mail exchanger = 10 aspmx.l.google.com.
indriver.com    mail exchanger = 12 alt2.aspmx.l.google.com.
indriver.com    mail exchanger = 11 alt1.aspmx.l.google.com.
indriver.com    mail exchanger = 13 alt3.aspmx.l.google.com.

Authoritative answers can be found from:

hohuy@ubuntu:~$ dig indriver.com MX

; <>> DiG 9.18.28-0ubuntu0.20.04.1-Ubuntu <>> indriver.com MX
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 35411
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;indriver.com.           IN      MX

;; ANSWER SECTION:
indriver.com.        0       IN      MX      13 alt3.aspmx.l.google.com.
indriver.com.        0       IN      MX      11 alt1.aspmx.l.google.com.
indriver.com.        0       IN      MX      12 alt2.aspmx.l.google.com.
indriver.com.        0       IN      MX      10 aspmx.l.google.com.
indriver.com.        0       IN      MX      14 alt4.aspmx.l.google.com.

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Tue Nov 19 09:39:54 PST 2024
;; MSG SIZE rcvd: 156

hohuy@ubuntu:~$
```

- Thông tin được cung cấp thêm bởi lệnh DIG:

- + HEADER: giúp biết rằng truy vấn đã được thực hiện thành công, không có lỗi xảy ra, và cho thấy các đặc tính của truy vấn

- + OPT PSEUDOSECTION: Phần này cho biết rằng lệnh dig đã sử dụng tính năng mở rộng của DNS (EDNS), cho phép truyền dữ liệu lớn hơn, cải thiện tốc độ và độ tin cậy của truy vấn DNS

- + QUESTION SECTION: kiểm tra xem truy vấn đã thực hiện đúng như yêu cầu hay chưa

- + ANSWER SECTION: Cho biết kết quả của truy vấn và thông tin MX record có thể được lưu trữ (cached) trong khoảng thời gian TTL

Bài tập 3: Thực hiện truy vấn IP với tên miền indriver.com? Địa chỉ IP nào map với indriver.com? Tên miền nào trả đến địa chỉ 134.209.24.248? Mail server nào liên quan đến tên miền indriver.com?

Trả lời:

- Video thực hiện: <https://youtu.be/HFVLM-jaDi8>
- Truy vấn IP với tên miền indriver.com bằng câu lệnh `nslookup indriver.com`

```
(kali㉿kali)-[~]
└─$ nslookup indriver.com
Server: Startup tron 192.168.64.2
Address: 192.168.64.2#53

Non-authoritative answer:
Name: indriver.com
Address: 108.157.32.99
Name: indriver.com
Address: 108.157.32.115
Name: indriver.com
Address: 108.157.32.3
Name: indriver.com
Address: 108.157.32.21
```

- Địa chỉ IP map với indriver.com là 108.157.32.21

```
(kali㉿kali)-[~]
└─$ host 134.209.24.248
248.24.209.134.in-addr.arpa domain name pointer inlanefreight.com.
```

- Tên miền trả đến địa chỉ 134.209.24.248 là inlanefreight.com

```
(kali㉿kali)-[~]
└─$ nslookup -query=mx indriver.com
Server: 192.168.64.2
Address: 192.168.64.2#53

Non-authoritative answer:
indriver.com mail exchanger = 13 alt3.aspmx.l.google.com.
indriver.com mail exchanger = 12 alt2.aspmx.l.google.com.
indriver.com mail exchanger = 10 aspmx.l.google.com.
indriver.com mail exchanger = 14 alt4.aspmx.l.google.com.
indriver.com mail exchanger = 11 alt1.aspmx.l.google.com.

Authoritative answers can be found from:
```

- Mail server liên quan đến tên miền indriver.com là:

```
mail exchanger = 13 alt3.aspmx.l.google.com.
mail exchanger = 12 alt2.aspmx.l.google.com.
mail exchanger = 10 aspmx.l.google.com.
mail exchanger = 14 alt4.aspmx.l.google.com.
mail exchanger = 11 alt1.aspmx.l.google.com.
```

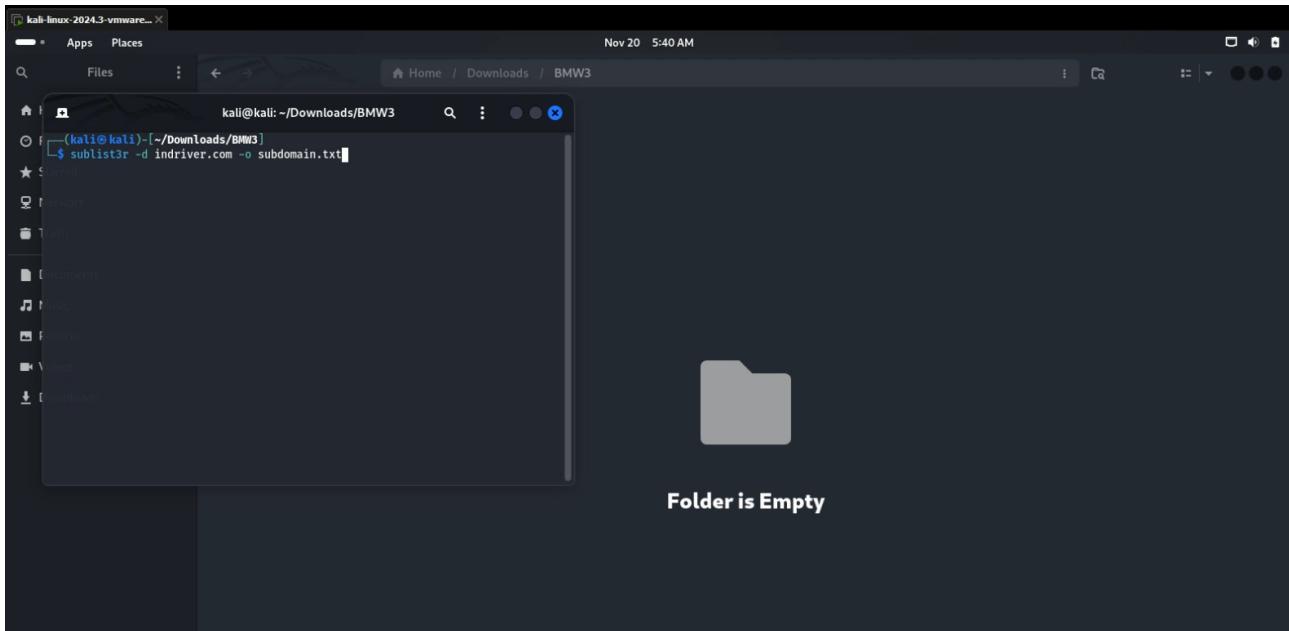
Bài tập 4: Liệt kê các tên miền phụ của indriver.com, kết quả được lưu trong file csv

- Video thực hiện: <https://youtu.be/lo28WLkCu8I>

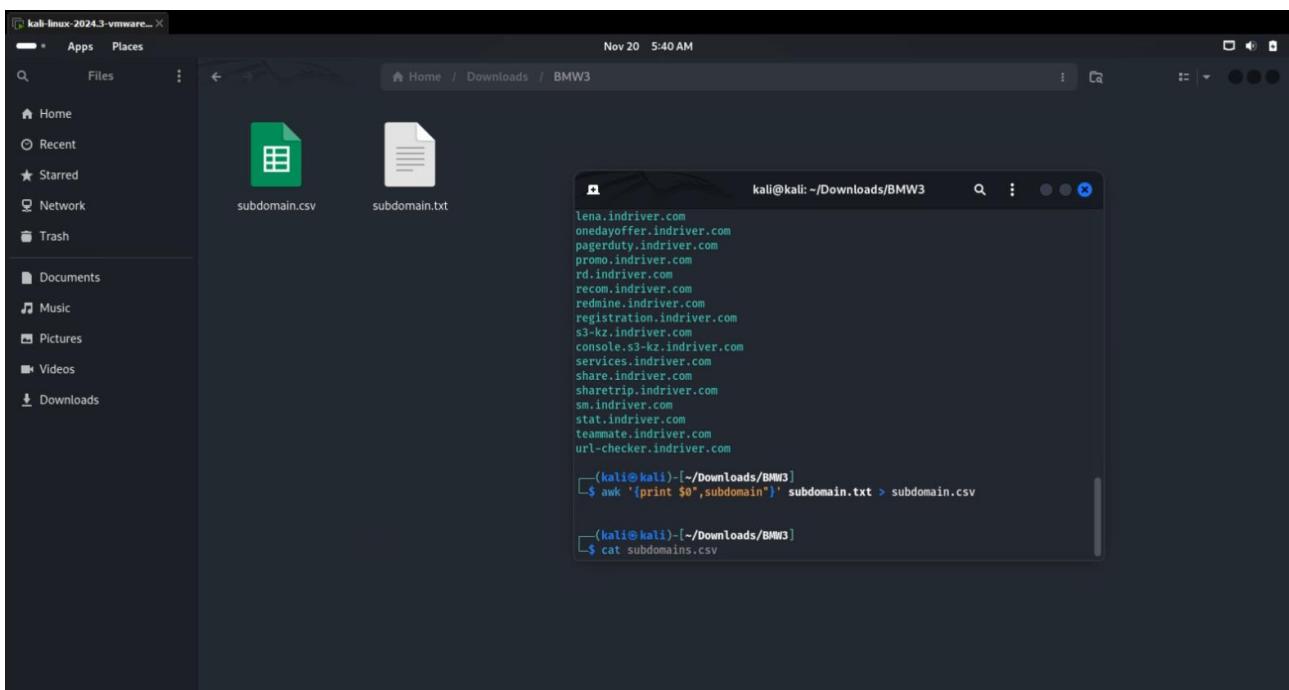
- Sử dụng lệnh “sublist3r -d indriver.com -o subdomain.txt” để sử dụng công cụ sublist3r nhằm liệt kê ra được các miền phụ của indriver.com

+ Cờ -d indriver.com chỉ định tên miền đích là indriver.com mà bạn muốn thu thập các subdomain

+ Cờ -o subdomain.txt cho biết rằng tất cả các subdomain được tìm thấy sẽ được lưu vào file subdomain.txt



- Sử dụng “awk '{print \$0",subdomain"}' subdomain.txt > subdomain.csv” để chuyển kết quả từ file txt sang csv





- Kết quả:

The terminal window shows the following command and its output:

```
services.indriver.com
share.indriver.com
sharetrip.indriver.com
sm.indriver.com
stat.indriver.com
teammate.indriver.com
url-checker.indriver.com

(kali㉿kali)-[~/Downloads/BMW3]
$ awk '{print $0",subdomain"}' subdomain.txt > subdomain.csv

(kali㉿kali)-[~/Downloads/BMW3]
$ cat subdomain.csv
aldan.indriver.com,subdomain
amga.indriver.com,subdomain
apple.indriver.com,subdomain
auth.indriver.com,subdomain
book.indriver.com,subdomain
cargo.indriver.com,subdomain
classified.indriver.com,subdomain
confluence.indriver.com,subdomain
cr.indriver.com,subdomain
e.indriver.com,subdomain
www.e.indriver.com,subdomain
multimedia.e.indriver.com,subdomain
freelancebr.indriver.com,subdomain
www.freelancebr.indriver.com,subdomain
freelanceec.indriver.com,subdomain
www.freelanceec.indriver.com,subdomain
freelancekz.indriver.com,subdomain
www.freelancekz.indriver.com,subdomain
freelanceme.indriver.com,subdomain
www.freelanceme.indriver.com,subdomain
freelancepu.indriver.com,subdomain
www.freelancepu.indriver.com,subdomain
freelanceru.indriver.com,subdomain
www.freelanceru.indriver.com,subdomain
freight.indriver.com,subdomain
freight.indriver.com,subdomain
groupbuy.indriver.com,subdomain
groupbuykz.indriver.com,subdomain
ic.indriver.com,subdomain
injob.indriver.com,subdomain
intercity.indriver.com,subdomain
jira.indriver.com,subdomain
job.indriver.com,subdomain
```

Bài tập 5. Dựa vào các tên miền phụ đã tìm kiếm được ở bài tập 1 và các tên miền đã bruteforce được thêm bằng burpsuite intruder. Phân loại các tên miền có kết quả trả về status code 200 và các tên miền có kết quả trả về khác

- Video thực hiện: <https://youtu.be/1s8N-57NX7U>
- B1: Dùng Burp Suite bắt gói tin Request từ indriver.com và Send to Intruder

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
293	https://indriver.com	GET	/			301	567	HTML		301 Moved Permanently	
294	https://indriver.com	GET	/			301	567	HTML		301 Moved Permanently	
295	https://indriver.com					307	381	text			
296	https://indrive.com					308	402	text			
297	https://indrive.com					200	266970	HTML		Earn With inDrive or O...	
300	https://indrive.com					ins-Semi...	200	127028	otf		
301	https://indrive.com					ins-Regu...	200	158776	ttf		
302	https://indrive.com					randir-B...	200	79300	otf		
307	https://indrive.com					pack-a94...	200	4870	script	js	
308	https://indrive.com					ework-0...	200	141005	script	js	
309	https://indrive.com					i-71e5b1...	200	144775	script	js	
310	https://indrive.com					s/_app...	200	488148	script	js	

- B2: Chọn vị trí thay thế bởi các payload trong quá trình brute-force là indriver.com và phần payload là các tên miền phụ vừa tìm được ở bài trước

1	GET / HTTP/2
2	Host: indriver.com
3	Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
4	Sec-Ch-Ua-Mobile: ?0
5	Sec-Ch-Ua-Platform: "Linux"
6	Accept-Language: en-US,en;q=0.9
7	Upgrade-Insecure-Requests: 1
8	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
9	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10	Sec-Fetch-Site: none
11	Sec-Fetch-Mode: navigate
12	Sec-Fetch-User: ?1
13	Sec-Fetch-Dest: document
14	Accept-Encoding: gzip, deflate, br
15	Priority: u=0, i

- B3: Nhấn Start Attack và xem kết quả

13. Intruder attack of https://\$indriver.com\$								
Attack Save		Attack Save ?						
Results Positions		Intruder attack results filter: Showing all items						
...								
Request	Payload	Target	Status code	Response ...	Error	Timeout	Length	Comment
6	book.indriver.com	https://book.indriver.com	505	122			372	
49	sm.indriver.com	https://sm.indriver.com	404	526			915	
4	apple.indriver.com	https://apple.indriver.com	403	272			14850	
36	lena.indriver.com	https://lena.indriver.com	403	270			14850	
42	redmine.indriver.com	https://redmine.indriver.com	403	340			14850	
47	share.indriver.com	https://share.indriver.com	403	52			4857	
1	www.indriver.com	https://www.indriver.com	302	358			532	
0		https://indriver.com	301	541			567	
7	cargo.indriver.com	https://cargo.indriver.com	301	547			574	
26	freight.indriver.com	https://freight.indriver.com	301	478			576	
31	injob.indriver.com	https://injob.indriver.com	301	360			566	
34	job.indriver.com	https://job.indriver.com	301	476			572	
39	promo.indriver.com	https://promo.indriver.com	301	464			574	
48	sharetrip.indriver.com	https://sharetrip.indriver.com	301	513			578	
51	teammate.indriver.com	https://teammate.indriver.com	301	270			347	
38	pagerduty.indriver.com	https://pagerduty.indriver.com	200	271			1991	
52	url-checker.indriver.com	https://url-checker.indriver.com	200	273			1320	
2	aldan.indriver.com	https://aldan.indriver.com	0					

- Status code:

- + 200: Yêu cầu đã thành công và server đã gửi về kết quả mong đợi
- + 301: URL đã được chuyển hướng vĩnh viễn đến một URL mới
- + 302: Tài nguyên được tìm thấy nhưng tại một URL tạm thời
- + 403: Server từ chối cung cấp tài nguyên, dù yêu cầu có hợp lệ
- + 404: Server không tìm thấy tài nguyên được yêu cầu
- + 505: Server không hỗ trợ phiên bản HTTP được sử dụng trong yêu cầu

Bài tập 6: Ghi nhận lại các địa chỉ IP của tên miền phụ tìm được của *.indriver.com. Kết quả lưu trong file csv.

Trả lời:

- Video thực hiện: <https://youtu.be/3rxUURDpgr0>
 - Sử dụng amass để quét các tên miền phụ của *.indriver.com và IP của chúng, sau đó lưu vào file ip_subdomain.csv

```
[kali㉿kali] ~]$ amass enum -d indriver.com -o IP_subdomain.csv
[+] Starting enum module against indriver.com
[+] Subdomains found: 100
[+] Writing output to IP_subdomain.csv
[+] Done

indriver.com (FQDN) → mx_record → alt2.aspmx.l.google.com (FQDN)
indriver.com (FQDN) → mx_record → alt4.aspmx.l.google.com (FQDN)
indriver.com (FQDN) → mx_record → aspmx.l.google.com (FQDN)
indriver.com (FQDN) → mx_record → alt3.aspmx.l.google.com (FQDN)
indriver.com (FQDN) → mx_record → alt1.aspmx.l.google.com (FQDN)
indriver.com (FQDN) → ns_record → ns-1696.awsdns-20.co.uk (FQDN)
indriver.com (FQDN) → ns_record → ns-294.awsdns-36.com (FQDN)
indriver.com (FQDN) → ns_record → ns-1336.awsdns-39.org (FQDN)
indriver.com (FQDN) → ns_record → ns-621.awsdns-13.net (FQDN)
indriver.com (FQDN) → node → msk.indriver.com (FQDN)
indriver.com (FQDN) → node → cargo.indriver.com (FQDN)
indriver.com (FQDN) → node → url-checker.indriver.com (FQDN)
indriver.com (FQDN) → node → sm.indriver.com (FQDN)
indriver.com (FQDN) → node → www.indriver.com (FQDN)
indriver.com (FQDN) → node → promo.indriver.com (FQDN)
indriver.com (FQDN) → node → injob.indriver.com (FQDN)
indriver.com (FQDN) → node → freight.indriver.com (FQDN)
indriver.com (FQDN) → node → job.indriver.com (FQDN)
indriver.com (FQDN) → node → ic.indriver.com (FQDN)
indriver.com (FQDN) → node → sharetrip.indriver.com (FQDN)
indriver.com (FQDN) → node → pagerduty.indriver.com (FQDN)
indriver.com (FQDN) → node → share.indriver.com (FQDN)
indriver.com (FQDN) → node → fddkim.indriver.com (FQDN)
indriver.com (FQDN) → node → s3-kz.indriver.com (FQDN)
indriver.com (FQDN) → node → apple.indriver.com (FQDN)
msk.indriver.com (FQDN) → cname_record → d2jiggylp22sfu.cloudfront.net (FQDN)
cargo.indriver.com (FQDN) → cname_record → d2jiggylp22sfu.cloudfront.net (FQDN)
url-checker.indriver.com (FQDN) → cname_record → indriver.github.io (FQDN)
sm.indriver.com (FQDN) → cname_record → d2jiggylp22sfu.cloudfront.net (FQDN)
www.indriver.com (FQDN) → cname_record → indriver.com (FQDN)
promo.indriver.com (FQDN) → cname_record → d2jiggylp22sfu.cloudfront.net (FQDN)
injob.indriver.com (FQDN) → cname_record → d2jiggylp22sfu.cloudfront.net (FQDN)
freight.indriver.com (FQDN) → cname_record → d2jiggylp22sfu.cloudfront.net (FQDN)
job.indriver.com (FQDN) → cname_record → d2jiggylp22sfu.cloudfront.net (FQDN)
ic.indriver.com (FQDN) → cname_record → intercity.indrive.com (FQDN)
sharetrip.indriver.com (FQDN) → cname_record → d2jiggylp22sfu.cloudfront.net (FQDN)
pagerduty.indriver.com (FQDN) → cname_record → indriver.github.io (FQDN)
share.indriver.com (FQDN) → cname_record → indriver.customlinks.appsflyer.com (FQDN)
fddkim.indriver.com (FQDN) → cname_record → spfmx1.domainkey.freshemail.io (FQDN)
s3-kz.indriver.com (FQDN) → a_record → 185.102.74.214 (IPAddress)
apple.indriver.com (FQDN) → a_record → 188.42.196.189 (IPAddress)
apple.indriver.com (FQDN) → a_record → 188.42.196.15 (IPAddress)
185.102.72.0/22 (Netblock) → contains → 185.102.74.214 (IPAddress)
188.42.196.0/24 (Netblock) → contains → 188.42.196.189 (IPAddress)

[+] Subdomains found: 100
[+] Writing output to subdomain_ip.txt
[+] Done
echo "Subdomain,IP-Address" > $output_file
while read -r subdomain; do
    ip=$(dig $subdomain +short | tail -n 1)
    if [[ -n $ip ]]; then
        echo "$subdomain,$ip" >> $output_file
    else
        echo "[+] $subdomain --> No IP found"
    fi
done < $input_file > $output_file
Message ChatGPT
```

- Kiểm tra lại file ip_subdomain.csv

```
(kali㉿kali)-[~]
$ cat IP_subdomain.csv
indriver.com (FQDN) → mx_record → alt2.aspmx.l.google.com (FQDN)
indriver.com (FQDN) → mx_record → alt4.aspmx.l.google.com (FQDN)
indriver.com (FQDN) → mx_record → aspmx.l.google.com (FQDN)
indriver.com (FQDN) → mx_record → alt3.aspmx.l.google.com (FQDN)
indriver.com (FQDN) → mx_record → alt1.aspmx.l.google.com (FQDN)
indriver.com (FQDN) → ns_record → ns-1696.awsdns-20.co.uk (FQDN)
indriver.com (FQDN) → ns_record → ns-294.awsdns-36.com (FQDN)
indriver.com (FQDN) → ns_record → ns-1336.awsdns-39.org (FQDN)
indriver.com (FQDN) → ns_record → ns-621.awsdns-13.net (FQDN)
indriver.com (FQDN) → node → msk.indriver.com (FQDN)
indriver.com (FQDN) → node → cargo.indriver.com (FQDN)
indriver.com (FQDN) → node → url-checker.indriver.com (FQDN)
indriver.com (FQDN) → node → sm.indriver.com (FQDN)
indriver.com (FQDN) → node → www.indriver.com (FQDN)
indriver.com (FQDN) → node → promo.indriver.com (FQDN)
indriver.com (FQDN) → node → injob.indriver.com (FQDN)
indriver.com (FQDN) → node → freight.indriver.com (FQDN)
indriver.com (FQDN) → node → job.indriver.com (FQDN)
indriver.com (FQDN) → node → ic.indriver.com (FQDN)
indriver.com (FQDN) → node → sharetrip.indriver.com (FQDN)
indriver.com (FQDN) → node → pagerduty.indriver.com (FQDN)
indriver.com (FQDN) → node → share.indriver.com (FQDN)
indriver.com (FQDN) → node → fddkim.indriver.com (FQDN)
indriver.com (FQDN) → node → s3-kz.indriver.com (FQDN)
indriver.com (FQDN) → node → apple.indriver.com (FQDN)
msk.indriver.com (FQDN) → cname_record → d2jiggylp22sfu.cloudfront.net (FQDN)
cargo.indriver.com (FQDN) → cname_record → d2jiggylp22sfu.cloudfront.net (FQDN)
url-checker.indriver.com (FQDN) → cname_record → indriver.github.io (FQDN) ↴ echo "$subdomain_no_IP found" >> $output_file
sm.indriver.com (FQDN) → cname_record → d2jiggylp22sfu.cloudfront.net (FQDN) ↴ echo "[+] $subdomain_no_IP found"
www.indriver.com (FQDN) → cname_record → indriver.com (FQDN)
promo.indriver.com (FQDN) → cname_record → d2jiggylp22sfu.cloudfront.net (FQDN)
injob.indriver.com (FQDN) → cname_record → d2jiggylp22sfu.cloudfront.net (FQDN) ↴ echo "[+] $subdomain_no_IP found"
freight.indriver.com (FQDN) → cname_record → d2jiggylp22sfu.cloudfront.net (FQDN)
job.indriver.com (FQDN) → cname_record → d2jiggylp22sfu.cloudfront.net (FQDN)
ic.indriver.com (FQDN) → cname_record → intercity.indrive.com (FQDN) ↴ echo "[+] $subdomain_no_IP found" >> $output_file
sharetrip.indriver.com (FQDN) → cname_record → d2jiggylp22sfu.cloudfront.net (FQDN)
pagerduty.indriver.com (FQDN) → cname_record → indriver.github.io (FQDN) ↴ echo "[+] $subdomain_no_IP found"
share.indriver.com (FQDN) → cname_record → indriver.customlinks.appsflyer.com (FQDN)
fddkim.indriver.com (FQDN) → cname_record → spfmx1.domainkey.freshemail.io (FQDN)
s3-kz.indriver.com (FQDN) → a_record → 185.102.74.214 (IPAddress)
apple.indriver.com (FQDN) → a_record → 188.42.196.189 (IPAddress)
apple.indriver.com (FQDN) → a_record → 188.42.196.15 (IPAddress)
185.102.72.0/22 (Netblock) → contains → 185.102.74.214 (IPAddress)
```

Bài tập 7: Brute-force các vhosts với trang web indriver.com, có tên miền nào trả về status-code 200 không?

Trả lời:

- Video thực hiện: <https://youtu.be/hl7o1p7TQ4Q>

- Bước 1: sử dụng **Gobuster** để brute-force tìm các **virtual hosts (vhosts)** của trang web [https://indriver.com](http://indriver.com), trong đó:

```
(root@thinnnlinux)-[~/home/kali/Documents/NT213/Lab_3]
# gobuster vhost -u http://indriver.com -w subdomains-top1million-110000.txt --append-domain --output gobuster_output.txt|
```

+ Giải thích từng phần lệnh

1. gobuster vhost:

- Chế độ **vhost** trong Gobuster dùng để brute-force các virtual hosts trên một domain.
- Virtual hosts là các subdomains hoặc domain được định danh bằng cách sử dụng Host header trong HTTP request.

2. -u http://indriver.com:

- Chỉ định URL của trang web cần kiểm tra. Ở đây là http://indriver.com.
- Gobuster sẽ gửi các yêu cầu HTTP đến địa chỉ này.

3. -w subdomains-top1million-110000.txt:

- Sử dụng file wordlist chứa các tên miền con (subdomains) để brute-force.
- File subdomains-top1million-110000.txt có danh sách khoảng 110.000 từ thường được sử dụng làm subdomains (VD: admin, login, api).

4. --append-domain: Tự động thêm domain chính indriver.com vào sau mỗi từ trong wordlist. Ví dụ:

- Từ wordlist: admin
- Kết quả brute-force: admin.indriver.com

5. --output gobuster_output.txt: Ghi kết quả brute-force vào file gobuster_output.txt. File này sẽ chứa các subdomains được tìm thấy cùng với mã trạng thái (status code) trả về từ server.

Lab 3: Reconnaissance

+ Sau khi brute force xong:

```
root@thinnnlinux:/home/kali ~ Command Prompt x + v
Found: super5.indriver.com Status: 403 [Size: 915]
Found: ip204-134.indriver.com Status: 403 [Size: 915]
Found: www.apollon.indriver.com Status: 403 [Size: 915]
Found: hudsons.indriver.com Status: 403 [Size: 915]
Found: rogerfederer.indriver.com Status: 403 [Size: 915]
Found: cessna.indriver.com Status: 403 [Size: 915]
Found: haider.indriver.com Status: 403 [Size: 915]
Found: gamegami.indriver.com Status: 403 [Size: 915]
Found: showyourcolours.indriver.com Status: 403 [Size: 915]
Found: remoteapps.indriver.com Status: 403 [Size: 915]
Found: teamon2.indriver.com Status: 403 [Size: 915]
Found: apro.indriver.com Status: 403 [Size: 915]
Found: jc1.indriver.com Status: 403 [Size: 915]
Found: msx002.indriver.com Status: 403 [Size: 915]
Found: acadmin.indriver.com Status: 403 [Size: 915]
Found: paulsen.indriver.com Status: 403 [Size: 915]
Found: ip204-170.indriver.com Status: 403 [Size: 915]
Found: tipweb.indriver.com Status: 403 [Size: 915]
Found: ip204-125.indriver.com Status: 403 [Size: 915]
Found: bolla.indriver.com Status: 403 [Size: 915]
Found: goodwill.indriver.com Status: 403 [Size: 915]
Found: ip204-109.indriver.com Status: 403 [Size: 915]
Found: nichop.indriver.com Status: 403 [Size: 915]
Found: sugiyamal.indriver.com Status: 403 [Size: 915]
Found: ip204-105.indriver.com Status: 403 [Size: 915]
Found: ip204-120.indriver.com Status: 403 [Size: 915]
Found: sp12.indriver.com Status: 403 [Size: 915]
Found: ip204-117.indriver.com Status: 403 [Size: 915]
Found: ns2.cc.indriver.com Status: 403 [Size: 915]
Found: access11.indriver.com Status: 403 [Size: 915]
Found: hazelnut.indriver.com Status: 403 [Size: 915]
Found: hitech1.indriver.com Status: 403 [Size: 915]
Found: ip204-149.indriver.com Status: 403 [Size: 915]
Found: ns2.cs.indriver.com Status: 403 [Size: 915]
Found: www.forumtest.indriver.com Status: 403 [Size: 915]
Found: email15.indriver.com Status: 403 [Size: 915]
Found: ingatlan.indriver.com Status: 403 [Size: 915]
Found: ttbsoc.indriver.com Status: 403 [Size: 915]
Found: koko10.indriver.com Status: 403 [Size: 915]
Found: ip204-148.indriver.com Status: 403 [Size: 915]
Progress: 114441 / 114442 (100.00%)
=====Finished=====
```

- Bước 2: Kiểm tra kết quả:

kali-linux-2024.3-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help || ⌂ ⌄ ⌅ ⌆ ⌇ ⌈ ⌉ ⌊ ⌋ ⌁ ⌃

kali-linux-2024.3-vmware-a... x

Nov 19 5:09 AM

gobuster_output.txt - Visual Studio Code

File Edit Selection View Go Run Terminal Help

gobuster_output.txt x

```
home > kali > Documents > NT213 > Lab_3 > gobuster_output.txt
  1 [32m[Found[0m: whm.indriver.com [33m[Status: 403%[0m [Size: 915]
  2 [32m[Found[0m: webmail.indriver.com [33m[Status: 403%[0m [Size: 915]
  3 [32m[Found[0m: webdisk.indriver.com [33m[Status: 403%[0m [Size: 915]
  4 [32m[Found[0m: pop.indriver.com [33m[Status: 403%[0m [Size: 915]
  5 [32m[Found[0m: smtp.indriver.com [33m[Status: 403%[0m [Size: 915]
  6 [32m[Found[0m: cpanel.indriver.com [33m[Status: 403%[0m [Size: 915]
  7 [32m[Found[0m: mail.indriver.com [33m[Status: 403%[0m [Size: 915]
  8 [32m[Found[0m: ftp.indriver.com [33m[Status: 403%[0m [Size: 915]
  9 [32m[Found[0m: ns1.indriver.com [33m[Status: 403%[0m [Size: 915]
  10 [32m[Found[0m: localhost.indriver.com [33m[Status: 403%[0m [Size: 915]
  11 [32m[Found[0m: test.indriver.com [33m[Status: 403%[0m [Size: 915]
  12 [32m[Found[0m: ns2.indriver.com [33m[Status: 403%[0m [Size: 915]
  13 [32m[Found[0m: ns.indriver.com [33m[Status: 403%[0m [Size: 915]
  14 [32m[Found[0m: autodiscover.indriver.com [33m[Status: 403%[0m [Size: 915]
  15 [32m[Found[0m: m.indriver.com [33m[Status: 403%[0m [Size: 915]
  16 [32m[Found[0m: autoconfig.indriver.com [33m[Status: 403%[0m [Size: 915]
  17 [32m[Found[0m: www2.indriver.com [33m[Status: 403%[0m [Size: 915]
  18 [32m[Found[0m: ns3.indriver.com [33m[Status: 403%[0m [Size: 915]
  19 [32m[Found[0m: dev.indriver.com [33m[Status: 403%[0m [Size: 915]
  20 [32m[Found[0m: blog.indriver.com [33m[Status: 403%[0m [Size: 915]
  21 [32m[Found[0m: forum.indriver.com [33m[Status: 403%[0m [Size: 915]
  22 [32m[Found[0m: vpn.indriver.com [33m[Status: 403%[0m [Size: 915]
  23 [32m[Found[0m: pop3.indriver.com [33m[Status: 403%[0m [Size: 915]
  24 [32m[Found[0m: mx.indriver.com [33m[Status: 403%[0m [Size: 915]
  25 [32m[Found[0m: admin.indriver.com [33m[Status: 403%[0m [Size: 915]
  26 [32m[Found[0m: new.indriver.com [33m[Status: 403%[0m [Size: 915]
  27 [32m[Found[0m: mail2.indriver.com [33m[Status: 403%[0m [Size: 915]
  28 [32m[Found[0m: old.indriver.com [33m[Status: 403%[0m [Size: 915]
  29 [32m[Found[0m: imap.indriver.com [33m[Status: 403%[0m [Size: 915]
  30 [32m[Found[0m: mobile.indriver.com [33m[Status: 403%[0m [Size: 915]
  31 [32m[Found[0m: demo.indriver.com [33m[Status: 403%[0m [Size: 915]
  32 [32m[Found[0m: shop.indriver.com [33m[Status: 403%[0m [Size: 915]
  33 [32m[Found[0m: ns4.indriver.com [33m[Status: 403%[0m [Size: 915]
```

- Bước 3: Tìm xem mã code 200 trong file output:

```

1 [32mFound[0m: whm.indriver.com [33mStatus: 403[0m [Size: 915]
2 [32mFound[0m: webmail.indriver.com [33mStatus: 403[0m [Size: 915]
3 [32mFound[0m: webdisk.indriver.com [33mStatus: 403[0m [Size: 915]
4 [32mFound[0m: pop.indriver.com [33mStatus: 403[0m [Size: 915]
5 [32mFound[0m: smtp.indriver.com [33mStatus: 403[0m [Size: 915]
6 [32mFound[0m: cpanel.indriver.com [33mStatus: 403[0m [Size: 915]

```

- Kết quả cuối cùng ta có thể thấy là không có tên miền nào trả về status-code 200, có thể do:

+ **Vhost không tồn tại:** Các subdomains hoặc virtual hosts trong wordlist có thể không tồn tại thực sự trên máy chủ indriver.com. Trong trường hợp này, server sẽ trả về mã lỗi 404 (Not Found) hoặc 403 (Forbidden) nếu server tồn tại nhưng không cho phép truy cập.

+ **Trang web yêu cầu xác thực:** Nếu một trang web yêu cầu xác thực người dùng (như đăng nhập), Gobuster có thể nhận được mã lỗi 403 (Forbidden) vì không có thông tin xác thực trong yêu cầu.

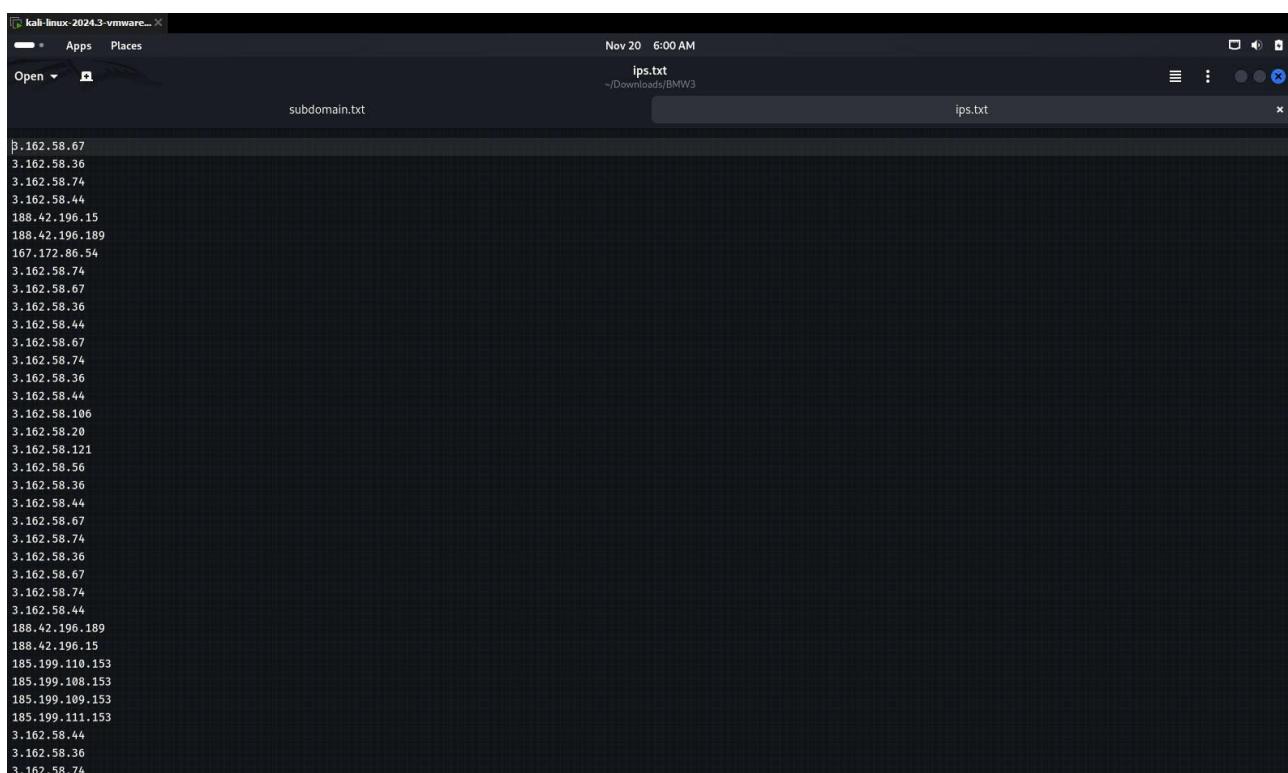
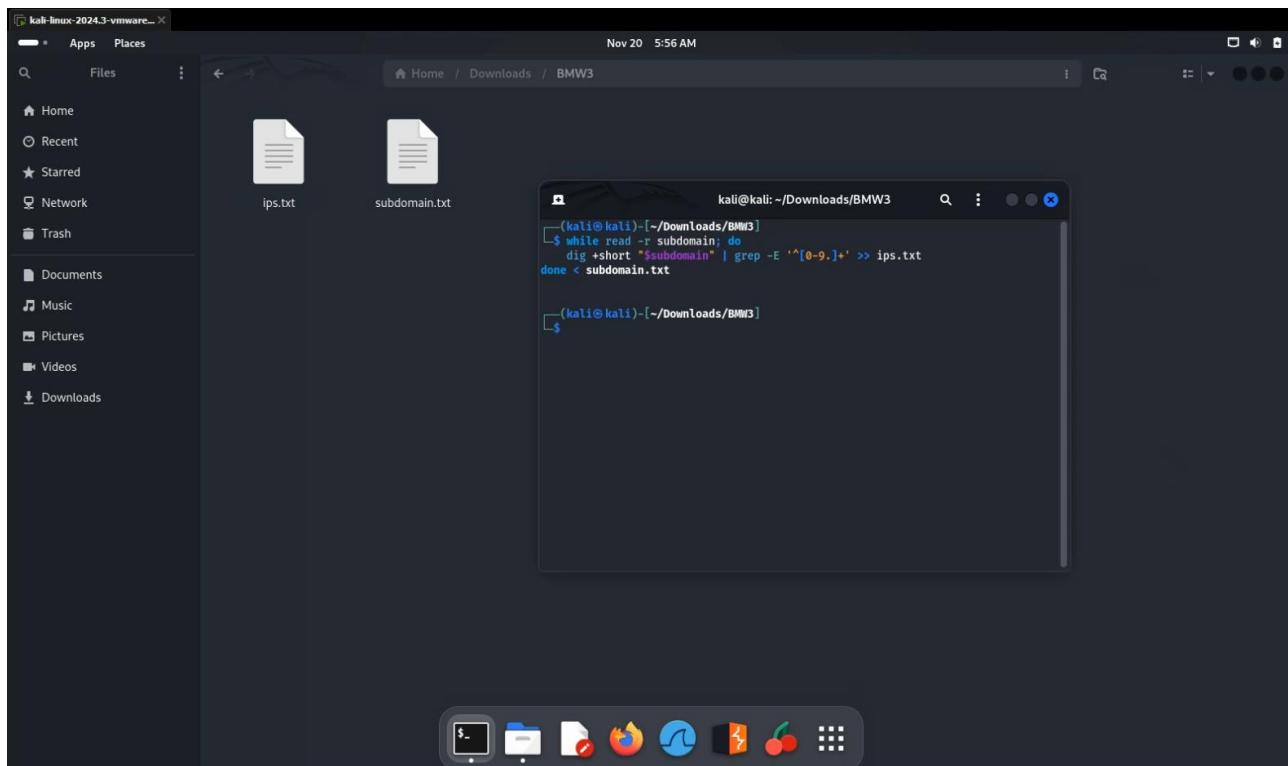
+ **Cấu hình server chặn brute-force:** Server có thể sử dụng các biện pháp bảo mật (như rate limiting, firewall, hoặc các phương pháp bảo vệ khác) để chặn các yêu cầu từ các công cụ như Gobuster, khiến tất cả các yêu cầu trả về mã 403 hoặc các mã trạng thái khác.

+ **Tên miền bị ẩn hoặc không cấu hình:** Một số subdomains có thể đã được cấu hình nhưng bị ẩn hoặc không được phép truy cập công khai (có thể đã bị tắt hoặc bị chặn trong cấu hình của máy chủ).

Bài tập 8: Brute-force các vhosts với trang web indrider.com, có tên miền nào trả về status-code 200 không?

Trả lời:

- Video thực hiện: <https://youtu.be/R6b0RqCLl1I>
- Ta sẽ sử dụng lại danh sách subdomain submain.txt đã lấy được ở các task trước
- Sử dụng lệnh dig để lấy địa chỉ IP từ các subdomain trong danh sách vào file ips.txt



Lab 3: Reconnaissance

Nhóm 6

- Thực hiện lấy danh sách 1000 port phổ biến về file top_ports.csv

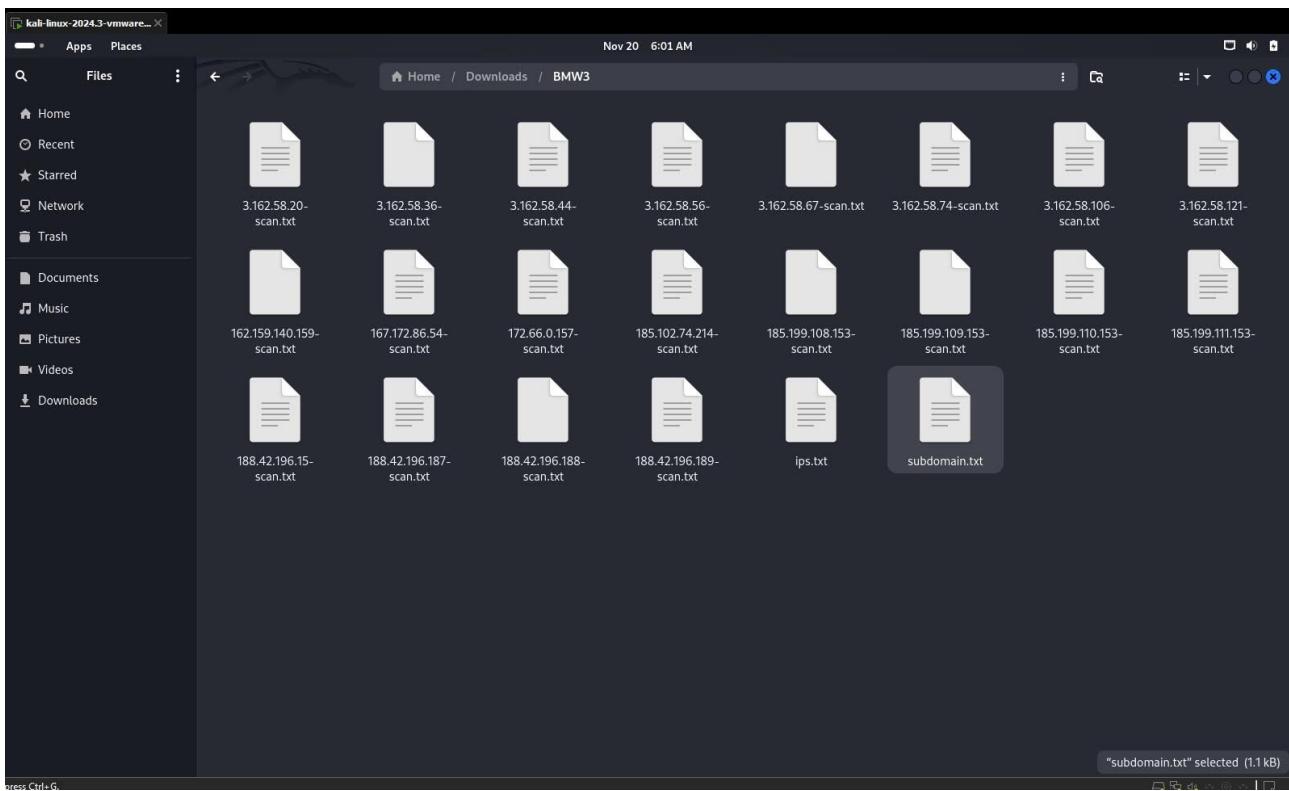
```
Nov 20 6:01 AM
top_ports.csv
ips.txt
top_ports.csv

$0,23,443,21,22,25,3389,110,445,139,143,53,135,3386,8080,1723,111,995,993,5900,1025,587,8888,199,1720,465,548,113,81,6001,10000,514,5060,179,1026,2000,8443,8000,32768,554,26,1433,49152,2001,5
15,8008,49154,1027,5666,646,5000,5631,631,49153,8881,2049,88,79,5800,106,2121,1110,49155,6000,513,990,5357,427,49156,543,544,5101,144,7,389,8089,3128,444,9999,5009,7079,190,3000,543,2000,39
86,13,1029,9,5051,6646,49157,1027,1828,873,1757,2717,4899,9100,119,37,1000,3001,5001,89,10010,1038,9098,2107,1024,2103,6004,1801,5050,19,8031,1041,255,1049,1048,2967,1053,3703,1056,1065,1064,1054,
17,808,3689,1031,1044,104,100,9102,8010,2869,1039,5120,4001,2000,2185,636,1038,2601,1,7008,1005,1059,625,311,280,254,4000,1999,563,1717,2008,992,32770,32772,7001,8802,2007,740,5550,2009,5801,1043,512,2701,7019,
2,1080,2401,4045,902,7937,787,1058,2383,32771,1033,1040,1059,50000,5555,1001,1494,593,2301,3,1,3268,7938,1234,1022,1074,8002,1036,1035,9001,1037,464,497,1935,6666,2003,0543,1352,24,3269,1111
,407,500,20,2006,3268,15000,1218,1034,4444,264,2004,33,1042,42510,999,3052,1023,1068,222,7108,888,4827,1999,563,1717,2008,992,32770,32772,7001,8802,2007,740,5550,2009,5801,1043,512,2701,7019,
50001,1700,4662,2065,2010,42,9535,2602,3333,161,5100,5002,2604,4002,6059,1047,8192,8193,2702,6789,9595,1851,9594,9593,16993,16992,5226,5225,32769,3283,1852,8194,1055,1062,9415,8701,8652,8651,
8889,65389,55000,64680,64623,55600,55555,52869,35000,3354,23502,28828,1311,1060,4443,730,731,709,1067,13782,5902,566,9050,1002,85,5000,5431,1864,1863,8085,51103,49999,45180,10243,49,3495,666
7,90,475,27000,1503,6881,1508,8021,340,78,5566,8088,2222,9071,8899,6005,9876,1501,5102,32774,32773,7001,8801,8803,5004,3476,8884,5214,14238,12348,912,30,2605
,2030,6,541,8007,3005,4,1248,2500,880,306,4242,1097,9009,2525,1086,1088,8291,52822,6101,908,7200,2809,393,800,32775,12000,1083,211,987,705,20005,711,13783,6969,3071,5269,5222,1085,1046,5087,5
989,5988,2190,11967,8600,3766,7627,8087,30000,9010,7741,14000,3367,1899,1098,3031,2718,5680,15002,4129,6901,3827,3580,2144,9900,8181,3801,1718,2811,9080,2135,1045,2399,3017,10002,1148,9002,88
73,2875,9811,5718,8086,3998,2667,1110,6126,5911,5910,9618,2381,1096,3300,3351,1073,8333,3784,5633,15660,6123,3211,1078,3659,3551,2268,2160,2100,16001,3325,3323,1104,9968,9583,9502,9485,9290,
9220,8994,8649,8222,7911,7912,7205,7106,65129,633331,6156,6129,60020,5962,5961,5960,5959,5925,5877,5825,5810,58080,57294,50800,50000,50003,49100,49159,49158,48080,40193,34573,34572,34571,3404,33899
,3301,32782,32781,31038,30718,28201,27715,25734,24800,22930,21571,20221,20301,19842,19881,19101,17988,1783,16018,16016,15003,14442,13456,10629,10628,10626,10621,10617,10616,10566,10025,10024,
10012,1169,5030,5414,1057,6788,1947,1094,1075,1108,4003,1081,1093,4449,1687,1840,1100,1063,1061,1107,1106,9500,20222,7778,1077,1310,2119,2492,1070,20000,8400,1272,6389,7777,1072,1079,1082,840
2,89,691,1001,32775,1999,212,2020,6003,7002,2998,50002,3372,898,5510,32,2033,4165,3061,5903,99,749,425,43,5405,6106,13722,6502,7007,458,9666,8100,3737,5298,1152,8090,2191,3011,1580,5200,3851,
337,3309,3369,7402,5954,3918,3077,7443,3493,3828,1186,2179,1183,19315,19281,3995,5963,1124,8500,1089,10004,2251,1087,5280,3871,3038,62078,9981,4111,1334,1261,2522,5859,1247,9944,9943,9877,91
10,8654,8254,8180,8011,7512,7435,7103,61900,61532,5922,5915,5904,5822,56738,55055,51493,50636,50389,49175,49165,49163,3546,32784,27355,27353,24444,19780,18988,16012,15742,10778,4006,212
6,4446,3880,1782,1296,9998,9848,32779,1021,32777,2021,32778,616,666,708,5802,4221,545,1524,1112,49400,84,38292,2040,32780,3006,2111,1084,1600,2048,2638,6699,9111,16088,6547,6007,1533,5560,210
6,1443,667,720,2034,555,801,0025,3221,3826,9200,2608,4279,7025,11111,3527,1151,8200,8300,6689,9878,10009,8800,5730,2394,2393,275,5061,6566,3080,1201,3168,3814,1862,1114,8
510,3905,3383,3914,3971,3809,5033,7676,3517,4908,3869,9418,2909,3878,8042,1091,1090,3926,6567,1138,3945,1175,10003,3398,3889,1131,8292,5087,1119,1117,4848,7800,16000,3324,2222,4445,9917,
9575,9099,9803,8290,8099,8093,8045,7921,7920,7496,6839,6792,6779,6692,6565,60443,5952,5950,5967,5862,5850,5815,5811,57797,56737,5544,55050,5440,54328,54045,52848,52673,50500,50300,40176,
49167,49161,44501,44176,41511,40911,32785,32783,30951,27356,26214,25735,19350,18101,18040,17877,16113,15804,14441,12265,12174,10215,10180,4567,6100,4004,4005,8022,8888,7999,1271,1199,3003,112
2,2323,2224,2022,617,777,417,714,6346,981,722,1809,4998,70,1076,5999,10082,765,301,524,668,2041,6009,1417,1434,259,44443,1984,2068,7004,1007,4343,416,2038,6006,189,4125,1461,9103,911,726,1018
,2046,2035,7201,687,2013,481,129,6669,6668,903,1455,683,1011,2043,2047,31337,256,9929,5998,406,4442,783,843,2842,2045,4040,6066,6051,1145,3916,9443,9444,1875,7272,4252,4280,7024,1556,13724,1
141,1233,3765,1137,3063,5938,9191,3808,8866,3981,2710,3852,3849,3944,3853,9988,1163,4164,3820,6481,3731,5081,40000,8097,4555,3863,1287,4430,7744,1812,7913,1166,1164,1165,8019,10160,4658,7878,
3304,3307,1259,1092
```

- Sử dụng nmap để scan 1000 port phổ biến trên các IP tìm được

```
Nov 20 5:57 AM
top_ports.csv
ips.txt
top_ports.csv

$0,23,443,21,22,25,3389,110,445,139,143,53,135,3386,8080,1723,111,995,993,5900,1025,587,8888,199,1720,465,548,113,81,6001,10000,514,5060,179,1026,2000,8443,8000,32768,554,26,1433,49152,2001,5
15,8008,49154,1027,5666,646,5000,5631,631,49153,8881,2049,88,79,5800,106,2121,1110,49155,6000,513,990,5357,427,49156,543,544,5101,144,7,389,8089,3128,444,9999,5009,7079,190,3000,543,2000,39
86,13,1029,9,5051,6646,49157,1027,1828,873,1757,2717,4899,9100,119,37,1000,3001,5001,89,10010,1038,9098,2107,1024,2103,6004,1801,5050,19,8031,1041,255,1049,1048,2967,1053,3703,1056,1065,1064,1054,
17,808,3689,1031,1044,104,100,9102,8010,2869,1039,5120,4001,2000,2185,636,1038,2601,1,7008,1005,1059,625,311,280,254,4000,1999,563,1717,2008,992,32770,32772,7001,8802,2007,740,5550,2009,5801,1043,512,2701,7019,
2,1080,2401,4045,902,7937,787,1058,2383,32771,1033,1040,1059,50000,5555,1001,1494,593,2301,3,1,3268,7938,1234,1022,1074,8002,1036,1035,9001,1037,464,497,1935,6666,2003,0543,1352,24,3269,1111
,407,500,20,2006,3268,15000,1218,1034,4444,264,2004,33,1042,42510,999,3052,1023,1068,222,7108,888,4827,1999,563,1717,2008,992,32770,32772,7001,8802,2007,740,5550,2009,5801,1043,512,2701,7019,
50001,1700,4662,2065,2010,42,9535,2602,3333,161,5100,5002,2604,4002,6059,1047,8192,8193,2702,6789,9595,1851,9594,9593,16993,16992,5226,5225,32769,3283,1852,8194,1055,1062,9415,8701,8652,8651,
8889,65389,55000,64680,64623,55600,55555,52869,35000,3354,23502,28828,1311,1060,4443,730,731,709,1067,13782,5902,566,9050,1002,85,5000,5431,1864,1863,8085,51103,49999,45180,10243,49,3495,666
7,90,475,27000,1503,6881,1508,8021,340,78,5566,8088,2222,9071,8899,6005,9876,1501,5102,32774,32773,7001,8801,8803,5004,3476,8884,5214,14238,12348,912,30,2605
,2030,6,541,8007,3005,4,1248,2500,880,306,4242,1097,9009,2525,1086,1088,8291,52822,6101,908,7200,2809,393,800,32775,12000,1083,211,987,705,20005,711,13783,6969,3071,5269,5222,1085,1046,5087,5
989,5988,2190,11967,8600,3766,7627,8087,30000,9010,7741,14000,3367,1899,1098,3031,2718,5680,15002,4129,6901,3827,3580,2144,9900,8181,3801,1718,2811,9080,2135,1045,2399,3017,10002,1148,9002,88
73,2875,9811,5718,8086,3998,2667,1110,6126,5911,5910,9618,2381,1096,3300,3351,1073,8333,3784,5633,15660,6123,3211,1078,3659,3551,2268,2160,2100,16001,3325,3323,1104,9968,9583,9502,9485,9290,
9220,8994,8649,8222,7911,7912,7205,7106,65129,633331,6156,6129,60020,5962,5961,5960,5959,5925,5877,5825,5810,58080,57294,50800,50000,50003,49100,49159,49158,48080,40193,34573,34572,34571,3404,33899
,3301,32782,32781,31038,30718,28201,27715,25734,24800,22930,21571,20221,20301,19842,19881,19101,17988,1783,16018,16016,15003,14442,13456,10629,10628,10626,10621,10617,10616,10566,10025,10024,
10012,1169,5030,5414,1057,6788,1947,1094,1075,1108,4003,1081,1093,4449,1687,1840,1100,1063,1061,1107,1106,9500,20222,7778,1077,1310,2119,2492,1070,20000,8400,1272,6389,7777,1072,1079,1082,840
2,89,691,1001,32775,1999,212,2020,6003,7002,2998,50002,3372,898,5510,32,2033,4165,3061,5903,99,749,425,43,5405,6106,13722,6502,7007,458,9666,8100,3737,5298,1152,8090,2191,3011,1580,5200,3851
,337,3309,3369,7402,5954,3918,3077,7443,3493,3828,1186,2179,1183,19315,19281,3995,5963,1124,8500,1089,10004,2251,1087,5280,3871,3038,62078,9981,4111,1334,1261,2522,5859,1247,9944,9943,9877,91
10,8654,8254,8180,8011,7512,7435,7103,61900,61532,5922,5915,5904,5822,56738,55055,51493,50636,50389,49175,49165,49163,3546,32784,27355,27353,24444,19780,18988,16012,15742,10778,4006,212
6,4446,3880,1782,1296,9998,9848,32779,1021,32777,2021,32778,616,666,708,5802,4221,545,1524,1112,49400,84,38292,2040,32780,3006,2111,1084,1600,2048,2638,6699,9111,16088,6547,6007,1533,5560,210
6,1443,667,720,2034,555,801,0025,3221,3826,9200,2608,4279,7025,11111,3527,1151,8200,8300,6689,9878,10009,8800,5730,2394,2393,275,5061,6566,3080,1201,3168,3814,1862,1114,8
510,3905,3383,3914,3971,3809,5033,7676,3517,4908,3869,9418,2909,3878,8042,1091,1090,3926,6567,1138,3945,1175,10003,3398,3889,1131,8292,5087,1119,1117,4848,7800,16000,3324,2222,4445,9917,
9575,9099,9803,8290,8099,8093,8045,7921,7920,7496,6839,6792,6779,6692,6565,60443,5952,5950,5967,5862,5850,5815,5811,57797,56737,5544,55050,5440,54328,54045,52848,52673,50500,50300,40176,
49167,49161,44501,44176,41511,40911,32785,32783,30951,27356,26214,25735,19350,18101,18040,17877,16113,15804,14441,12265,12174,10215,10180,4567,6100,4004,4005,8022,8888,7999,1271,1199,3003,112
2,2323,2224,2022,617,777,417,714,6346,981,722,1809,4998,70,1076,5999,10082,765,301,524,668,2041,6009,1417,1434,259,44443,1984,2068,7004,1007,4343,416,2038,6006,189,4125,1461,9103,911,726,1018
,2046,2035,7201,687,2013,481,129,6669,6668,903,1455,683,1011,2043,2047,31337,256,9929,5998,406,4442,783,843,2842,2045,4040,6066,6051,1145,3916,9443,9444,1875,7272,4252,4280,7024,1556,13724,1
141,1233,3765,1137,3063,5938,9191,3808,8866,3981,2710,3852,3849,3944,3853,9988,1163,4164,3820,6481,3731,5081,40000,8097,4555,3863,1287,4430,7744,1812,7913,1166,1164,1165,8019,10160,4658,7878,
3304,3307,1259,1092
```



- Sau đó dùng 1 file python với tác dụng tổng hợp kết quả từ các file .txt của nmap thành csv

```

import csv
import os
import glob

# Ghi kết quả vào file CSV
with open('scan_results.csv', 'w', newline='') as csvfile:
    fieldnames = ['IP', 'Port', 'State', 'Service']
    writer = csv.DictWriter(csvfile, fieldnames=fieldnames)
    writer.writeheader()

    for file in glob.glob("*-scan.txt"):
        ip = os.path.basename(file).replace("-scan.txt", "")
        with open(file, 'r') as f:
            for line in f:
                if '/tcp' in line:
                    parts = line.split('/')
                    writer.writerow({
                        'IP': ip,
                        'Port': parts[0].split('/')[0],
                        'State': parts[1],
                        'Service': parts[2] if len(parts) > 2 else "Unknown"
                    })

```

- Ta được file kết quả như sau:

A screenshot of a terminal window titled "kali-linux-2024.3-vmware...". The window shows two tabs: "ips.txt" and "scan_results.csv". The "ips.txt" tab contains a list of IP addresses and ports, each followed by a status (open or filtered) and a service (HTTP). The "scan_results.csv" tab shows the same data in CSV format. The terminal interface includes a menu bar with "Apps" and "Places", a date and time indicator (Nov 20 5:57 AM), and a bottom status bar.

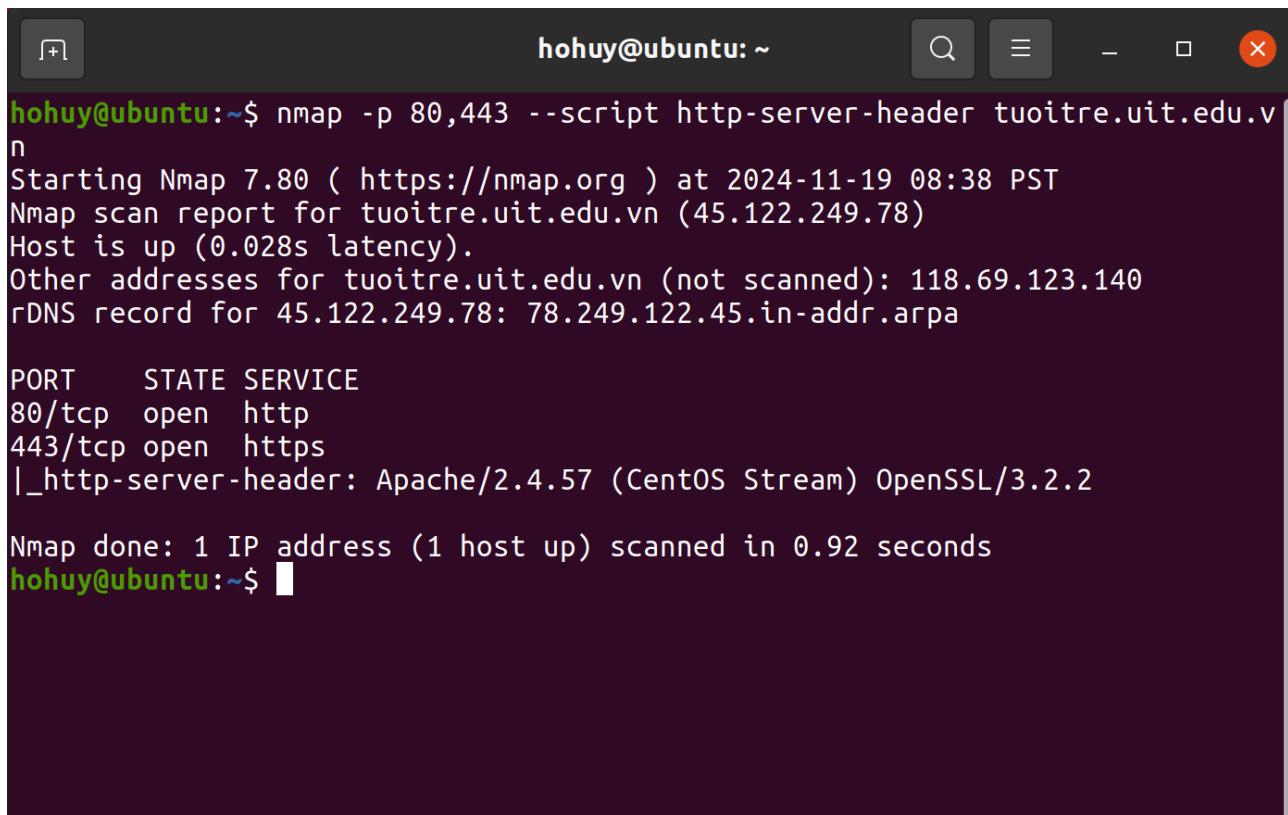
IP	Port	State	Service
188.42.196.15	80	filtered	http
185.102.74.214	80	filtered	http
3.162.58.56	80	open	http
3.162.58.36	80	open	http
172.66.0.157	80	open	http
3.162.58.106	80	open	http
185.199.108.153	80	open	http
188.42.196.188	80	filtered	http
3.162.58.74	80	open	http
188.42.196.187	80	filtered	http
167.172.86.54	80	open	http
3.162.58.67	80	open	http
188.42.196.189	80	filtered	http
3.162.58.44	80	open	http
185.199.111.153	80	open	http
3.162.58.121	80	open	http
162.159.140.159	80	open	http
185.199.110.153	80	open	http
3.162.58.20	80	open	http
185.199.109.153	80	open	http

Bài tập 9. Xác định phiên bản Apache được sử dụng của web tuoitre.uit.edu.vn.

- Video thực hiện: <https://youtu.be/Sv9SQxOT8ug>

- Sử dụng nmap để thực hiện quét, lệnh này sẽ quét các cổng 80 và 443 (HTTP và HTTPS) và kiểm tra các thông tin phiên bản từ tiêu đề HTTP Server.

```
nmap -p 80,443 --script http-server-header tuoitre.uit.edu.vn
```



```
hohuy@ubuntu:~$ nmap -p 80,443 --script http-server-header tuoitre.uit.edu.vn
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-19 08:38 PST
Nmap scan report for tuoitre.uit.edu.vn (45.122.249.78)
Host is up (0.028s latency).
Other addresses for tuoitre.uit.edu.vn (not scanned): 118.69.123.140
rDNS record for 45.122.249.78: 78.249.122.45.in-addr.arpa

PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
|_http-server-header: Apache/2.4.57 (CentOS Stream) OpenSSL/3.2.2

Nmap done: 1 IP address (1 host up) scanned in 0.92 seconds
hohuy@ubuntu:~$
```

- Kết quả: Apache/2.4.57

Bài tập 10: CMS nào được sử dụng của trang web tuoitre.uit.edu.vn.

Trả lời:

- Video thực hiện: <https://youtu.be/vEOiJD637yo>
- Sử dụng công cụ whatweb để quét trang tuoitre.uit.edu.vn

```
(kali㉿kali)-[~]
$ whatweb tuoitre.uit.edu.vn
http://tuoitre.uit.edu.vn [302 Found] IP[45.122.249.78], RedirectLocation[https://tuoitre.uit.edu.vn/]
https://tuoitre.uit.edu.vn/ [200 OK] Apache[2.4.57], Content-Language[vi], Drupal, Email[vpdoan@uit.edu.vn], HTML5, HTTPServer[CentOS][Apache/2.4.57 (CentOS Stream) OpenSSL/3.2.2], IP[45.122.249.78], MetaGenerator[Drupal 7 (https://www.drupal.org)], OpenSSL[3.2.2], PHP[8.1.29], Script[text/javascript], Title[Tuổi trẻ UIT], UncommonHeaders[x-content-type-options,x-generator,link], X-Frame-Options[SAMEORIGIN], X-Powered-By[PHP/8.1.29]
```

- Ta biết được rằng trang này sử dụng CMS Drupal 7 qua trường thông tin MetaGenerator

Bài tập 11: Hệ điều hành và webserver nào được sử dụng của trang web tuoitre.uit.edu.vn.

Trả lời:

- Video thực hiện: <https://youtu.be/ncjIVS1peDE>
- Ta sử dụng WhatWeb - 1 công cụ giúp xác định các công nghệ đang được sử dụng trên một trang web.

```
(kali㉿thinlinux)-[~]
$ whatweb tuoitre.uit.edu.vn
http://tuoitre.uit.edu.vn [302 Found] Country[VIET NAM][VN], IP[118.69.123.140], RedirectLocation[https://tuoitre.uit.edu.vn/]
https://tuoitre.uit.edu.vn/ [200 OK] Apache[2.4.57], Content-Language[vi], Drupal, Email[vpdoan@uit.edu.vn], HTML5, HTTPServer[CentOS][Apache/2.4.57 (CentOS Stream) OpenSSL/3.2.2], IP[45.122.249.78], MetaGenerator[Drupal 7 (https://www.drupal.org)], OpenSSL[3.2.2], PHP[8.1.29], Script[text/javascript], Title[Tuổi trẻ UIT], UncommonHeaders[x-content-type-options,x-generator,link], X-Frame-Options[SAMEORIGIN], X-Powered-By[PHP/8.1.29]
```

- Dựa trên kết quả từ công cụ WhatWeb, trang web **tuoitre.uit.edu.vn** sử dụng các công nghệ sau:

- + Webserver: Apache 2.4.57 (CentOS Stream)
- + Hệ điều hành: CentOS Stream
- + CMS: Drupal 7
- + Phiên bản PHP: 8.1.29
- + OpenSSL: 3.2.2
- + Header HTTP: X-Frame-Options: SAMEORIGIN, X-Powered-By: PHP/8.1.29

- Trang web sử dụng:

- + Hệ điều hành: **CentOS Stream**
- + Webserver: **Apache/2.4.57 (CentOS Stream)**

Bài tập 12: Sử dụng <https://web.archive.org/> tìm kiếm và ghi nhận lại dữ liệu quá khứ các tên miền phụ không còn tồn tại hiện nay của terra-1.indriverapp.com. File <https://terra-1.indriverapp.com/robots.txt> có chứa nội dung gì?

Trả lời:

- Video thực hiện: <https://youtu.be/AEP3oXgUhIo>
- Sử dụng <https://web.archive.org/> tìm kiếm và ghi nhận lại dữ liệu quá khứ các tên miền phụ không còn tồn tại hiện nay của terra-1.indriverapp.com

URL	MIME Type	From	To	Captures	Duplicates	Unique
https://terra-1.indriverapp.com/	text/html	May 17, 2022	Mar 20, 2024	3	0	3
https://terra-1.indriverapp.com/api/authorization	application/octet-stream	Apr 5, 2023	Apr 5, 2023	1	0	1
https://terra-1.indriverapp.com/api/authorization?locale=ru	application/octet-stream	Apr 3, 2023	Apr 3, 2023	1	0	1
https://terra-1.indriverapp.com/content/46550038e1802eb1952edc6dea015d6ff38a40-15f50fb6818ab27307.js	application/javascript	May 17, 2022	May 17, 2022	1	0	1
https://terra-1.indriverapp.com/content/77139f25b60580223d87180cd53082072b7543e-caeac4a7203bda9b7efc.js	application/javascript	Apr 3, 2023	Apr 3, 2023	1	0	1
https://terra-1.indriverapp.com/content/881d182534a9b28a01994030384f5f537c5e641-9cf95b54d679511b832.js	application/javascript	May 17, 2022	May 17, 2022	1	0	1
https://terra-1.indriverapp.com/content/app-362b2d7b31ad7e48116a.js	application/javascript	Apr 3, 2023	Apr 3, 2023	1	0	1
https://terra-1.indriverapp.com/content/app-4968a8b03c15e5543411e.js	application/javascript	May 17, 2022	May 17, 2022	1	0	1
https://terra-1.indriverapp.com/content/component--arc-pages-index-tsx-2b4a263c6d5d3d1910ad.js	application/javascript	Apr 3, 2023	Apr 3, 2023	1	0	1
https://terra-1.indriverapp.com/content/component--arc-pages-index-tsx-4c83949204b25b1779e7.js	application/javascript	May 17, 2022	May 17, 2022	1	0	1

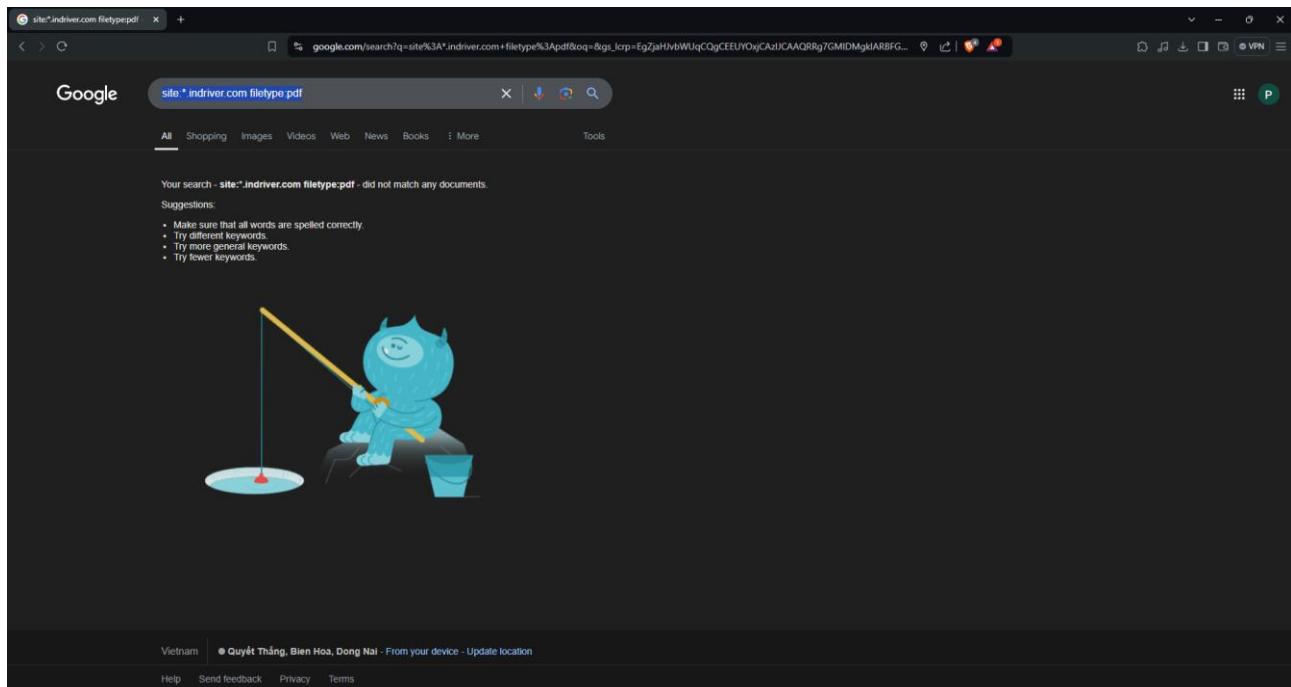
- Ta tìm thấy file <https://terra-1.indriverapp.com/robots.txt>

<https://terra-1.indriverapp.com/robots.txt>

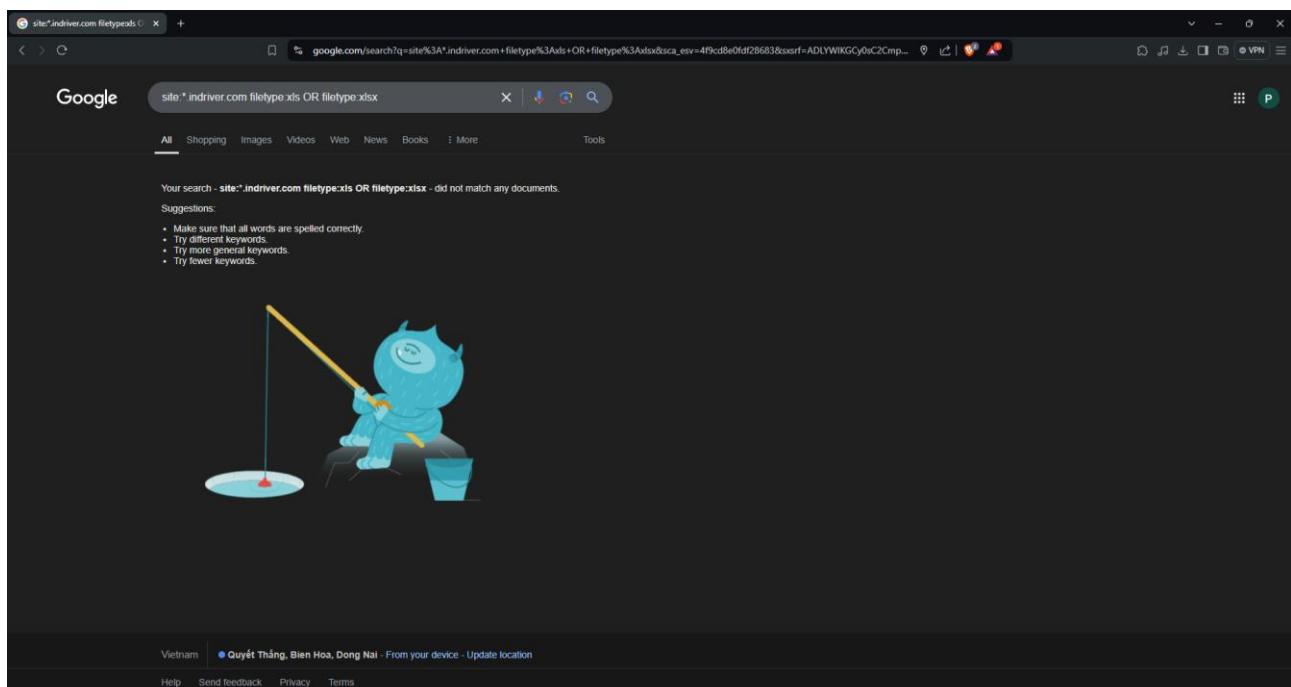
- Theo kết quả tìm kiếm trên Internet, file robots.txt là tệp văn bản trong thư mục gốc của trang web, dùng để hướng dẫn bot công cụ tìm kiếm (web crawler) về các khu vực được phép hoặc không được phép thu thập dữ liệu. Nó chứa các chỉ thị như User agent (bot áp dụng), Disallow (chặn truy cập), và Sitemap (đường dẫn sơ đồ trang web). Tuy nhiên, robots.txt không bảo mật và chỉ là một hướng dẫn cho bot.

Bài tập 13: Tìm kiếm các tập tin pdf, excel, word, trên *.indriver.com.**Trả lời:**

- Video thực hiện: <https://youtu.be/7QuJ3VYoqiU>
- Lần lượt thực hiện các tìm kiếm trên google như sau:
 - + Tìm kiếm các tập tin pdf: site:*.indriver.com filetype:pdf



- + Tìm kiếm các tập tin excel: site:*.indriver.com filetype:xls OR filetype:xlsx



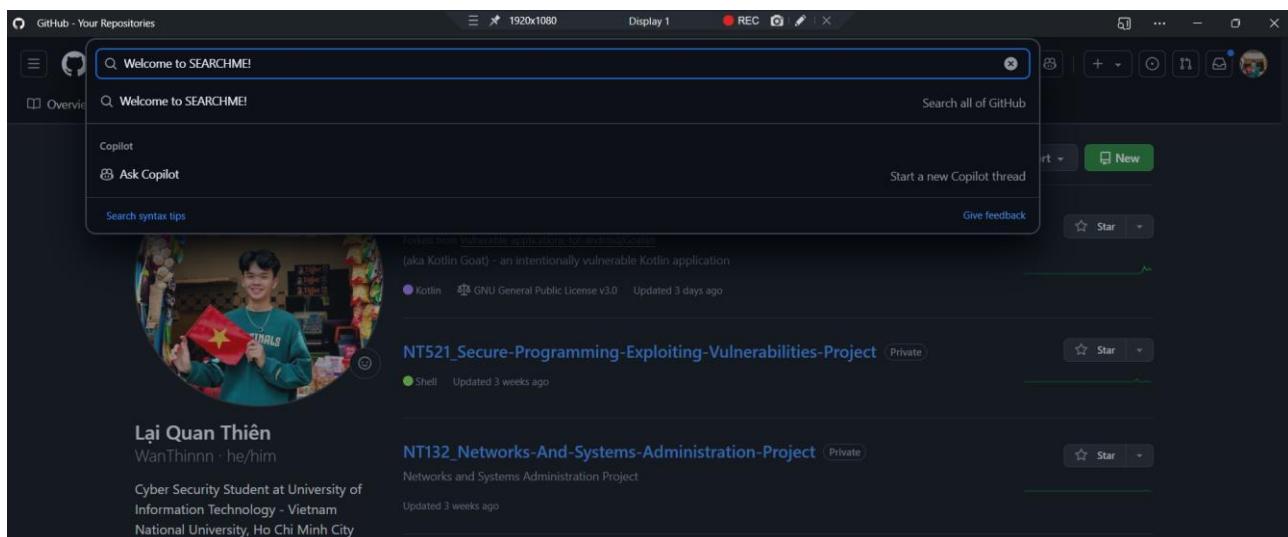
- + Tìm kiếm các tập tin Word: site:*.indriver.com filetype:doc OR filetype:docx

Bài tập 14: Chúng tôi có 1 trang web đang trong quá trình phát triển, hãy tìm thử API key cho phép user tạo tài khoản trên website này.

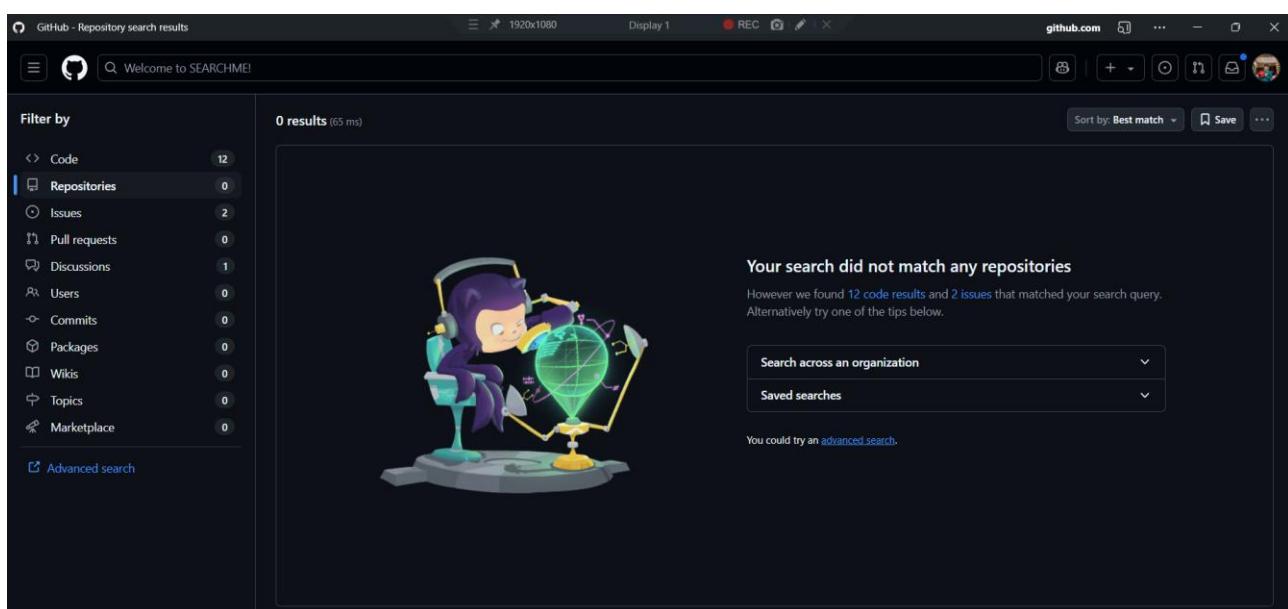
Trả lời:

- Video thực hiện: <https://youtu.be/jS2w4ziKww0>

- Trước tiên, ta cần tìm kiếm trong github với cụm từ được gợi ý trên trang bài tập: “Welcome to SEARCHME!”



- Có thể thấy ta tìm được [12 code results](#) và [2 issues](#) trên github:



- Ta truy cập vào mục “Code” và tìm được đoạn code khá tương đồng với giao diện được gợi ý trong bài lab.

The screenshot shows the GitHub Code search interface. The left sidebar has a red box around the 'Filter by' section, with 'Code' selected. The main area displays search results for 'Code' across 12 files. A red box highlights the first result, which is the 'index.php' file from the 'supersecurerdeveloper/searchmecms' repository. The code snippet shows:

```

25 </nav>
26
27 <div class="container mt-4">
28   <h1 class="text-center">Welcome to SearchME!</h1>
29   <p class="text-center">This website is under development.</p>
30 </div>
31
32
33
34
35
36
37
38
39

```

Below this, there are two more results: 'alexjercan/learning-cybersecurity' with its README.md file and 'aarikpokras/aarikpokras.github.io' with its searchme-devs-glitch/script.js file.

- Truy cập vào Repo -> API

The screenshot shows the GitHub repository page for 'supersecurerdeveloper/searchmecms'. The 'Code' tab is selected. A red box highlights the 'api' folder in the file list. The right sidebar provides repository details:

- In progress...**
- Activity**: 0 stars, 9 watching, 1 fork
- Report repository**
- Releases**: No releases published
- Packages**: No packages published
- Languages**: PHP 61.4%, Hack 38.6%

- Vậy là ta đã tìm thấy API key cho phép user tạo tài khoản:

```

1 <?php
2 require_once 'config.php';
3 header('Content-Type: application/json');
4
5 $headers = apache_request_headers();
6
7 if (isset($headers['X-THM-API-Key']) && $headers['X-THM-API-Key'] === 'TBA') {
8     $input = json_decode(file_get_contents('php://input'), true);
9
10    $stmt = $mysqli->prepare("INSERT INTO users (username, password, email, name) VALUES (?, ?, ?, ?)");
11    $stmt->bind_param("ssss", $input['username'], password_hash($input['password'], PASSWORD_DEFAULT), $input['email'], $input['name']);
12
13    if ($stmt->execute()) {
14        echo json_encode(['message' => 'Registration successful.']);
15    } else {
16        echo json_encode(['error' => 'Registration failed: ' . $stmt->error]);
17    }
18    $stmt->close();
19 } else {
20     echo json_encode(array('error' => 'Invalid or Expired API key'));
21 }
22
23 ?>

```

- Nhận định: Trong đoạn mã PHP trên, **API key** được sử dụng để bảo vệ và xác thực các yêu cầu đăng ký tài khoản từ người dùng. Cụ thể, khi một yêu cầu được gửi tới máy chủ, API key sẽ được kiểm tra trong phần **header** của yêu cầu. Cụ thể:

+ **Kiểm tra API key:** Đoạn mã sẽ kiểm tra xem yêu cầu có chứa header X-THM-API-Key hay không và nếu có, nó sẽ so sánh giá trị của API key với giá trị 'TBA'. Nếu API key khớp, yêu cầu sẽ được tiếp tục xử lý; nếu không, hệ thống sẽ trả về thông báo lỗi.

+ **Xử lý dữ liệu đăng ký:** Nếu API key hợp lệ, mã sẽ đọc dữ liệu JSON từ thân yêu cầu (sử dụng php://input) và thực hiện thao tác thêm người dùng vào cơ sở dữ liệu. Cụ thể, nó sẽ chuẩn bị một câu lệnh SQL để thêm thông tin người dùng mới vào bảng users, bao gồm tên đăng nhập, mật khẩu (được mã hóa), email và tên.

+ **Thông báo kết quả:** Sau khi thực hiện thao tác thêm người dùng vào cơ sở dữ liệu, hệ thống trả về thông báo thành công hoặc lỗi dưới dạng JSON, giúp hệ thống phía client xử lý tiếp.

+ **Nếu API key không hợp lệ:** Nếu API key không hợp lệ hoặc không có trong header, mã sẽ trả về thông báo lỗi rằng API key không hợp lệ hoặc đã hết hạn.

- Tóm tắt API key trong đoạn mã này:

+ **Mục đích:** Xác thực và bảo mật yêu cầu trước khi cho phép thực hiện các thao tác tạo tài khoản.

+ **Kiểm tra:** API key phải được gửi trong header của yêu cầu dưới tên X-THM-API-Key, và giá trị phải khớp với 'TBA' để yêu cầu tiếp tục.

+ **Nếu không hợp lệ:** Trả về thông báo lỗi "Invalid or Expired API key".

=> Đoạn mã này cho phép tạo tài khoản người dùng qua một API được bảo vệ bằng API key, giúp ngăn chặn các truy cập không hợp lệ từ những người dùng không có quyền.

Bài tập 15: Viết code crawling trang web <https://indriver.com> để lấy các thông tin liên quan như list email, các đường dẫn liên kết (links), danh sách js, images, comment. Gợi ý: có thể dùng thư viện scrapy của python.

- Video thực hiện: <https://youtu.be/U4caBbkQzFk>

- Tạo dự án scrapy bằng lệnh:

```
scrapy startproject indriver_crawler
```

- Thêm file code crawling vào indriver_crawler/spiders ta được dự án như hình:

The screenshot shows the Microsoft Visual Studio Code interface with the following details:

- File Explorer (Left):** Shows the project structure under "BAI14". The "pipelines.py" file is currently selected.
- Code Editor (Right):** Displays the content of "task14.py". The code defines an `IndriverSpider` class that implements the `parse` method to extract links, scripts, images, emails, and comments from the page content.
- Status Bar (Bottom):** Shows the current file is "task14.py", the line number is 27, column 28, and the file is saved in Python 3.12.7 64-bit (Microsoft Store).

```
File Edit Selection View Go ... 🔍 bai14 🌐 🔍 task14.py ● pipelines.py  
EXPLORER BAI14  
inriver_crawler  
└ inriver_crawler  
    ├── _pycache_  
    │   └ _pycache_  
    ├── spiders  
    │   ├── _pycache_  
    │   └ __init__.py  
    └ task14.py  
        ├── __init__.py  
        ├── items.py  
        ├── middlewares.py  
        ├── pipelines.py  
        ├── settings.py  
        └ scrapy.cfg  
pipelines.py  
task14.py  
inriver_crawler > inriver_crawler > spiders > task14.py > IndriverSpider > parse  
2 import re  
3 from urllib.parse import urljoin  
4  
5 class IndriverSpider(scrapy.Spider):  
6     name = 'inriver'  
7     allowed_domains = ['inriver.com']  
8     start_urls = ['https://inriver.com']  
9  
10    def parse(self, response):  
11  
12        links = response.css('a::attr(href)').getall()  
13        links = [urljoin(response.url, link) for link in links if link]  
14        yield {'links': links}  
15  
16        scripts = response.css('script::attr(src)').getall()  
17        scripts = [urljoin(response.url, script) for script in scripts if script]  
18        yield {'js_files': scripts}  
19  
20        images = response.css('img::attr(src)').getall()  
21        images = [urljoin(response.url, img) for img in images if img]  
22        yield {'images': images}  
23  
24        emails = re.findall(r'[a-zA-Z0-9._%+-]+@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,}', response.text)  
25        yield {'emails': emails}  
26  
27        comments = response.xpath('//comment()').getall()  
28        yield {'comments': comments}  
29  
30        # Theo các đường dẫn khác để tiếp tục thu thập  
31        for link in links:  
32            yield scrapy.Request(link, callback=self.parse)
```

- Chay Spider scrapy crawl indriver -o output.json:

```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS COMMENTS

PS D:\test\bail14\indriver_crawler\indriver_crawler\spiders>
● PS D:\test\bail14\indriver_crawler\indriver_crawler\spiders scrapy crawl indriver -o output.json
2024-11-20 00:29:07 [scrapy.utils.log] INFO: Scrapy 2.12.0 started (bot: indriver_crawler)
2024-11-20 00:29:07 [scrapy.utils.log] INFO: Versions: lxml 5.3.0.0, libxml2 2.11.7, cssselect 1.2.0, parse 1.9.1, w3lib 2.2.1, Twisted 24.10.0, Python 3.12.7 (tags/v3.12.7, Oct 1 2024, 03:06:41) [MSC V141 64 bit (AMD64)], pyOpenSSL 24.2.1 (OpenSSL 3.3.2 3 Sep 2024), cryptography 43.0.3, Platform Windows-11-0.0.22631-P0
2024-11-20 00:29:07 [scrapy.addons] INFO: Enabled addons:
[]
2024-11-20 00:29:07 [asyncio] DEBUG: Using selector: SelectSelector
2024-11-20 00:29:07 [scrapy.utils.log] DEBUG: Using reactor: twisted.internet.asyncioreactor.AsyncioSelectorReactor
2024-11-20 00:29:07 [scrapy.utils.log] DEBUG: Using asyncio event loop: asyncio.windows_events._WindowsSelectorEventLoop
2024-11-20 00:29:07 [scrapy.utils.log] DEBUG: Using reactor: twisted.internet.asyncioreactor.AsyncioSelectorReactor
2024-11-20 00:29:07 [scrapy.utils.log] DEBUG: Using asyncio event loop: asyncio.windows_events._WindowsSelectorEventLoop
2024-11-20 00:29:07 [scrapy.extensions.telnet] INFO: Telnet Password: 602fb51e7d70b05a
2024-11-20 00:29:07 [scrapy.middleware] INFO: Enabled extensions:
['scrapy.extensions.corestats.CoreStats',
 'scrapy.extensions.telnet.TelnetConsole',
 'scrapy.extensions.feedexport.FeedExporter',
 'scrapy.extensions.logstats.LogStats']
2024-11-20 00:29:07 [scrapy.crawler] INFO: Overridden settings:
{'BOT_NAME': 'indriver_crawler',
 'FEED_EXPORT_ENCODING': 'utf-8',
 'NEWSPIIDER_MODULE': 'indriver_crawler.spiders',
 'ROBOTSTXT_OBEY': True,
 'SPIDER_MODULES': ['indriver_crawler.spiders'],
 'TWISTED_REACTOR': 'twisted.internet.asyncioreactor.AsyncioSelectorReactor'}
2024-11-20 00:29:08 [scrapy.middleware] INFO: Enabled downloader middlewares:
['scrapy.downloadermiddlewares.offsite.OffsiteMiddleware',
 'scrapy.downloadermiddlewares.robotstxt.RobotsTxtMiddleware',
 'scrapy.downloadermiddlewares.httpauth.HttpAuthMiddleware',
 'scrapy.downloadermiddlewares.downloadtimeout.DownloadTimeoutMiddleware',
 'scrapy.downloadermiddlewares.defaultheaders.DefaultHeadersMiddleware',
 'scrapy.downloadermiddlewares.useragent.UserAgentMiddleware',
 'scrapy.downloadermiddlewares.retry.RetryMiddleware']
```

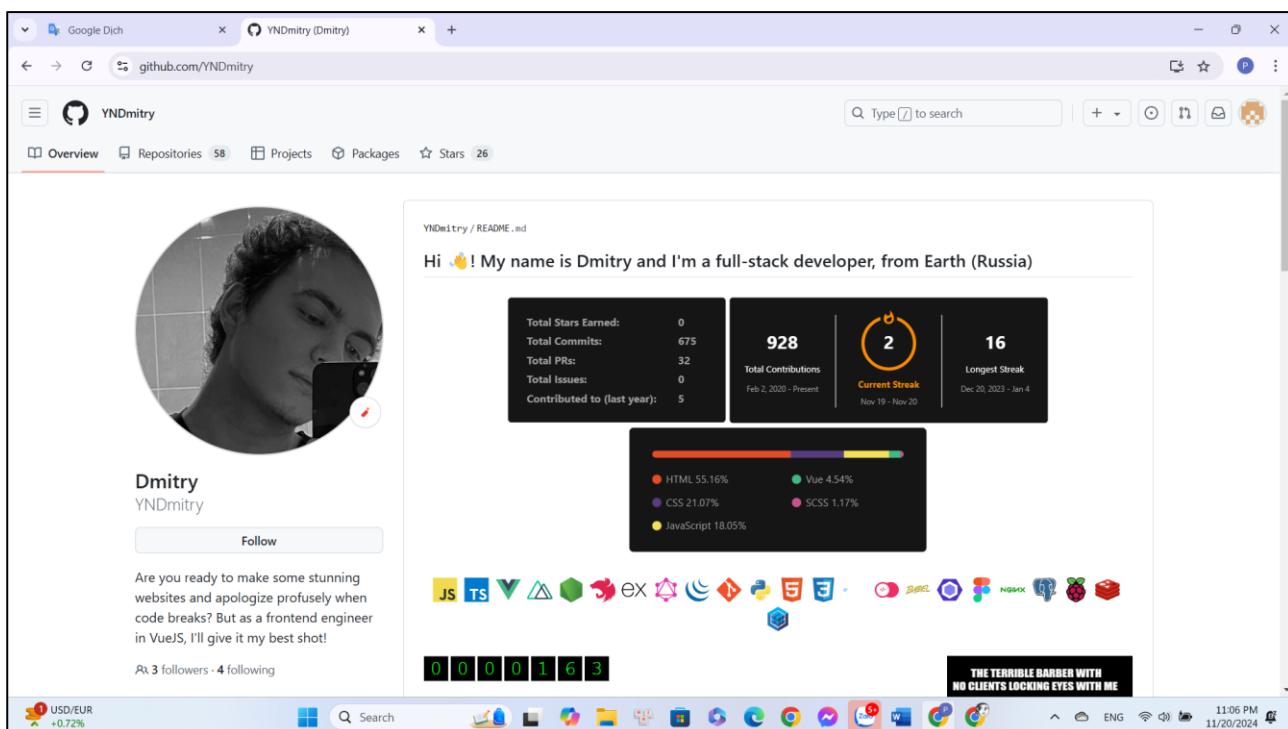
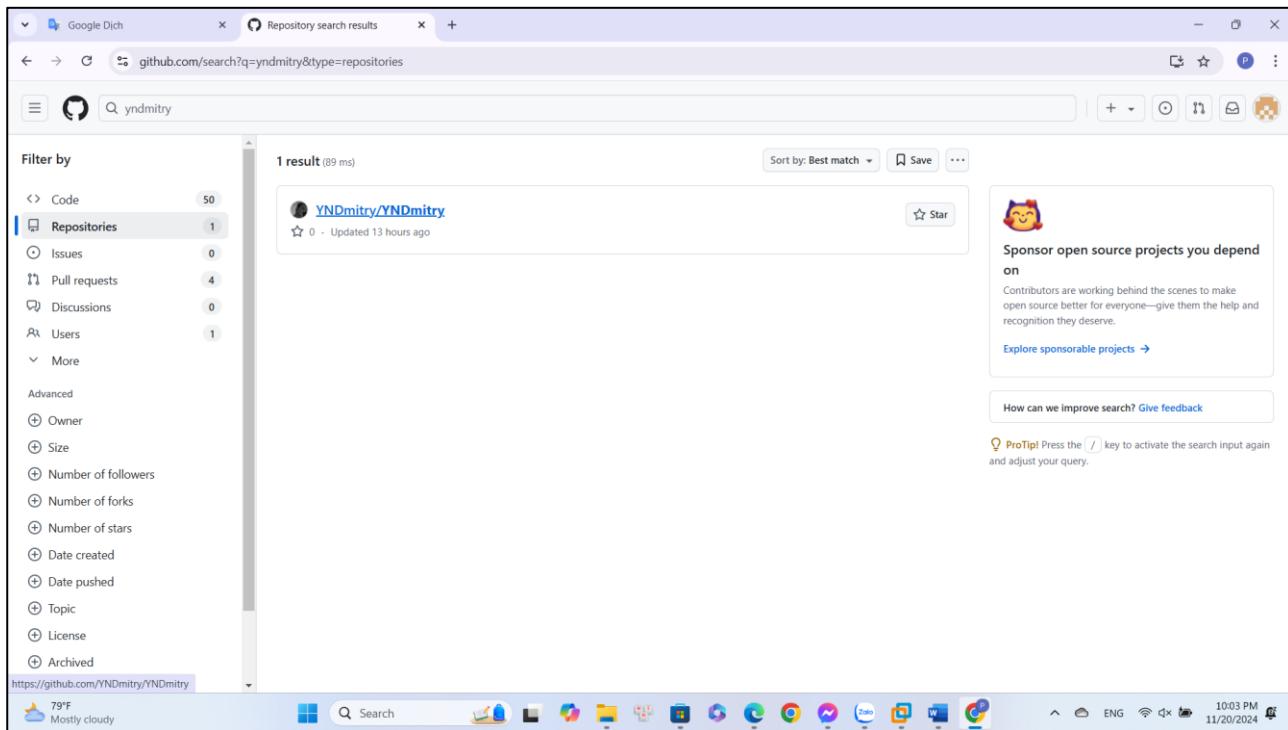
- output.json:

```
indriver_crawler > indriver_crawler > spiders > ① output.json > ...  
1  [  
2   {"links": ["https://indrive.com/en-vn", "https://indrive.com/en-vn/fair-services", "https://indrive.com/en-vn/city-rides", "https://indrive.com/en-vn/intercity-rides", "https://indrive.com/en-vn/ride-history"], "js_files": ["https://indrive.com/_next/static/chunks/polyfills-42372ed130431b0a.js", "https://indrive.com/_next/static/chunks/webpack-4ae7d6faa12f89f1.js", "https://indrive.com/_next/static/chunks/main-4ae7d6faa12f89f1.js"], "images": ["https://indrive.com/images/logo/logo--white.svg", "https://indrive.com/images/logo/logo--dark.svg", "https://indstatic.io/indstatic-main/flags/VN.svg"], "emails": ["support@indrive.com", "support@indriver.com", "support@indrive.com", "u003esupport@indrive.com", "gr@indrive.com", "u003egr@indrive.com"], "comments": ["<!-- -->", "<!-- -->", "<!-- -->", "<!-- -->"]}  
7 ]
```

Bài tập luyện tập: Which sites did YNDmitry develop on inDrive.com?

Trả lời:

- Video thực hiện: <https://youtu.be/15eylePVNLg>
 - Ta tìm kiếm thông tin về YNDmitry trên git



- Ta thấy được Repository inDrive như sau

The screenshot shows a list of GitHub repositories owned by the user YNDmitry. The repositories are:

- webflow-publish** (Public) - Updated on Aug 26
- onwater-dev** (Public) - Updated on Jun 29
- inDrive** (Public) - Updated on Jun 26
- directus** (Public) - Forked from directus/directus. Description: The Modern Data Stack. Updated on Mar 9
- tambas-case-studies** (Public) - Updated on Mar 6

- Ta thấy sites mà YNDmitry đã phát triển trên inDrive.com ở đây

The screenshot shows the GitHub repository page for **inDrive**. The repository details are:

- Code: master, 1 Branch, 0 Tags
- Activity: 88 Commits, 0f9242b - 5 months ago
- Watchers: 1, Forks: 0, Stars: 0
- About: No description, website, or topics provided.
- Releases: No releases published.
- Packages: No packages published.
- Languages: JavaScript 96.0%, HTML 3.2%, TypeScript 0.8%

Bài tập luyện tập: TryHackMe

Trả lời:

- Video thực hiện: <https://youtu.be/DXHwy1pj1PE>
- Task 1: Không cần câu trả lời
- Task 2: Dựa vào các thông tin trong Whois ta trả lời được các câu hỏi trong lab

Domain name:	RepublicOfKoffee.com
Registry Domain ID:	2582024072_DOMAIN_COM-VRSN
Registrar WHOIS Server:	whois.namecheap.com
Registrar URL:	http://www.namecheap.com
Updated Date:	2024-01-11T02:08:15.56Z
Creation Date:	2021-01-01T17:33:07.00Z
Registrar Registration Expiration Date:	2025-01-01T17:33:07.00Z
Registrar:	NAMECHEAP INC
Registrar IANA ID:	1068
Registrar Abuse Contact Email:	abuse@namecheap.com
Registrar Abuse Contact Phone:	+1 9854014545
Reseller:	NAMECHEAP INC
Domain Status:	clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:	
Registrant Name:	Redacted for Privacy
Registrant Organization:	Privacy service provided by Withheld for Privacy ehf
Registrant Street:	Kalkofnsvegur 2
Registrant City:	Reykjavik
Registrant State/Province:	Capital Region
Registrant Postal Code:	101
Registrant Country:	IS
Registrant Phone:	+354.4212434
Registrant Phone Ext:	
Registrant Fax:	
Registrant Fax Ext:	
Registrant Email:	744b407022364a2f8212bb43b0f7edf8.protect@withheldforprivacy.com
Registry Admin ID:	
Admin Name:	Redacted for Privacy
Admin Organization:	Privacy service provided by Withheld for Privacy ehf
Admin Street:	Kalkofnsvegur 2
Admin City:	Reykjavik
Admin State/Province:	Capital Region
Admin Postal Code:	101
Admin Country:	IS
Admin Phone:	+354.4212434
Admin Phone Ext:	
Admin Fax:	
Admin Fax Ext:	
Admin Email:	744b407022364a2f8212bb43b0f7edf8.protect@withheldforprivacy.com

Lab 3: Reconnaissance

Nhóm 6

Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
 Registry Registrant ID:
 Registrant Name: Redacted for Privacy
 Registrant Organization: Privacy service provided by Withheld for Privacy ehf
 Registrant Street: Kalkofnseggur 2
 Registrant City: Reykjavik
 Registrant State/Province: Capital Region
 Registrant Postal Code: 101
 Registrant Country: IS
 Registrant Phone: +354.4212434
 Registrant Phone Ext:
 Registrant Fax:
 Registrant Fax Ext:
 Registrant Email: 744b407022364a2f8212bb43b0f7edf8.protect@withheldforprivacy.com
 Registry Admin ID:
 Admin Name: Redacted for Privacy
 Admin Organization: Privacy service provided by Withheld for Privacy ehf
 Admin Street: Kalkofnseggur 2
 Admin City: Reykjavik
 Admin State/Province: Capital Region
 Admin Postal Code: 101
 Admin Country: IS
 Admin Phone: +354.4212434
 Admin Phone Ext:
 Admin Fax:
 Admin Fax Ext:
 Admin Email: 744b407022364a2f8212bb43b0f7edf8.protect@withheldforprivacy.com
 Registry Tech ID:
 Tech Name: Redacted for Privacy
 Tech Organization: Privacy service provided by Withheld for Privacy ehf
 Tech Street: Kalkofnseggur 2
 Tech City: Reykjavik
 Tech State/Province: Capital Region
 Tech Postal Code: 101
 Tech Country: IS
 Tech Phone: +354.4212434
 Tech Phone Ext:
 Tech Fax:
 Tech Fax Ext:
 Tech Email: 744b407022364a2f8212bb43b0f7edf8.protect@withheldforprivacy.com
 Name Server: ns1.brainydns.com
 Name Server: ns2.brainydns.com
 DNSSEC: unsigned
 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.icann.org/

+ Kết quả:

A 'whois' lookup is the most basic form of domain recon available. There are multiple websites that will do it for you as well.

Personally, I recommend just going directly to [Namecheap WHOIS Tool](#). This should tell you the current hosting company used and name servers. Looking at the raw data option will show further details.

We're looking for any data we might be able to use as pivot points. Maybe an email address? Or better yet, a physical address or phone number?

Technically these are required in order to register any domain, but most domain registrars offer some kind of privacy protection for a trivial fee, if not free.

Anyway, let's see what we can find out!

Answer the questions below

What is the name of the company the domain was registered with?
 ✓ Correct Answer

What phone number is listed for the registration company? (do not include country code or special characters/spaces)
 ✓ Correct Answer 💡 Hint

What is the first nameserver listed for the site?
 ✓ Correct Answer

What is listed for the name of the registrant?
 ✓ Correct Answer

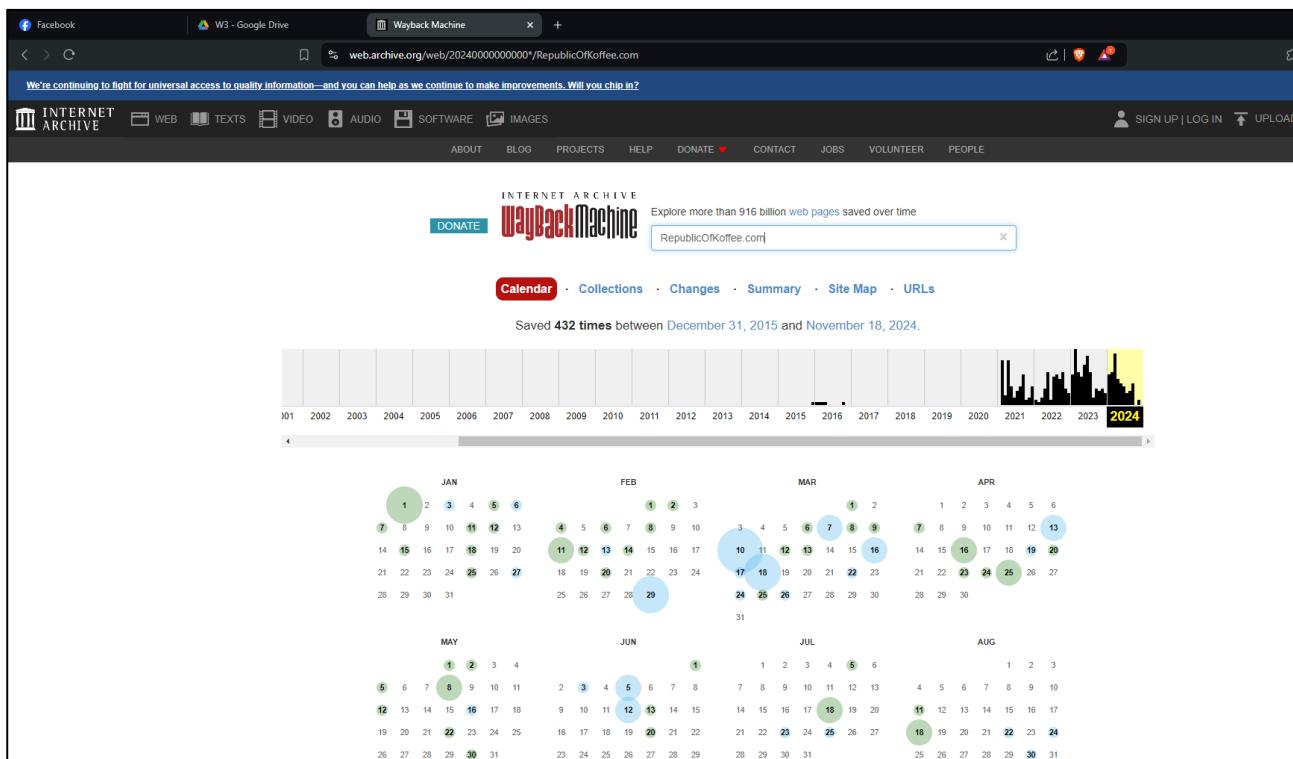
What country is listed for the registrant?
 ✓ Correct Answer

Task 3 ✓ Ghosts of Websites Past

Lab 3: Reconnaissance

Nhóm 6

- Task 3: Sử dụng trang web Archive.org và truy cập vào 1 blog bất kì ta sẽ thấy tên tác giả là Steve, địa chỉ của tác giả ở Gwangju là 1 thành phố của Hàn Quốc (South Korea). Ngoài ra ta có thể tìm thấy thông tin của ngôi chùa thông qua tìm kiếm google



The screenshot shows a Wayback Machine archive of a blog post. The post is titled "CAFFE BONITO; MUDEUNGSAN". It was posted on June 24, 2015, by user "Steve". The content describes the Caffe Bonito in Mudeungsan, noting its spacious interior, parking issues, and scenic views. The sidebar includes sections for RECENT POSTS, RECENT COMMENTS, ARCHIVES, and CATEGORIES.

Lab 3: Reconnaissance

Nhóm 6

Mudeungsan Jeungsimsa Temple

23 reviews • #9 of 64 things to do in Gwangju • Religious Sites

[Write a review](#)

About

Duration: <1 hour

Suggest edits to improve what we show. [Improve this listing](#)

Task 2 ✓ Whois Registration

Task 3 ✓ Ghosts of Websites Past

Don't be discouraged when your initial searches on a website turn up empty.
That's where Archive.org and the Internet Wayback Machine come into play.
Do yourself a favor and install the archive.org browser extension that will automatically pull up an option to search for a site on the Wayback Machine when it fails to load in the web browser.
Either with the browser extension, or just by going to archive.org and searching for it, see what snapshots are available of our target domain, RepublicOfKoffee.com.
Looking at the historical information available for the site, you should be able to answer the following questions without too much trouble.

Answer the questions below

What is the first name of the blog's author?
 ✓ Correct Answer ✓ Hint

What city and country was the author writing from?
 ✓ Correct Answer ✓ Hint

[Research] What is the name (in English) of the temple inside the National Park the author frequently visits?
 ✓ Correct Answer ✓ Hint

Task 4 ✓ Digging into DNS

Task 5 ✓ Taking Off The Training Wheels

- Task 4: Thực hiện truy cập vào trang web <https://viewdns.info/>

+ Dựa vào tiện ích IP History của trang web, ta sẽ check được lịch sử IP sử dụng của domain mà ta muốn tìm kiếm (cụ thể ở đây là RepublicOfKoffee.com)

Lab 3: Reconnaissance

Nhóm 6

IP Address	Location	Domain	Date
185.107.56.52	Roozendael - The Netherlands	NForce Entertainment B.V.	2022-02-26
185.107.56.194	The Netherlands	NForce Entertainment B.V.	2022-02-26
162.210.199.65	Manassas - United States	LEASEWEB-USA-WDC	2022-02-26
96.47.230.69	Miami - United States	ASN-QUADRANET-GLOBAL	2022-02-25
74.63.241.23	Dallas - United States	LINESTONENETWORKS	2022-02-25
192.157.56.139	Buffalo - United States	SERVER-MANIA	2022-02-25
185.107.56.53	Roozendael - The Netherlands	NForce Entertainment B.V.	2022-02-25
185.107.56.193	The Netherlands	NForce Entertainment B.V.	2022-02-25
162.210.199.87	Manassas - United States	LEASEWEB-USA-WDC	2022-02-25
162.210.199.87	Manassas - United States	LEASEWEB-USA-WDC	2022-02-25
162.210.199.87	Manassas - United States	LEASEWEB-USA-WDC	2022-02-25
37.45.65.145	Amsterdam - The Netherlands	LeaseWeb Netherlands B.V.	2022-02-24
192.157.56.139	Buffalo - United States	SERVER-MANIA	2022-02-24
185.107.56.55	Roozendael - The Netherlands	NForce Entertainment B.V.	2022-02-24
185.107.56.193	The Netherlands	NForce Entertainment B.V.	2022-02-24
162.210.199.87	Manassas - United States	LEASEWEB-USA-WDC	2022-02-24
74.63.241.24	Dallas - United States	LINESTONENETWORKS	2022-02-23
185.107.56.53	Roozendael - The Netherlands	NForce Entertainment B.V.	2022-02-23
96.47.230.67	Miami - United States	ASN-QUADRANET-GLOBAL	2022-02-22
92.192.82.228	The Netherlands	LeaseWeb Netherlands B.V.	2022-02-22
74.63.241.27	Dallas - United States	LINESTONENETWORKS	2022-02-22
74.63.241.27	Dallas - United States	LINESTONENETWORKS	2022-02-22
192.157.56.149	Buffalo - United States	SERVER-MANIA	2022-02-22
185.107.56.54	Roozendael - The Netherlands	NForce Entertainment B.V.	2022-02-22
162.210.199.65	Manassas - United States	LEASEWEB-USA-WDC	2022-02-22
162.210.199.65	Manassas - United States	LEASEWEB-USA-WDC	2022-02-22
99.93.154.118	United States	AMAZON-02	2022-02-09
192.64.119.238	United States	NNAMECHEAP-NET	2022-01-01
69.64.147.10	United States	RIGHTSIDE	2017-07-30
173.248.188.152	United States	WEHOSTWEBSITES.COM	2014-10-03
173.248.187.2	United States	WEHOSTWEBSITES-COM	2016-02-01

+ Dựa trên các tên miền khác được lưu trữ trên cùng một địa chỉ IP ta có thể nhận ra đây là Shared web hosting – một dịch vụ lưu trữ web cho phép nhiều website cùng chia sẻ tài nguyên của một máy chủ vật lý duy nhất

So far we've gathered some good info about the content that was on our target website, even though it hasn't been live for several years.

But what about technical details?

That's where ViewDNS.info comes in.

ViewDNS.info provides a convenient UI for looking up registration information on a target website. Using this information, it may be possible to draw certain conclusions that are not clearly spelled out, such as whether the website is hosted on a shared or dedicated IP address. The answer to this question can imply things about the website's budget as well as traffic.

Take a look at the search options available and see if you can answer these questions.

Answer the questions below

What was RepublicOfKoffee.com's IP address as of October 2016?

173.248.188.152

Based on the other domains hosted on the same IP address, what kind of hosting service can we safely assume our target uses?

shared

- Task 5: Tương tự như ở Task 2, ta sẽ tiếp tục sử dụng các trang web ở các task trước để khai thác nhưng bây giờ mục tiêu của ta sẽ là domain heat.net

+ What is the second nameserver listed for the domain?

Lab 3: Reconnaissance

Nhóm 6

Whois results: heat.net is already registered. Want it? Make an offer now.

heat.net REGISTERED IN 1997

Domain Name: heat.net
 Registry Domain ID: 4878759_DOMAIN_NET-VRSN
 Registrar WHOIS Server: whois.godaddy.com
 Registrar URL: http://www.godaddy.com
 Updated Date: 2024-01-30T14:02:40Z
 Creation Date: 1997-02-03T05:00:00Z
 Registry Expiry Date: 2025-02-04T05:00:00Z
 Registrar: GoDaddy.com, LLC
 Registrar IANA ID: 146
 Registrar Abuse Contact Email: abuse@godaddy.com
 Registrar Abuse Contact Phone: 480-624-2505
 Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
 Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
 Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
 Name Server: NS1.heat.net
 Name Server: NS2.heat.net
 DNSSEC: unsigned
 URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
 >>> Last update of whois database: 2024-11-20T11:11:45Z <<

For more information on Whois status codes, please visit <https://icann.org/epp>

NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring

- + What IP address was the domain listed on as of December 2011?
- + Based on domains that share the same IP, what kind of hosting service is the domain owner using?

Viewdns.info > Tools > IP History

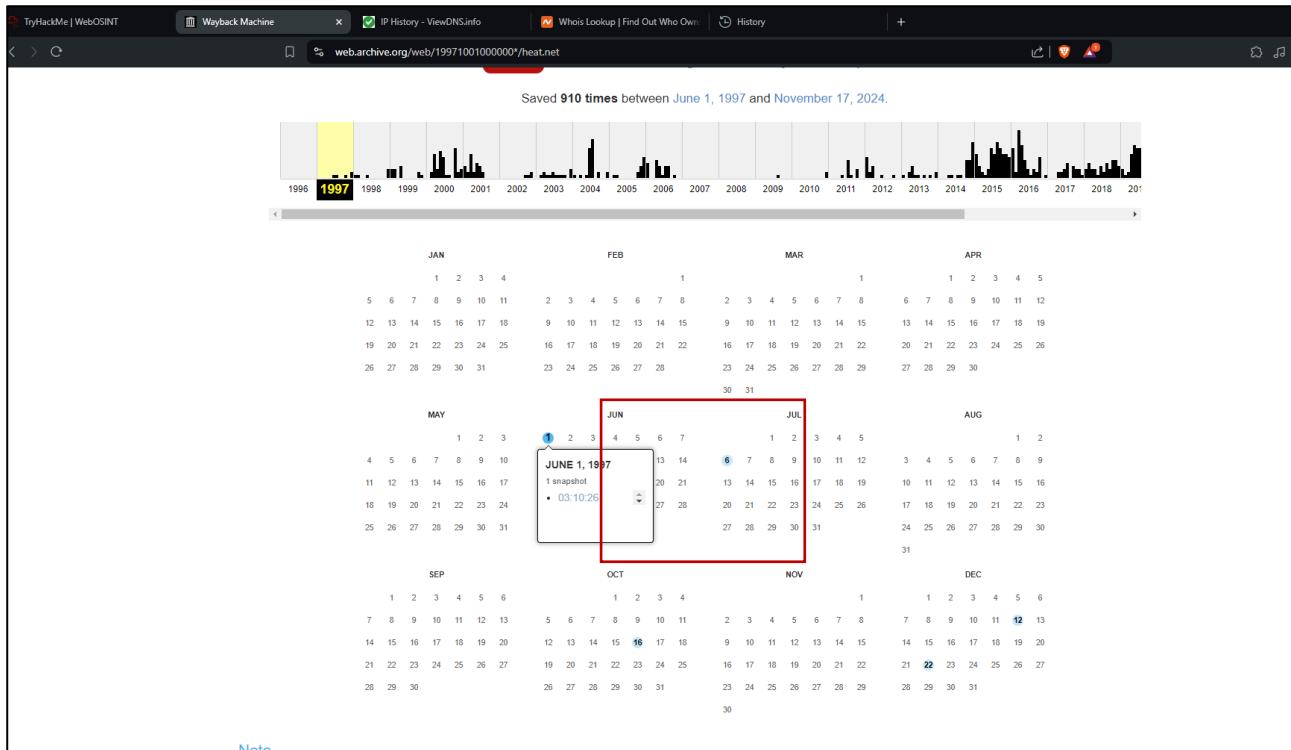
Shows a historical list of IP addresses a given domain name has been hosted on as well as where that IP address is geographically located, and the owner of that IP address.

Domain (e.g. domain.com): GO

IP history results for heat.net.

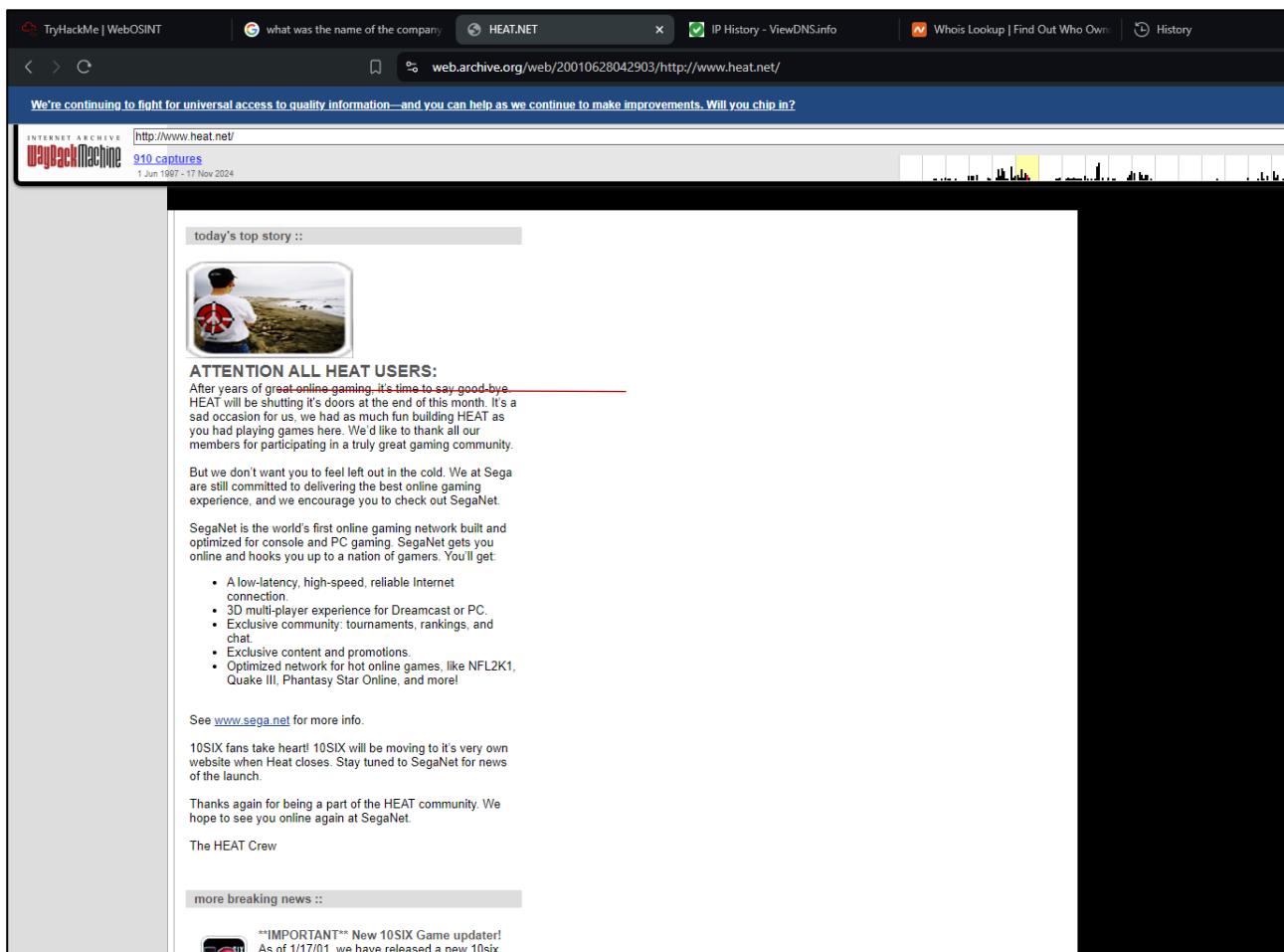
IP Address	Location	IP Address Owner	Last seen on this IP
208.117.87.195	United States	ATLANTIC-NET-1	2024-11-20
74.116.2.147	United States	PERFORMIVE	2019-06-19
72.52.192.240	United States	LIQUIDWEB	2011-12-19

- + On what date did the site first capture by the internet archive? (MM/DD/YY format)



Note

- + What is the first sentence of the first body paragraph from the final capture of 2001?



+ Using your search engine skills, what was the name of the company that was responsible for the original version of the site?

Google search results for the query "what was the name of the company that was responsible for the original version of the site?".

SegaSoft

SegaSoft was responsible for, among other things, the Heat.net multiplayer game system and publishing the last few titles made by Rocket Science Games.

[SegaSoft - Wikipedia](https://en.wikipedia.org/wiki/SegaSoft)

Sega Retro

Heat.net was an online PC gaming system produced by **SegaSoft**, Sega's PC game division. Heat.net hosted both Sega-published first- and second-party games, ...

Heat.net

Heat.net was an online PC gaming system produced by **SegaSoft**, Sega's PC game division. Heat.net hosted both Sega-published first- and second-party games, ...

Heat (1995 film)

This edition contains the original theatrical cut. The initial Blu-ray Disc was released by **Warner Home Video** on November 10, 2009, featuring a high ...

[H]ardForum

HEAT.NET - Were you there, do you remember? Post up!

Nov 8, 2011 — For those of you who don't know, HEAT.NET was founded by "Gary" who I remember being the CEO of **Segasoft** during the late 90's.

+ What does the first header on the site on the last capture of 2010 say?

Lab 3: Reconnaissance

Nhóm 6

We're continuing to fight for universal access to quality information—and you can help as we continue to make improvements. Will you chip in?

INTERNET ARCHIVE http://www.heat.net/ 910 captures 1 Jun 1997 - 17 Nov 2024

Heat.net

HEAT.net

Heating

Ventilation

Air Conditioning

Residential / Commercial

RATED #1 - Heating and Cooling (Nationwide)

Don't Get Left in the Cold! Get 3 Furnace Estimates Now!

QualitySmith

CLICK HERE

BBB

CERTIFIED Be Certain. Call Certified!

Heat.net – Heating and Cooling

No matter how you think about it, a house is simply not a home without proper functioning **heating** and **cooling** systems and devices. And the same can be said about any business or commercial property.

Think about it for a moment. Is it any use having a nice house to provide shelter if you end up shivering and shivering all through the night on those long, cold winter nights or dripping in sweat all summer long? Or having an office space that you dread heading to every day?

Whether you are looking to purchase a new home or commercial space, or simply want to make the most of the one you have, heating and cooling systems are often the most important factor of real estate ownership on the whole.

And that is precisely why we here at Heat.net want to break down the details, cover the bases, and make sure you understand all of the aspects and intricacies of **HVAC**.

Good luck!

Room completed (100%)

Answer the questions below

What is the second nameserver listed for the domain?

NS2.HEAT.NET ✓ Correct Answer

What IP address was the domain listed on as of December 2011?

72.52.192.240 ✓ Correct Answer

Based on domains that share the same IP, what kind of hosting service is the domain owner using?

shared ✓ Correct Answer

On what date did the site first capture by the internet archive? (MM/DD/YY format)

06/01/97 ✓ Correct Answer

What is the first sentence of the first body paragraph from the final capture of 2001?

After years of great online gaming, it's time to say good-bye. ✓ Correct Answer

Using your search engine skills, what was the name of the company that was responsible for the original version of the site?

SegaSoft ✓ Correct Answer

What does the first header on the site on the last capture of 2010 say?

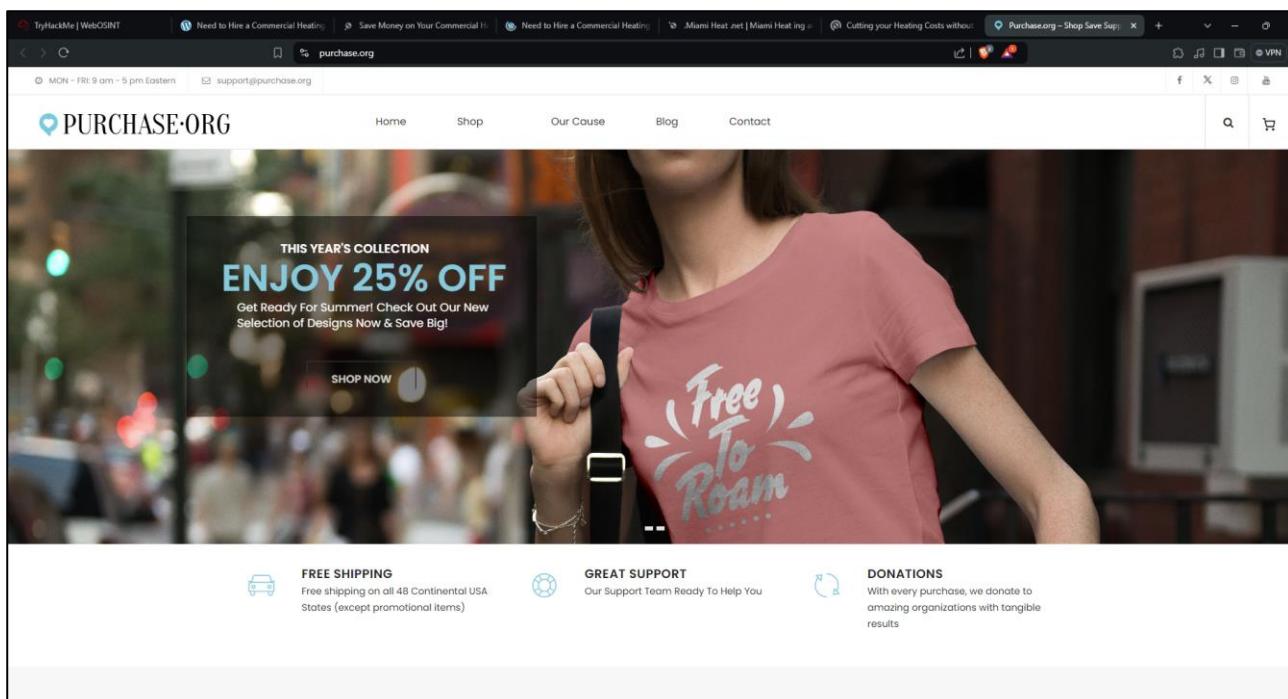
Heat.net – Heating and Cooling ✓ Correct Answer

- Task 6: Truy cập vào đường dẫn yêu cầu đưa ra là heat.net/36/need-to-hire-a-commercial-heating-contractor/

+ Đầu tiên ta thấy được có 6 link ta có thể hover vào, truy cập từng link một ta sẽ thấy có 5 link thuộc heat.net và 1 link là đường dẫn đến purchase.org

Lab 3: Reconnaissance

Nhóm 6



+ Tiếp theo ở trang web chính, thực hiện F12 -> ở tab Element ta Ctrl F rồi điền vào chữ google => tìm kiếm lần lượt để tìm Google Analytics code

The screenshot shows a search result from the heat.net website. The page title is "Need to Hire a Commercial Heating Contractor?". The content includes a brief introduction, a list of steps to find a contractor, and a sidebar with recent articles and sponsored results. On the right side, the Google Chrome DevTools Elements tab is open, showing the source code of the page. A search term "google" has been entered in the search bar, and the results show the Google Analytics tracking code: `window.google_analytics_wacct = "UA-251372-24";`.

+ Truy cập <https://www.nerdydata.com/> và tìm kiếm những trang web có sử dụng mã code này sẽ thấy chỉ có duy nhất 1 trang web là heat.net sử dụng nó nên câu trả lời sẽ là nay

+ Ngoài ra khi truy cập vào purchase.org thì không có mã liên kết nào được dính kèm vào đó nên câu trả lời là Nay

- Task 7: Sử dụng IP History để tìm điểm chung của heat.net và purchase.org
- + Purchase.org

Lab 3: Reconnaissance

Nhóm 6

IP Address	Location	IP Address Owner	Last seen on this IP
172.67.197.177	Unknown	Cloudflare, Inc	2022-05-12
104.21.92.201	Unknown	Cloudflare, Inc	2022-05-12
188.114.97.2	Unknown	Cloudflare, Inc	2022-04-23
188.114.96.2	Unknown	Cloudflare, Inc	2022-04-23
172.67.197.177	Unknown	Cloudflare, Inc	2022-04-23
104.21.92.201	Unknown	Cloudflare, Inc	2022-04-23
188.114.97.2	Unknown	Cloudflare, Inc	2022-03-19
188.114.96.2	Unknown	Cloudflare, Inc	2022-03-19
172.67.197.177	Unknown	Cloudflare, Inc	2022-03-17
104.21.92.201	Unknown	Cloudflare, Inc	2022-03-17
188.114.97.2	Unknown	Cloudflare, Inc	2022-03-12
188.114.96.2	Unknown	Cloudflare, Inc	2022-03-12
172.67.197.177	Unknown	Cloudflare, Inc	2022-03-12
104.21.92.201	Unknown	Cloudflare, Inc	2022-03-12
188.114.97.2	Unknown	Cloudflare, Inc	2022-03-05
188.114.96.2	Unknown	Cloudflare, Inc	2022-03-05
172.67.197.177	Unknown	Cloudflare, Inc	2022-03-05
104.21.92.201	Unknown	Cloudflare, Inc	2022-03-05
188.114.97.2	Unknown	Cloudflare, Inc	2022-02-12
188.114.96.2	Unknown	Cloudflare, Inc	2022-02-12
172.67.197.177	Unknown	Cloudflare, Inc	2022-02-12
104.21.92.201	Unknown	Cloudflare, Inc	2022-02-12
188.114.97.2	Unknown	Cloudflare, Inc	2022-02-05
188.114.96.2	Unknown	Cloudflare, Inc	2022-02-05
172.67.197.177	Unknown	Cloudflare, Inc	2022-02-03
104.21.92.201	Unknown	Cloudflare, Inc	2022-02-03
104.27.185.115	Unknown	Cloudflare, Inc	2021-01-14
104.27.184.115	Unknown	Cloudflare, Inc	2021-01-14
206.196.110.108	United States	CDM	2017-11-03
67.43.1.187	United States	LIQUIDWEB	2013-04-19
72.52.193.127	United States	LIQUIDWEB	2012-11-16

+ heat.net

IP Address	Location	IP Address Owner	Last seen on this IP
208.117.87.195	United States	ATLANTIC-NET-1	2024-11-20
74.116.2.147	United States	PERFORMIVE	2019-06-19
72.52.192.240	United States	LIQUIDWEB	2011-12-19

⇒ Có thể thấy cả hai đều có chung chủ sở hữu là LIQUIDWEB

Room completed (100%)

Task 5 ✓ Taking Off The Training Wheels

Task 6 ✓ Taking A Peek Under The Hood Of A Website

Task 7 ✓ Final Exam: Connect the Dots

Experienced OSINT researchers will tell you that chasing rabbit holes all day and night without being able to make some solid connections is not OSINT. OSINT refers to the patterns that start to emerge as we connect the dots in the analysis of the data.

Congrats! you found that our target, heatl.net, links to an interesting external site. A question remains though: Why???

There is no affiliate code in the link, so there is no obvious financial connection between the two. Maybe there's another kind of connection.

This is your final exam, and there is exactly one question.

Get busy!

Answer the questions below

Use the tools in Task 4 to confirm the link between the two sites. Try hard to figure it out without the hint.

Liquid Web, L.L.C

Correct Answer

Hint

- Task 8 và Task 9: hai task này cho ta biết thêm các thông tin hữu ích về OSINT, vì vậy chỉ cần submit trống là được

Bài Tập Làm Thêm HackTheBox: <https://academy.hackthebox.com/module/details/54>

Task: Directory Fuzzing

- Video thực hiện: <https://youtu.be/ATXu4l0yzUo>
 - Target IP:

Questions

Answer the question(s) below to complete this Section and earn cubes!

Target(s): 94.237.51.81:40025 🔍

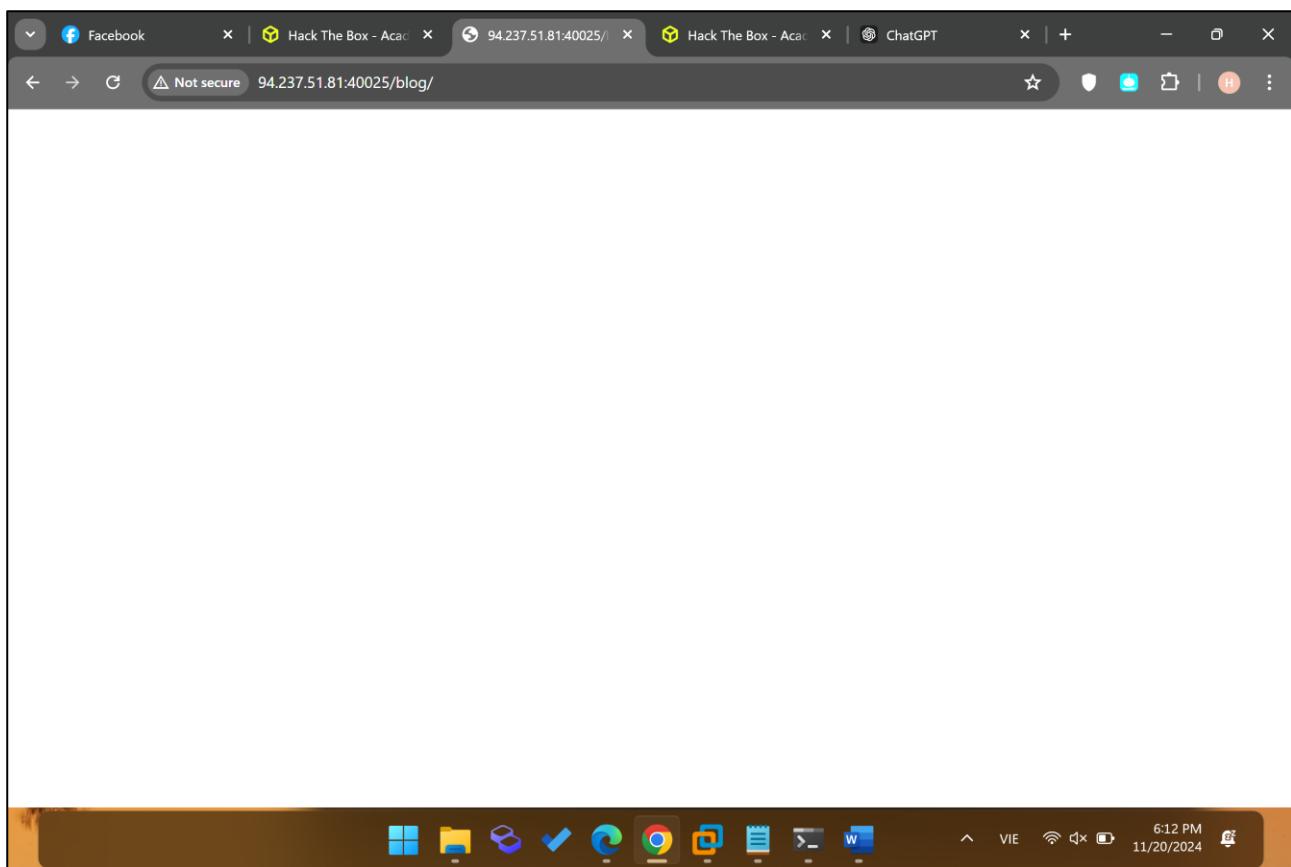
Life Left: 11 minute(s)

+ 0 🎁 In addition to the directory we found above, there is another directory that can be found. What is it?

forum

Submit Hint

- Thực hiện theo hướng dẫn bài Lab



Task: Page Fuzzing

- Video thực hiện: <https://youtu.be/Zb-TPK92c8c>
- Server IP:

Questions

Answer the question(s) below to complete this Section and earn cubes!

Target(s): 94.237.51.74:59536

Life Left: 88 minute(s)

+ 1 🎁 Try to use what you learned in this section to fuzz the '/blog' directory and find all pages. One of them should contain a flag.

What is the flag?

HTB{bru73_f0r_c0mm0n_p455w0rd5}

Submit **Hint**

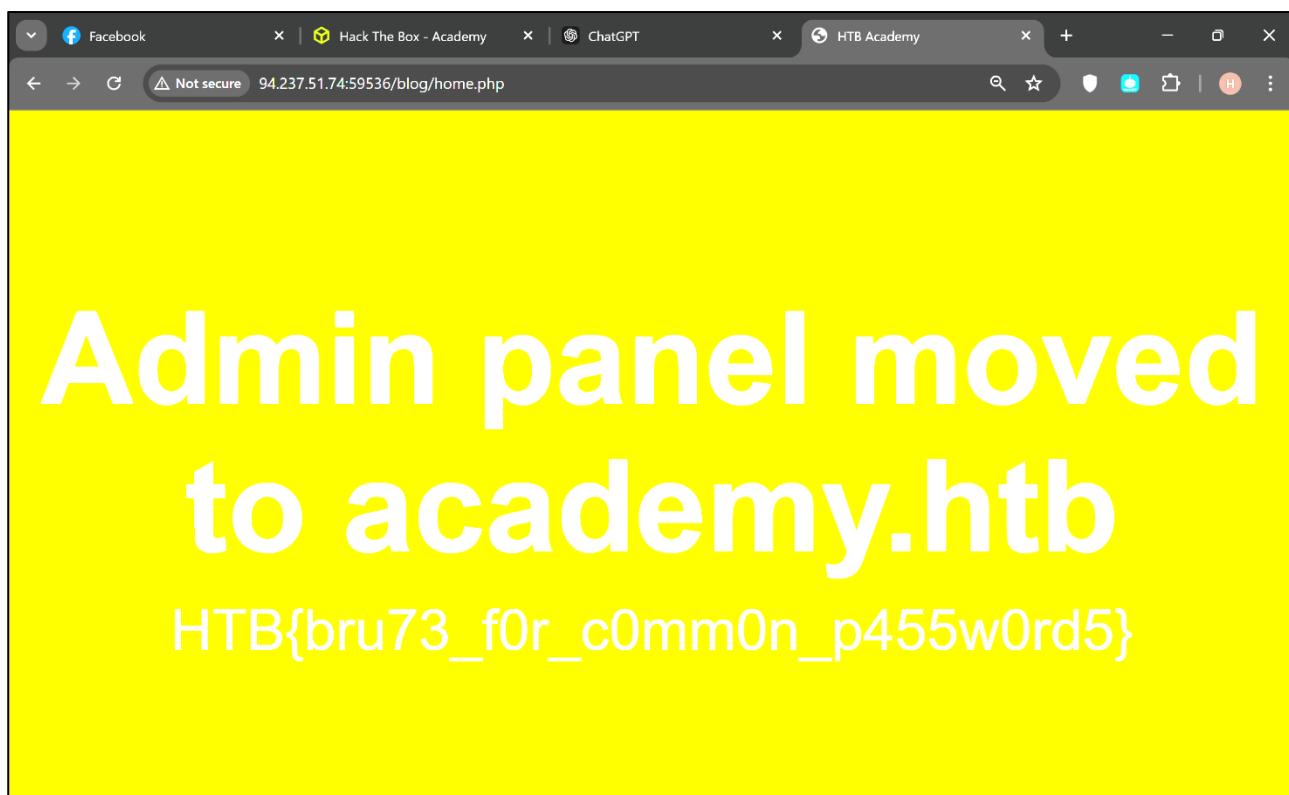
- Thực hiện:

```
hohey@huy: ~ x Windows PowerShell x + v
[hohey@huy ~]$ ffuf -w /usr/share/seclists/Discovery/Web-Content/web-extensions.txt:FUZZ -u http://94.237.51.74:59536/blog/indexFUZZ

v1.5.0 Kali Exclusive <3
-----
:: Method      : GET
:: URL         : http://94.237.51.74:59536/blog/indexFUZZ
:: Wordlist    : FUZZ: /usr/share/seclists/Discovery/Web-Content/web-extensions.txt
:: Follow redirects : false
:: Calibration   : false
:: Timeout       : 10
:: Threads       : 40
:: Matcher       : Response status: 200,204,301,302,307,401,403,405,500
-----
.php           [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 2754ms]
.php           [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 4740ms]
:: Progress: [41/41] :: Job [1/1] :: 9 req/sec :: Duration: [0:00:06] :: Errors: 0 ::

[hohey@huy ~]$
```

- Kết quả:



Task: Recursive Fuzzing

- Video thực hiện: <https://youtu.be/MX1w-BnmnsM>
 - Target IP:

Questions

Answer the question(s) below to complete this Section and earn cubes!

Target(s): 94.237.51.74:59536 🔗

Life Left: 51 minute(s)

+ 1 🎁 Try to repeat what you learned so far to find more files/directories. One of them should give you a flag. What is the content of the flag?

HTB{fuzz1n6_7h3_w3bl!}

+10 Streak pts

 Submit

 Hint

- Thực hiện:

- Kết quả:

```
hohuy@huy:~          X + ▾

| URL | http://94.237.51.74:59536/forum/# on at least 3 different hosts
 * FUZZ: # on at least 3 different hosts

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 252ms]
| URL | http://94.237.51.74:59536/forum/# This work is licensed under the Creative Commons
 * FUZZ: # This work is licensed under the Creative Commons

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 252ms]
| URL | http://94.237.51.74:59536/forum/# Attribution-Share Alike 3.0 License. To view a copy of this.php
 * FUZZ: # Attribution-Share Alike 3.0 License. To view a copy of this.php

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 252ms]
| URL | http://94.237.51.74:59536/forum/
 * FUZZ:

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 256ms]
| URL | http://94.237.51.74:59536/forum/# Attribution-Share Alike 3.0 License. To view a copy of this
 * FUZZ: # Attribution-Share Alike 3.0 License. To view a copy of this

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 264ms]
| URL | http://94.237.51.74:59536/forum/# license, visit http://creativecommons.org/licenses/by-sa/3.0/.php
 * FUZZ: # license, visit http://creativecommons.org/licenses/by-sa/3.0/.php

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 264ms]
| URL | http://94.237.51.74:59536/forum/# or send a letter to Creative Commons, 171 Second Street,
 * FUZZ: # or send a letter to Creative Commons, 171 Second Street,

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 202ms]
| URL | http://94.237.51.74:59536/forum/index.php
 * FUZZ: index.php

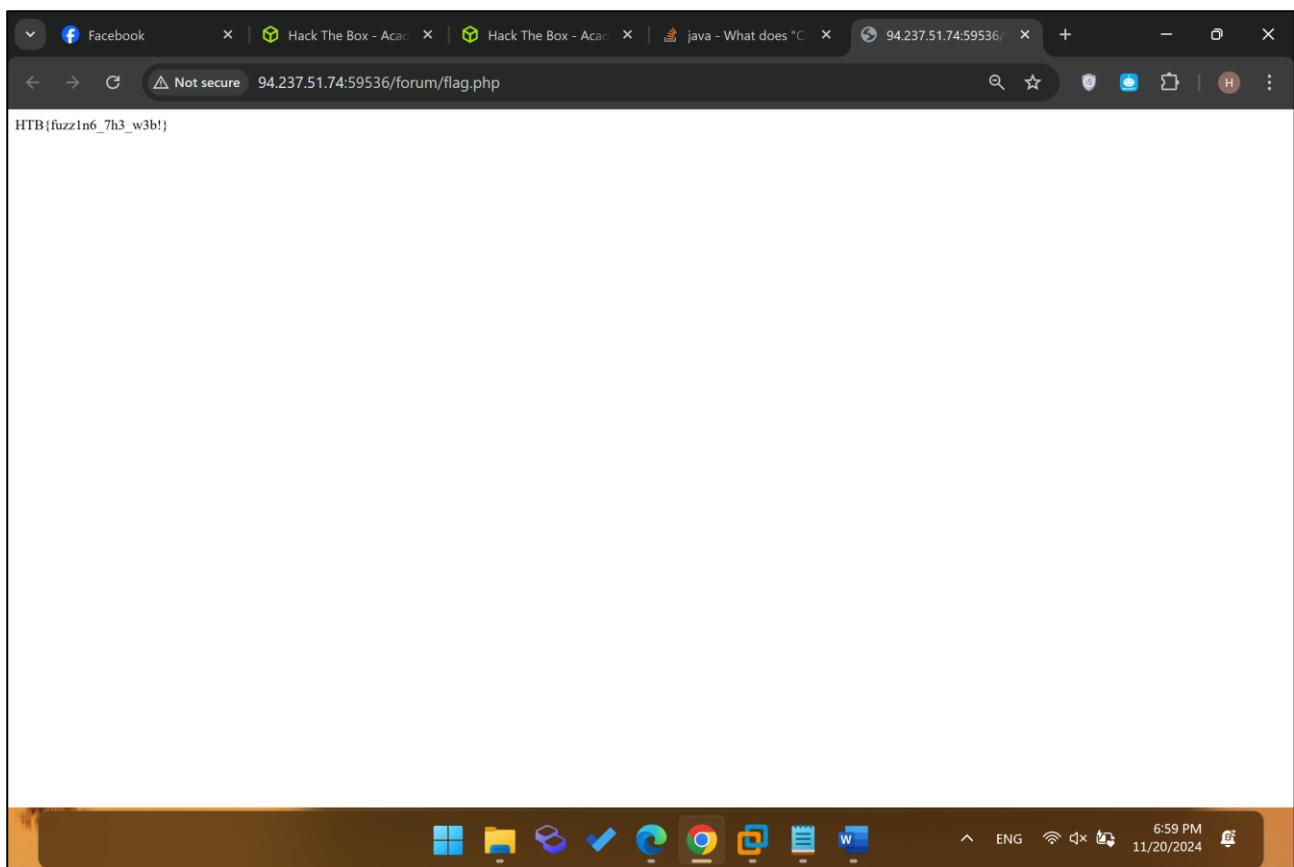
[Status: 200, Size: 21, Words: 1, Lines: 1, Duration: 237ms]
| URL | http://94.237.51.74:59536/forum/flag.php
 * FUZZ: flag.php

[Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 238ms]
| URL | http://94.237.51.74:59536/forum/.php
 * FUZZ: .php

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 240ms]
| URL | http://94.237.51.74:59536/forum/
 * FUZZ:

:: Progress: [175328/175328] :: Job [3/3] :: 166 req/sec :: Duration: [0:05:04] :: Errors: 4996 ::

(hohuy@huy)-[~]
$
```



Task: Sub-domain Fuzzing

- Video thực hiện: https://youtu.be/MdWl69ig_M0
 - Thực hiện:

```
hohuy@huy: ~ + | v
[~] $ ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u https://FUZZ.inlanefreight.com/ -t 400

v1.5.0 Kali Exclusive <3

:: Method      : GET
:: URL         : https://FUZZ.inlanefreight.com/
:: Wordlist    : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 400
:: Matcher     : Response status: 200,204,301,302,307,401,403,405,500
-----
my           [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 559ms]
www          [Status: 200, Size: 22266, Words: 2903, Lines: 316, Duration: 621ms]
support       [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 494ms]
customer     [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 861ms]
:: Progress: [4989/4989] :: Job [1/1] :: 37 req/sec :: Duration: [0:02:26] :: Errors: 4985 ::

[~] $
```

- Kết quả:

Questions

Answer the question(s) below to complete this Section and earn cubes!

+ 0 Try running a sub-domain fuzzing test on 'inlanefreight.com' to find a customer sub-domain portal. What is the full domain of it?

customer.inlanefreight.com

Submit Hint

Task: Filtering Results

- Video thực hiện: <https://youtu.be/kxeTYCckg8c>
- Câu hình hosts:

```
root@thinnlinux: /home/kali ~ + - 
GNU nano 8.2 /etc/hosts
127.0.0.1 localhost
127.0.1.1 kali
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
94.237.51.74 academy.htb
```

Enable step-by-step solutions for all questions

Questions
Answer the question(s) below to complete this Section

Target(s): 94.237.51.74:43405
Life Left: 85 minute(s)

+ 0 Try running a VHost fuzzing scan on 'academy.htb'. What other VHosts did you get?

Submit your answer here...

^C Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^A Replace ^U Paste ^J Justify ^V Go To Line M-B Redo

- Chạy lệnh như hình dưới, ở đây ta lấy thông số -fs là 900

```
(root@thinnlinux)-[~/Documents/NT213/Lab_3]
# ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u http://academy.htb:43405/ -H 'Host: FUZZ.academy.htb' -fs 900 -t 200
v2.1.0-dev
-----
:: Method : GET
:: URL : http://academy.htb:43405/
:: Wordlist : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
:: Header : Host: FUZZ.academy.htb
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 200
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500
:: Filter : Response size: 900
-----
:: Progress: [1/4989] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::|
```

Enable step-by-step solutions

Questions
Answer the question(s) below to complete this Section

Target(s): 94.237.51.74:43405
Life Left: 85 minute(s)

+ 0 Try running a VHost fuzzing scan on 'academy.htb'. What other VHosts did you get?

Submit your answer here...

Lab 3: Reconnaissance

Nhóm 6

```
content2 [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9134ms]
ppc [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9165ms]
www.reklama [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9165ms]
qmail [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9118ms]
i4 [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9165ms]
openfire [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9165ms]
robo [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9118ms]
impact [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9129ms]
date [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9165ms]
xg [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9096ms]
bid [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9096ms]
chemistry [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9096ms]
tps [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9120ms]
doors [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9109ms]
popo [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9113ms]
shiva [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9125ms]
agri [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9094ms]
fund [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9138ms]
vsp [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9139ms]
www.school [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9135ms]
webdisk.crm [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9139ms]
ivr [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9140ms]
lime [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9139ms]
autoconfig.email [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9135ms]
www.dom [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9139ms]
p80.pool [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9111ms]
asterix [Status: 200, Size: 986, Words: 423, Lines: 56, Duration: 9137ms]
:: Progress: [4989/4989] :: Job [1/1] :: 140 req/sec :: Duration: [0:00:19] :: Errors: 0 ::
```

- Tại đây kết quả trả về với size là 986 rất nhiều, ta tiến hành lọc nó, thay đổi thông số -fs là 986:

=> Kết quả trả về là “test”

Waiting to start...

Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

Target(s): 94.237.51.74:43405

Life Left: 84 minute(s)

+ 0 Try running a VHost fuzzing scan on 'academy.htb', and see what other VHosts you get. What other VHosts did you get?

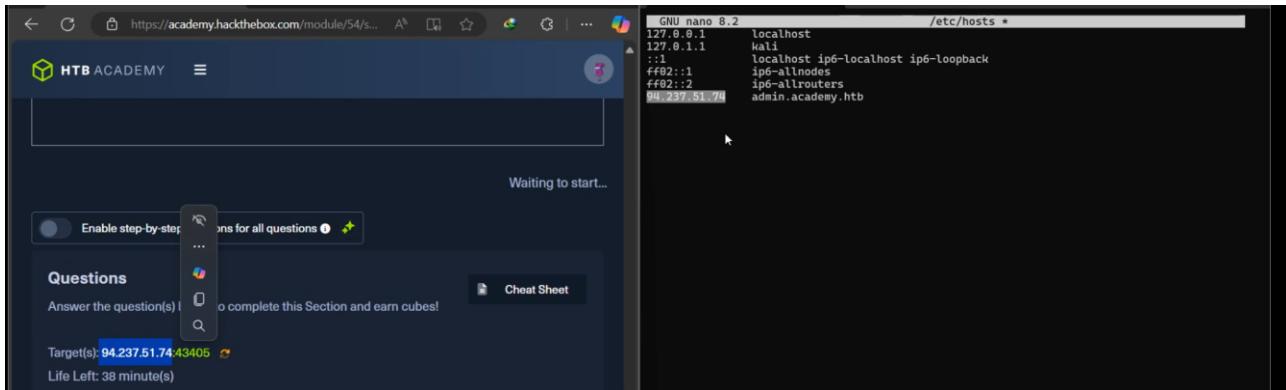
test.academy.htb

✓ Success
Congratulations! You earned 0 cubes!

=> Vhost là test.academy.htb

Task: Parameter Fuzzing – GET

- Video thực hiện: <https://youtu.be/k2a2XRLteao>
- Cấu hình hosts:



- Chạy với thông số -fs 100, ta thấy được kết quả trả về với size 798 rất nhiều:

```
(root㉿thinnnlinux)-[~/home/kali/Documents/NT213/Lab_3]
└─# ffuf -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt:FUZZ -u http
: //admin.academy.htb:43405/admin/admin.php?FUZZ=key -fs 100
          _/\_ _/\_ _/\_
         /  \ /  \ /  \
        /    \ /    \ /    \
       /      \ /      \ /      \
      /        \ /        \ /        \
     /          \ /          \ /          \
    /            \ /            \ /            \
   /              \ /              \ /              \
  /                \ /                \ /                \
 v2.1.0-dev

:: Method      : GET
:: URL         : http://admin.academy.htb:43405/admin/admin.php?FUZZ=key
:: Wordlist    : FUZZ: /usr/share/seclists/Discovery/Web-Content/burp-parameter-names
.txt
:: Follow redirects : false
:: Calibration   : false
:: Timeout       : 10
:: Threads       : 40
:: Matcher        : Response status: 200-299,301,302,307,401,403,405,500
:: Filter         : Response size: 100

-----
16          [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 208ms]
AMOUNT       [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 208ms]
15          [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 209ms]
21          [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 212ms]
Artist       [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 213ms]
Article      [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 211ms]
AddAuthItemForm [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 212ms]
A             [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 213ms]
Albania      [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 226ms]
AUTH          [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 225ms]
AudioPlayerSubmit [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 222ms]
AuthChildForm [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 222ms]
AuthItem      [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 222ms]
AuthItemChild [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 233ms]
BIGGER        [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 233ms]
BackURL      [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 233ms]
```

Lab 3: Reconnaissance

Nhóm 6

- Chạy lại với -fs=798, ta được kết quả trả về là user

```

www.BANDICAM.COM
root@thinnnlinux:/home/kali

yy [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 204ms]
zz [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 204ms]
zipcode [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 214ms]
zip [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 214ms]
zipName [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 214ms]
zid [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 214ms]
zoneid [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 212ms]
zonefile [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 212ms]
zone [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 212ms]
zhsv [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 230ms]
zoom [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 217ms]
zonesub [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 223ms]
zonet [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 223ms]
zoomtxt [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 229ms]
zpage [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 215ms]
zrecord [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 232ms]
:: Progress: [6453/6453] :: Job [1/1] :: 177 req/sec :: Duration: [0:00:45] :: Errors: 0 ::

[root@thinnnlinux]~/home/kali/Documents/NT213/Lab_3
# ffuf -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt:FUZZ -u http://admin.academy.htb:43405/admin/admin.php?FUZZ=key -fs 798

v2.1.8-dev

:: Method : GET
:: URL   : http://admin.academy.htb:43405/admin/admin.php?FUZZ=key
:: Wordlist: FUZZ: /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout   : 10
:: Threads    : 40
:: Matcher    : Response status: 200-299,301,302,307,401,403,405,500
:: Filter     : Response size: 798

user [Status: 200, Size: 783, Words: 221, Lines: 54, Duration: 228ms]
:: Progress: [6453/6453] :: Job [1/1] :: 155 req/sec :: Duration: [0:00:39] :: Errors: 0 ::

[root@thinnnlinux]~/home/kali/Documents/NT213/Lab_3
#

```

Task: Value Fuzzing

- Video thực hiện: <https://youtu.be/hg-F7Mqlh0c>
- Tạo file text 1000 số:

```

www.BANDICAM.COM
root@thinnnlinux:/home/kali

(root@thinnnlinux)~/home/kali/Documents/NT213/Lab_3
# for i in $(seq 1 1000); do echo $i >> ids.txt; done

(root@thinnnlinux)~/home/kali/Documents/NT213/Lab_3
# ls
apple-domain.csv      main.sh          subdomains_ip.csv
gol.23.3.linux-amd64.tar.gz nmap_scan_results.gnmap subdomains-top1million-110000.txt
gobuster_output_2.txt   nmap_scan_results.nmap   subdomains-top1million-5000.txt
gobuster_output.txt    nmap_scan_results.xml  subdomains.txt
gobuster_output.txtclea subdomains.csv       Sublist3r
ids.txt                subdomains_indriver.txt vhosts_200.txt

(root@thinnnlinux)~/home/kali/Documents/NT213/Lab_3
# cat ids.txt

```

- Chạy với lệnh bên dưới, ta set -fs = 100, kết quả trả về cho ta size=768 khá nhiều

```
(root@thinlinux)-[~/Documents/NT213/Lab_3]
# ffuf -w ids.txt:FUZZ -u http://admin.academy.htb:43405/admin/admin.php -X POST -d 'id=F
UZZ' -H 'Content-Type: application/x-www-form-urlencoded' -fs 100

<--> <--> <-->
<\--> \--> \-->
<--> <\--> <\-->
<\--> <\--> <\-->

v2.1.0-dev

:: Method      : POST
:: URL         : http://admin.academy.htb:43405/admin/admin.php
:: Wordlist    : FUZZ: /home/kali/Documents/NT213/Lab_3/ids.txt
:: Header      : Content-Type: application/x-www-form-urlencoded
:: Data         : id=FUZZ
:: Follow redirects : false
:: Calibration   : false
:: Timeout       : 10
:: Threads       : 40
:: Matcher       : Response status: 200-299,301,302,307,401,403,405,500
:: Filter        : Response size: 100

31          [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 217ms]
25          [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 255ms]
16          [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 248ms]
7           [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 249ms]
39          [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 248ms]
17          [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 250ms]
28          [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 251ms]
8            [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 251ms]
10           [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 251ms]
26           [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 250ms]
:: Progress: [50/2000] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::
```

Lab 3: Reconnaissance

Nhóm 6

- Chạy lại với -fs=768, ta được id = 73:

```
(root@thinlinux)-[~/home/kali/Documents/NT213/Lab_3]
# ffuf -w ids.txt:FUZZ -u http://admin.academy.htb:43405/admin/admin.php -X POST -d 'id=F
UZZ' -H 'Content-Type: application/x-www-form-urlencoded' -fs 768

<--> <--> <-->
v2.1.0-dev

:: Method      : POST
:: URL         : http://admin.academy.htb:43405/admin/admin.php
:: Wordlist    : FUZZ: /home/kali/Documents/NT213/Lab_3/ids.txt
:: Header      : Content-Type: application/x-www-form-urlencoded
:: Data         : id=FUZZ
:: Follow redirects : false
:: Calibration   : false
:: Timeout       : 10
:: Threads        : 40
:: Matcher        : Response status: 200-299,301,302,307,401,403,405,500
:: Filter         : Response size: 768

73          [Status: 200, Size: 787, Words: 218, Lines: 54, Duration: 321ms]
73          [Status: 200, Size: 787, Words: 218, Lines: 54, Duration: 399ms]
:: Progress: [2000/2000] :: Job [1/1] :: 129 req/sec :: Duration: [0:00:18] :: Errors: 0 ::
```

- sử dụng lệnh curl với id như trên để lấy flag:

```
root@thinlinux-:~/home/kali/Documents/NT213/Lab_3]
# curl http://admin.academy.htb:43405/admin/admin.php -X POST -d 'id=73' -H 'Content-Type: application/x-www-form-urlencoded' -fs 768
<div><center><p>HTB{p4r4m373r_fuzzin6_15_k3y!}</p></center></div>
<html>
<head>
<title>HTB Academy</title>
<style>
*
{
margin: 0;
padding: 0;
border: 0;
}

html {
width: 100%;
height: 100%;
}

body {
width: 100%;
```

Skills Assessment - Web Fuzzing

*** Question 1:**

Video thực hiện: <https://youtu.be/Mz6u69jz6VE>

*** Question 2:**

Video thực hiện: https://youtu.be/KhjZE_UszWc