

LAB 3 - Reconnaissance

GVHD: Ngô Khánh Khoa

Mã môn: NT213.P11.ANTN.1

Thành viên	MSSV
Vũ Ngọc Quốc Khanh	22520661
Nguyễn Đức Luân	22520825
Đào Hoàng Phúc	22521110

Bài tập 1

Đề bài

Thực hiện lệnh whois lookup với tên miền **indrider.com**

Các bước thực hiện

Link video: <https://youtu.be/lNumU82EMW0>

```
(semloh4869㉿kali)-[~]
$ 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: 2024-11-05T06:39:03Z <<<
```

Domain Name: indriver.com
Registry Domain ID: 130600645_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2024-08-26T10:18:16Z
Creation Date: 2004-09-21T17:01:04Z
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: +1.8887802723
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: +357.22667740
Registrant Fax Ext:
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

+Id của IANA của tên miền trên là gì?

Đáp án: 299

+Tên miền trên được đăng ký khi nào

Đáp án: 21/09/2004

+register của tên miền trên

Đáp án: CSC Corporate Domains, Inc.

+Công ty nào được sử dụng cho dịch vụ name server

Đáp án: AWS

+Địa chỉ admin contact email cho tên miền trên.

Đáp án: domainmaster@indriver.com

Bài tập 2

Đề bài

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

Các bước thực hiện

Link video: https://youtu.be/_JapyibzKk8

Kết quả khi dùng lệnh dig với option "mx"

```
(semloh4869㉿kali)-[~]
$ dig indriver.com mx

; <>> DiG 9.20.0-Debian <>> indriver.com mx
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: NOERROR, id: 17750
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096
;; QUESTION SECTION:
;indriver.com.           IN      MX

;; ANSWER SECTION:
indriver.com.      5       IN      MX      10 aspmx.l.google.com.
indriver.com.      5       IN      MX      11 alt1.aspmx.l.google.com.
indriver.com.      5       IN      MX      12 alt2.aspmx.l.google.com.
indriver.com.      5       IN      MX      13 alt3.aspmx.l.google.com.
indriver.com.      5       IN      MX      14 alt4.aspmx.l.google.com.

;; Query time: 4 msec
;; SERVER: 192.168.15.2#53(192.168.15.2) (UDP)
;; WHEN: Mon Nov 04 22:59:52 PST 2024
;; MSG SIZE rcvd: 159
```

```
(semloh4869㉿kali)-[~]
$
```

Giải thích:

HEADER Section:

status: NOERROR: Truy vấn thành công, không có lỗi.

flags: qr rd ra: Đánh dấu đây là một truy vấn (qr), với yêu cầu đệ quy (rd) và đã nhận được câu trả lời từ truy vấn đệ quy (ra).

QUESTION SECTION:

Xác nhận rằng truy vấn là cho tên miền indriver.com với loại truy vấn MX.

ANSWER SECTION: Đây là danh sách các bản ghi MX của indriver.com, cùng với độ ưu tiên và tên máy chủ email của Google:

indriver.com. 5 IN MX 10 aspmx.l.google.com.: Bản ghi MX có độ ưu tiên 10, trỏ đến máy chủ aspmx.l.google.com.

indriver.com. 5 IN MX 11 alt1.aspmx.l.google.com.: Độ ưu tiên 11, trỏ đến alt1.aspmx.l.google.com.

indriver.com. 5 IN MX 12 alt2.aspmx.l.google.com.: Độ ưu tiên 12, trỏ đến alt2.aspmx.l.google.com.

indrider.com. 5 IN MX 13 alt3.aspmx.l.google.com.: Độ ưu tiên 13, trỏ đến alt3.aspmx.l.google.com.

indrider.com. 5 IN MX 14 alt4.aspmx.l.google.com.: Độ ưu tiên 14, trỏ đến alt4.aspmx.l.google.com.

Độ ưu tiên này xác định thứ tự ưu tiên của các máy chủ email, trong đó độ ưu tiên thấp hơn sẽ được thử trước khi đến các máy chủ có độ ưu tiên cao hơn.

Thông tin bổ sung:

Query time: Thời gian để hoàn thành truy vấn là 4 mili giây.

SERVER: Máy chủ DNS thực hiện truy vấn là 192.168.15.2, đây là một địa chỉ IP nội bộ.

WHEN: Thời gian thực hiện truy vấn là Mon Nov 04 22:59:52 PST 2024.

MSG SIZE rcvd: Kích thước thông điệp nhận được là 159 byte.

Kết quả khi dùng lệnh nslookup:

```
Home
└─(semloh4869㉿kali)-[~]
$ nslookup -query=mx indriver.com

Server:      192.168.15.2
Address:     192.168.15.2#53

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

Authoritative answers can be found from:

└─(semloh4869㉿kali)-[~]
$
```

Bài tập 3

Đề bài

Thực hiện truy vấn IP với tên miền indriver.com.

Các bước thực hiện

Link video: <https://youtu.be/fSI7PYC2SGQ>

+Địa chỉ IP nào map với indriver.com

```
[semloh4869@kali] ~]$ nslookup indriver.com  
Server: 192.168.15.2  
Address: 192.168.15.2#53  
  
Non-authoritative answer:  
Name: indriver.com  
Address: 3.165.82.24  
Name: indriver.com  
Address: 3.165.82.80  
Name: indriver.com  
Address: 3.165.82.101  
Name: indriver.com  
Address: 3.165.82.90
```

+Tên miền nào trả đến địa chỉ 134.209.24.248

```
[semloh4869@kali] ~]$ nslookup 134.209.24.248  
248.24.209.134.in-addr.arpa name = inlanefreight.com.  
  
Authoritative answers can be found from:
```

+Mail server nào liên quan đến tên miền indriver.com

```
[semloh4869@kali] ~]$ nslookup -query=mx indriver.com  
Server: 192.168.15.2  
Address: 192.168.15.2#53  
  
Non-authoritative answer:  
indriver.com mail exchanger = 10 aspmx.l.google.com.  
indriver.com mail exchanger = 11 alt1.aspmx.l.google.com.  
indriver.com mail exchanger = 12 alt2.aspmx.l.google.com.  
indriver.com mail exchanger = 13 alt3.aspmx.l.google.com.  
indriver.com mail exchanger = 14 alt4.aspmx.l.google.com.  
  
Authoritative answers can be found from:
```

aspmx.l.google.com với độ ưu tiên 10

alt1.aspmx.l.google.com với độ ưu tiên 11

alt2.aspmx.l.google.com với độ ưu tiên 12

alt3.aspmx.l.google.com với độ ưu tiên 13

alt4.aspmx.l.google.com với độ ưu tiên 14

Bài tập 4

Đề bài

Liệt kê các tên miền phụ của **indriver.com**, kết quả lưu trong file **csv**.

Các bước thực hiện

Link video: https://youtu.be/VSCBqLJZ9_M

Sử dụng Subdomainfinder : <https://subdomainfinder.c99.nl/> nhập domain cần tìm:

Result of indriver.com

<https://subdomainfinder.c99.nl/scans/2024-11-04/indriver.com>

Scan date 2024-11-04 00:00:30
Domain Country: Worldwide (COM)
Subdomains found: 52
Most used IP: 18.66.122.104 (2x)

[Whois Check](#) [Check Status](#) [Copy to clipboard](#) [Download CSV](#) [Download JSON](#)

Subdomain	IP	Cloudflare
apple.indriver.com	188.42.196.189	
book.indriver.com	167.172.86.54	
cargo.indriver.com	18.66.122.111	
console.s3-kz.indriver.com	185.102.74.214	
freight.indriver.com	18.66.122.111	
ic.indriver.com	3.165.136.77	
injob.indriver.com	18.66.122.27	
job.indriver.com	18.66.122.71	
lena.indriver.com	188.42.196.189	
pagerduty.indriver.com	185.199.110.153	
promo.indriver.com	18.66.122.104	
redmine.indriver.com	188.42.196.15	
s3-kz.indriver.com	185.102.74.214	
share.indriver.com	162.159.140.159	

Kết quả lưu file csv:

	A	B	C	D	E	F
1	Subdomain	IP	Cloudflare			
2	apple.indriver.com	188.42.196.189	FALSE			
3	book.indriver.com	167.172.86.54	FALSE			
4	cargo.indriver.com	18.66.122.111	FALSE			
5	console.s3-kz.indriver.com	185.102.74.214	FALSE			
6	freight.indriver.com	18.66.122.111	FALSE			
7	ic.indriver.com	3.165.136.77	FALSE			
8	injob.indriver.com	18.66.122.27	FALSE			
9	job.indriver.com	18.66.122.71	FALSE			
10	lena.indriver.com	188.42.196.189	FALSE			
11	pagerduty.indriver.com	185.199.110.153	FALSE			
12	promo.indriver.com	18.66.122.104	FALSE			
13	redmine.indriver.com	188.42.196.15	FALSE			
14	s3-kz.indriver.com	185.102.74.214	FALSE			
15	share.indriver.com	162.159.140.159	TRUE			
16	sharetrip.indriver.com	18.66.122.71	FALSE			
17	sm.indriver.com	18.66.122.104	FALSE			
18	teammate.indriver.com	188.42.196.188	FALSE			
19	url-checker.indriver.com	185.199.108.153	FALSE			
20	www.indriver.com	3.165.136.76	FALSE			
21						
22						
23						

Sử dụng công cụ khác là <https://dnsdumpster.com/> và nhập domain cần tìm.

The screenshot shows the dnsdumpster.com interface with the URL https://dnsdumpster.com/ in the address bar. The page displays host records for various subdomains of indriver.com, such as apple.indriver.com, lena.indriver.com, job.indriver.com, ic.indriver.com, etc. Each record includes the IP address, location (e.g., Czechia, Luxembourg, Netherlands), and the name of the DNS provider (e.g., ORATOR, SERVERS-COM, DDOS-GUARD). The interface also shows icons for a home button, a shield, a graduation cap, and a magnifying glass.

Domain	IP	Provider
indriver.com	185.104.210.6	ORATOR-Czechia
apple.indriver.com	188.42.196.15	SERVERS-COM-Luxembourg
lena.indriver.com	23.109.150.18	SERVERS-COM-Netherlands
job.indriver.com	185.104.209.7	ORATOR-Czechia
ic.indriver.com	185.215.4.20	DDOS-GUARD-Russia
classified.indriver.com	185.104.211.6	ORATOR-Czechia
rd.indriver.com	185.215.4.20	DDOS-GUARD-Russia
apple.indriver.com	188.42.196.189	SERVERS-COM-Luxembourg
redmine.indriver.com	188.42.196.189	SERVERS-COM-Luxembourg
teammate.indriver.com	188.42.196.188	SERVERS-COM

Kết quả lưu file csv:

	A	B	C	D	E	F	G	H
1	Hostname	IP Address	T	Reverse DNS	Netblock Owner	Country	Tech / Apps	HTTP / Title
2	indriver.com	185.104.210.6	A		QRATOR-	Czechia		QRATOR title: 302 Found
3	lena.indriver.com	188.42.196.15	A		SERVERS-COM	Luxembourg		
4	job.indriver.com	23.109.150.18	A		SERVERS-COM	Netherlands		
5	injob.indriver.com	185.104.209.7	A		QRATOR-	Czechia		QRATOR
6	ic.indriver.com	185.215.4.20	A		DDOS-GUARD	Russia		ddos-guard title: 403 Forbidden.
7	classified.indriver.com	185.104.211.6	A		QRATOR-	Czechia		QRATOR
8	rd.indriver.com	185.215.4.20	A		DDOS-GUARD	Russia		ddos-guard title: 403 Forbidden.
9	apple.indriver.com	188.42.196.189	A		SERVERS-COM	Luxembourg		
10	redmine.indriver.com	188.42.196.189	A		SERVERS-COM	Luxembourg		
11	teammate.indriver.com	188.42.196.188	A		SERVERS-COM	Luxembourg		
12	auth.indriver.com	23.109.150.17	A		SERVERS-COM	Netherlands		
13	msk.indriver.com	23.109.150.17	A		SERVERS-COM	Netherlands		
14	sm.indriver.com	185.215.4.20	A		DDOS-GUARD	Russia		ddos-guard title: 403 Forbidden.
15	aldan.indriver.com	23.105.241.120	A		UNITEDNET	Russia		

Bài tập 5

Đề bài

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.

Các bước thực hiện

Link video: <https://youtu.be/hogIdhkKJEo>

+ Sử dụng công cụ Burp Suite:

Bước 1: mở Browser và truy cập tên miền indriver.com và chọn một gói tin đem vào Intruder:

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x 2 x + Positions Payloads Resource pool Settings

Choose an attack type
Attack type: Sniper

Payload positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://indriver.com Update Host header to match target

```

1 GET / HTTP/1.1
2 Host: indriver.com
3 Sec-Ch-Ua: "Chromium";v="129", "Not=A?Brand";v="0"
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: "Windows"
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/129.0.6660.71 Safari/537.36
9 Accept: */*,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
16 Connection: keep-alive
17
18

```

Bước 2: Thêm subdomain vào url để tìm kiếm, sử dụng nút Add "\$"

Choose an attack type

Attack type: Sniper

Payload positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://\$subdomain\$indriver.com Update Host header to match target

```

1 GET / HTTP/1.1
2 Host: $subdomain$indriver.com
3 Sec-Ch-Ua: "Chromium";v="129", "Not=A?Brand";v="0"
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: "Windows"
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/129.0.6660.71 Safari/537.36
9 Accept: */*,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
16 Connection: keep-alive
17
18

```

Bước 3: Qua tab payload, tiến hành load list subdomain vào

Burp Suite Community Edition v2024.8.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x 2 x + Positions Payloads Resource pool Settings

Start attack

Payload sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 4,989
Payload type: Simple list Request count: 0

Payload settings [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.

Paste www
Load... mail
ftp
load items from file... host
jail
Clear smtp
webdisk
pop
cpanel
Add Enter a new item
Add from list... [Pro version only]

Payload processing

Bước 4: Start attack và kiểm tra kết quả trả về, có thể tùy chỉnh thời gian giữa 2 câu request tại Resource pool để phù hợp với tốc độ trả về của trang web cần tìm kiếm, tránh việc trang

web bị ddos.

The screenshot shows the NetworkMiner interface with the 'Results' tab selected. It displays a list of requests from various subdomains of indriver.com to the main domain. The columns include Request, Payload, Target, Status code, Response received, Error, Timeout, Length, and Comment. A 'baseline request' is noted for the 915 entry. Below this is a detailed view of a single request (line 1) in Pretty, Raw, and Hex formats, showing a GET request for the root URL with various headers including Host, User-Agent, and Sec-Fetch-Dest.

Request	Response	
Pretty	Raw	Hex
1 GET / HTTP/2 2 Host: promo.indriver.com 3 Sec-Ch-Ua: "Not(A)Brand";v="8", "Chromium";v="126" 4 Sec-Ch-Ua-Mobile: ?0 5 Sec-Ch-Ua-Platform: Linux 6 Sec-Ch-Ua-Platform-Version: 5.15 7 Upgrade-Insecure-Requests: 1 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 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: same-origin 11 Sec-Fetch-User: navigate 12 Sec-Fetch-Dest: document 13 Accept-Encoding: gzip, deflate, br 14 Priority: 0 15 Connection: keep-alive 16		

Từ kết quả thu được cho thấy không có tên miền nào có phản hồi là 200. Các tên miền có phản hồi khác bao gồm:

promo.indriver.com

job.indriver.com

book.indriver.com

spb.indriver.com

msk.indriver.com

cargo.indriver.com

www.indriver.com

s.indriver.com

redmine.indriver.com

share.indriver.com

apple.indriver.com

sm.indriver.com

Các tên miền này có các phản hồi trạng thái khác nhau như 301, 302, 403, hoặc 404.

Bài tập 6

Link youtube: <https://www.youtube.com/watch?v=Kmun3AuTYyA>

Đề bài

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

Các bước thực hiện

Thực hiện chạy bash script duyệt qua các subdomain kiểm được trong file csv từ câu trên và thực hiện nslookup từng subdomain

```
#!/bin/bash
```

```
# Define input and output files
```

```

input_file="domains.csv" # Change this to the path of your domain list
file
output_file="resolved_ips.csv"

# Initialize CSV file with header
echo "Subdomain,IP" > "$output_file"

# Loop through each line in the input file, skipping the header
tail -n +2 "$input_file" | while IFS=, read -r subdomain _ ; do
    # Skip empty lines
    if [[ -z "$subdomain" ]]; then
        continue
    fi

    # Perform nslookup and extract the IP address
    resolved_ip=$(nslookup "$subdomain" 2>/dev/null | awk '/^Address: / {
print $2; exit }')

    # If IP is found, append to the CSV file
    if [[ -n "$resolved_ip" ]]; then
        echo "$subdomain,$resolved_ip,$cloudflare" >> "$output_file"
    else
        echo "$subdomain,No IP found,$cloudflare" >> "$output_file"
    fi
done

echo "IP resolution completed. Results saved in $output_file."

```

Kết quả chạy lệnh

	Subdomain	IP
1	Subdomain	
2	apple.indriver.com	188.42.196.15
3	book.indriver.com	167.172.86.54
4	cargo.indriver.com	13.35.185.11
5	console.s3.kz.indriver.com	185.102.74.214
6	freight.indriver.com	13.35.185.11
7	ic.indriver.com	13.33.183.75
8	injob.indriver.com	13.35.185.74
9	job.indriver.com	13.35.185.11
10	lena.indriver.com	188.42.196.189
11	pagerduty.indriver.com	185.199.109.153
12	promo.indriver.com	13.35.185.74
13	redmine.indriver.com	188.42.196.15
14	s3-kz.indriver.com	185.102.74.214
15	share.indriver.com	172.66.0.157
16	sharetrip.indriver.com	13.35.185.125
17	sm.indriver.com	13.35.185.74
18	teammate.indriver.com	188.42.196.187
19	url-checker.indriver.com	185.199.110.153
20		
21		
22		
23		
24		
25		
26		
27		

Bài tập 7

Link video: <https://www.youtube.com/watch?v=k9jDkE8jlW4>

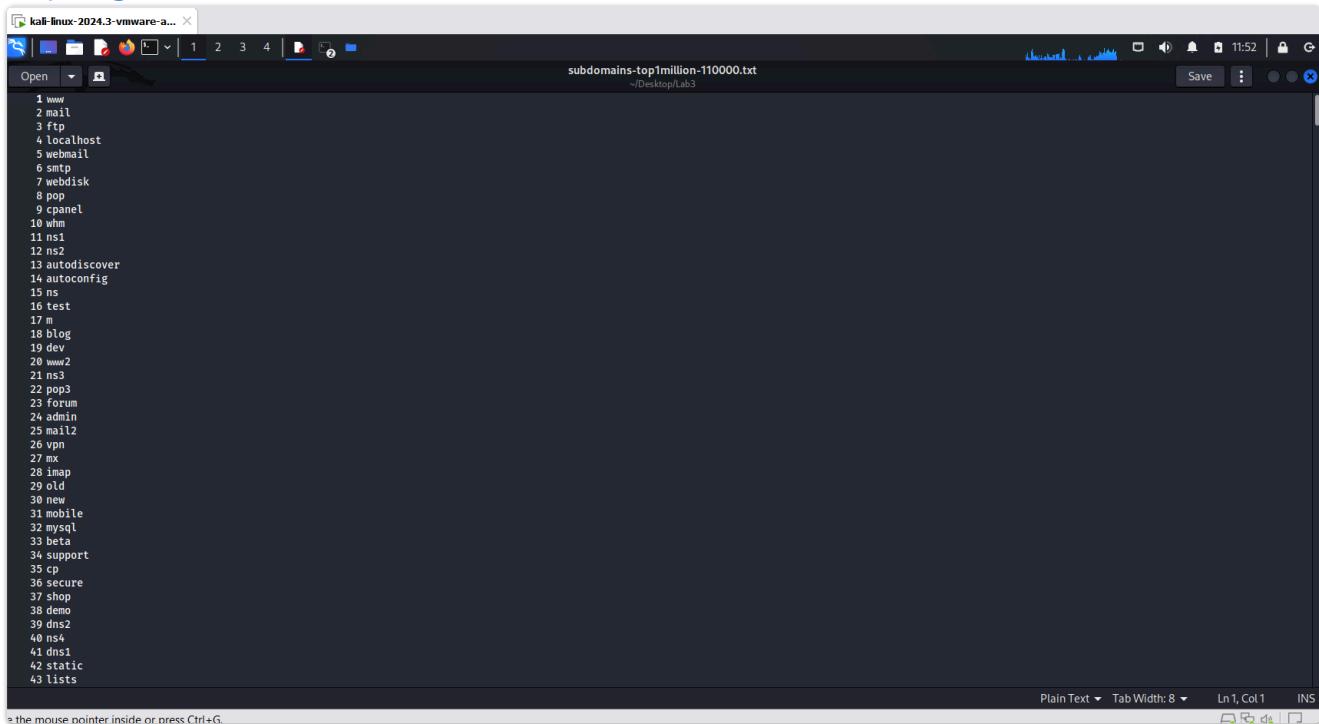
Đề bài

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

Các bước thực hiện

Tải file subdomains-top1million-110000.txt từ repository

<https://github.com/danielmiessler/SecLists>



```
1 www
2 mail
3 ftp
4 localhost
5 webmail
6 smtp
7 webdisk
8 pop
9 cpanel
10 whm
11 ns1
12 ns2
13 autodiscover
14 autoconfig
15 ns
16 test
17 m
18 blog
19 dev
20 www2
21 ns3
22 pop3
23 forum
24 admin
25 mail2
26 vpn
27 mx
28 imap
29 old
30 new
31 mobile
32 mysql
33 beta
34 support
35 cp
36 secure
37 shop
38 demo
39 dns2
40 ns4
41 dns1
42 static
43 lists
```

Chạy lệnh `gobuster vhost -u http://indriver.com -w subdomains-top1million-110000.txt --append-domain | grep "Status: 200"` không cho kết quả nào trả về status 200



```
kali㉿kali:[~/Desktop/Lab3]$ gobuster vhost -u http://indriver.com -w subdomains-top1million-110000.txt --append-domain | grep "Status: 200"
Progress: 114441 / 114442 (100.00%)
```

Bài tập 8

Link video: https://www.youtube.com/watch?v=amPMcHa_1Xg

Đề bài

Thực hiện scan 1000 port phổ biến trên các danh sách IP tìm được của *.indriver.com. Báo cáo kết quả tìm được trong file csv.

Các bước thực hiện

Ta thực hiện tải file `top-1000-most-popular-tcp-ports-nmap-sorted.csv` từ link github và tạo file domains.txt chỉ có subdomains từ file domains.csv ở câu 6

The screenshot shows three terminal windows on a Kali Linux system:

- Top Terminal:** Shows the command `ls` being run, listing files `domains.txt` and `top-1000-most-popular-tcp-ports-nmap-sorted.csv`.
- Middle Terminal:** Shows the command `cat top-1000-most-popular-tcp-ports-nmap-sorted.csv | sed 's/,/\n/' > domains.txt` being run to extract subdomains.
- Bottom Terminal:** Shows the contents of the `domains.txt` file, which lists numerous subdomains such as `apple.indriver.com`, `book.indriver.com`, etc.

Chạy script sau để scan port của các subdomains:

```
#!/bin/bash
```

```
# Đọc cổng từ tệp CSV và chuyển đổi chúng thành chuỗi cổng phân tách bằng dấu phẩy
```

```
port=$(tr '\n' ',' < top-1000-most-popular-tcp-ports-nmap-sorted.csv | sed 's/,$/\r/')
```

```
# Xuất header vào file CSV
```

```
if [ ! -f domain.csv ]; then
    echo "domain,port,state,service" > domain.csv
fi
```

```
# Đọc từng subdomain từ file domains.txt và quét từng subdomain với các
# port đã chỉ định
```

```

while IFS= read -r domain; do
    # Kiểm tra nếu dòng trong file không rỗng
    if [[ -n "$domain" ]]; then
        # Quét domain với nmap và xuất kết quả vào file CSV
        echo "Scanning subdomain: $domain"
        # Sử dụng lệnh nmap và định dạng lại kết quả để ghi vào CSV
        nmap -sS -T4 -p "$port" "$domain" | awk -v domain="$domain" '
        BEGIN {
            FS="[: /]";
            OFS=", "
        }
        /open/ {
            print domain, $1, $2, $3
        }' >> domain.csv
    fi
done < domains.txt

```

Chạy script

```

(kali㉿kali)-[~/Desktop/Lab3]
$ bash scan.sh
Scanning subdomain: apple.indriver.com
WARNING: Duplicate port number(s) specified. Are you alert enough to be using Nmap? Have some coffee or Jolt(tm).
Scanning subdomain: book.indriver.com
WARNING: Duplicate port number(s) specified. Are you alert enough to be using Nmap? Have some coffee or Jolt(tm).
Scanning subdomain: cargo.indriver.com
WARNING: Duplicate port number(s) specified. Are you alert enough to be using Nmap? Have some coffee or Jolt(tm).
Scanning subdomain: console.s3-kz.indriver.com
WARNING: Duplicate port number(s) specified. Are you alert enough to be using Nmap? Have some coffee or Jolt(tm).
Scanning subdomain: freight.indriver.com
WARNING: Duplicate port number(s) specified. Are you alert enough to be using Nmap? Have some coffee or Jolt(tm).
Scanning subdomain: job.indriver.com
WARNING: Duplicate port number(s) specified. Are you alert enough to be using Nmap? Have some coffee or Jolt(tm).
Scanning subdomain: injob.indriver.com
WARNING: Duplicate port number(s) specified. Are you alert enough to be using Nmap? Have some coffee or Jolt(tm).
Scanning subdomain: lena.indriver.com
WARNING: Duplicate port number(s) specified. Are you alert enough to be using Nmap? Have some coffee or Jolt(tm).
Failed to resolve "job.indriver.com".
WARNING: No targets were specified, so 0 hosts scanned.
Scanning subdomain: lena.indriver.com
WARNING: Duplicate port number(s) specified. Are you alert enough to be using Nmap? Have some coffee or Jolt(tm).
Failed to resolve "lena.indriver.com".
Scanning subdomain: injob.indriver.com
WARNING: Duplicate port number(s) specified. Are you alert enough to be using Nmap? Have some coffee or Jolt(tm).
Failed to resolve "injob.indriver.com".
WARNING: No targets were specified, so 0 hosts scanned.
Scanning subdomain: pagerduty.indriver.com
WARNING: Duplicate port number(s) specified. Are you alert enough to be using Nmap? Have some coffee or Jolt(tm).
Scanning subdomain: promo.indriver.com
WARNING: Duplicate port number(s) specified. Are you alert enough to be using Nmap? Have some coffee or Jolt(tm).
Failed to resolve "promo.indriver.com".
WARNING: No targets were specified, so 0 hosts scanned.
Scanning subdomain: redmine.indriver.com
WARNING: Duplicate port number(s) specified. Are you alert enough to be using Nmap? Have some coffee or Jolt(tm).
Failed to resolve "redmine.indriver.com".
WARNING: No targets were specified, so 0 hosts scanned.
Scanning subdomain: s3-kz.indriver.com
WARNING: Duplicate port number(s) specified. Are you alert enough to be using Nmap? Have some coffee or Jolt(tm).
Scanning subdomain: sharetrip.indriver.com
WARNING: Duplicate port number(s) specified. Are you alert enough to be using Nmap? Have some coffee or Jolt(tm).
Failed to resolve "sharetrip.indriver.com".
WARNING: No targets were specified, so 0 hosts scanned.
Scanning subdomain: sm.indriver.com
WARNING: Duplicate port number(s) specified. Are you alert enough to be using Nmap? Have some coffee or Jolt(tm).
Failed to resolve "sm.indriver.com".
WARNING: No targets were specified, so 0 hosts scanned.
Scanning subdomain: teammate.indriver.com
WARNING: Duplicate port number(s) specified. Are you alert enough to be using Nmap? Have some coffee or Jolt(tm).

```

File kết quả domain.csv

Open	Save
1 domain,port,state,service 2 apple.indriver.com,80,tcp, 3 apple.indriver.com,443,tcp,open 4 book.indriver.com,22,tcp, 5 book.indriver.com,80,tcp, 6 book.indriver.com,443,tcp, 7 cargo.indriver.com,80,tcp, 8 cargo.indriver.com,443,tcp,open 9 console.s3-kz.indriver.com,80,tcp,open 10 freight.indriver.com,80,tcp, 11 freight.indriver.com,443,tcp,open 12 ic.indriver.com,80,tcp, 13 ic.indriver.com,443,tcp,open 14 injob.indriver.com,80,tcp, 15 injob.indriver.com,443,tcp,open 16 pagerduty.indriver.com,80,tcp, 17 pagerduty.indriver.com,443,tcp,open 18 lena.indriver.com,80,tcp,open 19 share.indriver.com,80,tcp, 20 share.indriver.com,443,tcp, 21 share.indriver.com,8080,tcp,open 22 share.indriver.com,8443,tcp,open 23 teammate.indriver.com,80,tcp, 24 teammate.indriver.com,443,tcp, 25 url-checker.indriver.com,80,tcp, 26 url-checker.indriver.com,443,tcp,open	domain.csv ~/Desktop/Lab3

Bài tập 9

Link video: https://www.youtube.com/watch?v=xh_6kf-LtcY

Đề bài

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

Các bước thực hiện

Sử dụng công cụ wappalyzer ta lấy được version của Apache là 2.4.57

The screenshot shows the Wappalyzer interface. On the left is a screenshot of the website 'tuoitre.uit.edu.vn'. The website has a blue header with the logo 'Yuổi trẻ UIT' and navigation links like 'ĐIỂM TIN', 'BÁC HỒ', 'ĐOÀN THANH NIÊN', and 'HỘ SINH VIÊN'. Below the header is a banner with a group of people and the Vietnamese flag, with text about a charity event. On the right is the Wappalyzer analysis panel. It lists various technologies detected on the site:

- Technologies:** TECHNOLOGIES, MORE INFO, Export
- CMS:** Drupal 7
- Operating systems:** CentOS
- Analytics:** Google Analytics GA4
- Web server extensions:** OpenSSL 3.2.2
- Miscellaneous:** RSS
- Tag managers:** Google Tag Manager
- Web servers:** Apache HTTP Server 2.4.57
- JavaScript libraries:** Select2, jQuery 1.12.4
- Programming languages:**

Bài tập 10

Link video: https://www.youtube.com/watch?v=xh_6kf-LtcY

Đề bài

CMS nào được sử dụng của trang web tuoitre.uit.edu.vn

Các bước thực hiện

Sử dụng công cụ wappalyzer ta thấy rằng CMS là Drupal 7

The screenshot shows the homepage of the website tuoitre.uit.edu.vn. The main content features a photograph of a group of people, including children and adults, gathered around a table filled with various food items like Coca-Cola, Supe, and other packaged goods. In the background, there is a large portrait of Ho Chi Minh and a Vietnamese flag. The top navigation bar includes links for Home, Điểm tin (News), BÁC HỒ, ĐOÀN THANH NIÊN, HỘI SINH VIÊN, and others.

On the right side, the Wappalyzer analysis tool provides detailed information about the website's technologies:

- CMS:** Drupal 7
- Operating systems:** CentOS
- Analytics:** Google Analytics GA4
- Web server extensions:** OpenSSL 3.2.2
- Miscellaneous:** RSS
- Tag managers:** Google Tag Manager
- Web servers:** Apache HTTP Server 2.4.57
- JavaScript libraries:** Select2
- Programming languages:** jQuery 1.12.4

Bài tập 11

Link video: https://www.youtube.com/watch?v=xh_6kf-LtcY

Đề bài

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

Các bước thực hiện

Sử dụng công cụ wappalyzer ta thấy rằng OS là CentOS và webserver là Apache HTTP Server

The screenshot shows the homepage of the website tuoitre.uit.edu.vn. The main content features a photograph of a group of people, including children and adults, gathered around a table filled with various food items like Coca-Cola, Supe, and other packaged goods. In the background, there is a large portrait of Ho Chi Minh and a Vietnamese flag. The top navigation bar includes links for Home, Điểm tin (News), BÁC HỒ, ĐOÀN THANH NIÊN, HỘI SINH VIÊN, and others.

On the right side, the Wappalyzer analysis tool provides detailed information about the website's technologies:

- CMS:** Drupal 7
- Operating systems:** CentOS
- Analytics:** Google Analytics GA4
- Web server extensions:** OpenSSL 3.2.2
- Miscellaneous:** RSS
- Tag managers:** Google Tag Manager
- Web servers:** Apache HTTP Server 2.4.57
- JavaScript libraries:** Select2
- Programming languages:** jQuery 1.12.4

Bài tập 12

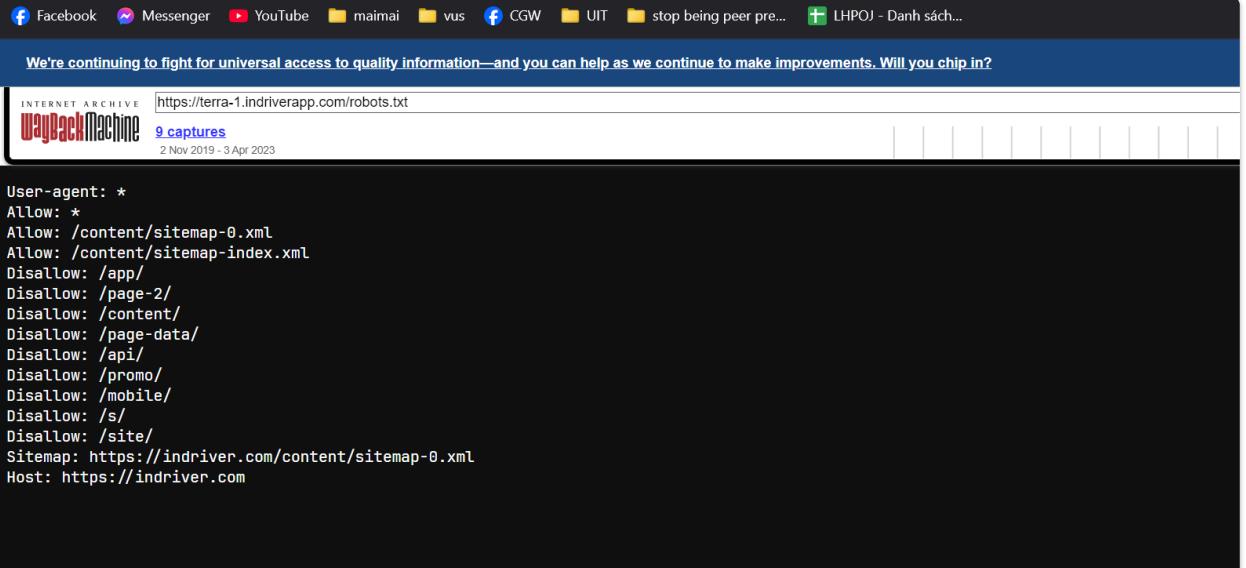
Link video: [link](#)

Đề bài

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

Các bước thực hiện

- Có thể tìm thấy các tên miền không còn tồn tại của trang web terra-1.indriverapp.com bằng [Internet Archiver](#) và chọn vào tab URLs.
- Có thể tìm thấy file <https://terra-1.indriverapp.com/robots.txt> bằng cách nhấn vào URL trong tab URLs



The screenshot shows a Wayback Machine page with the URL https://terra-1.indriverapp.com/robots.txt. The page content is as follows:

```
User-agent: *
Allow: *
Allow: /content/sitemap-0.xml
Allow: /content/sitemap-index.xml
Disallow: /app/
Disallow: /page-2/
Disallow: /content/
Disallow: /page-data/
Disallow: /api/
Disallow: /promo/
Disallow: /mobile/
Disallow: /s/
Disallow: /site/
Sitemap: https://indriver.com/content/sitemap-0.xml
Host: https://indriver.com
```

Bài tập 13

Link video: [link](#)

Đề bài

Tìm kiếm các tập tin pdf, excel, word, trên *.indriver.com.

Các bước thực hiện

Ta có thể dùng đoạn text sau để tìm kiếm

```
site:*.indriver.com filetype:pdf
site:*.indriver.com filetype:doc
site:*.indriver.com filetype:docx
site:*.indriver.com filetype:xls
site:*.indriver.com filetype:xlsx
```

Kết quả trả về

Google site:*.indriver.com (filetype:pdf OR filetype:xls OR filetype:xlsx C X

Tất cả Mua sắm Hình ảnh Video Sách Web Tin tức Thêm Công cụ

Không tìm thấy site:*.indriver.com (filetype:pdf OR filetype:xls OR filetype:xlsx OR filetype:doc OR filetype:docx) trong tài liệu nào.

Đề xuất:

- Xin bạn chắc chắn rằng tất cả các từ đều đúng chính tả.
- Hay thử những từ khóa khác.
- Hay thử những từ khóa chung hơn.
- Hay thử bỏ từ khóa.



Thử tìm kiếm với domain *.uit.edu.vn

Facebook Messenger YouTube maimai vus CGW UIT stop being peer pre... LHPOJ - Danh sách...

Google site:*.uit.edu.vn (filetype:pdf OR filetype:xls OR filetype:xlsx OR PDF)

Tất cả Mua sắm Hình ảnh Video Sách Web Tin tức Thêm Công cụ

 Trường Đại học Công nghệ Thông tin - UIT
<https://qlhc.uit.edu.vn> download PDF

ĐẠI HỌC QUỐC GIA TP.HCM
Căn cứ Quyết định số 867/QĐ-DHQG ngày 17/08/2016 của Giám đốc, ĐHQG-HCM về việc ban hành Quy chế tổ chức và hoạt động của Trường đại học.

 Trường Đại học Công nghệ Thông tin - UIT
<https://qlhc.uit.edu.vn> download PDF

đại học quốc gia thành phố hồ chí minh
31 thg 12, 2020 — CÔNG NGHỆ THU Về việc ban hành Quy định tổ chức, quản lý và sử dụng Hệ thống học liệu. Đại học Quốc gia Thành phố Hồ Chí Minh.

 Trường Đại học Công nghệ Thông tin - UIT
<https://qlhc.uit.edu.vn> download PDF

QUYETIIINH QUYET IIIINH:
HI-U TRƯONG TRUONG I>I HQC CONG NGH~ THONG TIN. Can cu Quy-t dinh s6 134/2006/QD-TTg ngay 08 thang 6 nam 2006 cua Thu tuong Chinh.

 Trường Đại học Công nghệ Thông tin - UIT
<https://qlhc.uit.edu.vn> download PDF

BCH ĐOÀN TỈNH ĐẮK NÔNG
cỗ vũ, khích lệ tinh thần phấn đấu, vươn lên trong học tập và trong các hoạt động phong trào Đoàn, Hội. Qua đó, thúc đẩy phong trào học tập và rèn luyện.,

 Trường Đại học Công nghệ Thông tin - UIT
<https://qlhc.uit.edu.vn> download PDF

ĐẠI HỌC QUỐC GIA TP.HCM TRUNG TÂM ĐÀO TẠO TIỀN ...
13 thg 2, 2015 — quý đơn vị hỗ trợ cho các ứng viên có đủ điều kiện cần thiết được tham gia dự tuyển đúng thời hạn quy định. Trần trọng. Nơi nhận:

Bài tập 14

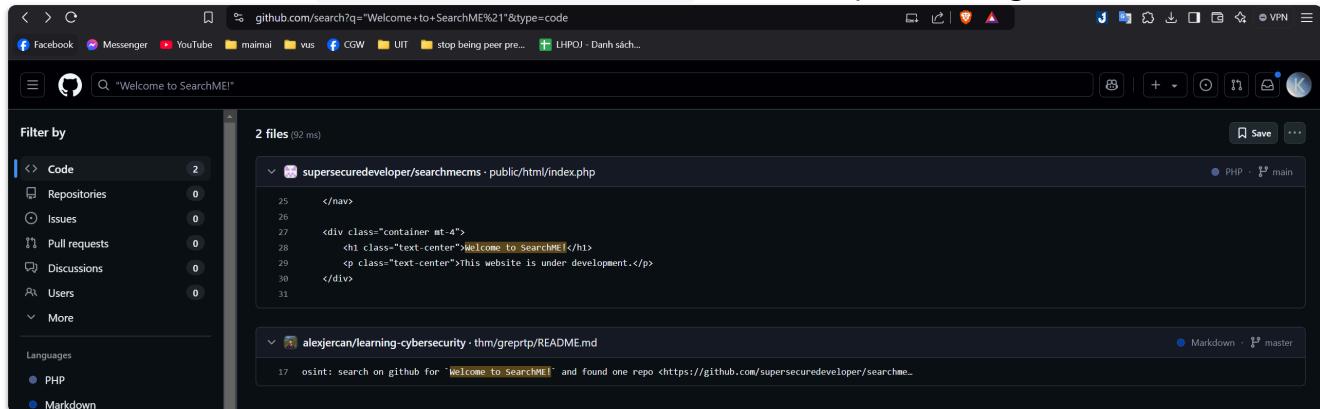
[Link video](#) [link](#)

Đề bài

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

Các bước thực hiện

Tìm kiếm với từ khóa "Welcome to SearchME!" , ta có kết quả là mã nguồn của web



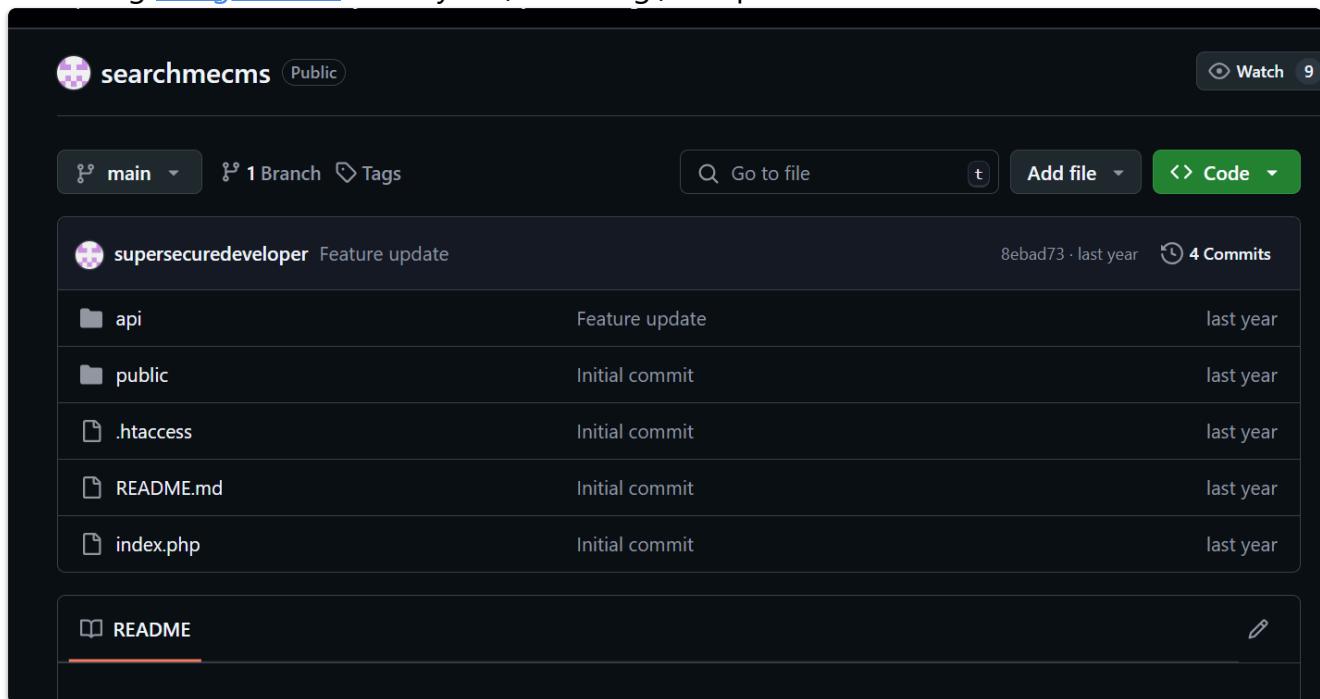
The screenshot shows a browser search results page for "Welcome to SearchME!". It displays two files found:

- supersecuredeveloper/searchmecms · public/html/index.php**:
Content of index.php:

```
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
```
- alexjercan/learning-cybersecurity · thm/greptp/README.md**:
Content of README.md:

```
17 osint: search on github for "Welcome to SearchME!" and found one repo <https://github.com/supersecuredeveloper/searchme...
```

Vào trong [trang GitHub](#), ta thấy được folder gọi là api



The screenshot shows the GitHub repository `searchmecms`. The `api` folder contains the following files:

- `index.php`: Feature update, last year
- `.htaccess`: Initial commit, last year
- `README.md`: Initial commit, last year
- `public`: Initial commit, last year

Vào folder apu vào xem mã nguồn của register.php

```
<?php
require_once 'config.php';
header('Content-Type: application/json');

$headers = apache_request_headers();

if (isset($headers['X-THM-API-Key']) && $headers['X-THM-API-Key'] ===
'TBA') {
    $input = json_decode(file_get_contents('php://input'), true);

    $stmt = $mysqli->prepare("INSERT INTO users (username, password,
```

```

email, name) VALUES (?, ?, ?, ?, ?)");
$stmt→bind_param("sssss", $input['username'],
password_hash($input['password'], PASSWORD_DEFAULT), $input['email'],
$input['name']);

if ($stmt→execute()) {
    echo json_encode(['message' => 'Registration successful.']);
} else {
    echo json_encode(['error' => 'Registration failed: ' . $stmt-
>error]);
}
$stmt→close();
} else {
    echo json_encode(array('error' => 'Invalid or Expired API key'));
}

?>

```

Ta thấy có dòng

```

if (isset($headers['X-THM-API-Key']) && $headers['X-THM-API-Key'] ===
'TBA')

```

Vậy api key là TBA

Bài tập 15

[Link video: link](#)

Đề bài

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.

Các bước thực hiện

Sử dụng `beautifulsoup` để tìm kiếm

```

import requests
from bs4 import BeautifulSoup, Comment
import re
from urllib.parse import urljoin
import json

url = 'https://indriver.com'

response = requests.get(url)

```

```

response.raise_for_status()

soup = BeautifulSoup(response.text, 'lxml')

emails = set(re.findall(r'[a-zA-Z0-9._%+-]+@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,}', response.text))

links = set()
for link in soup.find_all('a', href=True):
    full_url = urljoin(url, link['href'])
    links.add(full_url)

js_files = set()
for script in soup.find_all('script', src=True):
    js_url = urljoin(url, script['src'])
    js_files.add(js_url)

images = set()
for img in soup.find_all('img', src=True):
    img_url = urljoin(url, img['src'])
    images.add(img_url)

comments = [str(comment) for comment in soup.find_all(string=lambda text: isinstance(text, Comment))]

data = {
    "emails": list(emails),
    "links": list(links),
    "js_files": list(js_files),
    "images": list(images),
    "comments": comments
}

with open("output.json", "w", encoding="utf-8") as f:
    json.dump(data, f, ensure_ascii=False, indent=4)

print("Data has been saved to output.json")

```

```
{
  "emails": [
    "u003emarketing@indrive.com",
    "support@indriver.com",
    "marketing@indrive.com",
    "gr@indrive.com",
    "support@indrive.com",
    "u003egr@indrive.com",
    "u003esupport@indrive.com"
  ],
}
```

```
"links": [
    "https://indriver.com/vi-vn/blog",
    "https://indriver.com/vi-vn/legal",
    "https://indriver.com/vi-vn/driver",
    "https://indriver.com/vi-vn/book",
    "https://en.wikipedia.org/wiki/InDrive",
    "https://services.indrive.com/",
    "https://x.com/indrive",
    "https://indriver.com/vi-vn/company",
    "https://www.auroratechaward.com/",
    "https://indriver.com/vi-vn/fair-services",
    "https://alternativa.film/",
    "https://indriver.com/vi-vn/newsroom",
    "https://indriver.com/vi-vn/contacts",
    "https://www.facebook.com/indrive/",
    "https://indriver.com/vi-vn/sustainability",
    "https://underdogtechaward.com/",
    "https://movie.indrive.com/",
    "https://supernovas.indrive.com/en/home",
    "https://indriver.com/vi-vn/earn-courier",
    "https://couriers.indrive.com/",
    "https://beginit.indrive.com/",
    "https://indriver.com/vi-vn/delete-account",
    "https://indriver.com/vi-vn/offer",
    "https://indriver.com/vi-vn/intercity-rides",
    "https://indriver.com/vi-vn/safety",
    "https://indriver.com/vi-vn/intercity-driver",
    "https://indriver.com/vi-vn",
    "https://indriver.com/vi-vn/city-rides",
    "https://indriver.com/vi-vn/business",
    "https://indriver.com/vi-vn/earn-services",
    "https://ventures.indrive.com/",
    "https://www.instagram.com/indrive/",
    "https://indriver.com/vi-vn/invision",
    "https://indriver.com/vi-vn/freight-delivery",
    "https://careers.indrive.com/"
],
"js_files": [
    "https://indriver.com/_next/static/chunks/124-753c43ebf799764c.js",
    "https://indriver.com/_next/static/chunks/pages/index-fd7485b58dc7f26.js",
    "https://indriver.com/_next/static/chunks/polyfills-42372ed130431b0a.js",
    "https://indriver.com/_next/static/chunks/822-2b3dc504816a838f.js",
    "https://indriver.com/_next/static/05MgPxEu9Xdm6RQ2TY2yh/_ssgManifest.js",
    "https://indriver.com/_next/static/chunks/pages/_app-9a022731aa7a7917.js",

```



```
        "https://indriver.com/_next/image?  
url=%2Fimages%2Fpeople%2F4.png&w=3840&q=75",  
        "https://indriver.com/_next/image?  
url=%2Fimages%2Fservices%2Fservices.jpg&w=828&q=75",  
        "https://indriver.com/_next/image?  
url=%2Fimages%2Fvalues%2Fperformance.jpeg&w=3840&q=75",  
        "https://indriver.com/images/icons/arrow-right.svg",  
        "https://indriver.com/_next/image?  
url=%2Fimages%2Fvalues%2Fpeople.jpeg&w=3840&q=75",  
        "https://indriver.com/_next/image?  
url=%2Fimages%2Fimpact%2Fus%2Fl%2F5.png&w=3840&q=75",  
        "https://indriver.com/images/icons/close.svg",  
        "https://indriver.com/images/header/about-us.svg",  
        "https://indriver.com/images/book-section/layer.svg",  
        "https://indriver.com/_next/image?  
url=%2Fimages%2Fimpact%2Fus%2Fl%2F7.png&w=3840&q=75",  
        "https://indriver.com/images/icons/fb.svg",  
        "https://indriver.com/images/logo/logo--white.svg",  
        "https://indriver.com/images/icons/app-gallery.svg",  
        "https://indriver.com/_next/image?  
url=%2Fimages%2Fvalues%2Fpurpose.png&w=3840&q=75",  
        "https://indriver.com/images/logo/logo--dark.svg",  
        "https://indriver.com/images/icons/arrow.svg",  
        "https://indriver.com/_next/image?  
url=%2Fimages%2Fservices%2Fintercity.jpg&w=828&q=75",  
        "https://indriver.com/_next/image?  
url=%2Fimages%2Fservices%2Fcity.jpg&w=828&q=75",  
        "https://indriver.com/images/icons/circle-close.svg",  
        "https://indriver.com/images/header/fair-services.svg",  
        "https://indriver.com/_next/image?url=%2Fimages%2Fbook-  
section%2Fbook-bg-mobile.jpg&w=750&q=75",  
        "https://indriver.com/_next/image?  
url=%2Fimages%2Fimpact%2Fus%2Fl%2F4.png&w=3840&q=75",  
        "https://indriver.com/_next/image?  
url=%2Fimages%2Fimpact%2Fus%2Fl%2F3.png&w=3840&q=75",  
        "https://indriver.com/images/safety-section/safety.svg",  
        "https://indriver.com/_next/image?  
url=%2Fimages%2Fslides%2Fus%2Fl%2Fslide_3.jpg&w=3840&q=75",  
        "https://indriver.com/_next/image?  
url=%2Fimages%2Fservices%2Ffreight.jpg&w=828&q=75"  
    ],  
    "comments": [  
        "",  
        "",  
        "",  
        ""  
    ]  
}
```

Bài tập thực hành

Recon Royale

Kết quả

The screenshot shows the results of a Recon Royale challenge for the target domain `smule.com`. At the top, it displays the current target as `smule.com` with a timer indicating the time until the next round: `08:03:34`. Below this, the word "dead" is prominently displayed in white. The submission details are listed as follows:

- Your submission for this round:
- Valid subdomains: 467
- Invalid subdomains: 0
- Total points: 467

At the bottom, a message thanks the participant for participating and encourages them to see you next round!

Các bước thực hiện

Sử dụng [SecurityTrails](#)

Tryhackme - WebOSINT

Link video: [link](#)

Task 2

Sau khi tra [whois của trang web](#), ta có các thông tin mình cần

Whois results for republicofkoffee.com is available. Want it? Register now.

✓ **republicofkoffee.com** PREMIUM ⓘ

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 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: Kalkofnsvegur 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.internic.net/
>>> Last update of WHOIS database: 2024-11-17T22:17:55.05Z <<<
For more information on Whois status codes, please visit <https://icann.org/epp>

Answer the questions below

What is the name of the company the domain was registered with?

Namecheap Inc

✓ Correct Answer

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

9854014545

✓ Correct Answer

💡 Hint

What is the first nameserver listed for the site?

ns1.brainydns.com

✓ Correct Answer

What is listed for the name of the registrant?

redacted for privacy

✓ Correct Answer

What country is listed for the registrant?

Iceland

✓ Correct Answer

Task 3

Vào trong [Web Archiver của RepulicOfKoffee](#) và vào [bài viết này](#) ta sẽ có thông tin mình cần



CAFFE BONITO; MUDEUNGSAN

⌚ June 24, 2015 ⚖ Steve

On occasion I find myself having meetings in the Mudeungsan national park area of Gwangju. On these occasions, I typically set the meeting place as the Starbucks there. It has a small dedicated parking area and several floors of seating, including the rooftop, with gorgeous views of the surrounding area.

Đến thăm công viên khi tìm trên Google

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

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

✓ Correct Answer

Task 4

Vào [viewDNS](#) để tìm

69.64.147.10	United States	RIGHTSIDE	2017-07-30
173.248.188.152	United States	WEHOSTWEBSITES-COM	2016-10-03
173.248.187.2	United States	WEHOSTWEBSITES-COM	2016-02-01

Dùng tool Reverse IP Lookup để tìm hiểu IP này đang host các website nào

Reverse IP results for 173.248.188.152

=====

There are 72 domains hosted on this server.

The complete listing of these is below:

Domain	Last Resolved Date
acmx.com	2018-04-02
adventuratransport.com	2017-05-17
advisicon.com.mx	2017-11-01
animaenglish.org	2018-07-06
assaggiogourmet.com	2017-10-02
assistant-andrew.com	2017-05-31
assistat-daniel.com	2017-06-12
aztecaaceros.com	2017-06-17
bjj-tech.com	2024-11-17
bnbspacemanagement.com	2017-05-12
carrpropertymgmtnc.com	2017-06-01
coursesinlondon.org	2017-06-09
desayunovirtual.com	2017-01-02
drillcodemexico.mx	2017-08-09
drillcodemexico.net	2017-10-09
dumogtutors.com	2018-04-02
enphasesunshinecoast.com.au	2018-07-15
epix.mobi	2017-06-15
esgytsa.com	2018-06-01
farmmap.com.au	2016-10-16
fishingkayakreviews.co	2018-03-31
florackcolo.com	2017-05-17
freskosalon.com.mx	2017-10-11
gumaexpresscleaners.com	2017-06-01
hangitstraight.co.nz	2017-11-25
healthychanges.life	2017-10-24
hitchedwebservices.com	2017-05-04
homelabel.info	2017-10-10
hufhas.life	2017-10-24
hungrylizard.com.au	2018-07-01
iamliv.be	2017-10-10

Vậy là họ đang shared

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?

Correct Answer

Hint

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

Correct Answer

Hint

Task 5

Kiểm tra Whois

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



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: 2024-11-18T09:40:26Z <<<

Kiểm tra IP history

Viewdns.info

Tools API Research Data

[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	2024-11-17
74.116.2.147	United States	PERFORMIVE	2019-06-19
72.52.192.240	United States	LIQUIDWEB	2011-12-19

Kiểm tra reverse IP

Viewdns.info

Tools API Research Data

[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	2024-11-17
74.116.2.147	United States	PERFORMIVE	2019-06-19
72.52.192.240	United States	LIQUIDWEB	2011-12-19

Kiểm tra trên Internet Archive

ABOUT BLOG PROJECTS HELP DONATE CONTACT JOBS VOLUNTEER PEOPLE



Explore more than 916 billion web pages saved over time

DONATE

https://www.heat.net/

Calendar · Collections · Changes · Summary · Site Map · URLs

Saved 903 times between June 1, 1997 and October 7, 2024.



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 https://www.heat.net/ 903 captures 1 Jun 1997 - 7 Oct 2024

today's top story ::



ATTENTION ALL HEAT USERS:

After years of great fun, it's time to say good-bye. HEAT will be shutting its doors at the end of this month. It's a sad occasion for us, we had as much fun building HEAT as you had playing games here. We'd like to thank all our members for participating in a truly great gaming community.

But we don't want you to feel left out in the cold. We at Sega are still committed to delivering the best online gaming experience, and we encourage you to check out SegaNet.

SegaNet is the world's first online gaming network built and optimized for console and PC gaming. SegaNet gets you online and hooks you up to a nation of gamers. You'll get:

- A low-latency, high-speed, reliable Internet connection.
- 3D multi-player experience for Dreamcast or PC.
- Exclusive community: tournaments, rankings, and chat.
- Exclusive content and promotions.

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

Go | MAY JUN SEP 2000 2001 2002 About this capture

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?

http://www.heat.net/ 903 captures 1 Jun 1997 - 7 Oct 2024

Heat.net

Heating and Cooling, HVAC, Residential & Commercial Heat



Heating
 Ventilation
 Air Conditioning

Residential / Commercial

RATED #1 - Heating and Cooling (Nationwide)
Don't Get Left in the Cold! Get 3 Furnace Estimates Now!
Free Estimates - Next 48 Hours

CLICK HERE



CERTIFIED AC & HEATING 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

Tìm kiếm trên Google

heat.net play games online

Tất cả Hình ảnh Video Mua sắm Tin tức Sách Web : Thêm Công cụ

 heat.net
http://www.heat.net › games · Dịch trang này · :

Heat.net Online Gaming
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, as ...

 Sega Retro
https://segaretro.org › Heat · Dịch trang này · :

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, ...

 Wikipedia
https://en.wikipedia.org › wiki › Sega... · Dịch trang này · :

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.
History · Published games · Heat.net

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

Sử dụng đoạn code python để tìm

```
from bs4 import BeautifulSoup
import re
url = "http://www.heat.net/36/need-to-hire-a-commercial-heating-
contractor/"
def check(link):
    if link.startswith("http://www.heat.net") and link != url and not
```

```
link.endswith('.php') and not link.endswith('uncategorized/'):
    return True
return False
with open("task6.html", "r") as f:
    data = f.read()
soup = BeautifulSoup(data, 'html.parser')
#Google analytics code
ga_code = soup.find_all(string=re.compile("UA-"))
article = soup.find_all(id="post-36")
#find internal links
internal_links = []
for link in article[0].find_all('a', href=True):
    if check(link['href']) and link['href'] not in internal_links:
        internal_links.append(link['href'])

#find external links
external_links = []
for link in article[0].find_all('a', href=True):
    if not link['href'].startswith("http://www.heat.net"):
        external_links.append(link['href'])

print("Internal Links: ", len(internal_links))
print("External Links: ", len(external_links))
print("Domain of external link: ", external_links[0].split('/')[2])
print("Google Analytics Code: ", ga_code[0])
```

Internal Links: 5

External Links: 1

Domain of external link: www.purchase.org

Google Analytics Code:

window.google_analytics_uacct = "UA-251372-24";

Have at it!

Answer the questions below

How many internal links are in the text of the article?

5

✓ Correct Answer

✗ Hint

How many external links are in the text of the article?

1

✓ Correct Answer

✗ Hint

Website in the article's only external link (that isn't an ad)

purchase.org

✓ Correct Answer

Try to find the Google Analytics code linked to the site

UA-251372-24

✓ Correct Answer

Is the the Google Analytics code in use on another website? Yay or nay

nay

✓ Correct Answer

✗ Hint

Does the link to this website have any obvious affiliate codes embedded with it? Yay or Nay

Nay

✓ Correct Answer

✗ Hint

Task 7

IP history của purchase.org

IP Address	Location	Provider	Date
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

IP history của heat.net

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.

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

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	2024-11-18
74.116.2.147	United States	PERFORMIVE	2019-06-19
72.52.192.240	United States	LIQUIDWEB	2011-12-19

 Like  Share

Đều có LIQUIDWEB

Vào trang của [LIQUIDWEB](#) và nhìn vào tên công ty

© 2024 Liquid Web, LLC

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, heat[.]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