



МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ

СІКОРСЬКОГО»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра Інформаційної Безпеки

Технічний аудит

Лабораторна робота №1

Збір інформації, розвідка та OSINT

Перевішив:

Котов Д. О.

Виконав:

студент IV курсу

групи ФБ-01

Сахній Н. Р.

Приходько І. Ю.

Корабельський Т. Б.

Київ 2023

1. Отримання інформації про домен/IP за допомогою whois

Мета: зрозуміти яку інформацію надає утиліта whois

Після роботи студент повинен

- **знати:** як працює whois, які домени та IP-блоки делегуються клієнтам;
- **вміти:** отримувати всю інформацію від утиліти whois.

Завдання:

- зібрати інформацію про домен обраної компанії за допомогою команди whois,
- зібрати інформацію про домен обраної компанії за допомогою веб-послуги whois

ЗАВДАННЯ 1

Отримати всю інформацію про вибраний домен за допомогою команди whois (довести за допомогою знімка екрана). Коли зареєстрували / змінили домен? Хто є власником домену? Які відмінності між адміністративними, технічними та іншими контактами? Поясніть.

Відповідь:

- Інформація про обраний домен epicentrk.ua

```
(nazar@snz24)-[~]
$ whois epicentrk.ua --verbose
Using server whois.ua.
Query string: "epicentrk.ua"

% Request from 178.158.203.107
% This is the Ukrainian Whois query server #W.
% The Whois is subject to Terms of use
% See https://hostmaster.ua/services/
%
% IN THE PROCESS OF DELEGATION OF A DOMAIN NAME,
% THE REGISTRANT IS AN ENTITY WHO USES AND MANAGES A CERTAIN DOMAIN NAME,
% AND THE REGISTRAR IS A BUSINESS ENTITY THAT PROVIDES THE REGISTRANT
% WITH THE SERVICES NECESSARY FOR THE TECHNICAL MAINTENANCE OF THE REGISTRATION AND OPERATION OF THE DOMAIN NAME.
% FOR INFORMATION ABOUT THE REGISTRANT OF THE DOMAIN NAME, YOU SHOULD CONTACT THE REGISTRAR.

domain:          epicentrk.ua
dom-public:      NO
license:         198678
mnt-by:          ua.imena
nserver:         khloe.ns.cloudflare.com
nserver:         quinton.ns.cloudflare.com
status:          ok
created:         2015-05-06 12:48:04+03
modified:        2023-04-13 15:11:23+03
expires:         2024-05-06 12:48:04+03
source:          UAEPF
```

```
% Registrar:
%
% The following disclaimer was provided by the domain name registrar
% =====
% Надана інформація є неповною і може містити помилки, пов'язані з особливостями механізмів кешування інформації,
% та надається виключно для ознайомлення.
% У зв'язку із зазначеним вище, дана інформація не може бути використана з метою вирішення спорів, конфліктів, ви-
% Єдиним джерелом первинних даних про доменне ім'я є реєстратор (registrar) доменного імені, який може надати нео-
%
% The provided information is incomplete and may contain errors related to the specificity
% of information caching mechanisms, asynchronous updating of registries, etc.,
% therefore it is not reliable and is provided for informational purposes only.
% In connection with the above, this information can not be used to resolve disputes,
% conflicts, determine property and non-property rights, etc.
% The only source of primary data about the domain name is the registrar of the domain name,
% which can provide the required information upon request, in accordance with the procedure established by law.
% =====
registrar: ua.imena
organization: Internet Invest Ltd
organization-loc: ТОВ "Інтернет Інвест"
url: http://www.imena.ua
city: Kyiv
country: UA
abuse-email: abuse@imena.ua
abuse-phone: +380442010102
abuse-postal: 50-B Simi Prakhovykh St., Kyiv, 01033, Ukraine
abuse-postal-loc: вул. Сім'ї Прахових 50-Б, Київ, 01033, Україна
source: UAEPP
```

- Дата реєстрації, оновлення та термін дії домену

```
created: 2015-05-06 12:48:04+03
modified: 2023-04-13 15:11:23+03
expires: 2024-05-06 12:48:04+03
```

- Відмінності між контактами

- **Адміністративний контакт** (Administrative Contacts) – це особа, яка має право отримувати та відповідати на запити від реєстратора щодо домену, включаючи із можливістю зміни інформації про цей домен.
- **Технічний контакт** (Technical Contacts) – це особа або організація, яка зазвичай отримує інформацію про оновлення та інші технічні аспекти, пов'язані з функціонуванням домену або IP-адреси.

```
% Administrative Contacts:
% =====
person: n/a
person-loc: WEST OIL GROUP LLC
organization-loc: WEST OIL GROUP LLC
e-mail: olk@wog.ua
address: n/a
address-loc: 38 Kremenetska
address-loc: Lutsk
postal-code-loc: 43010
country-loc: UA
phone: +380.332200177
mnt-by: ua.imena
status: ok
status: linked
created: 2014-04-03 02:58:28+03
modified: 2015-08-07 13:04:42+03
source: UAEPP
```

```
% Technical Contacts:
% =====
person: n/a
person-loc: Олег Любомирович Кушіль
organization-loc: СП УКР-АНГ.ПІД-ВО "ЗАХІДНА НАФТОВА ГРУПА" У ФОРМІ ТЗОВ
e-mail: it_support@wog.ua
address: n/a
address-loc: 38 Kremenetska
address-loc: Lutsk
postal-code-loc: 43010
country-loc: UA
phone: +380.332200848
mnt-by: ua.imena
status: ok
status: linked
created: 2014-04-03 02:58:29+03
modified: 2015-08-07 13:04:39+03
source: Shadow UAEPP
```

Для прикладу, наведемо контактні дані, що відповідають компанії wog.ua

ЗАВДАННЯ 2

Отримати всю інформацію про вибраний домен за допомогою веб-служби who.is (довести за допомогою знімка екрана).

Відповідь:

Registrar Data

We will display stored WHOIS data for up to 30 days.

 Make Private Now

```
% Request from 102.165.52.7
% This is the Ukrainian Whois query server #5.
% The Whois is subject to Terms of use
% See https://hostmaster.ua/services/
%
% IN THE PROCESS OF DELEGATION OF A DOMAIN NAME,
% THE REGISTRANT IS AN ENTITY WHO USES AND MANAGES A CERTAIN DOMAIN NAME,
% AND THE REGISTRAR IS A BUSINESS ENTITY THAT PROVIDES THE REGISTRANT
% WITH THE SERVICES NECESSARY FOR THE TECHNICAL MAINTENANCE OF THE REGISTRATION AND OPERATION OF THE DOI
% FOR INFORMATION ABOUT THE REGISTRANT OF THE DOMAIN NAME, YOU SHOULD CONTACT THE REGISTRAR.
```

```
domain: epicentrk.ua
dom-public: NO
license: 198678
mnt-by: ua.imena
nserver: khloe.ns.cloudflare.com
nserver: quinton.ns.cloudflare.com
status: ok
created: 2015-05-06 12:48:04+03
modified: 2023-04-13 15:11:23+03
expires: 2024-05-06 12:48:04+03
source: UAEPP
```

.....

.....

ЗАВДАННЯ 3

Чи є відмінності між отриманими результатами?

Відповідь:

Отримані результати веб-ресурсу **who.is** та команди **whois** були майже ідентичні. Єдина відмінність, що веб-ресурс не виводить символи кирилиці.

abuse-email: abuse@imena.ua	Веб-ресурс who.is
abuse-phone: +380442010102	
abuse-postal: 50-B Simi Prakhovyykh St., Kyiv, 01033, Ukraine	
abuse-postal-loc: ???.'???' ??????? 50-?, ????, 01033, ???????	
source: UAEPF	

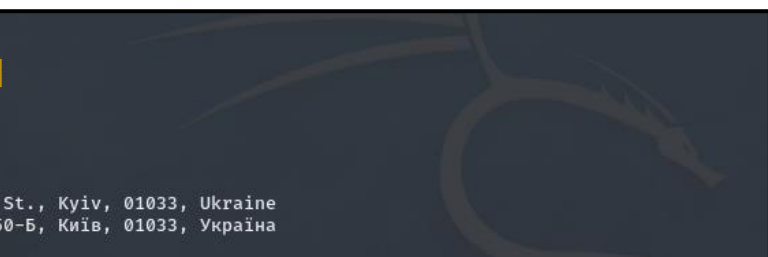
abuse-email: abuse@imena.ua	Команда whois
abuse-phone: +380442010102	
abuse-postal: 50-B Simi Prakhovyykh St., Kyiv, 01033, Ukraine	
abuse-postal-loc: вул. Сім'ї Прахових 50-Б, Київ, 01033, Україна	
source: UAEPF	

ЗАВДАННЯ 4

Що таке діапазон мережі? Хто є регіональним реєстратором? (довести за допомогою скріншотів)

Відповідь:

Діапазон мереж – це проміжок адрес, які належать домену.

registrar: ua.imena	
organization: Internet Invest Ltd	
organization-loc: ТОВ "Інтернет Інвест"	
url: http://www.imena.ua	
city: Kyiv	
country: UA	
abuse-email: abuse@imena.ua	
abuse-phone: +380442010102	
abuse-postal: 50-B Simi Prakhovyykh St., Kyiv, 01033, Ukraine	
abuse-postal-loc: вул. Сім'ї Прахових 50-Б, Київ, 01033, Україна	
source: UAEPF	

ЗАВДАННЯ 5

Що таке NS сервер?

Відповідь:

NS (Name Server, DNS) – це спеціалізований сервер в мережі Інтернет, призначені для перетворення доменних імен у відповідні числові IP-адреси та забезпечення правильної маршрутизації мережових запитів.

nserver: khloe.ns.cloudflare.com	NS (DNS) сервери для веб-ресурсу, що досліджується
nserver: quinton.ns.cloudflare.com	

2. Отримати загальну інформацію про вибраний домен за допомогою служби DNS

Мета: Зрозуміти основне призначення DNS

Після роботи студент повинен

- **знати:** як працює DNS, як працюють різні типи записів DNS;
- **вміти:** отримувати всю інформацію про доменні записи від служби DNS.

Завдання:

- отримати загальні записи DNS (A, AAAA, NS, MX, SPF, PTR) про домен, обраної компанії за допомогою команди dig,
- отримати загальні записи DNS (A, AAAA, NS, MX, SPF, PTR) про домен обраної компанії за допомогою веб-сервісів

Технічне оснащення робочого місця:

- командна консоль
 - команда dig
- веб-браузер
 - <https://bgp.he.net/>
 - <https://mxtoolbox.com/>

ЗАВДАННЯ 1

Отримайте всю інформацію про вибраний домен за допомогою команди dig (довести за допомогою знімка екрана). Які записи є доступними (MX/A/AAAA/NS)? На що вказують ці записи? Поясніть.

Відповідь:

```

(nazar@snz24)~$ dig epicentrk.ua

; <<>> DiG 9.19.17-1-Debian <<>> epicentrk.ua
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NXDOMAIN, id: 62736
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;epicentrk.ua.                IN      A

;; AUTHORITY SECTION:
ua.                3287    IN      SOA     in1.ns.ua. domain-master.ccTLD.ua. 2023092707 3636 1212 3024000 3535

;; Query time: 8 msec
;; SERVER: 192.168.50.1#53(192.168.50.1) (UDP)
;; WHEN: Wed Sep 27 16:29:06 EEST 2023
;; MSG SIZE rcvd: 103

```

На наступному фото ми можемо побачити, що доступні всі перераховані записи (MX/A/AAAA/NS). Одразу запишемо для чого вони потрібні.

```

(nazar@snz24)~$ dig epicentrk.ua MX +short
10 email.epicentrk.ua.

(nazar@snz24)~$ dig epicentrk.ua A +short
104.20.124.68
104.20.125.68

(nazar@snz24)~$ dig epicentrk.ua AAAA +short
2606:4700:10::6814:7d44
2606:4700:10::6814:7c44

(nazar@snz24)~$ dig epicentrk.ua NS +short
khloe.ns.cloudflare.com.
quinton.ns.cloudflare.com.

```

DNS-записи (MX, A, AAAA, NS) вказують на різні типи інформації про домен, яка зберігається в системі DNS (Domain Name System).

1. MX (Mail Exchange) записи:

- MX-записи вказують на поштові сервери, які відповідають за прийом електронної пошти для даного домену. Для цього, кожен MX-запис містить пріоритет (число) та доменне ім'я відповідного поштового сервера.

2. A (Address) записи:

- A-записи використовуються для перетворення доменного імені на відповідну IPv4-адресу.

3. AAAA (IPv6 Address) записи:

- AAAA-записи використовуються для перетворення доменного імені на відповідну IPv6-адресу.

4. NS (Name Server) записи:

- NS-записи використовуються для визначення того, які DNS-сервери слід опитувати, щоб отримати інші DNS-записи для цього домену.

Ці записи допомагають організувати та оптимізувати роботу мережі Інтернету, забезпечуючи правильну адресацію пошти, маршрутизацію мережевого трафіку і відповідність доменних імен числовим IP-адресам.

ЗАВДАННЯ 2

Отримати записи PTR, для отриманих IP-адрес, із записів NS/MX/A (не більше 5) (довести за допомогою знімка екрана). Чим вони відрізняються від запису A? Поясніть.

Відповідь:

```
(nazar@snz24)-[~]
$ nslookup epicentrk.ua
Server:      192.168.50.1
Address:     192.168.50.1#53

Non-authoritative answer:
Name:   epicentrk.ua
Address: 104.20.124.68
Name:   epicentrk.ua
Address: 104.20.125.68
Name:   epicentrk.ua
Address: 2606:4700:10::6814:7d44
Name:   epicentrk.ua
Address: 2606:4700:10::6814:7c44
```

```
(nazar@snz24)-[~]
$ dig epicentrk.ua A

;<<>> DiG 9.19.17-1-Debian <<>> epicentrk.ua A
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 25261
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;epicentrk.ua.                IN      A
;; ANSWER SECTION:
epicentrk.ua.                47      IN      A      104.20.124.68
epicentrk.ua.                47      IN      A      104.20.125.68

;; Query time: 8 msec
;; SERVER: 192.168.50.1#53(192.168.50.1) (UDP)
;; WHEN: Wed Sep 27 17:47:45 EEST 2023
;; MSG SIZE rcvd: 73
```



```
(nazar@snz24)-[~]
$ dig 104.20.124.68 PTR

; <<> DiG 9.19.17-1-Debian <<> 104.20.124.68 PTR
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NXDOMAIN, id: 48429
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;104.20.124.68.                IN      PTR

;; AUTHORITY SECTION:
.                1929    IN      SOA      a.root-servers.net. nstld.verisign-grs.com. 2023092700 1800 900 604800 86400

;; Query time: 12 msec
;; SERVER: 192.168.50.1#53(192.168.50.1) (UDP)
;; WHEN: Wed Sep 27 17:48:00 EEST 2023
;; MSG SIZE rcvd: 117
```

Запис **A** вказує на доменне ім'я для заданої IP-адреси, у свою чергу **PTR** вказує обернену адресацію, перетворюючи IP-адресу на доменне ім'я.

ЗАВДАННЯ 3

Перевірити записи SPF вибраного домену/субдомену за допомогою MxToolbox (довести за допомогою знімка екрана)? Поясніть результати.

Відповідь:

spf:epicentrk.ua

Find Problems

Solve Email Delivery Problems

spf

X

EMAILS BOUNCING? MxToolbox has your email delivery solutions

v=spf1 +a +mx ip4:194.183.174.42 ip4:46.201.88.236 ip4:79.137.70.68 -all

Prefix	Type	Value	PrefixDesc	Description
	v	spf1		The SPF record version
+	a		Pass	Match if IP has a DNS 'A' record in given domain.
+	mx		Pass	Match if IP is one of the MX hosts for given domain name.
+	ip4	194.183.174.42	Pass	Match if IP is in the given range.
+	ip4	46.201.88.236	Pass	Match if IP is in the given range.
+	ip4	79.137.70.68	Pass	Match if IP is in the given range.
-	all		Fail	Always matches. It goes at the end of your record.

	Test	Result
✓	SPF Record Published	SPF Record found
✓	SPF Record Deprecated	No deprecated records found
✓	SPF Multiple Records	Less than two records found
✓	SPF Contains characters after ALL	No items after 'ALL'.
✓	SPF Syntax Check	The record is valid
✓	SPF Included Lookups	Number of included lookups is OK
✓	SPF Type PTR Check	No type PTR found
✓	SPF Void Lookups	Number of void lookups is OK
✓	SPF MX Resource Records	Number of MX Resource Records is OK
✓	SPF Record Null Value	No Null DNS Lookups found

Бачимо, що всі тестування пройдено успішно. У цілому даний SPF-запис вказує, що валідні IP-адреси для надсилання пошти від імені домену "epicentrk.ua" включають DNS A-записи, MX-хости та конкретні IP-адреси, вказані у діапазонах. Проте, важливо врахувати, що SPF перевірка завершиться неуспішно для будь-яких інших IP, оскільки вказано "-all".

ЗАВДАННЯ 4

Чи є інформація про AS компанії? (довести за допомогою скріншотів). Що це означає?

Відповідь:

a:epicentrk.ua Find Problems ↻ a			
Type	Domain Name	IP Address	TTL
A	epicentrk.ua	104.20.124.68 <small>Unknown (AS13335)</small>	5 min
A	epicentrk.ua	104.20.125.68 <small>Unknown (AS13335)</small>	5 min
Test		Result	
✓ DNS Record Published		DNS Record found	

ASN: 13335	
Source Registry	ARIN
Number	13335
Name	CLOUDFLARENET
Handle	AS13335
Registration	Wed, 14 Jul 2010 22:35:57 GMT (Thu Jul 15 2010 local time)
Last Changed	Fri, 17 Feb 2017 23:04:32 GMT (Sat Feb 18 2017 local time)
Self	https://rdap.arin.net/registry/autnum/13335
Alternate	https://whois.arin.net/rest/asn/AS13335
Comments	All Cloudflare abuse reporting can be done via https://www.cloudflare.com/abuse
Port 43 Whois	whois.arin.net

AS13335 є автономною системою (Autonomous System, AS) в Інтернеті, і це присвоєний номер (AS-номер), який ідентифікує окремий блок IP-адрес в мережі Інтернет. У цьому випадку AS13335 (CLOUDFLARENET) є AS-номером, який належить компанії "Cloudflare, Inc".

3. Отримати загальну інформацію про цільову AS

Мета: Зрозуміти призначення протоколу BGP

Після роботи студент повинен

- **знати:** що таке AS, як AS передає трафік;
- **вміти:** отримати інформацію, пов'язану з AS (номер, підблоки, з'єднання, маршрути).

Завдання:

- отримати AS інформацію про цільову компанію за допомогою <https://bgp.he.net/>,
- отримати зміни в маршрутизації BGP до вибраної AS

Технічне оснащення робочого місця:

- командна консоль
 - команда traceroute
- веб-браузер
 - <https://bgp.he.net/>
 - <http://www.routeviews.org/routeviews/>
 - <https://stat.ripe.net/widget/bgplay>

ЗАВДАННЯ 1


Отримати всю інформацію про AS за допомогою bgp.he.net (довести за допомогою знімка екрана). Що таке номер AS? Які підблоки делеговані даній AS?

Відповідь:

Кожен **AS номер** визначає конкретну мережу або групу мереж, які мають спільну політику маршрутизації. Коли мережі входять до складу однієї автономної системи, вони взаємодіють між собою на основі цієї політики.

AS номери можуть бути розподілені на підблоки, які називаються префіксами. Префікси представляють собою блоки IP-адрес, які контролюються конкретною автономною системою. Ці префікси вказують, які конкретні ділянки IP-адрес призначені для цієї автономної системи.

Отже, на фото нижче наведемо підблоки, делеговані даний AS13335.

**HURRICANE ELECTRIC**
INTERNET SERVICES

AS13335 Cloudflare, Inc.

Quick Links
[BGP Toolkit Home](#)
[BGP Prefix Report](#)
[BGP Peer Report](#)
[Exchange Report](#)
[Bogon Routes](#)
[World Report](#)
[Multi Origin Routes](#)
[DNS Report](#)
[Top Host Report](#)
[Internet Statistics](#)
[Looking Glass](#)
[Network Tools App](#)
[Free IPv6 Tunnel](#)
[IPv6 Certification](#)
[IPv6 Progress](#)
[Going Native](#)
[Contact Us](#)

AS Info

Graph v4

Graph v6

Prefixes v4

Prefixes v6

Peers v4


Peers v6


Whois

IRR


IX































Company Website:
Country of Origin:
Internet Exchanges: 304
Prefixes Originated (all): 3,482
Prefixes Originated (v4): 1,966
Prefixes Originated (v6): 1,516
Prefixes Announced (all): 5,723
Prefixes Announced (v4): 4,207
Prefixes Announced (v6): 1,516
RPKI Originated Valid (all): 3,275
RPKI Originated Valid (v4): 1,764
RPKI Originated Valid (v6): 1,511
RPKI Originated Invalid (all): 7
RPKI Originated Invalid (v4): 6
RPKI Originated Invalid (v6): 1
BGP Peers Observed (all): 1,391
BGP Peers Observed (v4): 1,351
BGP Peers Observed (v6): 661
IPs Originated (v4): 1,693,696
AS Paths Observed (v4): 115,939
AS Paths Observed (v6): 96,757
Average AS Path Length (all): 4.857
Average AS Path Length (v4): 4.899
Average AS Path Length (v6): 4.808

<https://www.cloudflare.com>
United States




Security, reliability and speed everywhere
...powered by an intelligent global network




104.20.96.0/20	 	Cloudflare, Inc.	
104.20.112.0/20	 	Cloudflare, Inc.	
104.20.128.0/20	 	Cloudflare, Inc.	
104.20.144.0/20	 	Cloudflare, Inc.	
104.20.160.0/20	 	Cloudflare, Inc.	
104.20.176.0/20	 	Cloudflare, Inc.	
104.20.192.0/20	 	Cloudflare, Inc.	
104.20.208.0/20	 	Cloudflare, Inc.	
104.20.224.0/20	 	Cloudflare, Inc.	
104.20.240.0/20	 	Cloudflare, Inc.	

ЗАВДАННЯ 2

Чи якісь інші AS оголошують той самий підблок? Це правильно?



Відповідь:




HURRICANE ELECTRIC
INTERNET SERVICES

[104.20.112.0/20](#)

Quick Links
[BGP Toolkit Home](#)
[BGP Prefix Report](#)
[BGP Peer Report](#)
[Exchange Report](#)
[Bogon Routes](#)
[World Report](#)
[Multi Origin Routes](#)
[DNS Report](#)
[Top Host Report](#)
[Internet Statistics](#)
[Looking Glass](#)
[Network Tools App](#)
[Free IPv6 Tunnel](#)
[IPv6 Certification](#)
[IPv6 Progress](#)
[Going Native](#)
[Contact Us](#)

Network Info

Announced By		
Origin AS	Announcement	Description
AS13335	104.20.112.0/20  	Cloudflare, Inc.

Less Specific Announcements		
Origin AS	Announcement	Description
AS13335	104.16.0.0/12 	Cloudflare, Inc.
AS137554	104.16.0.0/12 	Cloudflare, Inc.

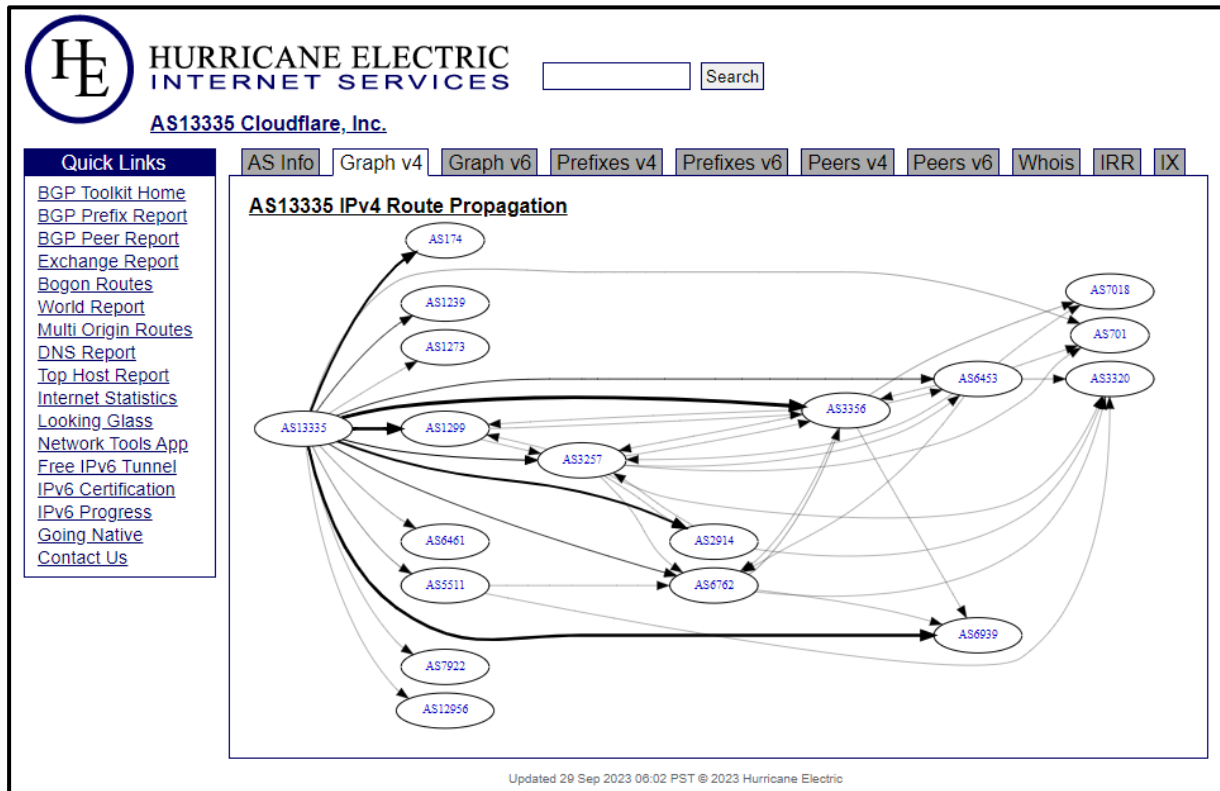
Updated 30 Sep 2023 05:17 PST © 2023 Hurricane Electric

Дійсно, іноді може статися ситуація, коли кілька різних автономних систем (AS) оголошують той самий IP-підблок. Це може бути результатом різних сценаріїв, іноді навмисно, іноді навіть не навмисно, і це може мати різні наслідки, як неправильна маршрутизація та можливий витік даних.

ЗАВДАННЯ 3

Скільки з'єднань має поточна AS? (довести за допомогою скріншота).

Відповідь:



ЗАВДАННЯ 4

Який основний шлях між цільовою AS та вами? Доведіть це за допомогою команди traceroute та знімка екрана та результату аналізу відносин IP-AS.

Відповідь:

```
(nazar@snz24)~$ traceroute epicentrk.ua
traceroute to epicentrk.ua (104.20.124.68), 30 hops max, 60 byte packets
 1  RT-AX55-0590 (192.168.50.1)  4.544 ms  4.077 ms  3.725 ms
 2  94.158.81.1 (94.158.81.1)  5.760 ms  5.539 ms  5.302 ms
 3  10.255.254.15 (10.255.254.15)  5.878 ms  5.665 ms  7.088 ms
 4  10.255.254.12 (10.255.254.12)  9.250 ms  9.039 ms  8.818 ms
 5  * * *
 6  10.255.249.1 (10.255.249.1)  6.209 ms  5.993 ms  5.269 ms
 7  * * cloudflare.1-ix.net (185.1.254.19)  36.252 ms
 8  104.20.124.68 (104.20.124.68)  5.737 ms  5.536 ms  5.323 ms
```

Traceroute from my Kali: Laptop > Router > Maximum NET (Vyshneve, Ukraine) > IXP-1-IX-EU (Warsaw, Poland) > Cloudflare, Inc (Епіцентр К)

The screenshot shows the Hurricane Electric Internet Services website. The main content area displays the "AS13335 Cloudflare, Inc." table. The table has the following columns: Exchange, CC, City, IPv4, and IPv6.

Exchange	CC	City	IPv4	IPv6
1-IX Internet Exchange	UA	Kyiv	185.1.213.92	2001:7f8:115:92
1-IX Warsaw	PL	Warsaw	185.1.254.19	2001:7f8:115:1::19

4. OSINT з Shodan

Мета: зрозуміти призначення Shodan

Після роботи студент повинен

- **знати:** як працює сервіс Shodan;

Завдання:

- підтвердити, вказати та розширити інформацію з попередніх кроків за допомогою сервісу Shodan

Технічне оснащення робочого місця:

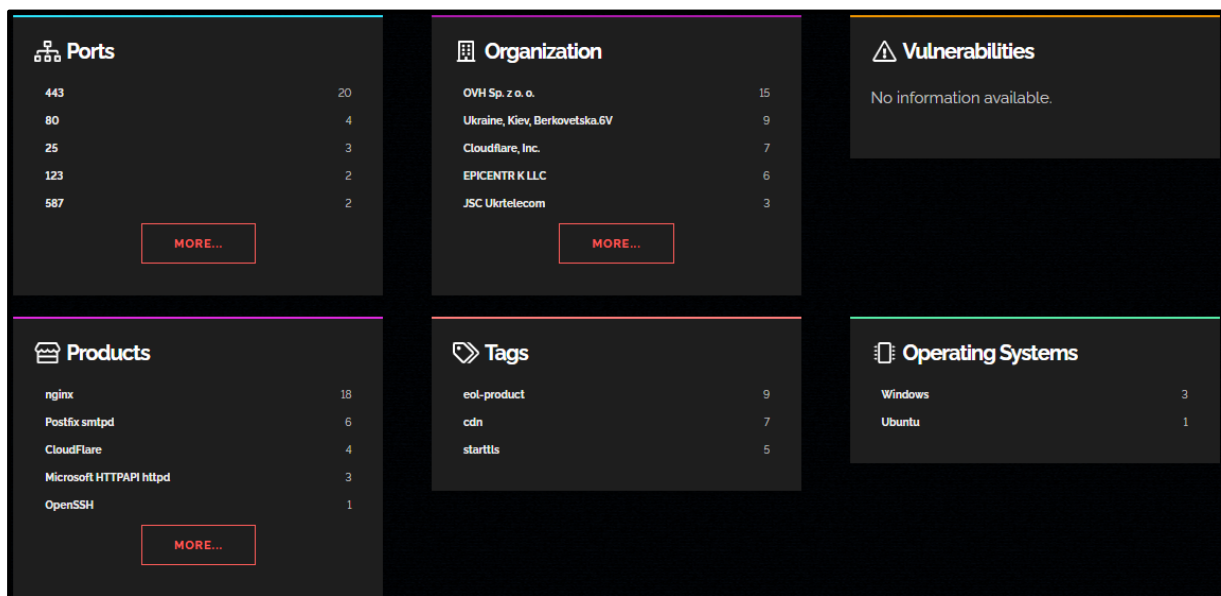
- командна консоль
 - команда traceroute
- веб-браузер
 - [https://www.shodan.io /](https://www.shodan.io/)

ЗАВДАННЯ 1

Яку інформацію ви змогли отримати з Shodan? (довести за допомогою скріншотів).

Відповідь:



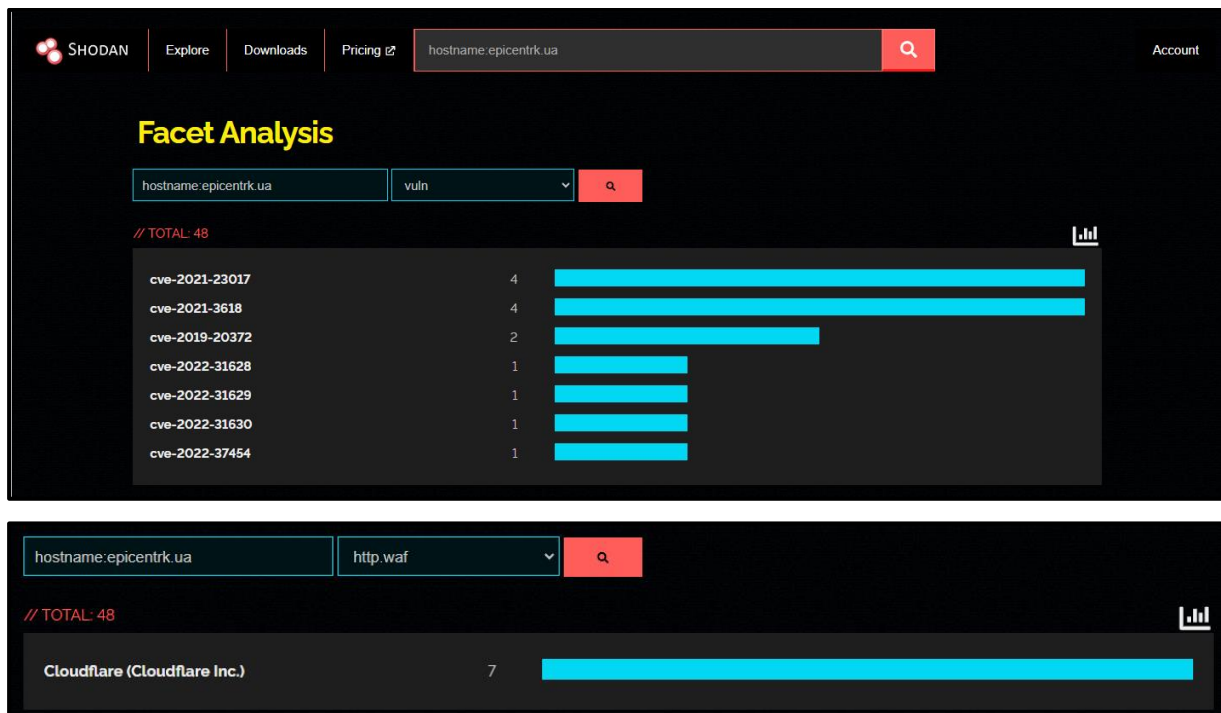


ЗАВДАННЯ 2

Чи є додаткова інформація про досліджувану ціль?

Відповідь:

Shodan дозволив зібрати дані про відкриті порти, веб-технології, вразливості, ОС та програмне забезпечення, яке використовує компанія.



5. Автоматизація OSINT за допомогою Maltego та FOCA

Мета: зрозуміти можливості Maltego

Після роботи студент повинен

- **знати:** як працює Maltego;
- **знати:** як працює Foca.

Завдання:

- отримати всю інформацію з попередніх кроків використавши Maltego
- отримати метадані за допомогою програми Foca

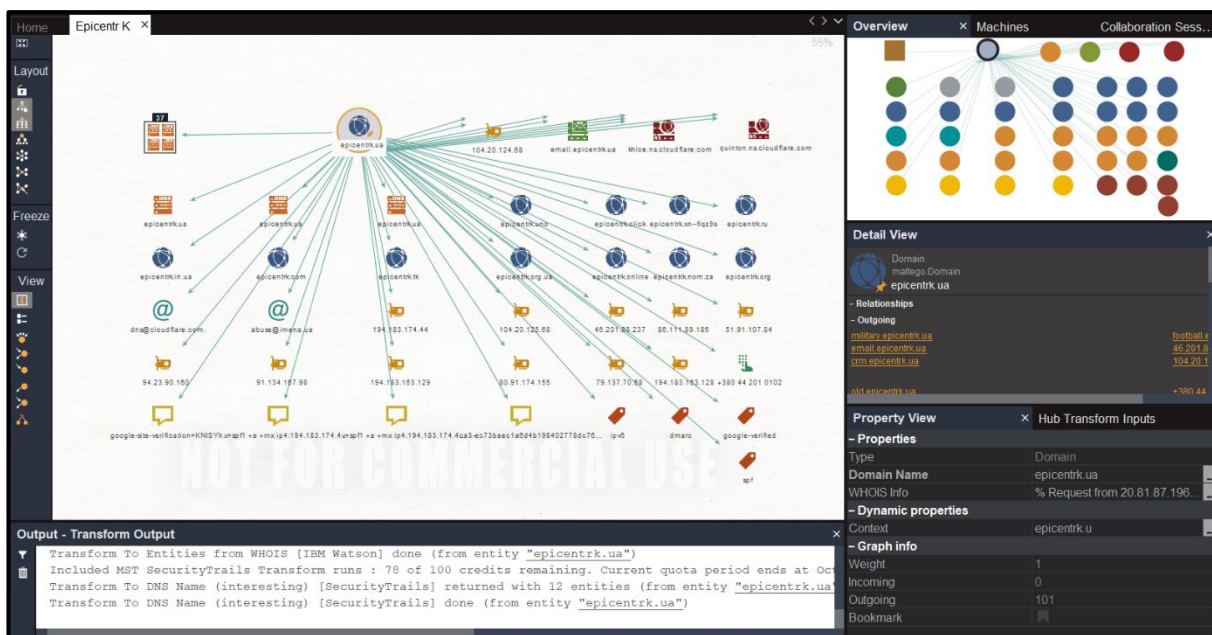
Технічне оснащення робочого місця:

- Maltego
- Foca

ЗАВДАННЯ 1

Яку інформацію ви змогли отримати за допомогою Maltego? (довести за допомогою скріншотів).

Відповідь:



На основі аналізу домену "epicentrk.ua" в Maltego ми змогли отримати структуру веб-сайту та пов'язані об'єкти. Це включає поштові адреси, IP-адреси, DNS-сервери, MX-записи та, можливо, номери телефонів.

ЗАВДАННЯ 2

Чи є відмінності від автоматизованого та ручного збору даних? (довести за допомогою скріншотів) Поясніть.

Відповідь:

Наведемо відмінності між автоматизованим та ручним збором даних, які стосуються процесу та якості зібраних даних:

➤ Щодо самого процесу збору:

- *Автоматизований збір:* Використовуючи програми та скрипти, дані збираються автоматично з визначених джерел та ресурсів відповідно до певних параметрів. Процес відбувається швидше та безпомилково.
- *Ручний збір:* Дані збираються вручну або напівавтоматично, що може бути часо- та працезатратним, особливо для великих обсягів даних.

➤ Обсяг та швидкість:

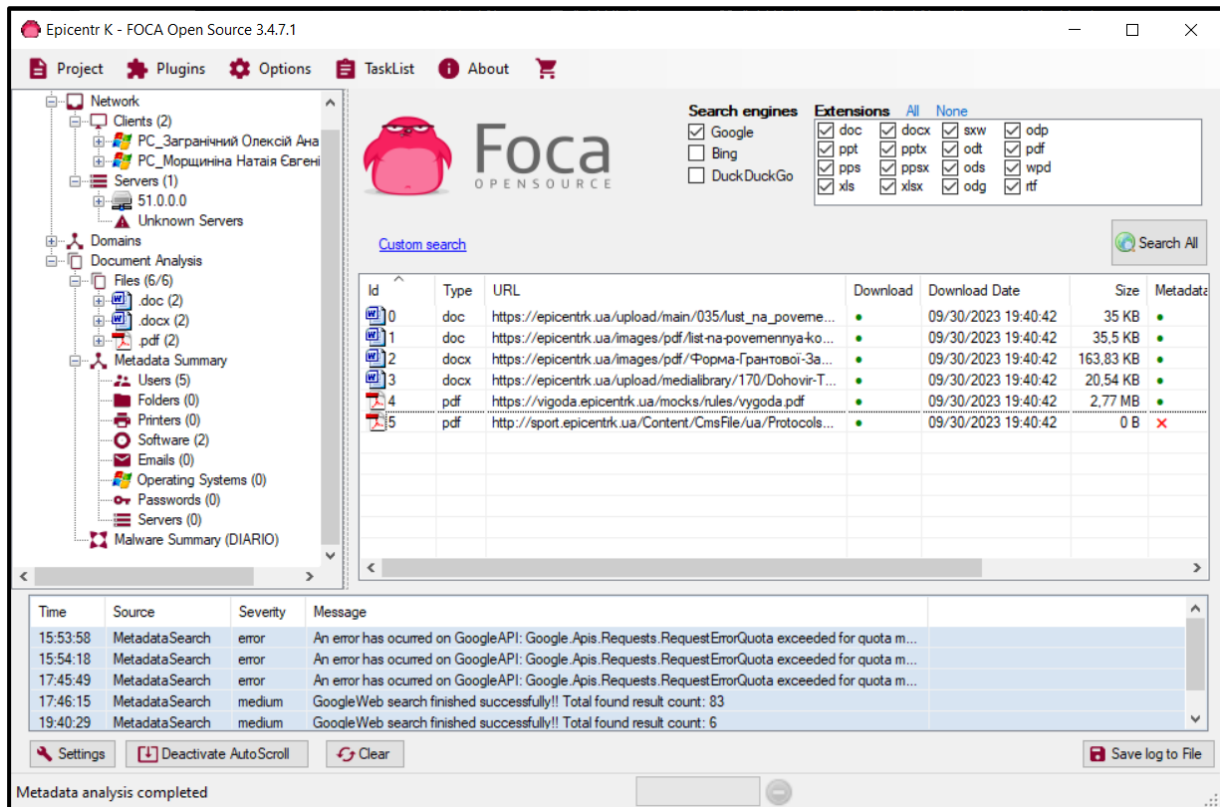
- *Автоматизований збір:* Дозволяє зібрати великий обсяг даних швидше, що особливо важливо для широкого аналізу.
- *Ручний збір:* Обмежений обсягом, який може бути зібраний вручну або напівавтоматично.

Загалом, автоматизований збір даних спрощує та прискорює процес, але може вимагати уваги до якості та точності даних. Ручний збір, хоча й часо- та працезатратний, може забезпечити вищу точність та надійність даних. **Оптимальний підхід полягає у комбінації обох методів** відповідно до завдань та потреб конкретного аналізу.

ЗАВДАННЯ 3

Завантажити та видобути метадані з файлів, отриманих із цільового домену/субдоменів компанії за допомогою FOCA? (довести за допомогою скріншотів) Поясніть.

Відповідь:

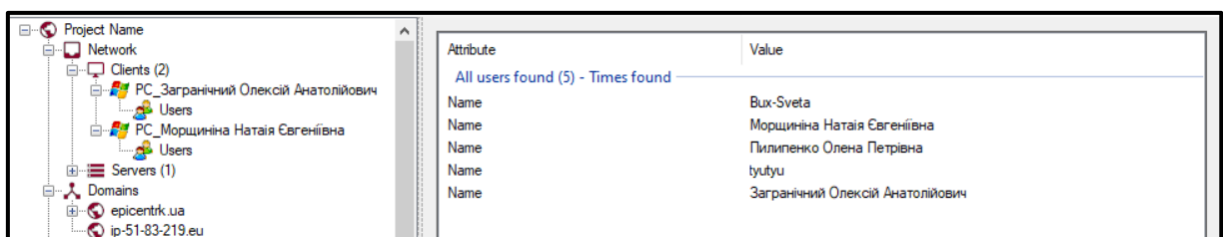


ЗАВДАННЯ 4

Чи є якісь імена користувачів / електронні листи? (довести за допомогою скріншотів).

Відповідь:

Для компанії “Епіцентр К” не так вже й багато вдалось знайти цікавої інформації із метаданих, так як FOCA знайшов лише близько 5-и файлів. Тому на наступному фото продемонструємо хоча б ПІБ деяких працівників.



6. Перевірка облікових даних за допомогою Pastebin та Haveibeenpwned

Мета: зрозуміти що таке OSINT

Після роботи студент повинен

- **знати:** як перевірити облікові дані в загальнодоступних базах даних.

Завдання:

- перевірити всі облікові дані з попередніх кроків із наданих ресурсів

Технічне оснащення робочого місця:

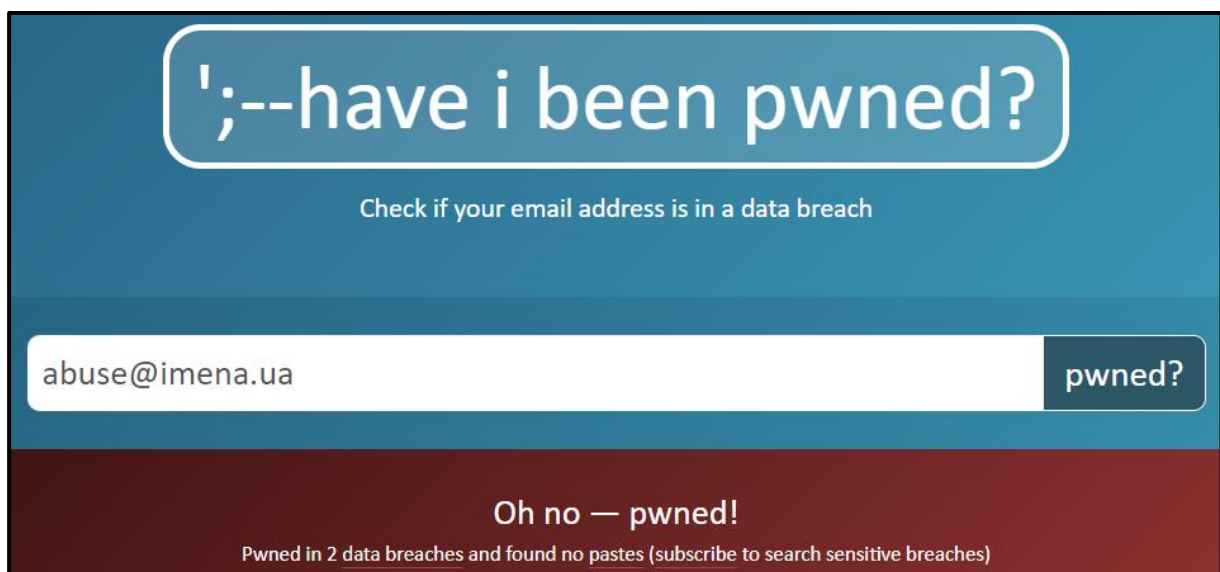
- <https://haveibeenpwned.com/>
- <https://pastebin.com/>

ЗАВДАННЯ 1

Перевірити електронні скриньки за допомогою сервісу Haveibeenpwned?
(надайте результати за допомогою скріншотів) Щось цікаве?

Відповідь:

➤ `abuse@imena.ua`



Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the [1Password password manager](#) helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.



Epik: In September 2021, the domain registrar and web host Epik suffered a significant data breach, allegedly in retaliation for hosting alt-right websites. The breach exposed a huge volume of data not just of Epik customers, but also scraped WHOIS records belonging to individuals and organisations who were not Epik customers. The data included over 15 million unique email addresses (including anonymised versions for domain privacy), names, phone numbers, physical addresses, purchases and passwords stored in various formats.

Compromised data: Email addresses, Names, Phone numbers, Physical addresses, Purchases



Eye4Fraud: In February 2023, data alleged to have been taken from the fraud protection service Eye4Fraud was listed for sale on a popular hacking forum. Spanning tens of millions of rows with 16M unique email addresses, the data was spread across 147 tables totalling 65GB and included both direct users of the service and what appears to be individuals who'd placed orders on other services that implemented Eye4Fraud to protect their sales. The data included names and bcrypt password hashes for users, and names, phone numbers, physical addresses and partial credit card data (card type and last 4 digits) for orders placed using the service. Eye4Fraud did not respond to multiple attempts to report the incident.

Compromised data: Email addresses, IP addresses, Names, Partial credit card data, Passwords, Phone numbers, Physical addresses

➤ dns@cloudflare.com

dns@cloudflare.com

pwned?

Oh no — pwned!

Pwned in 1 data breach and found 6 pastes (subscribe to search sensitive breaches)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the [1Password password manager](#) helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.



Epik: In September 2021, the domain registrar and web host Epik suffered a significant data breach, allegedly in retaliation for hosting alt-right websites. The breach exposed a huge volume of data not just of Epik customers, but also scraped WHOIS records belonging to individuals and organisations who were not Epik customers. The data included over 15 million unique email addresses (including anonymised versions for domain privacy), names, phone numbers, physical addresses, purchases and passwords stored in various formats.

Compromised data: Email addresses, Names, Phone numbers, Physical addresses, Purchases

Pastes you were found in

A paste is information that has been published to a publicly facing website designed to share content and is often an early indicator of a data breach. Pastes are automatically imported and often removed shortly after having been posted. Using the [1Password password manager](#) helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

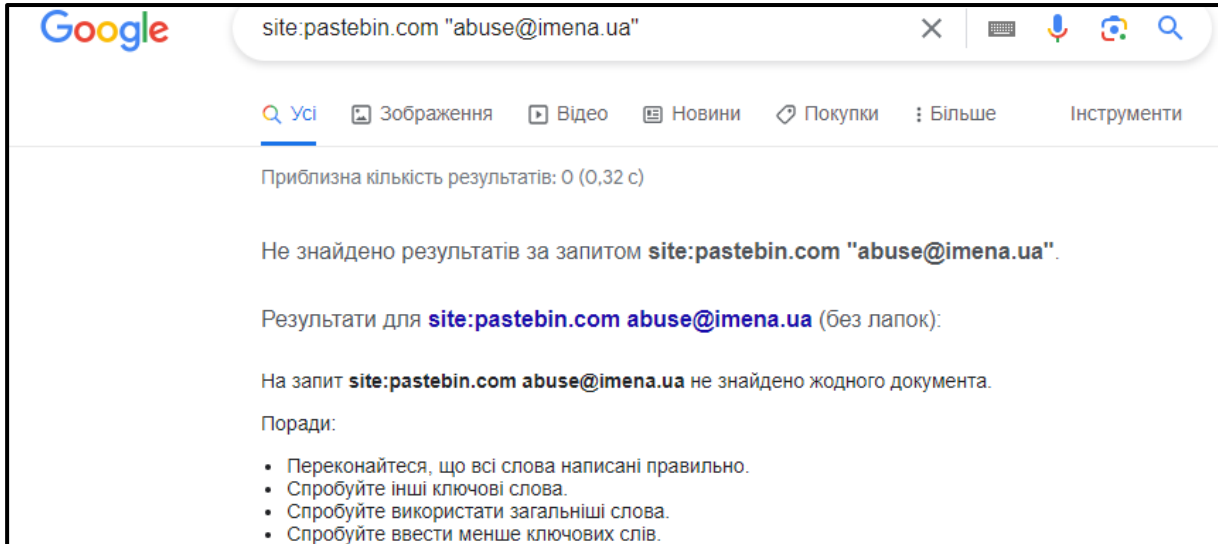
Paste title	Date	Emails
No title	14 Oct 2015, 00:27	1,218
Egypt gov stuff	1 May 2015, 14:13	1,218
more anons by Cru54d3r	2 Apr 2015, 01:43	1,073
PH1K3 EGYPT GOV LEAK	16 Sep 2014, 19:09	1,218
www.mysticstars.net	4 Oct 2014, 22:10	63
yeet	5 Aug 2015, 07:30	995

ЗАВДАННЯ 2

Перевірити електронні скриньки, домени та IP-адреси за допомогою Pastebin? (надайте результати за допомогою скріншотів) Щось цікаве?

Відповідь:

➤ `abuse@imena.ua`



➤ `dns@cloudflare.com`

