

АВТОМАТИЗОВАНА СИСТЕМА АНАЛІЗУ ЗАХИЩЕНОСТІ ВЕБ- ЗАСТОСУНКІВ ЗА ДОПОМОГОЮ OSINT

ГАЛИЦЬ В. О КН-4

КЕРІВНИК: ВОЗНЮК Я. І

- Дослідити найефективніші техніки OSINT
- Розробити систему для постійного моніторингу зовнішнього периметру
- Розробити систему моніторингу Stealer логів
- Показати ефективність заходів OSINT

МЕТА

ПЛАН

Розробити систему моніторингу OSINT

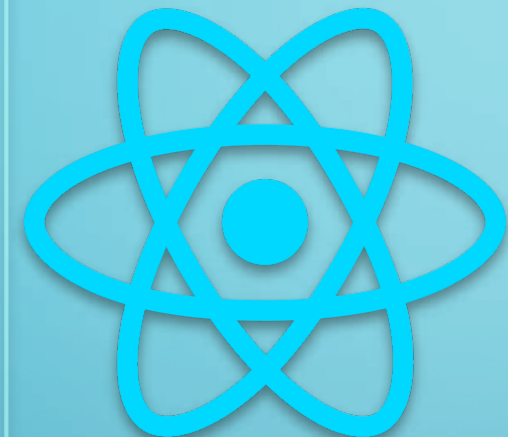
- Дослідити методи атаки та захисту інфраструктури

Пасивне сканування Мережевого простору

- DNS
- SubDomains
- Subdomain Takeover
- SSL
- Emails

Сканування та обробка Stealer logs

- Telegram API
- Python + Pandas
- Alerts



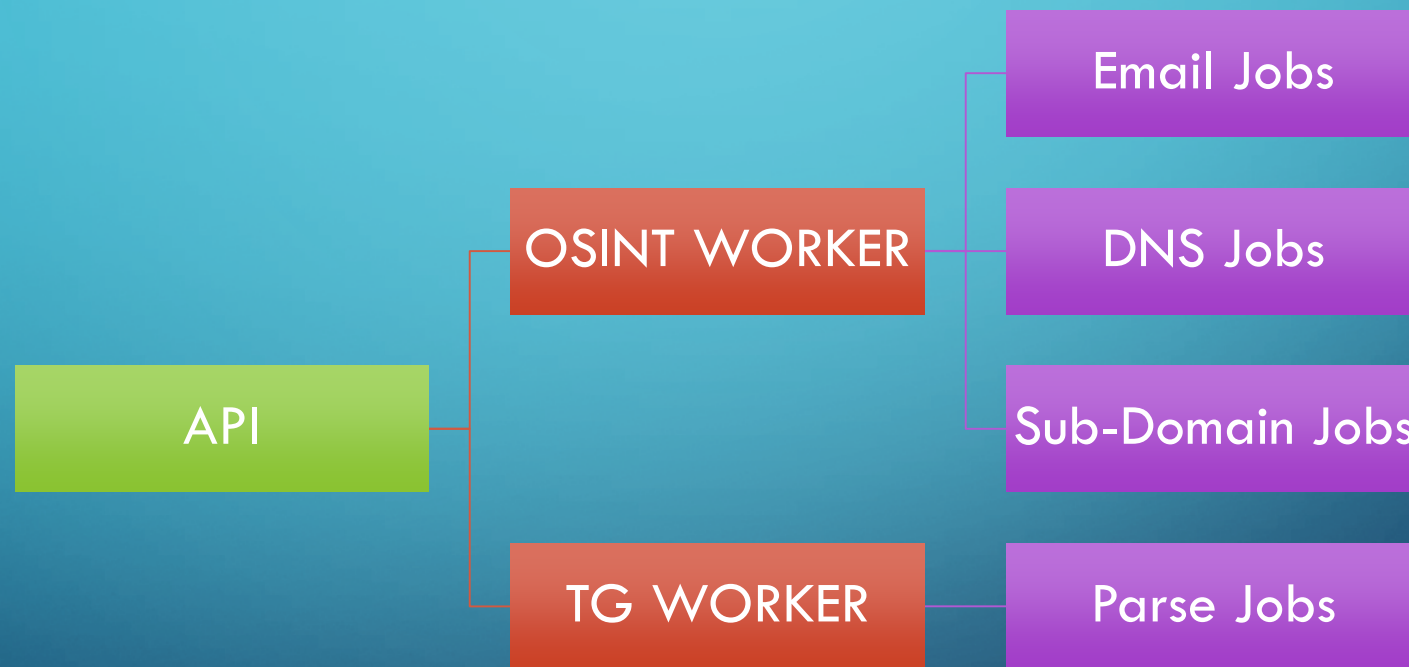
FastAPI
⚡

ІНСТРУМЕНТИ РОЗРОБКИ

ПОБУДОВА ВЕКТОРІВ АТАКИ ЧЕРЕЗ OSINT

- Passive DNS та CT-логи
- Пошук та аналіз субдоменів
- Subdirectory Enumeration
- Скан портів
- Перевірка можливості subdomain-takeover
- Аналіз TLS і заголовків безпеки
- Ланцюг DNSSEC
- Виявлення точок **непрямого** контролю
 - Здобич з Telegram-дампів

СХЕМА ЗАСТОСУНКУ



ОГЛЯД ВІДПОВІДІ ЗАСТОСУНКУ

Nmap Scan Results

Nmap Scan Results

[Push to Report](#)

Scan ID: 250

Status: DONE

Target URL: ukma.edu.ua

Port Results:

Port	State	Service	Details
22	open	ssh	OpenSSH
80	open	http	Apache httpd
443	open	http	Apache httpd

Security Headers Scan Results

Security Headers Scan Results

Asset: ukma.edu.ua

Scan ID: 102

Result ID: 171

Missing Headers

- **referrer-policy:** Specifies which referrer information should be included with requests made from the document.
- **x-frame-options:** Helps prevent clickjacking by controlling whether the content can be framed.
- **permissions-policy:** No description available.
- **x-content-type-options:** Prevents MIME-sniffing, ensuring proper content-type interpretation.
- **content-security-policy:** Prevents XSS attacks by specifying allowed content sources.
- **strict-transport-security:** Instructs browsers to only use HTTPS, preventing downgrade attacks.

All Headers

Created at: 5/27/2025, 11:46:23 AM

ОГЛЯД
ВІДПОВІДІ
ЗАСТОСУНКУ

ОГЛЯД ВІДПОВІДІ ЗАСТОСУНКУ

scan_id	domain	cname	a_records	mx_records	ns_records	potential_takeover	maybe_vulnerable
102 →	fin.university.smart-stage.	EMPTY	[["194.44.142.174"]]	[]	[]	FALSE	FALSE
102 →	itlaw.ukma.edu.ua	EMPTY	[["135.181.9.29"]]	[]	[]	FALSE	FALSE
102 →	documents.smart.ukma.edu.ua	EMPTY	[["185.131.52.158"]]	[]	[]	FALSE	FALSE
102 →	storage.smart.ukma.edu.ua	EMPTY	[["185.131.52.158"]]	[]	[]	FALSE	FALSE
102 →	smart-stage.ukma.edu.ua	EMPTY	[["194.44.142.174"]]	[]	[]	FALSE	FALSE
102 →	support.fin.ukma.edu.ua	EMPTY	[["194.44.143.139"]]	[]	[]	FALSE	FALSE
102 →	nextcloud.ukma.edu.ua	EMPTY	[["194.44.142.197"]]	[]	[]	FALSE	FALSE
102 →	edu.skovoroda.ukma.edu.ua	EMPTY	[["193.169.189.243"]]	[]	[]	FALSE	FALSE
102 →	alumni-fen.ukma.edu.ua	finance.ukma.edu.ua	[["91.206.226.31"]]	[]	[]	FALSE	FALSE
102 →	course-work.smart.ukma.edu.ua	EMPTY	[["185.131.52.158"]]	[]	[]	FALSE	FALSE
102 →	mag.ukma.edu.ua	EMPTY	[["135.181.9.29"]]	[]	[]	FALSE	FALSE
102 →	newdistedu.ukma.edu.ua	EMPTY	[["135.181.9.29"]]	[]	[]	FALSE	FALSE
102 →	nz.ukma.edu.ua	EMPTY	[["194.44.142.7"]]	[]	[]	FALSE	FALSE
102 →	nzpr.ukma.edu.ua	EMPTY	[["212.111.212.230"]]	[]	[]	FALSE	FALSE
102 →	notifications.smart-stage.	EMPTY	[["194.44.142.174"]]	[]	[]	FALSE	FALSE
102 →	nrplit.ukma.edu.ua	EMPTY	[["212.111.212.230"]]	[]	[]	FALSE	FALSE
102 →	marketing.ukma.edu.ua	finance.ukma.edu.ua	[["91.206.226.31"]]	[]	[]	FALSE	FALSE
102 →	www.fin.ukma.edu.ua	ww168.wixdns.net	[["34.149.87.45"]]	[]	[]	FALSE	FALSE
102 →	elib.ukma.edu.ua	ekmair.ukma.edu.ua	[["135.181.9.27"]]	[]	[]	FALSE	TRUE
102 →	www.ktm.ukma.edu.ua	EMPTY	[]	[]	[]	FALSE	FALSE
102 →	fen.university.smart.ukma.	EMPTY	[["185.131.52.158"]]	[]	[]	FALSE	FALSE
102 →	course-work.smart-stage.u.	EMPTY	[["194.44.142.174"]]	[]	[]	FALSE	FALSE
102 →	fin.university.smart.ukma.	EMPTY	[["185.131.52.158"]]	[]	[]	FALSE	FALSE
102 →	fsnst.university.smart.uk.	EMPTY	[["185.131.52.158"]]	[]	[]	FALSE	FALSE
102 →	md.ukma.edu.ua	EMPTY	[["135.181.9.29"]]	[]	[]	FALSE	FALSE

DNS Records for ukma.edu.ua

A Records (First seen: 2024-04-04)

IP	Count	Organization
135.181.9.30	0	Hetzner Online GmbH

MX Records (First seen: 2022-11-28)

Hostname	Priority	Count	Organization
ukma-edu-ua.mail.protection.outlook.com	0	0	Microsoft Corporation

NS Records (First seen: 2022-11-28)

Nameserver	Count	Organization
ns4.bdm.microsoftonline.com	0	Microsoft Corporation
ns3.bdm.microsoftonline.com	0	Microsoft Corporation
ns2.bdm.microsoftonline.com	0	Microsoft Corporation
ns1.bdm.microsoftonline.com	0	Microsoft Corporation

SOA Records (First seen: 2022-11-28)

TTL	Email	Count
3600	azuredns-hostmaster@microsoft.com	0

ОГЛЯД
ВІДПОВІДІ
ЗАСТОСУНКУ

Testssl Scan Results

Push to Report

Result ID: 245
Scan ID: 102
Host: ukma.edu.ua
IP Address: 135.181.9.30
Port: 443
Service: HTTP
RDNS: web.ukma.edu.ua

ID	Finding	Severity
rating_spec	SSL Labs's 'SSL Server Rating Guide' (version 2009q from 2020-01-30)	INFO
rating_doc	https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide	INFO
protocol_support_score	100	INFO
protocol_support_score_weighted	30	INFO
key_exchange_score	90	INFO
key_exchange_score_weighted	27	INFO
cipher_strength_score	90	INFO
cipher_strength_score_weighted	36	INFO
final_score	93	INFO
overall_grade	A	OK
grade_cap_reason_1	Grade capped to A. HSTS is not offered	INFO

Vulnerabilities

Protocols

Created at: 5/27/2025, 11:50:24 AM

ОГЛЯД
ВІДПОВІДІ
ЗАСТОСУНКУ

Domain: civic.ukma.edu.ua

Scan ID: 102

Result ID: 165

IP Addresses:

194.44.143.139

HTTP Status Code: N/A

HTTPS Status Code: N/A

Created at: 5/27/2025, 11:53:12 AM

Domain: cybsec.fin.ukma.edu.ua

Scan ID: 102

Result ID: 166

IP Addresses:

194.44.143.139

HTTP Status Code: N/A

HTTPS Status Code: N/A

Created at: 5/27/2025, 11:53:12 AM

Domain: course-work.smart-stage.ukma.edu.ua

Scan ID: 102

Result ID: 167

IP Addresses:

194.44.142.174

HTTP Status Code: 301

HTTPS Status Code: 200

Created at: 5/27/2025, 11:53:12 AM

Domain: accounts.smart-stage.ukma.edu.ua

Scan ID: 102

Result ID: 168

IP Addresses:

ОГЛЯД ВІДПОВІДІ ЗАСТОСУНКУ

ОГЛЯД ВІДПОВІДІ ЗАСТОСУНКУ

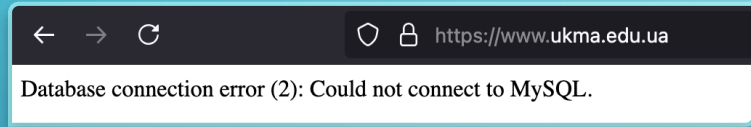
Search Credentials

Search Term:

ID	URL	Login	Password	File Name
14693777	https://mega.nz/register	Danechka.Zaruckiy@yandex.ru	ddDD2007@	/app/downloads/19/0/@TXTLog 12M Lines.txt
14693783	http://shopper.qwertykmv.ru/msshoppers	kiselchicanna@yandex.ru	annak1212	/app/downloads/19/0/@TXTLog 12M Lines.txt
14695934	https://passport.yandex.ru/profile	alena-yashkina1994	poker=face1994	/app/downloads/19/0/@TXTLog 12M Lines.txt
14696025	https://portal.gov.by	foks667@yandex.ru	h95-AXL-CCU- Zn9@	/app/downloads/19/0/@TXTLog 12M Lines.txt
14698124	https://online.sovcomins.ru/products/sanctum/authorization/4_registration.xhtml	verbov57@yandex.ru	Vgy40444988	/app/downloads/19/0/@TXTLog 12M Lines.txt
14701400	https://passport.yandex.ru/auth/welcome	renangkoon@gmail.com	Keng2525	/app/downloads/19/0/@TXTLog 12M Lines.txt
14701433	https://passport.yandex.ru/auth/welcome	bloodmastergamer1@yandex.ru	bloodmastercool12	/app/downloads/19/0/@TXTLog 12M Lines.txt

ВИСНОВКИ

- Було досліджено побудову вектору атаки та методів захисту після проведення розвідки
- Розроблено систему аналізу вразливостей зовнішнього периметру
- Розроблено систему моніторингу stealer логів



ДЯКУЮ ЗА УВАГУ!