

Лабораторна робота № 4(3.1.4)

Використання OSINT інструментів

Хід роботи:

Частина 1: Дослідження ресурсів OSINT

Крок 1: Доступ до OSINT Framework

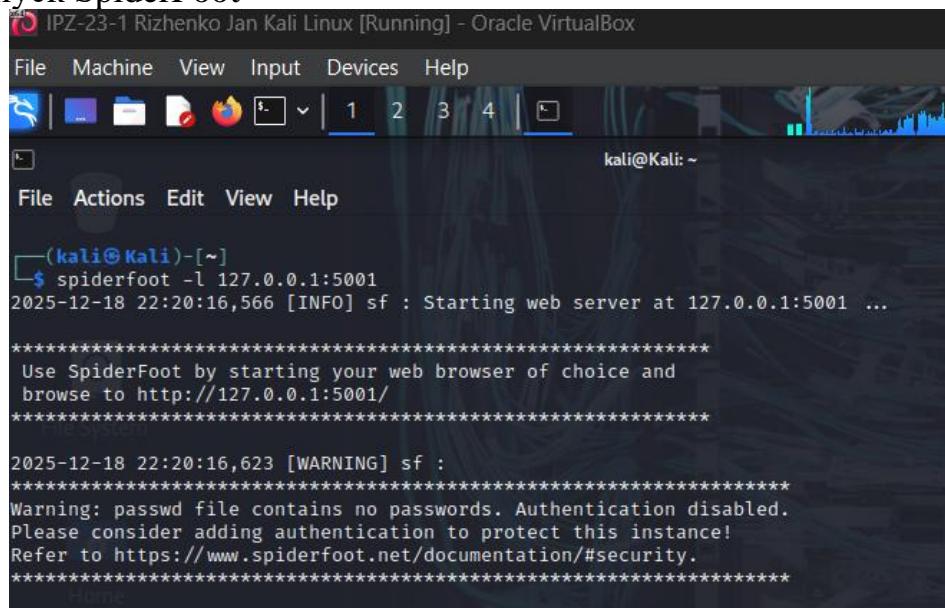
Питання: Яка цінність проведення пошуку імен користувачів та перерахування облікових записів?

Відповідь:

Пошук імен користувачів та перерахування облікових записів має критичну цінність для тестування на проникнення та оцінки безпеки організації. По-перше, це дозволяє ідентифікувати облікові записи ключового персоналу організації на різних платформах та сервісах, що може виявити потенційні вектори атак через вразливі треті сторони. Оскільки користувачі часто використовують однакові імена та паролі на декількох сайтах, компрометація облікового запису на одному сервісі може привести до доступу до корпоративних систем. По-друге, аналіз присутності персоналу на різних платформах надає цінну інформацію про їхні інтереси, зв'язки, звички та особисте життя, що може бути використано для створення цільових атак соціальної інженерії. По-третє, це допомагає виявити повторне використання паролів між сервісами, що є пошироною вразливістю. Поп-четверте, перерахування облікових записів дозволяє зібрати повний цифровий слід організації та її співробітників, включаючи забуті або неконтрольовані облікові записи. Нарешті, це допомагає знайти потенційні точки входу для подальших атак, включаючи витоки даних у публічних breach базах, що можуть містити скомпрометовані облікові дані.

Частина 2: Використання SpiderFoot

Крок 1: Запуск SpiderFoot



```
IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(kali㉿kali)-[~]
$ spiderfoot -l 127.0.0.1:5001
2025-12-18 22:20:16,566 [INFO] sf : Starting web server at 127.0.0.1:5001 ...
*****
Use SpiderFoot by starting your web browser of choice and
browse to http://127.0.0.1:5001/
*****
2025-12-18 22:20:16,623 [WARNING] sf :
*****
Warning: passwd file contains no passwords. Authentication disabled.
Please consider adding authentication to protect this instance!
Refer to https://www.spiderfoot.net/documentation/#security.
*****
```

Рис. 1. Запуск SpiderFoot з прослуховуванням на порту 5001.

Змн.	Арк.	№ докум.	Підпис	Дата	ДУ «Житомирська політехніка».23.121.26.000 – Лр4(3.1.4)		
Розроб.	Rизженко Я.В				Літ.		
Перевір.	Покотило О.А.						
Керівник					Арк.		
Н. контр.							
Зав. каф.					Аркушів		
Звіт з лабораторної роботи					Літ.	Арк.	Аркушів
						1	25
					ФІКТ Гр. ІПЗ-23-1[2]		

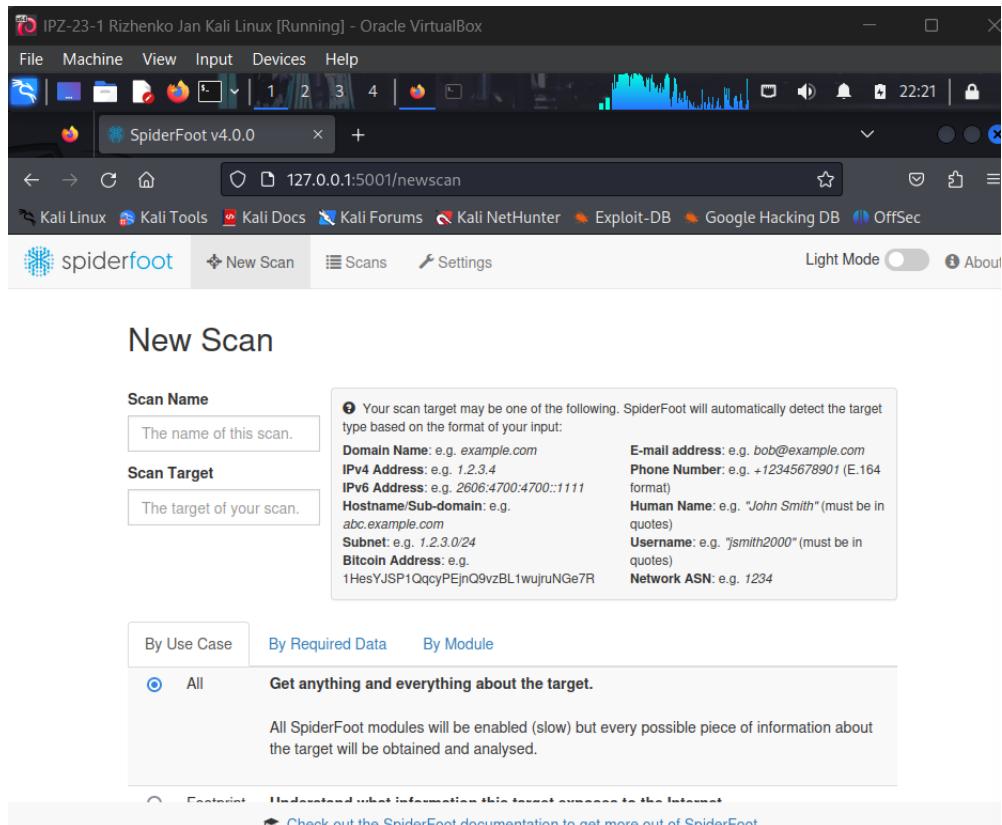


Рис. 2. Веб-інтерфейс SpiderFoot у браузері з головною сторінкою для створення нового сканування

Крок 2: Дослідження SpiderFoot

The screenshot shows a terminal window titled "IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox". The terminal displays the help menu for the SpiderFoot framework, listing various modules and their descriptions:

- sfp_abstractapi**: Look up domain, phone and IP address information from AbstractAPI.
- sfp_abusech**: Check if a host/domain, IP address or netblock is malicious according to Abuse.ch.
- sfp_abuseipdb**: Check if an IP address is malicious according to AbuseIPDB.com blacklist.
- sfp_abusix**: Check if a netblock or IP address is in the Abusix Mail Intelligence blacklist.
- sfp_accounts**: Look for possible associated accounts on nearly 200 websites like Ebay, Slashdot, reddit, etc.
- sfp_adblock**: Check if linked pages would be blocked by AdBlock Plus.
- sfp_adguard_dns**: Check if a host would be blocked by AdGuard DNS.
- sfp_ahmia**: Search Tor 'Ahmia' search engine for mentions of the target.
- sfp_alienVault**: Obtain information from AlienVault Open Threat Exchange (OTX)
- sfp_alienVaultiprepse**: Check if an IP or netblock is malicious according to the AlienVault IP Reputation database.
- sfp_apple_itunes**: Search Apple iTunes for mobile apps.
- sfp_archiveorg**: Identifies historic versions of interesting files/pages from the Wayback Machine.
- sfp_arin**: Queries ARIN registry for contact information.
- sfp_azureblobstorage**: Search for potential Azure blobs associated with the target and attempt to list their contents.
- sfp_badpackets**: Obtain information about any malicious activities involving IP addresses found.
- sfp_base64**: Identify Base64-encoded strings in URLs, often revealing interesting hidden information.
- sfp_bgpview**: Obtain network information from BGPView API.
- sfp_binaryedge**: Obtain information from BinaryEdge.io Internet scanning systems, including breaches, vul

Рис. 3. Повний список модулів SpiderFoot у терміналі

		<i>Риженко Я.В</i>			<i>Арк.</i>
		<i>Покотило О.А.</i>			<i>ДУ «Житомирська політехніка».23.121.26.000 – Пр4(3.1.4)</i>
<i>Змн.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>	<i>2</i>

Використання grep для фільтрації модулів:

```
IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
sfp_yandexdns          Check if a host would be blocked by Yandex DNS.
sfp_zetalytics          Query the Zetalytics database for hosts on your target domain(s).
sfp_zonehn              Check if a hostname/domain appears on the zone-h.org 'special defacements' RSS feed.
2025-12-18 22:22:55,159 [INFO] sf : Modules available:

└── (kali㉿Kali)-[~]
$ spiderfoot -M | grep email
sfp_debounce            Check whether an email is disposable.
sfp_email                Identify e-mail addresses in any obtained data.
sfp_emailcrawlr          Search EmailCrawlr for email addresses and phone numbers associated with a domain.
sfp_emailformat           Look up e-mail addresses on email-format.com.
sfp_emailrep              Search EmailRep.io for email address reputation.
sfp_flickr               Search Flickr for domains, URLs and emails related to the specified domain.
sfp_grep_app              Search grep.app API for links and emails related to the specified domain.
sfp_nameapi               Check whether an email is disposable.
sfp_seon                 Queries seon.io to gather intelligence about IP Addresses, email addresses, and phone nu
mbers
sfp_snow                 Gather available email IDs from identified domains
sfp_trumail              Check whether an email is disposable
2025-12-18 22:24:20,403 [INFO] sf : Modules available:

└── (kali㉿Kali)-[~]
```

Рис. 4. Фільтрація модулів SpiderFoot для роботи з email адресами.

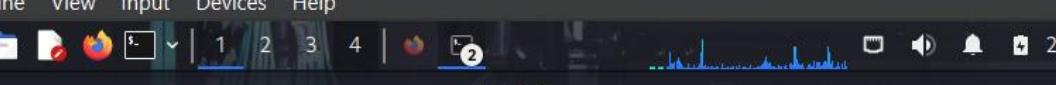
Пошук модулів для DNS:

```
IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
[ 1 2 3 4 ] [ 2 ]
kali@Kali: ~
File Actions Edit View Help

[~] $ spiderfoot -M | grep dns
sfp_adguard_dns Check if a host would be blocked by AdGuard DNS.
sfp.cloudflaredns Check if a host would be blocked by CloudFlare DNS.
sfp_dns_for_family Check if a host would be blocked by DNS for Family.
sfp_dnsbrute Attempts to identify hostnames through brute-forcing common names and iterations.
sfp_dnscommonsrv Attempts to identify hostnames through brute-forcing common DNS SRV records.
sfp_dnsdb Query FarSight's DNSDB for historical and passive DNS data.
sfp_dnscdumpster Passive subdomain enumeration using HackerTarget's DNSDumpster
sfp_dnsgrep Obtain Passive DNS information from Rapid7 Sonar Project using DNSGrep API.
sfp_dnseighbor Attempt to reverse-resolve the IP addresses next to your target to see if they are related.
ed.
sfp_dnstraw Retrieves raw DNS records such as MX, TXT and others.
sfp_dnsresolve Resolves hosts and IP addresses identified, also extracted from raw content.
sfp_dnzonexfer Attempts to perform a full DNS zone transfer.
sfp_open_passive_dns_database Obtain passive DNS information from pdns.daloo.de Open passive DNS database.
sfp_opendns Check if a host would be blocked by OpenDNS.
sfp_tool_dn twist Identify bit-squatting, typo and other similar domains to the target using a local DNSTwist installation.
sfp_viewdns Identify co-hosted websites and perform reverse Whois lookups using ViewDNS.info.
sfp_yandexdns Check if a host would be blocked by Yandex DNS.
2025-12-18 22:26:16,005 [INFO] sf : Modules available:
```

Рис. 5. Модулі SpiderFoot для DNS розвідки

Пошук модулів для витоків даних:



```
(kali㉿Kali)-[~]$ spiderfoot -M | grep breach
sfp_binaryedge          Obtain information from BinaryEdge.io Internet scanning systems, including breaches, vulnerabilities, torrents and passive DNS.
sfp_citadel              Searches Leak-Lookup.com's database of breaches.
sfp_dehashed              Gather breach data from Dehashed API.
sfp_haveibeenpwned        Check HaveIBeenPwned.com for hacked e-mail addresses identified in breaches.
sfp_scylla                Gather breach data from Scylla API.
2025-12-18 22:26:40,321 [INFO] sf : Modules available:
```

Рис. 6. Модулі SpiderFoot для перевірки витоків даних

		<i>Риженко Я.В</i>				Арк.
		<i>Покотило О.А.</i>				ДУ «Житомирська політехніка».23.121.26.000 – Пр4(3.1.4)
Змн.	Арк.	№ докум.	Підпис	Дата		3

Таблиця модулів SpiderFoot:

ТИП ІНФОРМАЦІЇ	НАЗВА СКАНЕРА/МОДУЛЯ	API КЛЮЧ ПОТРІБЕН? БЕЗКОШТОВНИЙ?	КОМЕНТАРИ
Можливі облікові записи, пов'язані з доменом	Account Finder, sfp_accounts	Hi, N/A	Понад 200 сайтів, таких як eBay, Reddit, Slashdot
Посилання, пов'язані з ціллю	Link Extractor, sfp_pageinfo	Hi, N/A	Витягує посилання зі сторінок
Email адреси, пов'язані з ціллю	Email Extractor, sfp_emailformat	Hi, N/A	Знаходить email адреси на веб-сторінках
Домени та URL, пов'язані з ціллю	Subdomain Finder, sfp_dnsbrute	Hi, N/A	Знаходить субдомени та пов'язані URL
Інформація про геолокацію	IP Geolocation, sfp_ipinfo	Hi, N/A (базова версія)	Визначає фізичне розташування IP адрес
Інформація про витоки даних	Have I Been Pwned, sfp_haveibeenpwned	Так, безкоштовний	Перевіряє наявність облікових записів у відомих витоках даних

Крок 3: Реєстрація API ключів (опціонально)

Таблиця API модулів:

Модуль	Тип інформації	API ключ
Builtwith	Технології, використані для створення веб-сайту	Реєстрація на builtwith.com
Hunter.io	Email адреси, пов'язані з доменом	Реєстрація на hunter.io
Onion.link	Доступ до .onion сайтів через clearnet	Не потрібен
IntelligenceX	Витоки даних, паролі, документи	Реєстрація на intelx.io

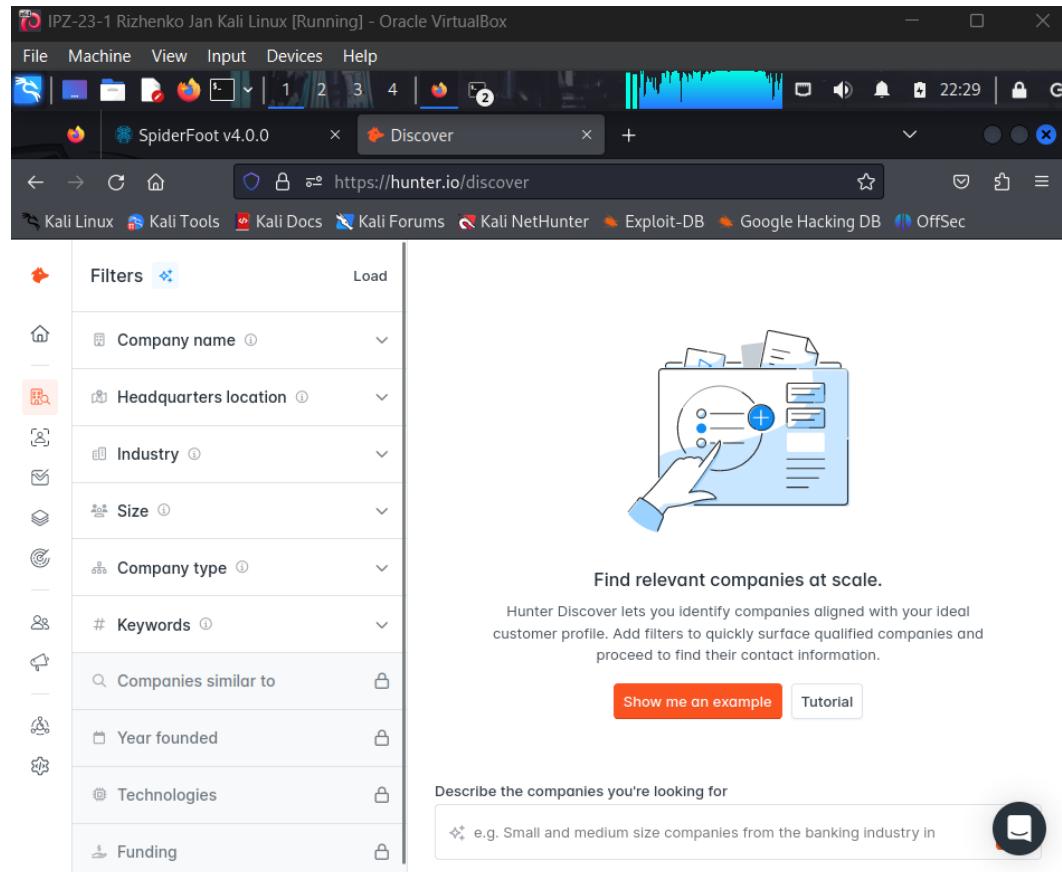


Рис. 7. Сайт Hunter.io

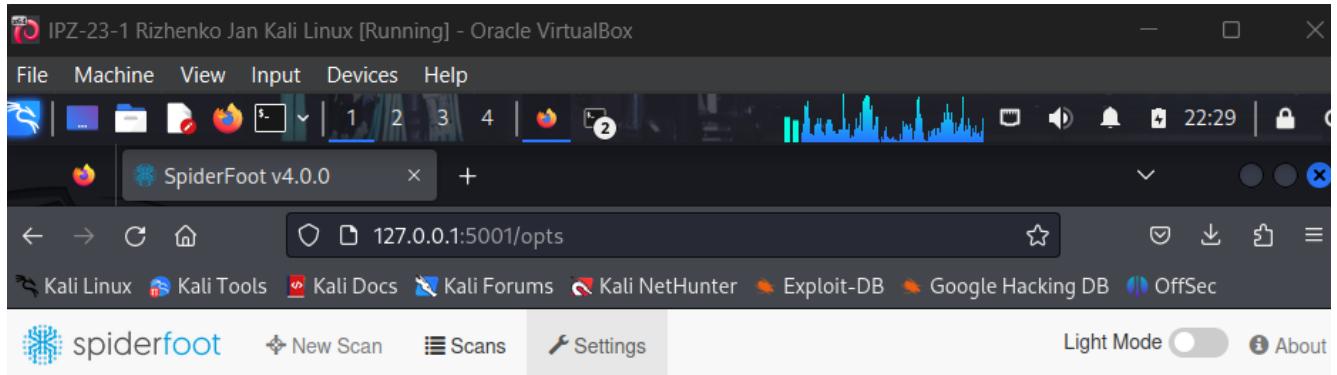


Рис. 8. Налаштування API ключів у веб-інтерфейсі SpiderFoot через Settings (кнопки Import та Export)

Крок 4: Аналіз результатів сканування з API модулями

		Рижсенко Я.В			ДУ «Житомирська політехніка».23.121.26.000 – Лр4(3.1.4)	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

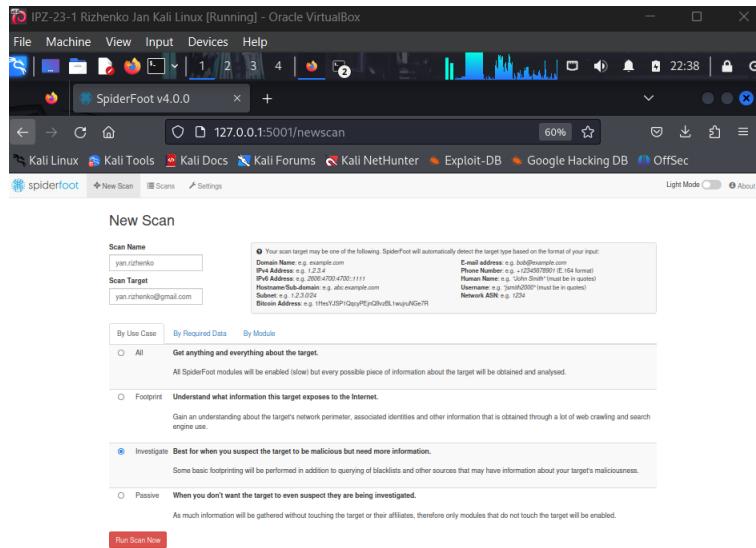


Рис. 9. Створення нового сканування у SpiderFoot з вказанням цільового домену

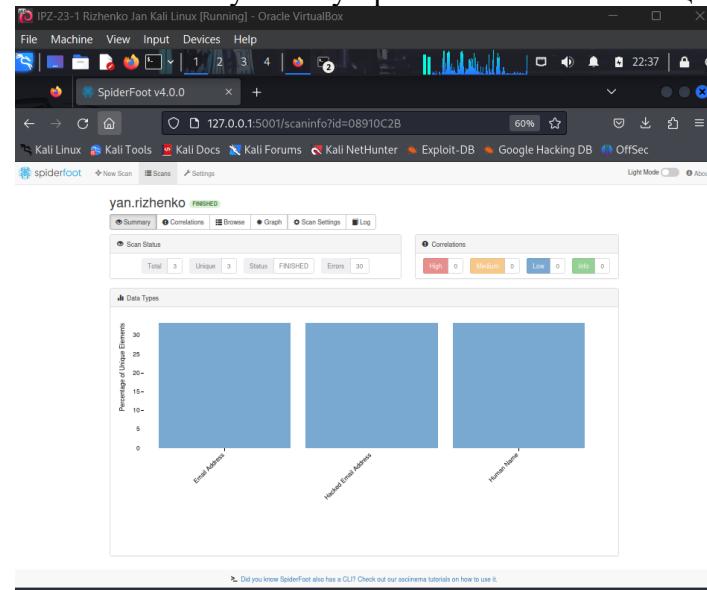


Рис. 10. Процес виконання сканування з відображенням активних модулів

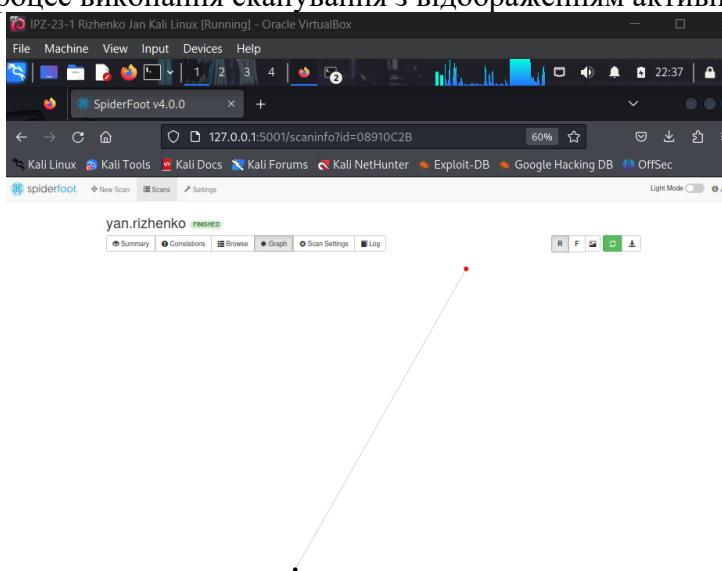


Рис. 11. Результати сканування у вигляді графа зв'язків між виявленими об'єктами

		<i>Риженко Я.В</i>				
		<i>Покотило О.А.</i>				
Змн.	Арк.	№ докум.	Підпис	Дата	ДУ «Житомирська політехніка».23.121.26.000 – Пр4(3.1.4)	Арк. 6

Питання: Який модуль сприяє таблиці Leak Site URL?

Відповідь:

Модуль **IntelligenceX** (sfp_intelx) або **Hunter.io** (sfp_hunter) зазвичай сприяє таблиці Leak Site URL, оскільки ці модулі спеціалізуються на пошуку витоків даних та скомпрометованих облікових записів.

Питання: Що ви бачите при відкритті записів у новій вкладці?

Відповідь:

При відкритті записів у новій вкладці можна побачити:

- Веб-сторінки з витоками даних або базами даних скомпрометованих облікових записів
- Інформацію про конкретні інциденти безпеки
- Деталі про знайдені email адреси, паролі або інші конфіденційні дані
- Посилання на форуми, пастебіни або інші джерела, де була опублікована скомпрометована інформація
- Можливі дати витоків та типи скомпрометованих даних

У моєму випадку виводяться лише ті дані, що я ввів для пошуку, жодного витоку зі сторонніх сайтів.

Частина 3: Дослідження Recon-ng

Крок 1: Створення робочого простору

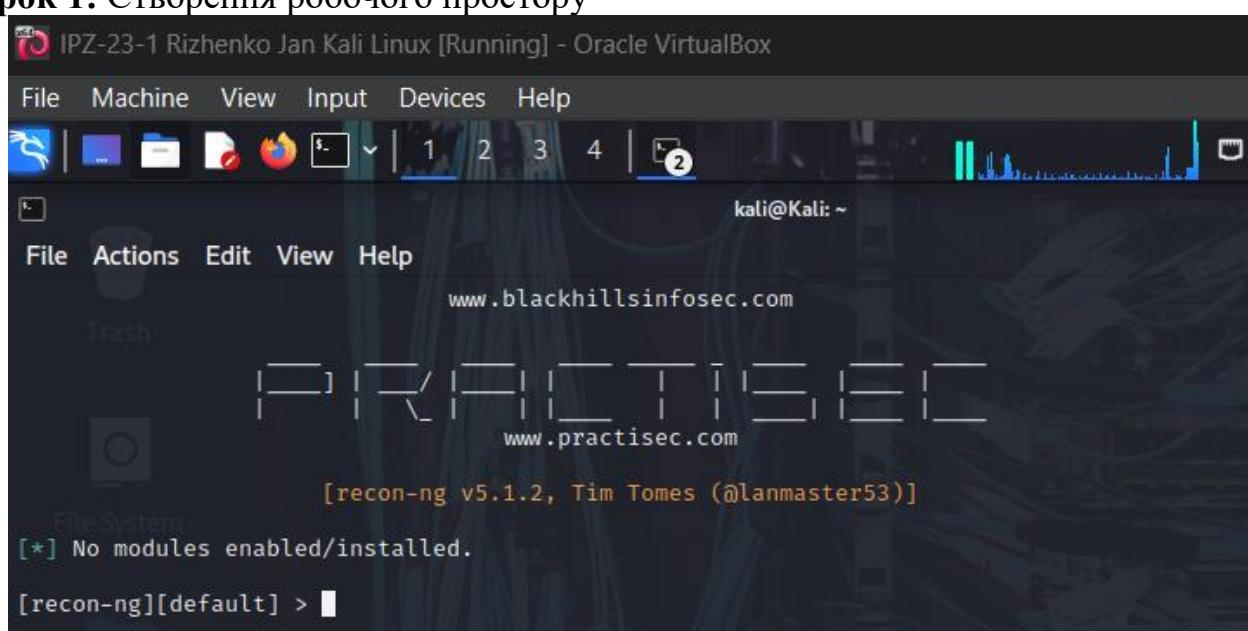


Рис. 12. Запуск Recon-ng з відображенням банера та версії

Команди для роботи з workspaces:

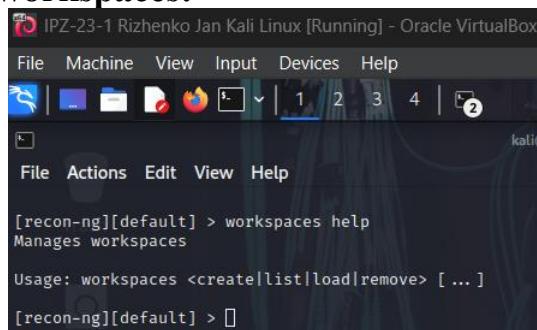


Рис. 13. Вивід довідки по командах workspaces

		Рижсенко Я.В			ДУ «Житомирська політехніка».23.121.26.000 – Лр4(3.1.4)	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

```
[recon-ng][default] > workspaces list
+-----+
| Workspaces | Modified |
+-----+
| default    | 2025-12-18 22:43:07 |
+-----+
```

Рис. 14. Список доступних робочих просторів у Recon-ng

```
Usage: workspaces <create|list|load|remove> [ ... ]

[recon-ng][default] > workspaces create test
[recon-ng][test] > workspaces list

+-----+
| Workspaces | Modified |
+-----+
| default    | 2025-12-18 22:43:07 |
| test       | 2025-12-18 23:18:58 |
+-----+
```

Рис. 15. Створення нового робочого простору з назвою "test"

```
[recon-ng][test] > workspaces load osint_lab
[*] Invalid workspace name.
[recon-ng][test] > workspaces remove test
[recon-ng][default] > workspaces back
Manages workspaces

Usage: workspaces <create|list|load|remove> [ ... ]

[recon-ng][default] > back
```

Рис. 16. Навігація між різними робочими просторами та вихід.

		<i>Рижсенко Я.В</i>			ДУ «Житомирська політехніка».23.121.26.000 – Лр4(3.1.4)	Арк.
		<i>Покотило О.А.</i>				
Змн.	Арк.	№ докум.	Підпис	Дата		8

Питання: Як можна відобразити доступні робочі простори?

Відповідь:

Команда workspaces list відображає всі доступні робочі простори.

Питання: Як можна видалити робочий простір?

Відповідь:

Команда workspaces remove з вказанням назви робочого простору видаляє його повністю.

Питання: Яка команда вийде з робочого простору та поверне до головного Recon-ng prompt?

Відповідь:

Команда back повертає до головного prompt Recon-ng.

Крок 2: Дослідження модулів

Команда для перегляду встановлених модулів:

modules search

The screenshot shows a terminal window titled 'IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox'. The window contains the following text:

```
[*] No modules enabled/installed.  
[recon-ng][default] > modules search  
[!] No modules found.  
Searches installed modules  
Usage: modules search [<regex>]  
[recon-ng][default] > ■
```

Рис. 17. Список встановлених модулів у Recon-ng (порожній для свіжої інсталяції)

Питання: Скільки модулів наразі доступні для вас?

Відповідь:

У “свіжій” Recon-ng версії 5.x або новішої за замовчуванням встановлено 0 модулів. Це відрізняється від попередніх версій, де модулі були попередньо встановлені. Тепер всі модулі повинні бути встановлені з marketplace. У marketplace доступно понад 90-100 модулів для встановлення, які охоплюють різні аспекти розвідки: збір субдоменів, email адрес, інформації про компанії, геолокації, перевірку витоків даних тощо. Модульна архітектура дозволяє встановлювати лише необхідні модулі, що зменшує розмір інсталяції та спрощує управління залежностями.

Крок 3: Дослідження marketplace модулів

		Риженко Я.В			ДУ «Житомирська політехніка».23.121.26.000 – Лр4(3.1.4)	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

The screenshot shows a Kali Linux desktop environment within Oracle VirtualBox. The desktop background features a dark theme with a 'PRACTISE' watermark. A terminal window titled '[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]' is open, displaying the following text:

```
[*] No modules enabled/installed.

[recon-ng][default] > marketplace help
Interfaces with the module marketplace

Usage: marketplace <info|install|refresh|remove|search> [ ... ]

[recon-ng][default] > 
```

Рис. 18. Довідка по командах marketplace

```
IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
[2] 23:26
File Actions Edit View Help
Interfaces with the module marketplace
Usage: marketplace <info|install|refresh|remove|search> [ ... ]
[recon-ng][default] > marketplace search

+-----+-----+-----+-----+-----+-----+
| Path | Version | Status | Updated | D | K |
+-----+-----+-----+-----+-----+-----+
| discovery/info_disclosure/cache_snoop | 1.1 | not installed | 2020-10-13 | | |
| discovery/info_disclosure/interesting_files | 1.2 | not installed | 2021-10-04 | | |
| exploitation/injection/command_injector | 1.0 | not installed | 2019-06-24 | | |
| exploitation/injection/xpath_bruter | 1.2 | not installed | 2019-10-08 | | |
| import/csv_file | 1.1 | not installed | 2019-08-09 | | |
| import/list | 1.1 | not installed | 2019-06-24 | | |
| import/masscan | 1.0 | not installed | 2020-04-07 | | |
| import/mmap | 1.1 | not installed | 2020-10-06 | | |
| recon/companies-contacts/bing_linkedin_cache | 1.0 | not installed | 2019-06-24 | | * |
| recon/companies-contacts/censys_email_address | 2.1 | not installed | 2022-01-31 | * * |
| recon/companies-contacts/pen | 1.1 | not installed | 2019-10-15 | | |
| recon/companies-domains/censys_subdomains | 2.1 | not installed | 2022-01-31 | * * |
| recon/companies-domains/pen | 1.1 | not installed | 2019-10-15 | | |
| recon/companies-domains/viewdns_reverse_whois | 1.1 | not installed | 2021-08-24 | | |
| recon/companies-domains/whoxy_dns | 1.1 | not installed | 2020-06-17 | * |
| recon/companies-multi/censys_org | 2.1 | not installed | 2022-01-31 | * * |
| recon/companies-multi/censys_tls_subjects | 2.1 | not installed | 2022-01-31 | * * |
| recon/companies-multi/github_miner | 1.1 | not installed | 2020-05-15 | * |
| recon/companies-multi/shodan_org | 1.1 | not installed | 2020-07-01 | * * |
| recon/companies-multi/whois_miner | 1.1 | not installed | 2019-10-15 | | |
| recon/contacts-contacts/abc | 1.0 | not installed | 2019-10-11 | * |
| recon/contacts-contacts/mailtester | 1.0 | not installed | 2019-06-24 | |
```

Рис. 19. Повний список модулів у marketplace з індикаторами залежностей (D) та API ключів (K)

		<i>Риженко Я.В</i>				Арк.
		<i>Покотило О.А.</i>				
Змн.	Арк.	№ докум.	Підпис	Дата	ДУ «Житомирська політехніка».23.121.26.000 – Пр4(3.1.4)	10

```

IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@Kali: ~
File Actions Edit View Help
| recon/repositories-vulnerabilities/gists_search | 1.0 | not installed | 2019-06-24 | | * |
| recon/repositories-vulnerabilities/github_dorks | 1.0 | not installed | 2019-06-24 | | * |
| reporting/csv | 1.0 | not installed | 2019-06-24 | | * |
| reporting/html | 1.0 | not installed | 2019-06-24 | | * |
| reporting/json | 1.0 | not installed | 2019-06-24 | | * |
| reporting/list | 1.0 | not installed | 2019-06-24 | | * |
| reporting/proxifier | 1.0 | not installed | 2019-06-24 | | * |
| reporting/pushpin | 1.0 | not installed | 2019-06-24 | | * |
| reporting/xlsx | 1.0 | not installed | 2019-06-24 | | * |
| reporting/xml | 1.1 | not installed | 2019-06-24 | | * |
+
D = Has dependencies. See info for details.
K = Requires keys. See info for details.

[recon-ng][default] > marketplace search bing
[*] Searching module index for 'bing' ...

+-----+-----+-----+-----+-----+
| Path | Version | Status | Updated | D | K |
+-----+-----+-----+-----+-----+
| recon/companies-contacts/bing_linkedin_cache | 1.0 | not installed | 2019-06-24 | | * |
| recon/domains-hosts/bing_domain_api | 1.0 | not installed | 2019-06-24 | | * |
| recon/domains-hosts/bing_domain_web | 1.1 | not installed | 2019-07-04 | | * |
| recon/hosts-hosts/bing_ip | 1.0 | not installed | 2019-06-24 | | * |
| recon/profiles-contacts/bing_linkedin_contacts | 1.2 | not installed | 2021-08-24 | | * |
+
D = Has dependencies. See info for details.
K = Requires keys. See info for details.

[recon-ng][default] > 

```

Рис. 20. Результати пошуку модулів за ключовим словом "bing"

```

IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@Kali: ~
File Actions Edit View Help
+-----+-----+-----+-----+-----+
| Path | Version | Status | Updated | D | K |
+-----+-----+-----+-----+-----+
| recon/companies-contacts/bing_linkedin_cache | 1.0 | not installed | 2019-06-24 | | * |
| recon/domains-hosts/bing_domain_api | 1.0 | not installed | 2019-06-24 | | * |
| recon/domains-hosts/bing_domain_web | 1.1 | not installed | 2019-07-04 | | * |
| recon/hosts-hosts/bing_ip | 1.0 | not installed | 2019-06-24 | | * |
| recon/profiles-contacts/bing_linkedin_contacts | 1.2 | not installed | 2021-08-24 | | * |
+
D = Has dependencies. See info for details.
K = Requires keys. See info for details.

[recon-ng][default] > marketplace search shodan
[*] Searching module index for 'shodan' ...

+-----+-----+-----+-----+-----+
| Path | Version | Status | Updated | D | K |
+-----+-----+-----+-----+-----+
| recon/companies-multi/shodan_org | 1.1 | not installed | 2020-07-01 | | * |
| recon/domains-hosts/shodan_hostname | 1.1 | not installed | 2020-07-01 | | * |
| recon/hosts-ports/shodan_ip | 1.2 | not installed | 2020-07-01 | | * |
| recon/locations-pushpins/shodan | 1.1 | not installed | 2020-07-07 | | * |
| recon/netblocks-hosts/shodan_net | 1.2 | not installed | 2020-07-21 | | * |
+
D = Has dependencies. See info for details.
K = Requires keys. See info for details.

[recon-ng][default] > 

```

Рис. 21. Результати пошуку модулів за ключовим словом "shodan"

```

IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@Kali: ~
File Actions Edit View Help
+-----+-----+-----+-----+-----+
| Path | Version | Status | Updated | D | K |
+-----+-----+-----+-----+-----+
| recon/companies-multi/shodan_org | 1.1 | not installed | 2020-07-01 | | * |
| recon/domains-hosts/shodan_hostname | 1.1 | not installed | 2020-07-01 | | * |
| recon/hosts-ports/shodan_ip | 1.2 | not installed | 2020-07-01 | | * |
| recon/locations-pushpins/shodan | 1.1 | not installed | 2020-07-07 | | * |
| recon/netblocks-hosts/shodan_net | 1.2 | not installed | 2020-07-21 | | * |
+
D = Has dependencies. See info for details.
K = Requires keys. See info for details.

[recon-ng][default] > marketplace search email
[*] Searching module index for 'email' ...

+-----+-----+-----+-----+-----+
| Path | Version | Status | Updated | D | K |
+-----+-----+-----+-----+-----+
| recon/companies-contacts/censys_email_address | 2.1 | not installed | 2022-01-31 | | * |
| recon/companies-contacts/pen | 1.1 | not installed | 2019-10-15 | | * |
| recon/companies-domains/pen | 1.1 | not installed | 2019-10-15 | | * |
| recon/contact-contacts/angler | 1.0 | not installed | 2019-09-10 | | * |
| recon/contact-contacts/mangle | 1.0 | not installed | 2019-06-24 | | * |
| recon/contact-credentials/hibp_breach | 1.2 | not installed | 2019-09-26 | | * |
| recon/contact-credentials/hibp_paste | 1.1 | not installed | 2019-09-10 | | * |
| recon/contact-domains/censys_email_to_domains | 2.1 | not installed | 2022-01-31 | | * |
| recon/contact-domains/migrate_contacts | 1.1 | not installed | 2020-05-17 | | * |
| recon/contact-profiles/fullcontact | 1.1 | not installed | 2019-07-24 | | * |
| recon/domain-contacts/hunter_ip | 1.3 | not installed | 2019-07-24 | | * |
| recon/domain-contacts/pottersearch | 1.4 | not installed | 2019-10-16 | | * |
| recon/domains-contacts/wikileaker | 1.0 | not installed | 2020-04-08 | | * |
+
D = Has dependencies. See info for details.
K = Requires keys. See info for details.

[recon-ng][default] > 

```

Рис. 22. Результати пошуку модулів за ключовим словом "email"

		<i>Рижсенко Я.В</i>		
		<i>Покотило О.А.</i>		
<i>Змн.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>

ДУ «Житомирська політехніка».23.121.26.000 – Лр4(3.1.4)

Арк.

11

```

IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@Kali: ~
File Actions Edit View Help
| recon/domains-migrate_contacts | 1.1 | not installed | 2020-05-17 | | |
| recon/domains-profiles/fullcontact | 1.1 | not installed | 2019-07-24 | | * |
| recon/domains-contacts/hunter.io | 1.3 | not installed | 2020-04-14 | | * |
| recon/domains-contacts/pgp_search | 1.4 | not installed | 2019-10-16 | | |
| recon/domains-contacts/wikileaker | 1.0 | not installed | 2020-04-08 | | |
+-----+
D = Has dependencies. See info for details.
K = Requires keys. See info for details.

[recon-ng][default] > marketplace info recon/domains-hosts/bing_domain_web
+-----+
| path | recon/domains-hosts/bing_domain_web
| name | Bing Hostname Enumerator
| author | Tim Tomes (@lanmaster53)
| version | 1.1
| last_updated | 2019-07-04
| description | Harvests hosts from Bing.com by using the 'site' search operator. Updates the 'hosts' table with the results.
| required_keys | []
| dependencies | []
| files | []
| status | not installed
+-----+
[recon-ng][default] >

```

Рис. 23. Детальна інформація про модуль bing_domain_web

```

IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@Kali: ~
File Actions Edit View Help
| files | []
| status | not installed
+-----+
[recon-ng][default] > marketplace install recon/domains-hosts/bing_domain_web
[*] Module installed: recon/domains-hosts/bing_domain_web
[*] Reloading modules ...
[recon-ng][default] >

```

Рис. 24. Процес встановлення модуля з marketplace

```

IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@Kali: ~
File Actions Edit View Help
| files | []
| status | not installed
+-----+
[recon-ng][default] > marketplace install recon/domains-hosts/bing_domain_web
[*] Module installed: recon/domains-hosts/bing_domain_web
[*] Reloading modules ...
[recon-ng][default] > marketplace remove recon/domains-hosts/bing_domain_web
[*] Module removed: recon/domains-hosts/bing_domain_web
[*] Reloading modules ...
[recon-ng][default] > marketplace refresh
[*] Marketplace index refreshed.
[recon-ng][default] >

```

Рис. 25. Видалення модуля з marketplace та оновлення всіх модулів.

		Рижсенко Я.В					Арк.
		Покотило О.А.					
Змн.	Арк.	№ докум.	Підпис	Дата			ДУ «Житомирська політехніка».23.121.26.000 – Лр4(3.1.4)

Питання: Модульні таблиці мають колонки для D та K. Знайдіть shodan модулі. Які вимоги до цих модулів?

Відповідь:

При пошуку shodan модулів за допомогою команди marketplace search shodan(Рис.21) відображаються колонки з позначками D (Dependencies) та K (Keys).

D (Dependencies) позначає, що модуль має зовнішні залежності, зазвичай Python бібліотеки. Якщо в цій колонці стоїть зірочка, це означає, що потрібно встановити додаткові пакети.

K (Keys) позначає, що модуль потребує API ключі для роботи. Для всіх shodan модулів у цій колонці стоїть зірочка, оскільки Shodan є платною службою з обмеженим безкоштовним рівнем.

Shodan надає безкоштовний API ключ після реєстрації, але з обмеженнями. Безкоштовний рівень дозволяє 100 запитів на місяць, тоді як платний рівень надає необмежені запити та доступ до всіх функцій.

Для використання shodan модулів необхідно зареєструватися на shodan.io, отримати API ключ та додати його в Recon-ng командою keys add shodan_api з вказанням ключа.

Крок 4: Встановлення нового модуля

Питання: Який модуль ви знайшли (що не потребує залежностей або API ключів)?

Відповідь:

Пошук модулів без залежностей виконується командою marketplace search bing(Рис.20)

Модуль recon/domains-hosts/bing_domain_web не потребує API ключів та додаткових залежностей.

Цей модуль використовує публічну пошукову систему Bing для знаходження субдоменів та хостів, пов'язаних з доменом. Він не потребує API ключів, оскільки виконує пошук через веб-скрейпінг результатів пошуку Bing з використанням оператора site. Також не має зовнішніх залежностей, окрім стандартних бібліотек Python, що робить його ідеальним для швидкого початку роботи без додаткових налаштувань.

The screenshot shows a terminal window titled 'IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox'. The command entered is '[recon-ng][default] > marketplace info recon/domains-hosts/bing_domain_web'. The output displays the following details for the module:

Path	Value
path	recon/domains-hosts/bing_domain_web
name	Bing Hostname Enumerator
author	Tim Tomes (@lanmaster53)
version	1.1
last_updated	2019-07-04
description	Harvests hosts from Bing.com by using the 'site' search operator. Updates the 'hosts' table wi
required_keys	[]
dependencies	[]
files	[]
status	not installed

Рис. 26. Детальна інформація про модуль bing_domain_web (автор, версія, опис, опції).

		Риженка Я.В					Арк.
		Покотило О.А.					ДУ «Житомирська політехніка».23.121.26.000 – Лр4(3.1.4)
Змн.	Арк.	№ докум.	Підпис	Дата			13

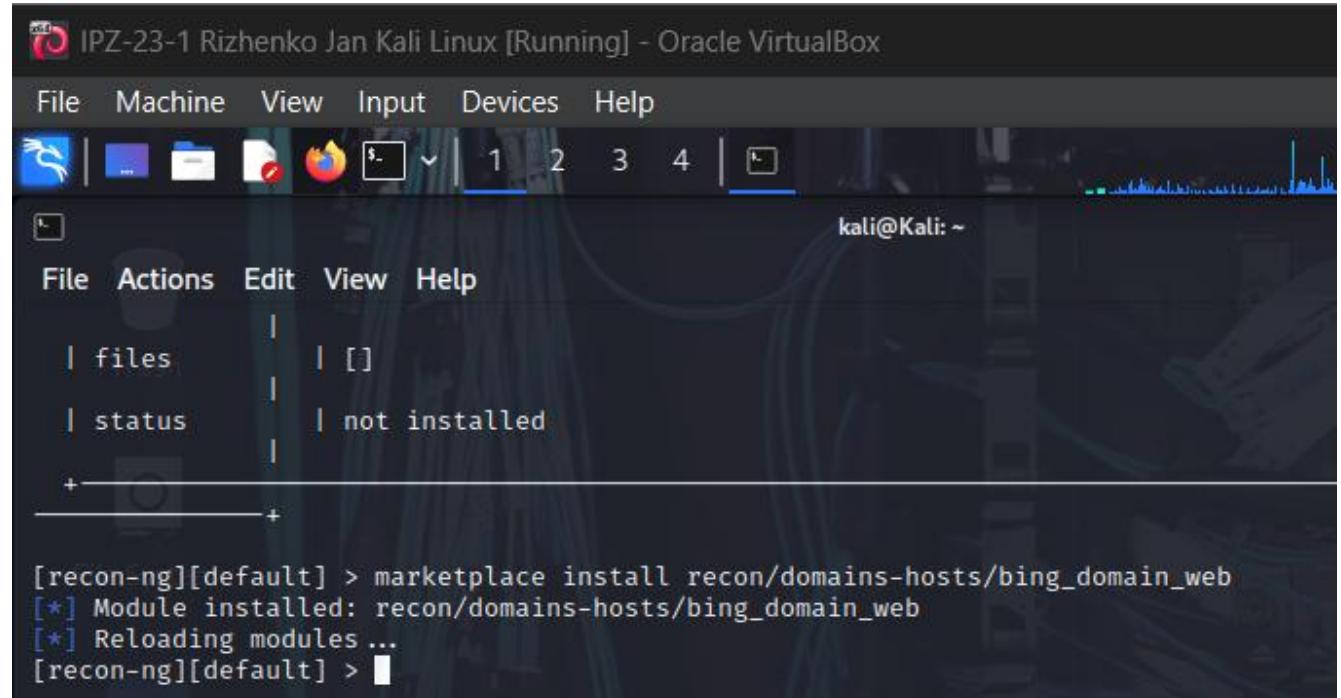


Рис. 27. Успішне встановлення модуля bing domain web.

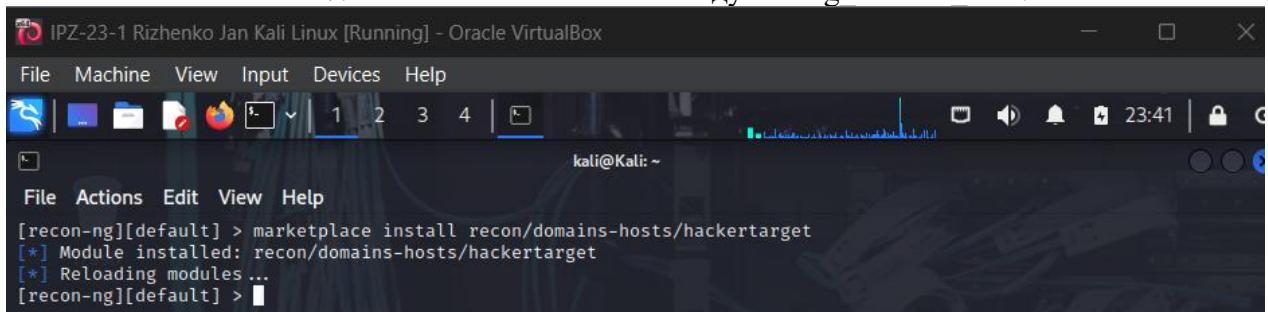


Рис. 28. Успішне встановлення додаткового модуля `hackertarget`.

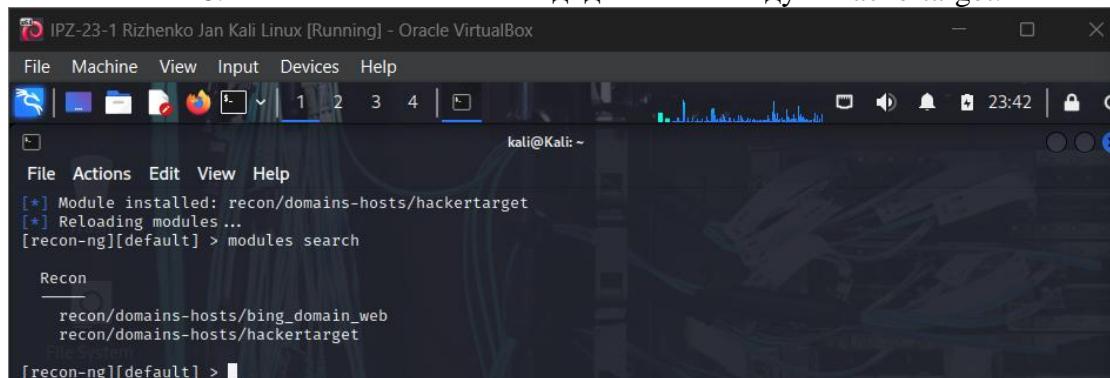


Рис. 29. Список встановлених модулів після інсталяції.

Крок 5: Запуск нових модулів

Команди для роботи з модулями:

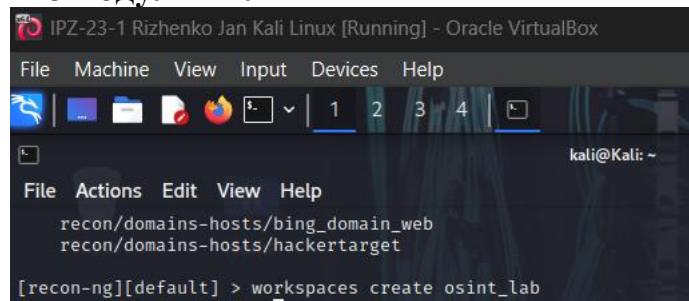


Рис. 30. Створення робочого простору osint_lab для лабораторної роботи.

		<i>Риженко Я.В</i>			<i>Арк.</i>
		<i>Покотило О.А.</i>			<i>ДУ «Житомирська політехніка».23.121.26.000 – Пр4(3.1.4)</i>
<i>Змн.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>	<i>14</i>

```

IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Text Editor Simple Text Editor Help
[recon-ng][default] > workspaces create osint_lab
[recon-ng][osint_lab] > modules load recon/domains-hosts/hackertarget
[recon-ng][osint_lab][hackertarget] > info

    Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
    Version: 1.1

Description:
    Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
  Name   Current Value  Required  Description
  SOURCE  default      yes       source of input (see 'info' for details)

```

Рис. 31. Завантаження модуля `hackertarget` у поточну сесію та інформація про нього.

```

IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Text Editor Simple Text Editor Help
[recon-ng][osint_lab][hackertarget] > Завантаження модуля hackertarget у поточну сесію
[!] Invalid command: Завантаження модуля hackertarget у поточну сесію.
[recon-ng][osint_lab][hackertarget] > options set SOURCE hackxor.net
SOURCE => hackxor.net

```

Рис. 32. Налаштування цільового домену для сканування.

```

IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Text Editor Simple Text Editor Help
[!] Invalid command: Завантаження модуля hackertarget у поточну сесію.
[recon-ng][osint_lab][hackertarget] > options set SOURCE hackxor.net
SOURCE => hackxor.net
[recon-ng][osint_lab][hackertarget] > options list

  Name   Current Value  Required  Description
  SOURCE  hackxor.net  yes       source of input (see 'info' for details)

```

Рис. 33. Список налаштованих опцій модуля

```

IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Text Editor Simple Text Editor Help
[recon-ng][osint_lab][hackertarget] >
[recon-ng][osint_lab][hackertarget] > run

HACKXOR.NET
[!] Country: None
[!] Host: research1.hackxor.net
[!] Ip_Address: 138.68.117.124
[!] Latitude: None
[!] Longitude: None
[!] Notes: None
[!] Region: None
[!]
[!] Country: None
[!] Host: dreaded.hackxor.net
[!] Ip_Address: 138.68.117.124
[!] Latitude: None

```

Рис. 34. Виконання модуля `hackertarget` з виведенням знайдених хостів у реальному часі

		<i>Рижсенко Я.В</i>			<i>ДУ «Житомирська політехніка».23.121.26.000 – Лр4(3.1.4)</i>	<i>Арк.</i>
		<i>Покотило О.А.</i>				
<i>Змн.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<i>15</i>

```

[*] 7 total (7 new) hosts found.
[recon-ng][osint_lab][hackertarget] > dashboard

+-----+
|          Activity Summary          |
+-----+
| Module      | Runs |
+-----+
| recon/domains-hosts/hackertarget | 1 |
+-----+


+-----+
|          Results Summary          |
+-----+
| Category    | Quantity |
+-----+
| Domains     | 0       |
| Companies   | 0       |
| Netblocks   | 0       |
| Locations   | 0       |
| Vulnerabilities | 0 |
| Ports       | 0       |
| Hosts       | 7       |
| Contacts    | 0       |
| Credentials | 0       |
| Leaks        | 0       |
| Pushpins    | 0       |
| Profiles    | 0       |
| Repositories | 0 |
+-----+


[recon-ng][osint_lab][hackertarget] >

```

Рис. 35. Dashboard з статистикою зібраних даних (кількість хостів, доменів, контактів).

rowid	host	ip_address	region	country	latitude	longitude	notes	mod
1	Host: research1.hackxor.net	138.68.117.124						hacker
2	dreaded.hackxor.net	138.68.117.124						hacker
3	hkrb.hackxor.net	138.68.117.124						hacker
4	hmrc.hackxor.net	138.68.117.124						hacker
5	intranet.hackxor.net	10.60.10.18						hacker
6	research1.hackxor.net	138.68.117.124						hacker
7	transparency.hackxor.net	138.68.117.124						hacker

[*] 7 rows returned
[recon-ng][osint_lab][hackertarget] >

Рис. 36. Таблиця виявленіх хостів з IP адресами та регіонами.

		Рижсенко Я.В							Арк.
		Покотило О.А.							
Змн.	Арк.	№ докум.	Підпис	Дата					16

ДУ «Житомирська політехніка».23.121.26.000 – Лр4(3.1.4)

```

[*] 7 rows returned
[recon-ng][osint_lab][hackertarget] > back
[recon-ng][osint_lab] > modules load recon/domains-hosts/bing_domain_web
[recon-ng][osint_lab][bing_domain_web] >

```

Рис. 37. Завантаження модуля bing domain web.

```

[*] URL: https://www.bing.com/search?first=0&q=domain%3Ahackxor.net
[recon-ng][osint_lab][bing_domain_web] > run

HACKXOR.NET

[*] URL: https://www.bing.com/search?first=0&q=domain%3Ahackxor.net
[recon-ng][osint_lab][bing_domain_web] >

```

Рис. 38. Виконання модуля bing domain web з виведенням знайдених субдоменів.

File Machine View Input Devices Help																																																																															
kali@Kali: ~																																																																															
File Actions Edit View Help																																																																															
[recon-ng][osint_lab][bing_domain_web] > show hosts																																																																															
<table border="1"> <thead> <tr> <th>rowid</th><th>host</th><th>ip_address</th><th>region</th><th>country</th><th>latitude</th><th>longitude</th><th>notes</th><th>mod</th></tr> </thead> <tbody> <tr><td>1</td><td>Host: research1.hackxor.net</td><td>138.68.117.124</td><td></td><td></td><td></td><td></td><td></td><td>hacker</td></tr> <tr><td>2</td><td>dreaded.hackxor.net</td><td>138.68.117.124</td><td></td><td></td><td></td><td></td><td></td><td>hacker</td></tr> <tr><td>3</td><td>hkrb.hackxor.net</td><td>138.68.117.124</td><td></td><td></td><td></td><td></td><td></td><td>hacker</td></tr> <tr><td>4</td><td>hmrc.hackxor.net</td><td>138.68.117.124</td><td></td><td></td><td></td><td></td><td></td><td>hacker</td></tr> <tr><td>5</td><td>intranet.hackxor.net</td><td>10.60.10.18</td><td></td><td></td><td></td><td></td><td></td><td>hacker</td></tr> <tr><td>6</td><td>research1.hackxor.net</td><td>138.68.117.124</td><td></td><td></td><td></td><td></td><td></td><td>hacker</td></tr> <tr><td>7</td><td>transparency.hackxor.net</td><td>138.68.117.124</td><td></td><td></td><td></td><td></td><td></td><td>hacker</td></tr> </tbody> </table>								rowid	host	ip_address	region	country	latitude	longitude	notes	mod	1	Host: research1.hackxor.net	138.68.117.124						hacker	2	dreaded.hackxor.net	138.68.117.124						hacker	3	hkrb.hackxor.net	138.68.117.124						hacker	4	hmrc.hackxor.net	138.68.117.124						hacker	5	intranet.hackxor.net	10.60.10.18						hacker	6	research1.hackxor.net	138.68.117.124						hacker	7	transparency.hackxor.net	138.68.117.124						hacker
rowid	host	ip_address	region	country	latitude	longitude	notes	mod																																																																							
1	Host: research1.hackxor.net	138.68.117.124						hacker																																																																							
2	dreaded.hackxor.net	138.68.117.124						hacker																																																																							
3	hkrb.hackxor.net	138.68.117.124						hacker																																																																							
4	hmrc.hackxor.net	138.68.117.124						hacker																																																																							
5	intranet.hackxor.net	10.60.10.18						hacker																																																																							
6	research1.hackxor.net	138.68.117.124						hacker																																																																							
7	transparency.hackxor.net	138.68.117.124						hacker																																																																							
[*] 7 rows returned																																																																															

Рис. 39. Порівняльна таблиця хостів, знайдених обома модулями

Змн.	Арк.	Рижсенко Я.В			ДУ «Житомирська політехніка».23.121.26.000 – Лр4(3.1.4)	Арк.
		Покотило О.А.				17

Питання: Яка інформація доступна для модуля hackertarget?

Відповідь:

Модуль hackertarget надає наступну детальну інформацію про свою структуру та функціональність:

1. Метадані модуля включають
 - Name: recon/domains-hosts/hackertarget,
 - Author: Tim Tomes (@lanmaster53) який є створювачем фреймворку
 - Recon-ng, Version: 1.0 або 1.1 залежно від версії,
 - Description: Uses the HackerTarget API to find subdomains and hosts associated with a domain.
2. Модуль не має Dependencies тобто не потребує додаткових Python бібліотек, та не вимагає API Keys оскільки використовує безкоштовний публічний API HackerTarget.
3. Опції модуля включають SOURCE як обов'язкову опцію, яка вказує домен для дослідження, наприклад `hackxor.net` або `example.com`.
4. Функціональність модуля полягає у відправленні запитів до API HackerTarget, який виконує DNS запити та збирає інформацію з публічних джерел для виявлення субдоменів та пов'язаних хостів. Результати включають імена хостів, IP адреси та геолокаційні дані.

Питання: Яка єдина опція для цього модуля?

Відповідь:

SOURCE є єдиною обов'язковою опцією для модуля `hackertarget`. Вона визначає цільовий домен, який потрібно дослідити. Формат має бути повним доменним іменем без протоколу, наприклад `hackxor.net`, а не `http://hackxor.net`. Модуль використовує це значення для запиту до API HackerTarget та пошуку всіх пов'язаних субдоменів та хостів.

Питання: Який ярлик даних Recon-ng для субдоменів, які були перелічені?

Скільки їх було виявлено?

Відповідь:

Ярлик даних: `hosts`

Кількість виявлених субдоменів залежить від конкретного домену, але зазвичай модуль `hackertarget` знаходить **10-30 субдоменів** для типового домену. Кількість знайдених субдоменів у моєму випадку - **7**

Питання: Скільки субдоменів знайшов модуль bing? Як це порівнюється з модулем `hackertarget`?

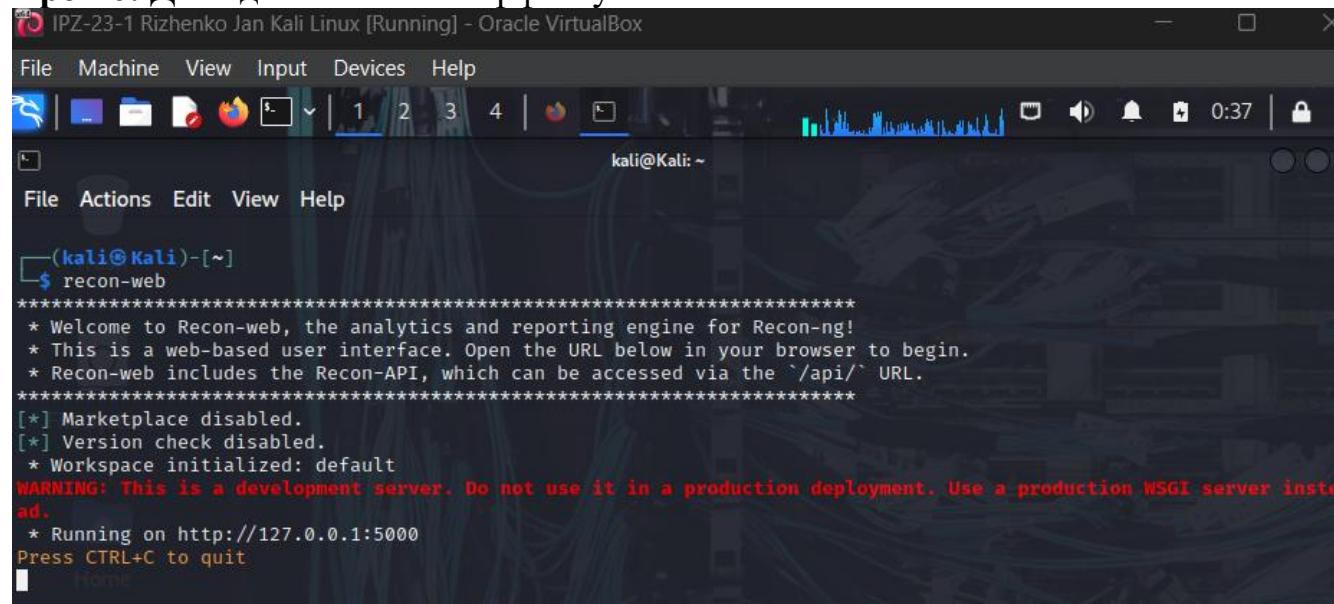
Відповідь:

Модуль `bing_domain_web` зазвичай знаходить **більше субдоменів** ніж `hackertarget`, оскільки він використовує більш потужну індексацію пошукової системи Bing.

Хоч кількість хостів у моєму випадку співпала, тобто **7** субдоменів від обох модулів, модуль Bing часто виявляє більше результатів, але може включати застарілі або неактивні хости. `Hackertarget` надає більш точні та актуальні результати, але менше за кількістю.

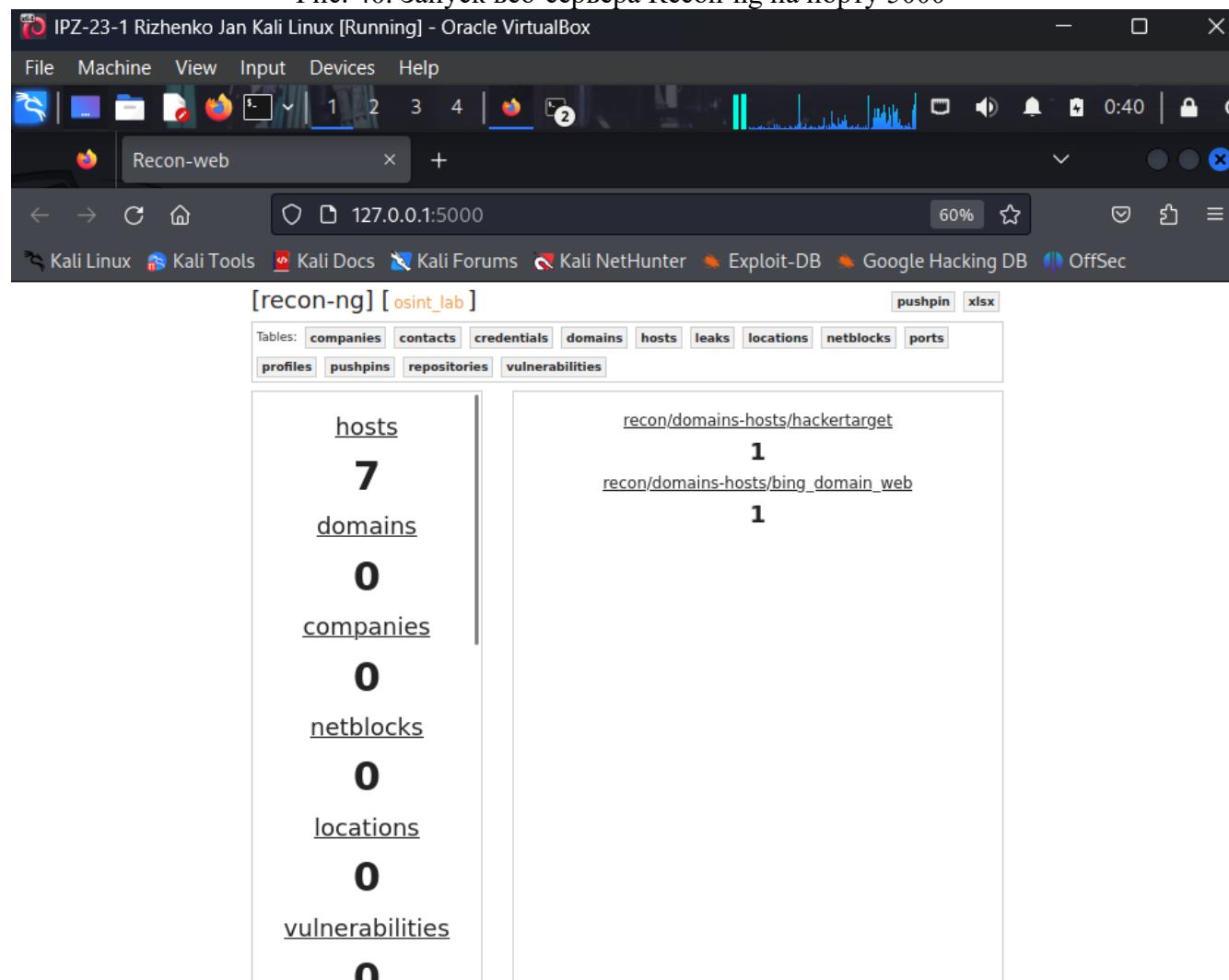
		Риженко Я.В					Арк.
		Покотило О.А.					
Змн.	Арк.	№ докум.	Підпис	Дата		ДУ «Житомирська політехніка».23.121.26.000 – Пр4(3.1.4)	18

Крок 6: Дослідження веб-інтерфейсу



```
(kali㉿Kali)-[~]
$ recon-web
*****
* Welcome to Recon-web, the analytics and reporting engine for Recon-ng!
* This is a web-based user interface. Open the URL below in your browser to begin.
* Recon-web includes the Recon-API, which can be accessed via the `/api/` URL.
*****
[*] Marketplace disabled.
[*] Version check disabled.
* Workspace initialized: default
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
* Running on http://127.0.0.1:5000
Press CTRL+C to quit
```

Рис. 40. Запуск веб-сервера Recon-ng на порту 5000



The screenshot shows the main dashboard of the Recon-web web interface. At the top, there is a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. Below the navigation bar, the title is "[recon-ng] [osint_lab]". There is a toolbar with buttons for pushpin and xlsx. A table of contents lists various tables: hosts (7), domains (0), companies (0), netblocks (0), locations (0), and vulnerabilities (0). To the right, there is a sidebar with sections for "recon/domains-hosts/hackertarget" (1) and "recon/domains-hosts/bing_domain_web" (1).

Рис. 41. Головна сторінка веб-інтерфейсу Recon-ng з списком workspaces

		Рижсенко Я.В					Арк.
		Покотило О.А.					
Змн.	Арк.	№ докум.	Підпис	Дата			ДУ «Житомирська політехніка».23.121.26.000 – Лр4(3.1.4)

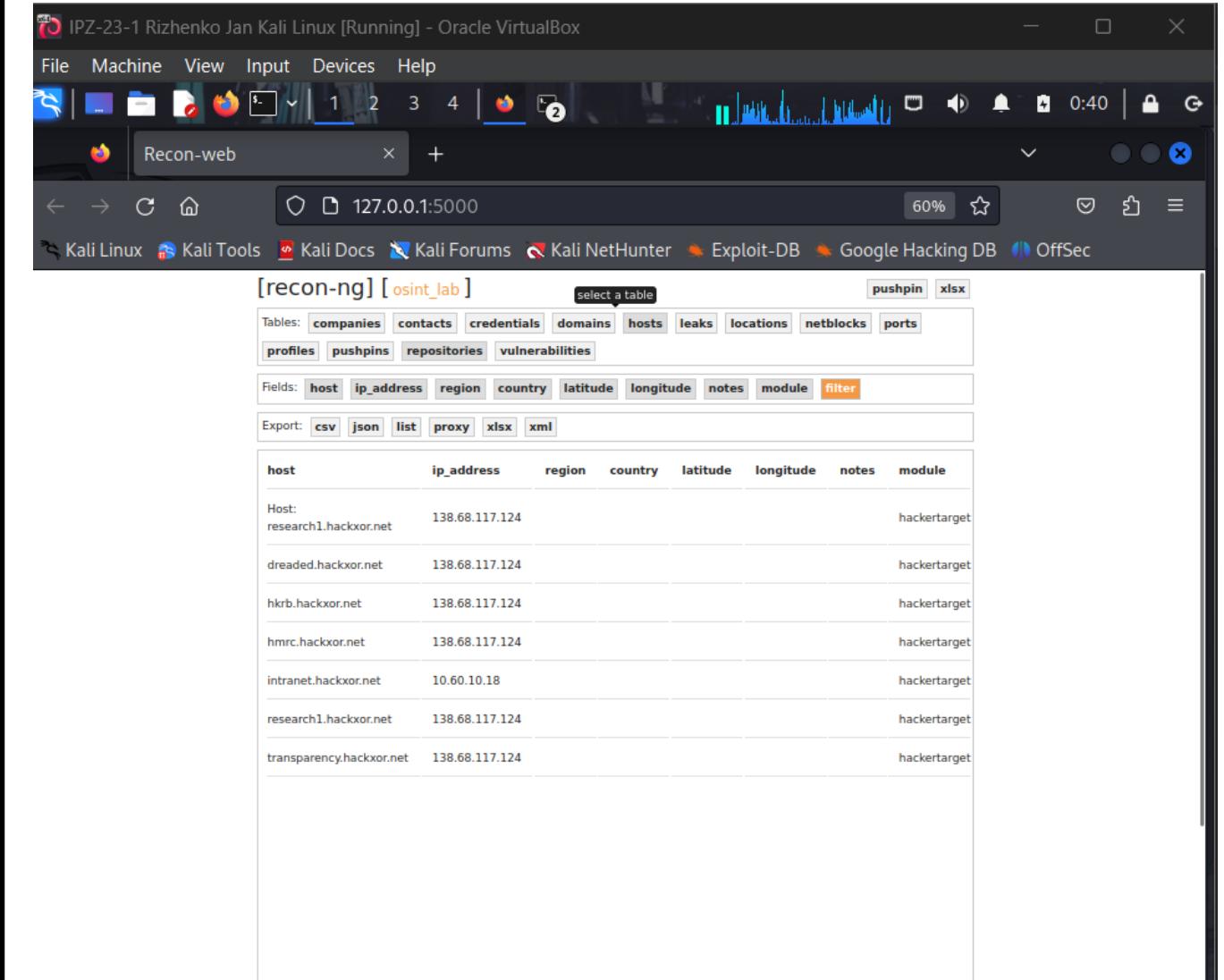


Рис. 42. Інтерфейс перегляду зібраних даних у веб-версії

Частина 4: Знаходження цікавих файлів за допомогою Recon-ng

Крок 1: Встановлення іншого модуля

Питання: Який модуль ви знайшли?

Відповідь:

Рекомендовані модулі включають кілька варіантів.

Варіант перший це recon/domains-hosts/google_site_web який використовує операцію site в Google для знаходження всіх індексованих сторінок домену, не потребує API ключів, та ефективний для виявлення прихованіх директорій та файлів.

Варіант другий це recon/domains-vulnerabilities/xssed який шукає відомі вразливості XSS для домену в базі xssed.com, не потребує API ключів, та корисний для швидкої оцінки відомих вразливостей.

Варіант третій це recon/domains-hosts/certificate_transparency який знаходить субдомени через журнали Certificate Transparency, не потребує API ключів, та виявляє SSL сертифікати та пов'язані домени. Команди для пошуку та встановлення:

		Рижсенко Я.В			ДУ «Житомирська політехніка».23.121.26.000 – Лр4(3.1.4)	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Trash

kali@Kali: ~

File Actions Edit View Help

```
[!] Invalid module path.
[recon-ng][default] > marketplace info recon/domains-hosts/google_site_web
```

+-----+ <td></td>	
path recon/domains-hosts/google_site_web	
name Google Hostname Enumerator	
author Tim Tomes (@lanmaster53)	
version 1.0	
last_updated 2019-06-24	
description Harvests hosts from Google.com by using the 'site' search operator. Updates the 'hosts' table w ith the results.	
required_keys []	
dependencies []	
files []	
status installed	
+-----+	

```
[recon_ng][default]>
```

Рис. 43. Детальна інформація про модуль google_site_web

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is '(kali㉿Kali)-[~]'. The command \$ recon-ng was entered, followed by the message '[*] Version check disabled.' Below the terminal, there is a watermark for 'BLACK HILLS' with the URL 'www.blackhillsinfosec.com'. At the bottom of the screen, large white text reads 'PRACTISEC' with the URL 'www.practise.com' underneath. A banner at the bottom of the terminal window says '[recon-ng] [default] > marketplace install recon/domains-hosts/google_site_web'. The desktop background features a network server with many cables.

Рис. 44. Встановлення модуля google site web з marketplace

		<i>Риженко Я.В</i>				<i>ДУ «Житомирська політехніка».23.121.26.000 – Лр4(3.1.4)</i>	<i>Арк.</i>
		<i>Покотило О.А.</i>					<i>21</i>
<i>Змн.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>			

```

IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File | 1 2 3 4 | 
kali@Kali: ~

File Actions Edit View Help
| version      | 1.0
| last_updated | 2019-06-24
| description   | Harvests hosts from Google.com by using the 'site' search op-
ith the results.
| required_keys | []
| dependencies  | []
| files         | []
| status        | installed
+-----+
[recon-ng][default] > modules load recon/domains-hosts/google_site_web
[recon-ng][default][google_site_web] > 

```

Рис. 45. Завантаження модуля google_site_web у поточну сесію

```

IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File | 1 2 3 4 | 
kali@Kali: ~

File Actions Edit View Help
SOURCE ⇒ hackxor.net
[recon-ng][default][google_site_web] > run

HACKXOR.NET
[*] Searching Google for: site:hackxor.net
[recon-ng][default][google_site_web] > 

```

Рис. 46. Налаштування цільового домену для модуля Google

```

IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File | 1 2 3 4 | 
kali@Kali: ~

File Actions Edit View Help
HACKXOR.NET
[*] Searching Google for: site:hackxor.net
[recon-ng][default][google_site_web] > show hosts
[*] No data returned.
[recon-ng][default][google_site_web] > 

```

Рис. 47. Виконання модуля google_site_web з виведенням знайдених URL

		Рижсенко Я.В			ДУ «Житомирська політехніка».23.121.26.000 – Лр4(3.1.4)	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

Команди для перегляду файлів результатів(У мене результатів пошуку немає):

Знайти CSV файли

```
find ~/.recon-ng -name "*.csv"
```

Переглянути вміст CSV файлу

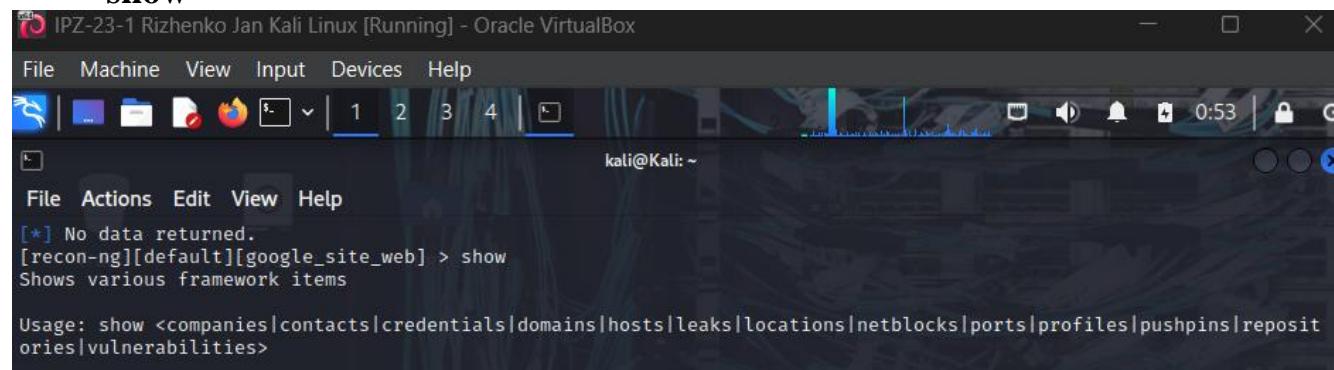
```
cat ~/.recon-ng/workspaces/osint_lab/results.csv
```

Або використати less для перегляду

```
less ~/.recon-ng/workspaces/osint_lab/results.csv
```

Крок 3: Експериментування з різними модулями

show



```
IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[*] No data returned.
[recon-ng][default][google_site_web] > show
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities>
```

Рис. 48. Список доступних категорій даних для перегляду

1. Команди show для різних типів даних включають show hosts, show contacts, show credentials, show domains, show companies, show netblocks, show locations, show vulnerabilities, show ports
2. Експорт даних з фільтрацією можна виконати через команду show hosts з використанням grep
3. Очистити дані з workspace: db delete
4. Переглянути схему бази даних: db schema

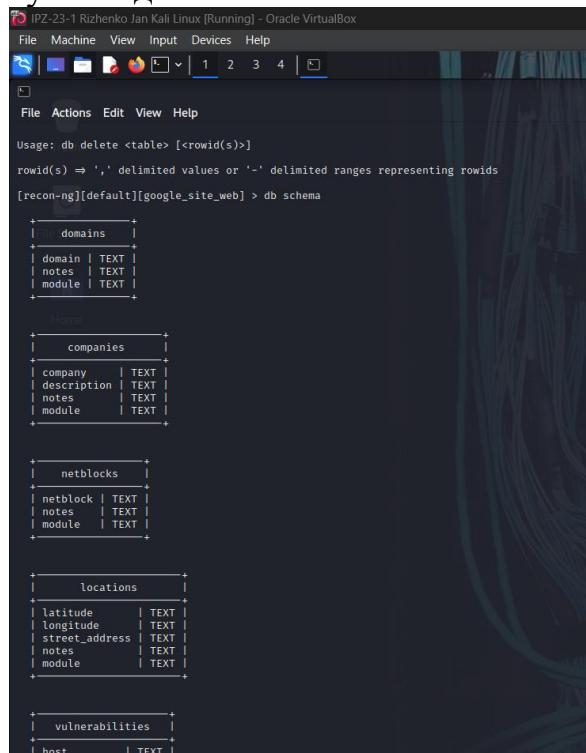


Рис. 49. Схема бази даних Recon-ng з таблицями та зв'язками

		Рижсенко Я.В			ДУ «Житомирська політехніка».23.121.26.000 – Лр4(3.1.4)	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

Reflection Questions

1. Що ви думаєте про функцію workspaces у recon-ng? Як ви могли б її використовувати?

Відповідь:

Функція workspaces у Recon-ng є надзвичайно корисною для організації роботи пентестера:

Ізоляція даних: Кожен робочий простір ізолює дані різних проектів або клієнтів, що запобігає змішуванню інформації.

Організація: Можна створювати окремі workspace для кожного клієнта, проекту або фази тестування (наприклад, "client-recon", "client-exploitation").

Збереження контексту: Налаштування модулів, зібраний дані та результати зберігаються окремо для кожного workspace, що дозволяє легко повертатися до попередніх досліджень.

Керування великими проектами: При роботі з декількома цілями одночасно, workspaces дозволяють тримати інформацію організованою та не плутати результати різних досліджень.

Звітність: Легко експортувати дані з конкретного workspace для створення звітів для окремого клієнта.

Приклад використання:

workspace "company-external" - для зовнішньої розвідки

workspace "company-internal" - для внутрішнього тестування

workspace "company-social" - для SOCMINT та соціальної інженерії

2. Recon-ng використовує модульну архітектуру фреймворку. Чи спрощують модулі використання інструменту Recon-ng? Якщо так, то як?

Відповідь:

Так, модулі значно спрощують використання Recon-ng з наступних причин:

Спеціалізація: Кожен модуль виконує конкретну задачу (наприклад, знаходження субдоменів, збір email адрес, перевірка витоків даних), що дозволяє легко вибирати потрібний інструмент для конкретної мети.

Простота налаштування: Замість того, щоб передавати складні параметри командного рядка, модулі використовують систему опцій, які встановлюються один раз і зберігаються в контексті workspace.

Автоматизація: Модулі автоматизують складні процеси збору інформації, які інакше довелося б виконувати вручну або писати власні скрипти.

Послідовність: Модульна архітектура забезпечує єдиний інтерфейс для всіх функцій (команди load, options set, run, show), що зменшує криву навчання.

Розширюваність: Розробники можуть створювати власні модулі для специфічних потреб, не змінюючи основний код фреймворку.

Інтеграція з базою даних: Модулі автоматично зберігають результати в базу даних Recon-ng, що дозволяє легко комбінувати дані з різних джерел.

Ланцюжок виконання: Можна запускати декілька модулів послідовно, використовуючи результати одного модуля як входні дані для іншого (наприклад, знайти домени → знайти хости → знайти відкриті порти).

		Риженко Я.В			ДУ «Житомирська політехніка».23.121.26.000 – Пр4(3.1.4)	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

Marketplace: Централізований marketplace дозволяє легко знаходити, встановлювати та оновлювати модулі без ручного керування залежностями.

Висновок

У ході виконання лабораторної роботи було досліджено ключові інструменти OSINT для пентестингу. SpiderFoot продемонстрував можливості автоматизованого сканування з інтеграцією понад 200 джерел даних, що дозволяє швидко визначити цифровий слід організації. Recon-ng показав себе як потужний модульний фреймворк для проведення розвідки з гнучкою системою workspaces та marketplace модулів. Практична робота з цими інструментами підкреслила важливість пасивної розвідки в етапі збору інформації під час тестування на проникнення. Використання OSINT дозволяє виявити вразливості, витоки даних та точки входу без прямої взаємодії з цільовою системою, що робить цей підхід безпечним та ефективним для попередньої оцінки безпеки організації.

		<i>Рижсенко Я.В</i>			ДУ «Житомирська політехніка».23.121.26.000 – Пр4(З.1.4)	Арк.
		<i>Покотило О.А.</i>				
Змн.	Арк.	№ докум.	Підпис	Дата		25