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 має велику цінність для пентестингу, оскільки дозволяє: Ідентифікувати облікові записи, які важливий персонал організації може мати на різних сайтах. Оскільки інші сайти можуть бути вразливими, існує можливість, що хакери можуть отримати доступ до особистої інформації персоналу з цих облікових записів, включаючи паролі, адреси та номери телефонів.

Типи сайтів, на яких персонал зареєстрований, також можуть надати деталі про їхнє життя та інтереси. Ці деталі можуть бути використані в атаках соціальної інженерії.

Виявити повторне використання паролів між різними сервісами.

Зібрати інформацію про цифровий слід організації та її співробітників.

Знайти потенційні точки входу для подальших атак.

Частина 2: Використання SpiderFoot

Крок 1: Запуск SpiderFoot

Команда для запуску:

```
┌──(kali㉿Kali)-[~]
└─$ spiderfoot -l 127.0.0.1:5001
```

Після запуску відкрийте браузер та введіть: http://127.0.0.1:5001

Крок 2: Дослідження SpiderFoot

Команда для перегляду всіх модулів:

```
┌──(kali㉿Kali)-[~]
└─$ spiderfoot -M | grep [search term]
```

Приклади використання grep:

Пошук модулів для email

```
└─$ spiderfoot -M | grep email
```

Пошук модулів для DNS

```
└─$ spiderfoot -M | grep dns
```

Пошук модулів для breach

```
└─$ spiderfoot -M | grep breach
```

Таблиця модулів SpiderFoot:

ТИП ІНФОРМАЦІЇ	НАЗВА СКАНЕРА/МОДУЛЯ	API КЛЮЧ ПОТРІБЕН? БЕЗКОШТОВНИЙ?	КОМЕНТАРІ
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	Ваш API ключ
Builtwith	Технології, використані для створення веб-сайту	[Ваш API ключ після реєстрації на builtwith.com]
Hunter.io	Email адреси, пов'язані з доменом	[Ваш API ключ після реєстрації на hunter.io]
Onion.link	Доступ до .onion сайтів через clearnet	Не потрібен API ключ
IntelligenceX	Витоки даних, паролі, документи	[Ваш API ключ після реєстрації на intelx.io]

Крок 4: Аналіз результатів сканування з API модулями

Питання: Який модуль сприяв 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

Частина 3: Дослідження Recon-ng
Крок 1: Створення робочого простору
Команди для запуску Recon-ng:

```
┌──(kali㉿Kali)-[~]
└─$ recon-ng
```

Команди для роботи з workspaces:

Переглянути допомогу по workspaces
[recon-ng][default] > workspaces help

Показати список workspaces
[recon-ng][default] > workspaces list

Створити новий workspace
[recon-ng][default] > workspaces create test

Перейти до іншого workspace
[recon-ng][test] > workspaces load [назва]

Видалити workspace
[recon-ng][default] > workspaces remove [назва]

Вийти з workspace (повернутися до default)
[recon-ng][test] > back
Питання: Як можна відобразити доступні робочі простори?
Відповідь:

[recon-ng][default] > workspaces list
Питання: Як можна видалити робочий простір?

Відповідь:

[recon-ng][default] > workspaces remove [назва_робочого_простору]
Питання: Яка команда вийде з робочого простору та поверне до головного Recon-ng prompt?
Відповідь:

[recon-ng][test] > back
Крок 2: Дослідження модулів
Команда для перегляду встановлених модулів:

[recon-ng][default] > modules search
Питання: Скільки модулів наразі доступні для вас?
Відповідь:
Зазвичай **0 модулів** встановлено за замовчуванням у свіжій установці Recon-ng v5 або новішої версії. Модулі повинні бути встановлені з marketplace. У marketplace доступно понад **90-100 модулів** для встановлення.
Крок 3: Дослідження marketplace модулів
Команди для роботи з marketplace:

Переглянути допомогу по marketplace
[recon-ng][default] > marketplace help

Показати всі доступні модулі в marketplace
[recon-ng][default] > marketplace search

Пошук модулів за ключовим словом
[recon-ng][default] > marketplace search bing
[recon-ng][default] > marketplace search shodan
[recon-ng][default] > marketplace search email

Інформація про конкретний модуль
[recon-ng][default] > marketplace info recon/domains-hosts/bing_domain_web

Встановити модуль
[recon-ng][default] > marketplace install recon/domains-hosts/bing_domain_web

Видалити модуль
[recon-ng][default] > marketplace remove recon/domains-hosts/bing_domain_web

Оновити всі модулі
[recon-ng][default] > marketplace refresh
Питання: Модульні таблиці мають колонки для D та K. Знайдіть shodan модулі. Які вимоги до цих модулів?

Відповідь:
При пошуку shodan модулів:

[recon-ng][default] > marketplace search shodan
D (Dependencies) - позначає, що модуль має залежності (зазвичай позначено зірочкою * якщо є)
K (Keys) - позначає, що модуль потребує API ключі (зазвичай позначено зірочкою * якщо потрібні)
Всі shodan модулі потребують **API ключ Shodan** (K = *), оскільки Shodan є платною службою з безкоштовним базовим рівнем. Shodan надає обмежену кількість безкоштовних запитів, але для повної функціональності потрібна платна підписка.
Крок 4: Встановлення нового модуля
Питання: Який модуль ви знайшли (що не потребує залежностей або API ключів)?
Відповідь:

[recon-ng][default] > marketplace search bing
Модуль: recon/domains-hosts/bing_domain_web
Цей модуль використовує пошукову систему Bing для знаходження субдоменів та хостів, пов'язаних з доменом, і не потребує API ключів або додаткових залежностей.
Команди для встановлення:

Переглянути інформацію про модуль
[recon-ng][default] > marketplace info recon/domains-hosts/bing_domain_web

Встановити модуль
[recon-ng][default] > marketplace install recon/domains-hosts/bing_domain_web

Встановити модуль hackertarget
[recon-ng][default] > marketplace install recon/domains-hosts/hackertarget

Перевірити встановлені модулі
[recon-ng][default] > modules search
Крок 5: Запуск нових модулів
Команди для роботи з модулями:

Створити новий workspace
[recon-ng][default] > workspaces create osint_lab

Завантажити модуль hackertarget
[recon-ng][osint_lab] > modules load recon/domains-hosts/hackertarget

Переглянути інформацію про модуль

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

Встановити опцію SOURCE
[recon-ng][osint_lab][hackertarget] > options set SOURCE hackxor.net

Переглянути налаштовані опції
[recon-ng][osint_lab][hackertarget] > options list

Запустити модуль
[recon-ng][osint_lab][hackertarget] > run

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

Показати знайдені хости
[recon-ng][osint_lab][hackertarget] > show hosts

Повернутися назад
[recon-ng][osint_lab][hackertarget] > back

Завантажити модуль bing
[recon-ng][osint_lab] > modules load recon/domains-hosts/bing_domain_web

Встановити опцію SOURCE
[recon-ng][osint_lab][bing_domain_web] > options set SOURCE hackxor.net

Запустити модуль
[recon-ng][osint_lab][bing_domain_web] > run

Переглянути результати
[recon-ng][osint_lab][bing_domain_web] > show hosts

Питання: Яка інформація доступна для модуля hackertarget?
Відповідь:
Модуль hackertarget надає наступну інформацію:
Name: recon/domains-hosts/hackertarget
Author: Tim Tomes (@lanmaster53)
Version: 1.0
Description: Uses the HackerTarget API to find subdomains and hosts associated with a domain
Options: SOURCE (domain to investigate)
Dependencies: None
API Keys: None required (використовує безкоштовний публічний API)

Питання: Яка єдина опція для цього модуля?
Відповідь:

SOURCE - домен, який потрібно дослідити (наприклад, hackxor.net)
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. Точна кількість відображається в dashboard або за допомогою команди show hosts.
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.
Наприклад:
hackertarget: 15-25 субдоменів
bing_domain_web: 30-50+ субдоменів
Модуль Bing часто виявляє більше результатів, але може включати застарілі або неактивні хости. Hackertarget надає більш точні та актуальні результати, але менше за кількістю.
Крок 6: Дослідження веб-інтерфейсу
Команди для запуску веб-інтерфейсу:

Відкрити новий термінал

```
┌──(kali㉿Kali)-[~]
└─$ recon-web
```

Веб-інтерфейс буде доступний за адресою:
http://127.0.0.1:5000
У браузері перейдіть на http://127.0.0.1:5000 для доступу до веб-інтерфейсу Recon-ng.
Частина 4: Знаходження цікавих файлів за допомогою Recon-ng
Крок 1: Встановлення іншого модуля
Питання: Який модуль ви знайшли?
Відповідь:
Варіант 1: recon/domains-vulnerabilities/xssed
Варіант 2: recon/domains-hosts/google_site_web
Варіант 3: recon/domains-hosts/certificate_transparency
Команди для пошуку та встановлення:

Пошук модулів для знаходження файлів

```
[recon-ng][default] > marketplace search google
[recon-ng][default] > marketplace search xss
[recon-ng][default] > marketplace search certificate
```

Переглянути інформацію про модуль
[recon-ng][default] > marketplace info recon/domains-hosts/google_site_web

Встановити модуль
[recon-ng][default] > marketplace install recon/domains-hosts/google_site_web

Завантажити модуль
[recon-ng][default] > modules load recon/domains-hosts/google_site_web
Обидва модулі можуть виявляти цікаві файли в домені:
xssed - шукає відомі вразливості XSS для домену
google_site_web - використовує оператор site: Google для знаходження індексованих файлів та сторінок домену
certificate_transparency - знаходить субдомени через журнали Certificate Transparency
Крок 2: Запуск нового модуля
Команди для запуску модуля:

Завантажити модуль
[recon-ng][osint_lab] > modules load recon/domains-hosts/google_site_web

Встановити опцію SOURCE
[recon-ng][osint_lab][google_site_web] > options set SOURCE hackxor.net
або
[recon-ng][osint_lab][google_site_web] > options set SOURCE h4cker.org

Запустити модуль
[recon-ng][osint_lab][google_site_web] > run

Переглянути результати
[recon-ng][osint_lab][google_site_web] > show hosts

Файли зберігаються в
/root/.recon-ng/workspaces/[workspace_name]/
або
/home/kali/.recon-ng/workspaces/[workspace_name]/
Команди для перегляду файлів результатів:

Знайти CSV файли
```
┌──(kali㉿Kali)-[~]
└─$ find ~/.recon-ng -name "*.csv"
```

Переглянути вміст CSV файлу
```
┌──(kali㉿Kali)-[~]
└─$ cat ~/.recon-ng/workspaces/osint_lab/results.csv
```

Або використати less для перегляду

```
┌──(kali㉿Kali)-[~]
└─$ less ~/.recon-ng/workspaces/osint_lab/results.csv
```

Крок 3: Експериментування з різними модулями

Додаткові корисні команди:

Експорт результатів у різних форматах

```
[recon-ng][osint_lab] > show
```

Доступні категорії для show:

```
[recon-ng][osint_lab] > show hosts
[recon-ng][osint_lab] > show contacts
[recon-ng][osint_lab] > show credentials
[recon-ng][osint_lab] > show domains
[recon-ng][osint_lab] > show companies
[recon-ng][osint_lab] > show netblocks
[recon-ng][osint_lab] > show locations
[recon-ng][osint_lab] > show vulnerabilities
[recon-ng][osint_lab] > show ports
```

Експорт даних

```
[recon-ng][osint_lab] > show hosts | grep -i "[ключове_слово]"
```

Очистити дані з workspace

```
[recon-ng][osint_lab] > db delete
```

Переглянути схему бази даних

```
[recon-ng][osint_lab] > db schema
```

Приклади інших корисних модулів:

Модулі для збору email адрес

```
marketplace install recon/domains-contacts/whois_pocs
marketplace install recon/domains-contacts/pgp_search
```

Модулі для збору інформації про компанії

```
marketplace install recon/companies-contacts/jigsaw_search
marketplace install recon/companies-domains/viewdns_reverse_whois
```

Модулі для перевірки витоків

```
marketplace install recon/domains-credentials/pwnedlist_domain
```

Модулі для геолокаціїb

```
marketplace install recon/hosts-hosts/resolve
marketplace install recon/netblocks-hosts/reverse_resolve
```

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, зібрані 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 вибрати 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 вхідні дані для іншого (наприклад, знайти домени → знайти хости → знайти відкриті порти).
Marketplace: Централізований marketplace дозволяє легко знаходити, встановлювати та оновлювати модулі без ручного керування залежностями.

Приклад робочого процесу:

Встановити модулі
[recon-ng][default] > marketplace install recon/domains-hosts/hackertarget
[recon-ng][default] > marketplace install recon/hosts-ports/shodan_ip

Завантажити та запустити перший модуль
[recon-ng][default] > modules load recon/domains-hosts/hackertarget
[recon-ng][default][hackertarget] > options set SOURCE example.com
[recon-ng][default][hackertarget] > run

Результати автоматично збережені в БД
[recon-ng][default][hackertarget] > show hosts

Використати знайдені хости для наступного сканування
[recon-ng][default][hackertarget] > back
[recon-ng][default] > modules load recon/hosts-ports/shodan_ip
[recon-ng][default][shodan_ip] > run
Модульна архітектура робить Recon-ng потужним, але інтуїтивно зрозумілим інструментом, який дозволяє навіть початківцям проводити складні OSINT дослідження.

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.