Лабораторна робота №13(4.4.7)
Дослідження Social Engineer Toolkit (SET)
Хід роботи:

Частина 1: Запуск SET та дослідження інструментарію

Крок 1: Завантаження додатку SET

Завдання: Запустіть Social Engineer Toolkit з правами root

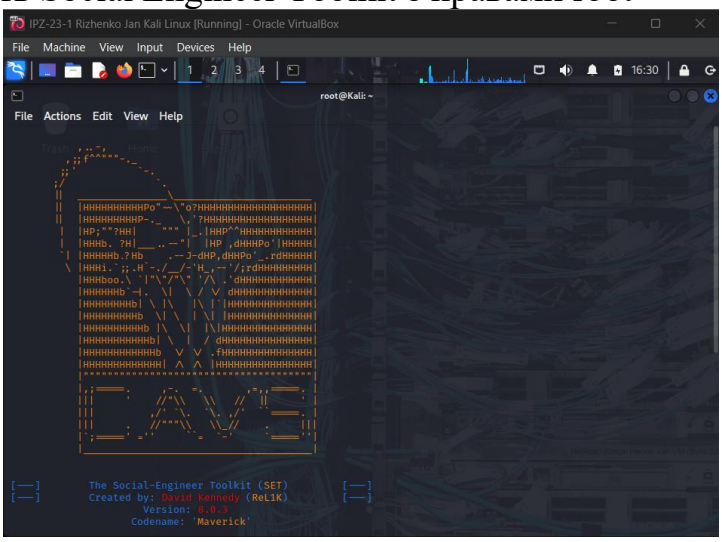

Рис. 1. Головне меню Social Engineer Toolkit з основними категоріями атак.

Крок 2: Дослідження доступних атак соціальної інженерії

Завдання: Ознайомтесь з меню атак соціальної інженерії

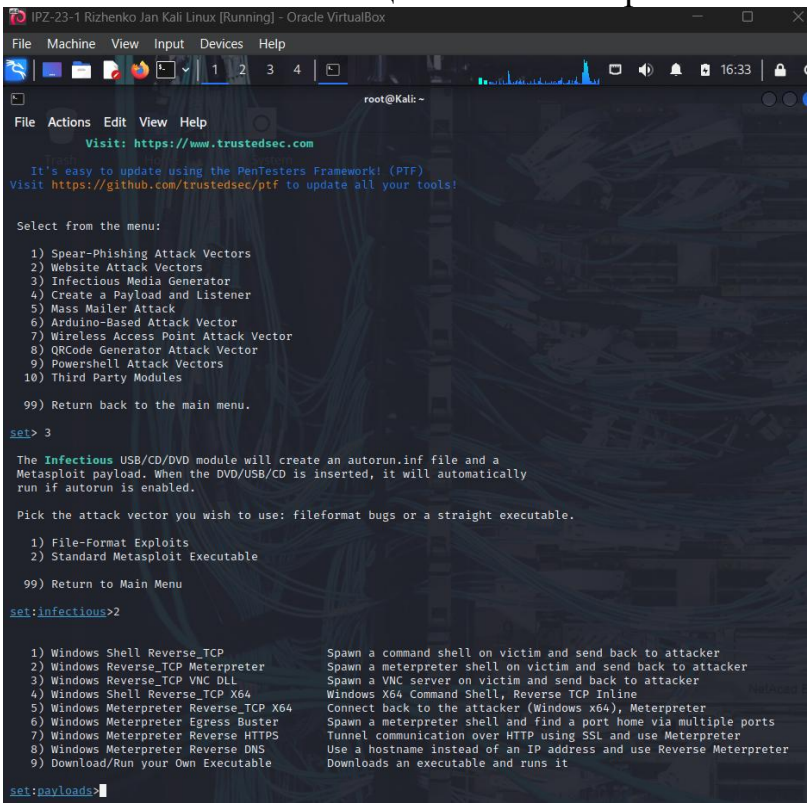

Рис. 2. Підменю атак соціальної інженерії з доступними векторами атак.

Питання: Яка опція створює DVD або USB флешку, що автоматично запускає шкідливе ПЗ при вставці в цільовий пристрій?
Відповідь: Опція 3) Infectious Media Generator створює заражені носії DVD або USB, які автоматично виконують шкідливий код при підключенні до цільового комп'ютера завдяки функції autorun операційної системи.
Питання: Як ця функціональність може бути використана в тесті на проникнення?
Відповідь: У тесті на проникнення цю функціональність можна використати для перевірки фізичної безпеки організації, залишивши підготовлені USB флешки у стратегічних місцях (парковка, приймальня, кафетерій) щоб оцінити, чи підключають їх співробітники до корпоративних комп'ютерів. Це тестує ефективність навчання персоналу щодо використання невідомих носіїв інформації та виявляє потенційні точки входу для реальних зловмисників.
Частина 2: Клонування веб-сайту для отримання облікових даних
Крок 1: Дослідження векторів веб-атак у SET
Завдання: Оберіть тип атаки для клонування веб-сайту

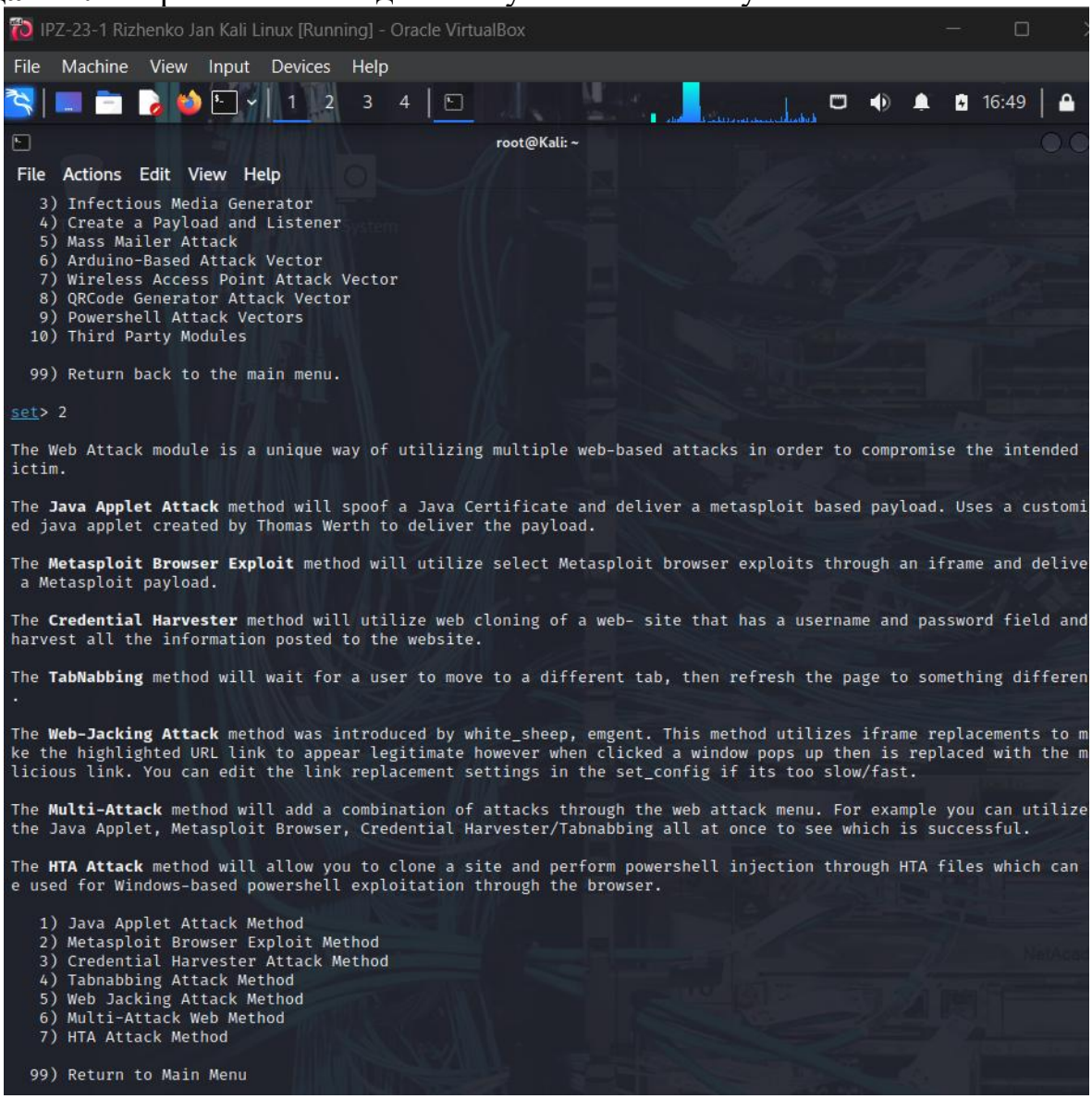

Рис. 3. Меню векторів веб-атак з різними методами експлуатації

Питання: Який тип атаки ви оберете для створення клонованого веб-сайту з метою отримання облікових даних користувачів?
Відповідь: Для отримання облікових даних користувачів необхідно обрати опцію 3) Credential Harvester Attack Method. Цей метод створює точну копію веб-сторінки входу, яка перехоплює всі дані форм (логіни та паролі), що вводяться користувачами, після чого перенаправляє їх на справжній сайт, не викликаючи підозр.
Завдання: Оберіть метод збору облікових даних

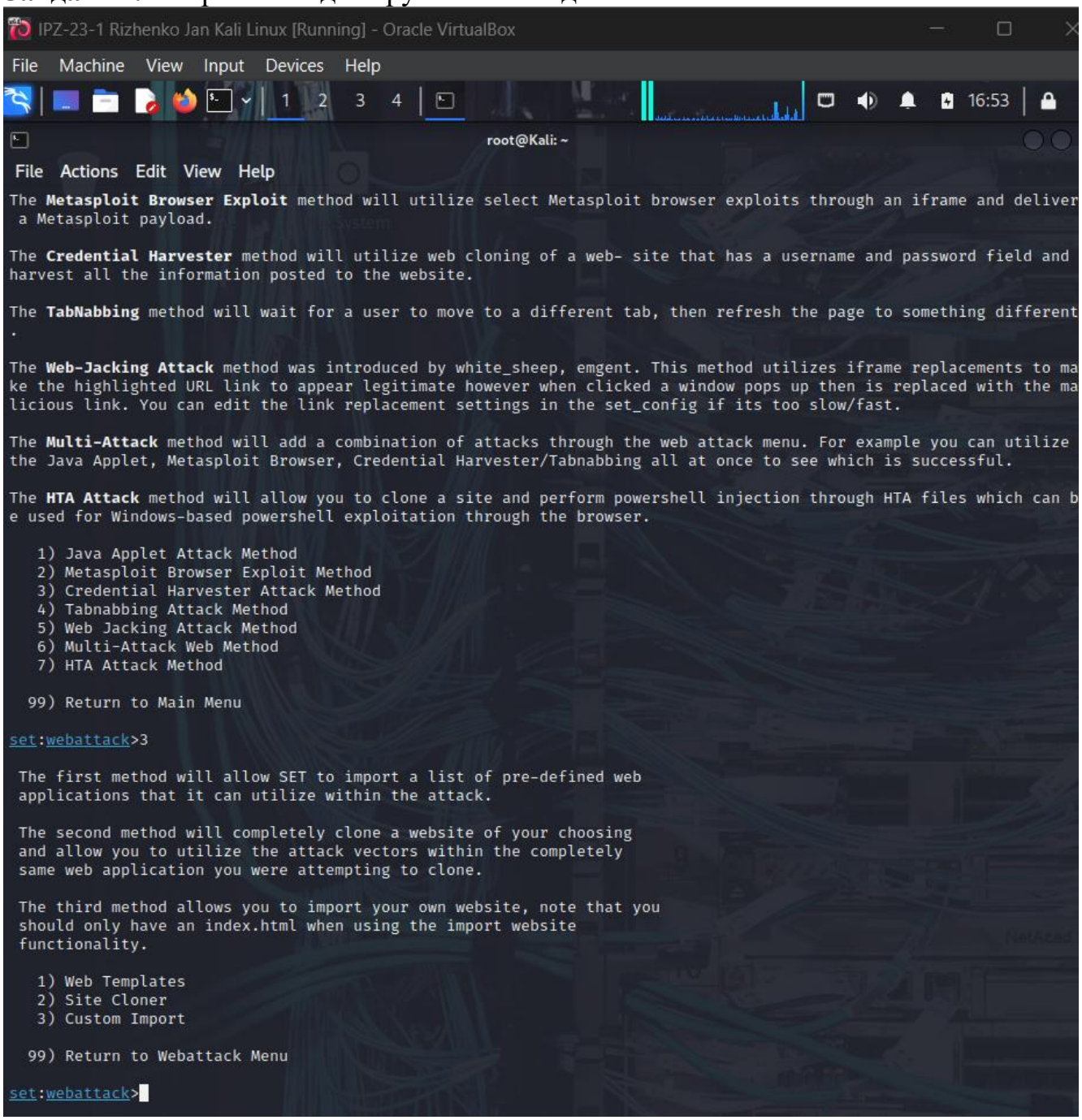

Рис. 4. Меню методів Credential Harvester з варіантами конфігурації

Питання: Який метод дозволяє використовувати власний веб-сайт для експлойту?

Відповідь: Метод 3) Custom Import дозволяє використовувати власний створений HTML файл веб-сайту для експлойту. Це надає максимальну гнучкість у налаштуванні фішингової сторінки під конкретні потреби тесту на проникнення.

Крок 2: Клонування сторінки входу DVWA.vm

Завдання: Створіть клон веб-сайту DVWA.vm для перехоплення облікових даних

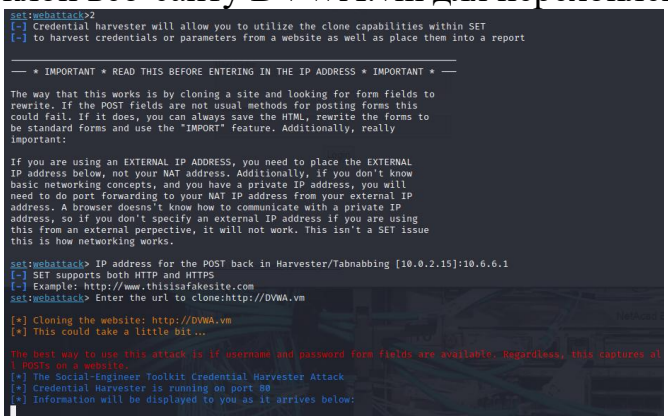

Рис. 5-6. Процес клонування веб-сайту DVWA з відображенням статусу операції, активний Credential Harvester, що очікує на підключення жертв

Питання: Яка URL-адреса сторінки входу?

Відповідь: URL-адреса оригінальної сторінки входу DVWA: http://DVWA.vm/login.php або http://10.6.6.13/login.php

Частина 3: Перехоплення та перегляд облікових даних

Крок 1: Створення експлойту соціальної інженерії

Завдання: Створіть HTML документ для перенаправлення на фальшивий сайт

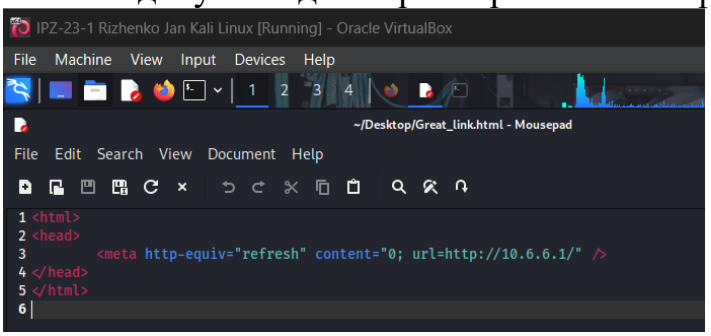

Рис. 7. Створення HTML файлу з перенаправленням на клонований сайт

Крок 2: Перехоплення облікових даних користувача

Завдання: Симулюйте вхід користувача для перехоплення даних

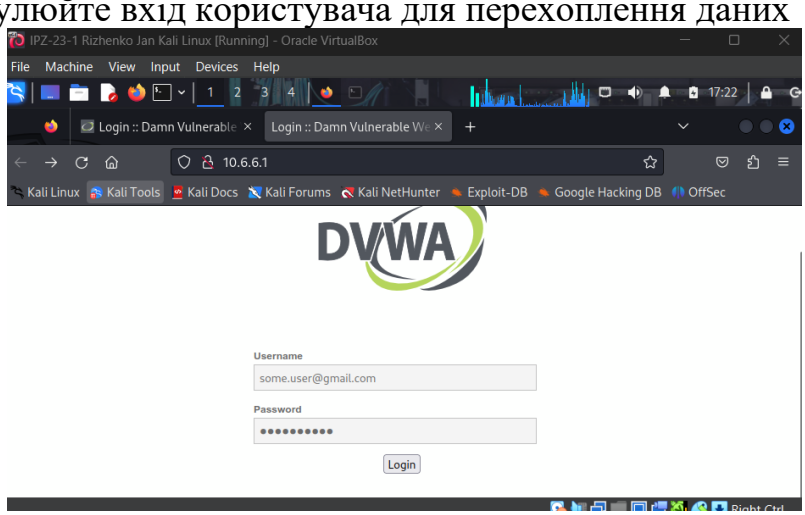

Рис. 8. Клонована сторінка входу DVWA з полями для введення облікових даних.

Питання: Яка URL відображається в браузері зараз? Чи збігається вона з URL, записаною в Частині 2, Крок 2?
Відповідь: Після відкриття Great_link.html у браузері відображається URL http://10.6.6.1/, яка відрізняється від оригінальної URL http://DVWA.vm/login.php або http://10.6.6.13/login.php. Це IP-адреса атакуючої машини Kali, де розміщено клонований сайт, а не справжній веб-сервер DVWA.
Питання: Яка URL після введення інформації та натискання кнопки Login? Чи збігається вона з URL, записаною в Частині 2, Крок 2?
Відповідь: Після натискання кнопки Login URL змінюється на оригінальну адресу справжнього сайту http://DVWA.vm/login.php або http://10.6.6.13/login.php. Це відбувається тому, що SET автоматично перенаправляє користувача на справжній веб-сайт після перехоплення облікових даних, щоб не викликати підозр у жертви.
Питання: Що сталося?
Відповідь: Відбулася атака типу credential harvesting. Користувач відкрив фішинговий HTML файл, який перенаправив його на клонований сайт, розміщений на машині атакуючого (10.6.6.1). Коли користувач ввів облікові дані та натиснув Login, SET перехопив всі дані форми (username, password, user_token) через POST запит. Після цього система автоматично перенаправила користувача на справжній сайт DVWA, щоб створити враження нормальної роботи та приховати факт компрометації даних. Весь процес відбувся непомітно для користувача.
Крок 3: Перегляд перехоплених даних
Завдання: Проаналізуйте перехоплену інформацію в терміналі SET

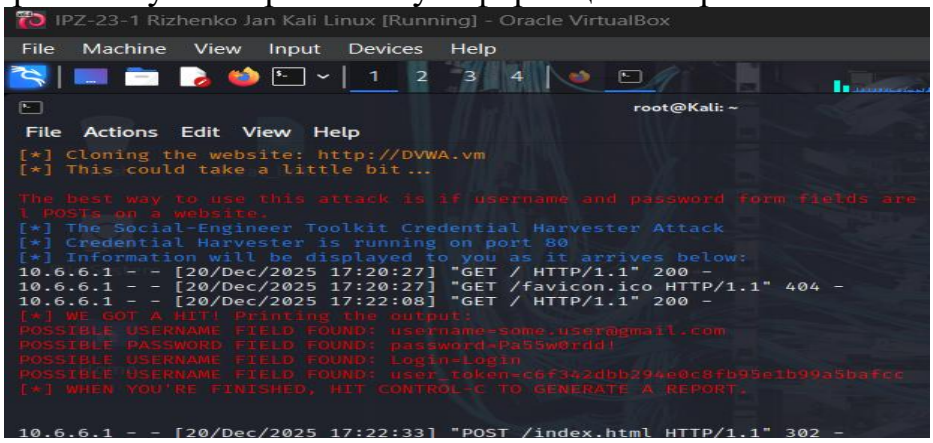

Рис. 9. Перехоплені облікові дані у термінальному виводі SET.

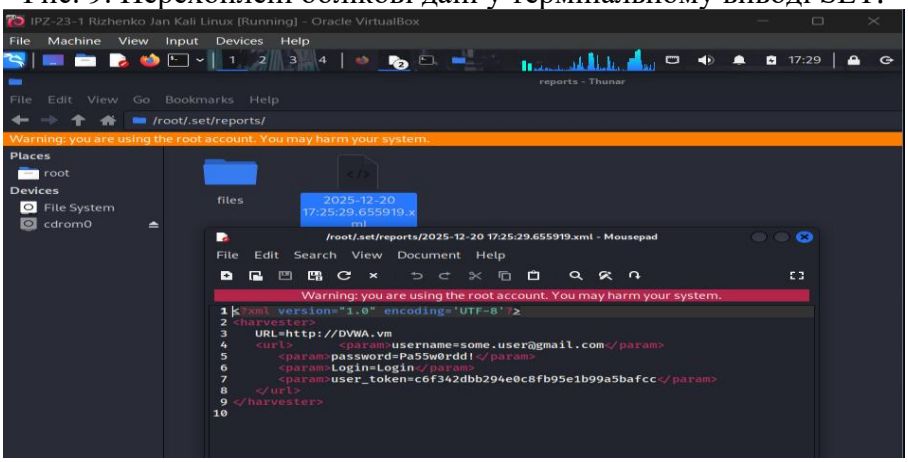

Рис. 10. Вміст XML звіту з детальною інформацією про перехоплені дані форми.

Питання: Яку інформацію зібрала клонована веб-сторінка?
Відповідь: Клонована веб-сторінка зібрала повну інформацію з форми входу: ім'я користувача (username=some.user@gmail.com), пароль у відкритому вигляді (password=Pa55w0rdd!), інформацію про натиснуту кнопку (Login=Login) та токен безпеки користувача (user_token=69c0375a6ee98b96a5b643eed1e97f94). Всі ці дані були перехоплені через POST запит до фальшивого сервера на машині атакуючого і збережені у XML файлі для подальшого аналізу.
Питання: Що тестувальник на проникнення може зробити з цією інформацією?
Відповідь: Тестувальник на проникнення може використати перехоплені облікові дані для входу в справжню систему DVWA від імені користувача, отримавши несанкціонований доступ до внутрішніх ресурсів. User token можна використати для обходу захисту CSRF (Cross-Site Request Forgery). Зібрані дані демонструють вразливість персоналу до фішингових атак і можуть бути включені в звіт про тестування безпеки з рекомендаціями щодо покращення навчання користувачів, впровадження багатофакторної автентифікації та систем виявлення фішингу.

Рефлексивне питання
Питання: Як етичний хакер може використати цю процедуру в тесті?
Відповідь: Етичний хакер може використати цю процедуру для оцінки людського фактора безпеки організації шляхом проведення контрольованої фішингової кампанії. Процес включає отримання письмового дозволу від керівництва, створення реалістичних фішингових email з посиланнями на клоновані сторінки входу корпоративних систем, відстеження, які співробітники вводять свої облікові дані, та документування результатів без фактичного використання отриманих даних для несанкціонованого доступу. Результати тесту виявляють рівень обізнаності персоналу про фішинг, ефективність поточних програм навчання безпеці, та допомагають організації розробити цільові освітні програми для груп співробітників з високим ризиком. Також тест може виявити технічні проблеми, такі як відсутність двофакторної автентифікації, слабкі політики паролів, недостатнє фільтрування email або відсутність систем моніторингу підозрілих URL.

Висновок: У процесі виконання лабораторної роботи було практично освоєно Social Engineer Toolkit для проведення атак соціальної інженерії в контрольованому середовищі Kali Linux. Використовуючи функціонал Credential Harvester Attack Method, було створено точну копію сторінки входу DVWA.vm, яка успішно перехопила тестові облікові дані користувача, включаючи логін, пароль та CSRF токен. Експеримент продемонстрував, як зловмисники можуть використовувати клонування веб-сайтів для крадіжки облікових даних через фішингові атаки, автоматично перенаправляючи жертв на справжні сайти для приховування факту компрометації. Робота підтвердила критичну важливість навчання користувачів розпізнавати фішингові атаки через перевірку URL-адрес, впровадження багатофакторної автентифікації та регулярного проведення тестів на проникнення для оцінки людського фактора безпеки організації.