PsychoBreak_THM

ENumuration

IN main Source code,we find a hidden directory /sadistRoom

we get a secret key 532219a04ab7a02b56faafbec1a4c1ea
and got redirected to a page where we use the key

THe page has a time limit to use the key so we use burp

NOw we get another key which is to be decode and to be used with a map Tizmg_nv_zxxvhh_gl_gsv_nzk_kovzhv

Decoded message is Grant_me_access_to_the_map_please

Now in safeheaven link we have to find keepers key

tried stegging the images but didnt work.Directory bruteforcing gave a keepers dir and from there we had to do some osint of a apic for answer and we got the key 48ee41458eb0b43bf82b986cecf3af01

NO in abondonedroom directory we get a hint in source code that theres a shell in this page. so tried adding a shell paramatere and execute a command and it worked..

in the shell we tried commands but werent executing. ls .. list contents of prevoius directories

we get two hashes and we crack them

I found that those hashes were directoires .I found out because one hash was the directory we weere currently in

We got a zip file and install it in our machine

We get a jpg file and upon string reading it we see a key.wav file in it

Its a morse code so we decode it using a morse decoder online and we get “SHOWME”

Then we use this code to extract from JOsephoday.jpg

we get ftp username and password joseph:intotheterror445

we get a dictionary file and a binary

we need to bruteforce the right key to run the binary so we used a python scipt which will do that for us

The key is kidman and we get a random hex numbers 55 444 3 6 2 66 7777 7 2 7777 7777 9 666 777 3 444 7777 7777 666 7777 8 777 2 66 4 33

It is multi tap cipher and output is KIDMANSPASSWORDISSOSTRANGE

NMAP

```
PORT    STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.5a
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 44:2f:fb:3b:f3:95:c3:c6:df:31:d6:e0:9e:99:92:42 (RSA)
|   256 92:24:36:91:7a:db:62:d2:b9:bb:43:eb:58:9b:50:14 (ECDSA)
|_  256 34:04:df:13:54:21:8d:37:7f:f8:0a:65:93:47:75:d0 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Welcome To Becon Mental Hospital
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), Linux 5.4 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 3.1
```

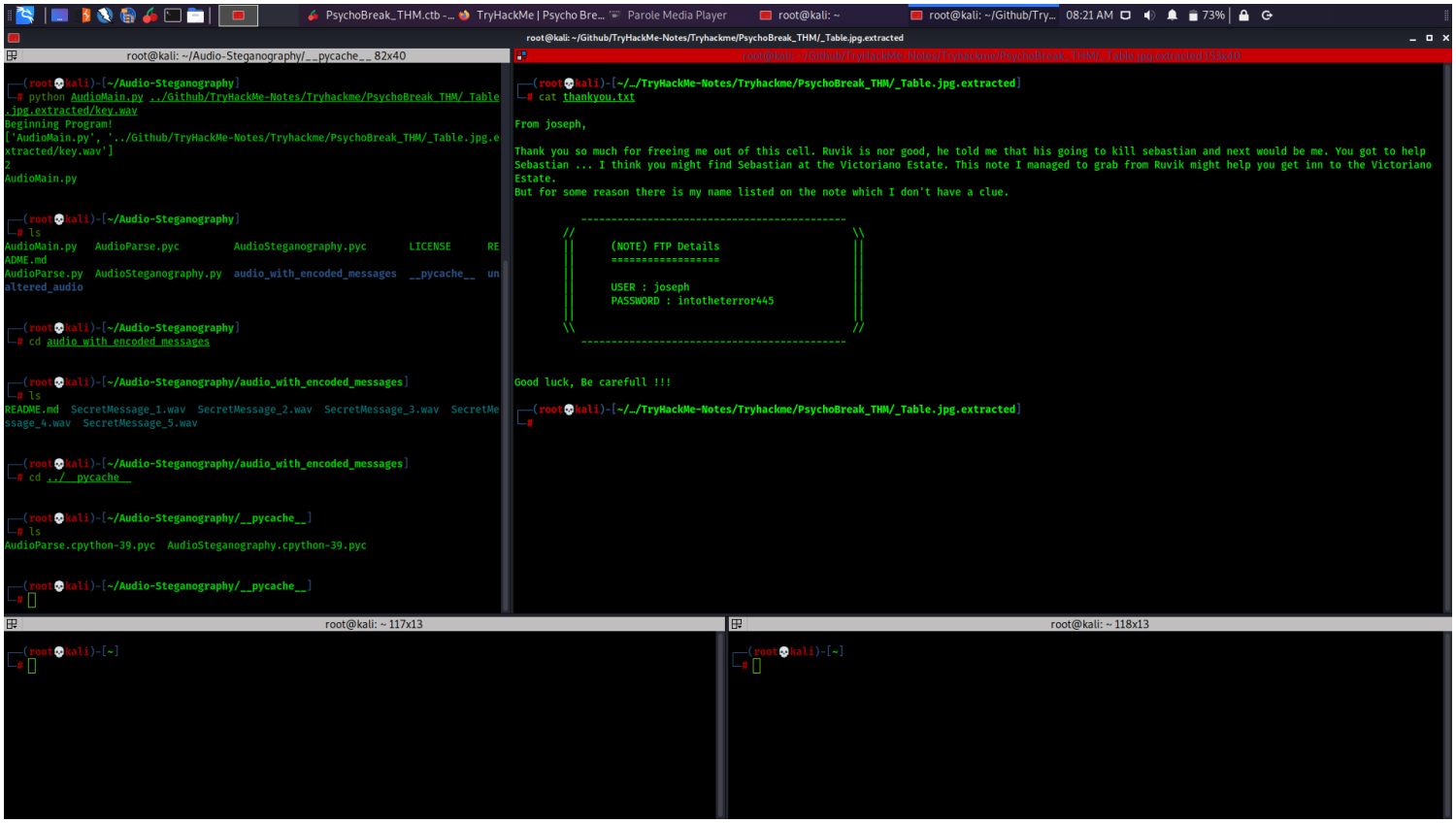
(93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Sony Android TV (Android 5.0) (92%), Android 5.0 - 6.0.1 (Linux 3.4) (92%), Android 5.1 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 203.95 ms 10.4.0.1
2 ... 3
4 459.73 ms 10.10.78.54

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.48 seconds

FTP:21

#



#

SSH:22

HTTP:80

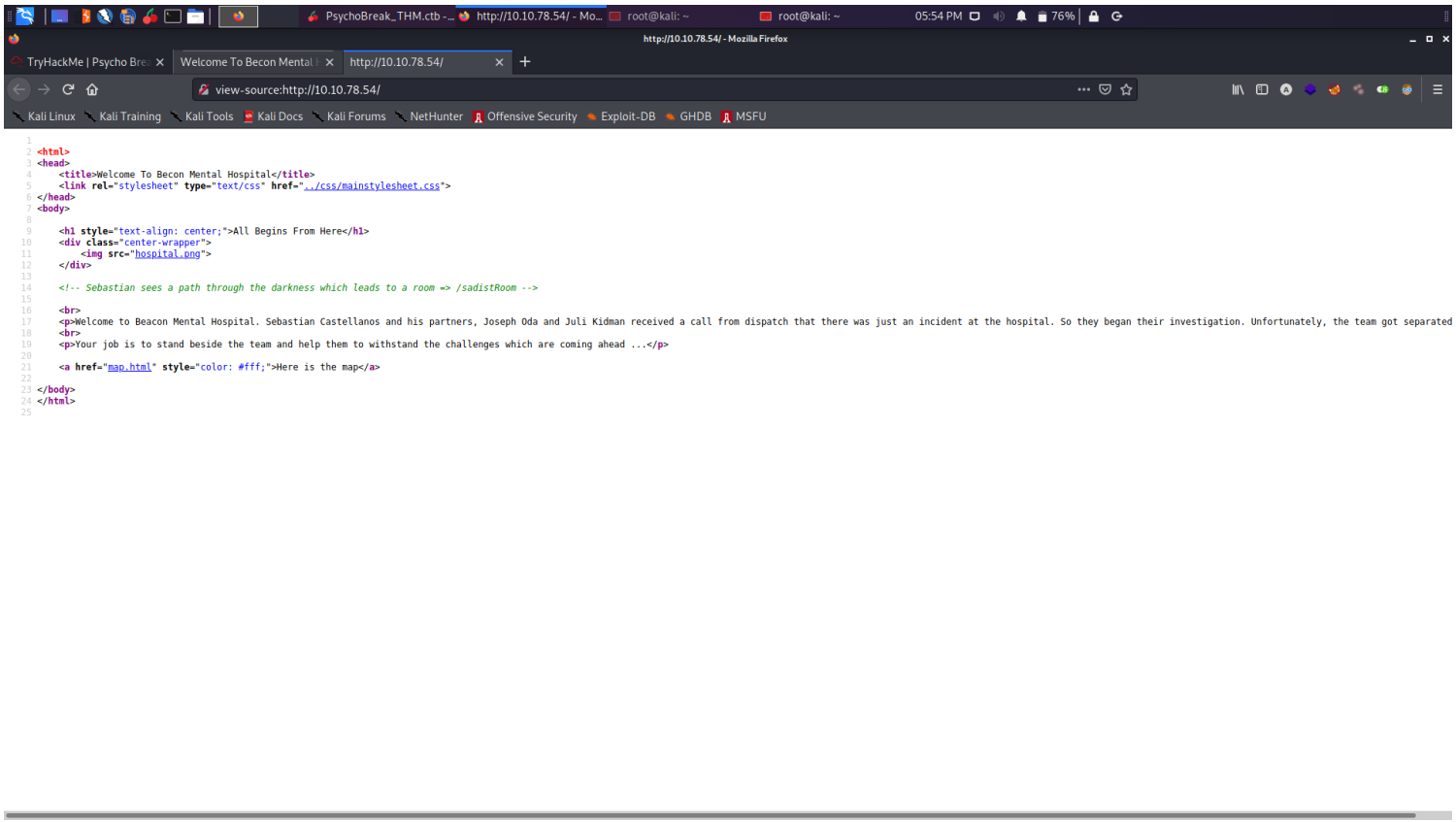
gobuster

/.hta (Status: 403) [Size: 276]
/.htaccess (Status: 403) [Size: 276]
/.htpasswd (Status: 403) [Size: 276]
/css (Status: 301) [Size: 308] [--> http://10.10.78.54/css/]

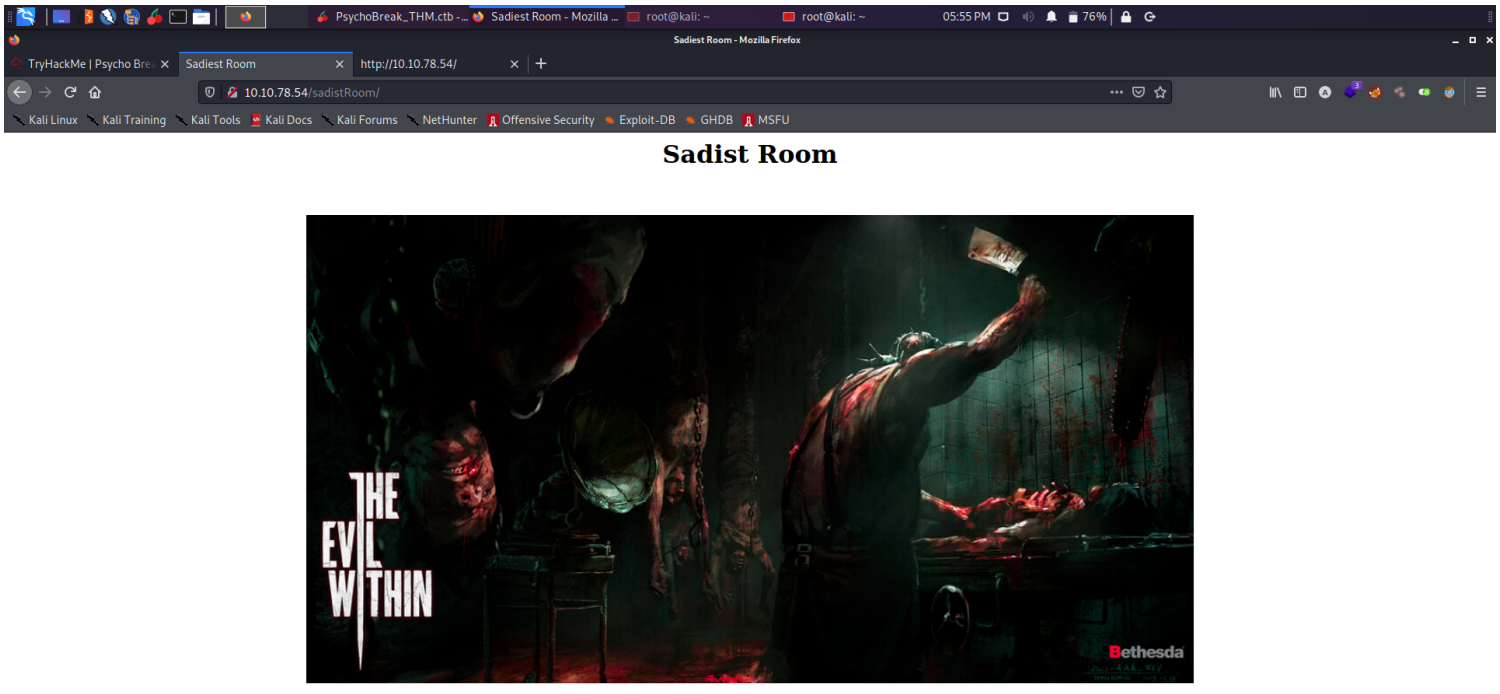
/index.php (Status: 200) [Size: 838]
/js (Status: 301) [Size: 307] [--> http://10.10.78.54/js/]
/server-status

/sadistRoom

Found a secret direcrory in main source code




```
<html>
<head>
    <title>Welcome To Becon Mental Hospital</title>
    <link rel="stylesheet" type="text/css" href="../css/mainstylesheet.css">
</head>
<body>

    <h1 style="text-align: center;">All Begins From Here</h1>
    <div class="center-wrapper">
        <img src="hospital.png">
    </div>

    <!-- Sebastian sees a path through the darkness which leads to a room => /sadistRoom -->

    <br>
    <p>Welcome to Beacon Mental Hospital. Sebastian Castellanos and his partners, Joseph Oda and Juli Kidman received a call from dispatch that there was just an incident at the hospital. So they began their investigation. Unfortunately, the team got separated
    <br>
    <p>Your job is to stand beside the team and help them to withstand the challenges which are coming ahead ...</p>

    <a href="map.html" style="color: #fff;">Here is the map</a>

</body>
</html>
```



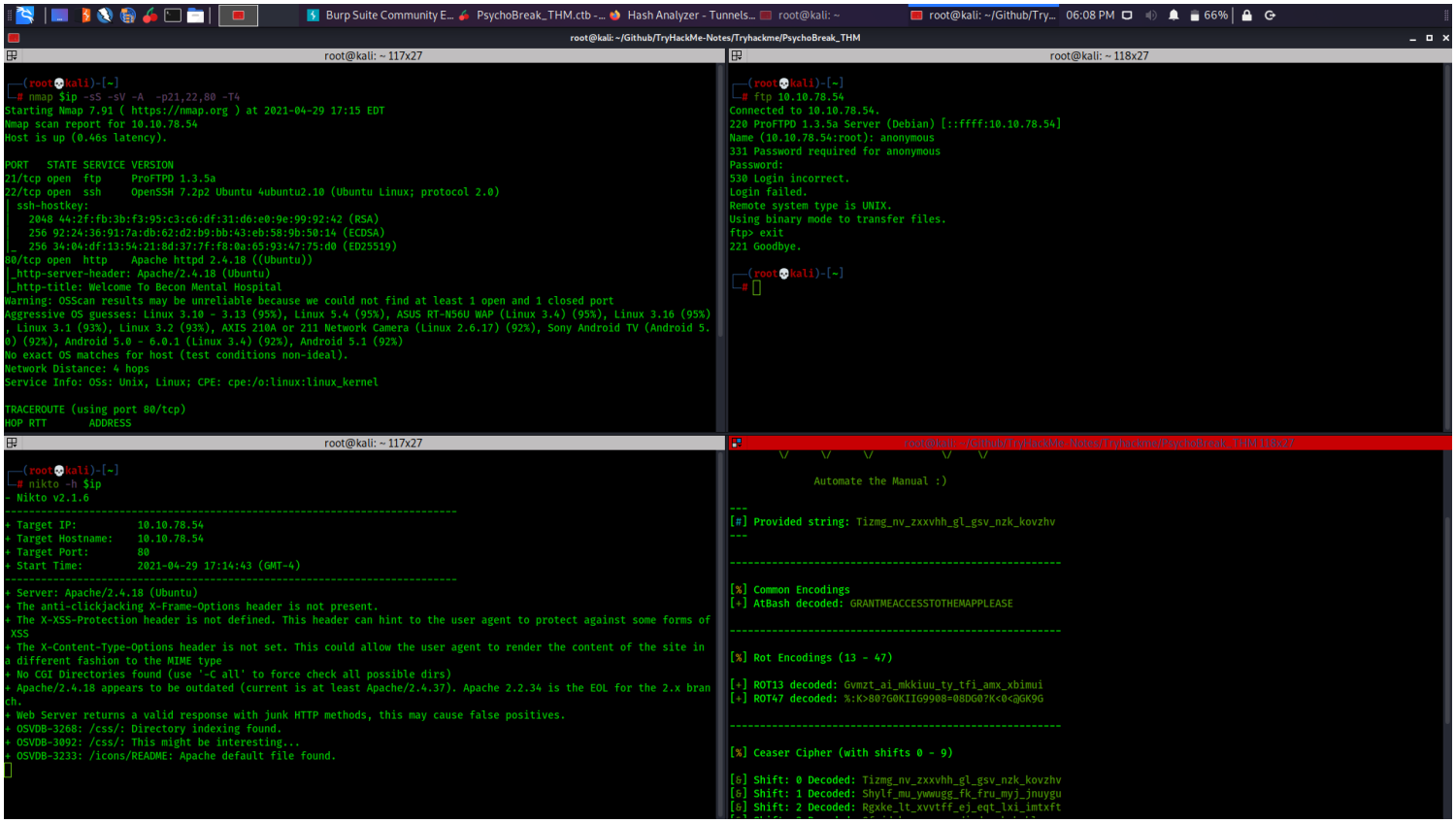
Sadist Room

Sebastian Found a key to the locker room. Click here to get the key.

#

Map key

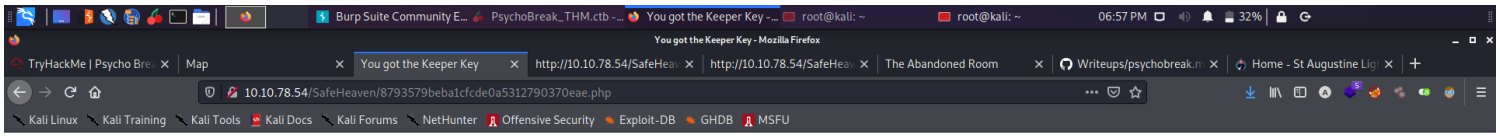
The key we found in the locker page is decoded



#

Keepers Key

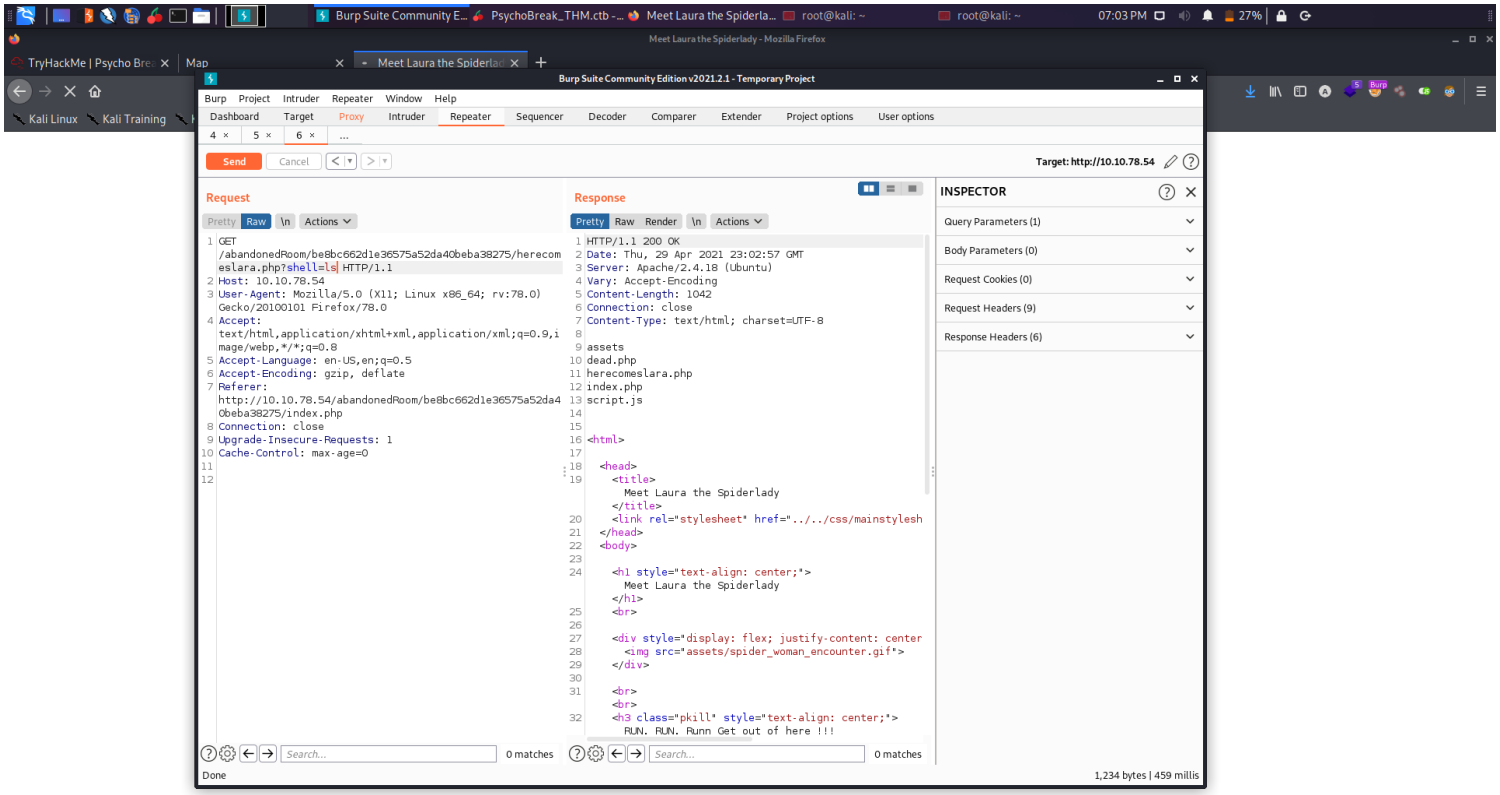
GOt the keepers key in safeheaven dir by doing some reverse image search 48ee41458eb0b43bf82b986cecf3af01



#

WebRCE

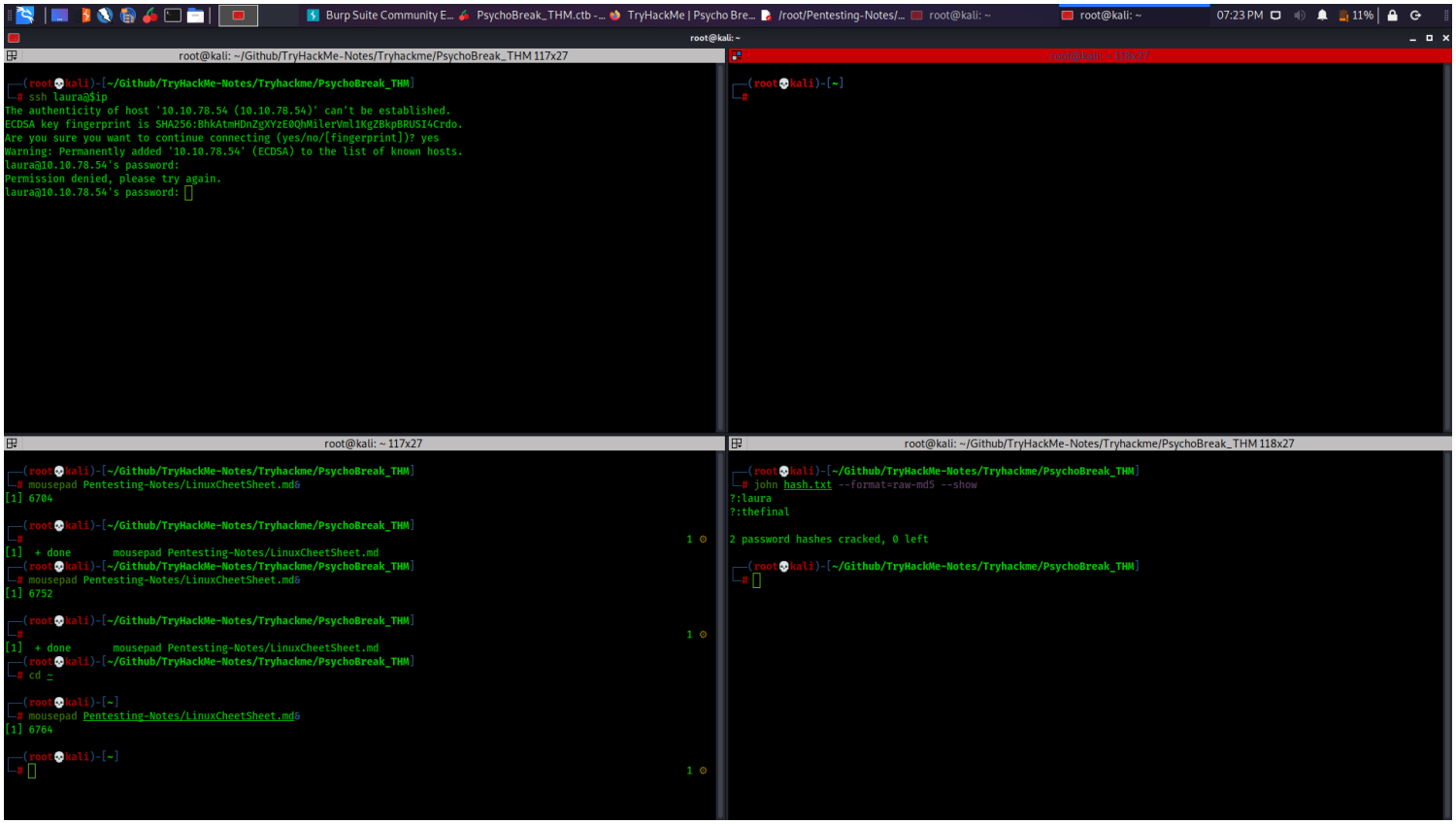
In abondonedroom directory we get hint that a shell is present so i added a shell paramter to the url and got rce



#

hashes decode

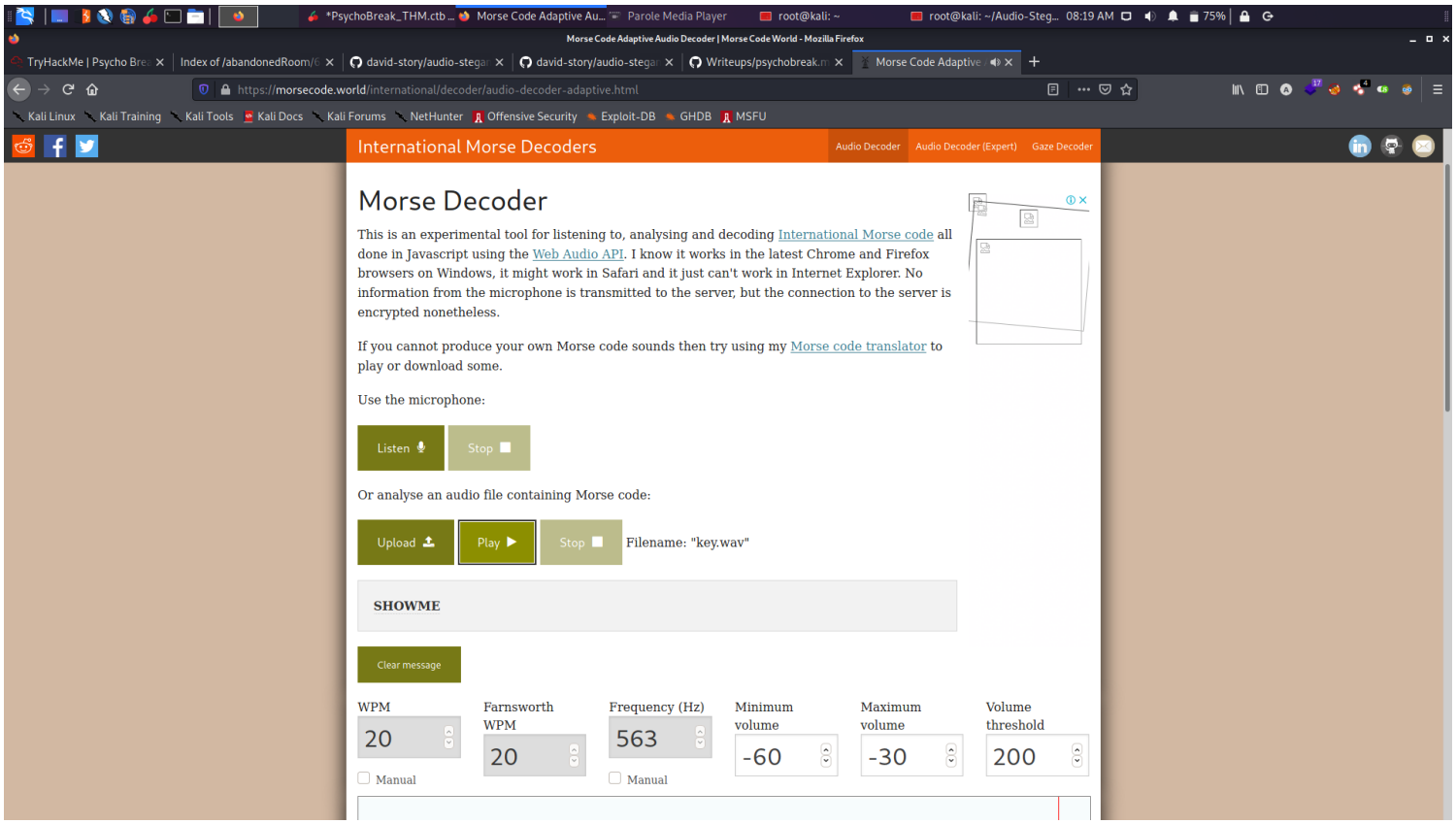
#



#

Key.wav

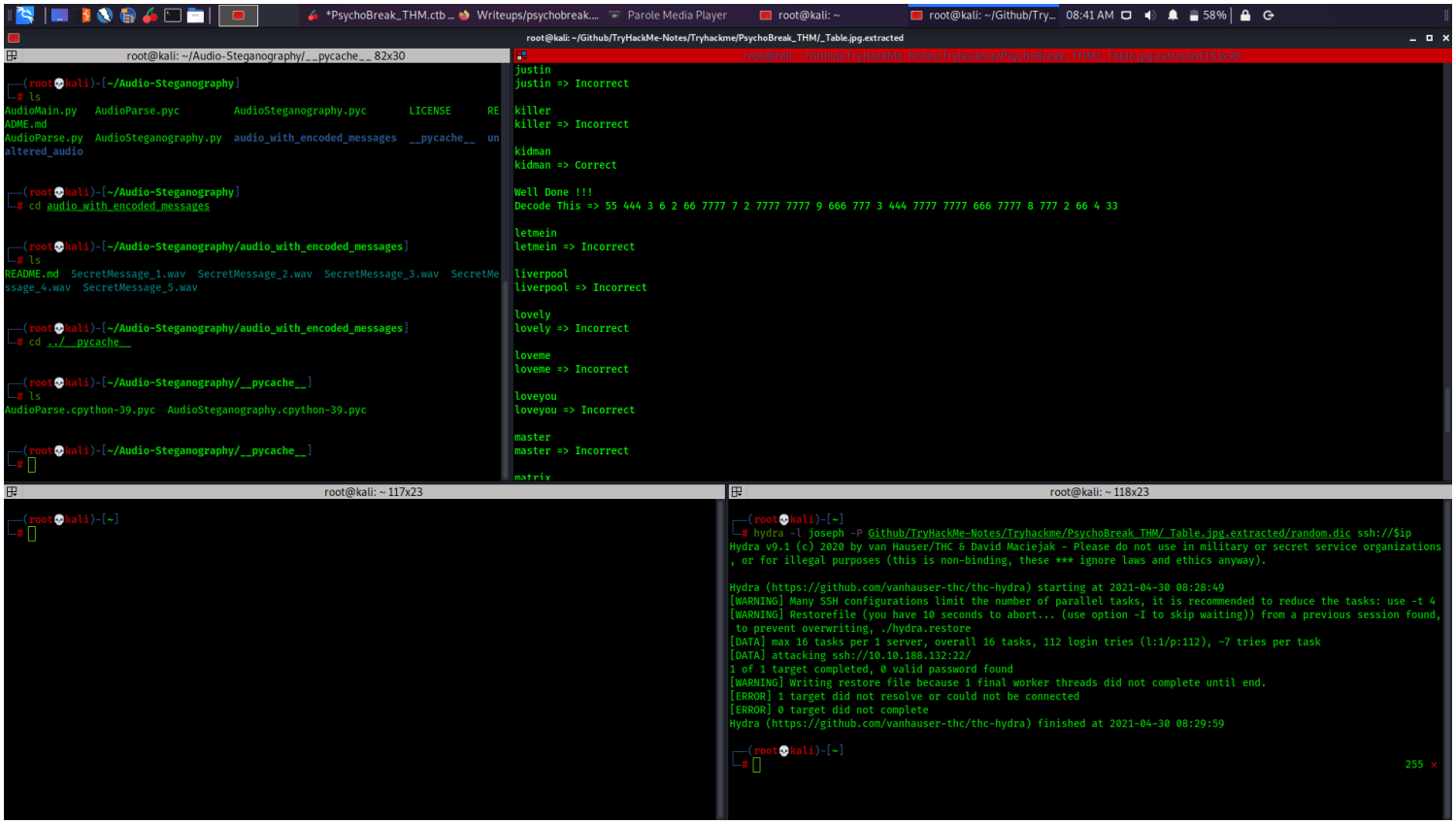
#



#

binary brut

The key for binary is kidman



Now we decode the output

KIDMANSPASSWORDISSOSTRANGE

Exploitation

Post Exploitation

AFter log in we see that we dont have access to sudo so do some mannual enumuraion

we see a cronjob which runs a python script and we an write to it

so we edit it and make it copy the bash binary to a tmp direcroty and giving it a suid permission

after waiting half a minute we run the copied binary with -p flag for priveleged mode and got root

Loot

Credentials

FTP

joseph:intotheterror445

#ssh

kidman:KIDMANSPASSWORDISSOSTRANGE

Flags

User Flag

4C72A4EF8E6FED69C72B4D58431C4254

Root Flag

BA33BDF5B8A3BFC431322F7D13F3361E