Report Pentesting

By Riccardo Bruzzese

**INDEX**

**1.Tools I used for this lab**

1.1 VPN Profile 2  
1.2 Software used for these machines: ssh2john, Dirbuster , Johntheripper, Exiftool and steghide 2  
1.3 Sites that were used for Capture the Flag 2  
**2. Purpose of this laboratory**

**3. Introduction and First sub-network 192.168.10.0/24 4**3.1. Machine 192.168.10.10 5  
3.1.2 Considerations of Machine 192.168.10.10 9  
3.2 Machine 192.168.10.20 9  
3.2.2 Considerations of Machine 192.168.10.20 11

**4. Machines of the second network 192.168.20.0/24 12**4.1 First machine of the second sub-network 192.168.20.10 12  
4.1.2 Considerations of Machine 192.168.20.10 17  
4.2 Second sub-network machine 192.168.20.20 17  
4.3 Last machine 192.168.20.30 19  
4.3.3 Considerations of machine 192.168.20.30 25

**5.Conclusions**

# **1.Tools I used for this lab**

## ***1.1 Profile VPN***

## to connect to the necessary machines of the sub-network 192.168.10.0/24 and 192.168.20.0/24

## ***1.2 Software used for these machines: ssh2john, Dirbuster , Johntheripper, Exiftool and steghide***

ssh2john was used to make recognize the rsa .key.private.bak key to Johntheripper while the latter was used to crack the private root key and then get it. Dirbuster was crucial for this experience because it was essential for scanning the machine and through it we found several clues as in the case of max@192.168.20.10 machine we found the codebreakers file.  
Exiftool was used to load the shell into the sobs.jpg image and then enter Karl’s machine.  
Steghide was used for steganography and through the passphrase we were able to find the password of Max

## ***1.3 Sites that were used for this CTF***

-Base64 (key decoding in base 64)  
site that I used for the keys of Karl, Thomas and Max  
-Base32 (key decoding in base32)  
site I used for Alice’s key for machine 192.168.20.20 -Cryptii (caesar cipher)  
essential to find Thomas' encrypted key

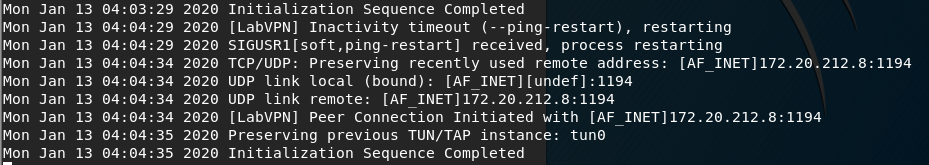
# ***2.* Purpuose of this laboratory**

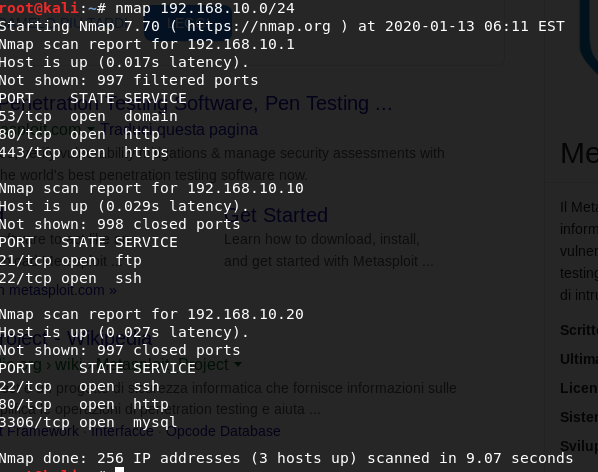
We have been assigned 5 machines to be pierced in particular:

First sub-network (192.168.10.0/24):  
192.168.10.10  
192.168.10.20

Second sub-network (192.168.20.0/24):  
192.168.20.10  
192.168.20.20  
192.168.20.30  
  
The goal of this lab was to find the flags that were in these five machines. The respective flags were in /Desktop/flag.txt for both the user we connected to and root. To find the root flag, a privilege escalation had to be applied.

# **3. Introduzione e Prima sottorete 192.168.10.0/24**

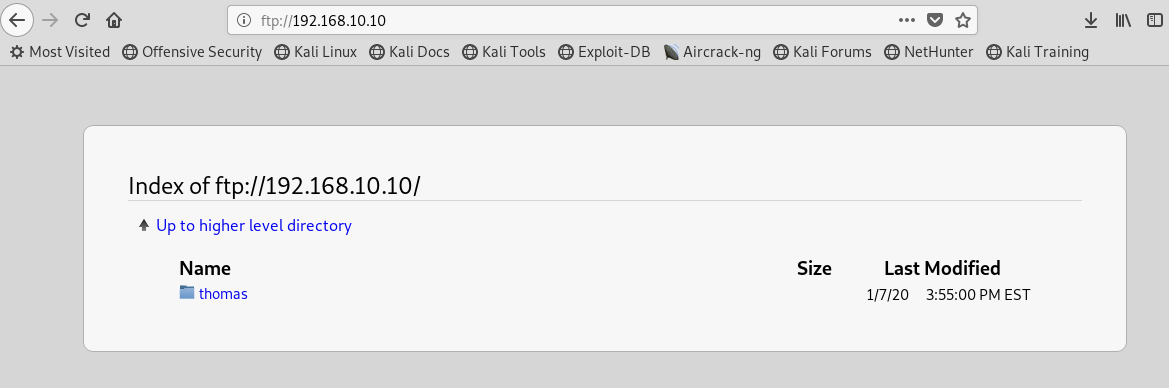
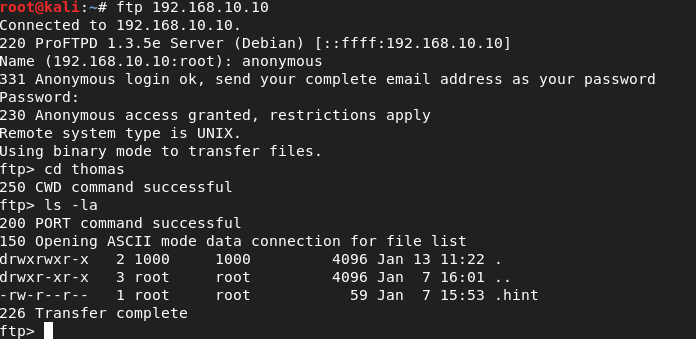
After downloading and installing the VPN profile correctly (riccardob):

We scan nmap for 192.168.10.0/24 machines

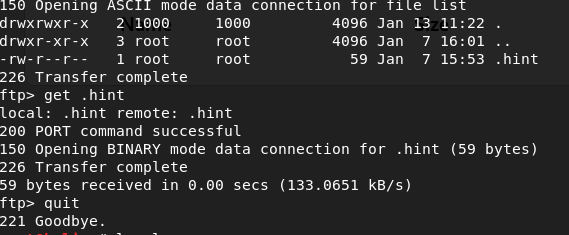
## 

## 

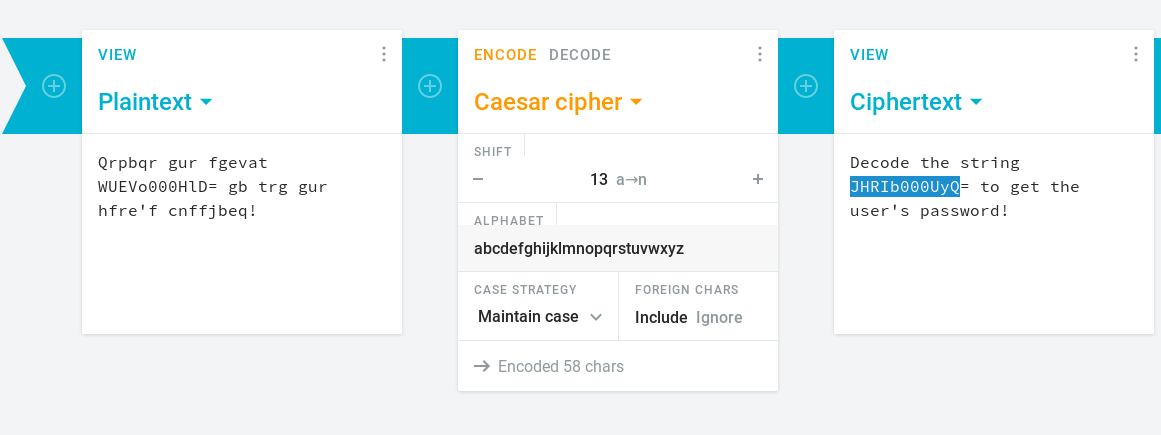
## 3.1. 192.168.10.10

Through the nmap we discover that the machine 192.168.10.10 has an ftp service so I decide to enter through Firefox:  
as you can see through the browser we discover in username thomas   
Then we logged in through the machine with the anonymous user 

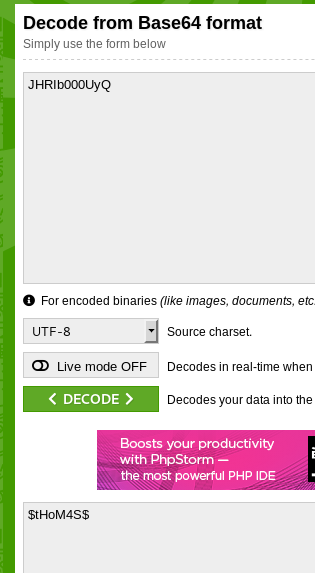
And thats our first .hint

We will get the .hint with the GET 

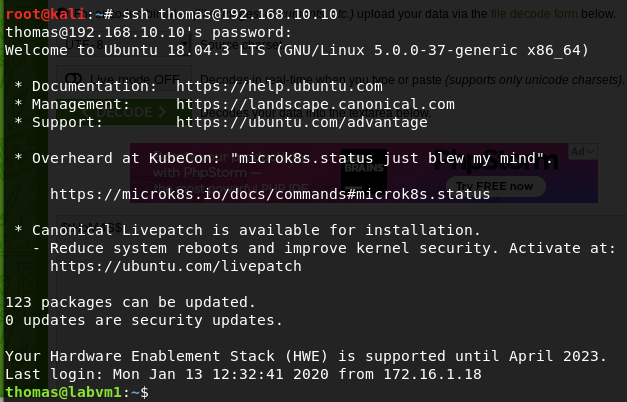
Next we will do just a cat .hint

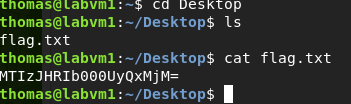


Through the website https://cryptii.com/pipes/caesar-cipher that we have the cipher of Caesar we get the cipher key of thomas

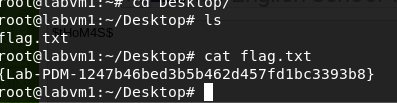


with base 64 we decrypt the encrypted key and get Thomas ssh key





We make the connection ssh thomas@192.168.10.10 and with the cat flag.txt of the folder Desktop we find the first flag.txt



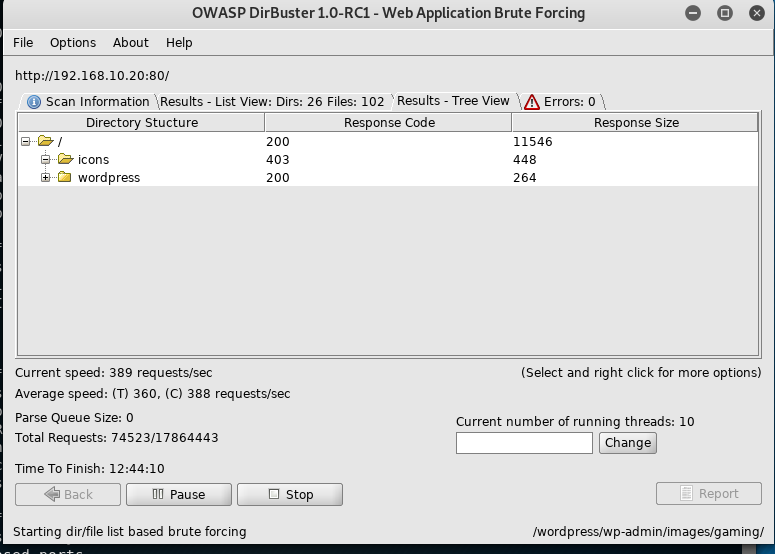
Through the simple sudo command on we become root and with the cat flag.txt we find the root flag

### **3.1.2 Considerations of 192.168.10.10**

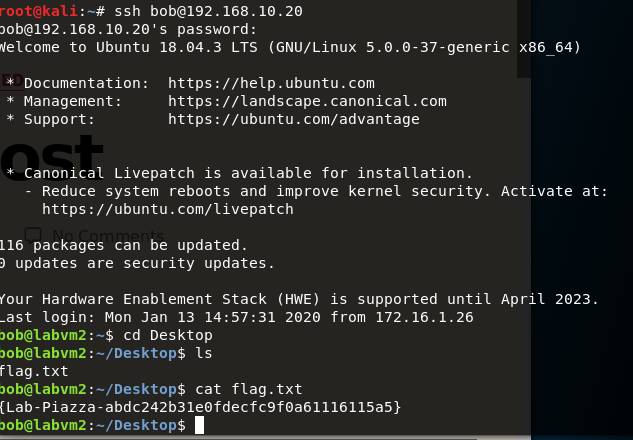
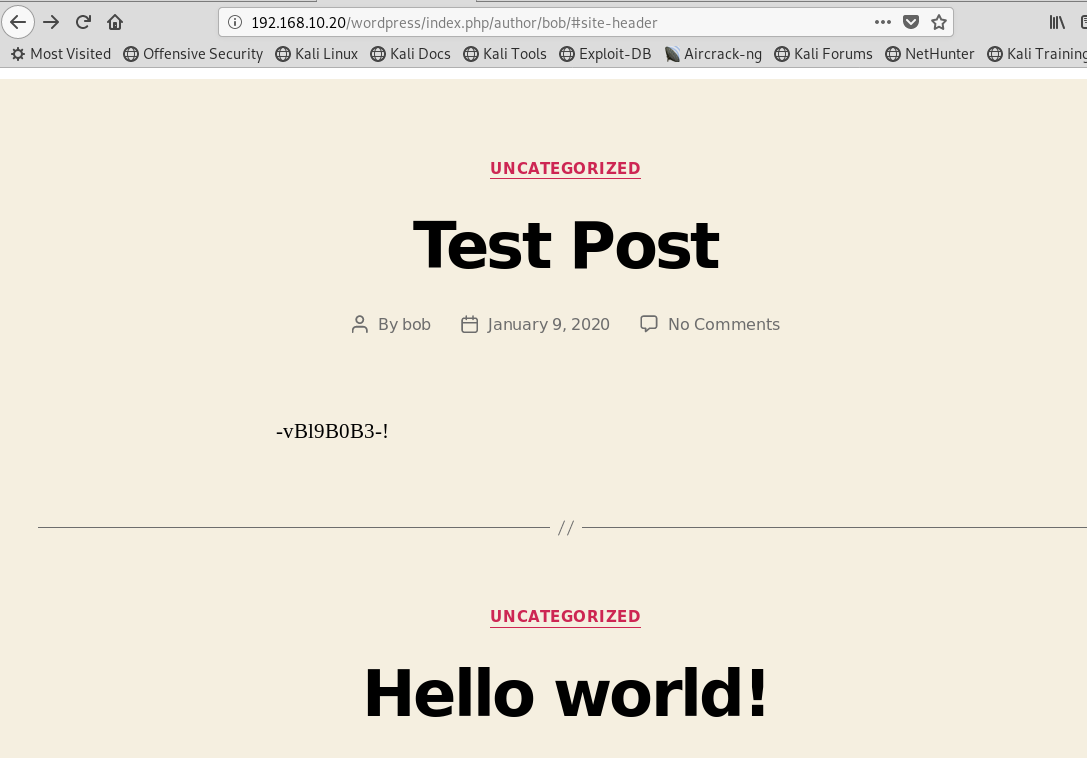
## The machine was quite easy to pierce. The only point I encountered was finding the site to encrypt the file. hint and then know that the key he used for that cipher was 13.

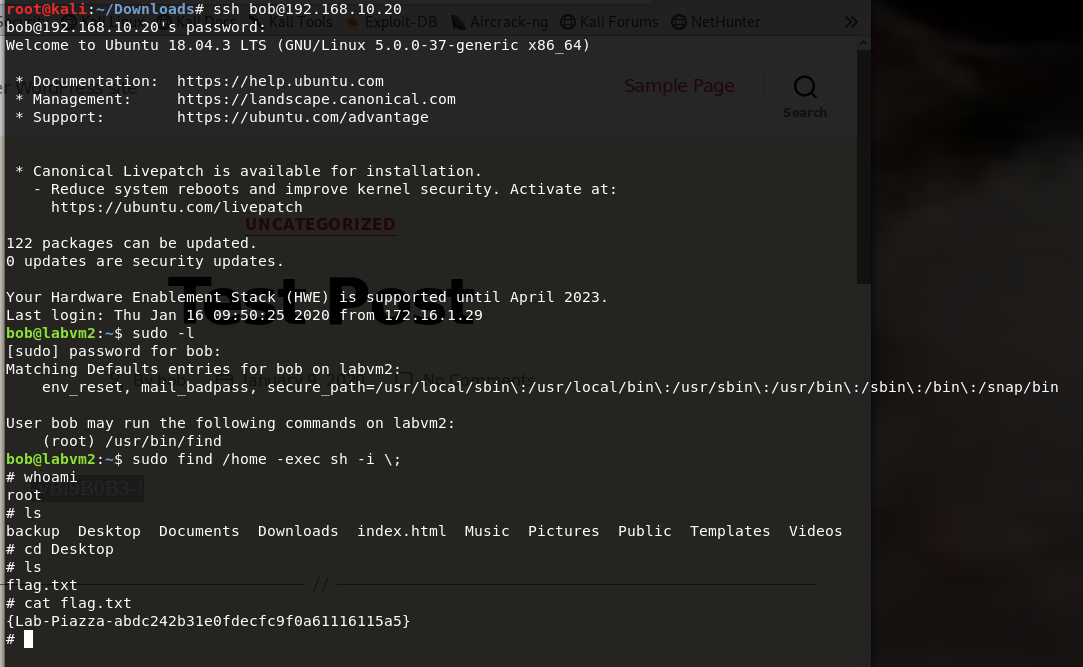
## **3. 192.168.10.20**

Through the dirbuster of the machine 192.168.10.20 we found the wordpress folder



Through it Firefox and we managed to find the user bob and even the key in ssh clear

 so through it we found the bob flag



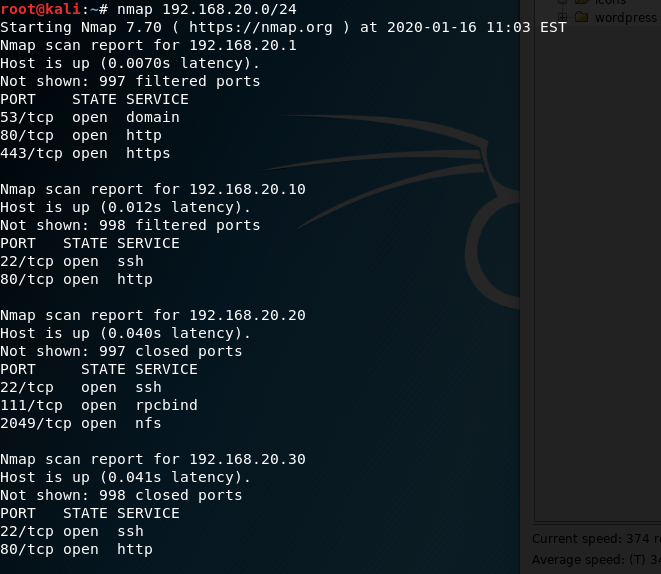
For the privilege escalation we did the sudo -l command to see what command he could do to become root. Then with the sudo command find /home -exec sh -i ; we become root and also get the root flag

### 3.2.2 Considerations of 192.168.10.20

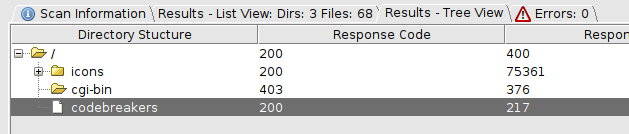
I think this is the easiest machine to pierce in my opinion. The password was clear despite privilage escalation was more "complicated" than 192.168.10.10

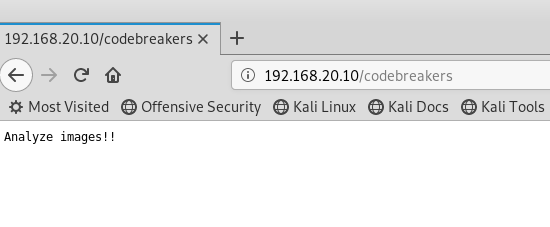
# **4. 192.168.20.0/24**

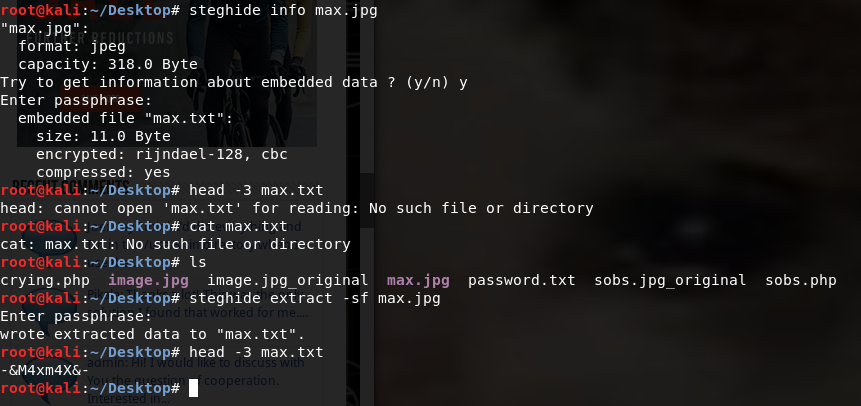
Now it gets a bit more serious. The machines of the second subnet were much more complex at the level of the first subnet.  
-The same procedure as for the first subnet then "Nmap of the machines of the second subnet":



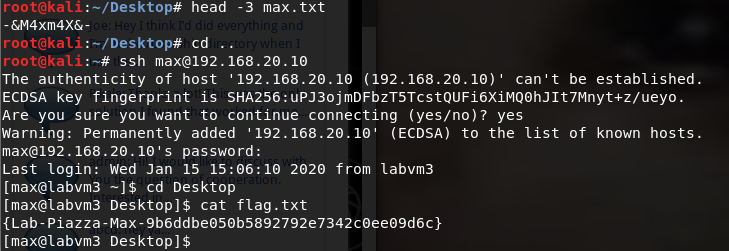
## **4.1 192.168.20.10**

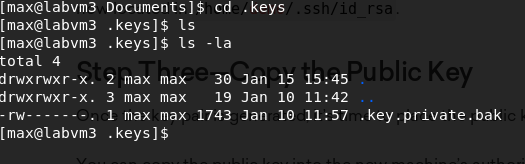
From the dirbsuter we notice that there is a codebreakers file that gives us a clue to analyze the images

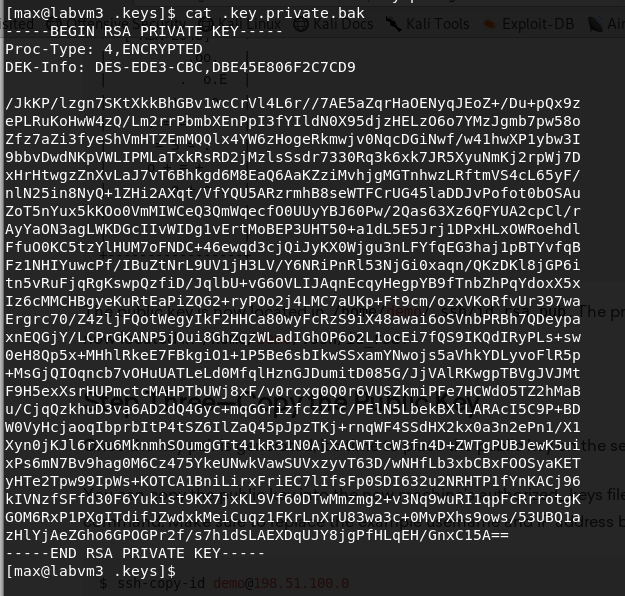


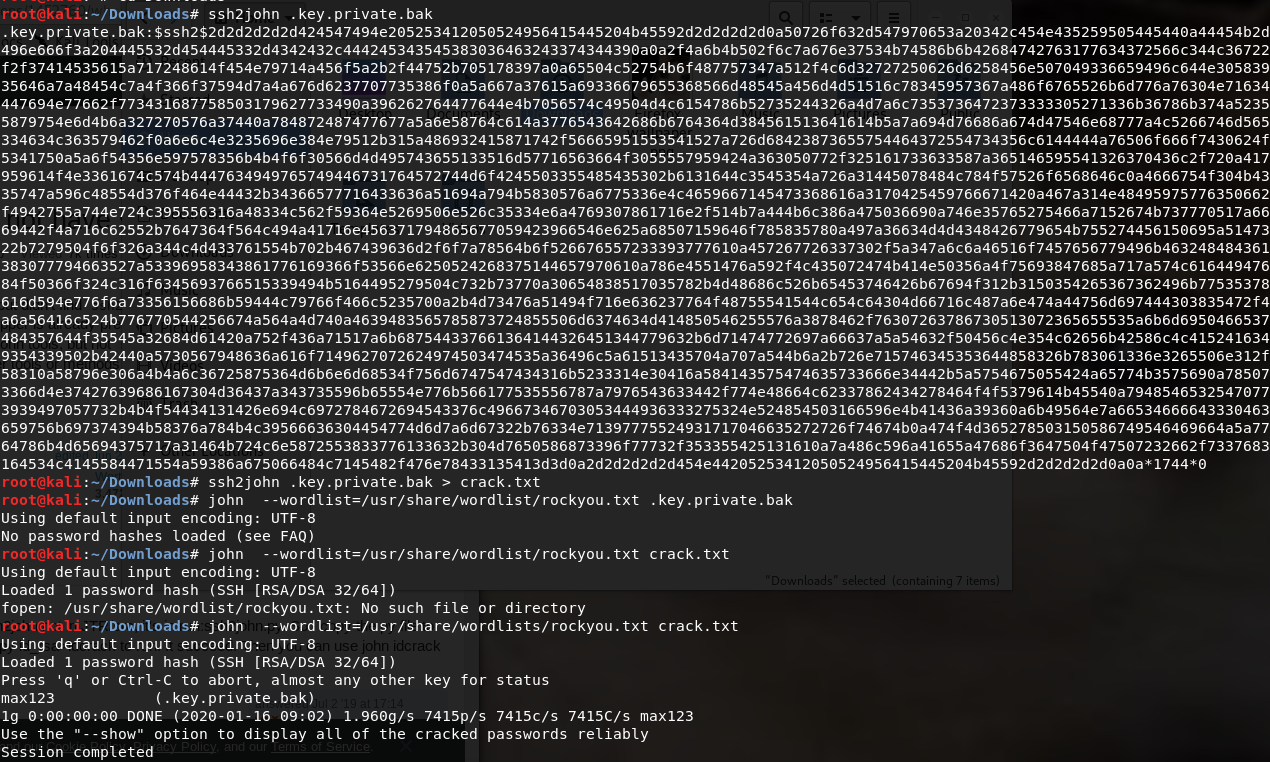
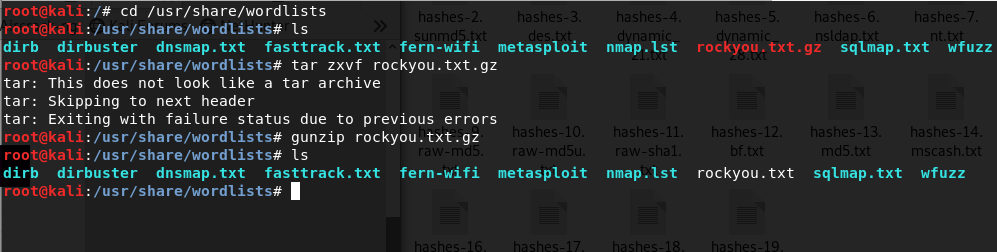
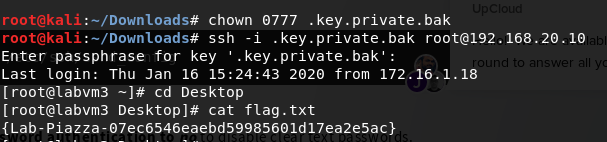
Documenting myself I noticed that to analyze the image I needed a tool for steganography: steghide executing the command info of max.jpg asked us the passphrase:

The passphrase was the codebreakers clue we found through the dirbuster

with the password we accessed max through ssh and thus also found the max user flag 

Later browsing the folders we found in Documents a hidden file . keys



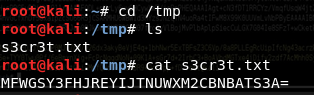
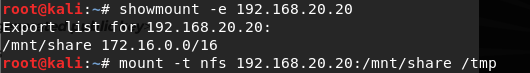
Through a cat we discover that a private key in RSA and to decipher it we needed John so we used gunzip for the rockyou file (wordlist that serves John ) we use ssh2john in order to be recognizable to John The Ripper and then we crack it with John The Ripper applying the wordlist we have unzipped 

let’s change the permissions because it had too high permissions so we put an 0777 so both user and root could access that key.  
Then we connect ssh using max123 as private key and we can access max’s machine and then get the root flag as well.

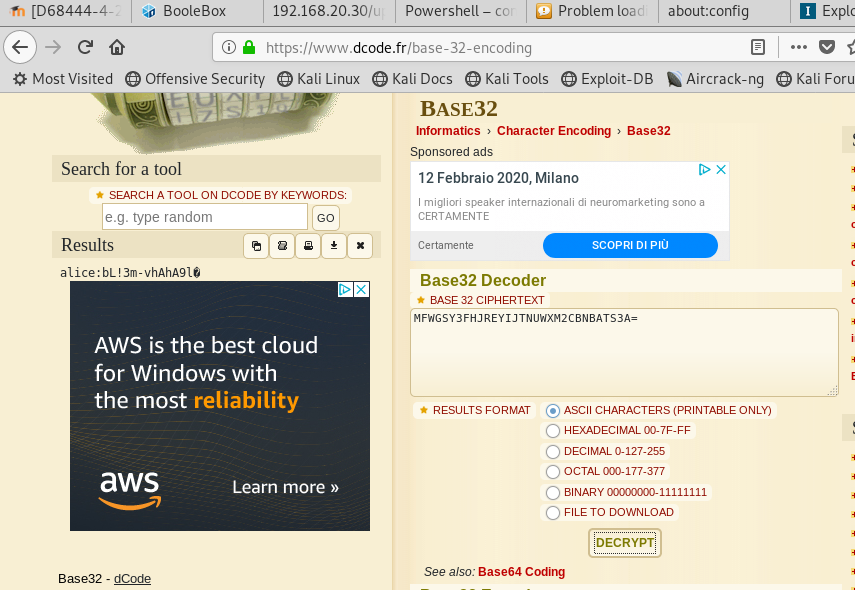
### **4.1.2 Considerations of 192.168.20.10**

So far the most complex machine regarding privilage escalation. I had several difficulties in making recognizable the key to John for everything else also for steganography was my first experience so it was very interesting to pierce this machine.

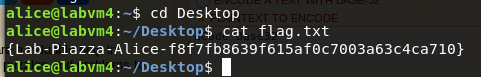
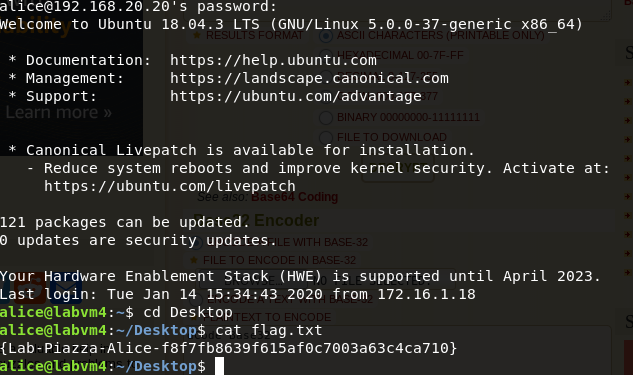
## **4.2 Second subnet 192.168.20.20**

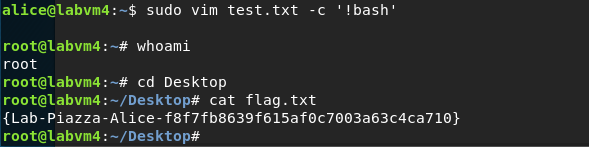
192.168.20.20 had the NFS service so I left immediately with the showmount of machine 192.168.20.20

mount and in the shared it is known that there is the first clue of the machine 192.168.20.20



through base 32 we find alice credentials to enter the machine 192.168.20.20 in ssh

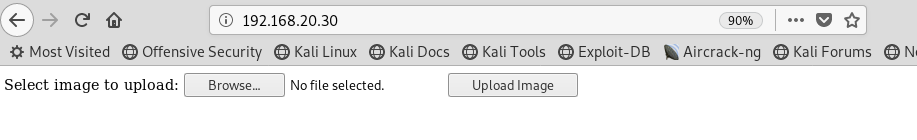
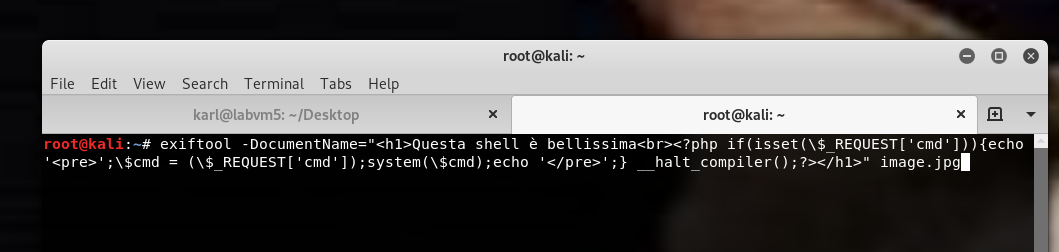
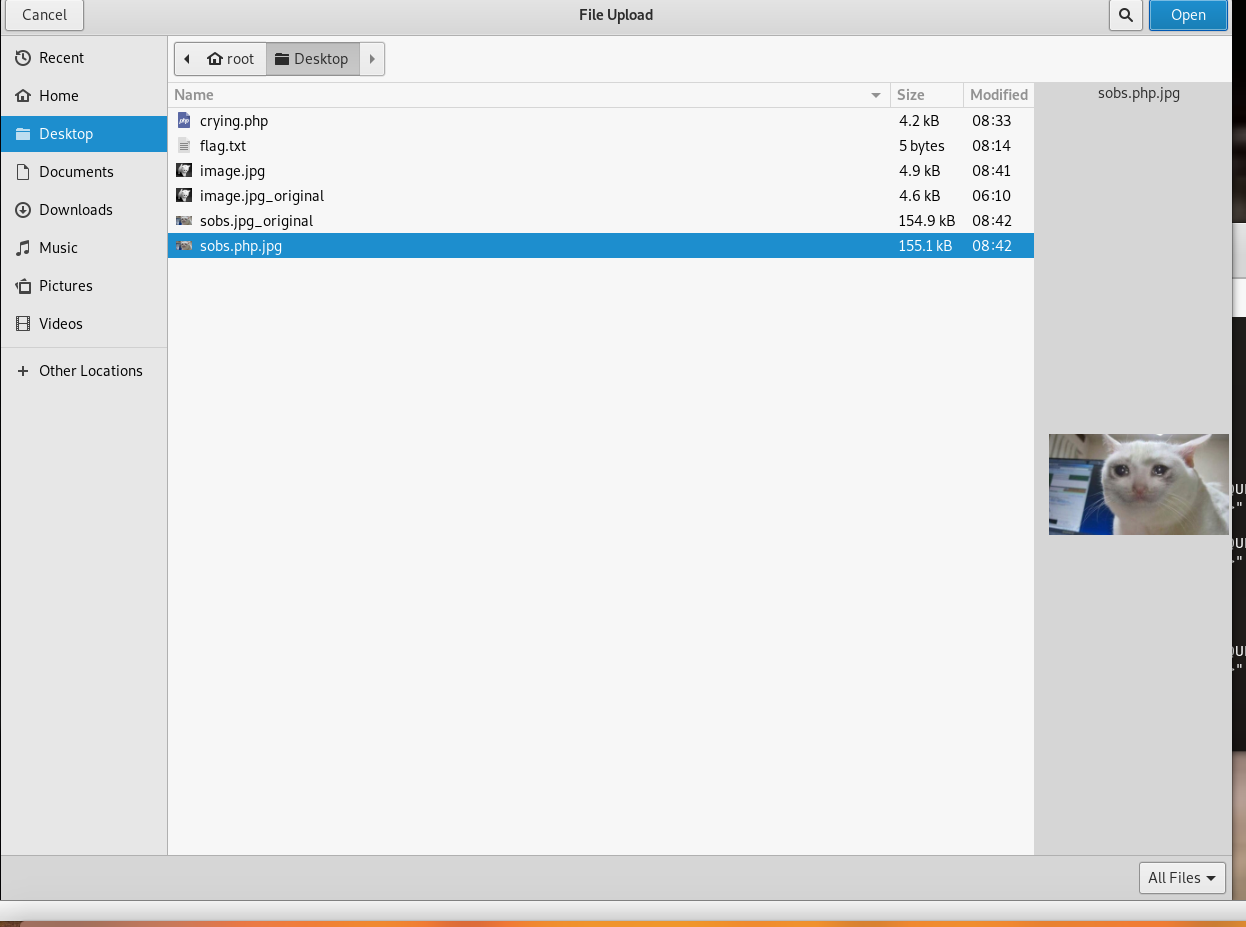
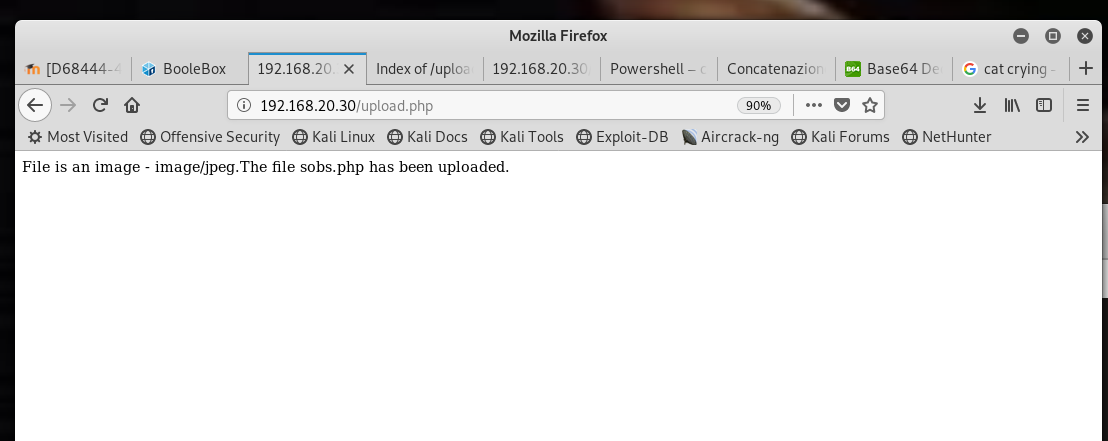
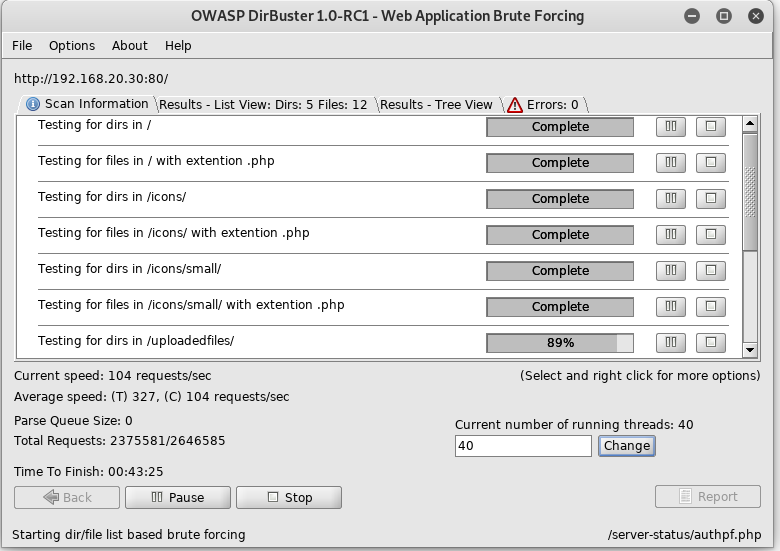


If we make the ssh, we find the flag of Alice. Immediately after we execute the command sudo -l and notice that alice we can become root through the text editor Vim 

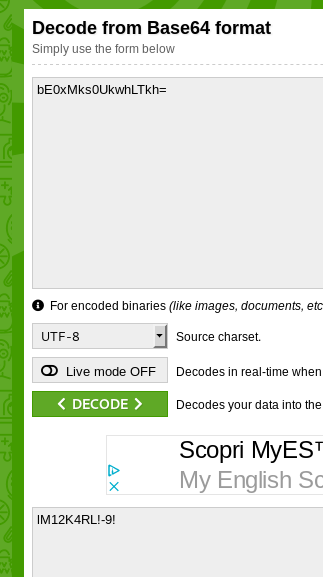
We get the root through a simple script in bash and with it also the flag.txt

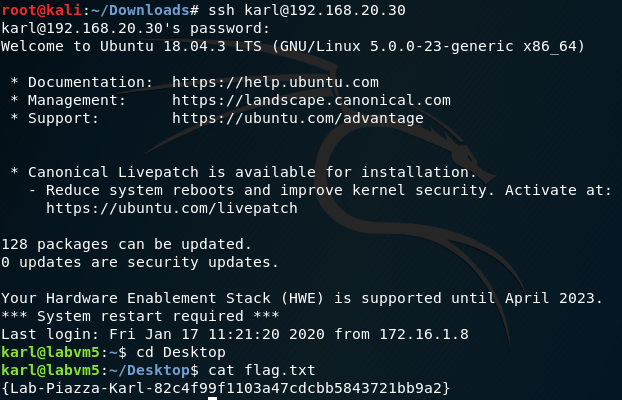
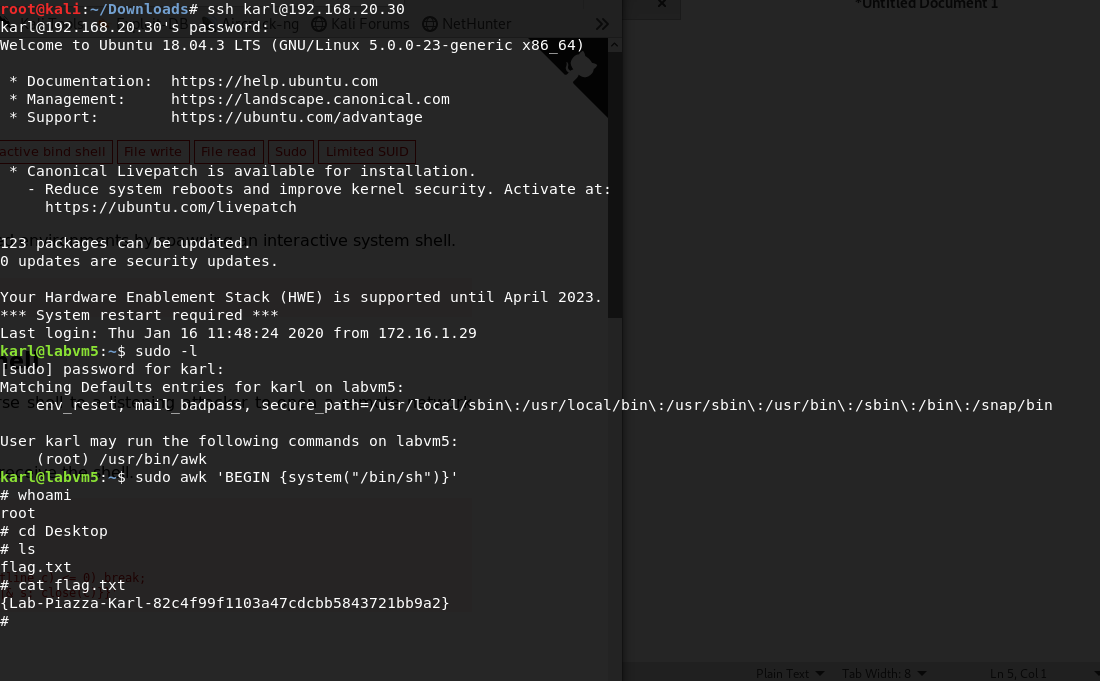
# **4.3 192.168.20.30**

# 

 The site looks so the solution much more likely was to insert a shell into an image and run it in order to enter into the machine and get the key and then later through ssh enter root. Through the exiftool tool we insert our shell into the image and then we make an mv of the file and change the extension in php  we upload our image to the site  Loaded the shell we use dirbuster and through the scan we notice that there is uploadedfiles and through it we also find our command shell sobs.php 

 Found our shell. Browsing through the files we found the file and with the cat command of the user-karl.txt file we find the encrypted password of our user karl.txt 



we decrypt our password encrypted through base64 and access the ssh connection with cd Desktop and cat flag we get the flag.txt  Through the command sudo -l we find that the user karl can get root through awk. Documenting myself I found a shell through awk and thus getting root privileges and the respective flag.txt

## **4.3.3 Considerations of 192.168.20.30**

Very interesting. The choice to insert a command shell into an image was a very clever choice. One of the cars I was most curious about.

# **5.Conclusions**

This experience has raised me a lot especially in the phase of attack. Many of these techniques I had never tried and being able to find these flags was very satisfying.