

BITS3613 HACKING TECHNIQUES AND PREVENTION

NAME: FAISAL

Project

Hack The Box Instruction Report

Contents

Project : Hack The Box Instruction Report	4
README FIRST!!!	4
HTB – INVITE CODE	4
MACHINE GAME.....	6
1. ACTIVE MACHINE NETMON = 20 Points	6
CHALLENGE GAME	7
CRYPTO CHALLENGES	7
1. KEYS = 40 POINTS	7
2. DECEITFUL BATMAN = 10 POINTS.....	7
3. CLASSIC YET COMPLICATED = 10 POINTS	8
4. YOU CAN DO IT! = 10 POINTS.....	8
5. BRAINY'S CIPHER = 30 POINTS	9
6. *INFINITE DESCENT* = 90 POINTS	10
7. *EBOLA VIRUS =100 POINTS	12
FORENSIC CHALLENGE	14
1. MARSHALL IN THE MIDDLE = 40 Points	14
2. DEADLY_ARTHROPOD = 40 Points	17
MISC CHALLENGE	18
1. FSOCIETY = 30 POINTS	18
2. INFERNO = 20 POINTS	18
3. ART = 20 POINTS	19
4. MISDIRECTION = 20 POINTS.....	20
5. OLD IS GOLD = 10 POINTS	21
6. BLACKHOLE = 20 POINTS.....	22
7. LONGBOTTOM'S LOCKER = 20 POINTS	24
8. ETERNAL LOOP = 20 POINTS	25
REVERSING CHALLENGE	26
1. IMPOSSIBLE PASSWORD = 30 POINTS	26
2. SNAKE = 10 Points	26
STEGO CHALLENGES	28
1. FOREST = 40 POINTS	28
2. RETRO = 50 Points.....	29
3. DA VINCI = 30 Points	30
4. DIGITALCUBE = 60 Points	32
5. BEATLES = 40 Points.....	33

6.	UNIFIED = 20 Points	34
7.	PUSHEEN LOVES GRAPHS = 30 Points.....	35
8.	SENSELESS BEHAVIOUR = 50 Points.....	36
WEB CHALLENGES		38
1.	HDC = 30 Points.....	38
2.	CARTOGRAPHER = 30 POINTS.....	41
3.	LERNAEAN = 20 POINTS	42
4.	*I KNOW MAG1K* = 50 Points.....	43

Project : Hack The Box Instruction Report

README FIRST!!!

HTB has 2 type of games; Machine and Challenge. The Machine game is like attack and defence style. I need to hack the active machine to get 2 flags (user.txt and root.txt). User.txt file is a user flag that mean the user account has been pawned and root.txt file is mean a root account/machine has been pawned/owned. The second game is Challenge game that is likely to CTF style. In this challenge, I have to get the flag in the format of **HTB{flag_here}**. Some of the challenge flags I just take screenshot to prevent from directly copy and paste of the flags from 3rd party. I have solved 31 challenges and 1 active machine recently.

HTB – INVITE CODE

1. Go to inviteapi.min.js in developer mode
2. Search for makeInviteCode() and press enter.
3. You will get {
 "0": 200,
 "success": 1,
 "data": {
 "data":
 "SW4gb3JkZXlmdG8gZ2VuZXJhdGUgdGhldm0ZSBjb2RlLCBtYWtlIGEGUE9TVCBYb2ZlZXN0IHRvIC9hcGkvaW52aXRIL2dlbmVvYXRRI",
 "enctype": "BASE64"
 }
4. Decode the data string base64 and we will get "In order to generate the invite code, make a POST request to /api/invite/generate".
5. Open terminal and type curl -i -X POST <https://www.hackthebox.eu/api/invite/generate>
- 6.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.316]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\faisa>curl -i -X POST https://www.hackthebox.eu/api/invite/generate
HTTP/1.1 200 OK
Date: Sun, 24 Feb 2019 16:58:12 GMT
Content-Type: application/json
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: __cfduid=d27573b6e4888f51654e33c22eabdf6c81551027492; expires=Mon, 24-Feb-20 16:58:12 GMT;
hackthebox.eu; HttpOnly; Secure
Vary: Accept-Encoding
Cache-Control: no-cache, private
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=0; includeSubDomains
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Server: cloudflare
CF-RAY: 4ae379c30966a9b4-SIN

{"success":1,"data":{"code":"UkhVVFQtTFpRRUctSFNMSEtVUVZU1ktVVVEWlA=","format":"encoded"},"0":200}
C:\Users\faisa>
```

7. Decode the data string again and you will get the invite code in plain text..

8. Input the invite code and insert your detail and verify the email.

Decode from Base64 format

Simply use the form below

UkhVVFQTFpRRUctSFNMSFetVUVZUIktVVVEWIA="

i For encoded binaries (like images, documents, etc.) upload your data

UTF-8

Source charset.


Live mode OFF

Decodes in real-time when you type or paste (.

< DECODE >

Decodes your data into the textarea below.

RHUTT-LZQEG-HSLHQ-UEYRY-UUDZP




Verify your Email

Email Verification required

Please check your inbox for an email verification link.

Resend Verification Email



Students and Teachers,
save up to 60% on Adobe
Creative Cloud.

ads via Carbon

MACHINE GAME

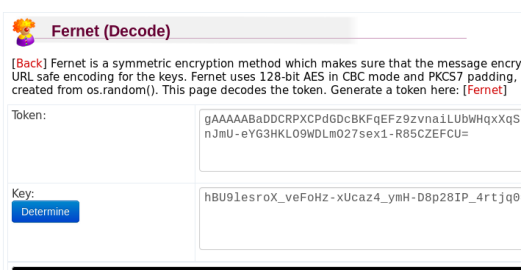
1. ACTIVE MACHINE NETMON = 20 Points

1	First nmap the target machine. We discover open port 21 ftp.	<pre> root@htb:fesal:~/Desktop/NetMon# nmap -sV 10.10.10.152 Starting Nmap 7.70 (https://nmap.org) at 2019-05-19 00:12 +08 Nmap scan report for 10.10.10.152 Host is up (0.25s latency). Not shown: 995 closed ports PORT STATE SERVICE VERSION 21/tcp open ftp Microsoft ftpd 80/tcp open http Indy httpd 18.1.37.13946 (Paessler PRTG bandwidth monitor) 135/tcp open msrpc Microsoft Windows RPC 139/tcp open netbios-ssn Microsoft Windows netbios-ssn 445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 59.48 seconds </pre>																								
2	Go to web browser and get to ftp://10.10.10.152 and click Users	<p>Index of ftp://10.10.10.152/</p> <p>⬆ Up to higher level directory</p> <table> <thead> <tr> <th>Name</th> <th>Size</th> <th>Last Modified</th> </tr> </thead> <tbody> <tr> <td>File: .rnd</td> <td>1 KB</td> <td>2/3/19 12:18:00 AM GMT+8</td> </tr> <tr> <td>inetpub</td> <td></td> <td>2/25/19 10:15:00 PM GMT+8</td> </tr> <tr> <td>PerfLogs</td> <td></td> <td>7/16/16 9:18:00 AM GMT+8</td> </tr> <tr> <td>Program Files</td> <td></td> <td>2/25/19 10:56:00 PM GMT+8</td> </tr> <tr> <td>Program Files (x86)</td> <td></td> <td>2/3/19 12:28:00 AM GMT+8</td> </tr> <tr> <td>Users</td> <td></td> <td>2/3/19 8:08:00 AM GMT+8</td> </tr> <tr> <td>Windows</td> <td></td> <td>2/25/19 11:49:00 PM GMT+8</td> </tr> </tbody> </table>	Name	Size	Last Modified	File: .rnd	1 KB	2/3/19 12:18:00 AM GMT+8	inetpub		2/25/19 10:15:00 PM GMT+8	PerfLogs		7/16/16 9:18:00 AM GMT+8	Program Files		2/25/19 10:56:00 PM GMT+8	Program Files (x86)		2/3/19 12:28:00 AM GMT+8	Users		2/3/19 8:08:00 AM GMT+8	Windows		2/25/19 11:49:00 PM GMT+8
Name	Size	Last Modified																								
File: .rnd	1 KB	2/3/19 12:18:00 AM GMT+8																								
inetpub		2/25/19 10:15:00 PM GMT+8																								
PerfLogs		7/16/16 9:18:00 AM GMT+8																								
Program Files		2/25/19 10:56:00 PM GMT+8																								
Program Files (x86)		2/3/19 12:28:00 AM GMT+8																								
Users		2/3/19 8:08:00 AM GMT+8																								
Windows		2/25/19 11:49:00 PM GMT+8																								
3	Then, go to Public folder	<p>Index of ftp://10.10.10.152/Users/</p> <p>⬆ Up to higher level directory</p> <table> <thead> <tr> <th>Name</th> <th>Size</th> <th>Last Modified</th> </tr> </thead> <tbody> <tr> <td>Administrator</td> <td></td> <td>2/25/19 11:44:00 PM GMT+8</td> </tr> <tr> <td>Public</td> <td></td> <td>5/18/19 11:54:00 AM GMT+8</td> </tr> </tbody> </table>	Name	Size	Last Modified	Administrator		2/25/19 11:44:00 PM GMT+8	Public		5/18/19 11:54:00 AM GMT+8															
Name	Size	Last Modified																								
Administrator		2/25/19 11:44:00 PM GMT+8																								
Public		5/18/19 11:54:00 AM GMT+8																								
4	Then, click user.txt to get the user flag	<p>Index of ftp://10.10.10.152/Users/Public/</p> <p>⬆ Up to higher level directory</p> <table> <thead> <tr> <th>Name</th> <th>Size</th> <th>Last Modified</th> </tr> </thead> <tbody> <tr> <td>Documents</td> <td></td> <td>2/3/19 8:05:00 AM GMT+8</td> </tr> <tr> <td>Downloads</td> <td></td> <td>7/16/16 9:18:00 AM GMT+8</td> </tr> <tr> <td>Music</td> <td></td> <td>7/16/16 9:18:00 AM GMT+8</td> </tr> <tr> <td>Pictures</td> <td></td> <td>7/16/16 9:18:00 AM GMT+8</td> </tr> <tr> <td>File: tester.txt</td> <td>1 KB</td> <td>5/18/19 11:54:00 AM GMT+8</td> </tr> <tr> <td>File: user.txt</td> <td>1 KB</td> <td>2/3/19 12:35:00 AM GMT+8</td> </tr> <tr> <td>Videos</td> <td></td> <td>7/16/16 9:18:00 AM GMT+8</td> </tr> </tbody> </table>	Name	Size	Last Modified	Documents		2/3/19 8:05:00 AM GMT+8	Downloads		7/16/16 9:18:00 AM GMT+8	Music		7/16/16 9:18:00 AM GMT+8	Pictures		7/16/16 9:18:00 AM GMT+8	File: tester.txt	1 KB	5/18/19 11:54:00 AM GMT+8	File: user.txt	1 KB	2/3/19 12:35:00 AM GMT+8	Videos		7/16/16 9:18:00 AM GMT+8
Name	Size	Last Modified																								
Documents		2/3/19 8:05:00 AM GMT+8																								
Downloads		7/16/16 9:18:00 AM GMT+8																								
Music		7/16/16 9:18:00 AM GMT+8																								
Pictures		7/16/16 9:18:00 AM GMT+8																								
File: tester.txt	1 KB	5/18/19 11:54:00 AM GMT+8																								
File: user.txt	1 KB	2/3/19 12:35:00 AM GMT+8																								
Videos		7/16/16 9:18:00 AM GMT+8																								
5	Yes, it is valid user flag and submit to HTB. I need to get root.txt to own the system. But, i did not managed to get root yet.																									

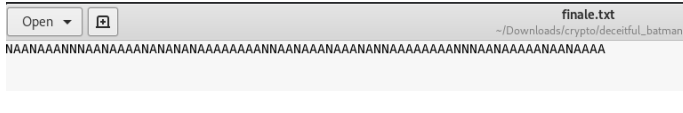
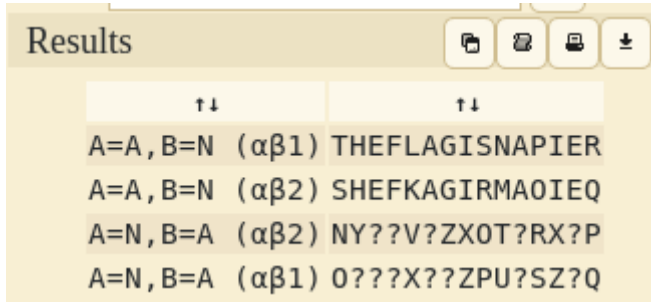
CHALLENGE GAME

CRYPTO CHALLENGES

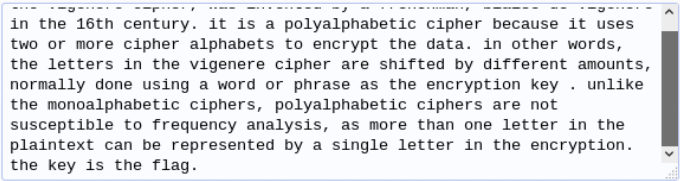
1. KEYS = 40 POINTS

1	The challenge contains an encrypted message	<pre>hBU9lesroX_veFoHz-xUcaz4_ymH-D8p28IP_4rtjq0= gAAAAABaDDCRPXCPdGdCBKFqEFz9zvna1LubWHqxXqScTTYwfZJcz -WhH7rf_fYHo67zGzJAdkrwATuMptY-nJmU-eYG3HKL09WDLm027sex1-R85CZEFcu=</pre>
2	After googling in the forum, it is fernet encryption. So, go to https://asecuritysite.com/encryption/ferdecode and decode it.	
3	Insert the token and key. Boommm!! HTB{N0t_A_Fl1g!}	<pre>Decoded: Flag : HTB{N0t_A_Fl1g!} Date created: Wed Nov 15 12:18:25 2017 Current time: Sun May 12 00:41:25 2019</pre>

2. DECEITFUL BATMAN = 10 POINTS

1	First unzip the folder and we found finale.txt file..it is baconian cipher exactly..	
2	Decode it online and get the flag. Put in htb format..HTB{NAPIER}	

3. CLASSIC YET COMPLICATED = 10 POINTS

1	Unzip the folder and got ciphertext.txt..it is classic vigenere cipher	<pre>root@htbfesal:~/Downloads/crypto/classic_yet_complicated# cat ciphertext.txt alp gwcsepul gtavaf, nlv prgbbpsu mb h jcpbyvdlq, iplta rv glniypfa we ekl l6xs nsjhlcb. px td o lccjdstslpahzn fptspf xstlxzi te iosj ezv sc xcns ttsoic lzlv mhaw ez sjqjsa xsp rwhr. tq vxspf sciov, alp wspvhcv pr ess rxpqlvp nwlvc dyi dswbhvo ef htqtafvyw hqzfbpg, ezutewmm zcep xzmyr o scio ry tscoos rd woi pyqnm gelvr vpm . qbctnl xsp akbflowllmtpwt nlwpcg, lccjdstslpahzn fptspfo oip qvx df gysgelipp ec bfvbxlrnj ojocjvpw, ld akfv ekhr zys hskedy my eva dclluxpih yoe mh yiacsoseehk fj l gebxwh sieesn we ekl iynfudktru. xsp yam zd woi qwoc.</pre>
2	Decode it online and get this output. The hint is “the key is the flag”!!	<p>Clear text using key "helloworld":</p> 
3	The key is the flag..so put in the HTB flag format	HTB{helloworld}

4. YOU CAN DO IT! = 10 POINTS

1	Unzip and get the you_can_do_it.txt file. It is unscramble text. Go and search for the tool online.	<pre>root@htbfesal:~/Downloads/cryp YHAOANUTDSYOE0IEUTC!</pre>
2	Decode it online..it is simple crack actually.. YOUSEETHATYOUcandoIT!	HTB{YOUSEETHATYOUcandoIT!}

5. BRAINY'S CIPHER = 30 POINTS

[illegible]

6. *INFINITE DESCENT* = 90 POINTS

1	Take a look at email.msg file. We have public key and message there. We can find the private key with help of public key....	<pre>-----BEGIN PUBLIC KEY----- MIGeMA0GCsQGSib3DQEBAQUAA4GMADCBiAKBgFbDk+zYy1tbjwPpsTWbYjIfBtZk waLARbJxLg6QhYalsGnBx064VFIH9XIKzPK/Dt1RzMO68gy7zL0iyipPtYb2n0M6 WcdD6gw9J9+xx4HjXZCHx4h4zQhfQe0YymeSPewXJ0e+GT31ymz6/Q1Ulyq/jWnD XZogxfbXi6bIwuN7AgMBAAE= -----END PUBLIC KEY----- -----BEGIN MESSAGE----- 4129629078717021256658192674755900069497953439203443979693333554255 7746317154546690027236571751344184125566532264397904753491077567029 7931356004359775501074138668004417061809481535231402802835349794859 3057870301472170081226286367998742656489363160067186295845181389566 -----END MESSAGE-----</pre>
2	This is the decoded public key from ASN.1 JavaScript decoder online.	<pre>Offset: 25 Length: 3+128 Value: (1023 bit) 60927735877056559130803069919621859729817223816091468870468728150535102345085544 19500114217949774730075697611835999153176610412137900414632997673208042812227220 59221121000734876311522442973431501541098154426813203111221347319912822819691524 92933055882377304091844616671159896354284349735375653609635116671867</pre>
3	Then go to http://www.mickybullock.com/blog/wp-content/RSA_Cryptography/ffactory.php to find the factor of above number. Then we got the p,q number based of N.	<p>N = <input type="text" value="60927735877056559130"/> Find Factors</p> <pre>6092773587705655913080306991962185972981722381609 = 7805622068551395034983074294227914827932592556281 x 7805622068551395034983074294227914827932592556281</pre>
4	Next, use the given fasterprimes.py and insert the p and q value based on above decoder.	<pre>p= 7805622068551395034983e7 709037828123 q= 780562206855139503498307 709037828129 e = 65537</pre>
5	Run fasterprimes.py and we got the decrypted message.	<pre>root@htbfeal:~/Downloads/crypto/Infinite Descent# python fasterprimes.py decrypted: 500491164140527509149577108534901274218266116126419727365281831678182 316</pre>

6	Go to given AESbootstrap.py and insert the decrypted message and do some coding.	<pre> line = '50049116414052750914957710853490127421826611612641972736 # separate into 3 digits n = 3 listOfNums = [int(line[i:i+n]) for i in range(0, len(line), n)] # print(listOfNums) resultString = "" for myNum in listOfNums: # decode each number using the given function list = str(bin(gen_and_check(myNum))) candidate = list[2::] candidate = candidate.zfill(8) print(candidate) </pre>
7	So that script outputs a binary for each number. Hmmm	<pre> decrypted:ke500491164 [500, 1491, 164, 1140, 365, 281, 831, 678, 1 01011010e> Zile to dump with --k 01101101 mp with --key. See -- 01111000y --key htbpu x62185972981722381609 011010005317661041213 h43150154109815442681 010110105428434973537 Z </pre>
8	Lets convert the binary into ASCII. Here the result. It look like base64 format.	<pre> ZmxhZz1Ccm9rM25fRzRtZQ== </pre>
9	Decode it and get the flag. Put flag in the format of HTB{flag}. yesss!!	<pre> flag=Brok3n_G4me </pre>

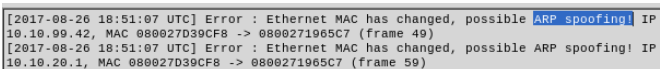
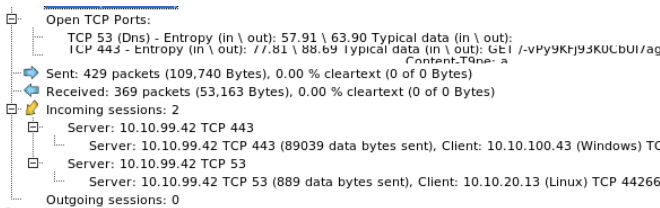
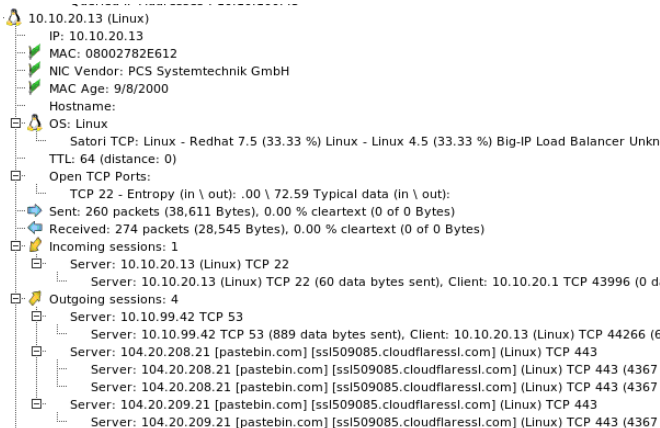
7. *EBOLA VIRUS =100 POINTS

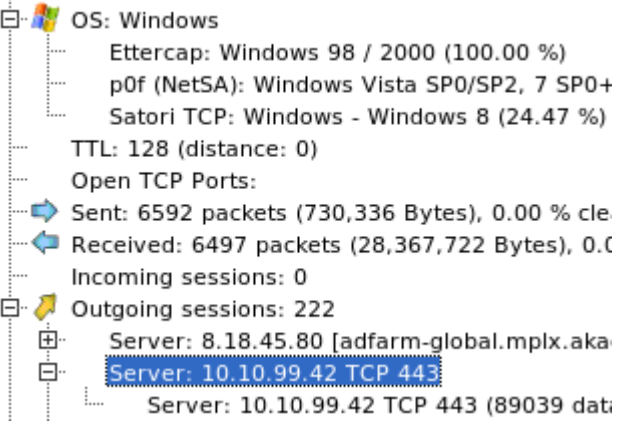
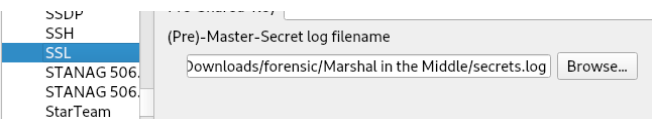
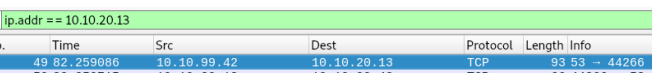
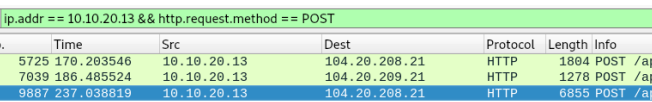
1	Go to https://www.cryptool.org/en/cto-cryptanalysis/n-gram-analysis to do frequency analysis and put the encrypted data.	<div><div>Your Text (Ciphertext):</div><div><div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div></div></div>
---	--	---

5	This will help us a lot. So, more modifications and we got this. Looks like the flag is at the bottom.	<pre> tion with the virus to onset of symptoms is 2 to 4 not infectious until they develop symptoms. First s den onset of fever fatigue, muscle pain, headache a s is followed by vomiting, diarrhoea, rash, symptom / and liver function, and in some cases, both inter eeding (e.g. oozing from the gums, blood in the sto ndings include low white blood cell and platelet co liver enzymes.NNHTBWO3MkN8wMh0wMtoMc8nTr8lMEb8lGJNN </pre>
6	'N' should be a line break and we know that the flag format is HTB {flag}. Therefore, 'W' and 'J' can be easily substituted. But it looks like unreadable text. I try this flag and it failed. So it is not the flag. Need some modification.	<pre> HTB{03MkN8wMh0wMtoMc8nTr8lMEb8lG} </pre>
7	'M' looks like an underscore. And the flag reads something like '...know how to control...'. So, a bit more logical analysis and trial and errors, end up with the correct flag.	<pre> HTB{W3_kN0w_h0w_to_c0nTr0l_Eb0l4} </pre>

FORENSIC CHALLENGE

1. MARSHALL IN THE MIDDLE = 40 Points

1	First, open the pcap file with NetworkMiner and i found anomalies here..it ARP spoofing																																																									
2	It has MAC address 080027D39CF8 and IP 10.10.99.42. Let's find out. It is windows OS and has open port of TCP 53,TCP 443.																																																									
3	It fishy here. At host tab, I found linux machine? It maybe an attacker with Kali OS. it also has outgoing session to 10.10.99.42 TCP 53. It could be related to windows OS.																																																									
4	At the session tab, i found client host with 10.10.100.43 and 10.10.20.13(attacker might be)	<div><div>Hosts (279)Files (340)Images (12)MessagesCredentials (46)Sessions (231)</div><div>Filter keyword:</div><table><thead><tr><th>Frame nr.</th><th>Client host</th><th>C. port</th><th>Server host</th></tr></thead><tbody><tr><td>1</td><td>10.10.100.43</td><td>49869</td><td>54.243.249.85</td></tr><tr><td>49</td><td>10.10.20.13</td><td>44266</td><td>10.10.99.42</td></tr><tr><td>285</td><td>10.10.100.43 (Windows)</td><td>49871</td><td>151.101.129.140 [reddit.map.fastly.r</td></tr><tr><td>283</td><td>10.10.100.43 (Windows)</td><td>49870</td><td>172.217.7.14 [www-google-analytics.</td></tr><tr><td>288</td><td>10.10.100.43 (Windows)</td><td>49872</td><td>151.101.193.140 [reddit.map.fastly.r</td></tr><tr><td>298</td><td>10.10.100.43 (Windows)</td><td>49873</td><td>151.101.1.140 [reddit.map.fastly.net</td></tr><tr><td>322</td><td>10.10.100.43 (Windows)</td><td>49874</td><td>54.208.254.144 [out.reddit.com]</td></tr><tr><td>331</td><td>10.10.100.43 (Windows)</td><td>49875</td><td>54.240.190.241 [dlykf07e75w7ss.clo</td></tr><tr><td>333</td><td>10.10.100.43 (Windows)</td><td>49876</td><td>52.86.21.31 [pixel.redditmedia.com]</td></tr><tr><td>351</td><td>10.10.100.43 (Windows)</td><td>49877</td><td>172.217.12.194 [pagead46.l.doublecl</td></tr><tr><td>377</td><td>10.10.100.43 (Windows)</td><td>49878</td><td>172.217.12.194 [pagead46.l.doublecl</td></tr><tr><td>381</td><td>10.10.100.43 (Windows)</td><td>49880</td><td>172.217.12.194 [pagead46.l.doublecl</td></tr><tr><td>379</td><td>10.10.100.43 (Windows)</td><td>49879</td><td>172.217.12.194 [pagead46.l.doublecl</td></tr></tbody></table></div>	Frame nr.	Client host	C. port	Server host	1	10.10.100.43	49869	54.243.249.85	49	10.10.20.13	44266	10.10.99.42	285	10.10.100.43 (Windows)	49871	151.101.129.140 [reddit.map.fastly.r	283	10.10.100.43 (Windows)	49870	172.217.7.14 [www-google-analytics.	288	10.10.100.43 (Windows)	49872	151.101.193.140 [reddit.map.fastly.r	298	10.10.100.43 (Windows)	49873	151.101.1.140 [reddit.map.fastly.net	322	10.10.100.43 (Windows)	49874	54.208.254.144 [out.reddit.com]	331	10.10.100.43 (Windows)	49875	54.240.190.241 [dlykf07e75w7ss.clo	333	10.10.100.43 (Windows)	49876	52.86.21.31 [pixel.redditmedia.com]	351	10.10.100.43 (Windows)	49877	172.217.12.194 [pagead46.l.doublecl	377	10.10.100.43 (Windows)	49878	172.217.12.194 [pagead46.l.doublecl	381	10.10.100.43 (Windows)	49880	172.217.12.194 [pagead46.l.doublecl	379	10.10.100.43 (Windows)	49879	172.217.12.194 [pagead46.l.doublecl
Frame nr.	Client host	C. port	Server host																																																							
1	10.10.100.43	49869	54.243.249.85																																																							
49	10.10.20.13	44266	10.10.99.42																																																							
285	10.10.100.43 (Windows)	49871	151.101.129.140 [reddit.map.fastly.r																																																							
283	10.10.100.43 (Windows)	49870	172.217.7.14 [www-google-analytics.																																																							
288	10.10.100.43 (Windows)	49872	151.101.193.140 [reddit.map.fastly.r																																																							
298	10.10.100.43 (Windows)	49873	151.101.1.140 [reddit.map.fastly.net																																																							
322	10.10.100.43 (Windows)	49874	54.208.254.144 [out.reddit.com]																																																							
331	10.10.100.43 (Windows)	49875	54.240.190.241 [dlykf07e75w7ss.clo																																																							
333	10.10.100.43 (Windows)	49876	52.86.21.31 [pixel.redditmedia.com]																																																							
351	10.10.100.43 (Windows)	49877	172.217.12.194 [pagead46.l.doublecl																																																							
377	10.10.100.43 (Windows)	49878	172.217.12.194 [pagead46.l.doublecl																																																							
381	10.10.100.43 (Windows)	49880	172.217.12.194 [pagead46.l.doublecl																																																							
379	10.10.100.43 (Windows)	49879	172.217.12.194 [pagead46.l.doublecl																																																							

5	So, i check who is 10.10.100.43 and it is Windows. It has outgoing session to 10.10.99.42 TCP 443.	 <p>OS: Windows</p> <ul style="list-style-type: none"> Ettercap: Windows 98 / 2000 (100.00 %) p0f (NetSA): Windows Vista SP0/SP2, 7 SP0+ Satori TCP: Windows - Windows 8 (24.47 %) TTL: 128 (distance: 0) Open TCP Ports: Sent: 6592 packets (730,336 Bytes), 0.00 % cle Received: 6497 packets (28,367,722 Bytes), 0.0 Incoming sessions: 0 Outgoing sessions: 222 Server: 8.18.45.80 [adfarm-global.mplx.aka Server: 10.10.99.42 TCP 443 Server: 10.10.99.42 TCP 443 (89039 dat
6	<p>After analyzing, 10.10.99.42 is a production web server.</p> <p>10.10.100.43 is a client communicate with production web server. 10.10.20.13 is the attacker. The title look like MITM case. Question say "any data was stolen from web server".</p>	client<-->attacker<-->web server
7	Now let open pcap file with wireshark. That say traffic is encrypted with SSL/TLS, let decrypt the SSL protocol in wireshark with the key in secret.log	
8	now , let filter ip add of attacker and look the first packet of filter list has TCP 53. Let check it out. select follow > TCP stream	
9	Attacker have accessed credit card info detail.	<pre>root@web-m1:/tmp/.h4x# head -n 4 c head -n 4 dumpdb IssuingNetwork,CardNumber American Express,345806846723249 American Express,345390632937883 American Express,348537668979836 root@web-m1:/tmp/.h4x# pastetext=9</pre>
10	we know that there was a POST call made, lets add that to the filter by ip.addr == 10.10.20.13 &&	

	http.request.method == POST	
11	It seen 3rd packet has large number of length. Take a look at http stream and voilaa. The flag!!!!!!!!!!!!	<p> American Express, 372202100444244 American Express, 377327829524687 American Express, 347637516705986 HTB{Th15_15_4_F3nD3r_Rh0d35_M0m3NT!!} American Express, 343588840524078 American Express, 375354542667439 American Express. 342786650506356 </p>

2. DEADLY_ARTHROPOD = 40 Points


[illegible]

MISC CHALLENGE

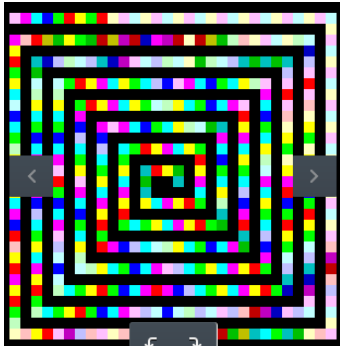
1. FSOCIETY = 30 POINTS

[illegible]

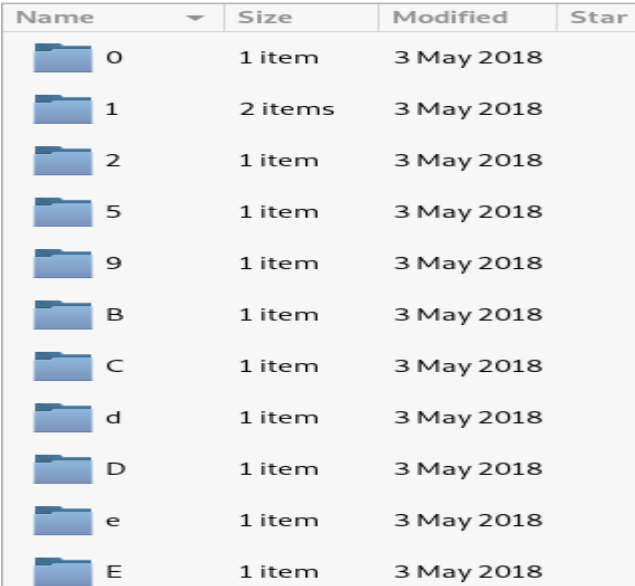

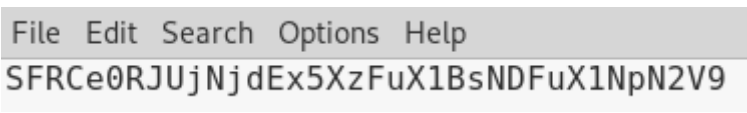
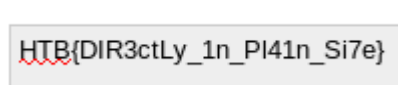
2. INFERNO = 20 POINTS

1	<p>decode the inferno.txt message to base64 and here is output</p> <pre>D" \$""7m5X32Vxfvu?1NMpLml\$GFEggUdSbb(<f})xqpunm3qpohmf+Lbgr_ ^j#a"Y^WVz=<XWVONrl_QJINGKEllHG)?c&BA: ?>=<5Yzy765432+O/.&%\$H(tg%\$#z@~jvu: srqvun4Uqjinmle+cKaf_dj#["_Xl ZYXWVUTSRQP2NMFKJCBfFE>&`@9! =<5Y9y7654_P0 /o-,%)h~}\$A a v(t:[Zvo5srTSonmf,jiKg`_dc ""BXWVzZ<;WVUTmqQP2NGFEllHGF?>bB\$@9)=<;4381Uvu-2+0/(K+*)"(~f B/</pre>
2	<p>Then convert the output to Malbolge programming language and the flag is appear.</p> <pre>HTB{!1t_1s_just_M4lb0lg3_l4ngu4g3!}</pre>  <p>The screenshot shows a terminal window with a title bar containing 'New program', 'Library', 'About the project', and 'New program'. The terminal output displays the flag: HTB{!1t_1s_just_M4lb0lg3_l4ngu4g3!}. Below the terminal, the 'Program code:' section shows the Malbolge code used to generate the output.</p> <pre>Program code: 1)ih~}\$A a v(t:[Zvo5srTSonmf,jiKg`_dc ""BXWVzZ<;WVUTmqQP2NGFEllHGF?>bB\$@9)=<;4381Uvu-2+0/(K+*)"(~f B/ 2 3</pre>

3. ART = 20 POINTS

1	It is a piet program image..	
2	So, decode it with tool online https://www.bertnase.de/npiet/npiet-execute.php and flag is here.	<p>Info: executing: npiet -e 1000000 art.png</p> <hr/> <p>HTB{p137_m0ndr14n}? ? \$? ? 18? 32464? ? ? 8? ? ? ?</p> <hr/> <p>run again !</p>

4. MISDIRECTION = 20 POINTS

1	Extract the folder and delete the folder that has no file in each folder	
2	Show the hidden file. From here you need to arrange the number and decode to get the flag. Let say 1=S, 2=R, 3=R and so on..	
3	After arrange it look like this	
4	Then decode base64 as usual and....	

5. OLD IS GOLD = 10 POINTS

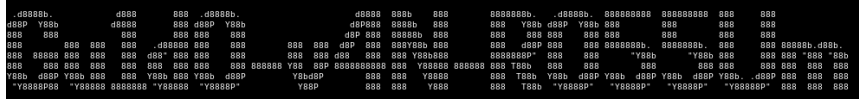
[illegible]

6. BLACKHOLE = 20 POINTS

1	Determine type of file and rename to correct file type. It is jpeg	<pre> root@htbfesal:~/Downloads/misc/Blackhole# file archive.zip archive.zip: Zip archive data, at least v2.0 to extract root@htbfesal:~/Downloads/misc/Blackhole# unzip archive.zip Archive: archive.zip inflating: hawking root@htbfesal:~/Downloads/misc/Blackhole# file hawking hawking: JPEG image data, JFIF standard 1.01, aspect ratio, density 72x72, segment length 16, baseline, precision 8, 794x579, components 3 root@htbfesal:~/Downloads/misc/Blackhole# mv hawking hawking.jpeg root@htbfesal:~/Downloads/misc/Blackhole# </pre>
2	That is the correct file type appear.	
3	Steghide the file with correct password is hawking.	<pre> root@htbfesal:~/Downloads/misc/Blackhole# steghide info hawking "hawking": format: jpeg capacity: 3.3 KB Try to get information about embedded data ? (y/n) y Enter passphrase: embedded file "flag.txt": size: 1.6 KB encrypted: rijndael-128, cbc compressed: yes </pre>
4	Steghide extract it and flag.txt appear in base64. Decode flag.txt in 2 times until caesar cipher text appear.	<pre> root@htbfesal:~/Downloads/misc/Blackhole# steghide extract -sf hawking Enter passphrase: the file "flag.txt" does already exist. overwrite ? (y/n) y wrote extracted data to "flag.txt". root@htbfesal:~/Downloads/misc/Blackhole# cat flag.txt UldaeFluUnhlaUJKZFhoNGRXMTVJRlJ0YVhkMwVuTwdhVzFsSUcxNklGRjZjM2gxwLhRZ1puUnhZV1J4 WmSWdmJYZ2dZblJyWlhWdmRXVmIMQ0J2WVdWNVLYaGhjM1ZsWmL3Z2JYcHdJRzFuWm5SaFpDd2dhWFJo SUDsdFpTQndkV1J4YjJaaFpDQmhjaUJrY1dWeGJXUnZkQ0J0WmLcbWRIRWdUM0Y2Wm1SeElISmhaQ0JH ZEhGaFpIRm1kVzL0ZUNCUFlXVjVZWGhoYzJzZ2JXWwdablJ4SUVkNmRXaHhaRlYxWm1zZ1lYSWdUMjE1 Ym1SMWNITnhJRzFtSudaMGNTQm1kWGx4SudGeULIUjFaU0J3Y1cxbWRDNGdWSEVnYVcxbeLHWjBjU0JJZ WjI5dFpYVnRlaUJDWkdGeWNXVmzV1FnWVhJZ1dXMWlkSEY1YldamWlYVWdiV1lnWm5SeElFZDZkV2h4 WkdWMVptc2dZWElndIXNWJtUjFjSE54SUC1eFptbHhjWG9nTVRrM09TQnRlbkFnTWpBd09TNGdWRzFw ZDNWnmN5QnRiM1IXY1doeGNDQnZZWGW1YldSdmRXMTRJRlZuYjI5eFpXVWdhWFZtZENCbGNXaHhaRzE0 SUDsaFpIZGxJR0Z5SudKaFltZDRiV1FnWlcSMWNYcHZjU0IXZWlCcGRIVnZkQ0IwY1NCd2RXVnZaMLZs Y1dVZ2RlVmxJR0ZwZWlCbWRIbmhaSEF4WlNCdGVuOWdiMkZsZVdGNElYTNJ1SEY2SUhQeGVuRmtiWGDl </pre>

5	This is the caesar cipher text after converting from base64 in 2 times.	<div><div>< DECODE ></div><div>Decodes your data into the textarea below.</div></div> <div><div><div>Exclusive Hari Raya Promotion</div><div><div>Buy 2 units of S-26 Progress or S-26 Promise 1.8KG and get 1x free Glasslock container.</div><div>Wyeth Nutrition</div></div><div>OPEN</div></div></div> <div>Efgbtgz luxxumy Tmiwuzs ime mz Qzxsuet ftqadqfuomx btkeuuef. qae yaxasuef. mzp mgftad. ita ime pudgotad ar dgeqmdot mf ftq Qgzfdg rad Ftqadqfuomx Qaeyaxask mf ftq Gzuhqdeufk ar Qmyndupsq mf ftq fuyg ar tue pgmft. Tq ime ftq Xgomeumz Bdarqeead ar Ymftqymfuee mf ftq Gzuhqdeufk ar Qmyndupsq nqfiqqz 1979 mzp 2009. Tmiwuzs motughqp qayyqduomx egoogee iuft eqhqdmx iadwe ar babgxmd eouqzoq uz ituot tq pueogeege tue aiz ftgaduge mzp qae yaxask uz sqzqdmx. Tue naaw M Nduqr Tuefadk ar Fuyq mbbgmddp az ftq Ndufuet Egzpmk Fuyqe ngef-egxxqd xuef rad m dqoadp-ndgmwuzs 237 iqowe. Tmiwuzs ime m raxxai ar ftq Dakmx Eacuatk, m xurafuyq yayngd ar ftq Bazfuruomx Mompqyk ar Eouqzoge, mzp m dqoubugzf ar ftq Bdgeupqzfumx Ygpmx ar Rdggpay, ftq tustqef ouhuxumz mimdp uz ftq Gzutfp Efmfge. Uz 2002, Tmiwuzs ime dmzwqp zgynqd 25 uz ftq NNQle baxx ar ftq 100 Sdgmfgef Ndufaze. TFN{Z3hqD_x3F_rT3_n4eFmDp5_S3f_K0g_p0iZ}</div>
6	Flag after decrypting from cipher text	<div>number 25 in the BBC's poll of the 100 Greatest Britons.</div> <div>HTB{N3veR_l3T_tH3_b4sTaRd5_G3t_Y0u_d0wN}</div>

7. LONGBOTTOM'S LOCKER = 20 POINTS

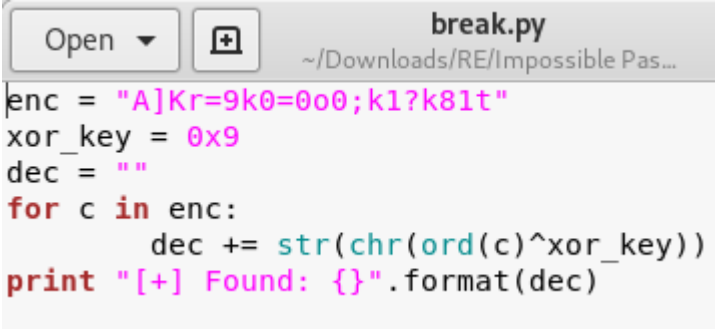
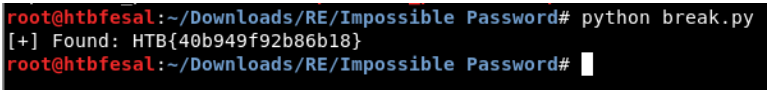
1	File all to view file type	<pre> root@htbfeal:~/Downloads/misc/Longbottom's_Locker# file * index.html: HTML document, UTF-8 Unicode text, with very long lines Longbottom's_Locker.zip: Zip archive data, at least v2.0 to extract neville.gif: GIF image data, version 89a, 244 x 244 socute.jpg: JPEG image data, JFIF standard 1.01, aspect ratio, dens ity 1x1, segment length 16, baseline, precision 8, 1280x720, components 3 </pre>																					
2	<p>We apply convert and</p> <p>We see that both files have different sizes, so we apply binwalk with -e. A folder _socute.jpg.extracted a file named 'donotshare' that contains a strange text</p>	<pre> root@htbfeal:~/Downloads/misc/Longbottom's_Locker# convert socute.jpg socute_conv.jpg root@htbfeal:~/Downloads/misc/Longbottom's_Locker# ls index.html "Longbottom's_Locker.zip" neville.gif socute_conv.jpg socute.jpg root@htbfeal:~/Downloads/misc/Longbottom's_Locker# binwalk -e socute.jpg </pre> <table border="1"> <thead> <tr> <th>DECIMAL</th><th>HEXADECIMAL</th><th>DESCRIPTION</th></tr> </thead> <tbody> <tr> <td>0</td><td>0x0</td><td>JPEG image data, JFIF standard 1.01</td></tr> <tr> <td>97465</td><td>0x17CB9</td><td>Zip archive data, at least v2.0 to extract, name: donotshare</td></tr> <tr> <td>99087</td><td>0x1830F</td><td>Zip archive data, at least v1.0 to extract, name: _MACOSX/</td></tr> <tr> <td>99142</td><td>0x18346</td><td>Zip archive data, at least v2.0 to extract, name: _MACOSX/</td></tr> <tr> <td>.donotshare</td><td></td><td></td></tr> <tr> <td>99574</td><td>0x184F6</td><td>End of Zip archive, footer length: 22</td></tr> </tbody> </table> <pre> root@htbfeal:~/Downloads/misc/Longbottom's_Locker# ls index.html neville.gif socute.jpg "Longbottom's_Locker.zip" socute_conv.jpg _socute.jpg.extracted </pre>	DECIMAL	HEXADECIMAL	DESCRIPTION	0	0x0	JPEG image data, JFIF standard 1.01	97465	0x17CB9	Zip archive data, at least v2.0 to extract, name: donotshare	99087	0x1830F	Zip archive data, at least v1.0 to extract, name: _MACOSX/	99142	0x18346	Zip archive data, at least v2.0 to extract, name: _MACOSX/	.donotshare			99574	0x184F6	End of Zip archive, footer length: 22
DECIMAL	HEXADECIMAL	DESCRIPTION																					
0	0x0	JPEG image data, JFIF standard 1.01																					
97465	0x17CB9	Zip archive data, at least v2.0 to extract, name: donotshare																					
99087	0x1830F	Zip archive data, at least v1.0 to extract, name: _MACOSX/																					
99142	0x18346	Zip archive data, at least v2.0 to extract, name: _MACOSX/																					
.donotshare																							
99574	0x184F6	End of Zip archive, footer length: 22																					
3	<p>I came to the conclusion that it is a banner and should be used python pickle:</p> <p>save this code as pick.py and convert the donotshare file.</p>	<pre> import pickle f = open('banner.p') o = pickle.load(f) outstr = '' for line in o: for char, n in line: outstr += char * n outstr += '\n' print outstrip </pre>																					
4	The output is ...	<pre> root@htbfeal:~/Downloads/misc/Longbottom's_Locker/_socute.jpg.extracted# python2 pickling.py </pre> 																					
5	<p>Then go to index.html and insert the output as password to get this flag.</p>	<p>Here's your secret Neville, HTB{n3v1LL3_Da_burM3s3-pyth0n_sL4y3r}</p> <div>OK</div>																					

8. ETERNAL LOOP = 20 POINTS

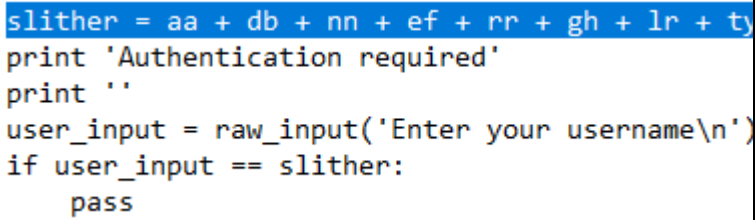
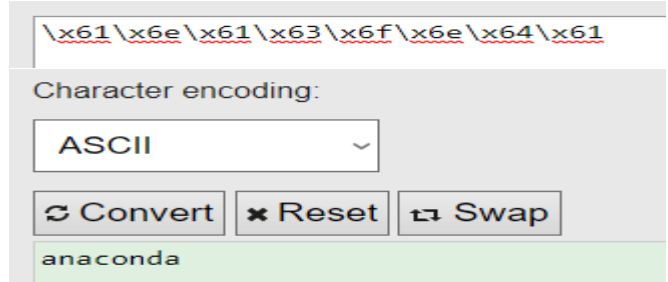
1	First, must make a script / program to decompress recursively inside the zip files. Go online and search for the script.	<pre> unzip_all() { zipfile="\$1" next_zipfile="\$(unzip -Z1 "\$zipfile" head -n1)" if echo "\$next_zipfile" grep "\.zip\$"; then unzip -P "\${next_zipfile%.*}" "\$zipfile" unzip_all "\$next_zipfile" fi } unzip_all "file1.zip" </pre>
2	Run the script and found the last zip. The last zip dont found the passwd. So had to crack	<pre> root@htbfesal:~/Downloads/misc/Eternal Loop# chmod +x script.sh root@htbfesal:~/Downloads/misc/Eternal Loop# ./script.sh 5900.zip Archive: 37366.zip inflating: 5900.zip 49805.zip Archive: 5900.zip inflating: 49805.zip 13811.zip Archive: 49805.zip inflating: 13811.zip 45133.zip Archive: 13811.zip inflating: 45133.zip 4030.zip Archive: 45133.zip inflating: 4030.zip 12132.zip Archive: 4030.zip </pre>
3	Run fcrackzip for the last zip and get the passwd.	<pre> root@htbfesal:~/Downloads/misc/Eternal Loop# fcrackzip -v -D -u -p /usr/share/wor dlists/rockyou.txt 6969.zip found file 'DoNotTouch', (size cp/uc 335181/884736, flags 9, chk 5b04) PASSWORD FOUND!!!!: pw == letmeinplease </pre>
4	Go to the last zip and enter the sqlite3 database and find the flag.	<p>Email:</p> <p>HTB{z1p_and_unz1p_ma_bruddahs}</p>

REVERSING CHALLENGE

1. IMPOSSIBLE PASSWORD = 30 POINTS

1	Make a script with the enc and xor_key	 <pre> enc = "A]Kr=9k0=0o0;k1?k81t" xor_key = 0x9 dec = "" for c in enc: dec += str(chr(ord(c)^xor_key)) print "[+] Found: {}".format(dec) </pre>
2	Flag appear!!	 <pre> root@htbfesal:~/Downloads/RE/Impossible Password# python break.py [+] Found: HTB{40b949f92b86b18} root@htbfesal:~/Downloads/RE/Impossible Password# </pre>


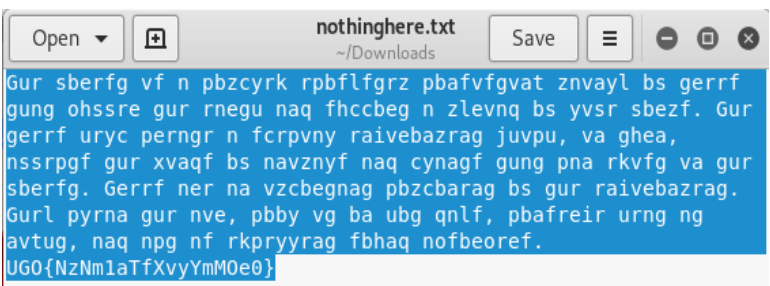
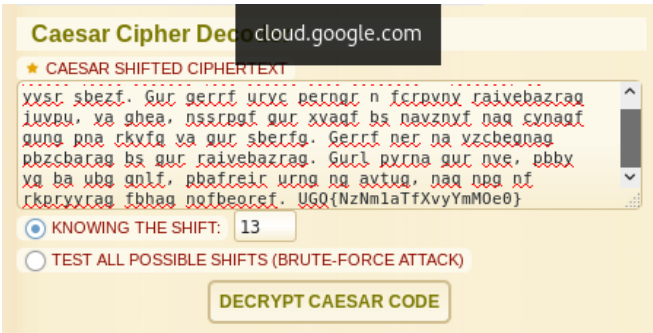
2. SNAKE = 10 Points

1	In the python code, we know that slither has username	 <pre> slither = aa + db + nn + ef + rr + gh + lr + ty print 'Authentication required' print '' user_input = raw_input('Enter your username\n') if user_input == slither: pass </pre>
2	So convert the "aa + db + nn + ef + rr + gh + lr + ty" to (\x61\x6e\x61\x63\x6f\x6e\x64\x61)	
3	Decode the Hex value to ASCII and value is anaconda. It is for username.	
4	Decode all the Hex value to get hint for the question. On the right are the converted hex.	<ol style="list-style-type: none"> 1. Chains = this is a troll (15) 2. Keys = password (10) 3. Password = its not that easy 4. Auth = keep trying

5	Add this code to get the password	<pre> 40 print 'password', 41 for char in chars: 42 print str(chr(char)), </pre>
6	<p>Run the snake.py and we get 25 characters of password but the hint said it is 10 chars long. So take only first 10 chars which is udvvrjwa\$\$ and we get the right password.</p> <p>The flag is HTB{anaconda:udvvrjwa\$\$}</p>	<pre> The Snake Created by 3XPL017 Your number is 215 password u d v v r j w a \$ \$ ~ r s } * s } * l Authentication required Enter your username anaconda Enter your password u d v v r j w a \$ \$ Good Job </pre>

STEGO CHALLENGES



1. FOREST = 40 POINTS

1	Open the image and brighten it in Image Magick to discover hidden text. Here the hidden text.	
2	Run command "steghide extract -sf forest.jpg" and enter the passphrase as the hidden text.	<pre>root@htbfesal:~/Downloads# steghide extract -sf forest.jpg Enter passphrase: wrote extracted data to "nothinghere.txt". root@htbfesal:~/Downloads#</pre>
3	after success you see nothinghere.txt and open it and copy the text to decode it.	
4	Go to https://www.dcode.fr/caesar-cipher and paste the text to decode. The shift key is 13.	
5	Then see the flag in format HTB{texthere} as below.	<pre>Caesar Cipher - Shift by 13 NOPQRSTUVWXYZABCDEFGHIJKLM ABCDEFGHIJKLMN0PQRSTUVWXYZ The forest is a complex ecosystem consisting mainly of trees that buffer the earth and support a myriad of life forms. The trees help create a special environment which, in turn, affects the kinds of animals and plants that can exist in the forest. Trees are an important component of the environment. They clean the air, cool it on hot days, conserve heat at night, and act as excellent sound absorbers. HTB{AmAzInGsKillZBr0}</pre>

2. RETRO = 50 Points



1	Extract binary file from image and got retro.jpg	<pre>root@htbfsal:~/Downloads# binwalk -e retro.jpg</pre> <table border="1"> <thead> <tr> <th>DECIMAL</th> <th>HEXADECIMAL</th> <th>DESCRIPTION</th> </tr> </thead> <tbody> <tr> <td>28</td> <td>0x1C</td> <td>TIFF image data, big-endian, offset of first image directory: 8</td> </tr> <tr> <td>233685</td> <td>0x390D5</td> <td>Zip archive data, at least v2.0 to extract, compressed size: 76, uncompressed size: 87, name: eighties_were_nice.txt</td> </tr> <tr> <td>233813</td> <td>0x39155</td> <td>Zip archive data, at least v2.0 to extract, compressed size: 3991, uncompressed size: 549308, name: retro.wav</td> </tr> <tr> <td>238038</td> <td>0x3A1D6</td> <td>End of Zip archive, footer length: 22</td> </tr> </tbody> </table>	DECIMAL	HEXADECIMAL	DESCRIPTION	28	0x1C	TIFF image data, big-endian, offset of first image directory: 8	233685	0x390D5	Zip archive data, at least v2.0 to extract, compressed size: 76, uncompressed size: 87, name: eighties_were_nice.txt	233813	0x39155	Zip archive data, at least v2.0 to extract, compressed size: 3991, uncompressed size: 549308, name: retro.wav	238038	0x3A1D6	End of Zip archive, footer length: 22
DECIMAL	HEXADECIMAL	DESCRIPTION															
28	0x1C	TIFF image data, big-endian, offset of first image directory: 8															
233685	0x390D5	Zip archive data, at least v2.0 to extract, compressed size: 76, uncompressed size: 87, name: eighties_were_nice.txt															
233813	0x39155	Zip archive data, at least v2.0 to extract, compressed size: 3991, uncompressed size: 549308, name: retro.wav															
238038	0x3A1D6	End of Zip archive, footer length: 22															
2	Decode wave file with turggen	<pre>root@htbfsal:~/Downloads/turgen_system-8.6.11.bin# java -jar turgen.jar "r3tr0-1s-4l1v3"</pre>															
3	Go to tab,tools>turbo decoder and select the retro.wav file and select the output directory. Set the jump to 341365 and click "decode until EOF".																
4	Set the jump to 87266 and click "decode one file"																
5	Open terminal in output directory of retro wav, and type "string *.tm" and flag is appear.	<pre>File Edit View Search Terminal Help root@htbfsal:~/Downloads/outputRetro# strings *.tm flag flag "r3tr0-1s-4l1v3" "r3tr0-1s-4l1v3"</pre>															

3. DA VINCI = 30 Points

1	The password is TOM at the image of people.													
2	"steghide extract -sf Thepassword_is_the_small_name_of_the_actor_named_Hanks.jpg" and insert the password	<pre>root@htbfesal:~/Downloads/stego/DaVinci# steghide extract -sf Thepassword_is_the_small_name_of_the_a ctor_named_Hanks.jpg Enter passphrase: wrote extracted data to "S3cr3t_m3ss@g3.txt".</pre>												
3	Let decode the md5 hash from the extracted data.. (key:020e60c6a84db8c5d4c2d56a4e4fe082) and found "leonardo"	<p>Enter your MD5 hash below and cross your fingers :</p> <div>020e60c6a84db8c5d4c2d56a4e4fe082</div> <div>Decrypt</div> <p>Found : leonardo (hash = 020e60c6a84db8c5d4c2d56a4e4fe082)</p>												
4	Check string at Plan.jpg file; "strings Plan.jpg" and found the youtube link and open. The title of youtube is Guernica	<pre>k]]@ https://www.youtube.com/watch?v=jc1Nfx4c5LQ root@htbfesal:~/Downloads/stego/DaVinci#</pre>												
5	Check the monalisa img "binwalk -e monalisa.jpg" and got file zip.	<pre>root@htbfesal:~/Downloads/stego/DaVinci# binwalk -e monalisa.jpg</pre> <table><thead><tr><th>DECIMAL</th><th>HEXADECIMAL</th><th>DESCRIPTION</th></tr></thead><tbody><tr><td>0</td><td>0x0</td><td>JPEG image data, JFIF standard 1.0</td></tr><tr><td>450363</td><td>0x6DF3B</td><td>Zip archive data, at least v2.0 to extract, uncompressed size: 117958, name: famous.zip</td></tr><tr><td>450440</td><td>0x6DF88</td><td>Zip archive data, encrypted at least v2.0</td></tr></tbody></table>	DECIMAL	HEXADECIMAL	DESCRIPTION	0	0x0	JPEG image data, JFIF standard 1.0	450363	0x6DF3B	Zip archive data, at least v2.0 to extract, uncompressed size: 117958, name: famous.zip	450440	0x6DF88	Zip archive data, encrypted at least v2.0
DECIMAL	HEXADECIMAL	DESCRIPTION												
0	0x0	JPEG image data, JFIF standard 1.0												
450363	0x6DF3B	Zip archive data, at least v2.0 to extract, uncompressed size: 117958, name: famous.zip												
450440	0x6DF88	Zip archive data, encrypted at least v2.0												
6	Extract the famous.zip with md5 decoded password and Mona.jpg appear.													

7	Steghide the image and use "Guernica" as password and key file appear.	<pre> root@htbfesal:~/Downloads/stego steghide extract -sf Mona.jpg Enter passphrase: wrote extracted data to "key". root@htbfesal:~/Downloads/stego </pre>
8	Show the key. It is base64	<pre> root@htbfesal:~/Downloads/stego/DaVinci/_monalisa.jpg.extracte cat key VTBaU1EyVXdNSGRpYTBKbVZFukdObEZHT0doak1UbEZUVEJDULdaU1BUMD0= </pre>
9	Decode the base64 key online. Decode three time of each value to show the final flag	<div>< DECODE > Decodes y</div> <div>HTB{M0n@_L1z@_!s_D3@D}</div>

4. DIGITALCUBE = 60 Points

1	Extract and found digitalcube.txt and it is binary so let convert it to image. The output is barcode.	<div> <h3>Binary Image Creator</h3> <p>★ BINARY LIST OF PIXELS (0 AND 1)</p> <pre> 110011111100110000001100000000011000000001100110011001 111110011000000110000000000110000000011001100110000000 001100110000001100111100001111110011110011000000000110 01100000011001111000011111100111100111111111111001100 1111001111110011000000110011111111111111111100110011110 0111111001100000011001111 </pre> <p>★ WIDTH OF THE PICTURE <input type="text" value="50"/> (optional)</p> <p>★ INVERT (WHITE = 0, BLACK = 1) <input checked="" type="checkbox"/></p> <p>DRAW</p> </div>
2	We got qrcode and let scan it	
3	Barcode reader online and scan it to view the flag	<div> <h3>Free Online Barcode Reader</h3> <p>1. Select barcode types</p> <div> <input checked="" type="checkbox"/> 1D: Code 39, Code 128... <input type="checkbox"/> PDF417 <input type="checkbox"/> Postal: IMB, 4state ... </div> <div> <input checked="" type="checkbox"/> QR code <input type="checkbox"/> DataMatrix <input type="checkbox"/> Driver License, ID cards </div> <p>2. Select Image File (PDF, TIFF, JPEG, BMP, GIF, PNG, WMF, WEBP)</p> <p><input type="button" value="Browse..."/> dcode-image(1).pi</p> <p>Maximum file size: 12 Mb.</p> <p>3. <input type="button" value="Read"/></p> </div>
4	The flag is.....	<div> <p>File: dcode-image(1).png <input type="button" value="New"/></p> <p>Pages: 1 Barcodes: 1 Page 1 of 1</p> <p>Barcode: 1 of 1 Type: QR Length: 17 Rotation: none Module: 2.0pix Rectangle: {X=0,Y=0,Width=48,Height=48}</p> <p>HTB{QR_!snt_d34d}</p>  </div>

5. BEATLES = 40 Points




1	Open m3ss@g#_f0r_pAuL file. Here we got random message. I think it is caesar cipher text .	<pre> Url Cnhy, Zl Sbyqre unf cnffcuenfr jvgu sbhe (4) punenpgref. Pbhyq lbh spenpx vg sbe zr??? V fraq lbh n zrffntr sbe bhe Gbhe arkg zbagu... Qba'g Funer vg jvgu bgure zrzuref bs bhe onaq... -Wbua Yraaba CF: Crnpr naq Ybir zl sevraq... Orngyrf Onaq sbe rire! </pre>
2	So , i decode it with shift key 13 and get this message	<pre> Caesar Cipher - Shift by 13 NOPQRSTUVWXYZABCDEFGHIJKLM ABCDEFGHIJKLMNOPQRSTUVWXYZ Hey Paul, My Folder has passphrase with four (4) characters. Could you fcrack it for me??? I send you a message for our Tour next month... Don't Share it with other members of our band... -John Lennon PS: Peace and Love my friend... Beatles Band for ever! </pre>
3	So let attack passphrase with dictionary file; "fcrackzip -u -D -p /usr/share/wordlists/fasttrack.txt BAND.zip" and found something!!	<pre> root@htbfesal:~/Downloads/stego/Beatles# fcrackzip -u -D -p /usr/share/wordlists /fasttrack.txt BAND.zip PASSWORD FOUND!!!!: pw == pass </pre>
4	Lets use steghide at the current image; "steghide extract -sf BAND.JPG -p THEBEATLES"	<pre> root@htbfesal:~/Downloads/stego/Beatles# steghide extract -sf BAND.JPG -p THEBEA TLES wrote extracted data to "testabeatle.out ". </pre>

5	Let try to strings the testabeatle.out file; and we get message to Paul. it has base64 message as well.	<pre> Hey Paul! If you are here... Give my your favourite character! Ok Paul... A little challenge for you mate, cause last month someone crazy man hacked.. .WTF! Let's Begin! #####Challenge##### ##### Tell me PAul! The result of 5+5? Ok!ok! it was easy... Tell me now... The result of: 5+5-5*(5/5)? Last one! The result of: (2.5*16.8+1.25*10.2+40*0.65+1.5*7.5+1.25*3.2):40 Hey Paul! nice!!! this is the message VGhlIHRvdXIgd2FzIGNhbmNlbGVkIGZvc1B0aGUgZm9sbG93aW5nIGlvdnRoLi4uIQ0KDQpJJ2xsIGdvIG91dCBmb3IgdGZlbnV5IHdpdGggYXkgZ2lybGZyaWVucyZCBuYW1lZCBZb2NvISA7K00KDQpIVEJ7UzByUnlfTXlflRlIxM25EfQ0K WTF! You are not Paul!! SOS SOS HACKER HERE!! I will call the police someone want t o steal my data!!! #####END OF CHALLENGE##### ##### </pre>
6	Let decode to base64 and what we got!!!	<div>< DECODE > Decodes your data into the textar</div> <div> <p>The tour was canceled for the following month...!</p> <p>I'll go out for dinner with my girlfriend named <u>Yoco!</u> ;)</p> <p><u>HTB</u>{S0rRy_My_FR13nD}</p> </div>


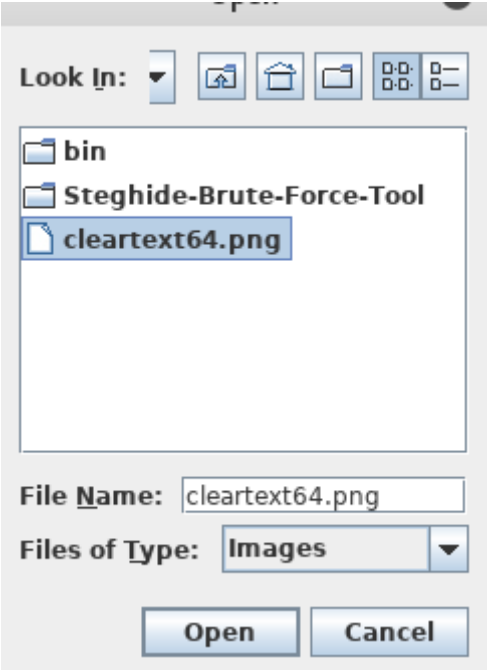
6. UNIFIED = 20 Points

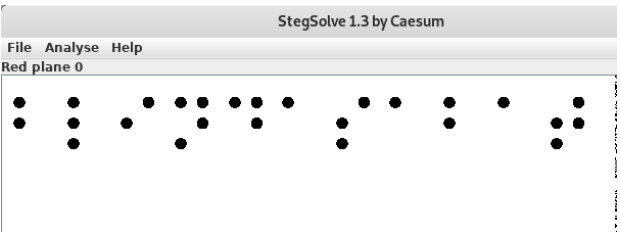
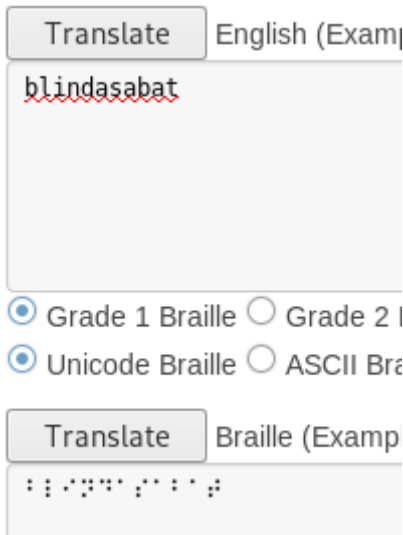
1	Extract the file and got BOD_30079.txt. Open it.	<p>The system works in many languages. 该系统以许多语言工作. يعمل النظام في العديد من اللغات.</p> <p>0000 0000 00 00000000 000 00000 0 0000 000 00</p> <p>To σύστημα λειτουργεί σε πολλές γλώσσες. Система работает на многих языках.</p>
2	Oh, it UTF character. Let decode in burpsuite.	<p> Burp Intruder Repeater Window Help Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder C </p> <p>The system works in many languages. 该系统以许多语言工作. يعمل النظام في العديد من اللغات.</p> <p>0000 0000 00 00000000 000 00000 0 0000 000 00</p> <p>To σύστημα λειτουργεί σε πολλές γλώσσες. Система работает на многих языках.</p>
3	The output is ...	<p>The system works in many languages. ðüßä, ðäL j9ED 'DF8'E AJ 'D9/JJ EF 'DO:*</p> <p>@H@T@B@{(@@r@1@t@h@3@m@1@u@5@_@1@4@9@9@jyýýý ýýýý ýý ýýýýýýýý ýýý ýýýý ýý ýýý ýý ýý</p> <p>ηζ ΑΙΑΑ %ζ± »μΰΑζΑΑΰι Αμ Αζ»»-Α *»ΙΑΑμΑ.Ι8ΑΒ5<0 @01>Β05Β =0 <=>38Ε 07Κ.0Ε.</p>
4	Here is the flag; HTB{tr1th3m1u5_1499}	

7. PUSHEEN LOVES GRAPHS = 30 Points

1	Extract the file and we got Pusheen file.	 Pusheen	 Pusheen.zip
2	Dissemble it in IDA. but,we got error when load the exe file. The error is the max amount of nodes is 1000. So, i change it to 20000. Boom, some text appear.		
3	The flag format is HTB{text_here}. So , just completed the format as well.	HTB{fUn_w17h_CFGz}	


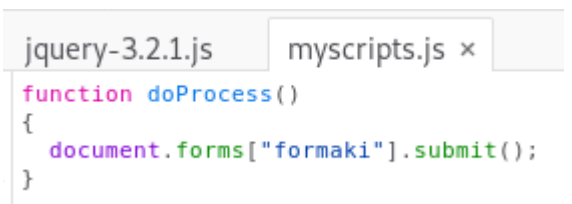
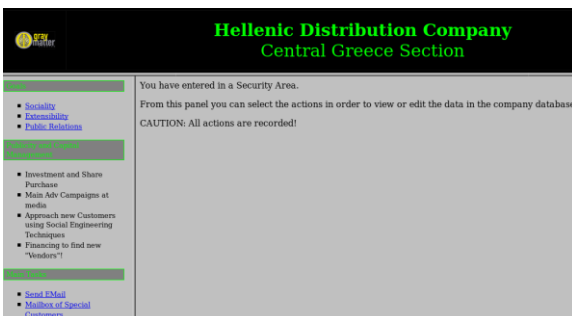
8. SENSELESS BEHAVIOUR = 50 Points

1	Let bruteforce the meow.wav file with steg_brute.py. We got password and extracted file name meow_flag.txt	<pre> root@htbfesal:~/Downloads/stego/Senseless Behaviour# python steg_brute.py -b -d rockyou.txt -f meow.wav [i] Searching... 0% wrote extracted data to "meow_flag.txt". [+] Information obtained with password: skittles ODK1MDR\NDcwZDBhMWEwYTAWMDAwMDBkNDk0ODQ8NTIwMDAwMDJiZTAwMDAwMThiMDgwNjAwMDAw Aw </pre>
2	The output is text with random character. It might be base64 format.let remove unwanted character and letter.	<pre> root@htbfesal:~/Downloads/stego/Senseless Behaviour# cat meow_flag.txt s ed '/^\s\$/d' base64 -d xxd -r -p > cleartext64.png </pre>
3	So , we will get the cleartext64.png as output .png file.	
4	Now, use stegsolve. Open the output file and find the interesting info.	<pre> root@htbfesal:~/Downloads/stego/Senseless Behaviour/bin# j ava -jar stegsolve.jar </pre> 

5	Wow, after navigating, i found braille text.	 <p>The screenshot shows a window titled "StegSolve 1.3 by Caesum" with a menu bar (File, Analyse, Help). Below the menu, it says "Red plane 0". The main area displays a series of Braille characters arranged in a single line.</p>
6	Let decode the braille and see what happen. It is "blindasabat". Change it to HTB{blindasabat} format.	 <p>The screenshot shows a web-based Braille translation tool. At the top, there is a "Translate" button and a dropdown menu set to "English (Example)". Below this is a text input field containing the text "blindasabat". Under the input field, there are four radio buttons: "Grade 1 Braille" (selected), "Grade 2 Braille", "Unicode Braille", and "ASCII Braille". Below the radio buttons, there is another "Translate" button and a dropdown menu set to "Braille (Example)". Below this is a text output field displaying the Braille representation of the input text.</p>

WEB CHALLENGES

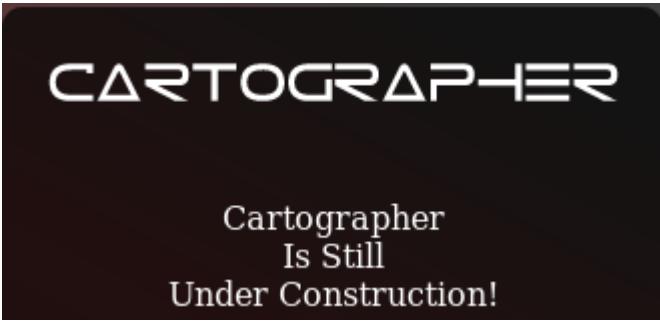
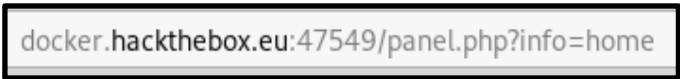

1. HDC = 30 Points

1	Go to http://docker.hackthebox.eu:47479/	
2	so i press f12 and digging around, i saw two hidden inputs and when we submit the form it triggers the doProcess() function	<pre><p align="center"> <input value="name=&quot;name1&quot;" type="hidden"> <input value="name=&quot;name2&quot;" type="hidden"> <input value="Submit" onclick="doProcess()" type="button"> </p></pre>
3	Then, i saw a custom js myscripts. I think it maybe scripted by the owner. It related to the submit function of hidden inputs.	
4	So, i decided to explore the jquery-3.2.1.js and search for doProcess and found value for input name1 and name2. It look like credential.	<pre>function doProcess() { var form = document.createElement("form"); form.setAttribute("method", "post"); form.setAttribute("action", "main/index.php"); form.setAttribute("target", "view"); var hiddenField = document.createElement("input"); hiddenField.setAttribute("type", "hidden"); hiddenField.setAttribute("name", "name1"); hiddenField.setAttribute("value", "TX1MaXR0bGU"); var hiddenField2 = document.createElement("input"); hiddenField2.setAttribute("type", "hidden"); hiddenField2.setAttribute("name", "name2"); hiddenField2.setAttribute("value", "cDB3bm1l"); form.appendChild(hiddenField2); form.appendChild(hiddenField); }</pre>
5	Let try login with the credential. look , we success to login!!	
6	Based on the question hint;	<div style="border: 1px solid black; padding: 5px;"><i>We believe a certain individual uses this website for shady business etc...</i></div>

7	<p>so now i had to find the mail of the individual.</p> <p>i clicked at Mailbox of Special Customers and i got this</p>	<div>Special Customers' Mailbox </div> <div>Up to now we have 5 special customers who will help us to achieve our goals.</div> <div>This list will soon be expanded with the new 'expansion program' for our corporate goi</div> <div>It is planned that within the next six months we will have reached 20 dedicated Special</div> <div>*****</div>
8	<p>based my little experience in ctf, I learned to check the path and the source code of the images so i decided to check the small image that appears in the right side in the page title. i opened the image on a new tap and i found url????!!.</p>	<div>/main/secret_area_/mails.gif</div>
9	<p>Here im try to traverse thru link backward and found interesting file.</p>	<div>Index of /main/secret</div> <div><div>Name</div><div>Last modified</div><div>Size</div><div>De</div></div> <div><div></div><div>Parent Directory</div><div>-</div></div> <div><div></div><div>mails.gif</div><div>2010-10-23 18:28</div><div>71</div></div> <div><div></div><div>mails.txt</div><div>2017-07-08 17:55</div><div>705</div></div>
10	<p>Click the mails.txt and got this!!</p>	<div>All good boys are here... hehehehehehe!</div> <div>-----</div> <div>Peter Punk CallMePink@newmail.com</div> <div>Nabuchodonosor BabyNavou@mailpost.gr</div> <div>Ilias Magkakos imagkakos@badmail.com</div> <div>Nick Pipshow NickTheGreek@mail.tr.gr</div> <div>Don Quixote Windmill@mail.gr</div> <div>Crazy Priest SeVaftise@hotmail.com</div> <div>Fishroe Salad fishroesalad@mail.com</div> <div>TaPanta Ola OlaMaziLeme@mail.gr</div> <div>Laertis George I8aki@mail.gr</div> <div>Thiseas Sparrow Pirates@mail.gr</div> <div>Black Dreamer SupaHacka@mail.com</div> <div>Callme Daddy FuckthemALL@mail.com</div> <div>Aggeliki Lykolouli FwsStoTounel@Traino.pourxetai</div> <div>Kompinadoros Yannnnis YannisWith4N@rolf.com</div> <div>Serafino Titamola Ombrax@mail.gr</div> <div>Joe Hard Soft@Butter.gr</div> <div>Bond James MyNameIsBond@JamesBond.com</div> <div>Endof Text EndOfLine@mail.com</div>
11	<p>Based on other question hint; hmmm. one thing come into my head !!Burpsuite!!</p>	<div>Can you find out who that is and send him an email to check, using the web site's functionality?</div>
12	<p>i intercepted the request, sent it to Intruder added the list of emails as payload and click attack. now after the attack completed i stated analyse all the request's and and yeah!! I finally got the Flag :D</p>	<div>Payload Options [Simple list]</div> <div>This payload type lets you configure a simple list of strings that are used as payloads.</div> <div><div><div>Paste</div><div>Load ...</div><div>Remove</div><div>Clear</div></div><div><div>i8aki@mail.gr</div><div>pirates@mail.gr</div><div>supaHacka@mail.com</div><div>fuckthemALL@mail.com</div><div>fwsStoTounel@Traino.pourxetai</div><div>yannisWith4N@rolf.com</div><div>Ombrax@mail.gr</div><div>Soft@Butter.gr</div><div>MyNameIsBond@JamesBond.com</div><div>EndOfLine@mail.com</div></div></div> <div><div>Add</div><div>Enter a new item</div></div> <div><div>Add from list ... [Pro version only]</div></div>

13	<p>So i enter the email and what !!</p> <p>The flag is in this picture!!</p>	<p>Re: Hello there!</p> <p>Hi, I am still alive, don't worry :) Congratz my friend!!</p> <p>The flag is:</p> <p>HTB{FuckTheB3stAndPlayWithTheRest!!}</p>
----	--	---

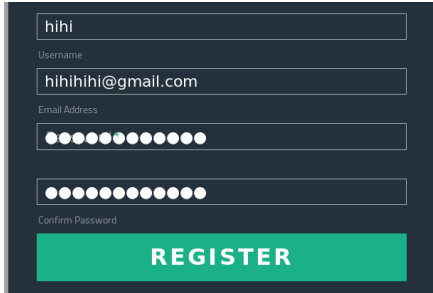


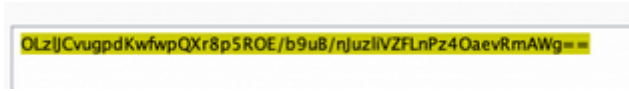

2. CARTOGRAPHER = 30 POINTS

1	First, i press f12 to see the code. Get the username and password field but there's no action parameter??	<pre><form method="post"> <input class="textbox" name="username" placeholder="Username" type="text">
 <input class="textbox" name="password" placeholder="Password" type="password">
 <input class="loginbutton" value="Login" type="submit"> </form></pre>
2	Then,im looking for hint in the forum and i try to make sql. Lulz..it work!	
3	Here is the url changed	
4	But, i dont know what to do yet. Looking for clue and it just change the link to what we are looking for?? It is flag broo! Just by changing info=home to info=flag...	

3. LERNAEAN = 20 POINTS

1	This is the login page. There is also Error message of invalid password. The error message is useful to bruteforce the password.	
2	Try to ping to look for IP	<pre>root@htbfesal:~# ping docker.hackthebox.eu PING docker.hackthebox.eu (159.65.208.41) 56(84)</pre>
3	Now, im tried hydra to bruteforce with info about the website needed. Haha, got the password. So, let try login	<pre>root@htbfesal:~/Desktop# hydra -l admin -P /usr/share/wordlists/rockyou.txt 159.65.208.41 http-post-form "[:password='PASS':Invalid password!]" -s 47563 Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes. Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-05-12 12:52:39 [WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore [DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (1:1/p:14344399), ~896525 tries per task [DATA] attacking http-post-form://159.65.208.41:47563/:password='PASS':Invalid password! [47563][http-post-form] host: 159.65.208.41 login: admin password: leonardo 1 of 1 target successfully completed, 1 valid password found Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-05-12 12:53:33</pre>
4	Success login but get this message. What the?? It say im too slow? What does it mean? I think we have to grab the request and look at the reply? Burpsuite again?	
5	Let try BS and intercept request. Use repeater and check the response. Nah...what we got there?? HTB{lik3_4_b0s5_s0n}	<p>Response</p> <p>Raw Headers Hex HTML Render</p> <pre>HTTP/1.1 200 OK Date: Sun, 12 May 2019 05:45:53 GMT Server: Apache/2.4.18 (Ubuntu) Vary: Accept-Encoding Connection: close Content-Type: text/html; charset=UTF-8 Content-Length: 618 <h1 style='color: #fff;'>HTB{lik3_4_b0s5_s0n}</h1><script window.location = "noooooooooope.html"></script> <html> <head> <title>Login - Lernaean</title> </head></pre>

4. *I KNOW MAG1K* = 50 Points

1	First create new account	
2	By logging into the system with the user information created, the interfaces and request contents sent in the application are started to be examined.	
3	After successful login, only session value görülmek iknowmag1k at is assigned to the user.	
4	Then, decode the base64 of the session value and got this....	
5	Then use padbuster and change to user: admin and role: admin. the session value created with the role value "admin m is obtained - "LDRCU61StZbYrdIXPROTGIpri45i7IsYMAovrw2IGp8AAAAA AAAAAA% 3D% 3D"	
6	The session value obtained in the last step is placed into the pr /profile.php "request in the" Burp Suite - Repeater "tab and access to the" admin "profile screen. Now, we got the final flag..yess	