



Sri Lanka Institute of Information Technology

CTF Walkthrough

ISP Project

Information Security Project 2022

Project ID: ISP-22-REG-10

Submitted by:

IT Number	Name
IT19065236	Maddumage M.
IT19172088	Kodagoda K. G. S. S. K

Step 01

Go to <http://13.233.103.145/> and it redirects to the login page. In the login page there is a hidden text “Hey I can’t register” Then go to register page and analyze page source to find text that encoded via Base 64

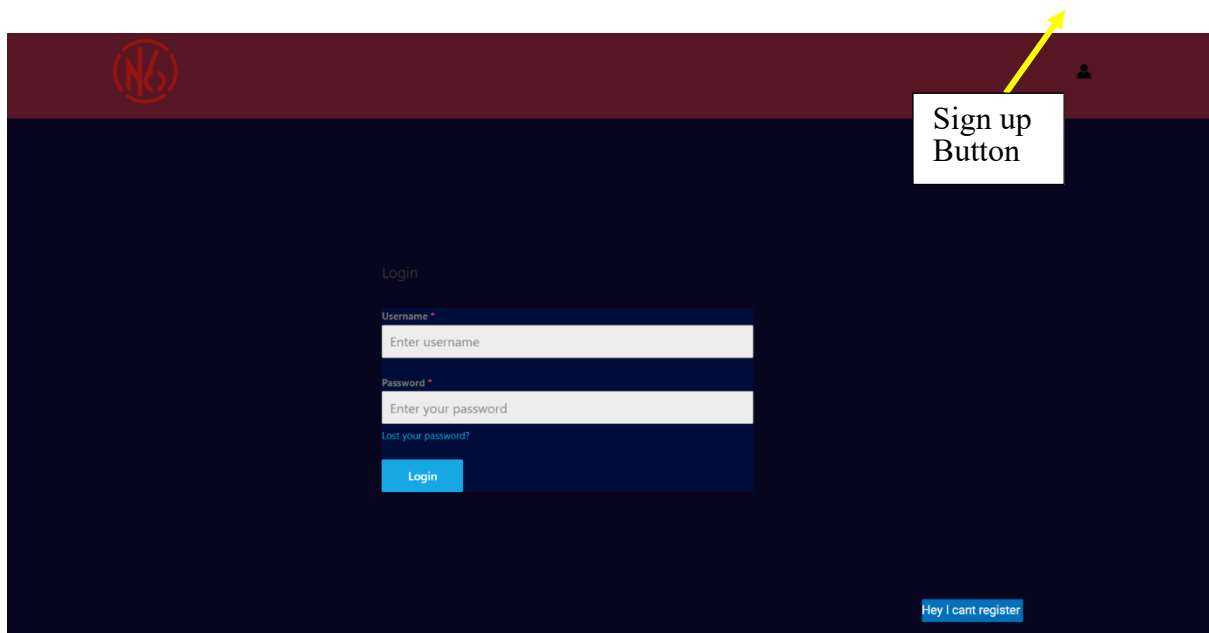


Figure 1 Login Page with Hidden text



Figure 2 Sign up Page

```

    <div class="forminator-response-message forminator-error" aria-hidden="true"></div><div class="forminator-row"><div id="text-1" class="forminator-col forminator-col-12"><div class="forminator-f
    </div>
    </div>
  </section>
  <section class="elementor-section elementor-top-section elementor-element elementor-element-18f76d3 elementor-section-boxed elementor-section-height-default elementor-section-height-default">
    <div class="elementor-container elementor-column-gap-default">
      <div class="elementor-column elementor-col-100 elementor-top-column elementor-element elementor-element-46e1261" data-id="46e1261" data-element_type="column">
        <div class="elementor-widget-wrap elementor-element-populated">
          <div class="elementor-element elementor-element-347af6d elementor-widget elementor-widget-html" data-id="347af6d" data-element_type="widget" data-widget_type="html.default">
            <div class="elementor-widget-container">
              <!-- Q1RGe1VzZW50bWUgYW50bWUgYXNzd29yZCBmb3JgdXNlIHBoZ2UgaXNlbnRmFtZSA6IGFnZW50c3NlYWd1bGwgcGFzc3dvcnQgOiAy dEckNnVUFQ -->
            </div>
          </div>
        </div>
      </div>
    </section>
  </div>
</div><!-- .entry-content .clear -->

</article><!-- #post-## -->
</main><!-- #main -->

```

Figure 3 Encoded Text in page source

Then decode the text to get login credentials to login as an agent.

Simply enter your data then push the decode button.

Q1RGe1VzZW50bWUgYW50bWUgYXNzd29yZCBmb3JgdXNlIHBoZ2UgaXNlbnRmFtZSA6IGFnZW50c3NlYWd1bGwgcGFzc3dvcnQgOiAy dEckNnVUFQ

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

☒ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

CTF{Username and the password for use page is username : agentsseagull password : 2tG\$6uT}

Figure 4 Decoded Text

Then login to the system using those credentials. And the link redirect to the website's home page.

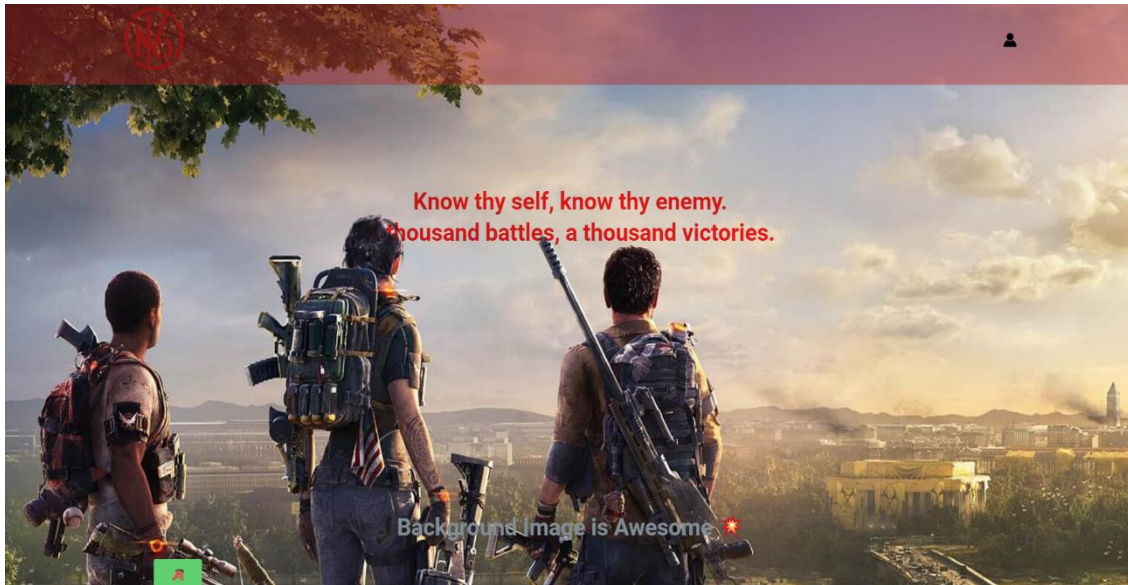


Figure 5home page

STEP 2 and 3 :

The goal of this step is to download the background image and find the hidden content in it (hidden map), using steganography.

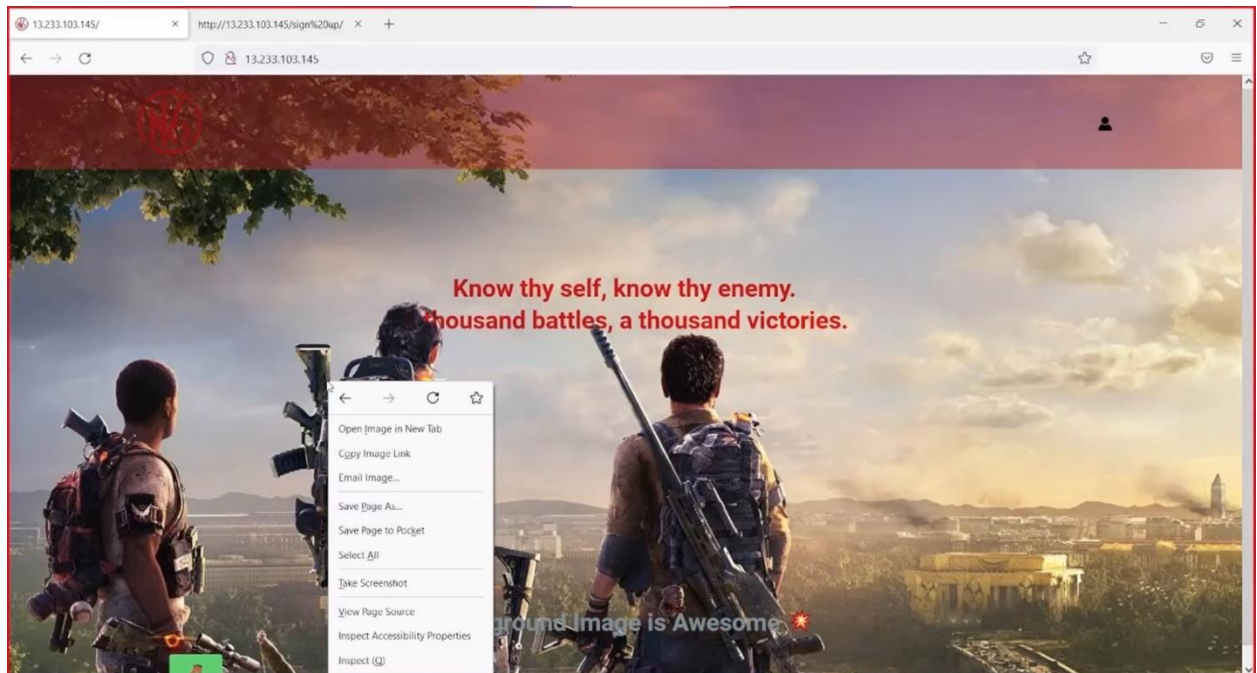


Figure 6

Use of QuickStego tool is recommended in this step.

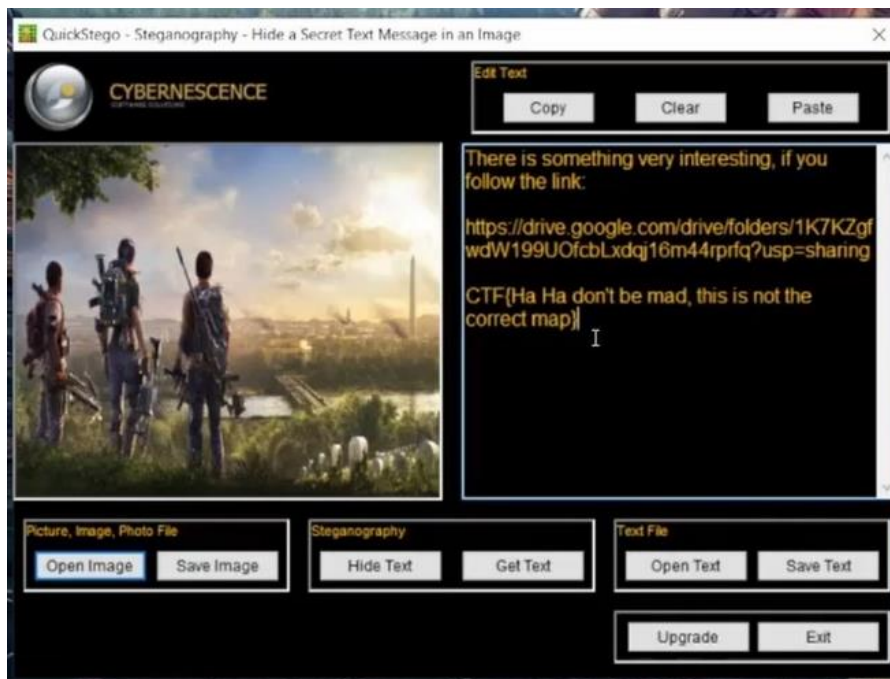


Figure 7

After revealing the image CTF{Ha Ha don't be mad, this is not the correct map} is the flag. As it is mentioned the image is not here and another link is given to reveal the secret content.

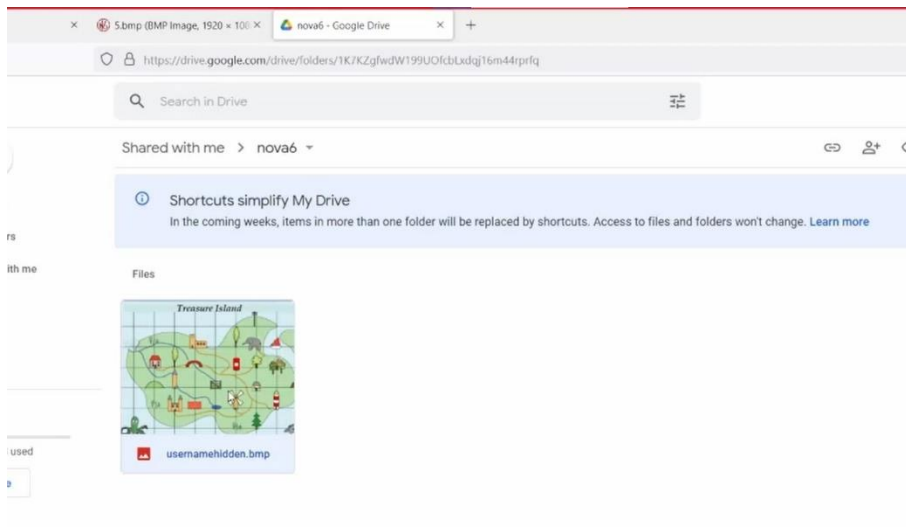


Figure 8

After downloading that image in the link, reveal the secrets via QuickStego tool again

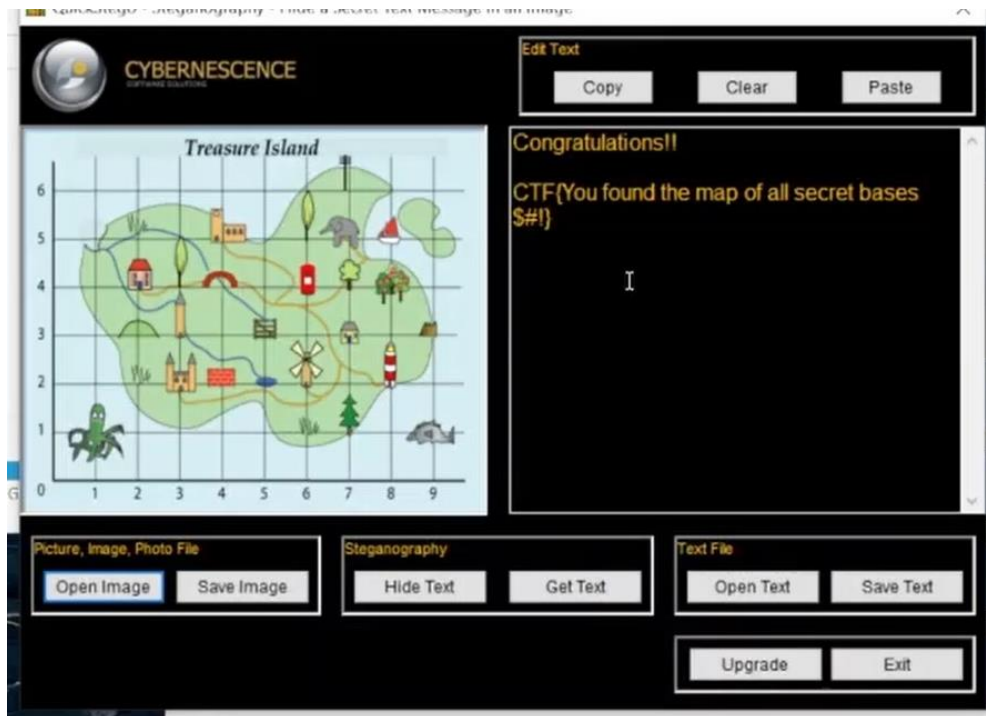


Figure 9

The flag will be CTF{ You found the map of all secret bases S#! }

Step 4

In order to start this step, download the pcap files in the error page on the website (trigger an error request in the page).

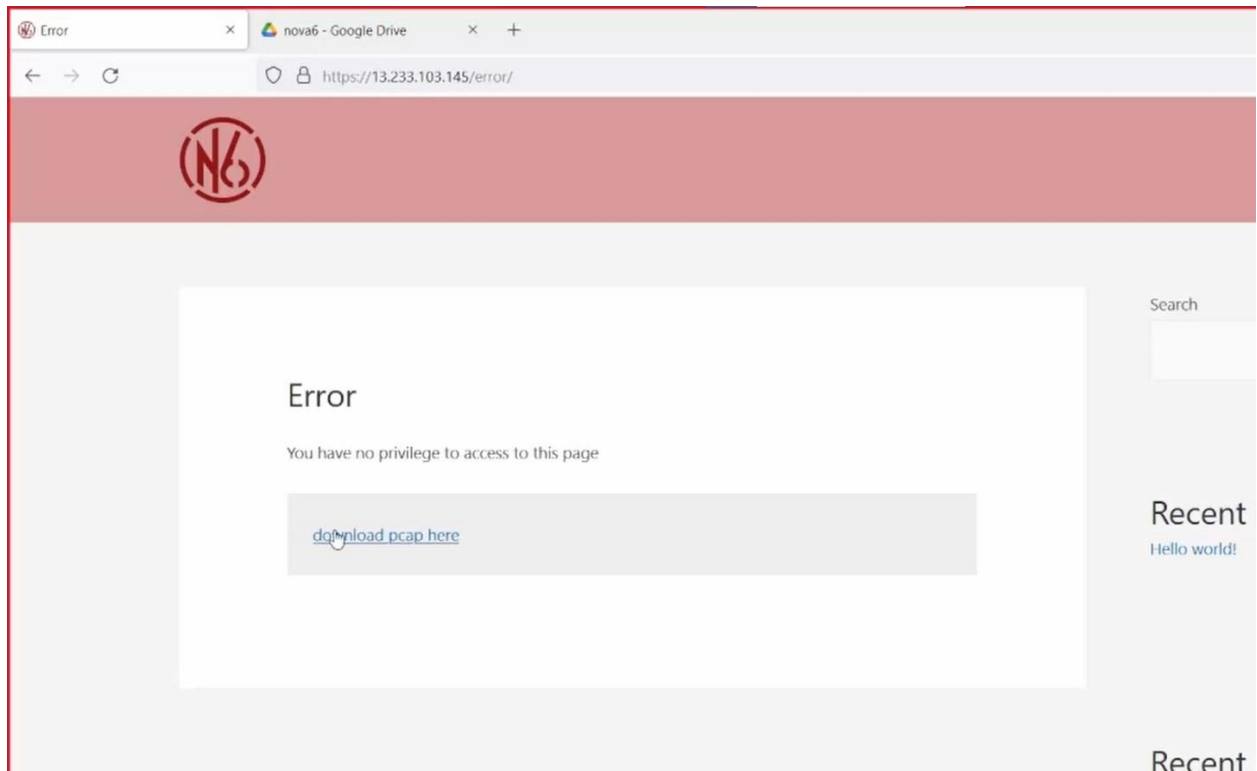


Figure 10

Then use Wireshark to analyse the pcap files. These pcap files contain information captured about communication via email. There are 9 Wireshark files. One file includes the details about the content and instructions about content to find. There is another file which has the flag details. Another file contains the URL which contains the username and password text files which will be useful in coming steps.

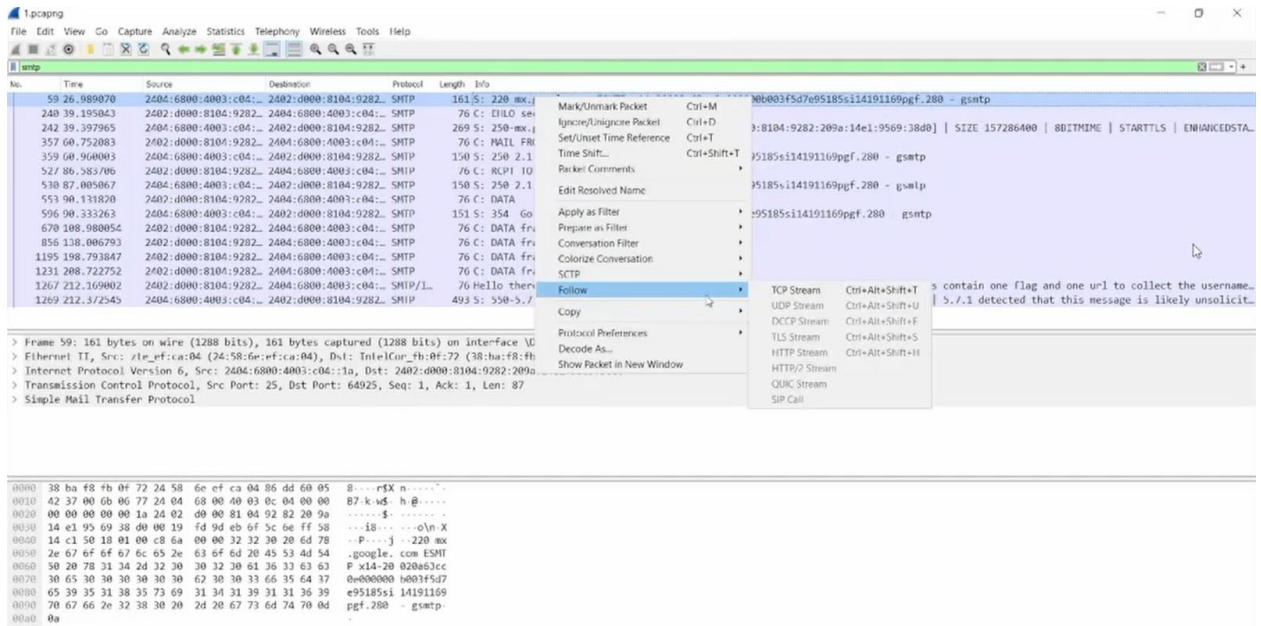


Figure 11

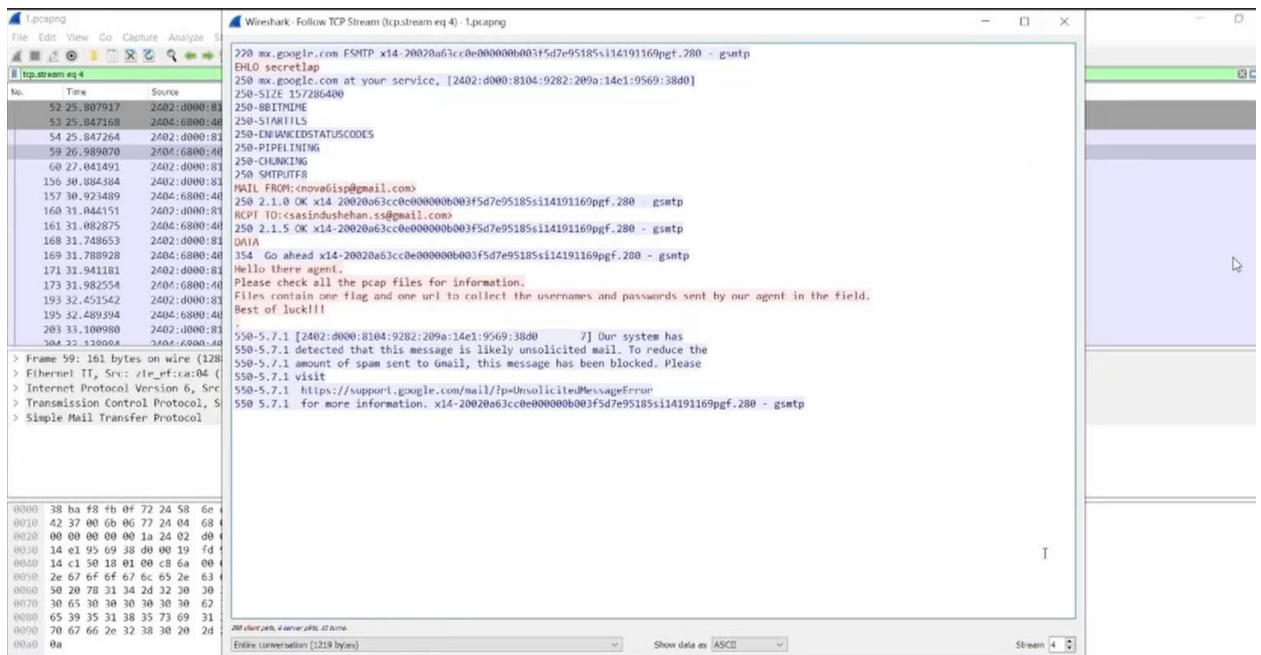


Figure 12

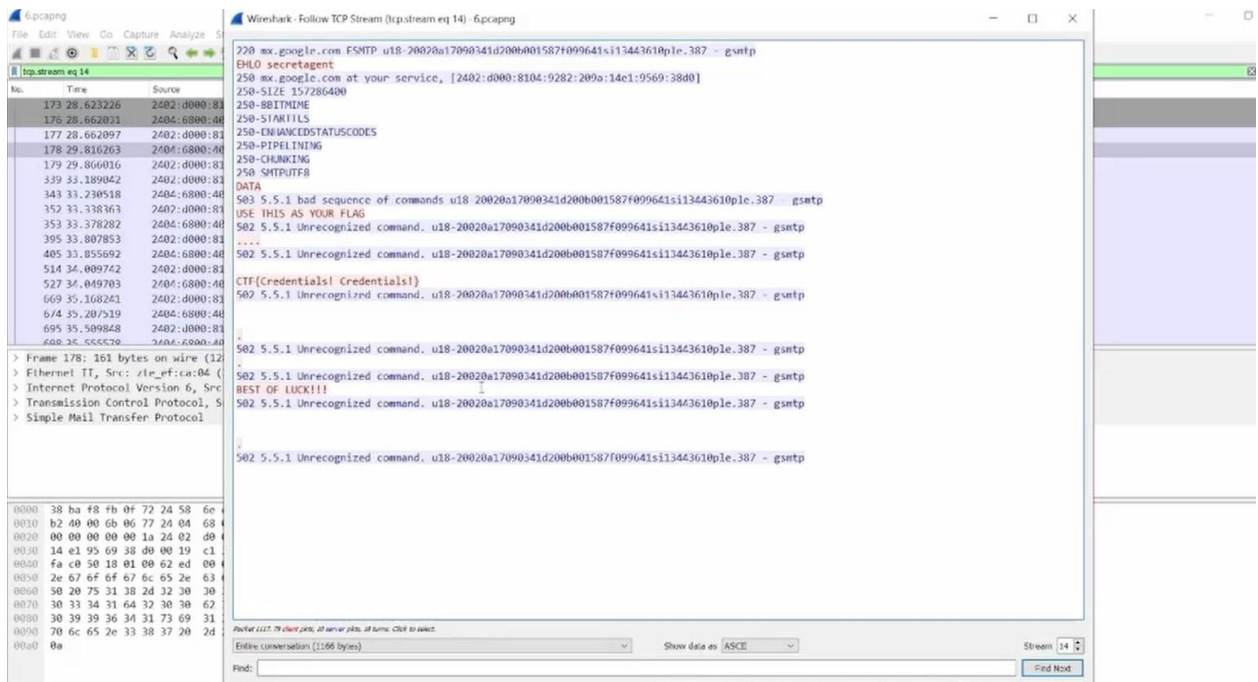


Figure 13

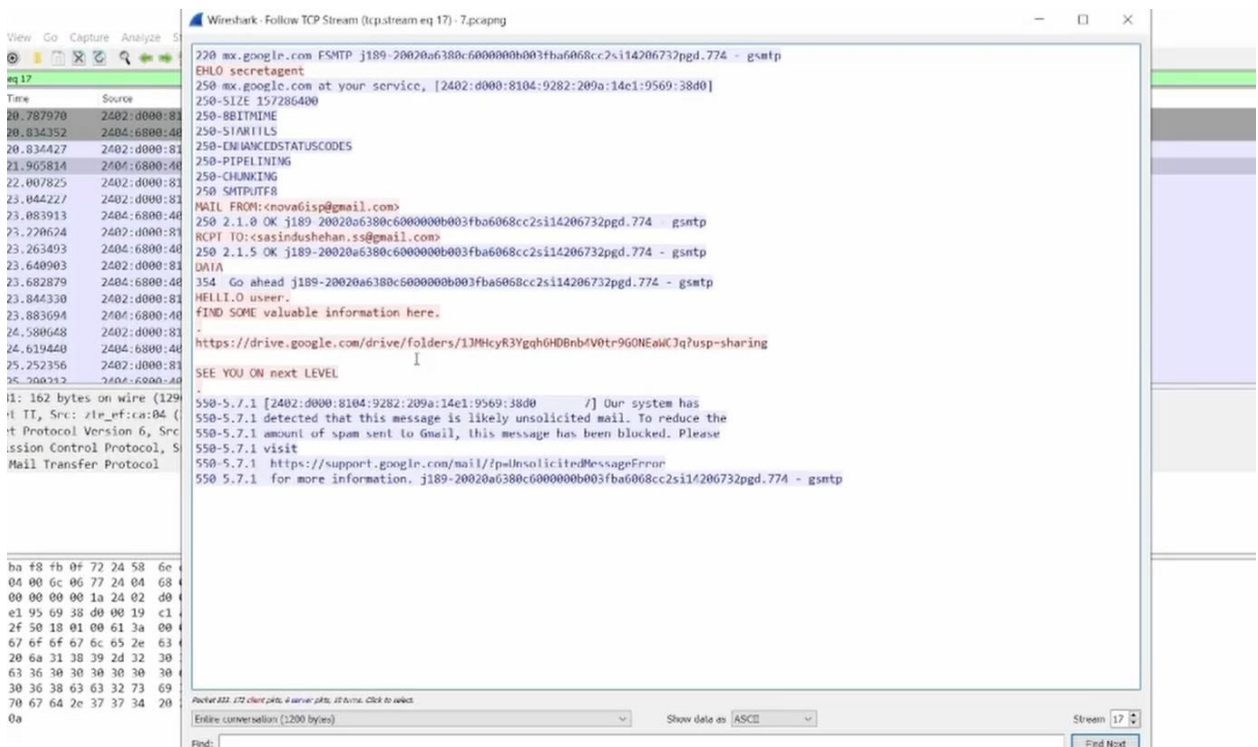


Figure 14

CTF{Credentials! Credentials!} will be the flag of the level. The link for the password and usernames text files also given here.

Step 5

Getting piece of information about main secret Base (First party of MD5 hash – users need to have all 3 parts to get the complete hash to crack md5 hash to access the main secret base)

Go to robots.txt file, then get the flag from there.

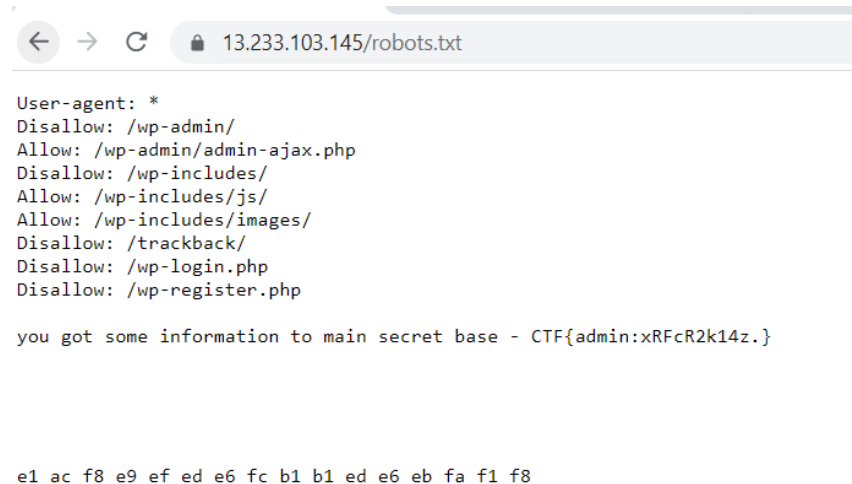


Figure 15 Robots.txt file

STEP 6

In order to complete this step, the text in the warhorses webpage (clickable link is given on the home page) should be translated from Greek to English. It contains information about the attack place but encrypted via AES algorithm.

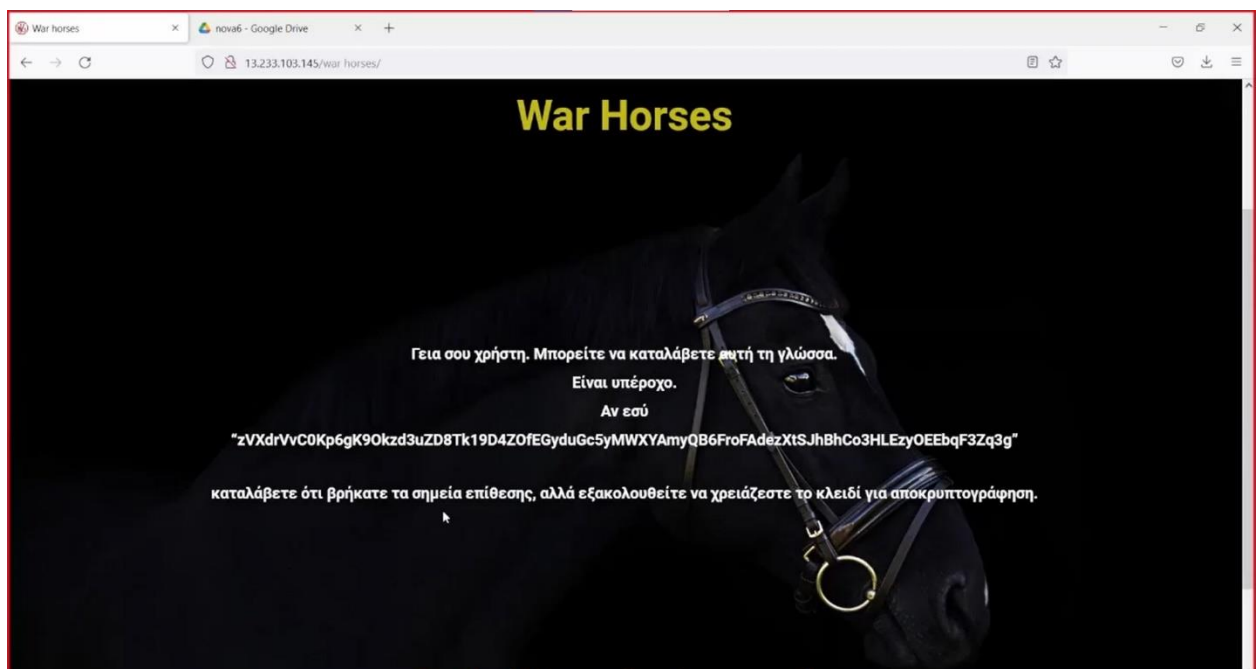


Figure 16

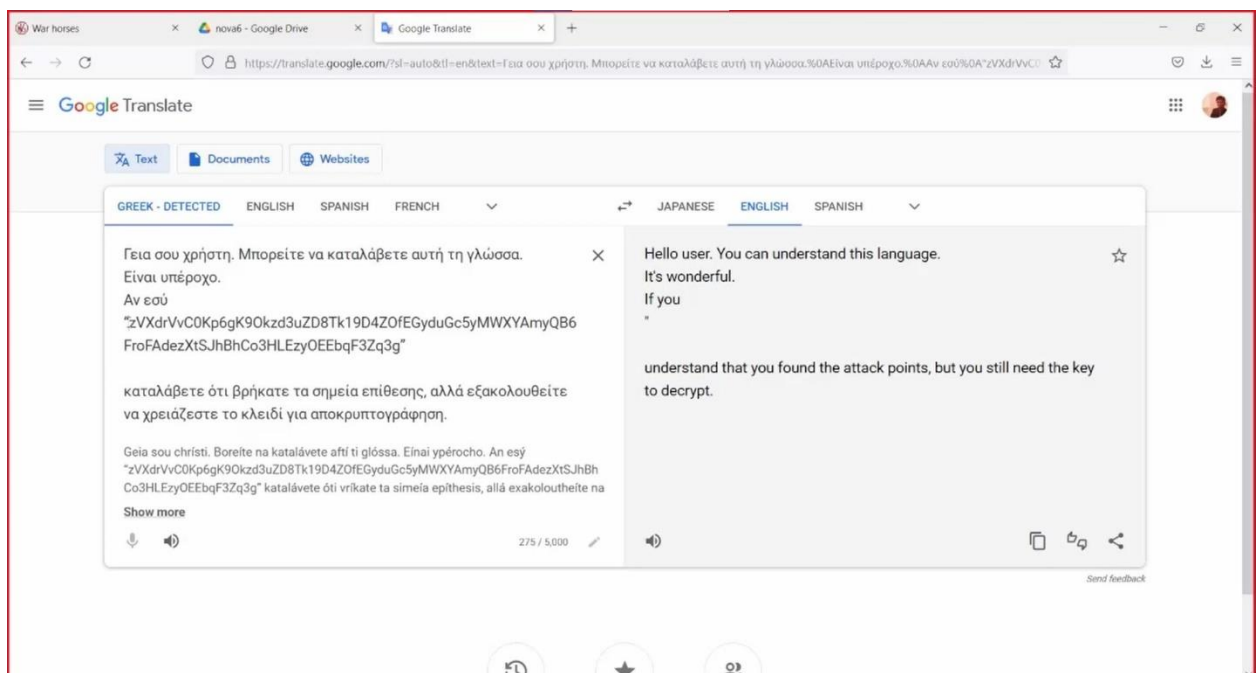


Figure 17

The encryption key can be found in the robots.txt webpage previously. This key is or the ASCII value of the key is turned into HEX format and shifted by 8.

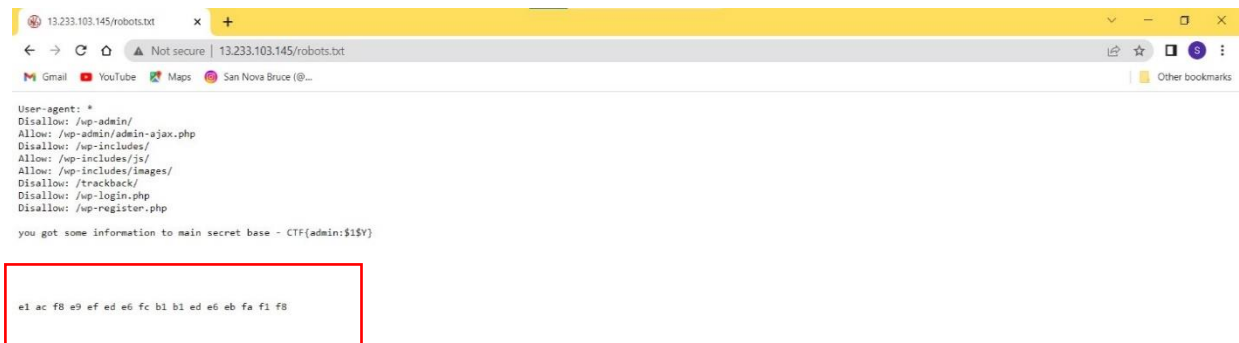
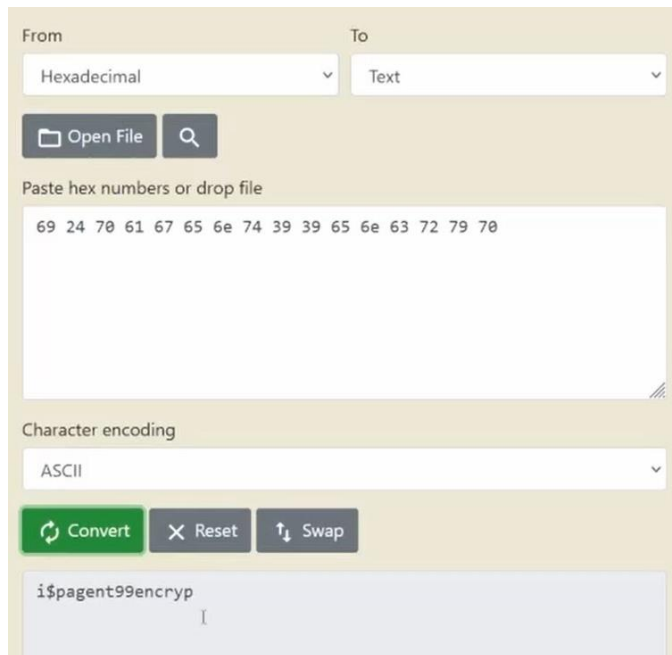


Figure 18

When +8 shift is removed key hex value will be:

69 24 70 61 67 65 6e 74 39 39 65 6e 63 72 79 70

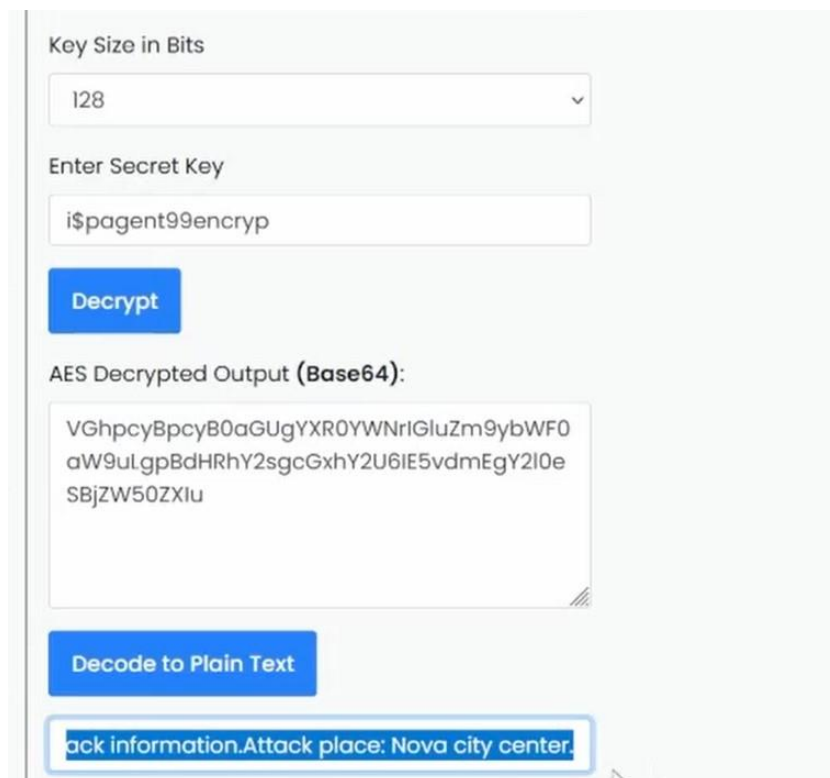
Then the hex value can be converted into ASCII value, the key will be:



A screenshot of a web-based hex-to-text conversion tool. The interface has a light beige background. At the top, there are two dropdown menus labeled 'From' and 'To'. 'From' is set to 'Hexadecimal' and 'To' is set to 'Text'. Below these are two buttons: 'Open File' with a folder icon and a search icon. A text area labeled 'Paste hex numbers or drop file' contains the hex string '69 24 70 61 67 65 6e 74 39 39 65 6e 63 72 79 70'. Below the text area is a dropdown menu for 'Character encoding' set to 'ASCII'. At the bottom of the input section are three buttons: 'Convert' (green), 'Reset' (grey with an 'X'), and 'Swap' (grey with up/down arrows). The output area at the bottom shows the converted text 'i\$pagent99encryp'.

Figure 19

Use the key to decrypt the cipher text



A screenshot of a web-based AES decryption tool. The interface is light grey. It has a dropdown menu for 'Key Size in Bits' set to '128'. Below it is a text input field labeled 'Enter Secret Key' containing the key 'i\$pagent99encryp'. A blue 'Decrypt' button is below the key field. The output section is labeled 'AES Decrypted Output (Base64):' and contains a text area with the Base64 string 'VGhpcyBpcyB0aGUgYXR0YWNrIGluZm9ybWFOaW9uLgpBdHRhY2sgcGxhY2U6IE5vdmEgY2l0eSBjZW50ZXlu'. Below the output area is a blue button labeled 'Decode to Plain Text'. At the bottom, a text area shows the decoded plain text: 'ack information.Attack place: Nova city center.'.

Figure 20

The flag for this level will be the attack place, CTF{Nova city center}

Step 7

Get the data fragment of virus information (to decrypt the text that contains the virus cure users need to find all 2 fragments and combine them together and use it as the decryption key)

First users need to download the mem file in war horses page. The names of the files to be found are given (K1.txt (key), Virus nova.txt(text)). One file contains the encrypted text and the other file contains the key.

After getting 2 files users need to decrypt the key and reveal the CTF flag.

K1.txt – key, encryption method, key size

Virus noca.txt – encrypted text

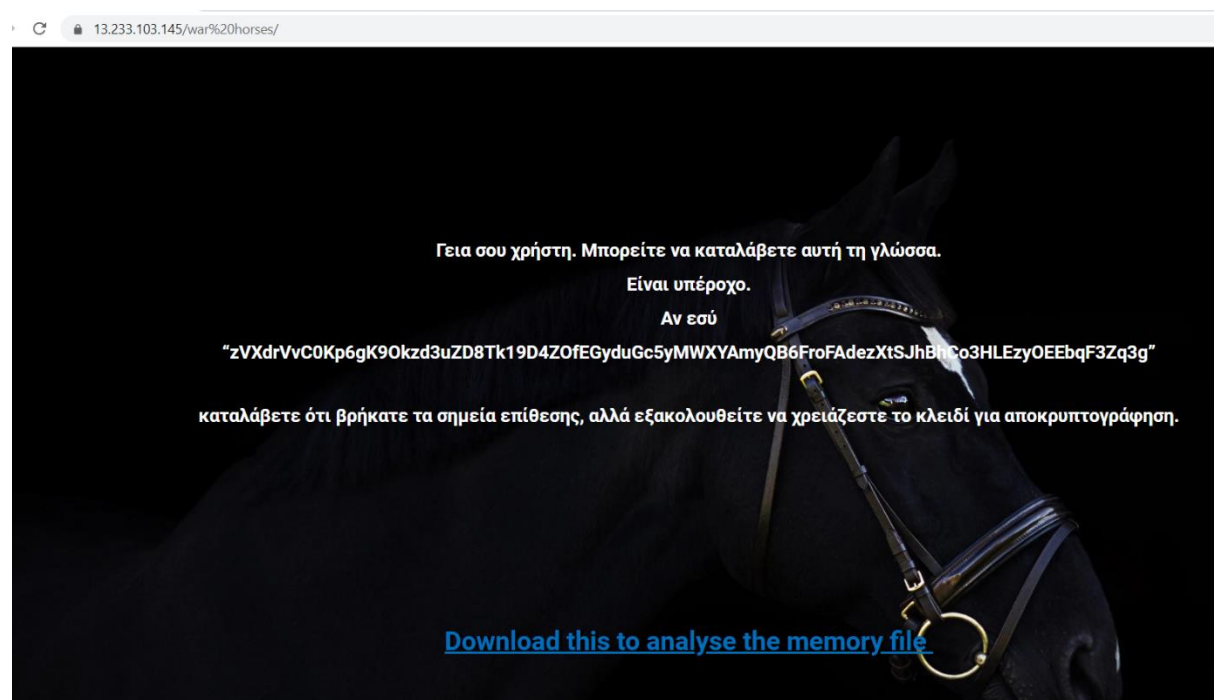


Figure 21mem file download location

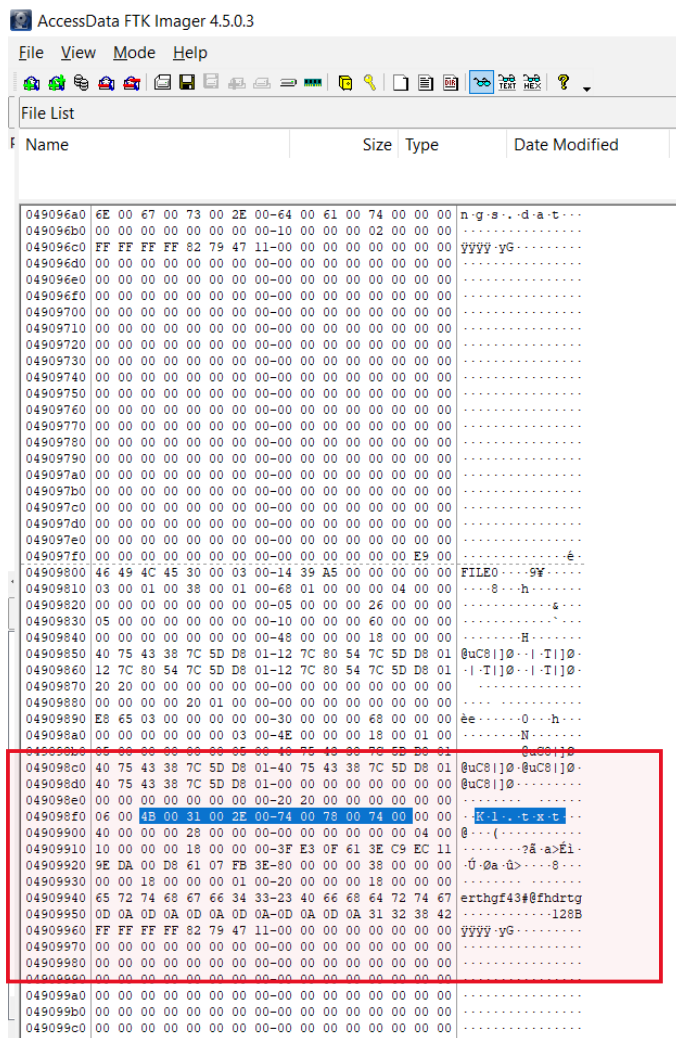


Figure 22K1.txt file analyzed with FTK Imager

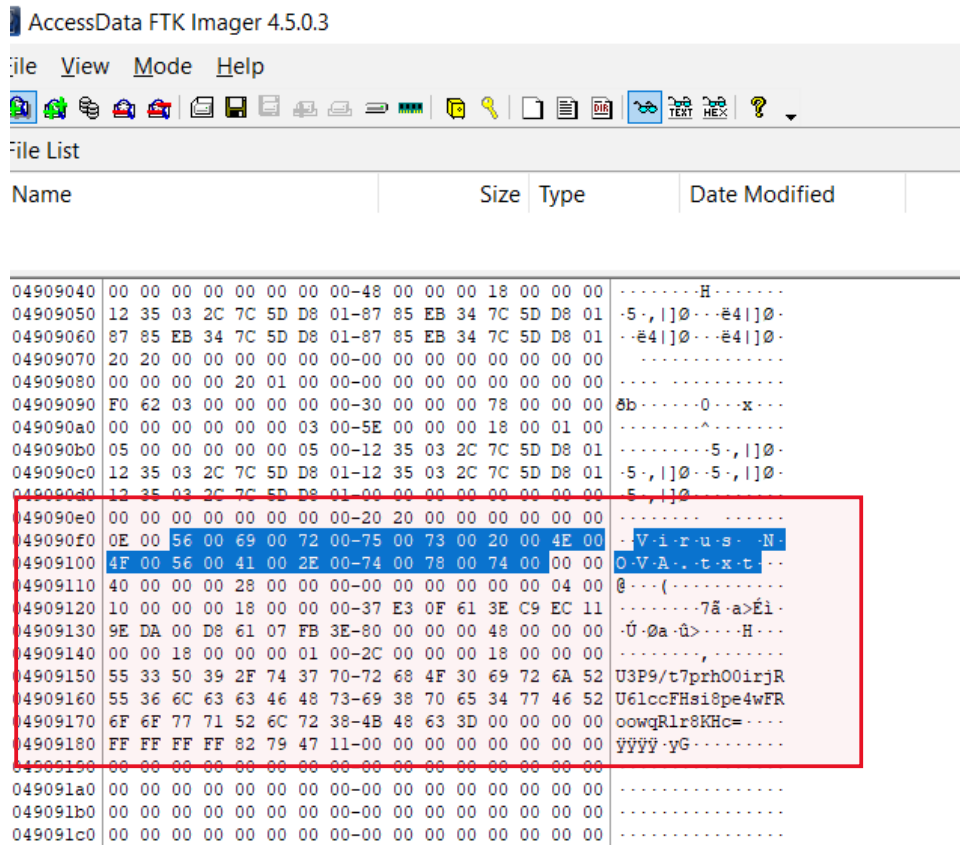


Figure 23 Virus nova.txt file analyzed with FTK Imager

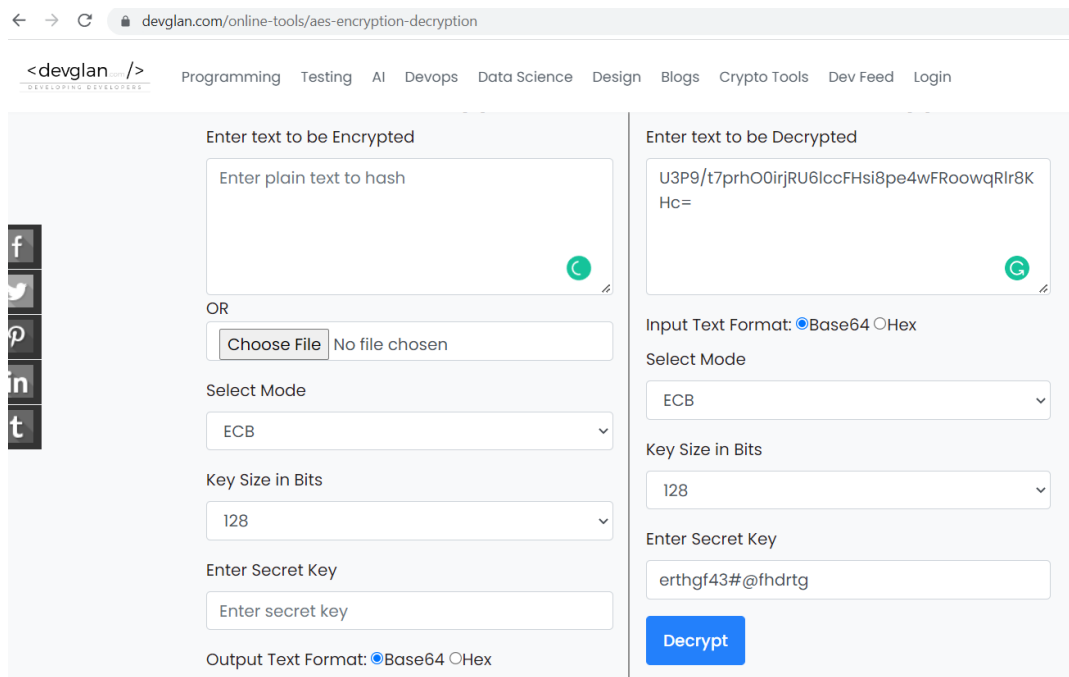


Figure 24 decrypted using devglan.com online decryptor

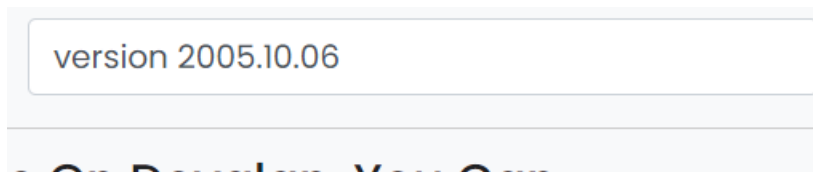


Figure 25

CTF flag – CTF{version 2005.10.06}

Step 8

Access into the second secret base (access into the website as an operator (privilege escalation and bruteforce))

User need to use username.txt and passwords.txt file that found on step 4 in order to bruteforce the login page.

Users need to use Wp-scan for bruteforce attack.

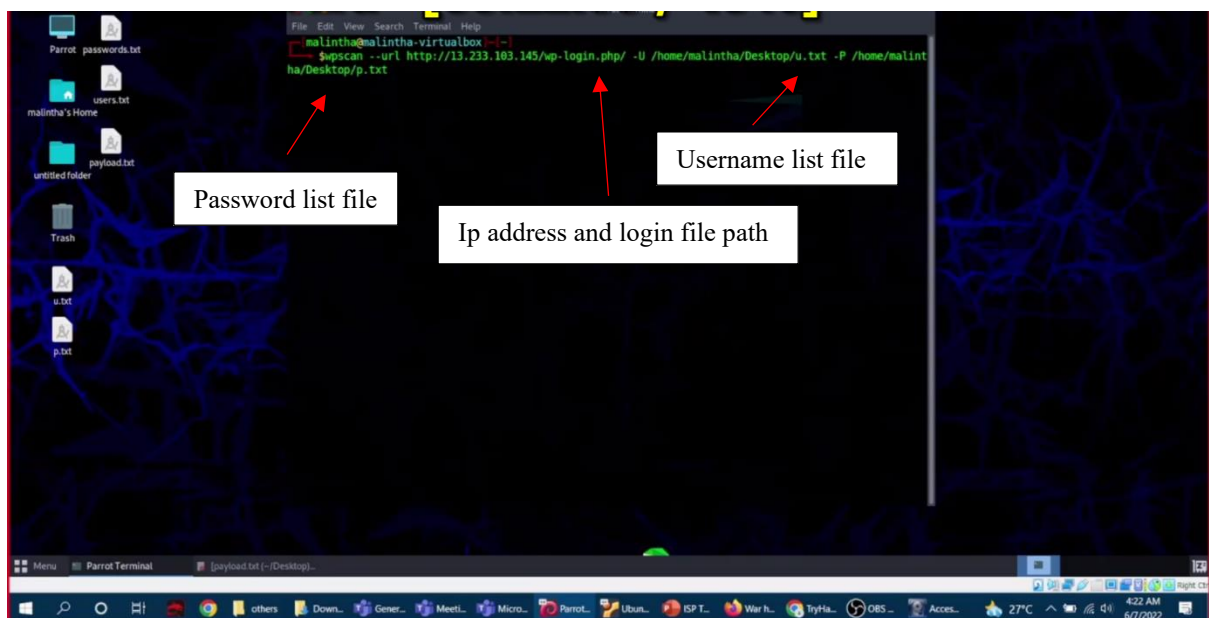


Figure 26

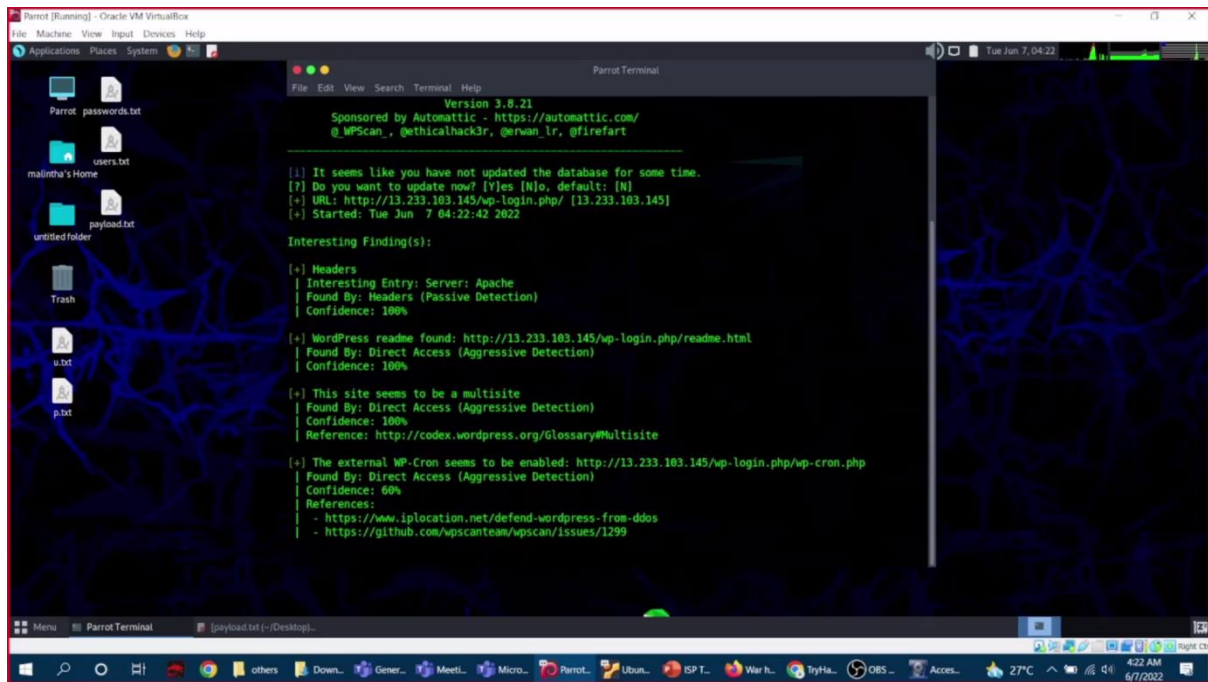


Figure 27

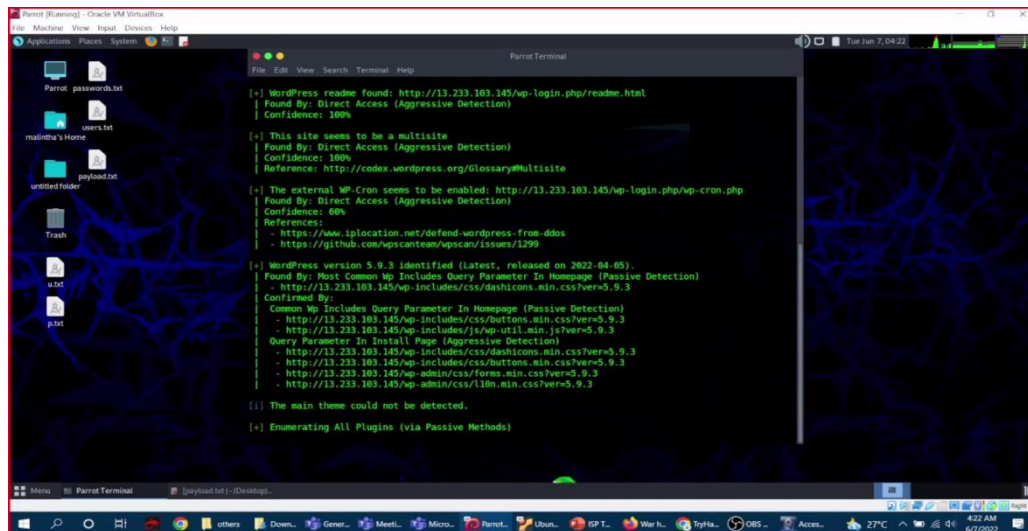


Figure 28

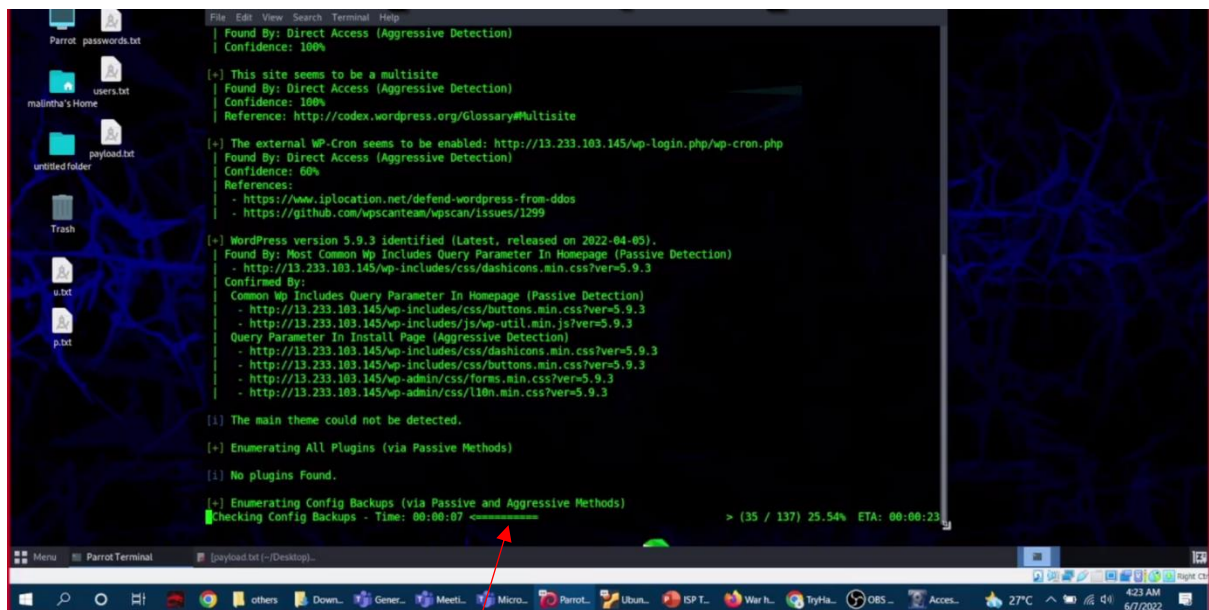
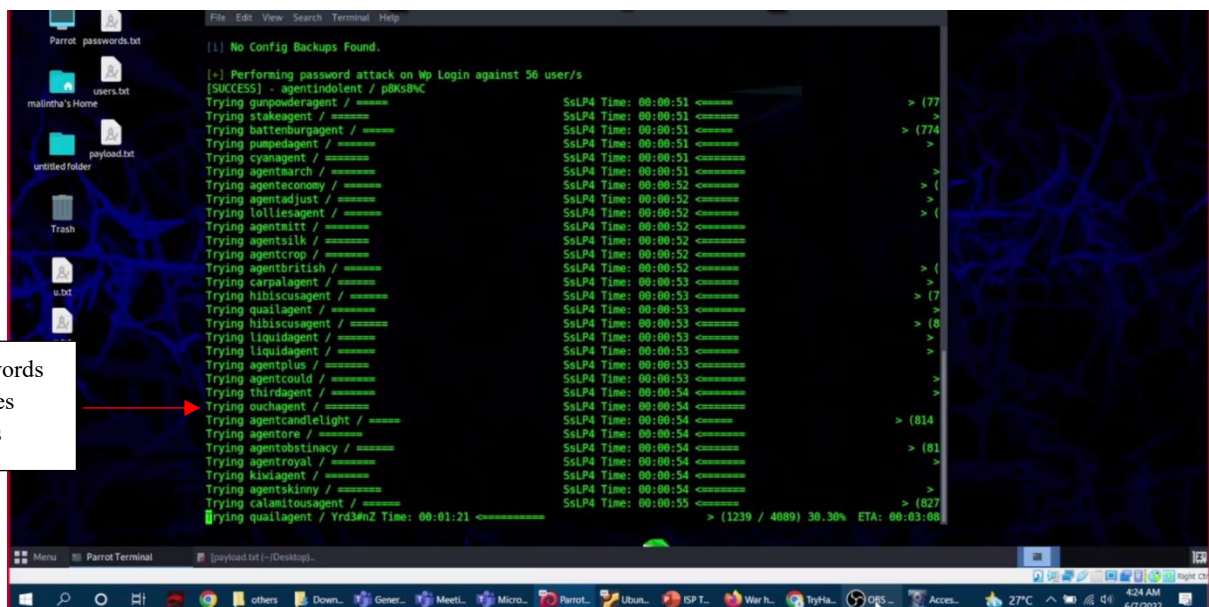


Figure 29

Progress



Trying passwords
and usernames
combinations

Figure 30

Final results found one username and password combination.

Username – agentindolent

Password – p8Ks8%C

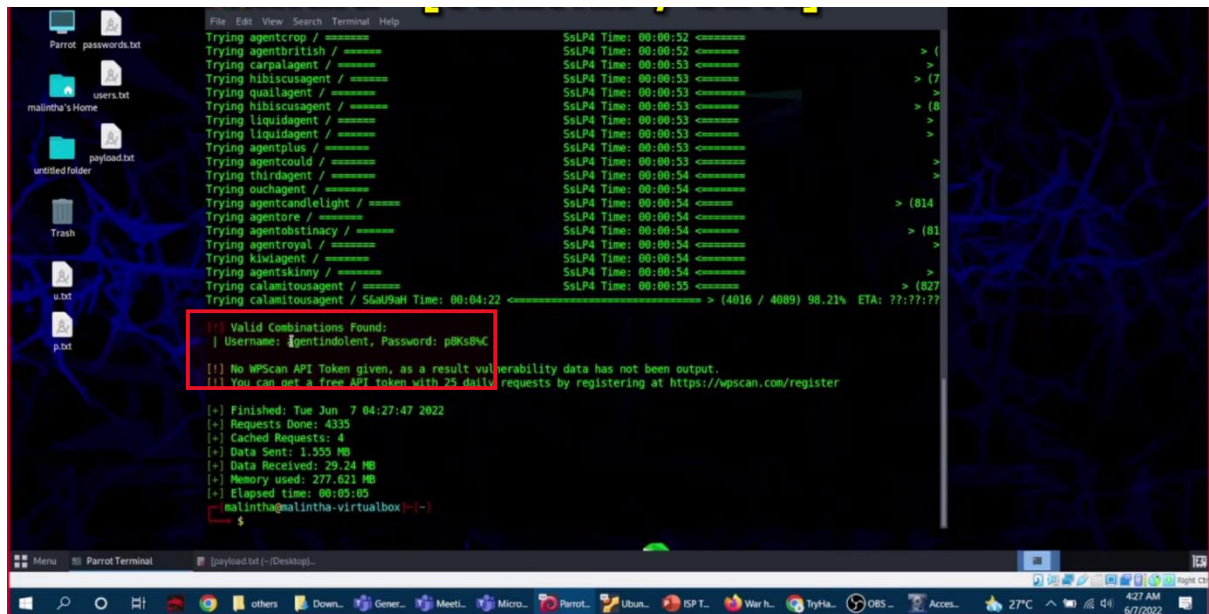


Figure 31

Flag - CTF{!Welcome to the Guernica} (flag appears as an alert after login as the operator.)

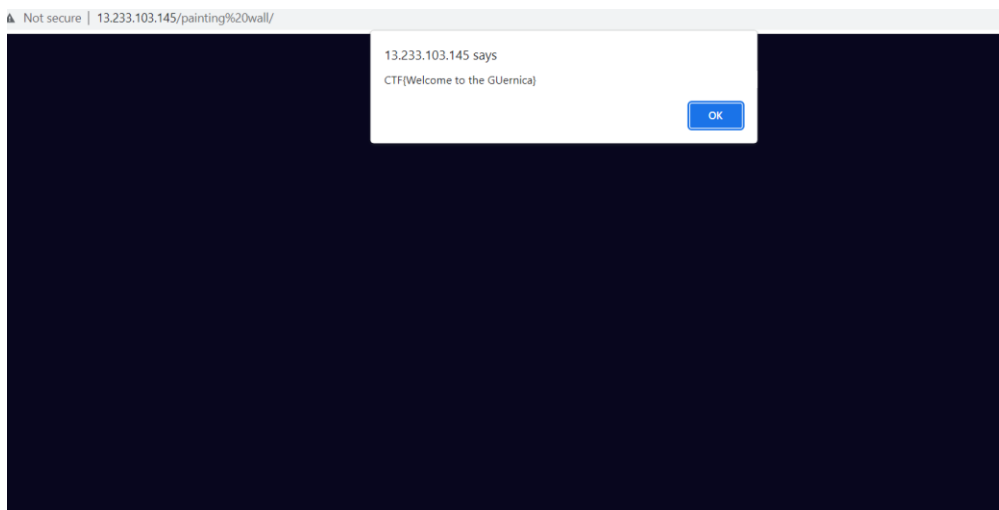


Figure 32

Step 9

Get second bases' attack place information.

In the painting wall page, there is a description about paintings. If user copy and paste the description, he will get the flag instead of description.

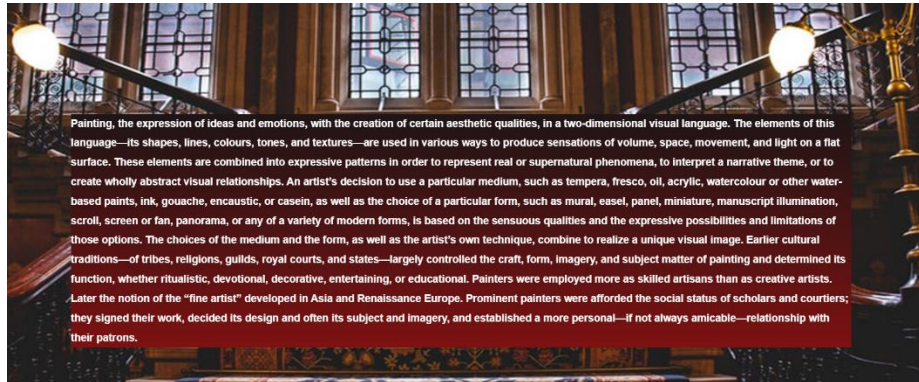


Figure 33

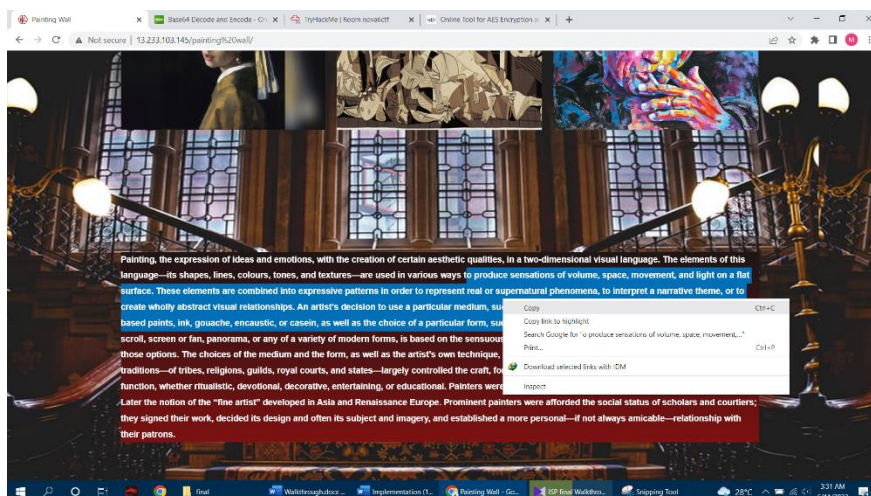


Figure 35

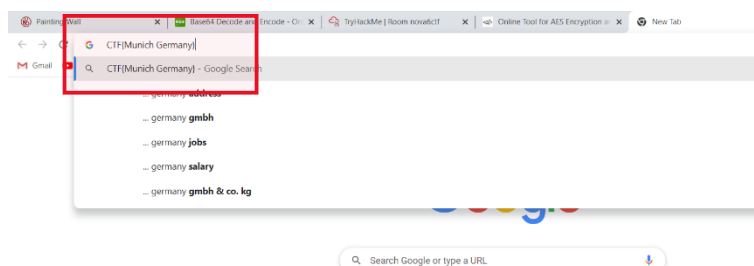


Figure 34

Step 10

Find the next secret base information (Information that helps to access to next secret base)

In the Painting wall page there is a painting called “Guernica”, user need to find that exact image by given hints and reveal the information that hidden form that painting by entering the password as guernica. Used S tool to encrypt the image.

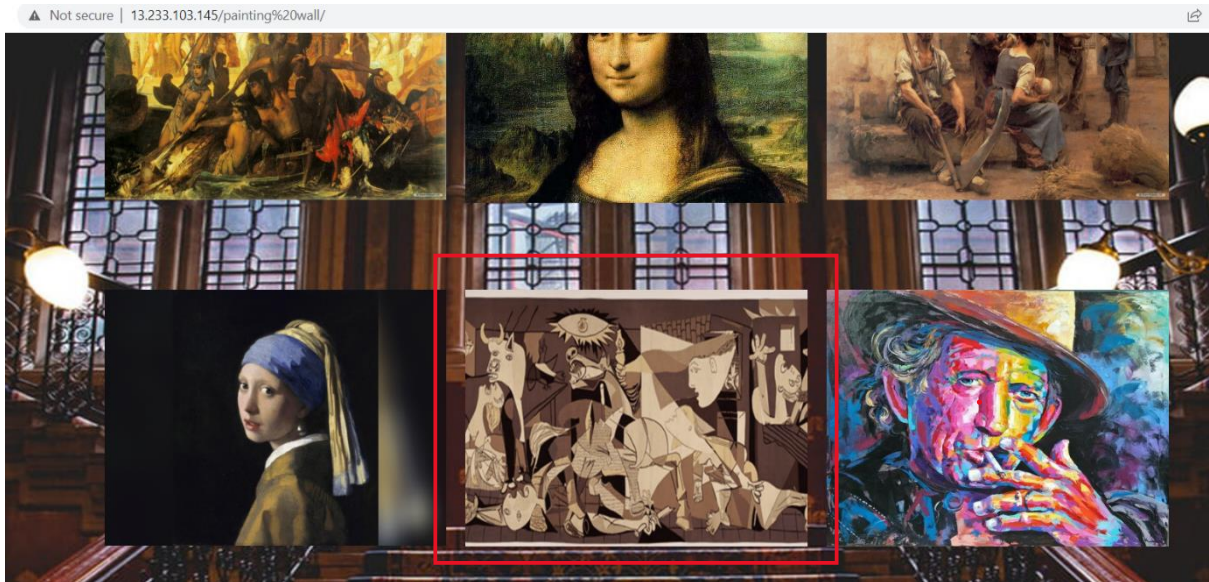


Figure 37 painting "Guernica" by Picasso

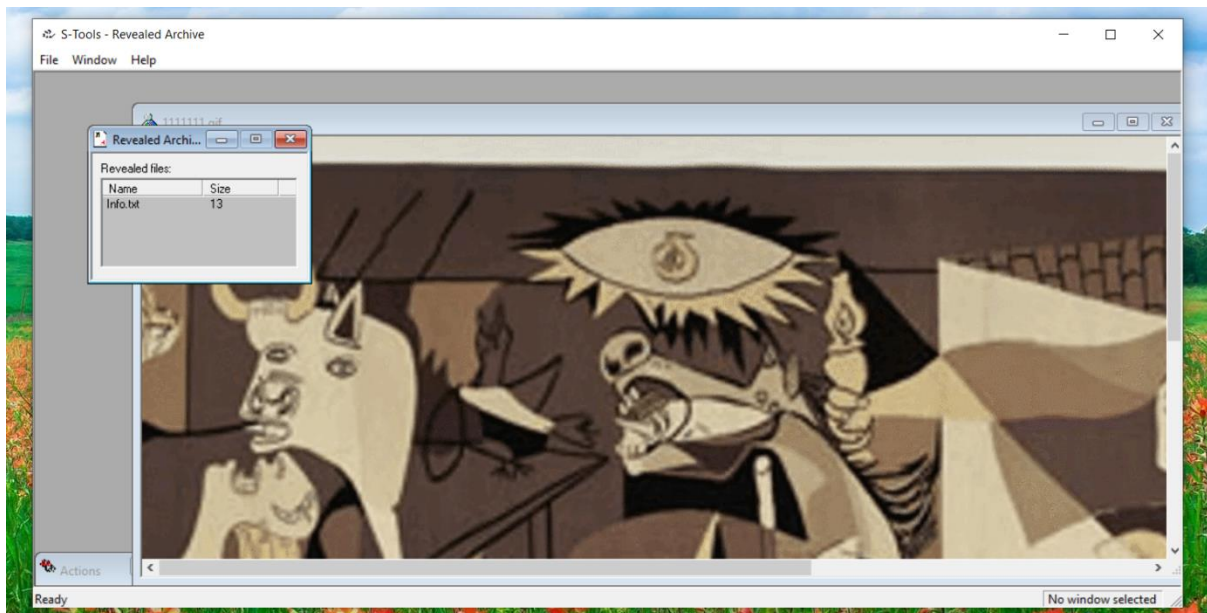


Figure 36 revealed file

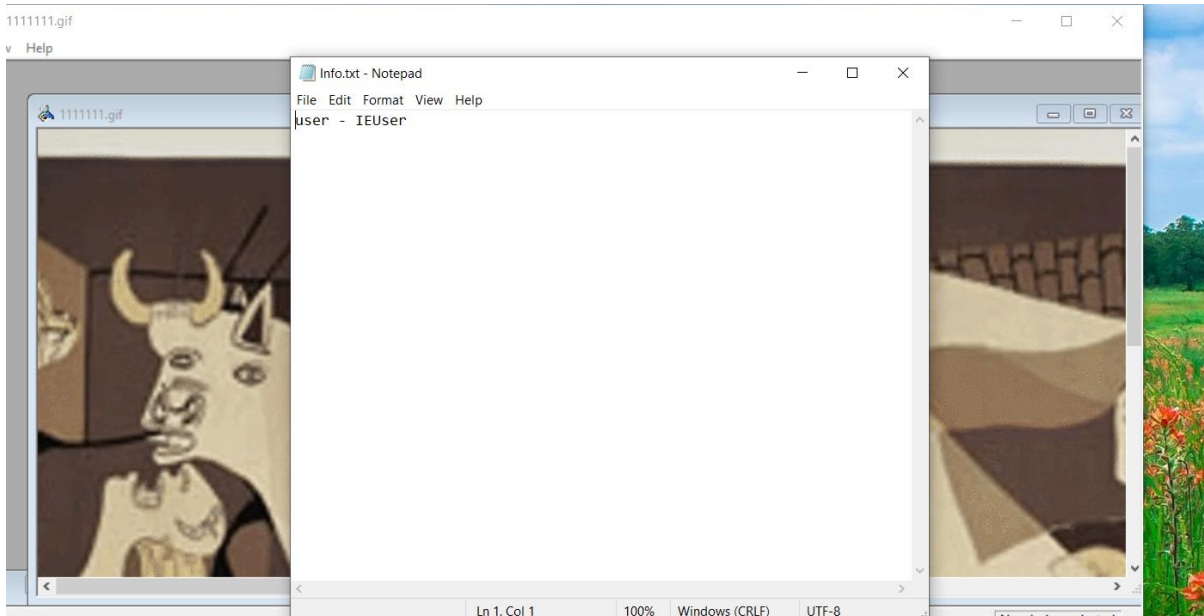


Figure 38 file content and the flag

The flag is – CTF{IEUser}

Step 11

Getting virus version fragment 2

First user need to search step11.txt in the URL

<https://13.233.103.145/step11.txt>

the file contains the program code in assembly. User need to understand the code and find the flag.

```

.LC0:
.string "Find the number till which you get the odd number pwd"
.LC1:
.string "%d"
.LC2:
.string "\n\n ecbdes - 3DiP1pqv9xfzM/tgfTDtog=="
main:
    push    rbp
    mov     rbp, rsp
    sub     rsp, 16
    mov     DWORD PTR [rbp-4], 1
    mov     edi, OFFSET FLAT:.LC0
    call    puts
    jmp     .L2
.L3:
    mov     eax, DWORD PTR [rbp-4]
    mov     esi, eax
    mov     edi, OFFSET FLAT:.LC1
    mov     eax, 0
    call    printf
    add     DWORD PTR [rbp-4], 2
.L2:
    cmp     DWORD PTR [rbp-4], 9
    jle     .L3
    mov     edi, OFFSET FLAT:.LC2
    mov     eax, 0
    call    printf
    nop
    leave

```

Password may be a sequence of odd numbers

Cipher text in des with ecb


Odd number until 9 (number < 10)

Figure 39

Used the-x.cn to decrypt cipher using DES. The CTF flag is – CTF{Nova6.02.01}



← → ↻ the-x.cn/en-US/cryptography/Des.aspx

The 

KeyConverter ▾ Cryptography ▾ Hash ▾ Formatter ▾ Coding ▾ Regular Informa

DES encryption / decryption

Online DES encryption decryption tool. Due to the des algorithm features, the Key length is fixed at 8Byte (64bit) and the excess is ignored. If less than 8Bytes will be filled v to process data (e.g. KEY/IV) if not specified. This tool is not fully tested, please give feedback if a problem is found.

DES TripleDes AES RSA SM2 SM4 SM3

3DIP1pqv9xfzM/tgTDTog==

UTF-8 ▾

ECB ▾

None ▾

13579

CTF{Nova6.02.01}

Figure 40

Step 12

Get piece of information about the main secret base.

In the painting wall page user can finde a secret code that used in word war 2 names “ATTIC” when he clicks the word it redirects to a twitter post that was delete by the post owner. User need to reveal the information by using wayback machine.

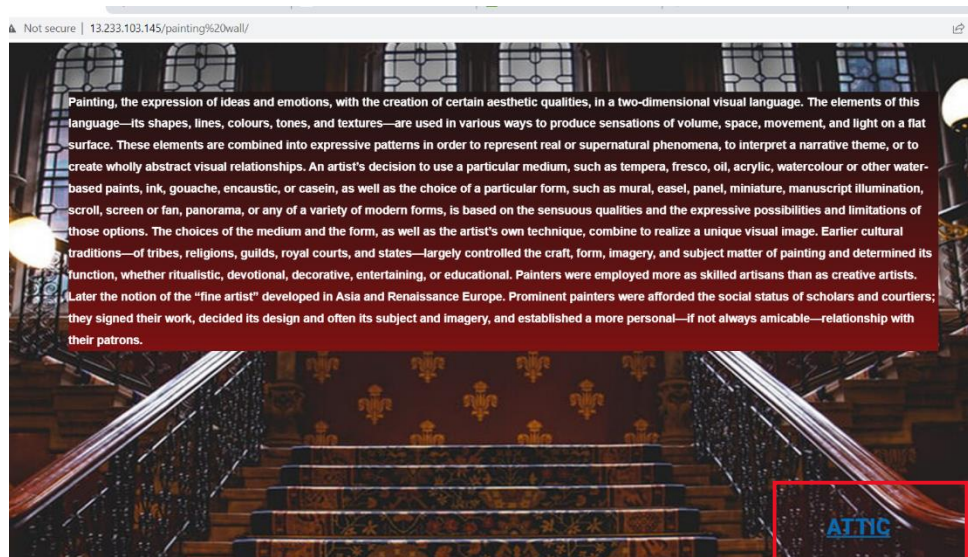


Figure 41

The post is deleted

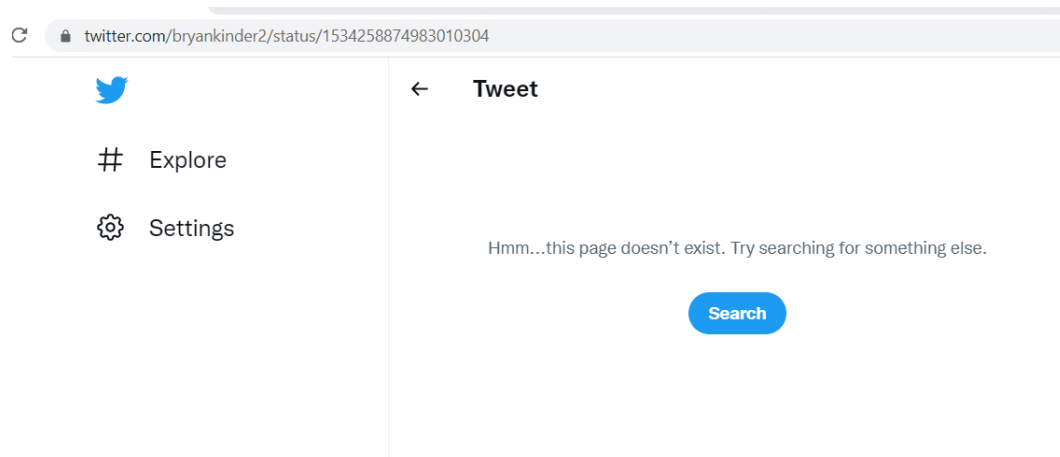


Figure 42

Go to wayback machine and paste the link in the search bar, click the on of below mentioned two dates.

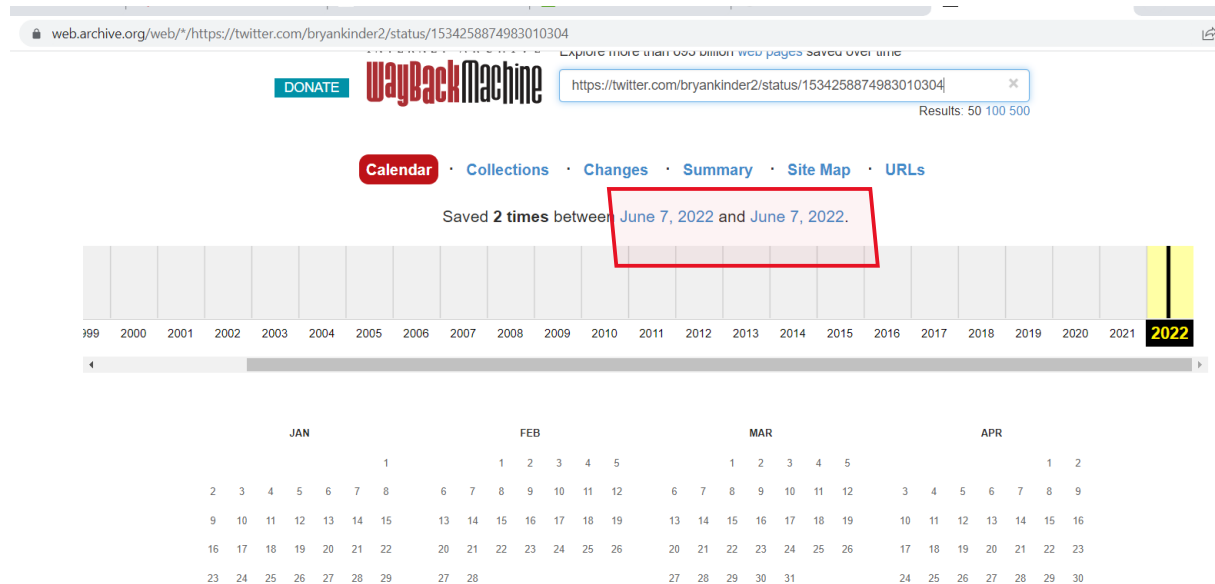


Figure 43

The wayback machins shows the deletes post and the flag is in the post.

Flag - CTF{J\$qREjtLxwBn5}

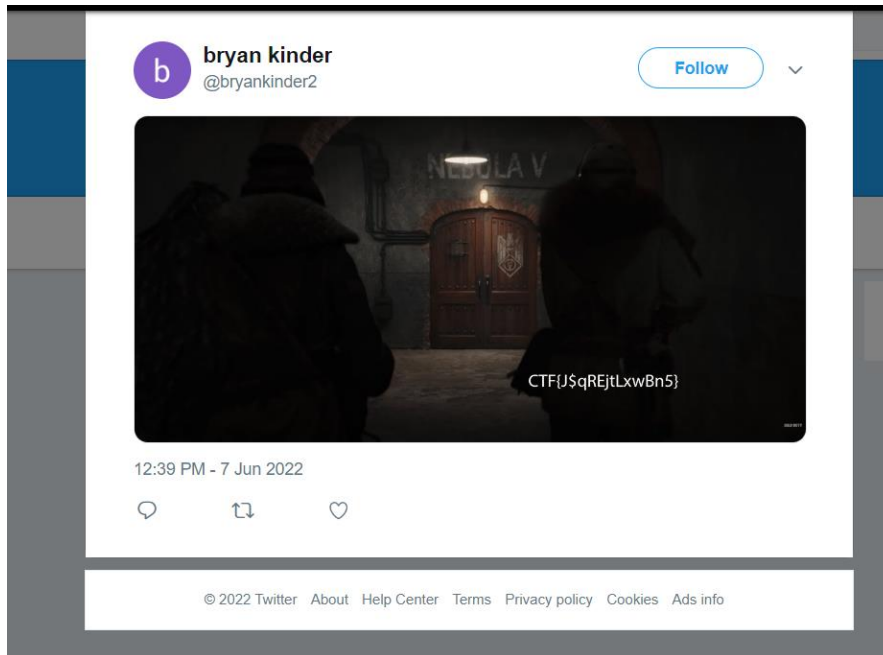
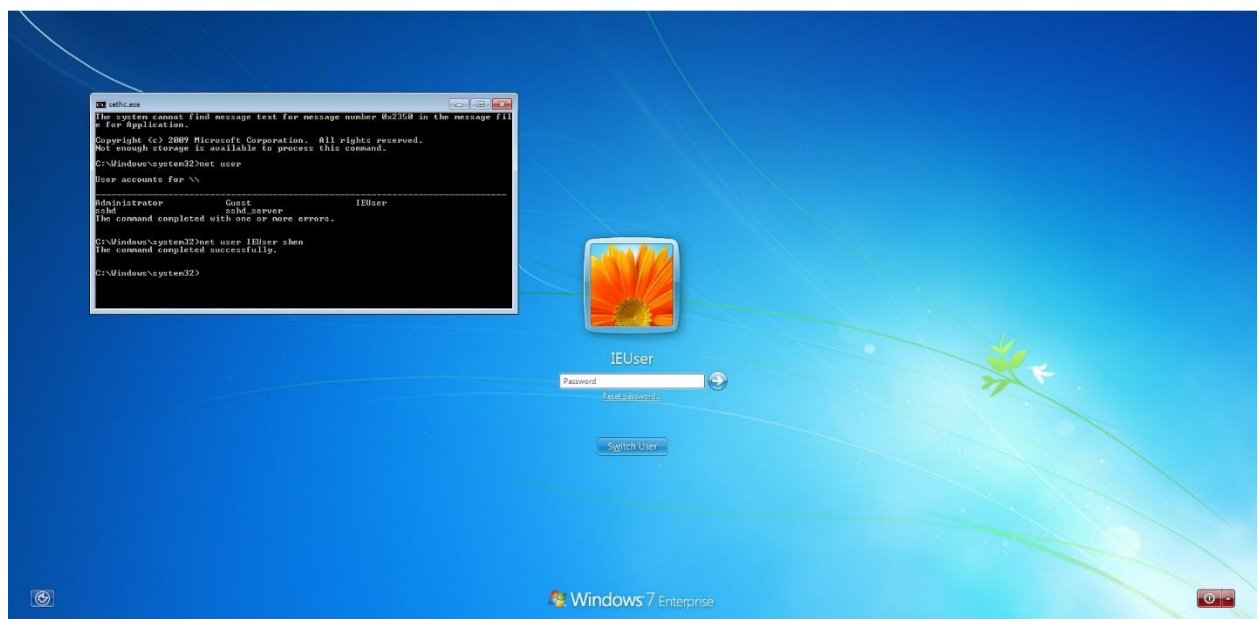


Figure 44

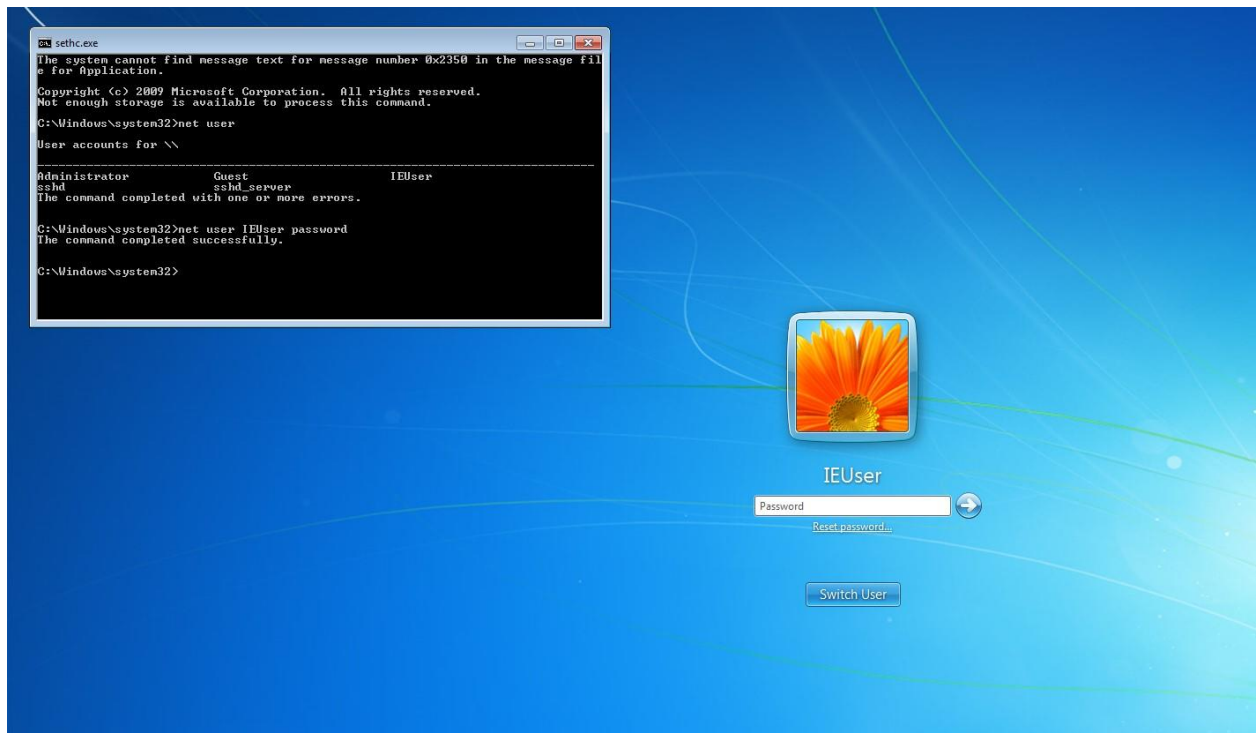
STEP 13 (Windows 7 VM)

To start the step, import the ova to any VM ware (VirtualBox is preferred). The backdoor here is implanted replacing the sticky key function with command prompt. Press the shift key until the command prompt appears (5 times).



Then in the command prompt type

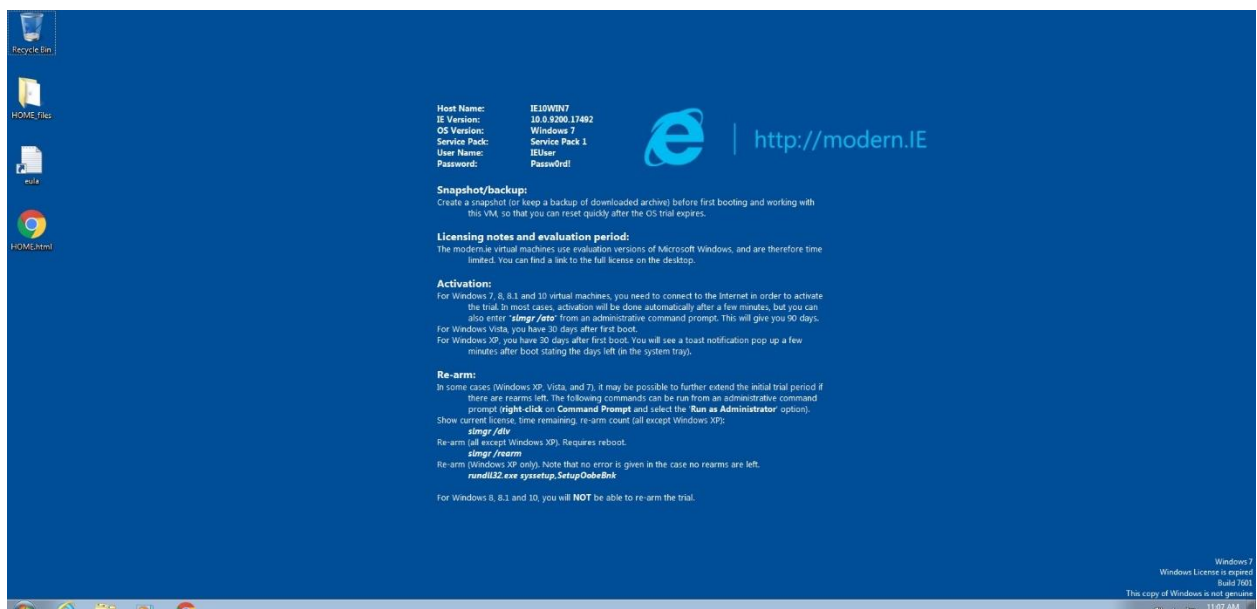
“net user IEUser NewPassword”



User names can be extracted by typing “net user”

“NewPassword” can be any word for the password

After login to windows use Host Name mentioned on the background image as the CTF flag
→ CTF{IE10WIN7}



Use the HOME html file to continue to the next stage

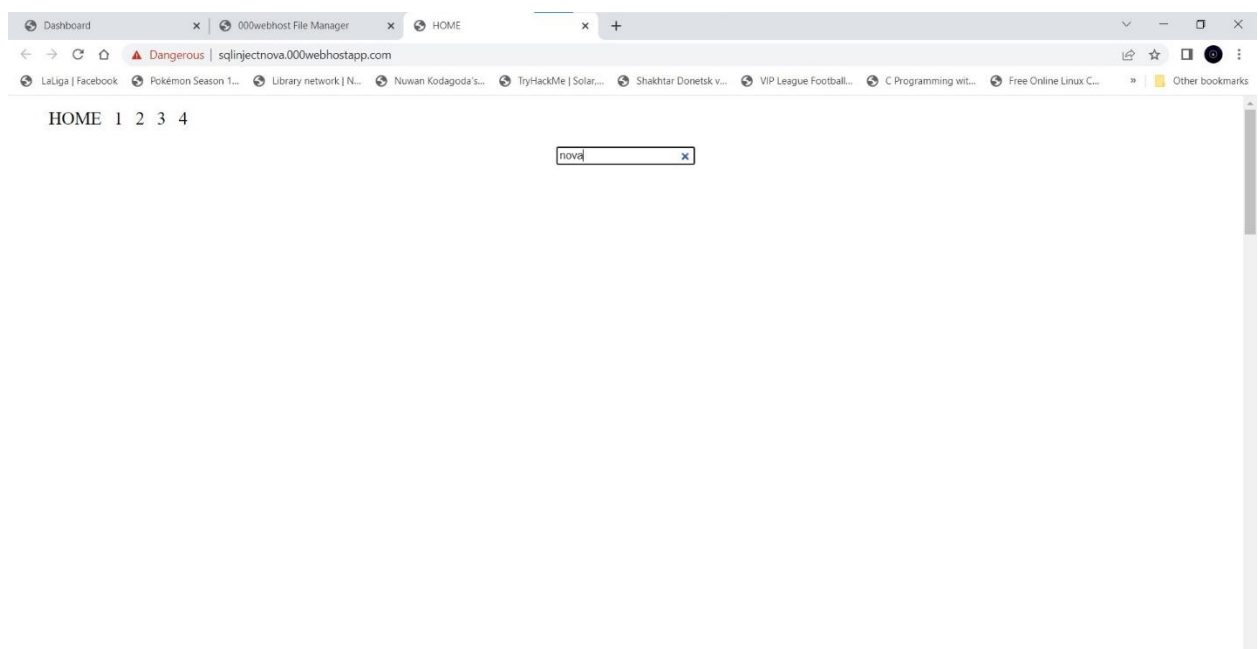


Figure 45

Step 14

In the home web page, you must find the attack place. This secret is hidden in secret.html page which has no link with the pages. A hint can be acquired when navigating into search page (using search).

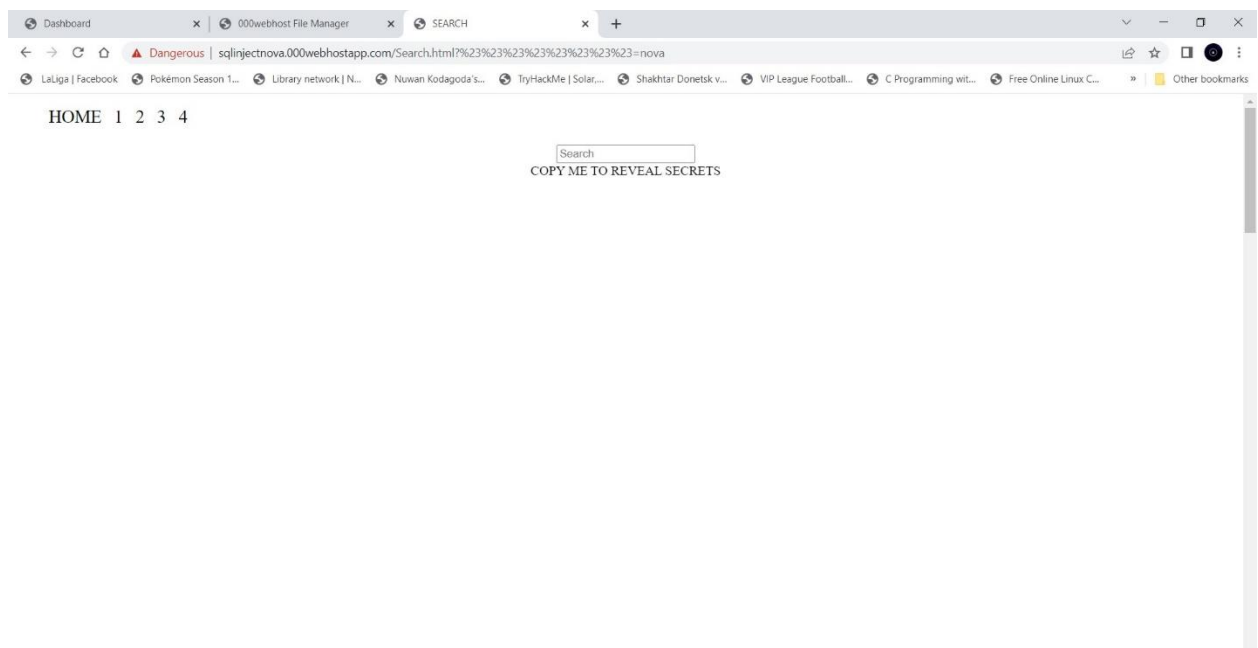


Figure 46

Copy the text and paste it into notepad file



Figure 47

Hint to the web page name is here.

Next type it in the address bar and navigate

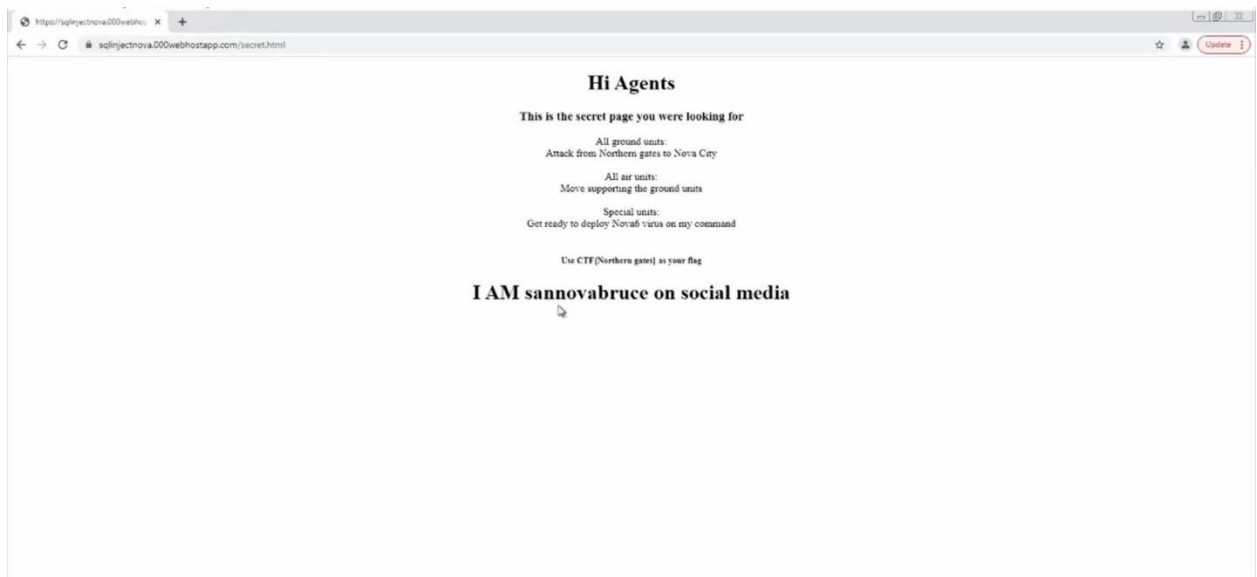


Figure 48

Use CTF{Northern gates} as the flag

Here the username of a social media account is given which will be useful in the next step.

STEP 15

In this step first it is required to find the social media account of the given username. Use of sherlock tool is recommended in this step (tool which check social media for a given username).

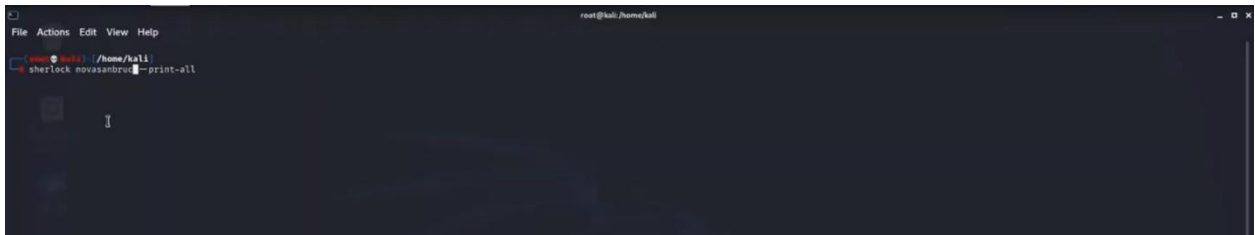


Figure 49

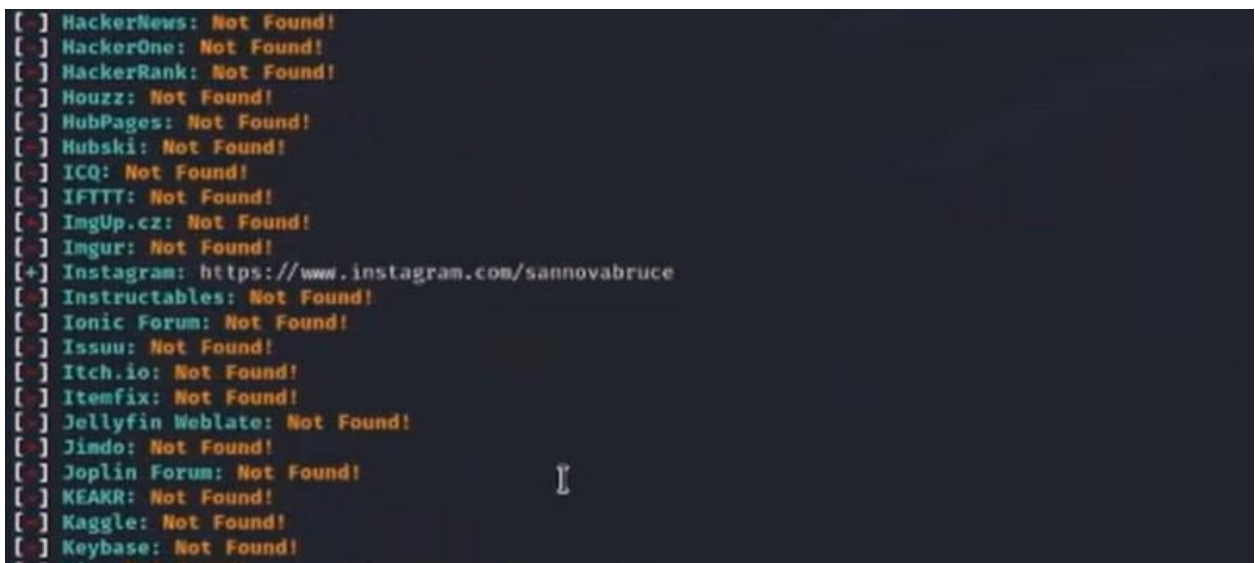


Figure 50

A match will be shown on Instagram. Next user should search the profile on Instagram for information on the account.

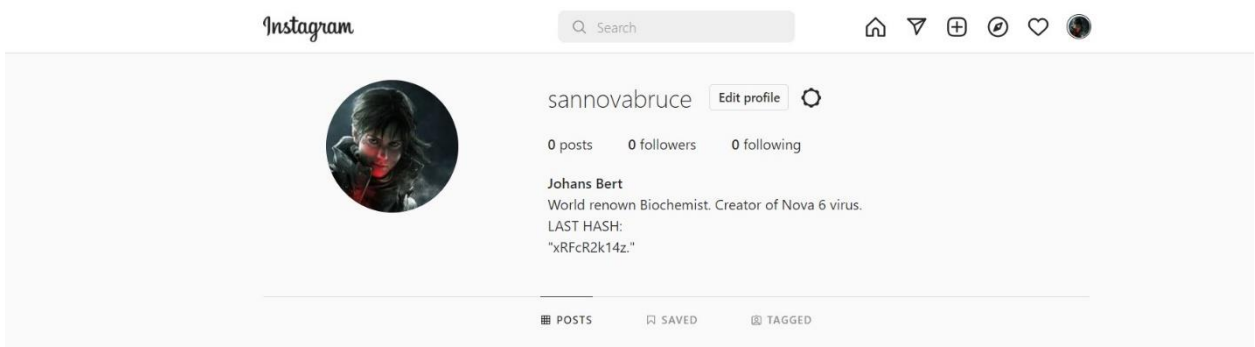


Figure 51

The flag for this step will be CTF{Johans Bert, Biochemist}

Information for the next step is present in the page too.

Step 16 (Ubuntu VM)

Access the admin account by cracking the MD5 hash by bruteforcing.

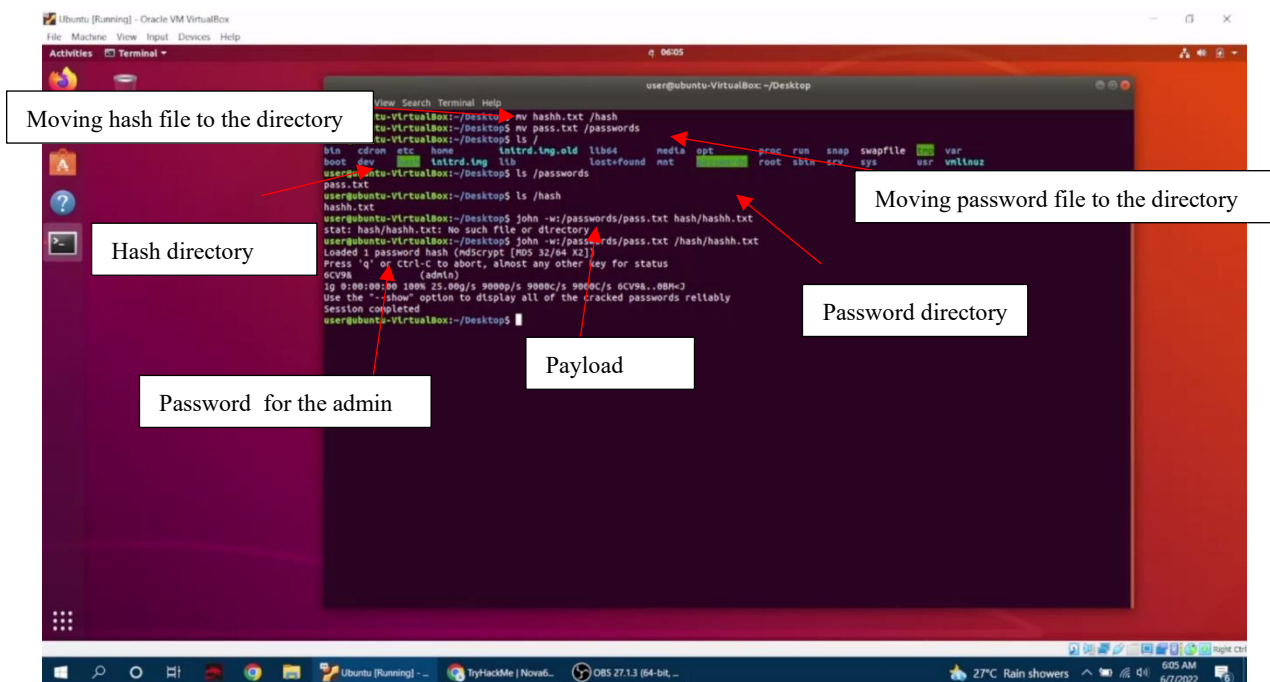
Assemble the fragments of the MD5 hash that found on previous steps (4,14,15).

The final hash will be – “admin:\$1\$JguaM1PJ\$qREjtLxwBn5xRFcR2k14z.” with the username.

The password list file was given to the user.

User need to bruteforce by using john the ripper tool to get password to the admin account.

Also the admin made 2 driectories called hash and passwords. User can mv necessary files into those driectories.



After login to the admin account there is a file calle won.txt in the desktop. The file contains the flag. The flag is - CTF{!Genius}

```

File Edit View Search Terminal Help
admin@ubuntu-VirtualBox: ~/Desktop
admin@ubuntu-VirtualBox:~/home$ cd home/admin/Desktop
bash: cd: home/admin/Desktop: No such file or directory
admin@ubuntu-VirtualBox:~/home$ ls
admin dell ubuntu user ww
admin@ubuntu-VirtualBox:~/home$ cd admin
admin@ubuntu-VirtualBox:~$ cd Desktop
admin@ubuntu-VirtualBox:~/Desktop$ ls
won.txt
admin@ubuntu-VirtualBox:~/Desktop$ cat won.txt
congratulations !!

CTF{IGentle}
admin@ubuntu-VirtualBox:~/Desktop$ █

```

Step 17

Get the cure to the virus.

After login to the admin account, there is file called “halflife.txt” it has the virus cure. But it is encrypted in 3DES format, to decrypt the text user need to assemble virus information fragments together that found in step 7 and 11.

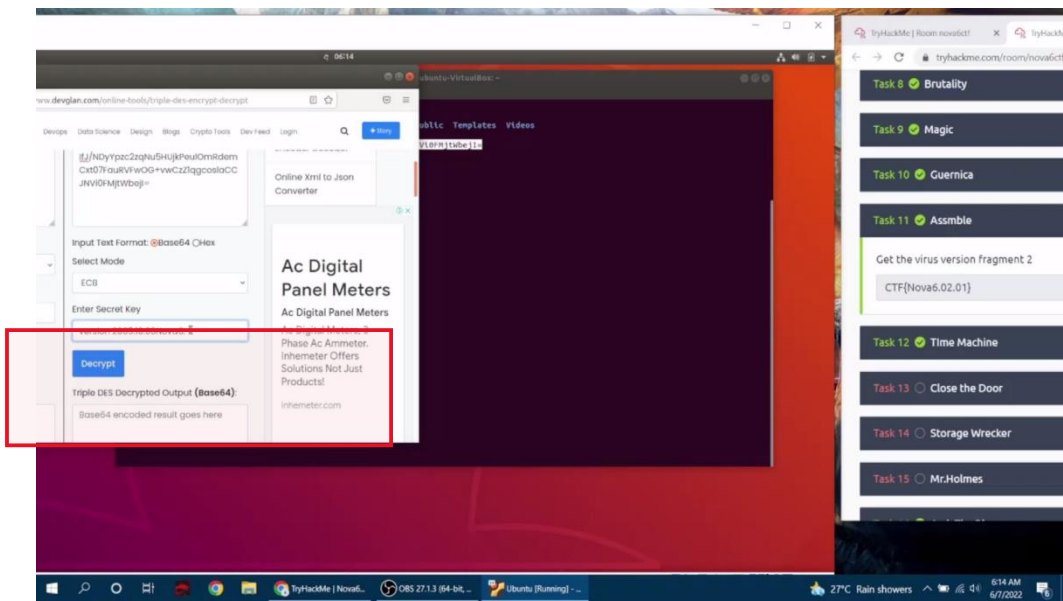
The key will be – version 2005.10.06Nova6.02.01

```
admin@ubuntu-VirtualBox: ~
File Edit View Search Terminal Help
admin@ubuntu-VirtualBox: /home$ cd /home/admin/Desktop
bash: cd: /home/admin/Desktop: no such file or directory
admin@ubuntu-VirtualBox: /home$ ls
admin dell ubuntu user ww
admin@ubuntu-VirtualBox: /home$ cd /admin
admin@ubuntu-VirtualBox: ~$ cd /Desktop
admin@ubuntu-VirtualBox: ~$ cd /Desktop$ ls
won.txt
admin@ubuntu-VirtualBox: ~$ cd /Desktop$ cat won.txt
congratulations !!

CTF{IGentus}
admin@ubuntu-VirtualBox: ~$ cd /Desktop$ cd ..
admin@ubuntu-VirtualBox: ~$ ls
Desktop Documents Downloads halflife.txt Music Pictures Public Templates Videos
admin@ubuntu-VirtualBox: ~$ cat halflife.txt
IfJ/NoyYpzcZzqNuSMUjKPeULomRdenCxt077auNVRwOG+vwCZzIagcoslaCCJNvI0RfHjtbeJi=

3De$
admin@ubuntu-VirtualBox: ~$ this encrypted text can be decrypted by using the virus version number that revealed from previous steps.
```

Used <https://www.devglan.com/> to decrypt the cipher text.



The final FLAG is - CTF{anit-nova ver nova6.2015.05.1. #546486686444443453}

