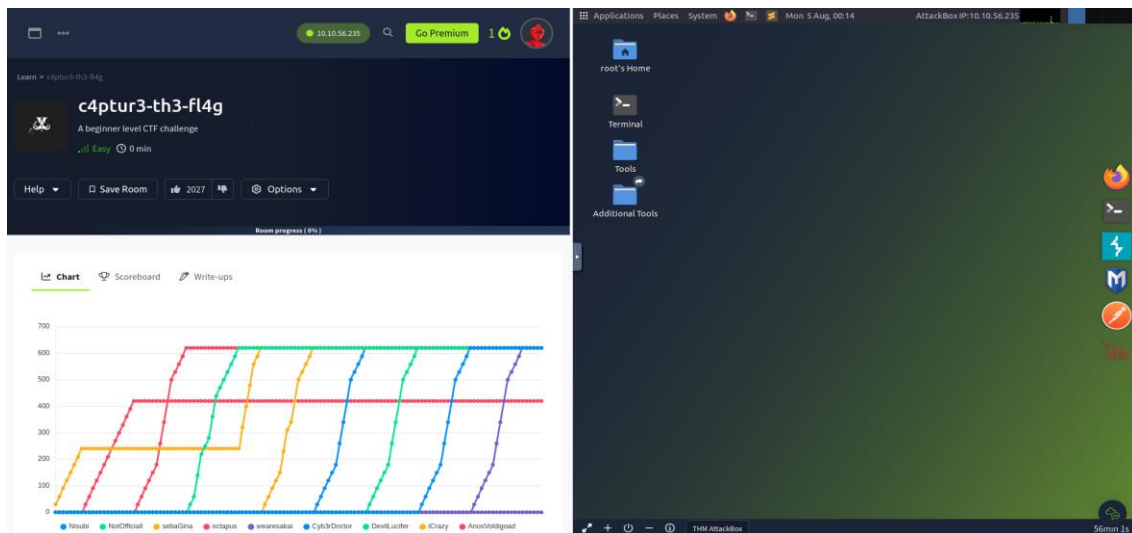




c4ptur3-th3-fl4g

C4ptur3-th3-fl4g es una maquina bastante sencilla que no toma mas de 15 minutos el poder resolverla y el proposito es poder obtener información como decodificar, descifrar y extraer datos ocultos.

Lo primero es iniciar la maquina mediante la VPN que ofrece TryHackMe, una vez conectada e iniciada la maquina, tienen una hora para poder resolverla sin la membresia mensual.



Tarea 1: Traducción y desplazamiento:

Pregunta 1: c4n y0u c4p7u23 7h3 f149?

Respuesta: can you capture the flag? (¿Puedes capturar la bandera?)

c4n y0u c4p7u23 7h3 f149?

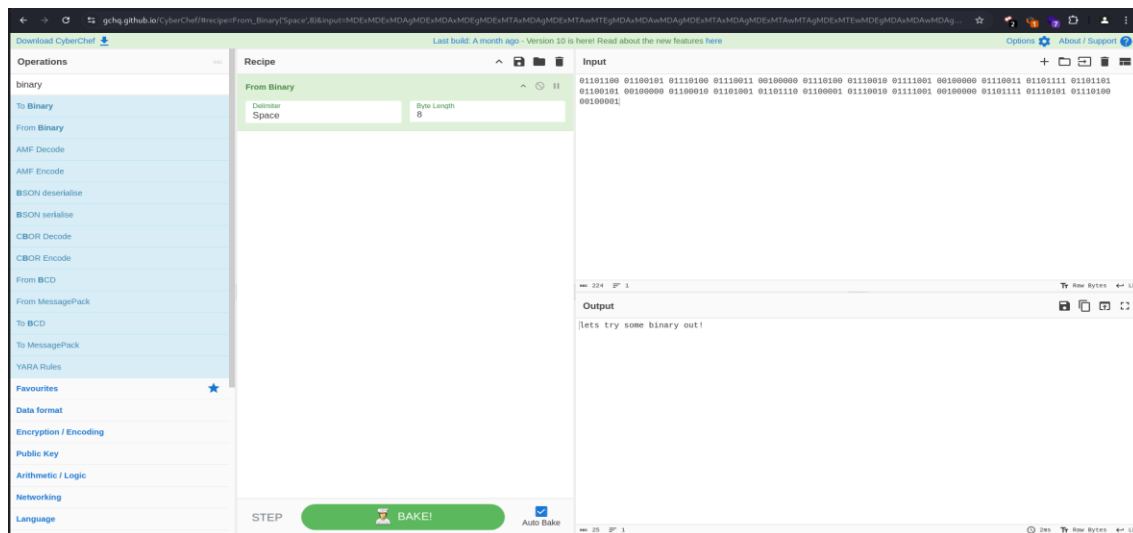
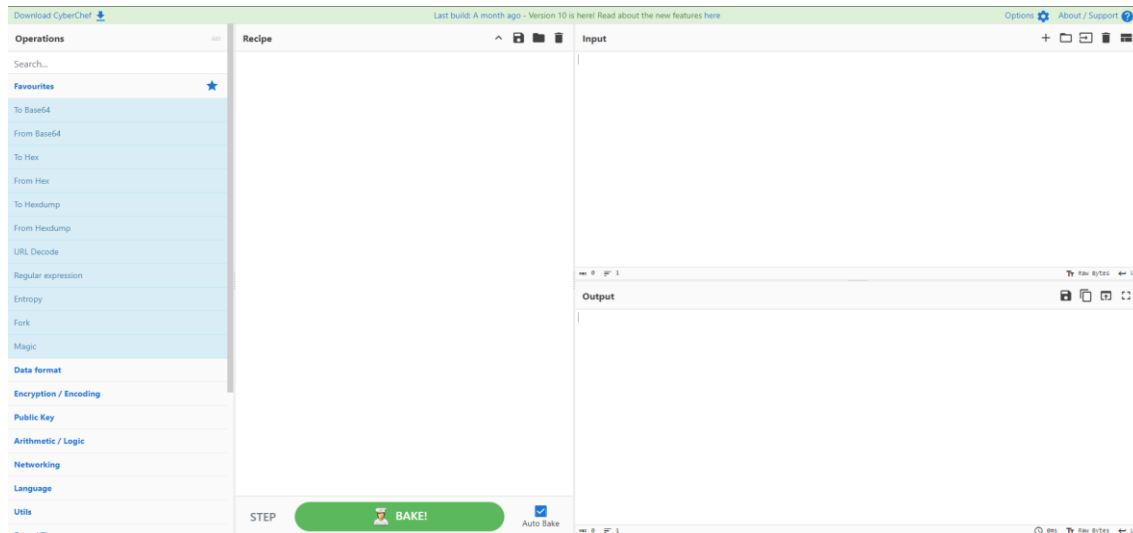
can you capture the flag?

✓ Correct Answer



Pregunta 2: 01101100 01100101 01110100 01110011 00100000 01110100 01110010 01111001
00100000 01110011 01101111 01101101 01100101 00100000 01100010 01101001 01101110
01100001 01110010 01111001 00100000 01101111 01110101 01110100 00100001

Aquí con el browser de preferencia ingresar a la página <https://gchq.github.io/CyberChef/> indicada en la imagen:



Respuesta: lets try some binary out! (¡Probemos con algo de código binario! (Codificación binaria))

01101100 01100101 01110100 01110011 00100000 01110100 01110010 01111001 00100000 01110011 01101111 01101101
01100101 00100000 01100010 01101001 01101110 01100001 01110010 01111001 00100000 01101111 01110101 01110100
00100001

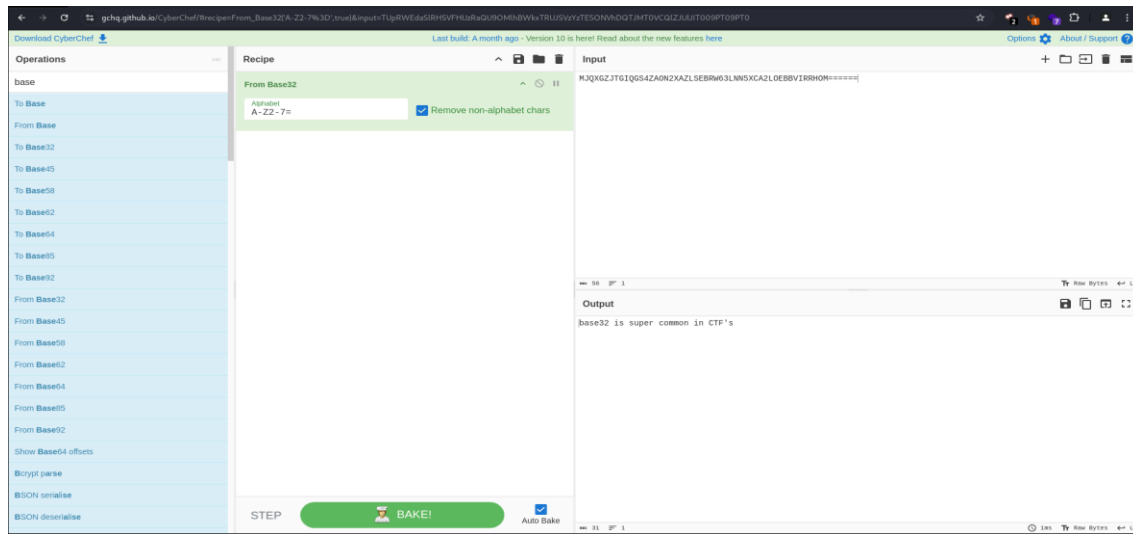
lets try some binary out!

✓ Correct Answer



Pregunta 3:

MJQXGZJTGIQGS4ZAON2XAZLSEBRW63LNN5XCA2LOEBBVIRRHOM=====



Respuesta: base32 is super common in CTF's (Base32 es muy común en los CTF. (Codificación Base32))

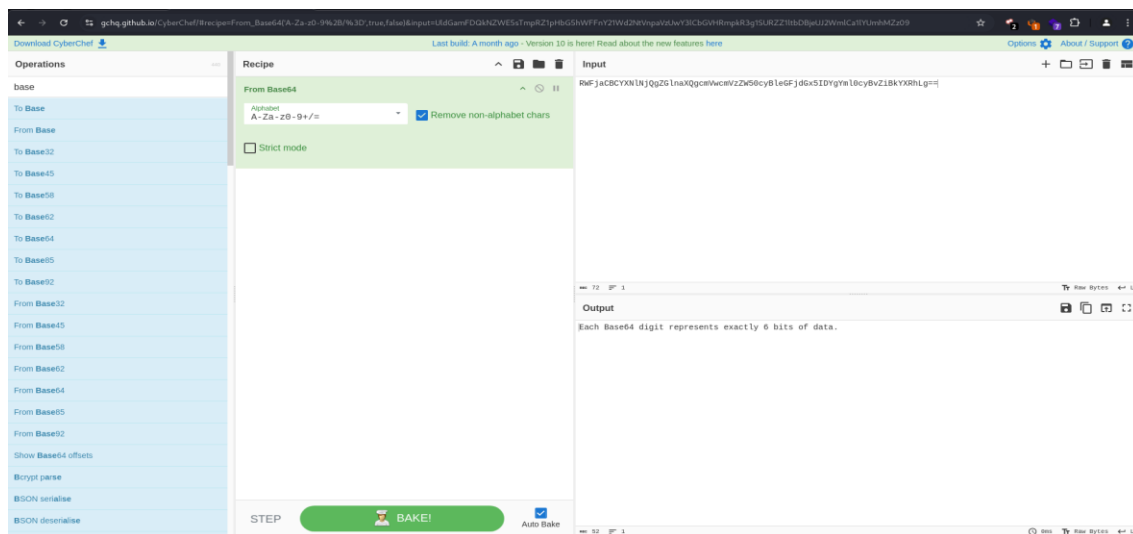
MJQXGZJTGIQGS4ZAON2XAZLSEBRW63LNN5XCA2LOEBBVIRRHOM=====

base32 is super common in CTF's

✓ Correct Answer

Pregunta 4:

RWFjaCBCYXNINjQgZGlnaXQgcmVwcmVzZW50cyBleGFjdGx5IDYgYml0cyBvZiBkYXRhLg==





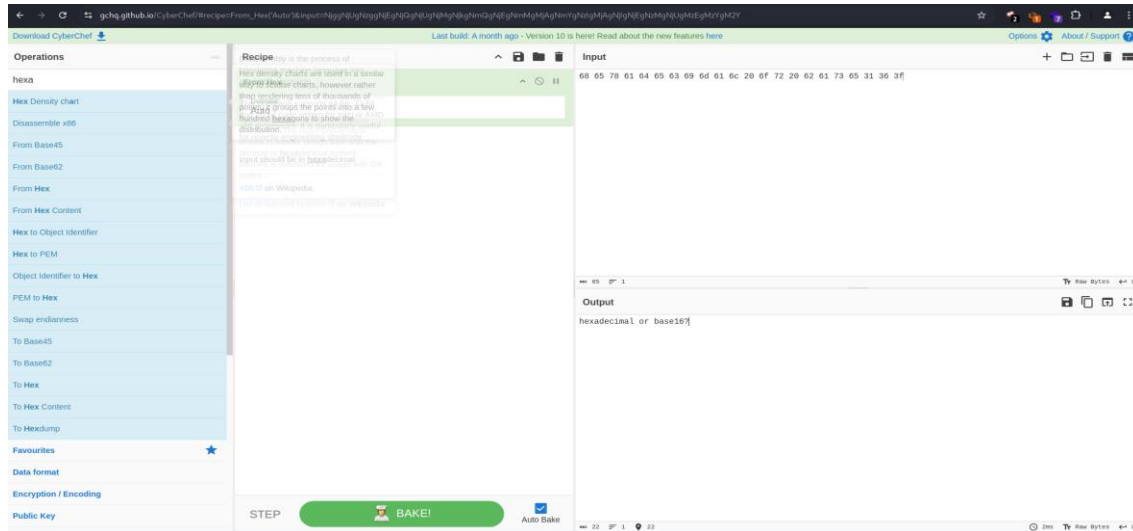
Respuesta: Each Base64 digit represents exactly 6 bits of data. (Cada dígito Base64 representa exactamente 6 bits de datos. (Codificación Base64))

RWFjaCBCYXNINjQgZGlnaXQgcmVwcmVzZW50cyBleGFjdGx5IDYgYml0cyBvZiBkYXRhLg==

Each Base64 digit represents exactly 6 bits of data.

✓ Correct Answer

Pregunta 5: 68 65 78 61 64 65 63 69 6d 61 6c 20 6f 72 20 62 61 73 65 31 36 3f



Respuesta: hexadecimal or base16? (¿hexadecimal o base 16? (hexadecimal))

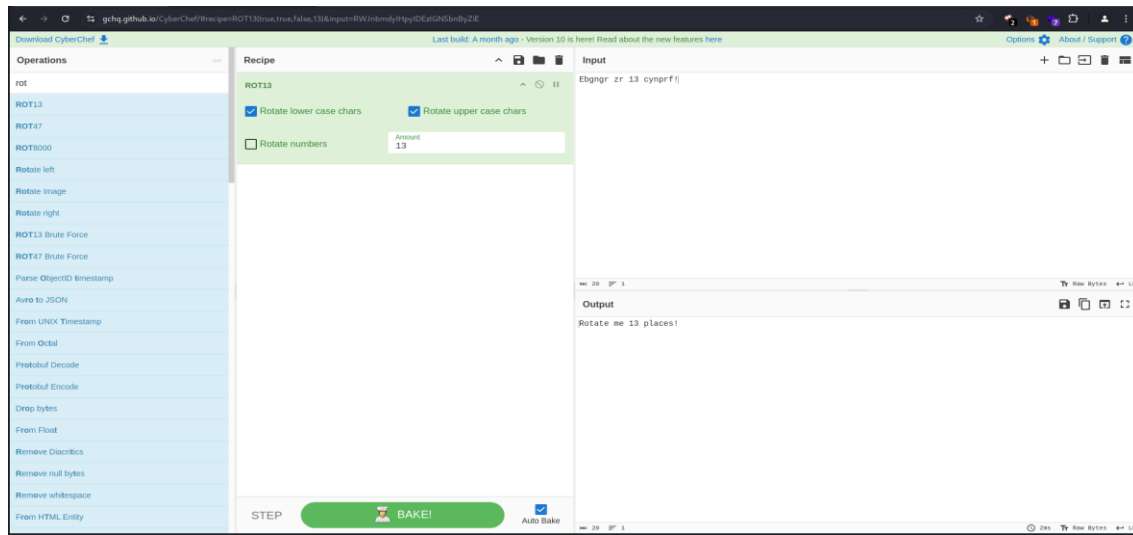
68 65 78 61 64 65 63 69 6d 61 6c 20 6f 72 20 62 61 73 65 31 36 3f

hexadecimal or base16?

✓ Correct Answer



Pregunta 6: ¡Ebgngz zr 13 cynprf! (¡Gírame 13 lugares! (Cifrado ROT -13))



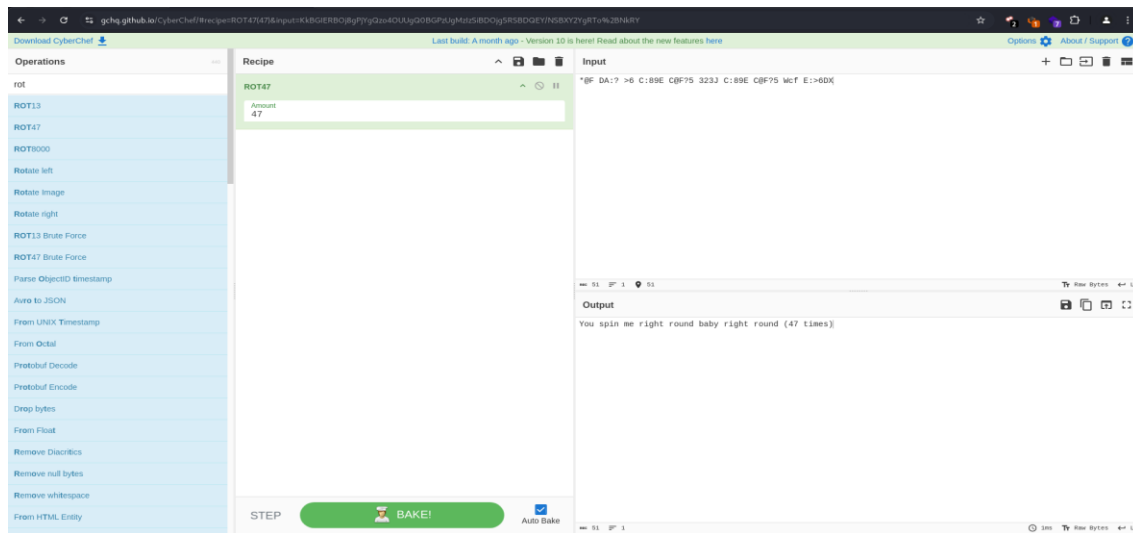
Respuesta: Rotate me 13 places!

Ebgngz zr 13 cynprf!

Rotate me 13 places!

✓ Correct Answer

Pregunta 7: *@F DA:? >6 C:89E C@F?5 323J C:89E C@F?5 Wcf E:>6DX



Respuesta: You spin me right round baby right round (47 times) (Me haces girar como un loco (47 veces) (código ROT -47))

*@F DA:? >6 C:89E C@F?5 323J C:89E C@F?5 Wcf E:>6DX

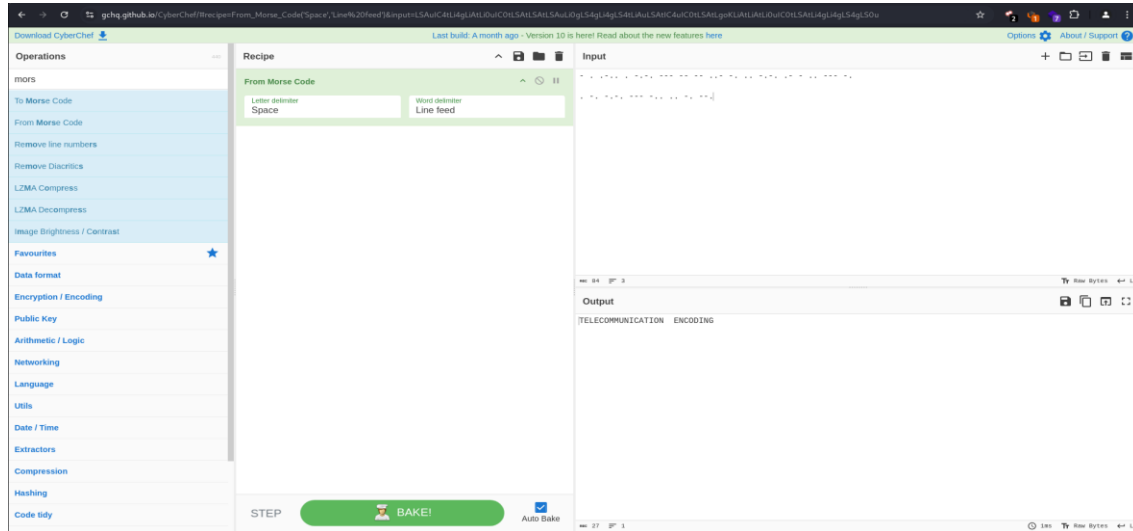
You spin me right round baby right round (47 times)

✓ Correct Answer



Pregunta 8: - - . - - - -

. - . - -



Respuesta: TELECOMMUNICATION ENCODING (codificación de telecomunicaciones (código Morse))

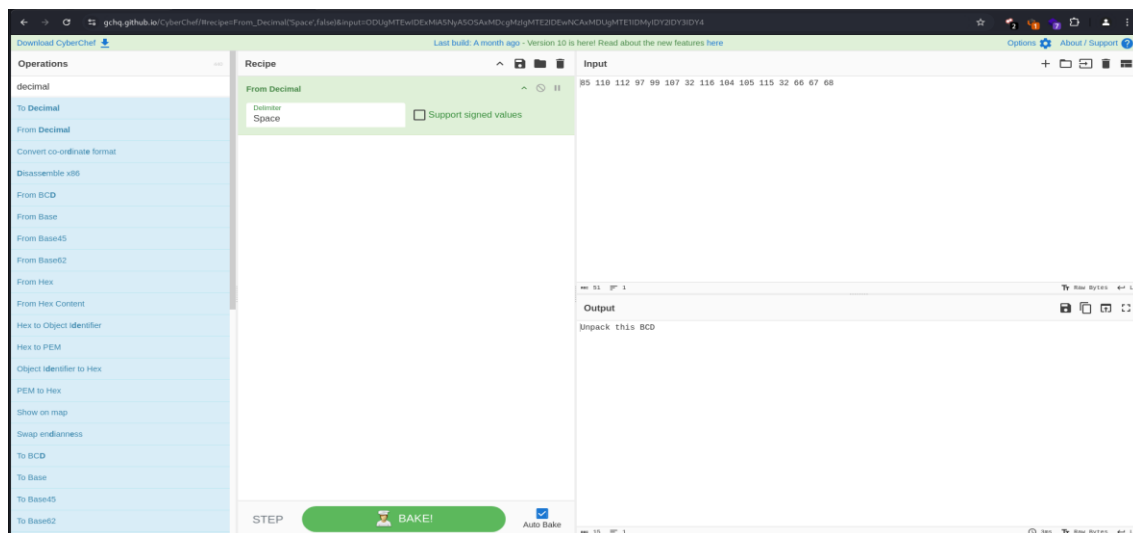
. - . - -

. - . - -

telecommunication encoding

✓ Correct Answer

Pregunta 9: 85 110 112 97 99 107 32 116 104 105 115 32 66 67 68





Respuesta: Unpack this BCD (Descomprima este BCD (decimal codificado en binario))

85 110 112 97 99 107 32 116 104 105 115 32 66 67 68

Unpack this BCD

✓ Correct Answer

Pregunta 10:

[illegible]

[illegible]





The screenshot displays the CyberChef web application. On the left, a sidebar lists various operations such as 'To Decimal', 'Decode', 'PGP Decrypt', and 'Hex to Object Identifier'. The main workspace is configured in 'Recipe' mode. The first operation is 'From Base64', which is active. Below it, the 'Strict mode' checkbox is unchecked. The 'Input' tab shows a long, repetitive Base64 string. The 'Output' tab displays the result of the decoding, which is a message: 'Let's make this a bit trickier...'. At the bottom, a 'STEP 1' indicator and a 'BAKE!' button are visible, along with a 'Support signed values' checkbox.



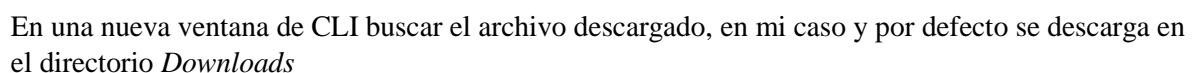
(Base64-> Código Morse-> Binario->ROT -47 -> Decimal)

Let's make this a bit trickier...

✓ Correct Answer

Para esta tarea, necesitas utilizar una herramienta web indicada más adelante:

En la imagen se puede observar que al momento de dar al boto *Download Task Files* se descarga un archivo del tipo audio.

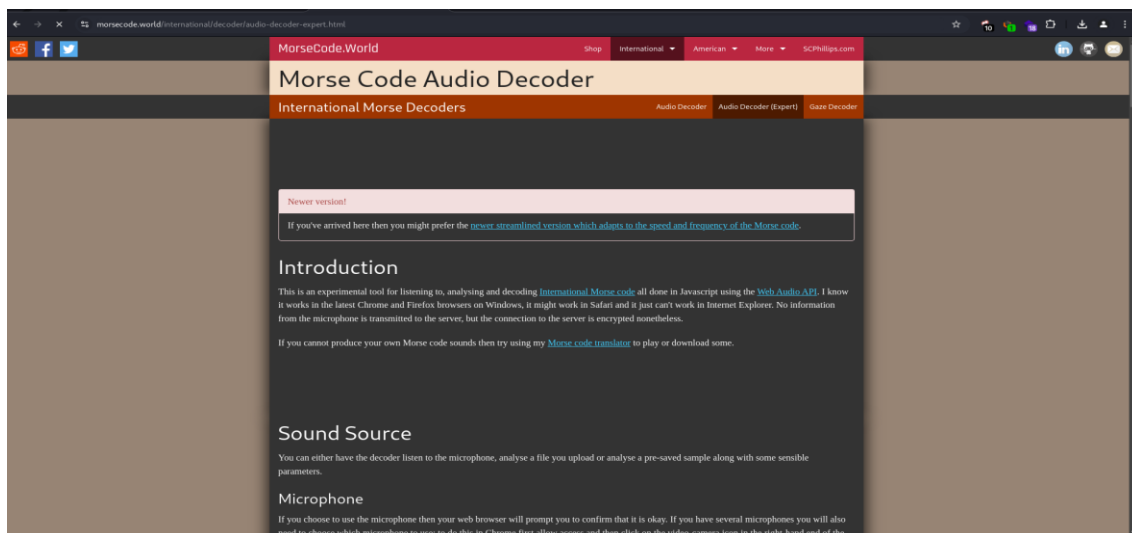




Aquí se utilizó el comando `#file (nombre del archivo descargado).wav`

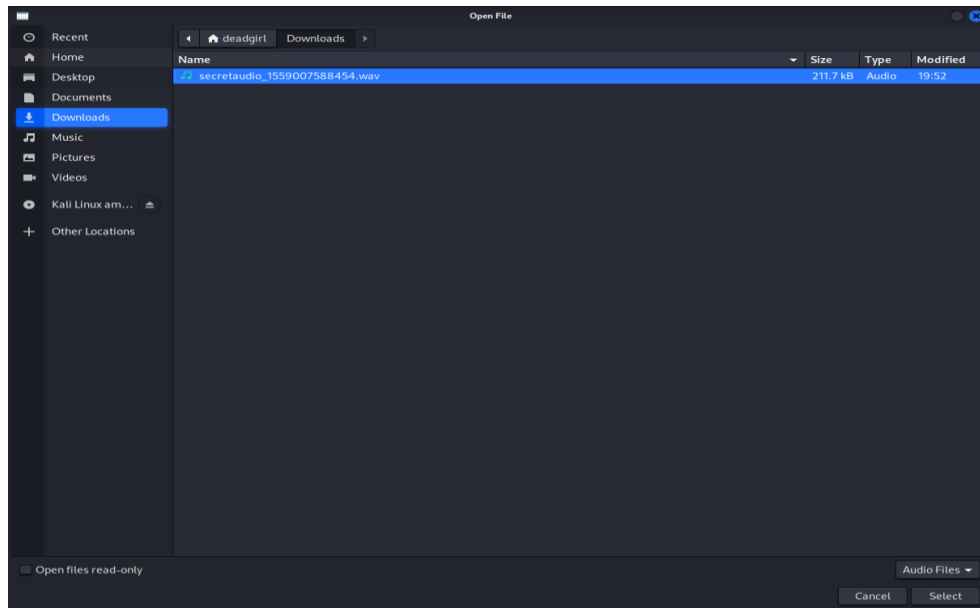
```
root@PeNteStiNg: /home/deadgirl/Downloads
File Actions Edit View Help
# cd Downloads
# ls
DeadGirl.ovpn google-chrome-stable_current_amd64.deb
WindowsXP_1551719014755.jpg secretaudio_1559007588454.wav
# file secretaudio_1559007588454.wav
secretaudio_1559007588454.wav: RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, mono 4
4100 Hz
#
```

Aquí el enlace que los llevara a *Morse Code Audio Decoder* la URL es:
<https://medium.com/@ria.banerjee005/tryhackme-c4ptur3-th3-fl4g-writeup-f230130b0cf9>

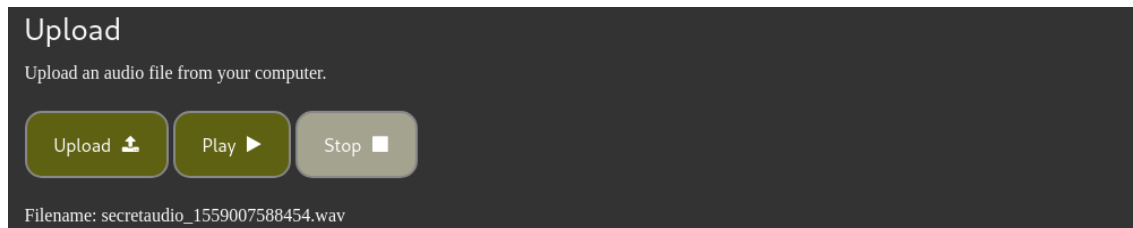


Si siguen bajando se observa una opción que se llama *Upload*, aquí se debe subir el archivo audio descargado anteriormente.





Posterior dar a la opción ***Play***, aquí se revelara un mensaje oculto...



Mensaje oculto ***Super Secret Message***





Respuesta: Super Secret Message (Mensaje Súper Secreto)

Task 2 Spectrograms

A spectrogram is a visual representation of the spectrum of frequencies of a signal as it varies with time. When applied to an audio signal, spectrograms are sometimes called sonographs, voiceprints, or voicegrams. When the data is represented in a 3D plot they may be called waterfalls.

[Download Task Files](#)

Answer the questions below

Download the file

Super Secret Message

Correct Answer

Hint

Tarea 3: Esteganografía:

Aquí utilicé la herramienta *steghide* para recuperar datos ocultos de la imagen proporcionada en el archivo de tarea que he descargado a mi equipo.

Task 3 Steganography

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video.

[Download Task Files](#)

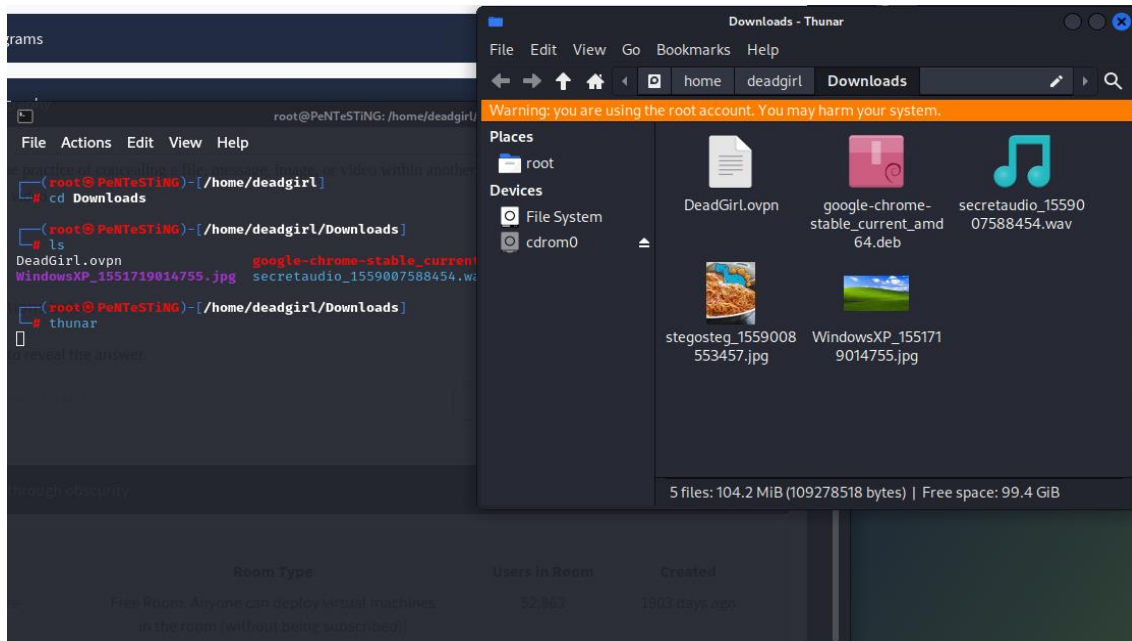
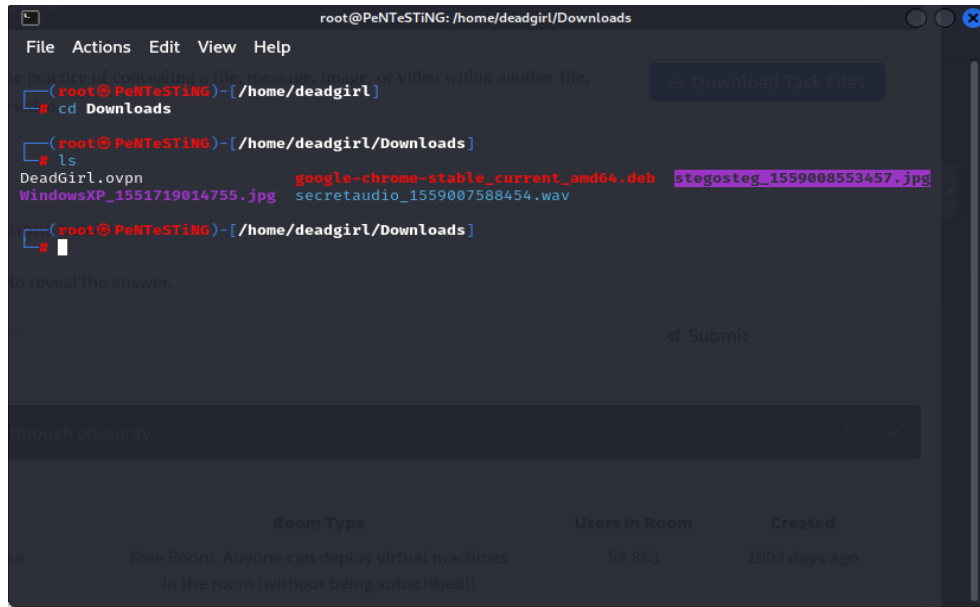
Answer the questions below

Decode the image to reveal the answer.

Answer format: *****

Submit







```
root@PeNteStiNg: /home/deadgirl/Downloads
File Actions Edit View Help
[+] Download Task Files
root@PeNteStiNg)-[/home/deadgirl]
# cd Downloads
root@PeNteStiNg)-[/home/deadgirl/Downloads]
# ls
DeadGirl.ovpn google-chrome-stable_current_amd64.deb stegosteg_1559008553457.jpg
WindowsXP_1551719014755.jpg secretaudio_1559007588454.wav
root@PeNteStiNg)-[/home/deadgirl/Downloads]
# thunar
^C
[+] Reveal the answer
root@PeNteStiNg)-[/home/deadgirl/Downloads]
# file stegosteg_1559008553457.jpg
stegosteg_1559008553457.jpg: JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96,
segment length 16, baseline, precision 8, 254x343, components 3
root@PeNteStiNg)-[/home/deadgirl/Downloads]
#
[+] Rough obscurity
[+] Submit
Room Type Users in Room Created
Free Room. Anyone can deploy virtual machines 52,863 1903 days ago
in the room (without being subscribed)!
```

```
root@PeNteStiNg: /home/deadgirl/Downloads
File Actions Edit View Help
[+] Download Task Files
root@PeNteStiNg)-[/home/deadgirl/Downloads] in another file,
# strings stegosteg_1559008553457.jpg
JFIF
$3br
%6'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxz
#3R
6'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxz
u-g[
.GN?
t1;H1;low
ARxs,
}UR+{n
6h:v of the answer.
YnPI.
2x'Af
wYlg
RL|M,k
WwzsZ
T*s
rjXN
qg+[jZ.
LrL%
Kd5K
J\$o
tH-T
B_].?
wR^iw
\zy0
'>i
v~v4
[+] Submit
Room Type Users in Room Created
Free Room. Anyone can deploy virtual machines 52,863 1903 days ago
in the room (without being subscribed)!
```




Utilicé el comando: steghide extract -sf stegosteg.jpg

```
root@PeNteStiNG: /home/deadgirl/Downloads
File Actions Edit View Help
Unpacking libmcrypt4 (2.5.8-7) ...
Selecting previously unselected package libmhash2:amd64.
Preparing to unpack .../libmhash2_0.9.9-9+b1_amd64.deb ...
Unpacking libmhash2:amd64 (0.9.9-9+b1) ...
Selecting previously unselected package steghide.
Preparing to unpack .../steghide_0.5.1-15_amd64.deb ...
Unpacking steghide (0.5.1-15) ...
Setting up libmhash2:amd64 (0.9.9-9+b1) ...
Setting up libmcrypt4 (2.5.8-7) ...
Setting up steghide (0.5.1-15) ...
Processing triggers for libc-bin (2.38-13) ...
Processing triggers for man-db (2.12.1-2) ...
Processing triggers for kali-menu (2024.3.1) ...

(root@PeNteStiNG)-[/home/deadgirl/Downloads]
# steghide extract -sf stegosteg_1559008553457.jpg
Enter passphrase:

(root@PeNteStiNG)-[/home/deadgirl/Downloads]
# ls
DeadGirl.ovpn                               google-chrome-stable_current_amd64.deb  stegosteg_1559008553457.jpg
WindowsXP_1551719014755.jpg                secretaudio_1559007588454.wav

(root@PeNteStiNG)-[/home/deadgirl/Downloads]
# steghide extract -sf stegosteg_1559008553457.jpg
Enter passphrase:
wrote extracted data to "steganopayload2248.txt".

(root@PeNteStiNG)-[/home/deadgirl/Downloads]
#
```

Una vez ejecutado el comando anterior solicita una password, en mi caso le di enter y se descargó o reveló un archivo txt. Con el comando `# cat steganopayload2248.txt` entrega la flag que se encuentra en dicho archivo.

```
root@PeNteStiNG: /home/deadgirl/Downloads
File Actions Edit View Help
Setting up steghide (0.5.1-15) ...
Processing triggers for libc-bin (2.38-13) ...
Processing triggers for man-db (2.12.1-2) ...
Processing triggers for kali-menu (2024.3.1) ...

(root@PeNteStiNG)-[/home/deadgirl/Downloads]
# steghide extract -sf stegosteg_1559008553457.jpg
Enter passphrase:

(root@PeNteStiNG)-[/home/deadgirl/Downloads]
# ls
DeadGirl.ovpn                               google-chrome-stable_current_amd64.deb  stegosteg_1559008553457.jpg
WindowsXP_1551719014755.jpg                secretaudio_1559007588454.wav

(root@PeNteStiNG)-[/home/deadgirl/Downloads]
# steghide extract -sf stegosteg_1559008553457.jpg
Enter passphrase:
wrote extracted data to "steganopayload2248.txt".

(root@PeNteStiNG)-[/home/deadgirl/Downloads]
# ls
DeadGirl.ovpn                               google-chrome-stable_current_amd64.deb  steganopayload2248.txt
WindowsXP_1551719014755.jpg                secretaudio_1559007588454.wav          stegosteg_1559008553457.jpg

(root@PeNteStiNG)-[/home/deadgirl/Downloads]
# cat steganopayload2248.txt
SpaghettiSteg

(root@PeNteStiNG)-[/home/deadgirl/Downloads]
#
```



Respuesta: SpaghettiSteg

Task 3 Steganography

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video.

[Download Task Files](#)

Answer the questions below

Decode the image to reveal the answer.

Correct Answer

Tarea 4: Seguridad a través de la oscuridad:

Intenté usar steghide nuevamente e intenté descomprimir el contenido, pero hay una manera aún más fácil.

¡Simplemente escribe cat meme.jpg en tu terminal y allí estará, al final del contenido del archivo!

Task 4 Security through obscurity

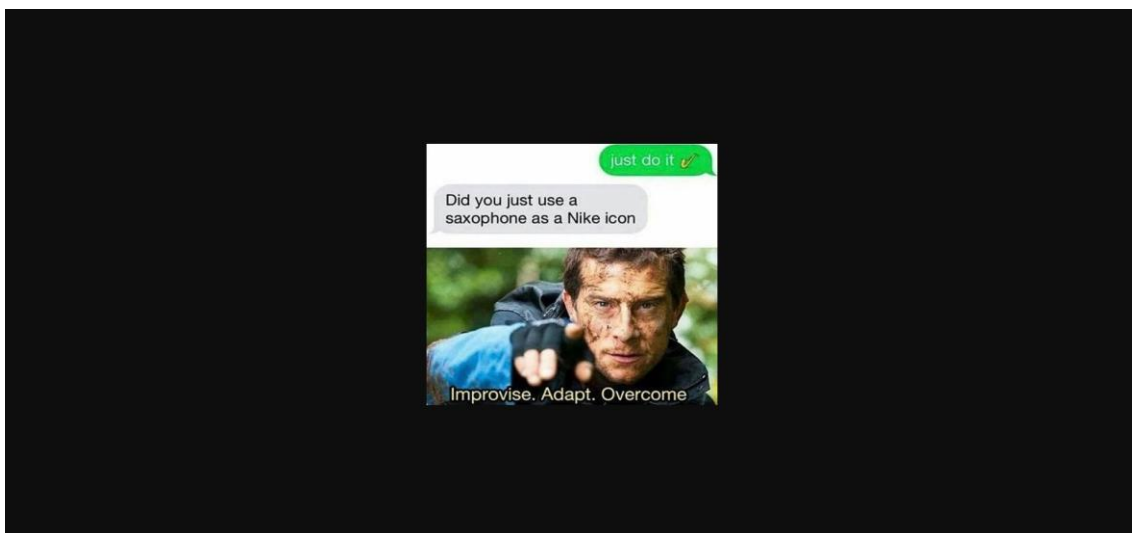
Security through obscurity is the reliance in security engineering on the secrecy of the design or implementation as the main method of providing security for a system or component of a system.

[Download Task Files](#)

Answer the questions below

Download and get 'inside' the file. What is the first filename & extension?

Get inside the archive and inspect the file carefully. Find the hidden text.





Respuesta: hackerchat.png

Entre en el archivo y examine el documento con atención. Encuentre el texto oculto.

Respuesta: AHH_YOU_FOUND_ME! (¡¡¡AHHH_ME_ENCONTRASTE!!!)

¡Eso es todo por hoy! ¡Espero que hayas disfrutado de este Write-Up!

```
root@PeNtEStiNg: /home/deadgirl/Downloads

File Actions Edit View Help

t+***"m+EP+P44+**w0x!4+JD+ _ 6-^7+o$*** **h+^+ _E+M+--VO+p _<+n@?+M;+,Q+rs`i\3+++`k/E+!l
+
**v1+v+ .+***+D+ +*****Hg+e+b9+RN4$+***** ,lG4+.r6+++ \l+*****mX+A+++c0\8`+?/f+p+*****A?C+++>rC
L +. .+I+**X' +***** .+Q+e+0/+***** **e+e+**r+j+RA+ox+++6+ ]+zP+~*d:++K+***W+***KH+***[+rx+***i+ZN+
+*****T(+ +-----+b+e+:+[b+{+0\`5+--+E+C' +*p+P+4*x)+3e4+*****m+z+ ]+q S+R8+++Z+*****8+`+b+*fD(+
0+***Z+++?3z+++l+z+S+ ]+***>+ _j+va+*C++=-F+,+(+*\VC0+*Y+H--+x1_+++ki[/O+d+*HASM+u1"ej+%+*****U+*E+:<ch
+Q?+2+n+++U+z+ +***** ]+v@NB+!+*****>Xw +@eo+*NFC+*Mw_+***i+ V6kb+*****p< +>+Po+*****cu+@+ed+
+j+l+6+9++++ _r+++5Jie+++q+043+0-9y+<G+*z+***s+*`!+i1M/W-a,+++I+}=u@#*+x+My+{`CnQrh+ 0}QnX+***e+
~6+ ]+**+K+*+ ]+*****RXw>+
+q@+1+g+***** +side the file. What is the first filename & extension?
-+`+e0n+p+`+j+***** ?D+***XU[+0+ .x+K+*mp+--+f+***; !#;>+--+x+*+r;%l@k4+{+i+^+3+*C+*f+*F^+;+U+*n; \
+T+*+ ]+(E+6Zá+***A+4x+N+*+Qxg7<+`+ ,+ ,+ ,+ ,+8z+z+ **=0fYp+***O+*W+*\@M+*B0,0+***X+***@V+*C@+*****@+:e+A
Z+*+h
:v+
+*****+`+?_+ _+ _+Yn9+T+***y%+UT$+<+0+ ,+KI+6UP6+*+i+*+vy_+ 0+*****r+*`%+eNk+)+9+*****N+
+*****+QX+*+>+Bxy.F+***=p+4+*H+*r4l+*+U+*+p#t+DQn+*+ ]+*+a+5+,u+ +**pA~q+*****2bXm+
km+*+H6+*+5+*+ .8P/+WF+***y+>X5_+m+_+`[SQP+*+f+*****p+z+*K+*U+u+*+kk+ ]+*****c+S~j@6h+ \+d+*****vA+}=+F+*+s6_+^
+*+*****+P+*+y' +*+^+ (6+
+ @9Xs+ }d+ + e+*****j+*+Qh+={@84+:)+<6+*+x+AnpE+*****D+Ah+1+`+*+â+N+ +*JR`js+ihm+*****zlw@+*r+
+P+ .k+
C+*+*+ ]+4+*+*+*+f+***+X+r+***+I+*+IiZ+ .+*+*+ ,+e+*+6+d+*C+d+*****i+*+a+L@2$Es+*+Dn+@i+S+*i2Mc+***y+*+j+q
IEND+B +`AHH_YOU_FOUND_ME!"
+ \+?+***QO+*+y3+*+ /+***A+
+hackerchat.png +*+ +*+
+U+*+wVQ

Created by Room Type

Free Room. Anyone can deploy virtual machines in the room (without being subscribed to a plan)
```

Download and get 'inside' the file. What is the first filename & extension?

hackerchat.png

✓ Correct Answer

🔍 Hint

```
root@PeNtEStiNg: /home/deadgirl/Downloads

File Actions Edit View Help

t+***"m+EP+P44+**w0x!4+JD+ _ 6-^7+o$*** **h+^+ _E+M+--VO+p _<+n@?+M;+,Q+rs`i\3+++`k/E+!l
+
**v1+v+ .+***+D+ +*****Hg+e+b9+RN4$+***** ,lG4+.r6+++ \l+*****mX+A+++c0\8`+?/f+p+*****A?C+++>rC
L +. .+I+**X' +***** .+Q+e+0/+***** **e+e+**r+j+RA+ox+++6+ ]+zP+~*d:++K+***W+***KH+***[+rx+***i+ZN+
+*****T(+ +-----+b+e+:+[b+{+0\`5+--+E+C' +*p+P+4*x)+3e4+*****m+z+ ]+q S+R8+++Z+*****8+`+b+*fD(+
0+***Z+++?3z+++l+z+S+ ]+***>+ _j+va+*C++=-F+,+(+*\VC0+*Y+H--+x1_+++ki[/O+d+*HASM+u1"ej+%+*****U+*E+:<ch
+Q?+2+n+++U+z+ +***** ]+v@NB+!+*****>Xw +@eo+*NFC+*Mw_+***i+ V6kb+*****p< +>+Po+*****cu+@+ed+
+j+l+6+9++++ _r+++5Jie+++q+043+0-9y+<G+*z+***s+*`!+i1M/W-a,+++I+}=u@#*+x+My+{`CnQrh+ 0}QnX+***e+
~6+ ]+**+K+*+ ]+*****RXw>+
+q@+1+g+***** +side the file. What is the first filename & extension?
-+`+e0n+p+`+j+***** ?D+***XU[+0+ .x+K+*mp+--+f+***; !#;>+--+x+*+r;%l@k4+{+i+^+3+*C+*f+*F^+;+U+*n; \
+T+*+ ]+(E+6Zá+***A+4x+N+*+Qxg7<+`+ ,+ ,+ ,+ ,+8z+z+ **=0fYp+***O+*W+*\@M+*B0,0+***X+***@V+*C@+*****@+:e+A
Z+*+h
:v+
+*****+`+?_+ _+ _+Yn9+T+***y%+UT$+<+0+ ,+KI+6UP6+*+i+*+vy_+ 0+*****r+*`%+eNk+)+9+*****N+
+*****+QX+*+>+Bxy.F+***=p+4+*H+*r4l+*+U+*+p#t+DQn+*+ ]+*+a+5+,u+ +**pA~q+*****2bXm+
km+*+H6+*+5+*+ .8P/+WF+***y+>X5_+m+_+`[SQP+*+f+*****p+z+*K+*U+u+*+kk+ ]+*****c+S~j@6h+ \+d+*****vA+}=+F+*+s6_+^
+*+*****+P+*+y' +*+^+ (6+
+ @9Xs+ }d+ + e+*****j+*+Qh+={@84+:)+<6+*+x+AnpE+*****D+Ah+1+`+*+â+N+ +*JR`js+ihm+*****zlw@+*r+
+P+ .k+
C+*+*+ ]+4+*+*+*+f+***+X+r+***+I+*+IiZ+ .+*+*+ ,+e+*+6+d+*C+d+*****i+*+a+L@2$Es+*+Dn+@i+S+*i2Mc+***y+*+j+q
IEND+B +`AHH_YOU_FOUND_ME!"
+ \+?+***QO+*+y3+*+ /+***A+
+hackerchat.png +*+ +*+
+U+*+wVQ

Created by Room Type

Free Room. Anyone can deploy virtual machines in the room (without being subscribed to a plan)
```



Get inside the archive and inspect the file carefully. Find the hidden text.

AHH_YOU_FOUND_ME!

✓ Correct Answer

🔍 Hint

The screenshot shows the TryHackMe dashboard for a challenge named 'c4ptur3-th3-fl4g'. A 'Congratulations!' modal is displayed in the center, indicating that the user has completed the room. The modal text says: 'You've completed the room! Share this with your friends:'. Below this, there are three social media sharing buttons: 'Twitter', 'Facebook', and 'LinkedIn'. At the bottom of the modal, there is a 'Leave Feedback' link. The background of the dashboard shows a scoreboard chart with multiple colored lines representing different users' progress. The top navigation bar includes links to 'Dashboard', 'Learn', 'Compete', and 'Other'. The right side of the dashboard has a 'Go Premium' button and a '2' icon. The challenge details on the left indicate it is a 'beginner level CTF challenge' and is 'Easy' with a '0 min' duration.