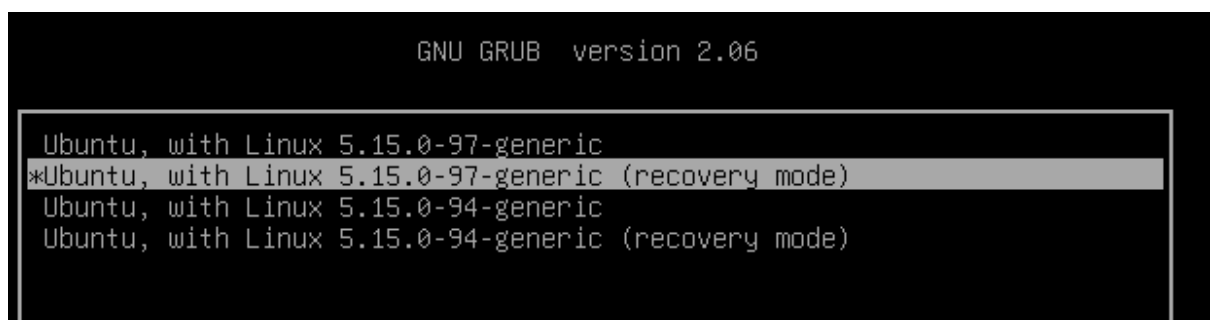


Hackathon – Los Jr.

Reiniciamos máquina virtual y mantenemos pulsados esc + mayus durante el reinicio para acceder a el boot menú.



Seleccionamos advanced options for Ubuntu y después un archivo de recuperación (recovery mode).



Una vez reiniciado nos aparece otro menú. Seleccionamos el root para acceder al Shell prompt.

```
Recovery Menu (filesystem state: read-only)

resume          Resume normal boot
clean           Try to make free space
dpkg            Repair broken packages
fsck            Check all file systems
grub            Update grub bootloader
network         Enable networking
root            Drop to root shell prompt
system-summary  System summary
```

Dentro del Shell utilizamos ls y podemos ver un archivo de texto.

```
root@web:~# [ OK ] Finished Daily apt upgrade and clean activities.
ls
note.txt  snap
root@web:~# _
```

Con la herramienta nano abierta, pulsamos ctrl+r para abrir un archivo y después ctrl+t para buscarlo.


```
..          (parent dir)  .local          (dir)  .ssh          (dir)
.task       (dir)        snap              (dir)  .bash_history  755 B
.bashrc     3 KB        .lessht       20 B  .profile      161 B
note.txt    53 B
```

Dentro del archivo vemos el siguiente código:

```
GNU nano 6.2      New Buffer *
RkxBR3s50TRkMD2mNzE5YmI4ZGY0YjI50TMyOWI50GI5YWVkyX0K
_
```


Con la herramienta base64decode podemos descifrar el código:

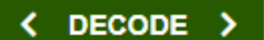
```
RkxBR3s50TRkMDZmNzE5Yml4ZGY0YjI50TMyOWI5OGI5YWVhYX0K
```

 For encoded binaries (like images, documents, etc.) use the file upload form a

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 on

 < **DECODE** > Decodes your data into the area below.

```
FLAG{94d06f719bb8df4b29329b98b9aeda}
```

Ya hemos encontrado nuestra primera bandera:

```
FLAG{94d06f719bb8df4b29329b98b9aeda}
```

Seguimos con el Shell en el root de la web para cambiar la contraseña del usuario.

Escribimos passwd root y nos dejará escribir una nueva contraseña.

```
root@web:~# passwd root
New password:
Retype new password:
passwd: password updated successfully
root@web:~#
```

Reiniciamos la máquina o ctrl+d y luego en el boot menú le damos a resume, y una vez cargada podremos acceder utilizando el usuario root y la contraseña que hemos cambiado anteriormente.

```
web login: root
Password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-97-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Wed Mar 13 07:17:17 PM UTC 2024

System load: 0.052734375      Memory usage: 14%   Processes:      167
Usage of /:  43.8% of 9.75GB   Swap usage:   0%   Users logged in: 0

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

Una vez dentro utilizamos el comando ls para ver el contenido.

```
System information as of Wed Mar 13 09:35:55 PM UTC 2024

System load: 0.11279296875    Memory usage: 14%    Processes:    168
Usage of /: 44.1% of 9.75GB    Swap usage: 0%      Users logged in: 0

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings

Last login: Wed Mar 13 21:26:23 UTC 2024 on tty1
root@web:~# ls
FLAG{94d06f719bb8df4b29329b98b9aeda}  note.txt  snap
root@web:~#
```

Introducimos comando cat note.txt para acceder al contenido y nos muestra el primer código ya descifrado anteriormente con la herramienta nano.

```
Last login: Wed Mar 13 21:26:23 UTC 2024 on tty1
root@web:~# ls
FLAG{94d06f719bb8df4b29329b98b9aeda}  note.txt  snap
root@web:~# cat note.txt
RkxBR3s50TRkMD2mNzE5YmI4ZGY0YjI5OTMyOWI5OGI5YWVhYX0K
root@web:~# _
```

Una vez descifrado utilizamos el comando cd /home para volver al inicio y ls para que me muestre la lista de contenido del directorio. Nos muestra **rawulf** y **sysadmin**, utilizando cat rawulf para que me muestre el contenido de ese archivo nos indica que es un directorio, así que entramos con cd rawulf y ls para que muestre los archivos y encontramos otro archivo de texto note.txt. Ingresamos comando cat note.txt y nos da el segundo código y lo analizamos en base64decode.

```
RkxBR3s50TRkMD2mNzE5YmI4ZGY0YjI5OTMyOWI5OGI5YWVhYX0K
MjUyYjZhNX0K
```

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).

< DECODE >

Success!

The Base64 decoded data is:

```
FLAG{10eu437a275cff1c03ded98f2252b6a5}
```

Volvemos atrás con el comando `cd ..` y `ls` para que me muestre la lista de archivos y seguidamente utilizo el comando `cd sysadmin` para ver el directorio y `ls -a` para que me muestre lo que esta oculto y encontramos archivos donde se podría hacer una inyección SQL.

```
root@web:/home# ls
rawulf  sysadmin
root@web:/home# cat rawulf
cat: rawulf: Is a directory
root@web:/home# cd rawulf
root@web:/home/rawulf# ls
note.txt
root@web:/home/rawulf# cat note.txt
RkxBR3sxMGVlNDM3YTI3NWNmZjFjMDNkZWQ5OGYyMjUyYjZhNX0K
root@web:/home/rawulf# cd ..
root@web:/home# ls
rawulf  sysadmin
root@web:/home# cat sysadmin
cat: sysadmin: Is a directory
root@web:/home# cd sysadmin
root@web:/home/sysadmin# ls
root@web:/home/sysadmin# ls -a
.      .bash_history  .bashrc  .profile  .sudo_as_admin_successful
..     .bash_logout  .cache   .ssh
```