

HACKATHON

Búsqueda de vulnerabilidades

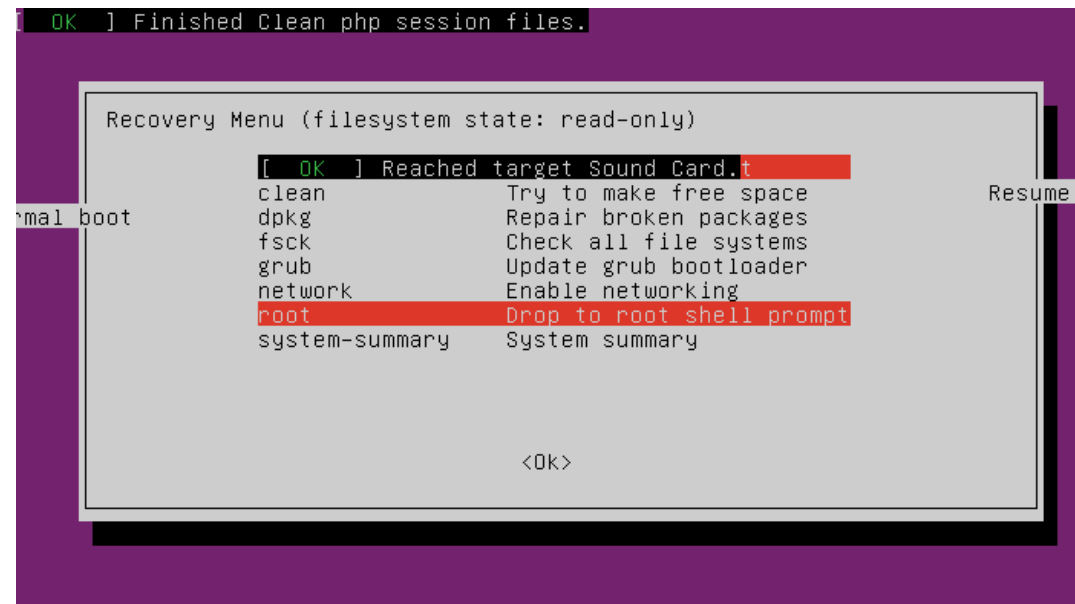
Índice

1. Root	2
2. Flags	3,4,5

Búsqueda de vulnerabilidades

1. Admin

Encontramos que en el modo recovery nos deja entrar como root al sistema:



Entramos y encontramos una nota la abrimos, esta en Base64 las des codificamos:


```
root@web:~/snap# cd ..
root@web:~# ls
note.txt  snap
root@web:~# cat note.txt
RKxBR3s50TRkMD2mNzE5YmI4ZGY0YjI5OTMyOWI5OGI5YWVhYX0K
root@web:~# _
```


Tenemos una flag:

Decode from Base64 format

Simply enter your data then push the decode button.



RkxBR3s5OTRkMDZmNzE5YmI4ZGY0YjI50TMyOWI5OGI5YWVhYX0K

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

AUTO-DETECT  Source character set. Detected: CP50220

☐ 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

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

FLAG{994d06f719bb8dfb474b7b7aeda}

Vemos los usuarios del sistema, en /etc/shadow/

```
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
lapt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
syslog:x:107:113::/home/syslog:/usr/sbin/nologin
uuidd:x:108:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:109:115::/nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:111:117::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:112:118:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:114:120:MySQL Server,,,:/nonexistent:/bin/false
rawulf:x:1001:1001::/home/rawulf:/bin/sh
```

Teniendo el root, creamos un usuario, le damos permisos de root y iniciamos sesión con ese usuario creado.

sudo adduser admin1

sudo usermod -aG sudo admin1

En el archivo shadow podemos ver que existe otro usuario llamado rawulf, ya que somos root le cambiamos el password y iniciamos sesión con el: cambiamos su password con passwd rawulf.

Tenemos el flag del usuario rawulf el cual está en Base64.

```
$ ls -la
total 32
drwxr-x--- 4 rawulf rawulf 4096 Mar 10 16:30 .
drwxr-xr-x 5 root    root   4096 Mar 10 14:21 ..
-rw-r--r-- 1 rawulf rawulf  220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 rawulf rawulf 3771 Jan  6  2022 .bashrc
drwx----- 2 rawulf rawulf 4096 Mar 10 16:30 .cache
-rw-r--r-- 1 rawulf rawulf   53 Mar  1 06:56 note.txt
-rw-r--r-- 1 rawulf rawulf  807 Jan  6  2022 .profile
drwxr-xr-x 2 rawulf rawulf 4096 Mar 10 16:33 .task
$ cat note.txt
RkxBR3sxMGVlNDM3YTI3NWNmZjFjMDNkZWQ5OGYyMjUyYjZhNX0K
$
```


Lo decodificamos:

Decode from Base64 format


Simply enter your data then push the decode button.

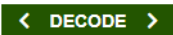

```
RkxBR3sxMGLNDM3YTl3NWNmZjFjMDNkZWQ5OGYyMjUyYjZhNX0K
```

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

AUTO-DETECT  Source character set. Detected: UTF-8

☐ 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.

```
FLAG{10eK437a275cff1c03ded98f2252b6a5}
```