hacemos arp -n para saber la ip

```
┌──(kali㉿kali)-[~]
└─$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.1              ether   0c:8e:29:2a:4a:6e   C                     eth1
192.168.1.113            ether   3c:a8:2a:97:61:3c   C                     eth1
```

hacemos un nmap

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -O -sV 192.168.1.113
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-08 12:19 EST
Nmap scan report for HP97613C.home (192.168.1.113)
Host is up (0.012s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
80/tcp   open  http       HP Deskjet 2540 series printer http config (Serial CN53O5F5W20604)
|_http-server-header: HP HTTP Server; HP Deskjet 2540 series - D3A78B; Serial Number: CN53O5F5W20604; Built:Tue Sep 09, 2014 0
9:29:37AM {CBP1FN1437AR}
| http-methods:
|_  Potentially risky methods: PUT DELETE
|_http-title: Site doesn't have a title (text/html).
443/tcp  open  ssl/http   HP Deskjet 2540 series printer http config (Serial CN53O5F5W20604)
|_http-title: Site doesn't have a title (text/html).
|_ssl-date: 2024-03-08T18:25:56+00:00; +57m47s from scanner time.
| ssl-cert: Subject: commonName=HP97613C/organizationName=HP/stateOrProvinceName=Washington/countryName=US
| Not valid before: 2014-09-09T08:29:37
|_Not valid after:  2034-09-04T08:29:37
631/tcp  open  http       HP Deskjet 2540 series printer http config (Serial CN53O5F5W20604)
|_http-server-header: HP HTTP Server; HP Deskjet 2540 series - D3A78B; Serial Number: CN53O5F5W20604; Built:Tue Sep 09, 2014 0
9:29:37AM {CBP1FN1437AR}
| http-methods:
|_  Potentially risky methods: PUT DELETE
8080/tcp open  http       HP Deskjet 2540 series printer http config (Serial CN53O5F5W20604)
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: HP HTTP Server; HP Deskjet 2540 series - D3A78B; Serial Number: CN53O5F5W20604; Built:Tue Sep 09, 2014 0
9:29:37AM {CBP1FN1437AR}
| http-methods:
|_  Potentially risky methods: PUT DELETE
9100/tcp open  jetdirect?
9220/tcp open  hp-gsg     HP Generic Scan Gateway 1.0
MAC Address: 3C:A8:2A:97:61:3C (Hewlett Packard)
Device type: general purpose
Running: Wind River VxWorks
OS CPE: cpe:/o:windriver:vxworks
OS details: VxWorks
Network Distance: 1 hop
Service Info: Device: printer; CPE: cpe:/h:hp:deskjet_2540_series

Host script results:
|_clock-skew: 57m46s

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 508.47 seconds
```

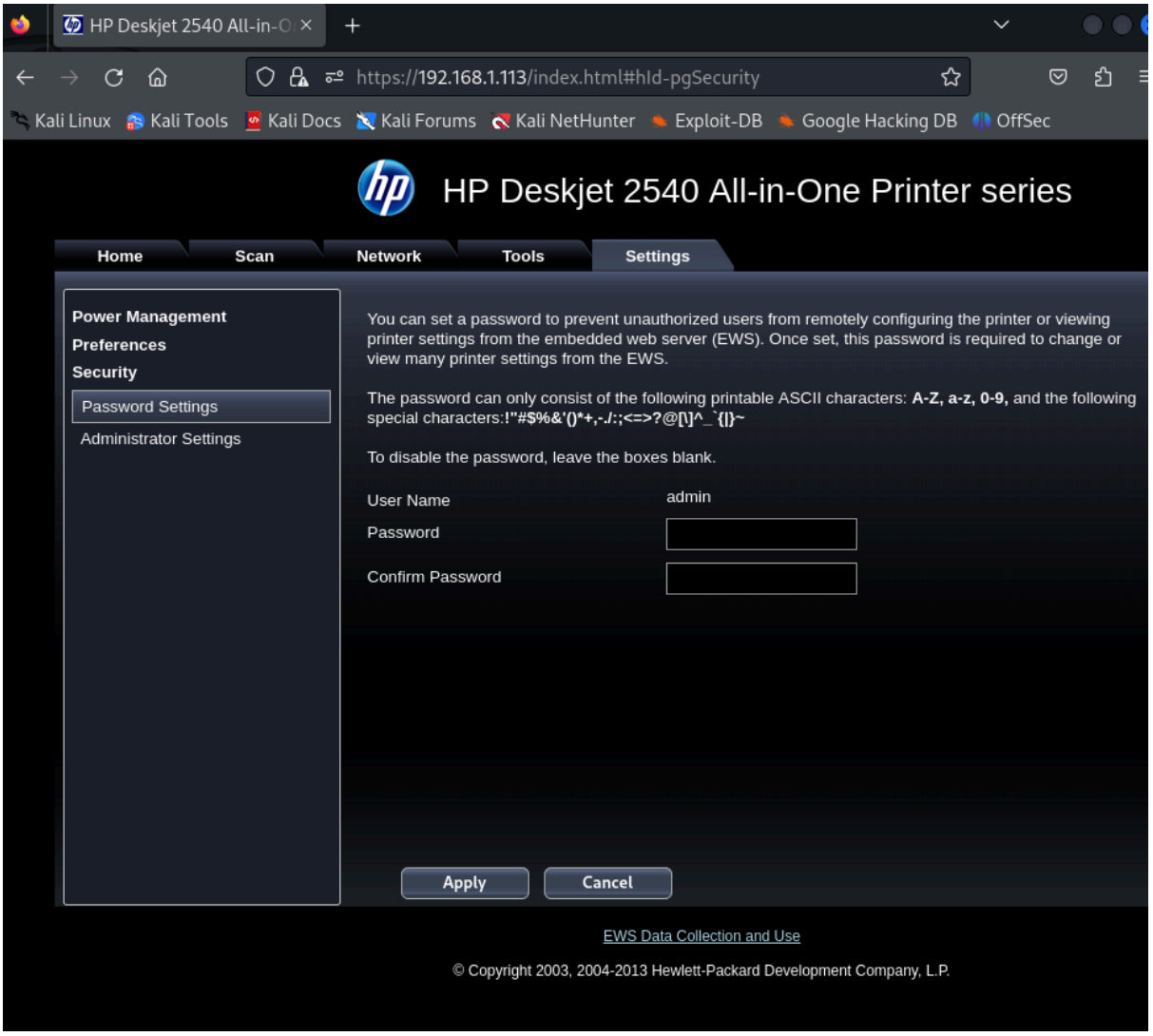
Ahora probaremos a hacer con nmap alguna prueba con los scripts que tiene en su base: Nos dá como resultado este **CVE-2011-1002.** El cual trata de que permite hacer un ataque de denegación de servicios.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -f --script vuln 192.168.1.113
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-07 16:20 EST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for HP97613C.home (192.168.1.113)
Host is up (0.038s latency).
All 1000 scanned ports on HP97613C.home (192.168.1.113) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 3C:A8:2A:97:61:3C (Hewlett Packard)

Nmap done: 1 IP address (1 host up) scanned in 80.33 seconds
```

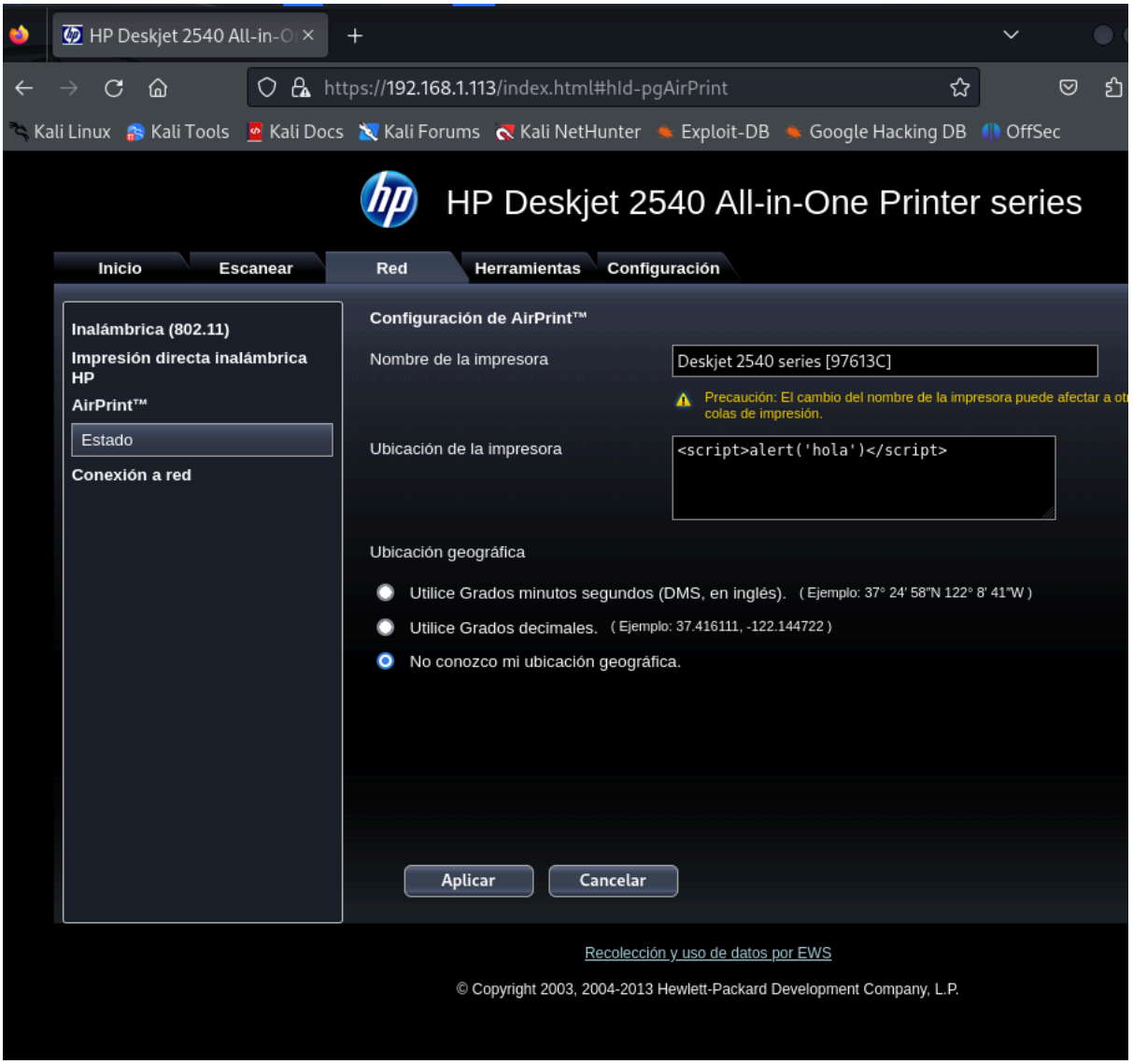
Ahora haremos un dirb con la wordlist dada: la cual nos encuentra dos directorios, el primero es solo una imagen. El segundo es una web, la abrimos en el buscador.

```
┌──(kali㉿kali)-[~]
└─$ dirb http://192.168.1.113 word.txt

_____________________
DIRB v2.22
By The Dark Raver
_____________________

START_TIME: Fri Mar  8 13:26:14 2024
URL_BASE: http://192.168.1.113/
WORDLIST_FILES: word.txt

_____________________

GENERATED WORDS: 4727

---- Scanning URL: http://192.168.1.113/ ----
+ http://192.168.1.113/favicon.ico (CODE:200|SIZE:766)
+ http://192.168.1.113/index.html (CODE:200|SIZE:679)

_____________________
END_TIME: Fri Mar  8 13:29:08 2024
DOWNLOADED: 4727 - FOUND: 2
```

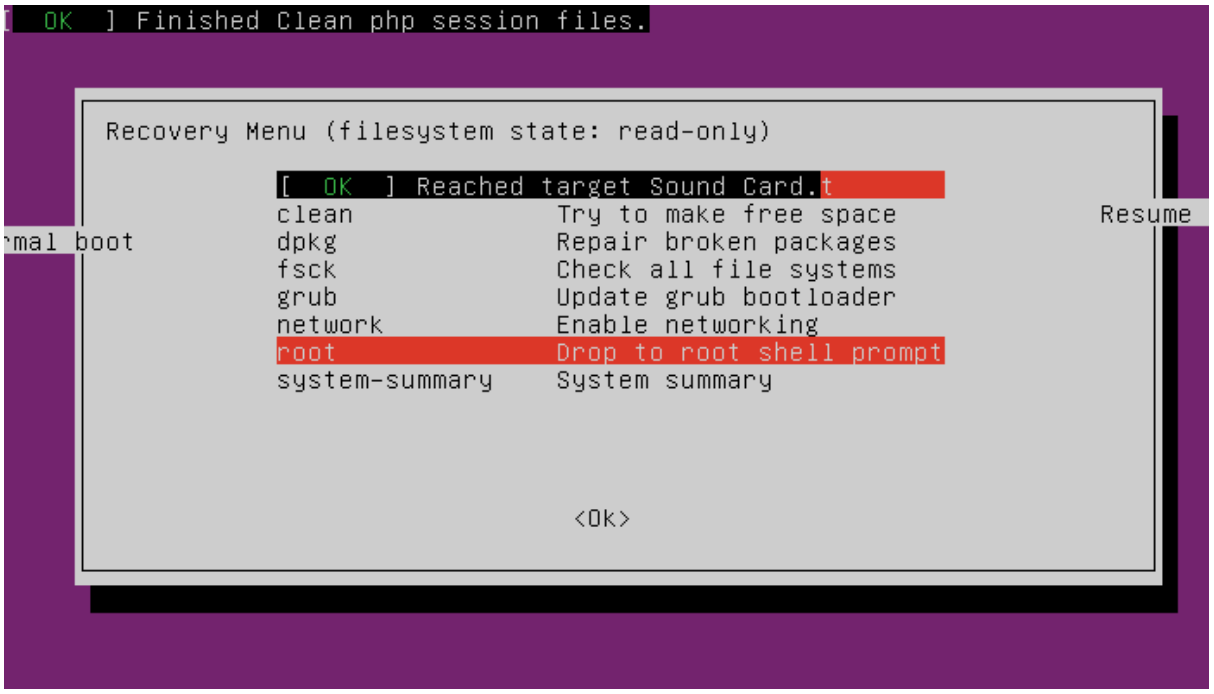
Vemos la web: aquí en la parte de configuración nos permite crear un password pero es solo para el acceso de la web.



Mirando por la web, encontramos en el apartado de la red un espacio donde podemos escribir: y vemos que es vulnerable a XSS Storage y Reflected. Podemos ejecutar scripts.



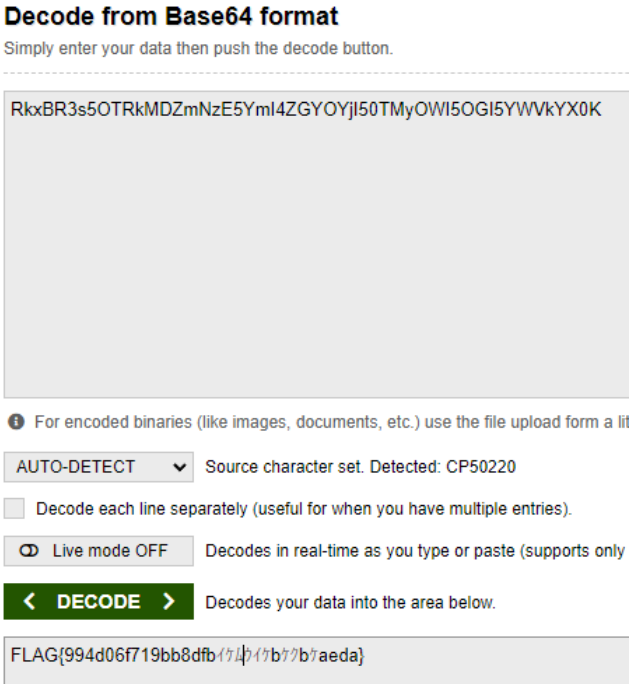
Encontramos que en el modo recovery nos deja entrar como root al sistema:



Entramos y encontramos una nota la abrimos:

```
root@web:~/snap# cd ..
root@web:~# ls
note.txt  snap
root@web:~# cat note.txt
RkxBR3s5OTRkMDZmNzE5YmI4ZGYOYjI5OTMyOWI5OGI5YWVkYX0K
root@web:~# _
```

Tenemos una flag:



vemos los usuarios del sistema

```
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/nologi
n
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/n
ologin
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/sbi
n/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.

RkxBR3sxMGVLNDM3YTI3NWNmZjFjMDNkZWQ5OGYyMjUyYjZhNX0K

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}