

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 CN5305F5W20604)
|_ http-server-header: HP HTTP Server; HP Deskjet 2540 series - D3A788; Serial Number: CN5305F5W20604; Built:Tue Sep 09, 2014 09:29:37AM {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 CN5305F5W20604)
|_ 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 CN5305F5W20604)
|_ http-server-header: HP HTTP Server; HP Deskjet 2540 series - D3A788; Serial Number: CN5305F5W20604; Built:Tue Sep 09, 2014 09:29:37AM {CBP1FN1437AR}
|_ http-methods:
|_   Potentially risky methods: PUT DELETE
8080/tcp   open  http           HP Deskjet 2540 series printer http config (Serial CN5305F5W20604)
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: HP HTTP Server; HP Deskjet 2540 series - D3A788; Serial Number: CN5305F5W20604; Built:Tue Sep 09, 2014 09:29:37AM {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.

The screenshot shows a web browser window with the address bar displaying `https://192.168.1.113/index.html#hId-pgSecurity`. The browser's address bar includes several bookmarks: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The page title is "HP Deskjet 2540 All-in-One Printer series". The navigation menu includes Home, Scan, Network, Tools, and Settings. The left sidebar shows a tree view with Power Management, Preferences, Security, Password Settings (selected), and Administrator Settings. The main content area is titled "Power Management Preferences Security Password Settings". It contains the following text: "You can set a password to prevent unauthorized users from remotely configuring the printer or viewing printer settings from the embedded web server (EWS). Once set, this password is required to change or view many printer settings from the EWS." and "The password can only consist of the following printable ASCII characters: A-Z, a-z, 0-9, and the following special characters: !\"#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~". Below this, it says "To disable the password, leave the boxes blank." The form has three fields: "User Name" with the value "admin", "Password" (empty), and "Confirm Password" (empty). At the bottom of the form are "Apply" and "Cancel" buttons. The footer of the page includes a link "EWS Data Collection and Use" and a copyright notice: "© Copyright 2003, 2004-2013 Hewlett-Packard Development Company, L.P."

HP Deskjet 2540 All-in-One Printer series

Home Scan Network Tools Settings

Power Management
Preferences
Security
Password Settings
Administrator Settings

You can set a password to prevent unauthorized users from remotely configuring the printer or viewing printer settings from the embedded web server (EWS). Once set, this password is required to change or view many printer settings from the EWS.

The password can only consist of the following printable ASCII characters: A-Z, a-z, 0-9, and the following special characters: !\"#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~

To disable the password, leave the boxes blank.

User Name admin

Password

Confirm Password

Apply Cancel

[EWS Data Collection and Use](#)

© Copyright 2003, 2004-2013 Hewlett-Packard Development Company, L.P.

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.

The screenshot shows a web browser window with the URL `https://192.168.1.113/index.html#hld-pgAirPrint`. The browser's address bar and tabs are visible, showing a tab for 'HP Deskjet 2540 All-in-One'. The browser's bookmark bar includes links to 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', and 'OffSec'.

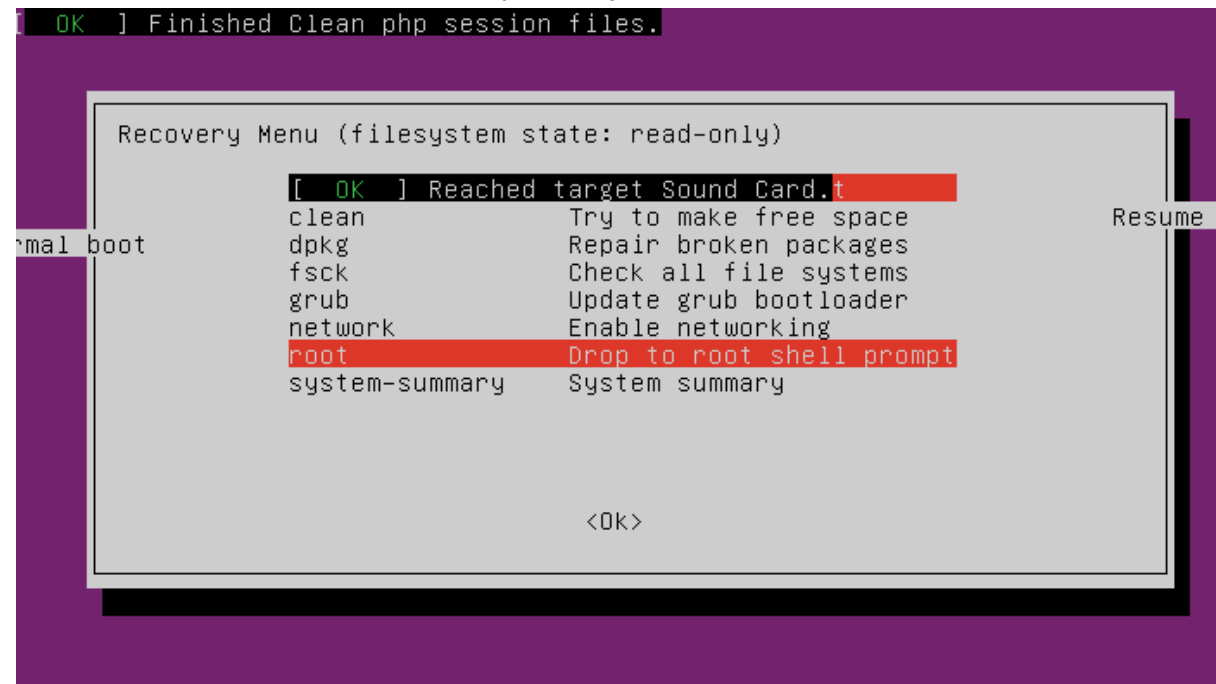
The HP logo is at the top center, followed by the text 'HP Deskjet 2540 All-in-One Printer series'. Below this is a navigation bar with tabs: 'Inicio', 'Escanear', 'Red', 'Herramientas', and 'Configuración'. The 'Red' tab is selected.

The main content area is titled 'Configuración de AirPrint™'. It contains several fields and options:

- Nombre de la impresora:** A text field containing 'Deskjet 2540 series [97613C]'. Below it is a warning icon and text: 'Precaución: El cambio del nombre de la impresora puede afectar a otras colas de impresión.'
- Ubicación de la impresora:** A text field containing the XSS payload `<script>alert('hola')</script>`.
- Ubicación geográfica:** Three radio button options:
 - ☐ Utilice Grados minutos segundos (DMS, en inglés). (Ejemplo: 37° 24' 58"N 122° 8' 41"W)
 - ☐ Utilice Grados decimales. (Ejemplo: 37.416111, -122.144722)
 - ☒ No conozco mi ubicación geográfica.

At the bottom of the configuration area are two buttons: 'Aplicar' and 'Cancelar'. Below the buttons is a link: 'Recolección y uso de datos por EWS'. At the very bottom is the copyright notice: '© Copyright 2003, 2004-2013 Hewlett-Packard Development Company, L.P.'

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
RkxBR3s5OTRkMDZmNzE5YmI4ZGY0YjI5OTMyOWI5OGI5YWVhYX0K
root@web:~# _
```

Tenemos una flag:

Decode from Base64 format

Simply enter your data then push the decode button.

RkxBR3s5OTRkMDZmNzE5YmI4ZGY0YjI5OTMyOWI5OGI5YWVhYX0K

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{994d06f719bb8dfb47d47b77b7aeda}

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/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
RkxBR3sxMGVlNDM3YTl3NWNmZjFjMDNkZWQ5OGYyMjUyYjZhNX0K
$
```


Lo decodificamos:

Decode from Base64 format


Simply enter your data then push the decode button.

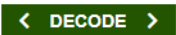

```
RkxBR3sxMGVLNDM3YTI3NWNmZjFjMDNkZWQ5OGYyMjUyYjZhNX0K
```

 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}
```