## FORGOTTEN PORTAL



Realizamos escaneo nmap, detectamos el puerto 22 y 80 abiertos.

Realizando un escaneo con dirb con el diccionario por defecto nos devuelve las siguientes urls. Siendo la de access\_log interesante.

En el contenido de access log encontramos lo que indica ser la clave codificada, vamos a comprobar lo que es realmente.

```
Exploit-DB Google Hacking DB  base64 | GTFOBins  Online - Reverse Shell ... Path Hijacking y Libr

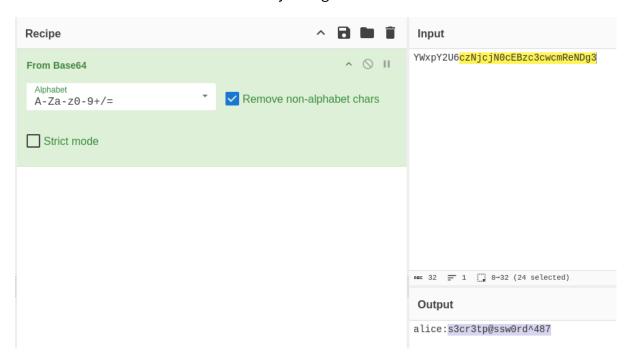
# --- Access Log ---
# Fecha: 2023-11-22
# Descripciùn: Registro de actividad inusual detectada en el sistema.
# Este archivo contiene eventos recientes capturados por el servidor web.

[2023-11-21 18:42:01] INFO: Usuario 'www-data' accedió 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: Sincronización 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: YwxpY2U6czNjcjNOcEBzc3cwcmReNDg3
[2023-11-21 19:56:00] 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 ---
```

Por lo visto está codificado en base64 y es login de la usuaria alice.



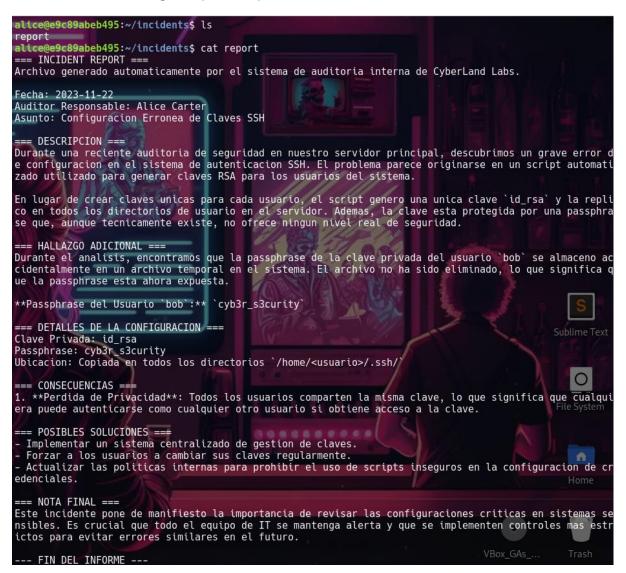
Accedemos mediante ssh con la usuaria alice la cual no está dentro del grupo sudoers.



En su directorio encontramos la flag.

```
alice@e9c89abeb495:~$ cat user.txt
```

Dentro del mismo directorio de alice, en la carpeta incidents, encontramos un reporte en el cual tenemos alguna que otra pista.



Si leemos detenidamente lo que pone en la nota anterior, vemos que todos los usuarios tienen la misma clave privada y que en caso del usuario bob tambíen se filtró la passphrase. Es por ello que vamos a ver la clave privada de la usuaria alice, copiarla y después de cambiarle los permisos vamos a probar a loguearnos con el usuario bob.

```
total 12
drwxrwxr-x 2 kali kali 4096 Dec 10 14:23 .
drwx----- 48 kali kali 4096 Dec 10 14:23 .
-rw-rw-r-- 1 kali kali 444 Dec 10 14:23 id_rsa

(kali@ kali) - [~/forgotten_portal]
$ chmod 600 id_rsa

(kali@ kali) - [~/forgotten_portal]
$ ls la
total 12
drwxrwxr-x 2 kali kali 4096 Dec 10 14:23 .
drwx----- 48 kali kali 4096 Dec 10 14:23 .
-rw----- 1 kali kali 444 Dec 10 14:23 id_rsa
```



Una vez conseguimos el acceso de bob comprobamos si se puede ejecutar algo como sudo. En este caso se puede ejecutar el comando tar

```
bob@e9c89abeb495:~$ sudo -l
Matching Defaults entries for bob on e9c89abeb495:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/snap/bin, use_pty

User bob may run the following commands on e9c89abeb495:
    (ALL) NOPASSWD: /bin/tar
```

Ahora, como siempre en estos casos, nos dirigimos a la página <a href="https://gtfobins.github.io/gtfobins/tar/#sudo">https://gtfobins.github.io/gtfobins/tar/#sudo</a> donde podemos ver o guiarnos que comandos utilizar para aprovechar este privilegio mal configurado para lograr la escalada a root y obtener la deseada flag.

