

Informe de Penetración: Máquina Fawn (HTB)

Lucas JPG

8 de octubre de 2025



Índice

1	Resumen Ejecutivo	3
1.1	Objetivos	3
1.2	Hallazgos	3
1.3	Consecuencias	3
2	Informe técnico	3
3	Alcance y Metodología	3
3.1	Iniciando la máquina vulnerable	3
4	Etapas de escaneo	4
4.1	Ping a la máquina vulnerable	4
4.2	Escaneo con NMAP	6
5	Acceso a la máquina vulnerable	8
5.1	Flag.txt	9
5.2	Descargamos la bandera con get y salimos del servidor ftp	10
5.3	Detalle de Hallazgos	10
6	Conclusiones	12
7	Recomendaciones	12
8	Respuesta a preguntas en HTB	12

1. Resumen Ejecutivo

1.1. Objetivos

El presente informe detalla los hallazgos de la evaluación de vulnerabilidades realizada sobre la infraestructura del sistema. El hallazgo crítico fue la exposición de servicios de administración remota inseguros en el sistema con IP 10.129.175.105, lo cual permitió la obtención de credenciales y acceso privilegiado al sistema.

1.2. Hallazgos

El riesgo es **ALTO**, ya que la información sensible, incluyendo las credenciales, fue transmitida sin cifrar. La recomendación urgente es deshabilitar Telnet y migrar a SSH.

1.3. Consecuencias

Permite el acceso total al sistema con un usuario con permisos de administrador, lo cual permite que ciberdelincuentes violen la integridad, disponibilidad y confidencialidad del sistema.

2. Informe técnico

Empezamos conectándonos a la VPN de HTB, con el fin de poder acceder a sus máquinas virtuales.

3. Alcance y Metodología

3.1. Iniciando la máquina vulnerable

Al iniciar la máquina vulnerable, nos darán una IP, en la cual trabajaremos.

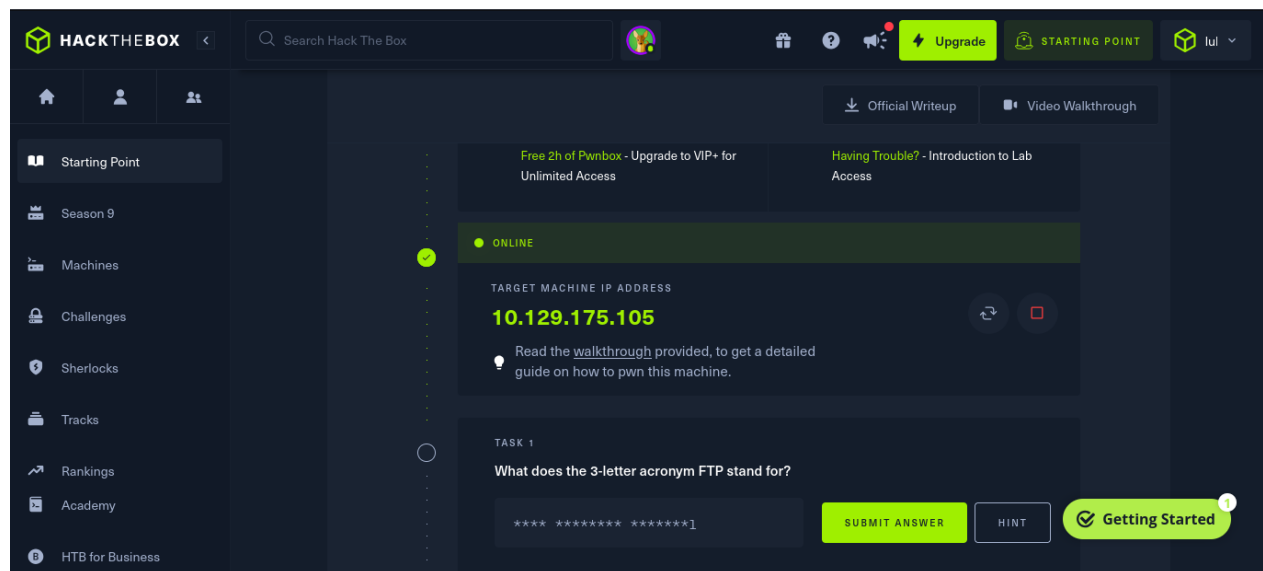


Figura 1: Dirección IP de la máquina objetivo

4. Etapa de escaneo

4.1. Ping a la máquina vulnerable

En esta etapa, realizamos un ping con el objetivo de verificar que la máquina vulnerable responde a los paquetes ICMP.

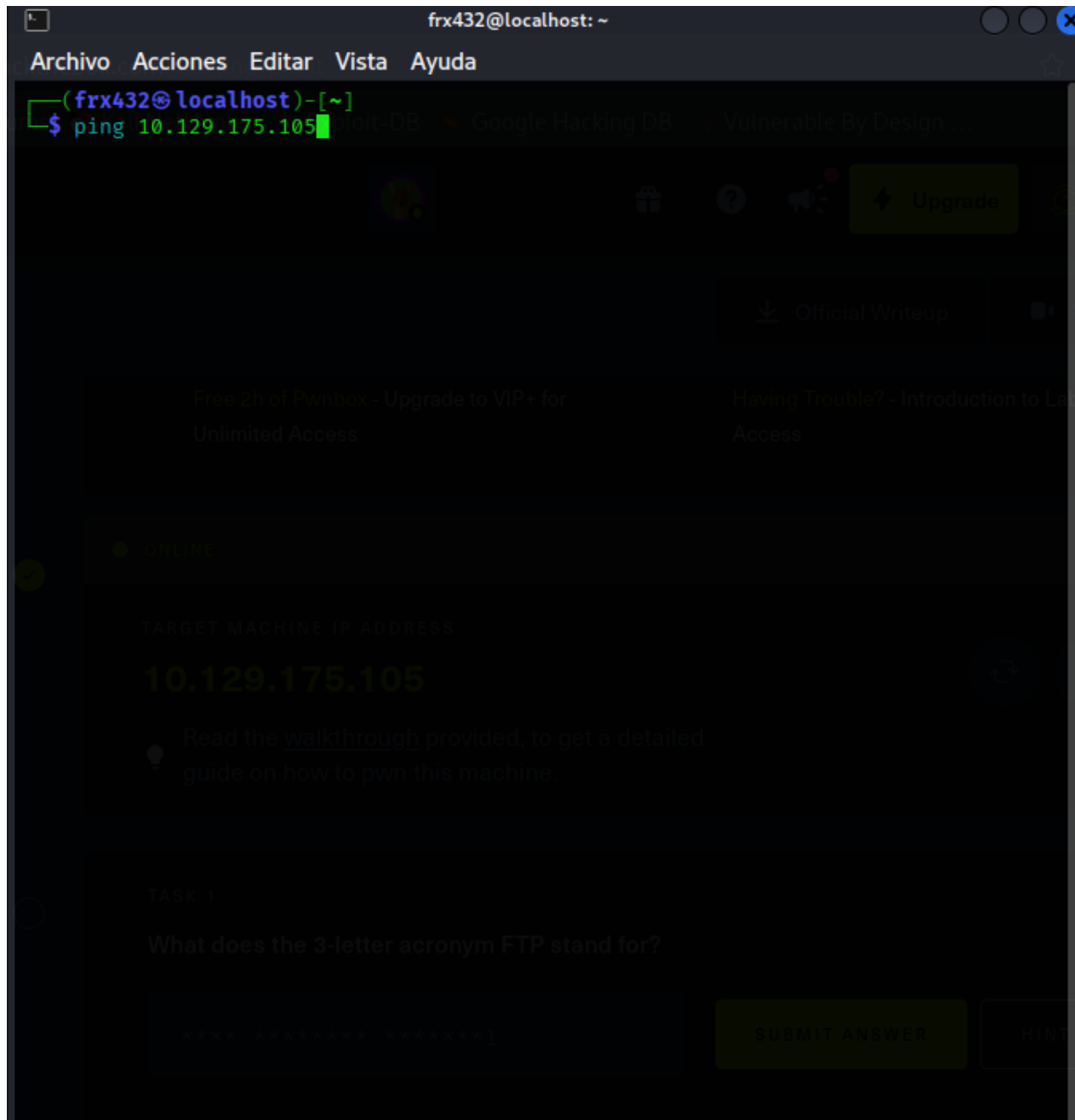
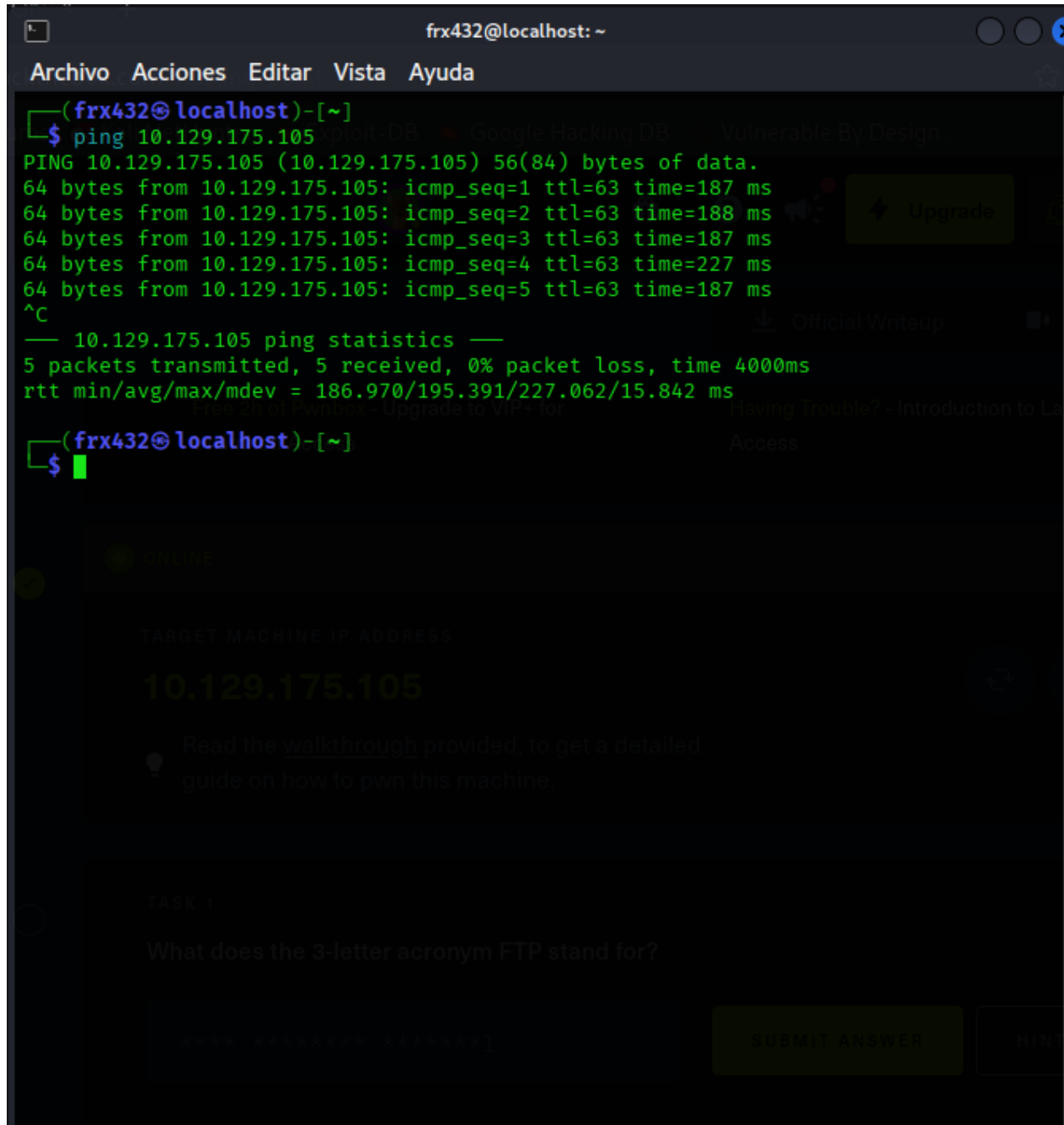


Figura 2: Código usando para enviar paquetes

Como podemos ver en la siguiente captura, la máquina vulnerable recibe y responde a los paquetes ICMP.



The image shows a terminal window with the title 'frx432@localhost: ~'. The terminal output is as follows:

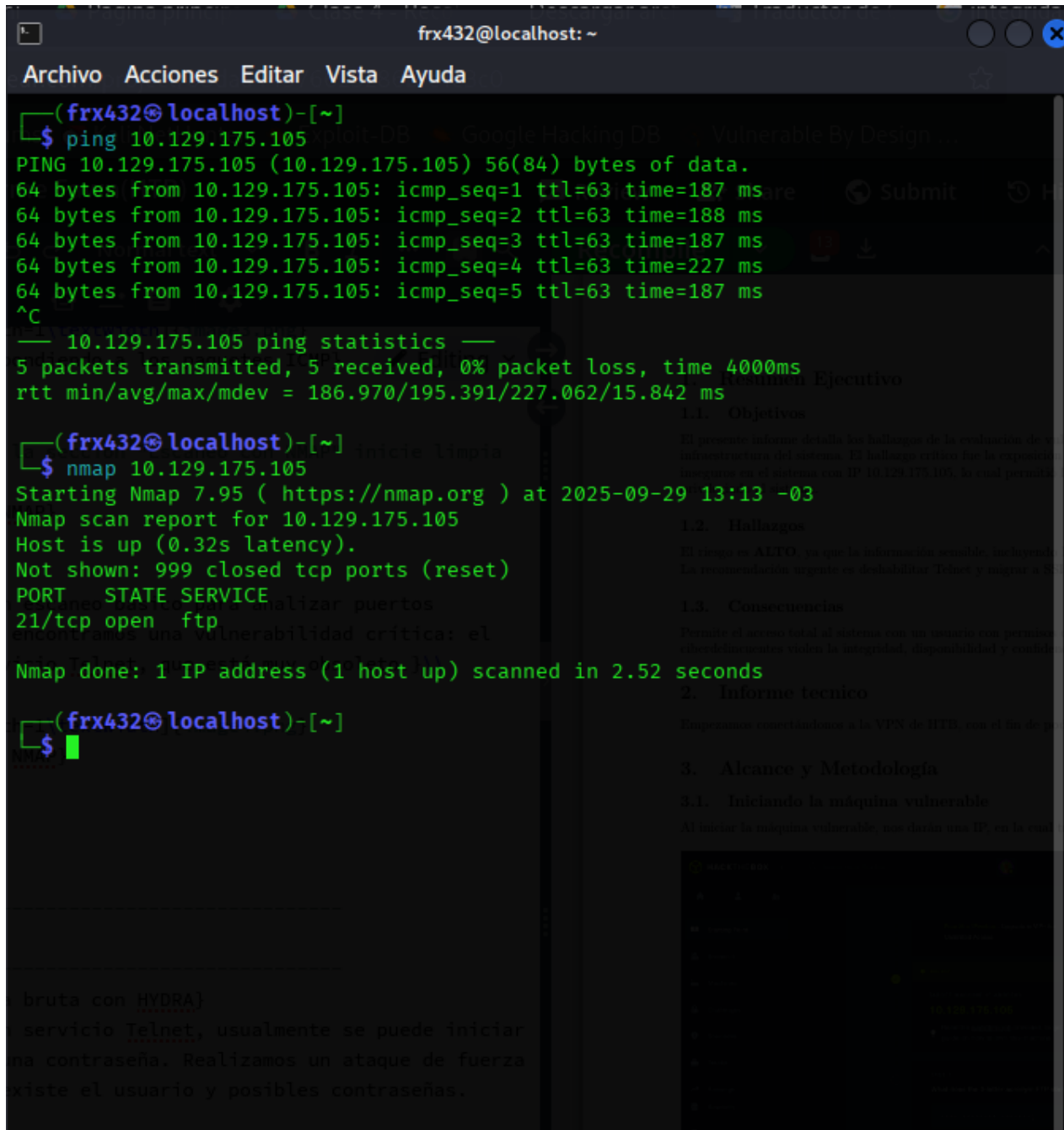
```
(frx432@localhost)-[~]  
$ ping 10.129.175.105  
PING 10.129.175.105 (10.129.175.105) 56(84) bytes of data.  
64 bytes from 10.129.175.105: icmp_seq=1 ttl=63 time=187 ms  
64 bytes from 10.129.175.105: icmp_seq=2 ttl=63 time=188 ms  
64 bytes from 10.129.175.105: icmp_seq=3 ttl=63 time=187 ms  
64 bytes from 10.129.175.105: icmp_seq=4 ttl=63 time=227 ms  
64 bytes from 10.129.175.105: icmp_seq=5 ttl=63 time=187 ms  
^C  
— 10.129.175.105 ping statistics —  
5 packets transmitted, 5 received, 0% packet loss, time 4000ms  
rtt min/avg/max/mdev = 186.970/195.391/227.062/15.842 ms  
(frx432@localhost)-[~]  
$
```

Below the terminal window, there is a web application interface. It features a 'TARGET MACHINE IP ADDRESS' field containing '10.129.175.105'. A lightbulb icon indicates a tip: 'Read the [walkthrough](#) provided, to get a detailed guide on how to pwn this machine.' Under the 'TASK 1' section, the question is 'What does the 3-letter acronym FTP stand for?'. At the bottom right, there are 'SUBMIT ANSWER' and 'HINT' buttons.

Figura 3: Máquina respondiendo a los paquetes ICMP

4.2. Escaneo con NMAP

Realizamos un escaneo básico para analizar puertos abiertos, en el cual encontramos un riesgo, el puerto 21 con el servicio ftp abierto



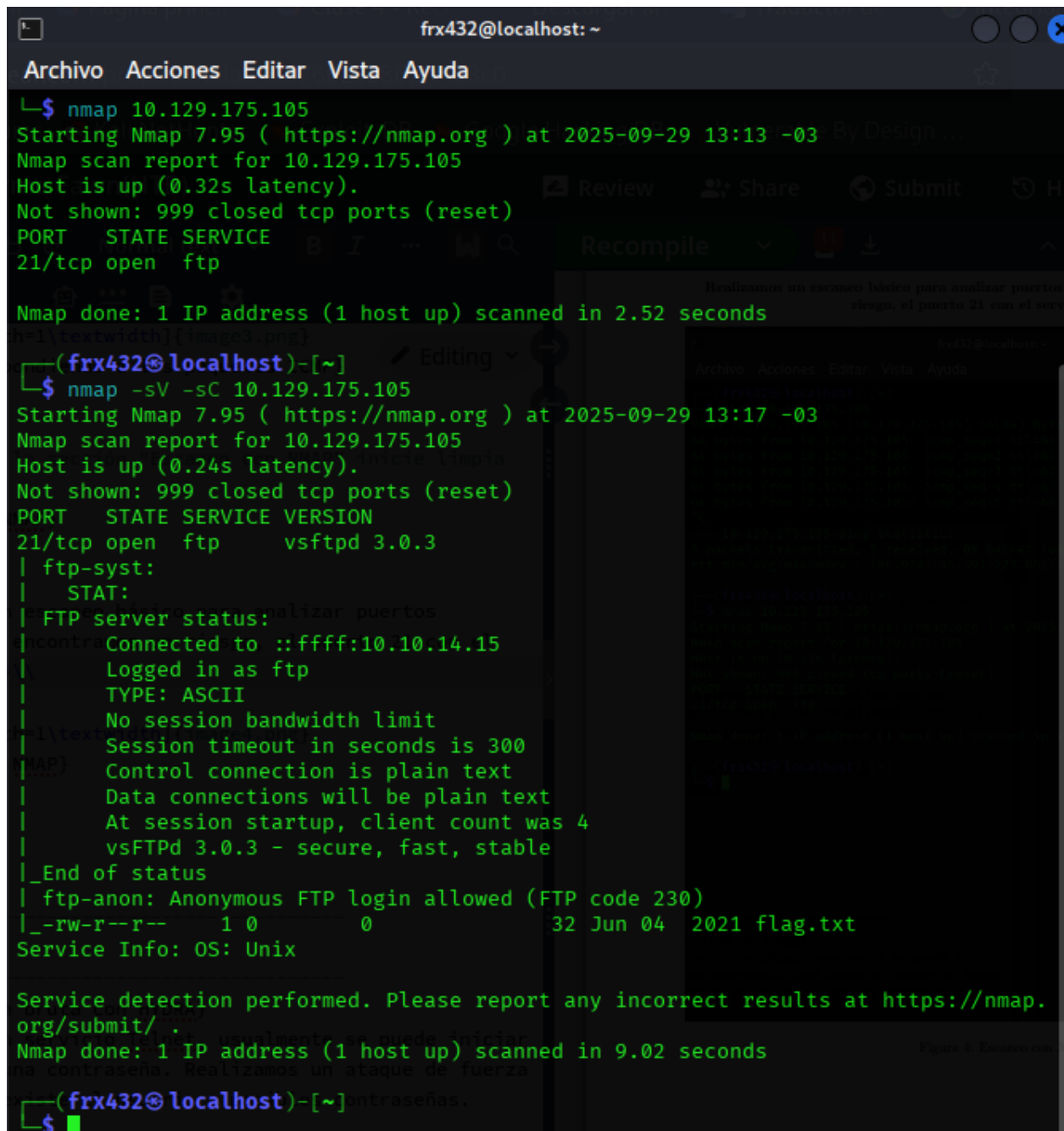
```
(frx432@localhost)-[~]
$ ping 10.129.175.105
PING 10.129.175.105 (10.129.175.105) 56(84) bytes of data:
64 bytes from 10.129.175.105: icmp_seq=1 ttl=63 time=187 ms
64 bytes from 10.129.175.105: icmp_seq=2 ttl=63 time=188 ms
64 bytes from 10.129.175.105: icmp_seq=3 ttl=63 time=187 ms
64 bytes from 10.129.175.105: icmp_seq=4 ttl=63 time=227 ms
64 bytes from 10.129.175.105: icmp_seq=5 ttl=63 time=187 ms
^C
— 10.129.175.105 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 186.970/195.391/227.062/15.842 ms

(frx432@localhost)-[~]
$ nmap 10.129.175.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-29 13:13 -03
Nmap scan report for 10.129.175.105
Host is up (0.32s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
Nmap done: 1 IP address (1 host up) scanned in 2.52 seconds

(frx432@localhost)-[~]
$
```

Figura 4: Escaneo con NMAP

Como podemos ver en la siguiente captura, Usando los parámetros como "sC" y "sV" en nmap, logramos obtener información sobre la versión del servicio y una mala configuración, permitiendo el acceso anónimo.

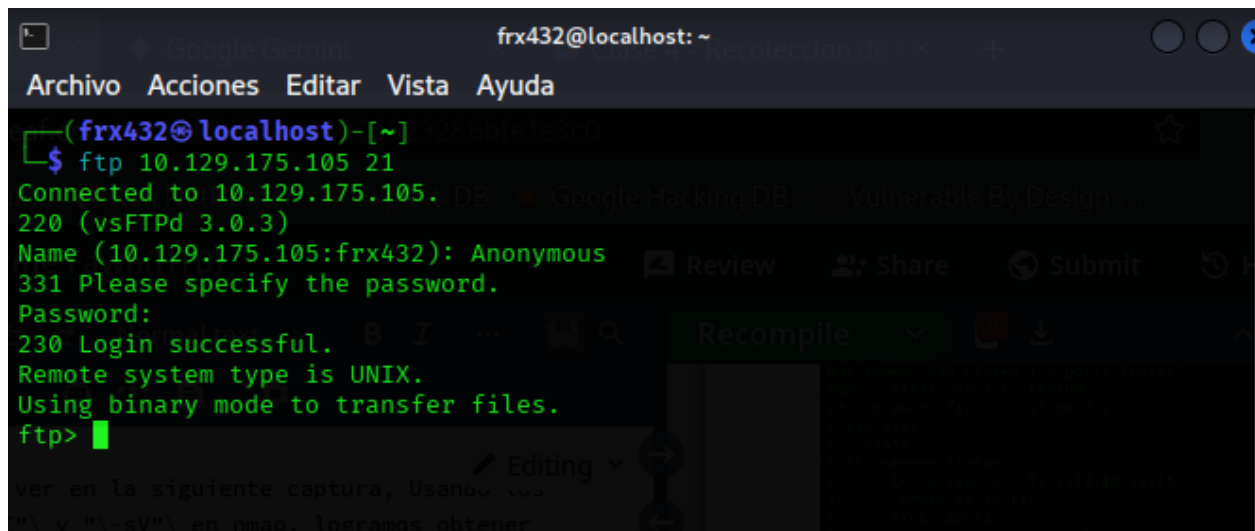


```
frx432@localhost: ~  
Archivo Acciones Editar Vista Ayuda  
$ nmap 10.129.175.105  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-29 13:13 -03  
Nmap scan report for 10.129.175.105  
Host is up (0.32s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
Nmap done: 1 IP address (1 host up) scanned in 2.52 seconds  
  
(frx432@localhost)-[~]  
$ nmap -sV -sC 10.129.175.105  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-29 13:17 -03  
Nmap scan report for 10.129.175.105  
Host is up (0.24s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp      vsftpd 3.0.3  
| ftp-syst:  
|   STAT:  
| FTP server status:  
| Connected to ::ffff:10.10.14.15  
| Logged in as ftp  
|   TYPE: ASCII  
| No session bandwidth limit  
| Session timeout in seconds is 300  
| Control connection is plain text  
| Data connections will be plain text  
| At session startup, client count was 4  
| vsFTPD 3.0.3 - secure, fast, stable  
|_End of status  
| ftp-anon: Anonymous FTP login allowed (FTP code 230)  
|_-rw-r--r--  1 0      0      32 Jun 04  2021 flag.txt  
Service Info: OS: Unix  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 9.02 seconds  
  
(frx432@localhost)-[~]  
$
```

Figura 5: Acceso anonimo

5. Acceso a la máquina vulnerable

Accedemos a la máquina a través del servicio ftp, usando el siguiente comando: `ftp <IP><puerto>`, como usuario `Anonymous`.

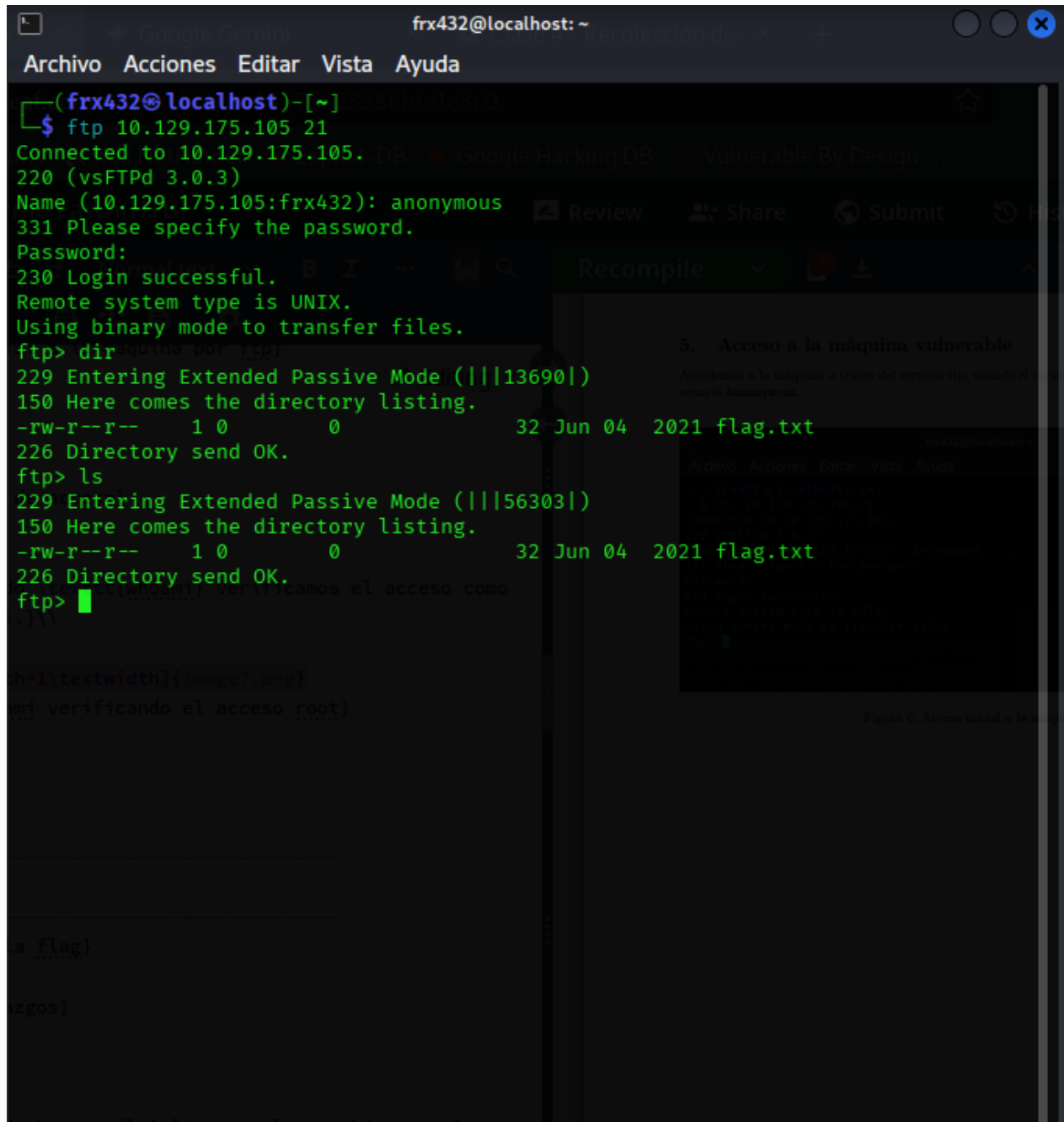


```
frx432@localhost: ~  
Archivo Acciones Editar Vista Ayuda  
(frx432@localhost)-[~]  
$ ftp 10.129.175.105 21  
Connected to 10.129.175.105. DB: Google Hacking DB Vulnerable By Design  
220 (vsFTPd 3.0.3)  
Name (10.129.175.105:frx432): Anonymous  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp>
```

Figura 6: Acceso inicial a la máquina por ftp

5.1. Flag.txt

Con el comando `ls` o `dir` buscamos la bandera `flag.txt`.

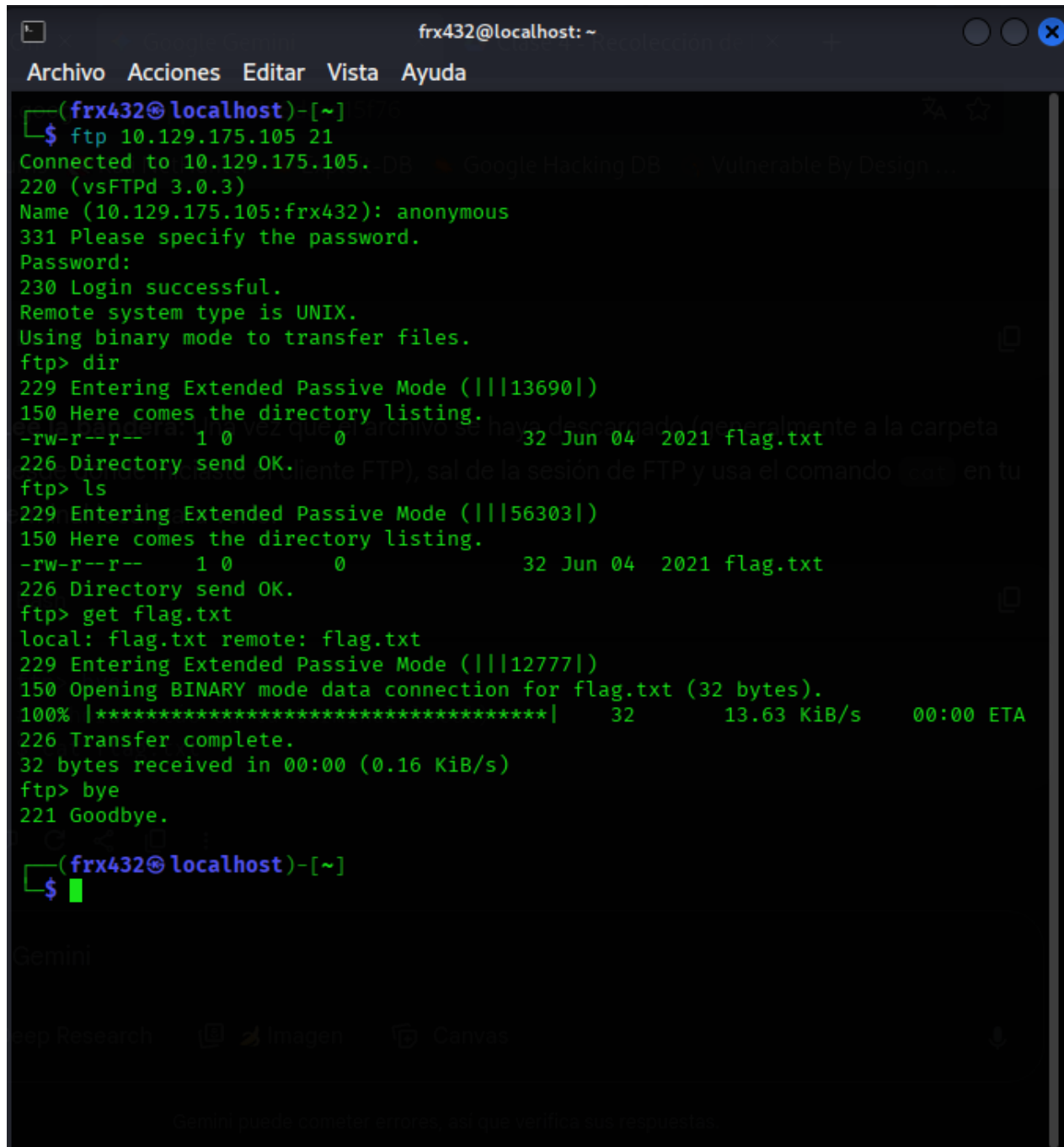


```
(frx432@localhost)-[~]
$ ftp 10.129.175.105 21
Connected to 10.129.175.105. DB
220 (vsFTPD 3.0.3)
Name (10.129.175.105:frx432): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||13690|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 32 Jun 04 2021 flag.txt
226 Directory send OK.
ftp> ls
229 Entering Extended Passive Mode (|||56303|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 32 Jun 04 2021 flag.txt
226 Directory send OK.
ftp>
```

Figura 7: Comando `ls` para buscar la flag

5.2. Descargamos la bandera con get y salimos del servidor ftp

Con el comando bye salimos del servidor ftp.

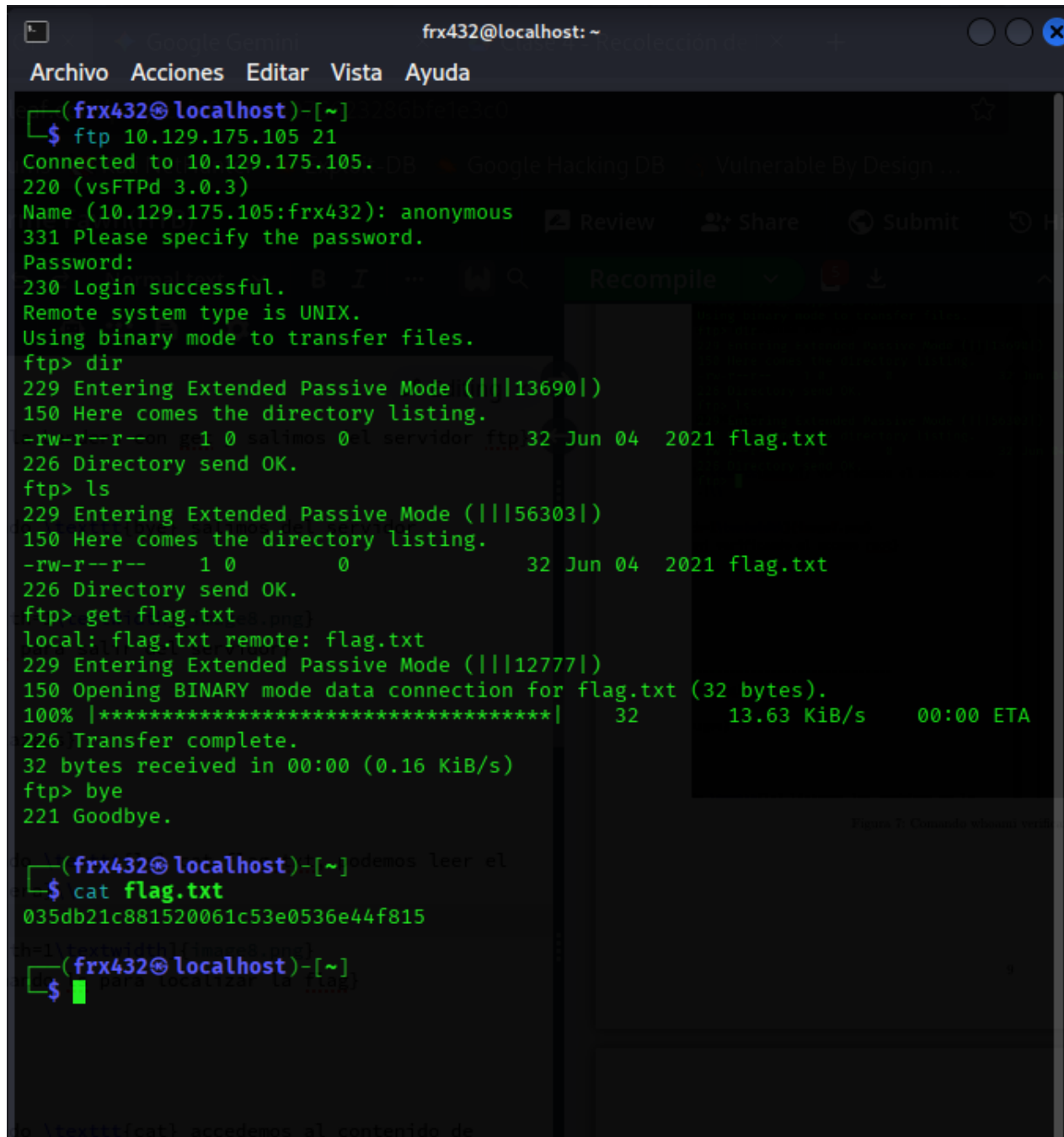


```
(frx432@localhost)-[~]
$ ftp 10.129.175.105 21
Connected to 10.129.175.105. DB - Google Hacking DB - Vulnerable By Design
220 (vsFTPd 3.0.3)
Name (10.129.175.105:frx432): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||13690|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 32 Jun 04 2021 flag.txt
226 Directory send OK.
ftp> ls
229 Entering Extended Passive Mode (|||56303|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 32 Jun 04 2021 flag.txt
226 Directory send OK.
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||12777|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% |*****| 32 13.63 KiB/s 00:00 ETA
226 Transfer complete.
32 bytes received in 00:00 (0.16 KiB/s)
ftp> bye
221 Goodbye.
(frx432@localhost)-[~]
$
```

Figura 8: Comando bye para salir del servidor

5.3. Detalle de Hallazgos

Con el comando `ls cat flag.txt`, podemos leer el contenido de la bandera

A screenshot of a terminal window with a dark background. The window title is 'frx432@localhost: ~'. The terminal shows an FTP session starting with 'ftp 10.129.175.105 21'. It connects to the server, prompts for a password, and logs in successfully. The user then runs 'dir' and 'ls' to list files, both showing 'flag.txt'. Next, the user runs 'get flag.txt', which downloads the file. Finally, the user runs 'cat flag.txt' at the shell prompt, displaying a long alphanumeric string: '035db21c881520061c53e0536e44f815'.

```
(frx432@localhost)-[~]  
$ ftp 10.129.175.105 21  
Connected to 10.129.175.105.  
220 (vsFTPD 3.0.3)  
Name (10.129.175.105:frx432): anonymous  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> dir  
229 Entering Extended Passive Mode (|||13690|)  
150 Here comes the directory listing.  
-rw-r--r--  1 0          0          32 Jun 04  2021 flag.txt  
226 Directory send OK.  
ftp> ls  
229 Entering Extended Passive Mode (|||56303|)  
150 Here comes the directory listing.  
-rw-r--r--  1 0          0          32 Jun 04  2021 flag.txt  
226 Directory send OK.  
ftp> get flag.txt  
local: flag.txt remote: flag.txt  
229 Entering Extended Passive Mode (|||12777|)  
150 Opening BINARY mode data connection for flag.txt (32 bytes).  
100% |*****| 32 13.63 KiB/s 00:00 ETA  
226 Transfer complete.  
32 bytes received in 00:00 (0.16 KiB/s)  
ftp> bye  
221 Goodbye.  
  
(frx432@localhost)-[~]  
$ cat flag.txt  
035db21c881520061c53e0536e44f815  
  
(frx432@localhost)-[~]  
$
```

Figura 9: Contenido de la bandera

6. Conclusiones

Se encontró el servicio Telnet, el cual es una ****vulnerabilidad crítica**** ya que no cifra la información, haciéndolo muy inseguro. Esto permitió que atacantes accedan a la información sin dificultad, con el riesgo de obtener acceso al sistema como usuario `root`.

7. Recomendaciones

1. Deshabilitar Telnet: Eliminar o deshabilitar completamente el servicio Telnet.
2. Migración a SSH: Migrar del servicio Telnet al servicio SSH (Secure Shell), el cual es más moderno y más seguro al cifrar la información de la conexión, incluyendo las credenciales.

8. Respuesta a preguntas en HTB

¿Qué significa la sigla de tres letras FTP?

Respuesta=File Transfer Protocol

¿En qué puerto suele escuchar el servicio FTP?

Respuesta=21

FTP envía datos sin cifrar, sin ningún tipo de encriptación. ¿Qué acrónimo se utiliza para un protocolo posterior diseñado para proporcionar una funcionalidad similar a la del FTP, pero de forma segura, como una extensión del protocolo SSH?

Respuesta=sftp

¿Cuál es el comando que podemos usar para enviar una solicitud de eco ICMP para probar nuestra conexión con el destino?

Respuesta=ping

Según tus análisis, ¿qué versión de FTP se está ejecutando en el objetivo?

Respuesta=vsftpd 3.0.3

Según tus análisis, ¿qué tipo de sistema operativo se está ejecutando en el objetivo?

Respuesta=unix

¿Cuál es el comando que debemos ejecutar para mostrar el menú de ayuda del cliente «ftp»?

Respuesta=ftp -?

¿Cuál es el nombre de usuario que se utiliza en FTP cuando se desea iniciar sesión sin tener una cuenta?

Respuesta=anonymous

¿Cuál es el código de respuesta que obtenemos para el mensaje FTP «Inicio de sesión correcto»?

Respuesta=230

Hay un par de comandos que podemos usar para listar los archivos y directorios disponibles en el servidor FTP. Uno es `dir`. ¿Cuál es el otro que se usa comúnmente para listar archivos en un sistema Linux?

Respuesta=ls

¿Cuál es el comando que se utiliza para descargar el archivo que encontramos en el servidor FTP?

Respuesta=get

Enviar bandera raíz

Respuesta=035db21c881520061c53e0536e44f815