

## Awkward Setup Guide

1. Spin up EC2 instance
  - Spin up an Ubuntu 20.04 LTS free tier instance
  - Make sure when creating the security group to allow TCP traffic on ports 20-21, 22, and 10000-10100 from anywhere (0.0.0.0/0)
2. (Mis)Configure ssh
  - `sudo vim /etc/ssh/sshd_config`
  - Make sure the following are set:
    - i. `PasswordAuthentication` yes
    - ii. `PermitRootLogin` no
  - You may need to disable configurations for ssh keys depending on how you set the server up. We want the contestants to be able to ssh into the machine without a key. If you do this, make sure to change the root and ubuntu user passwords before disabling this configuration so you don't lock yourself out.
3. Set up ftp
  - `sudo apt install vsftpd -y`
  - `sudo systemctl status vsftpd.service` (should be running now)
  - `sudo vim /etc/vsftpd.conf`
  - Add the following lines:
    - i. `anonymous_enable=YES` (this line may already be there, change it from no to yes if it is)
    - ii. `allow_writeable_chroot=YES`
    - iii. `pasv_enabled=YES`
    - iv. `pasv_min_port=10000`
    - v. `pasv_max_port=10100`
  - The ftp server should now be running and users should be able to connect to it using an anonymous user. They will be grabbing files from this ftp server to gain a foothold.
4. Plant some files
  - `cd /srv/ftp`
  - Make the following text files with their respective content:
    - i. `flag.txt` > lol you thought, nice try
    - ii. `test.txt` > just enable anonymous login, whats the worst that can happen?
    - iii. `ftp.txt` > `ftp-user: 67FCA05E075DA1306FA5B5D5191C2AF50E0251EB`
  - The other two files are there for fun but the ftp.txt file will contain a SHA-1 hash of the ftp-user's password which you will be creating shortly. Contestants will use this username and password to ssh into the machine as a user with limited privileges.
5. Create ftp-user
  - `sudo adduser ftp-user`
  - Password will be `letsgodude`
  - Make sure this user has no special privileges
  - Give this user sudo access to `awk`

- sudo visudo
  - Add the following line under # User privilege specification
    - i. ftp-user ALL=(root) /usr/bin/awk
  - This will allow the contestant to abuse the awk binary to spawn a root shell (hence the name Awkward)
6. Plant the flag
- Make a text file in the /root directory called flag.txt
  - byuctf{pls\_d1s@bl3\_an0nym0us\_ftp}

Once you complete this make sure to test everything on your kali box and confirm that a contestant can root the machine. I think I got everything in this walkthrough but if you have any questions let me know, I should be available most of the day you set this up.