Guides followed:

- 1.https://linux.die.net/man/8/dropbear
- 2.https://www.digitalocean.com/community/tutorials/how-to-set-up-ssh-keys-on-ubuntu-1804
- 3.https://linuxconfig.org/how-to-install-and-configure-dropbear-on-linux

making the typescript file for read everything on your terminal session.

The script command is part of the util-linux package which can be downloaded from Linux Kernel Archive. First of all you have to install ***colorized-logs*** and then run the ***script***.

```
arash@server:~$ sudo apt install colorized-logs
arash@server:~$ script
script started, file is typescript
```

There's an ansi2txt command in the colorized-logs package on Ubuntu. It removes ANSI color codes nicely, but it doesn't deal with things like progress bars produced by emitting ^H or ^M characters to overwrite text in place. col -b can deal with those, so for best results you can combine the two.

- ***To strip ansi control codes from file typescript and send to typescript_clean:***

```
arash@server:~$ cat typescript | ansi2txt | col -b >>typescript_clean
```

Initial Server Setup with Ubuntu 20.04

When you first create a new Ubuntu 20.04 server, you should perform some important configuration steps as part of the initial setup. These steps will increase the security and usability of your server, and will give you a solid foundation for subsequent actions.

- ***update and Upgrade Your System***

First of all, log in to the Ubuntu 20.04 system via the system terminal. Now, execute the following commands to update apt cache and upgrade all packages on your system.

```
arash@server:~$ sudo apt update
Hit:1 http://se.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://se.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:3 http://se.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Get:4 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
fetched 336 kB in 0s (1.030 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
43 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

```
arash@server:~$ sudo apt upgrade
43 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
97 standard security updates
Need to get 383 MB/458 MB of archives.
After this operation, 25,3 MB of additional disk space will be used.
```

```
Do you want to continue? [Y/n] y
........................
Extracting templates from packages: 100%
Preconfiguring packages ...
0 added, 0 removed; done.
```

- ***Set Up SSH Key***

The first thing we want to do is actully creat the RSA key pair.

```
46704@Lenovo5 MINGW64 ~
$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/c/Users/46704/.ssh/id_rsa):
/c/Users/46704/.ssh/id_rsa already exists.
Overwrite (y/n)? y
```

We have a few things that we need to respons to it will pop up with questions when this one will select the default, so press enter that's a default location. After that, it will prompt to enter a secure passphrase as below. Passphrase will add an additional security layer to your keys. It is optional, if you don’t want to set then you can skip it by just hitting Enter key.

```
Created directory '/home/arash/.ssh'.
Enter passphrase (empty for no passphrase): Enter
Enter same passphrase again: Enter
```

Next, you will see output as following:

```
Your identification has been saved in /c/Users/46704/.ssh/id_rsa
Your public key has been saved in /c/Users/46704/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:LV8P5YMjXwKAnQjciBtCeGwvRo83nxj8fTsajXBW3EY 46704@Lenovo5
The key's randomart image is:
```

```
+---[RSA 3072]----+
|oo o.+ +..  E    |
|o B o + oo o     |
| = B      + o .  |
|  = B    o o +   |
| . o *.oS o * +  |
|    . ++.=.+ * . |
|        o.o.. .  |
|         .o      |
|        .. .     |
+----[SHA256]-----+
46704@Lenovo5 MINGW64 ~
```

Copy the Public Key from client side to server side (Ubuntu Server). The next step is actually copying the public key to the server that you want to connect to, Simple and fast way to copy public is to use ssh-copy-id utility. Run the below command:

```
46704@Lenovo5 MINGW64 ~
$ ssh-copy-id arash@192.168.68.123
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed:
"/c/Users/46704/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out
any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now
it is to install the new keys
```

It's gonna ask you is to login or give you apassword.

```
arash@192.168.68.123's password:
Number of key(s) added: 1
Now try logging into the machine, with:   "ssh 'arash@192.168.68.123'"
and check to make sure that only the key(s) you wanted were added.
```

Now you can try login to your machine and check that only the key(s) added which you want to add.you should be able to login to the remote machine without the remote user’s password. You can try to connect using SSH command:

```
46704@Lenovo5 MINGW64 ~
$ ssh arash@192.168.68.123
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-91-generic x86_64)

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

  System information as of Mon 20 Dec 2021 10:58:35 AM UTC

  System load:  0.0                Processes:               115
  Usage of /:   11.6% of 39.12GB   Users logged in:         1
  Memory usage: 10%                IPv4 address for enp0s3: 192.168.68.123
  Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

0 updates can be applied immediately.


Last login: Mon Dec 20 10:52:05 2021
arash@server:~$
```

If you type ***exit*** you can close the connection to 192.168.68.123 .

```
arash@server:~$ exit
logout
Connection to 192.168.68.123 closed.
```

- ***install and configure Dropbear on Linux***

First i'm going to creat snapshot on Virtual Machine

1. select the VM in the left panel, click the Snapshots button, select Current State, and then click the Take button to take Snapshot, then you have to call this whith some name , for exemple "Before change".

2. if you make a change that breaks the system You roll back to one of your previous snapshots

   The dropbear suite provides both an ssh server and a client application (dbclient), and represents a light alternative to OpenSSH. First we have to escalate to root.

   ```
   arash@server:~$ sudo su
   [sudo] password for arash:
   root@server:/home/arash#
   ```

   Then you simply run apt to install dropbear

   ```
   root@server:/home/arash# apt install dropbear
   ```

   Next, we‘re going to want to configure Dropbear to work to our linkings’. To do so, go ahead and open /etc/default/dropbear with your favorite editor, i am using ***nano*** editor.

   ```
   root@server:/home/arash# nano /etc/default/dropbear
   ```

   Then, go ahead and change the line that says NO_START=1 to NO_START=0 and

   ```
   # disabled because OpenSSH is installed
   # change to NO_START=0 to enable Dropbear
   NO_START=0 #was 1
   # the TCP port that Dropbear listens on
   DROPBEAR_PORT=32445 #was 22
   # specify an optional banner file containing a message to be
   # sent to clients before they connect, such as "/etc/issue.net"
   DROPBEAR_BANNER=""
   ```

   whenever we change a configuration parameter, we need to restart the server.

   ```
   root@server:/home/arash# systemctl restart dropbear
   ```

   Now you can use your custom port: 32445 to login from client side(local shell) to your ubuntu server.

   ```
   46704@Lenovo5 MINGW64 ~
   $ ssh -p 32445 arash@192.168.68.123
   The authenticity of host '[192.168.68.123]:32445 ([192.168.68.123]:32445)'
   can't be established.
   ECDSA key fingerprint is SHA256:kWaRTEEUT+LO17cr8kKKjeGtXyRl29J8b5oJBOQiquw.
   This key is not known by any other names
   Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
   Warning: Permanently added '[192.168.68.123]:32445' (ECDSA) to the list of
   known hosts.
   ```

```
arash@192.168.68.123's password:
arash@server:~$
```