Project Title: *Step-by-Step Guide to Creating a T-Pot Honeypot Using Amazon AWS*

Author: imafidon joseph eromosele

Date: Tuesday 27 may 2025

Table of Contents:

Installing Required Dependencies

- Update and install: Git, Docker, Docker Compose
- Commands:

  ```
  bash
  CopyEdit
  sudo apt update && sudo apt upgrade -y
  sudo apt install git docker.io docker-compose -y
  ```

- *[Insert terminal screenshot]*

Cloning and Installing T-Pot

- Clone GitHub repo:
  `git clone https://github.com/telekom-security/tpotce`
- Navigate to the installer directory:
  `cd tpotce/iso/installer`
- Run installer script:
  `sudo ./install.sh`
- Select installation mode
- *[Insert installation process screenshots]*

Reboot and Initial Login

- Wait for system to reboot
- Login with new credentials
- *[Insert login screen screenshot]*

Accessing the T-Pot Web Interface

- Find public IP of EC2 instance
- Access T-Pot via browser: `https://<public-ip>`
- Login using web credentials
- *[Insert screenshot of dashboard]*

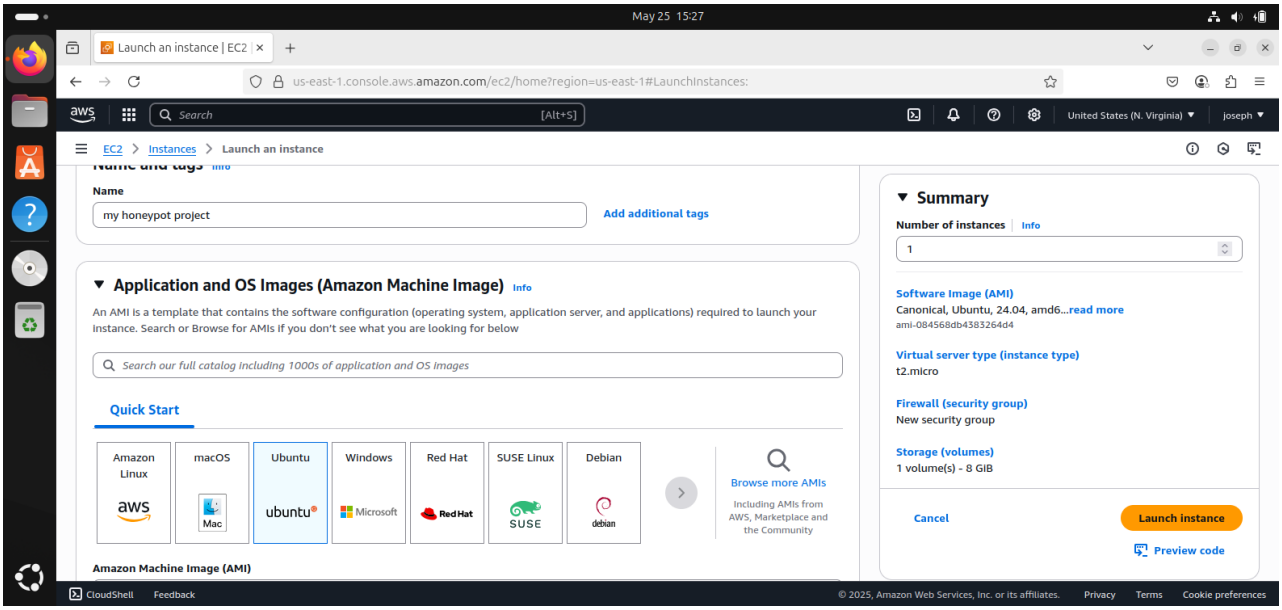
Overview of T-Pot Components

- Kibana: log and traffic visualization
- Suricata: intrusion detection
- Cowrie, Dionaea, etc.
- *[Insert component screenshots]*

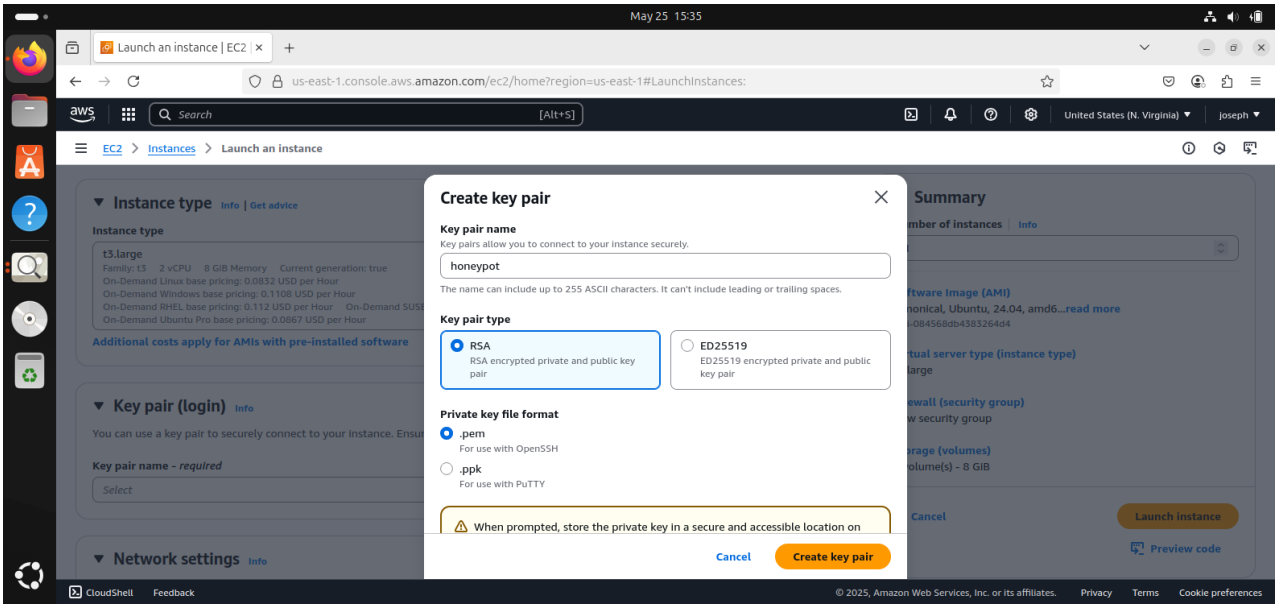
Project purpose:

This outline is structured for easy reading and documentation purposes, ideal for a report, guide, or instructional handout. It includes each major section and what should be covered within it, including screenshots.

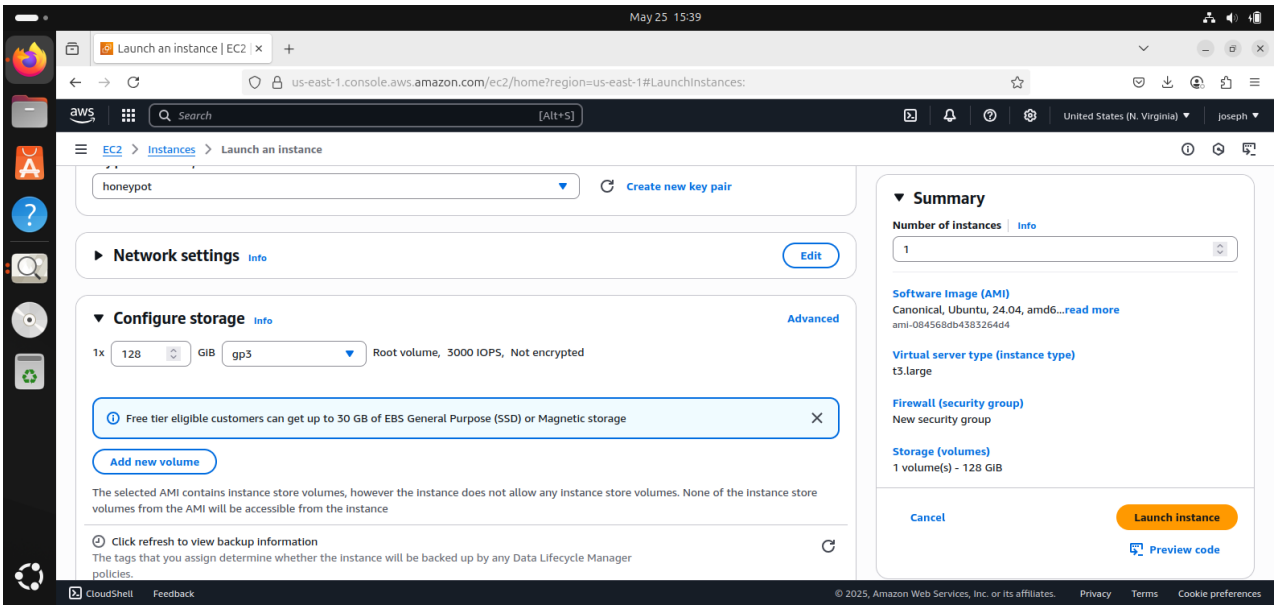
The first step is to have Amazon AWS account, then login and go to EC2 then navigate to instance.



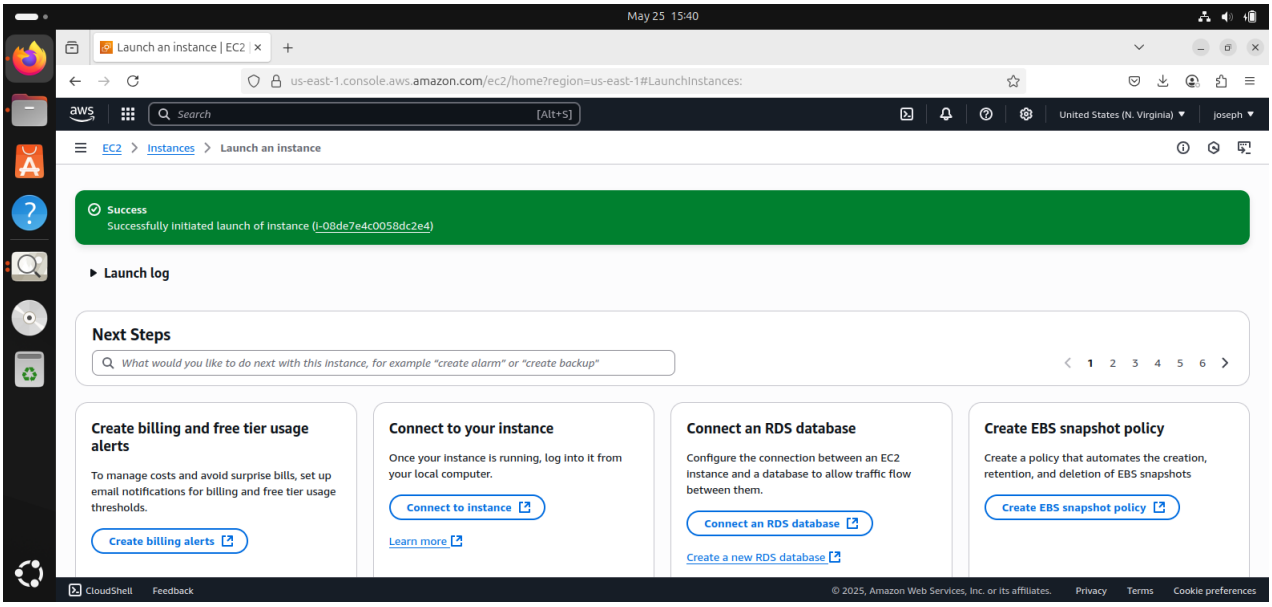
Name your honeypot project, like I did above, then under the quick start option choose Ubuntu.



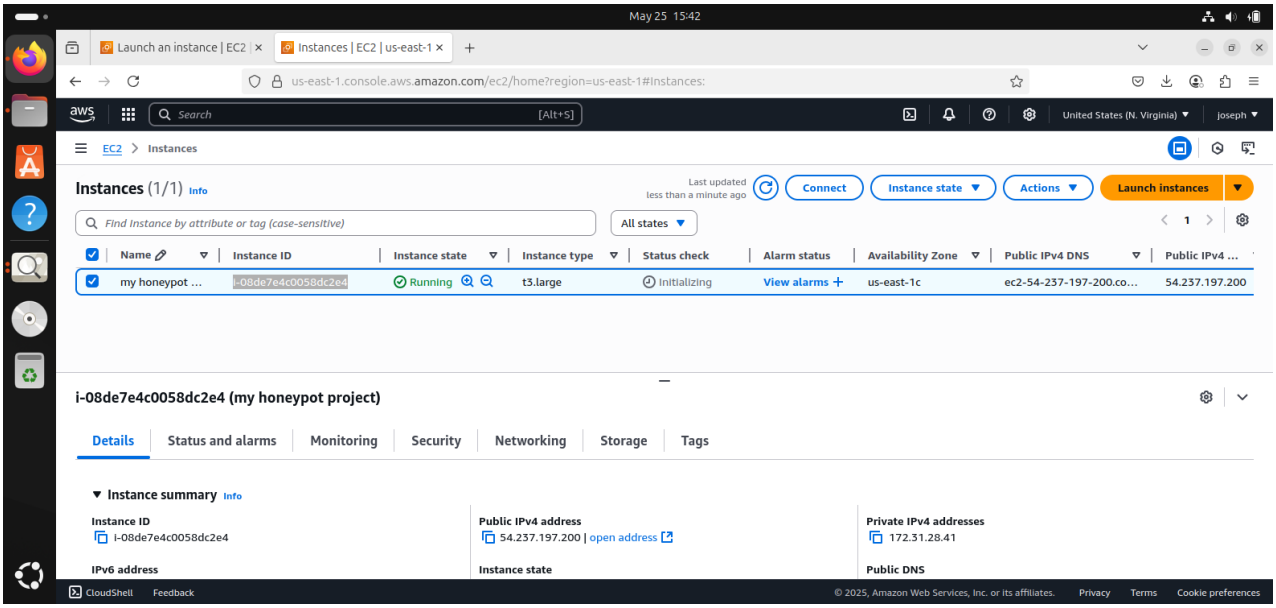
On the instances type choose t3 large, then create a key pair by choosing your preferred key pair name and leave the key pair type in its default (RSA), private key file format should also be in its default (.pem), and then create key pair.



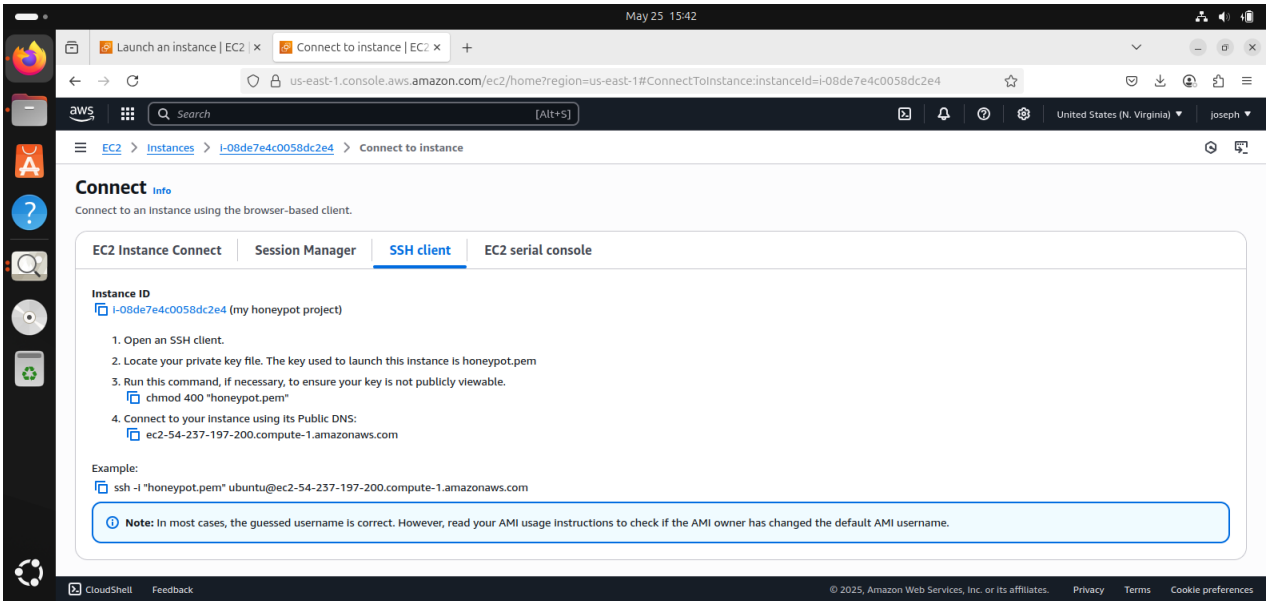
On configuration storage you can choose a storage size of your choice but for the cost of this project I'm using 128gb, then proceed to launch instance.



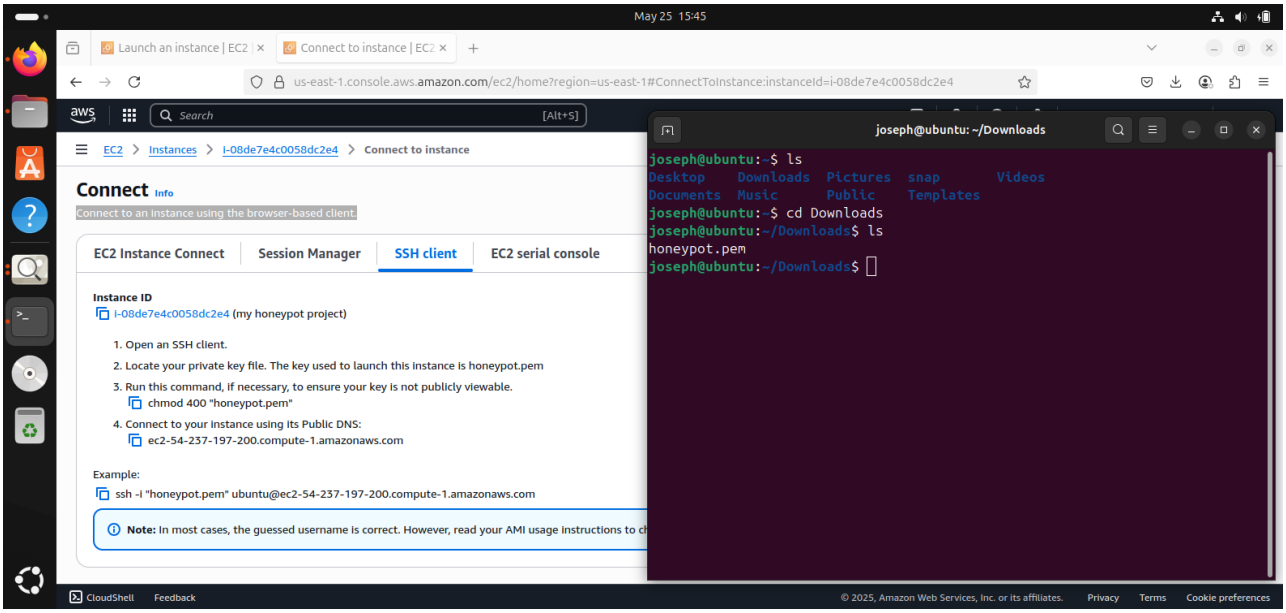
After successfully launching instance, click on the link on the on the instance to take you to the instance dashboard.



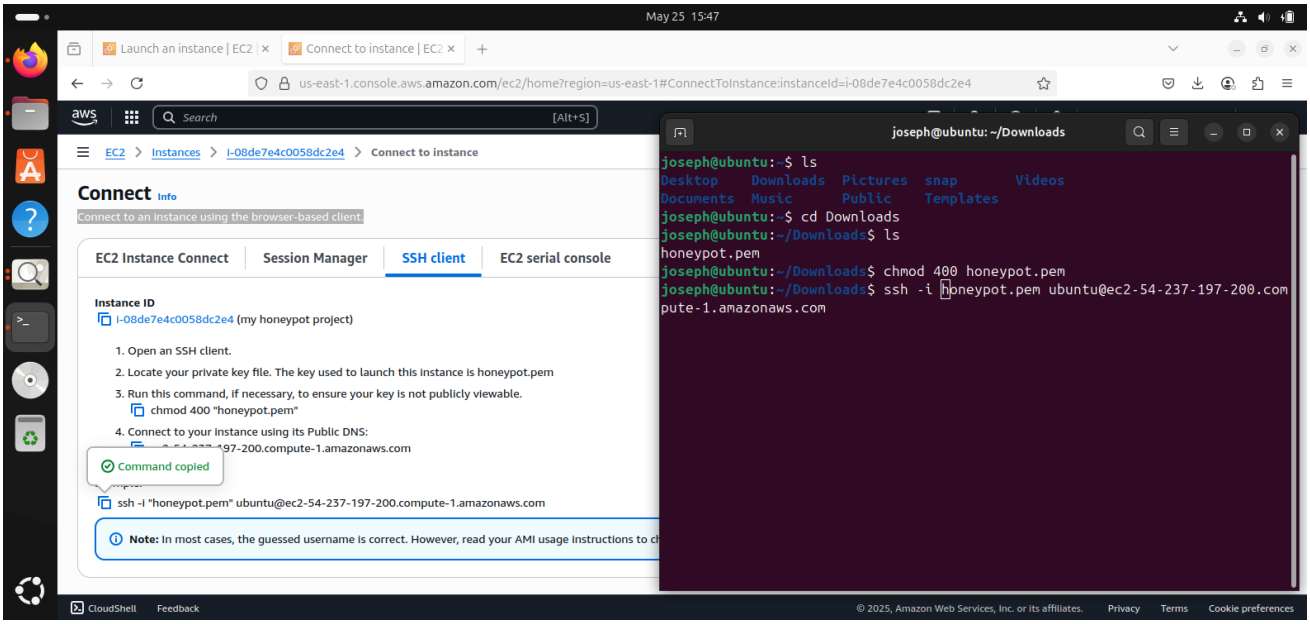
Click on the tick box on the instance and click connect at the top of the instance, you will be directed to a instance connection page.



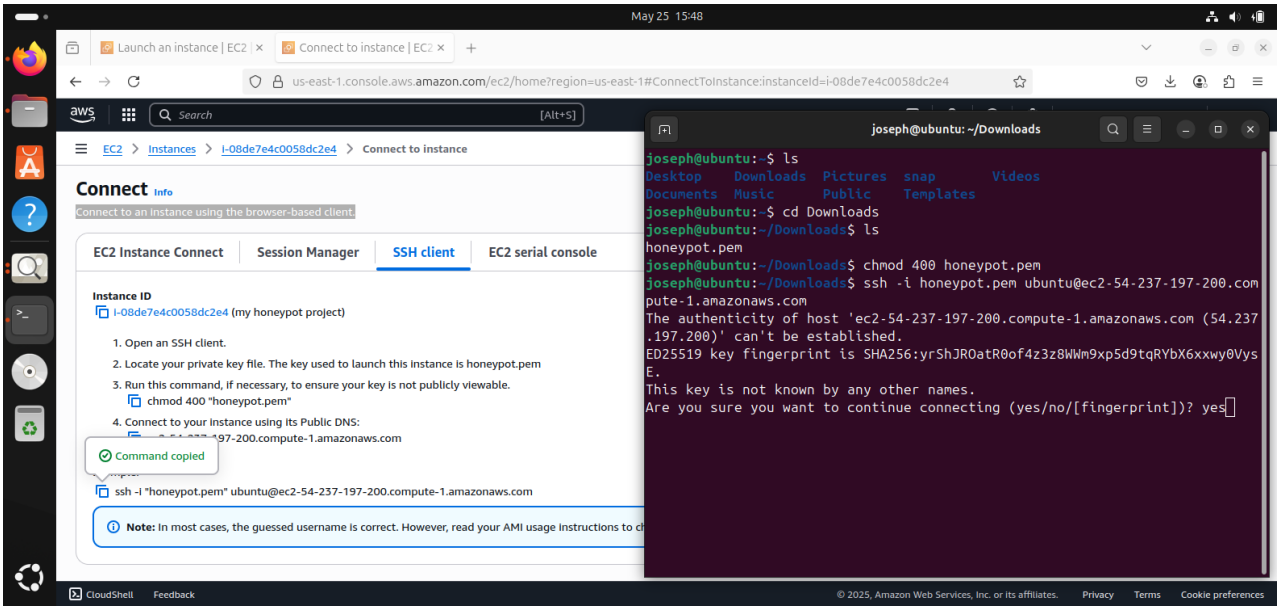
Click on the SSH client and open your terminal to follow the command instructions to connect the instance.



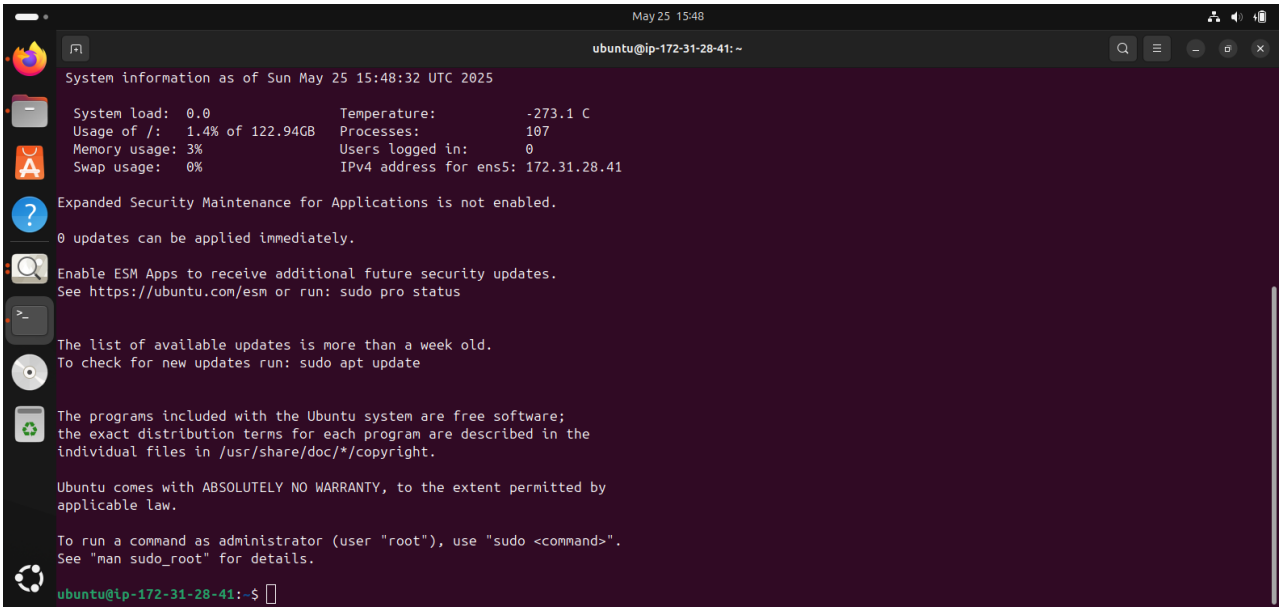
On your terminal change directory to downloads using ‘cd Downloads’, if you list the file inside downloads with ‘ls’ like I did above you will see the key pair you created while setting up the EC2 instance.



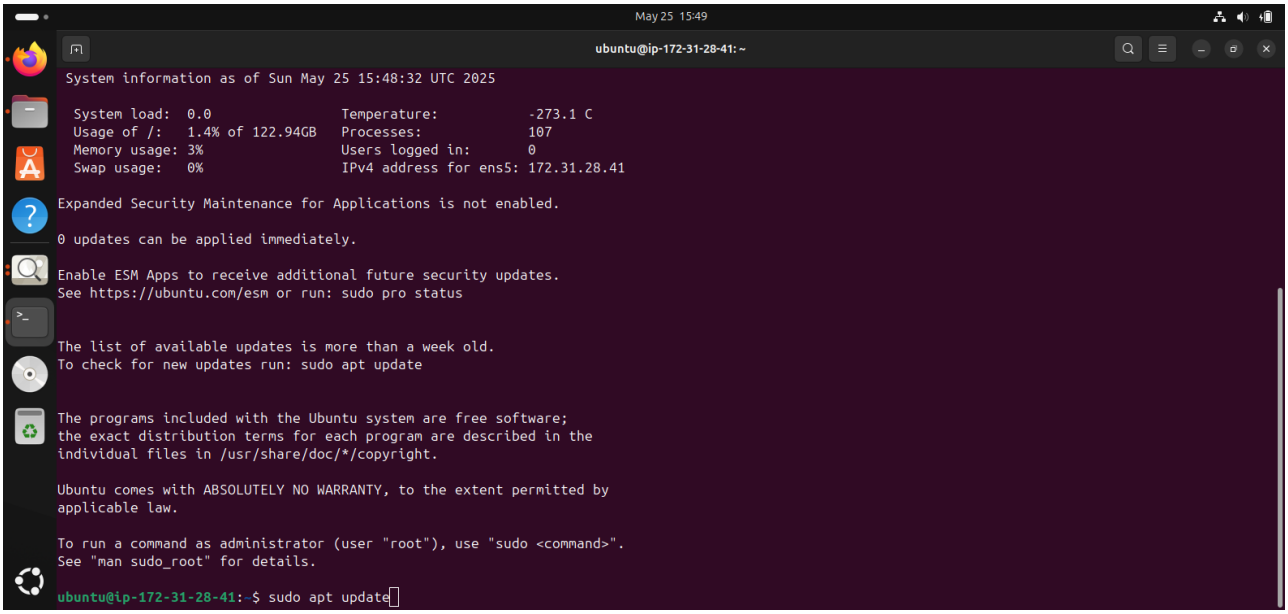
Following the instruction on the SSH client instance connection page put down the command chmod 400 and the key pair name you created, mine is ‘chmod 400 honeypot.pem’ then click enter.



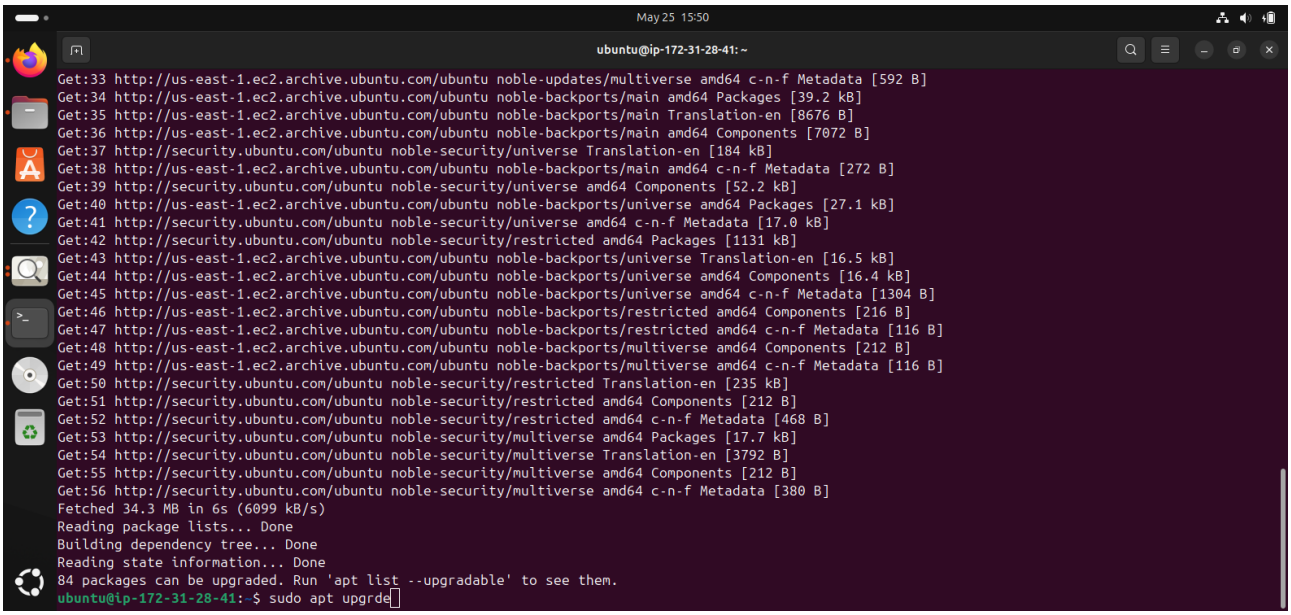
After clicking enter you need to connect to your instance using the 4th command on the SSH instance connection page, copy the command on the page and past it on your terminal and click enter it will ask you to continue connection click ‘y’ to confirm (make sure you remove the quotation mark on the key pair of the command if it’s not in the key pair saved on your file).



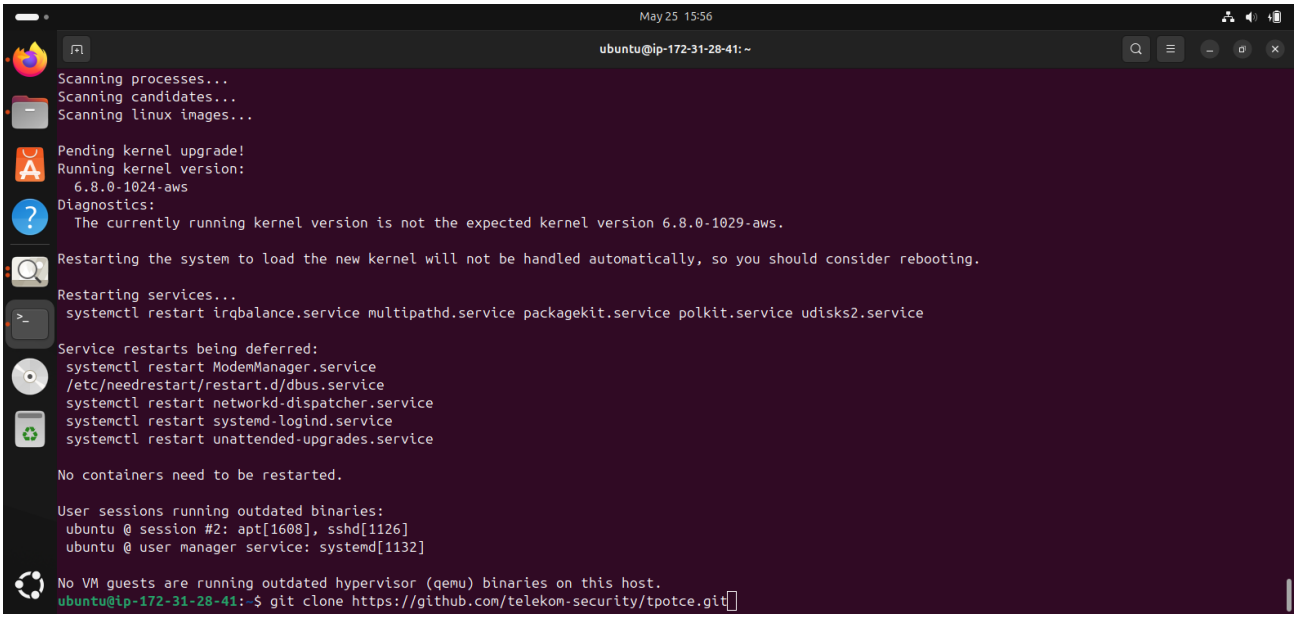
After clicking enter you will notice you will be login to the instance on your terminal just like mine in the picture above.



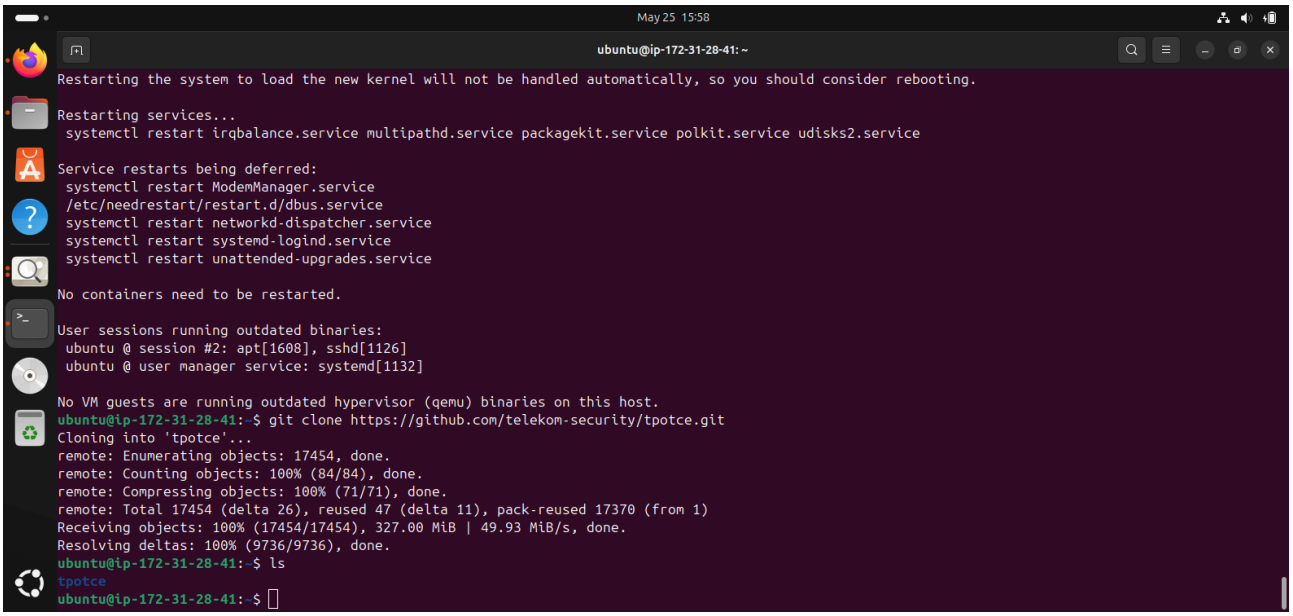
After logging in you need to update the system, to do that you need to run the command sudo apt update then click enter.



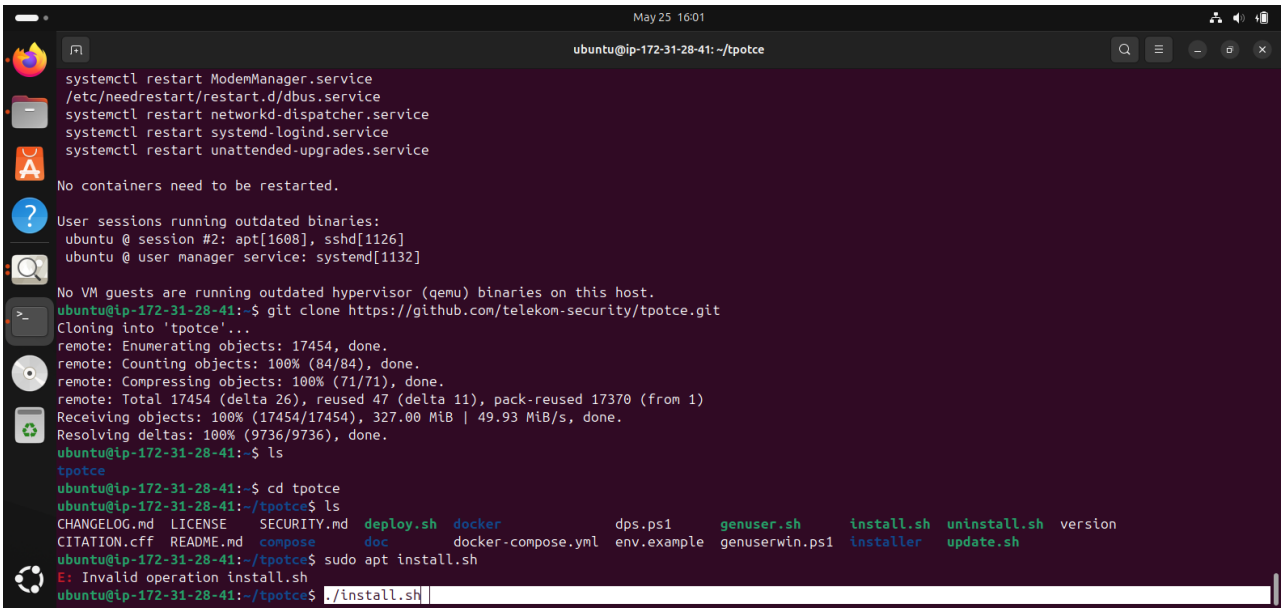
After system has updated you need to upgrade the system, to do that write the command sudo apt upgrade then click enter, it will ask you to confirm update click ‘y’ to confirm.



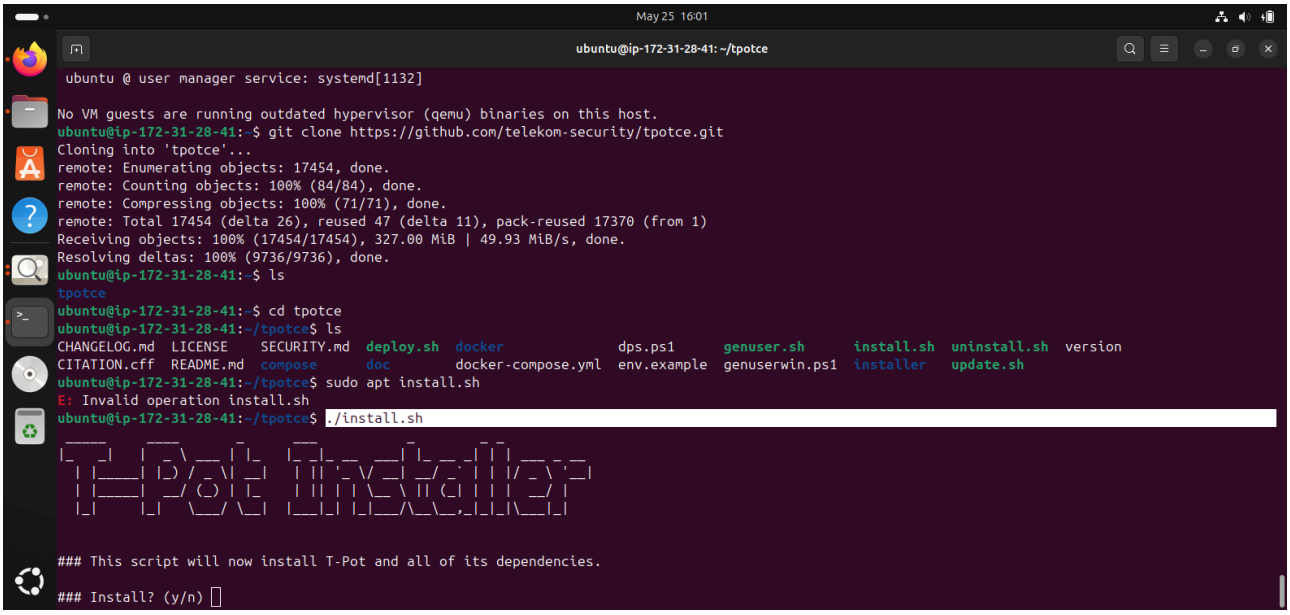
After upgrading we have to clone the github t-pot repository and to do that type the command: https://github.com/telekom.security/tpotce.git then click enter.



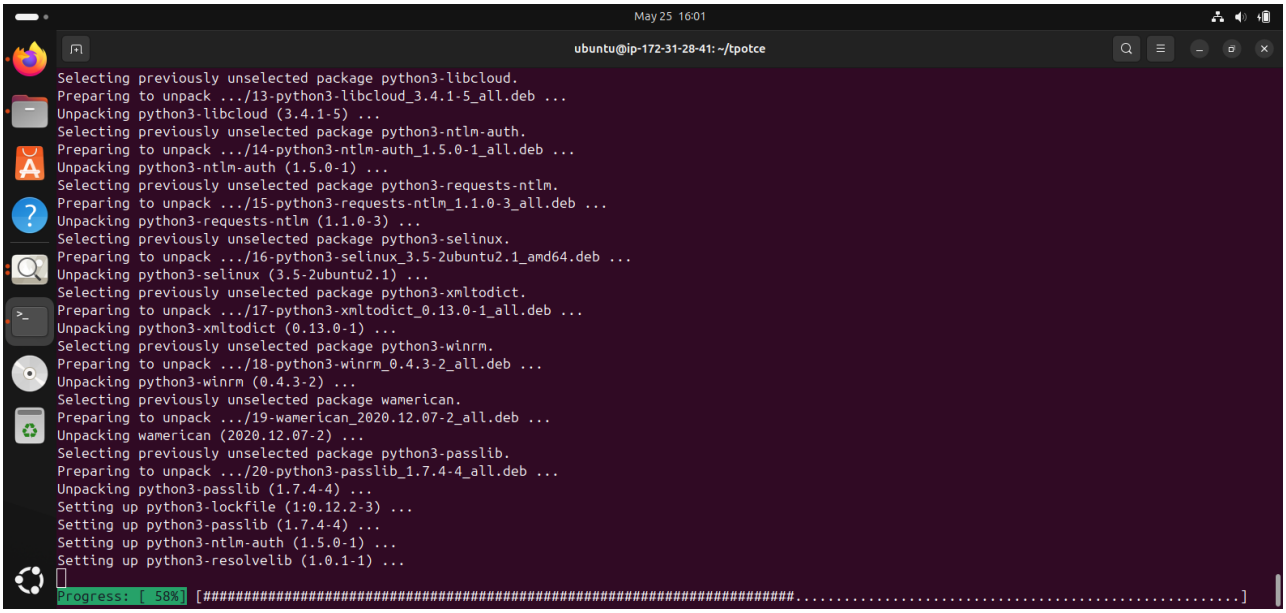
After cloning the github repository to list directories with the command ‘ls’ to see the newly cloned github repository.



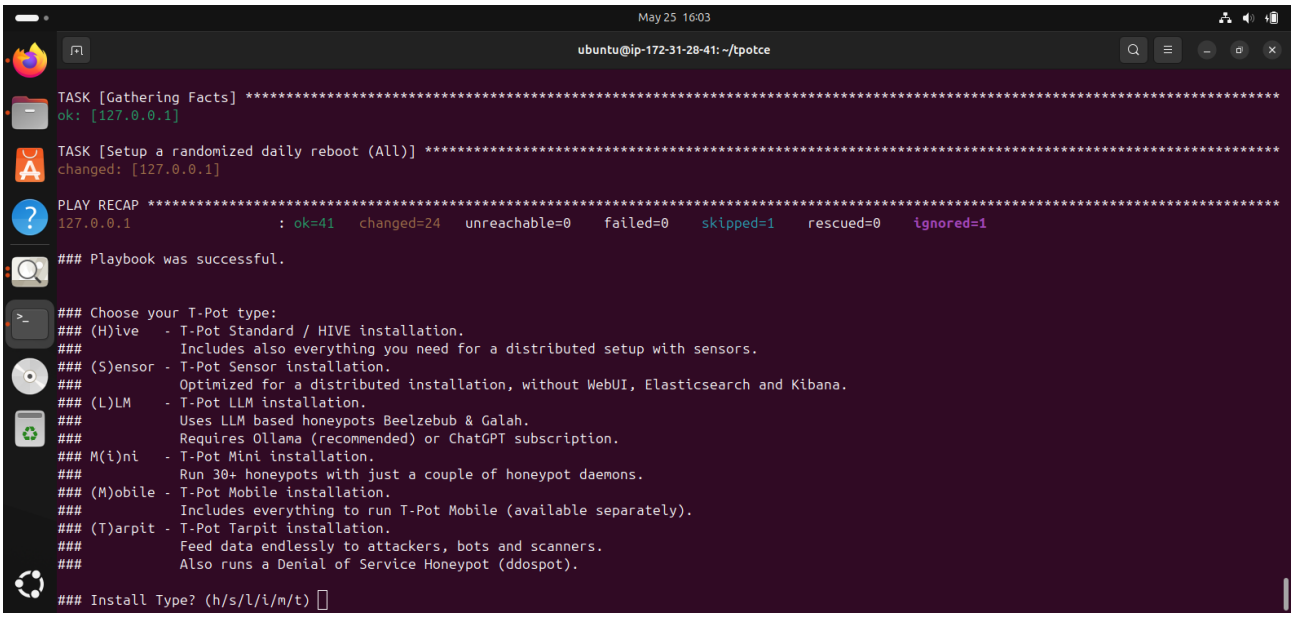
After listing the repository change directory to the tpotce file with the command ‘cd tpotce’ then click enter, there after list directories with the command ‘ls’ then install the tpot depository with the command ‘./install.sh’ then click enter.



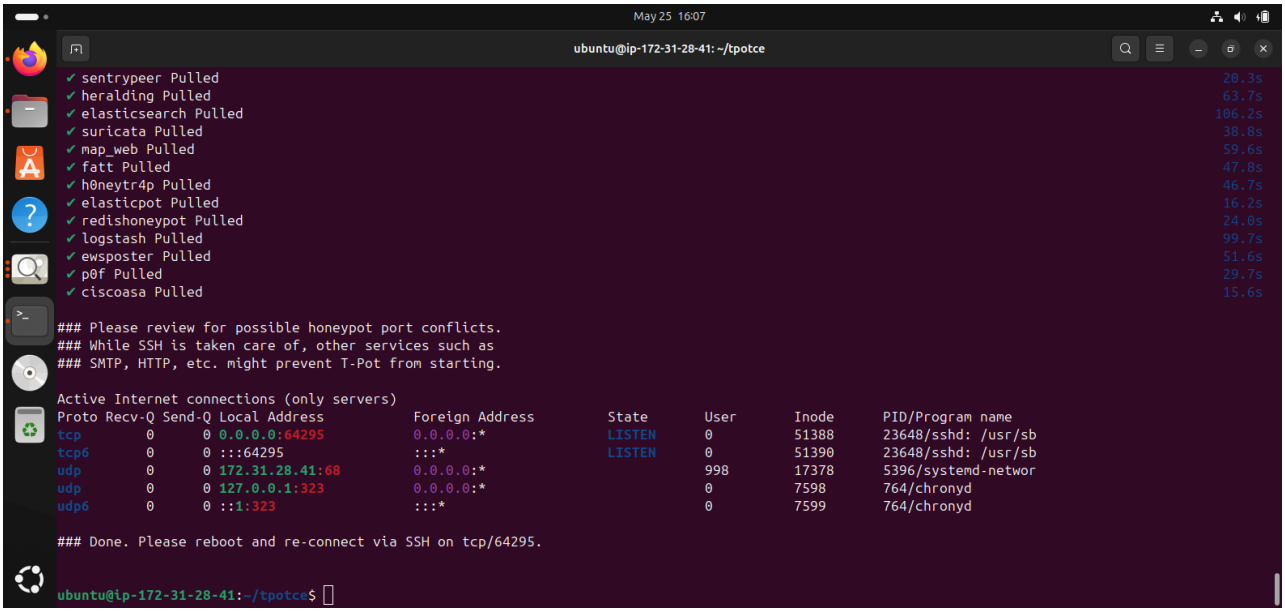
You will be asked if you want to install you should type ‘y’ to continue installation.



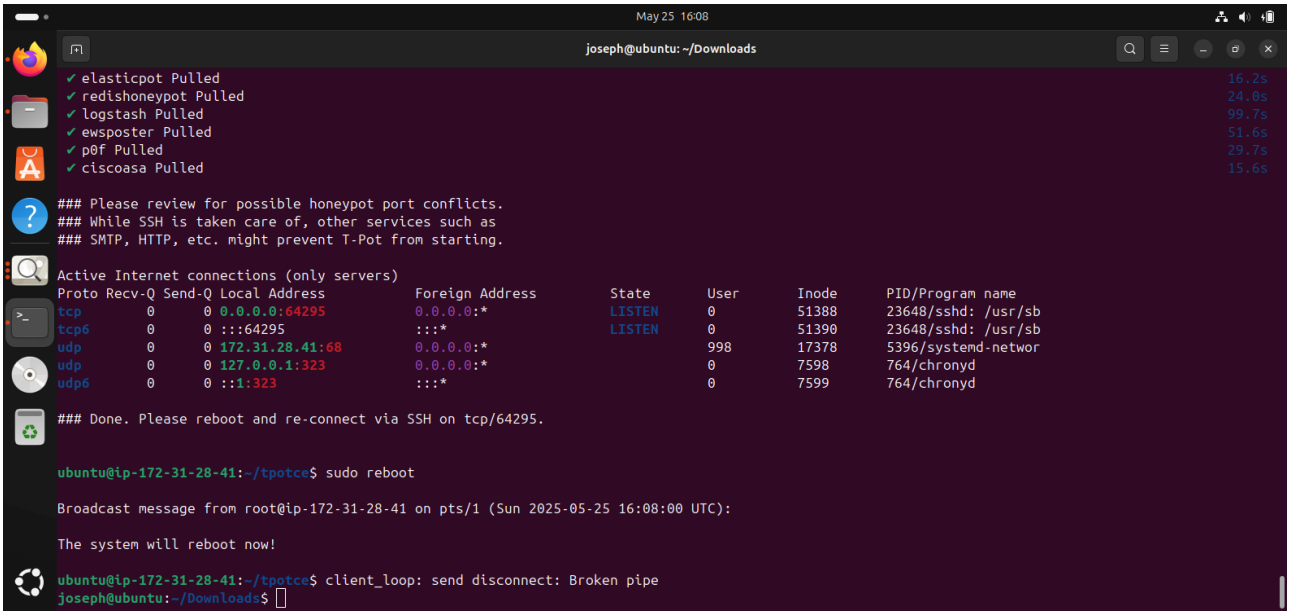
Installation process…



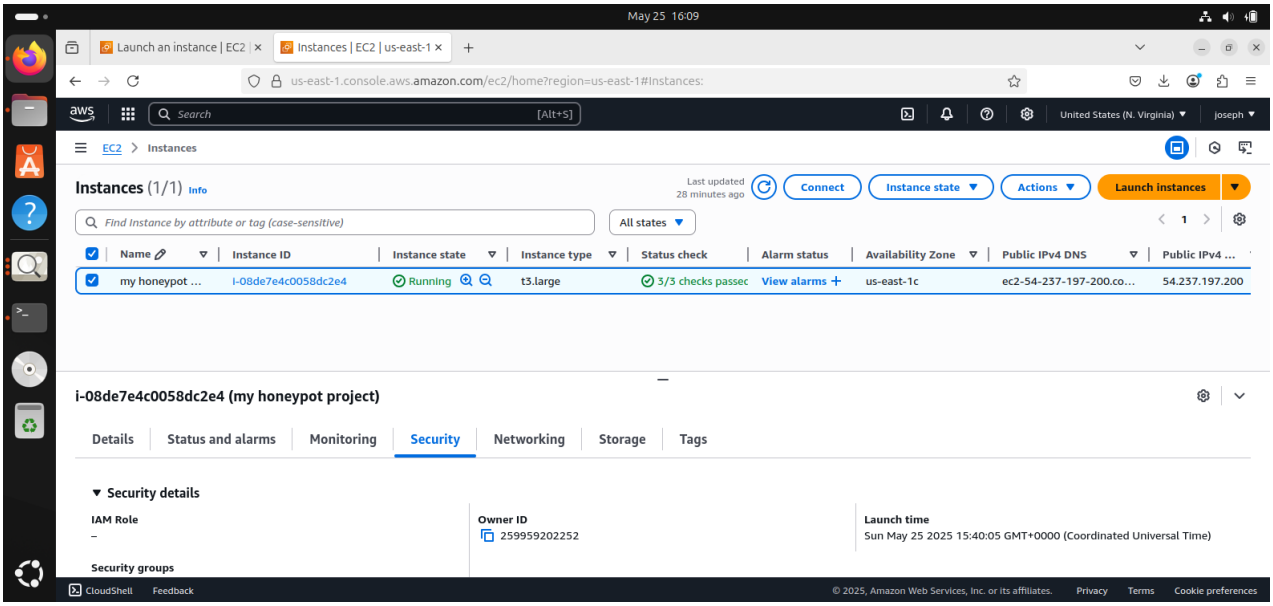
Before installation complete you will be ask to choose honeypot type, you have to choose –T-pot standard / hive installation, to do that simply type in ‘h’ and click enter.



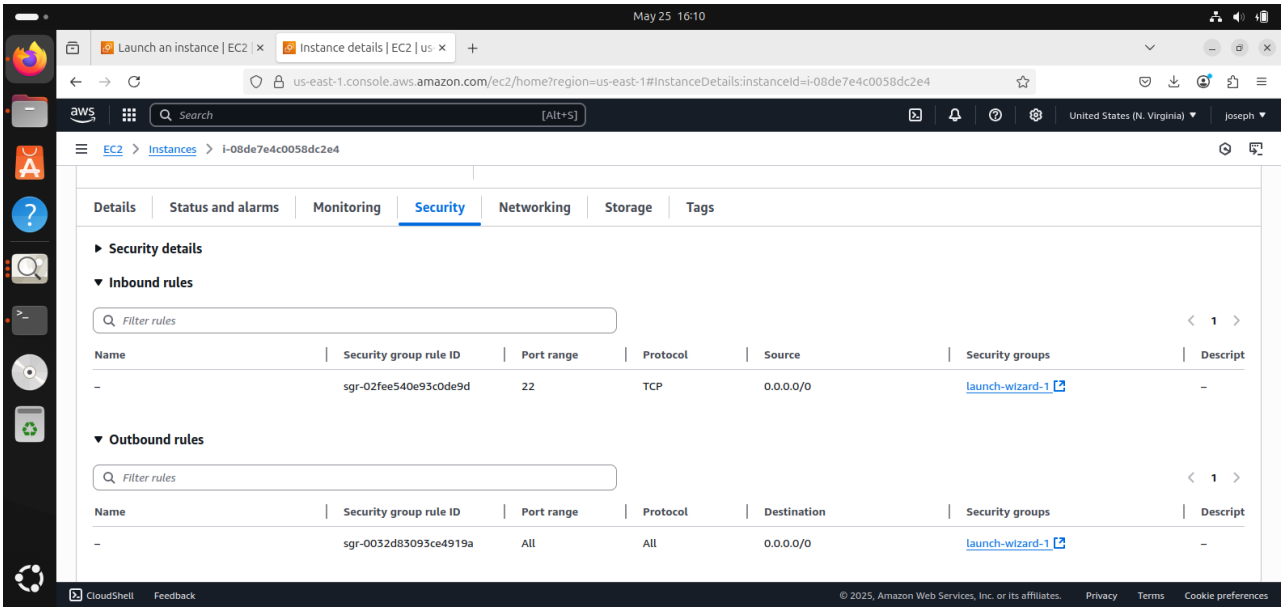
After choosing honeypot type installation will complete and you will be asked to reboot and reconnect, to do that type in the command ‘sudo reboot’ and click enter.



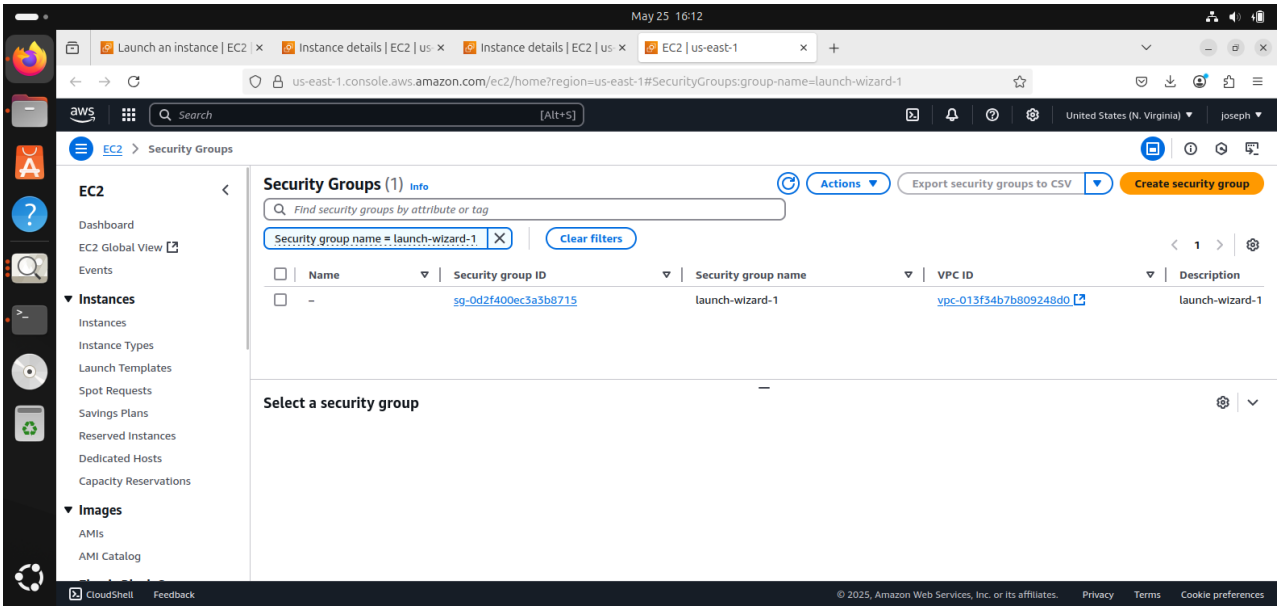
After reboot you will be kicked out as you can see in the picture above, now we need to setup some security protocol on our AWS EC2 instance.



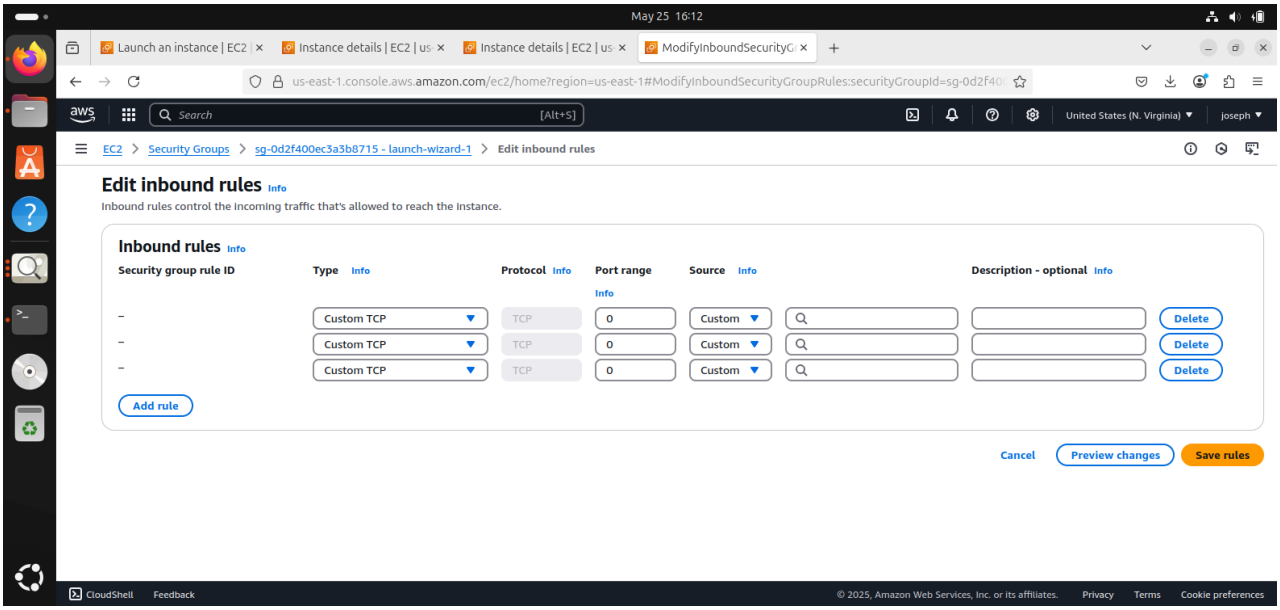
On the EC2 instance dashboard click on security to start setting security protocol setting.



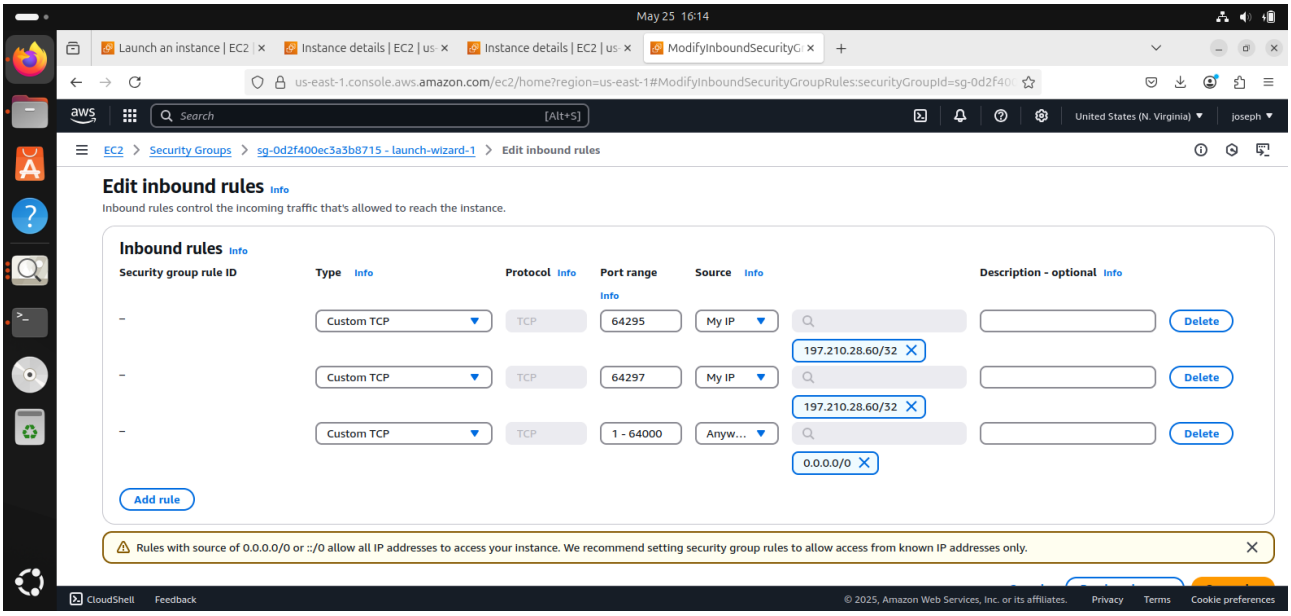
After clicking on security click on the blue spot which Is saying ‘lunch-wizard’



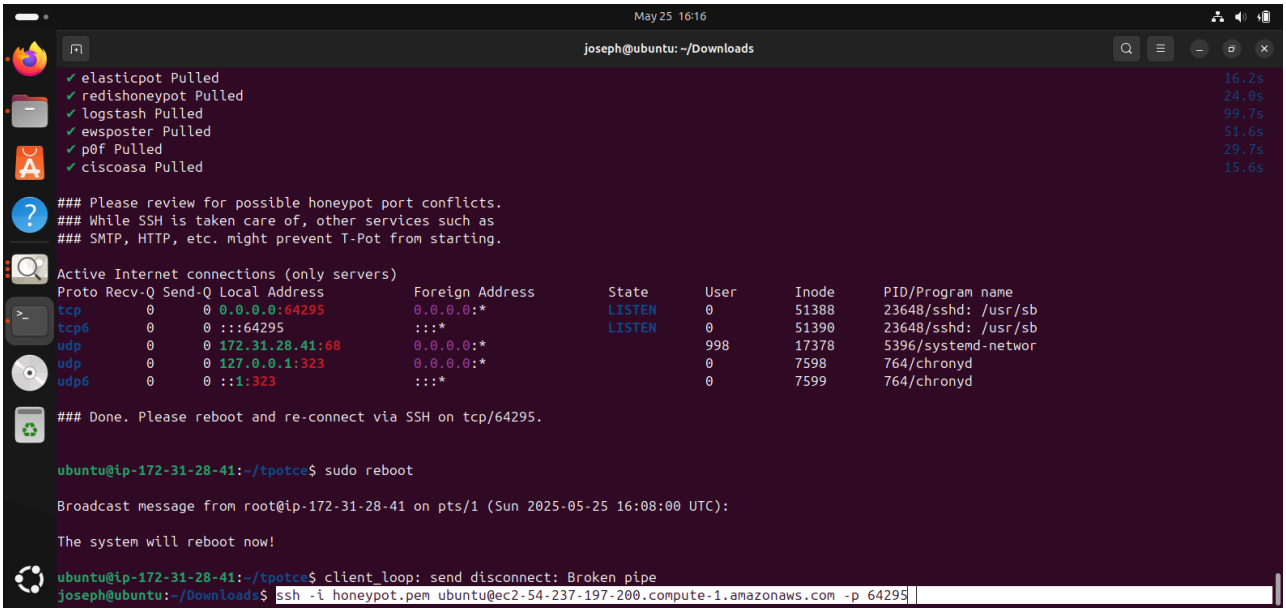
After that step click on the blue spot that starts with ‘vpc-’ to get to the page to set inbound rules.



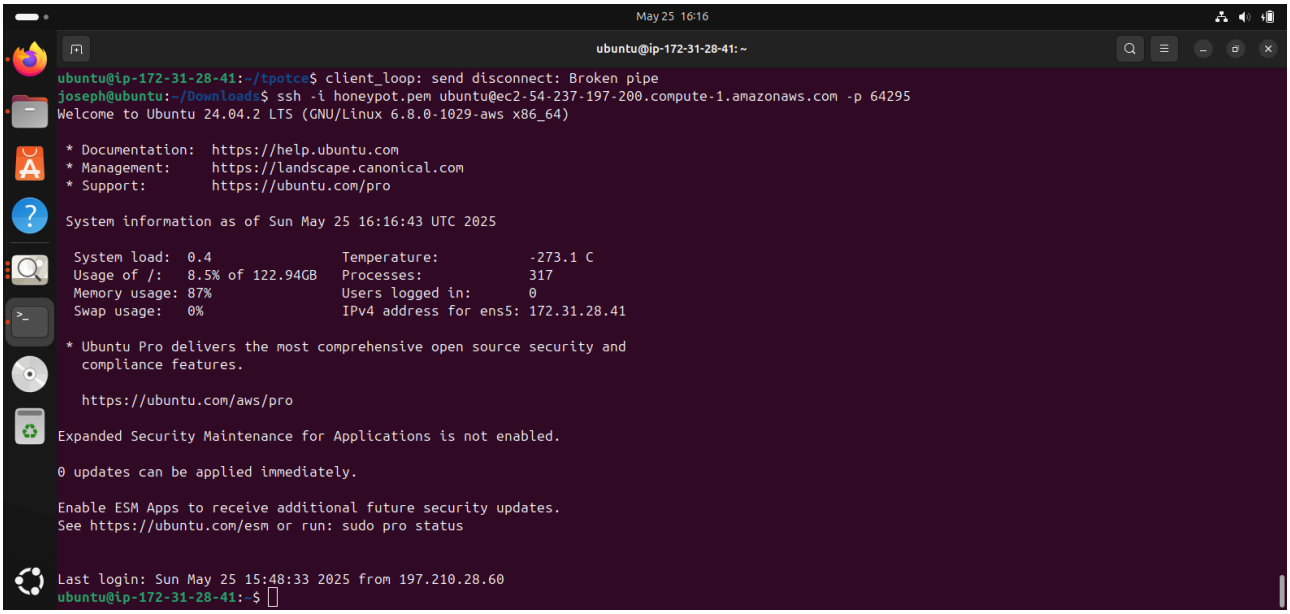
You are going to setup three security protocol which will be displayed and explain below.



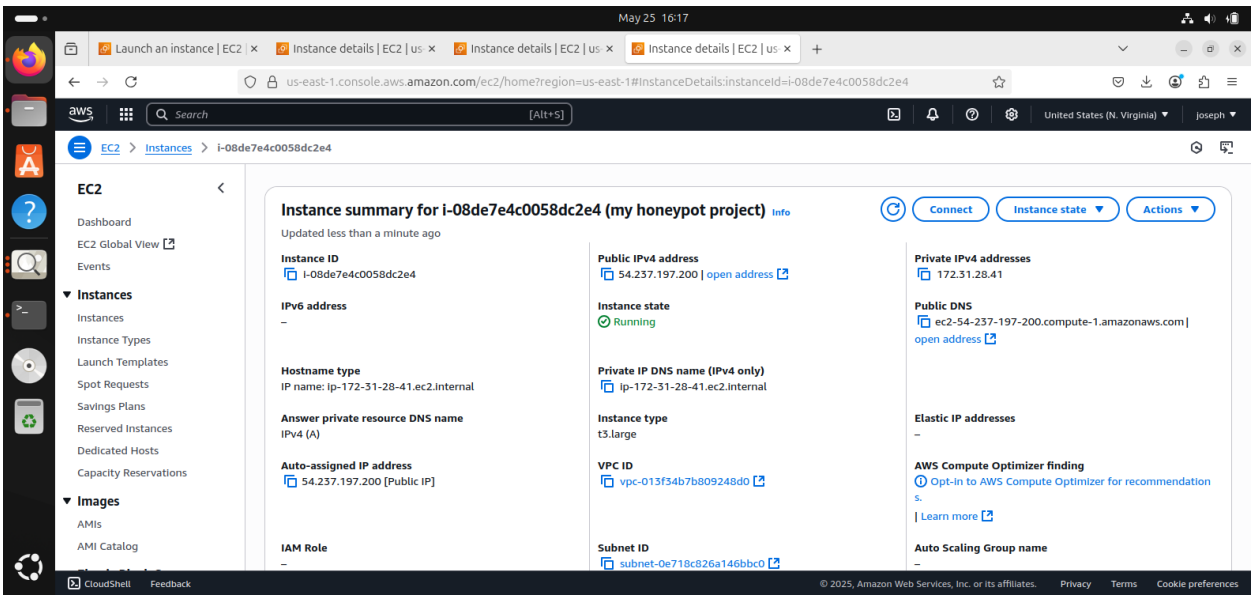
On the type leave the three rules as Custom TCP, on the pot range the first port should be set as 64295, this is the SSH port that will be used to login the command base interface of the honeypot, on the second port range input 64297, this port will be used to access the graphical interface, and the third port should be set from 1-64000, on the source, the first source should be set as ‘My IP’ the second source should also be set as ‘My IP’, then the last source should be set for ‘Anywhere ipv4’, then click on save rules.



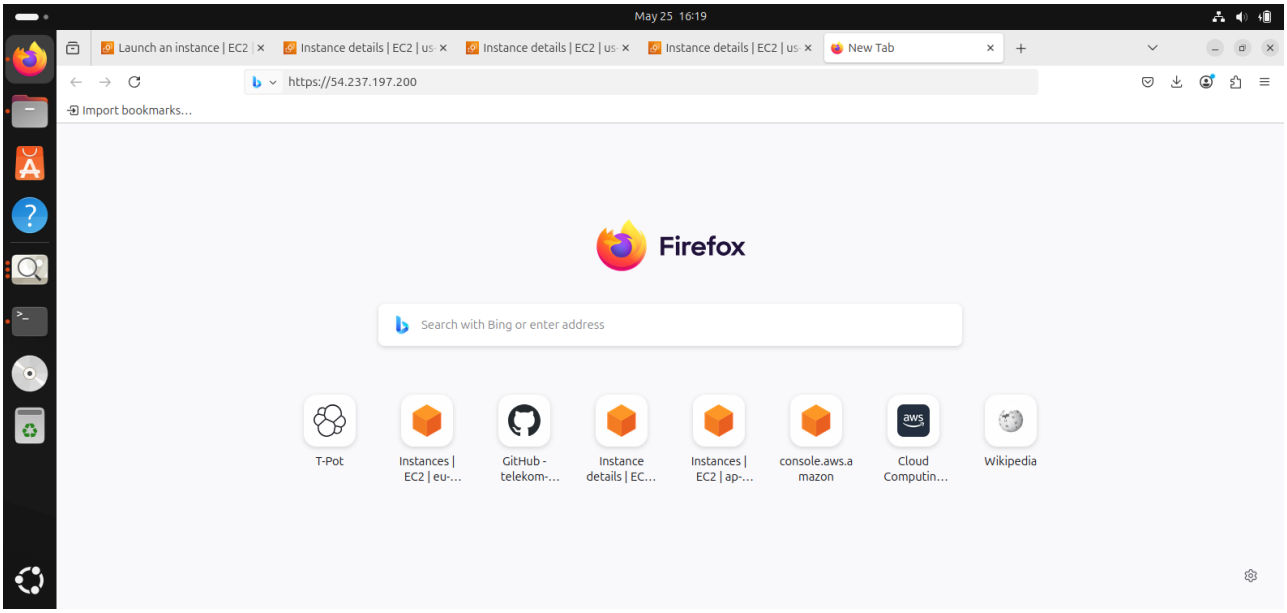
After that go back to your terminal and login with the SSH instance connection command but at the end you will add -p 64295 which is you command base interface login port.



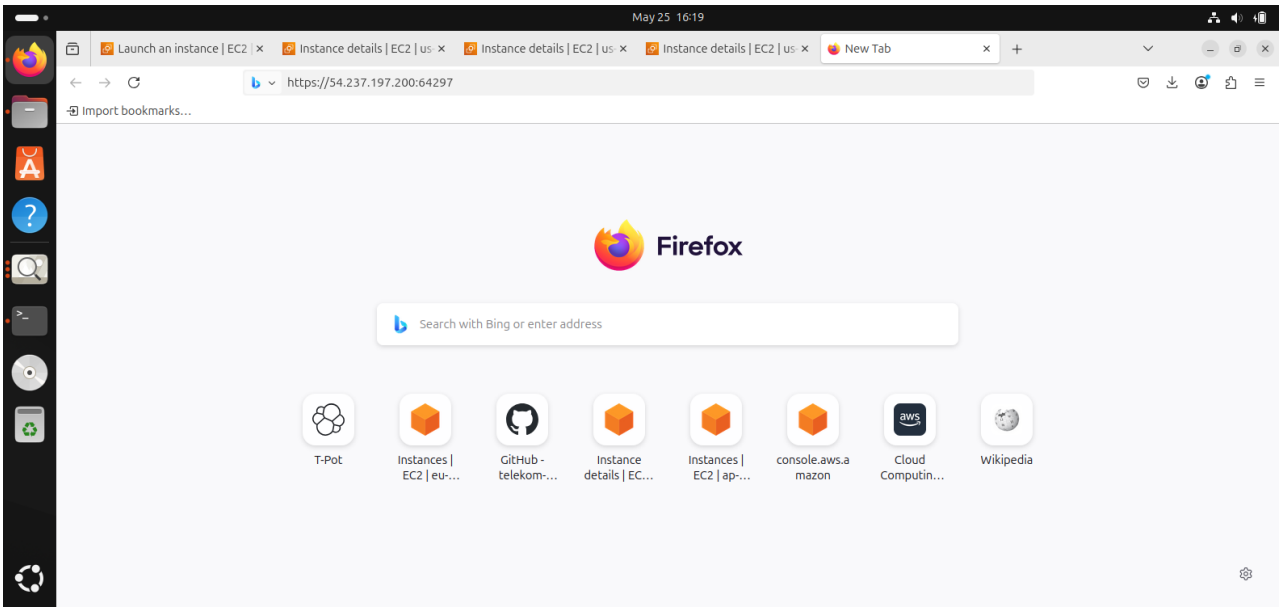
As you can see in the picture attach above the honeypot has been successfully login in the command base interface, now we have to go to our browser and login the graphical interface.



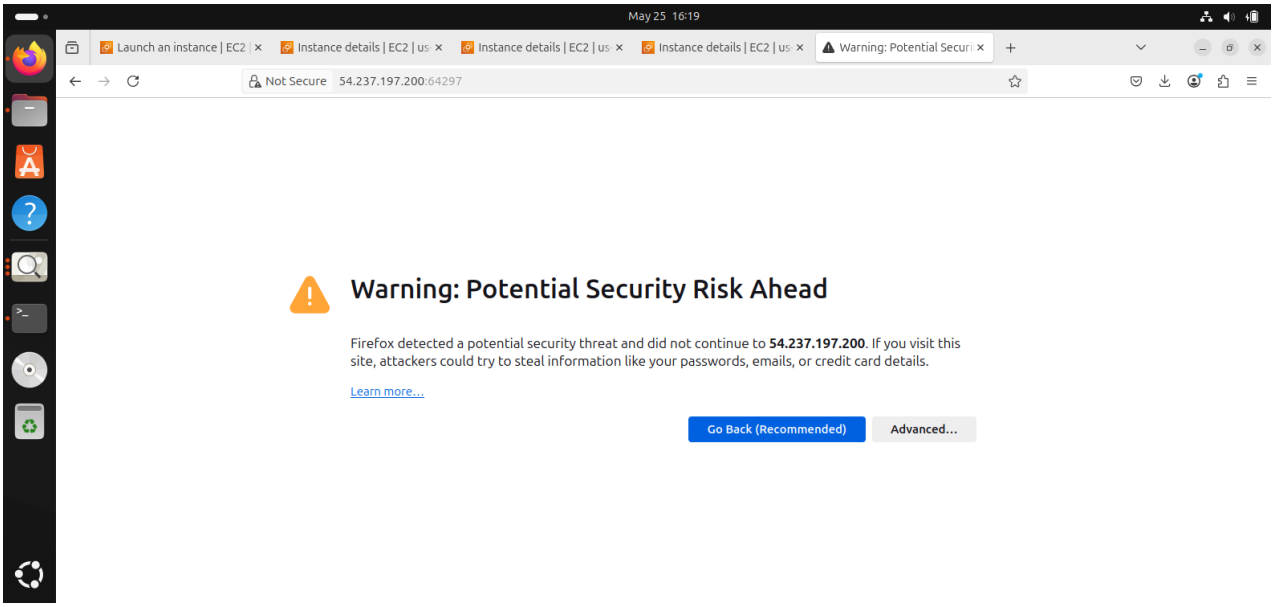
To be able to login our honeypot on the graphical interface we need to copy our instance public IP address and it can be found inside the EC2 instance as seen in the picture above.



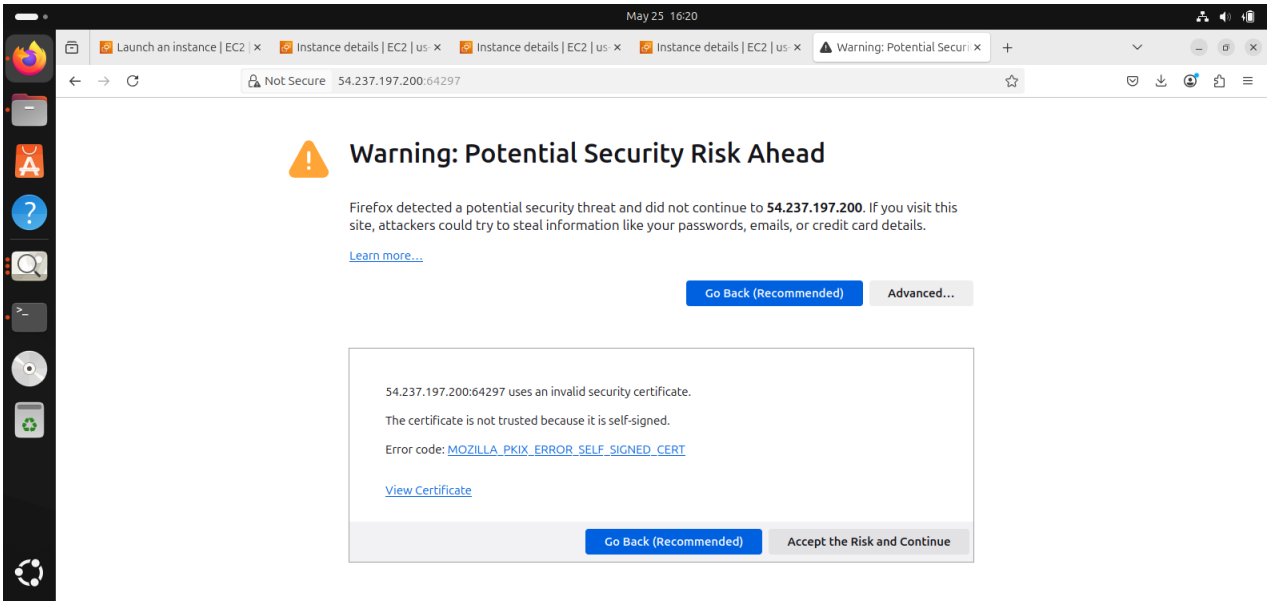
After coping the public address type: https:// then past the pubic address you copied just as its seen above.



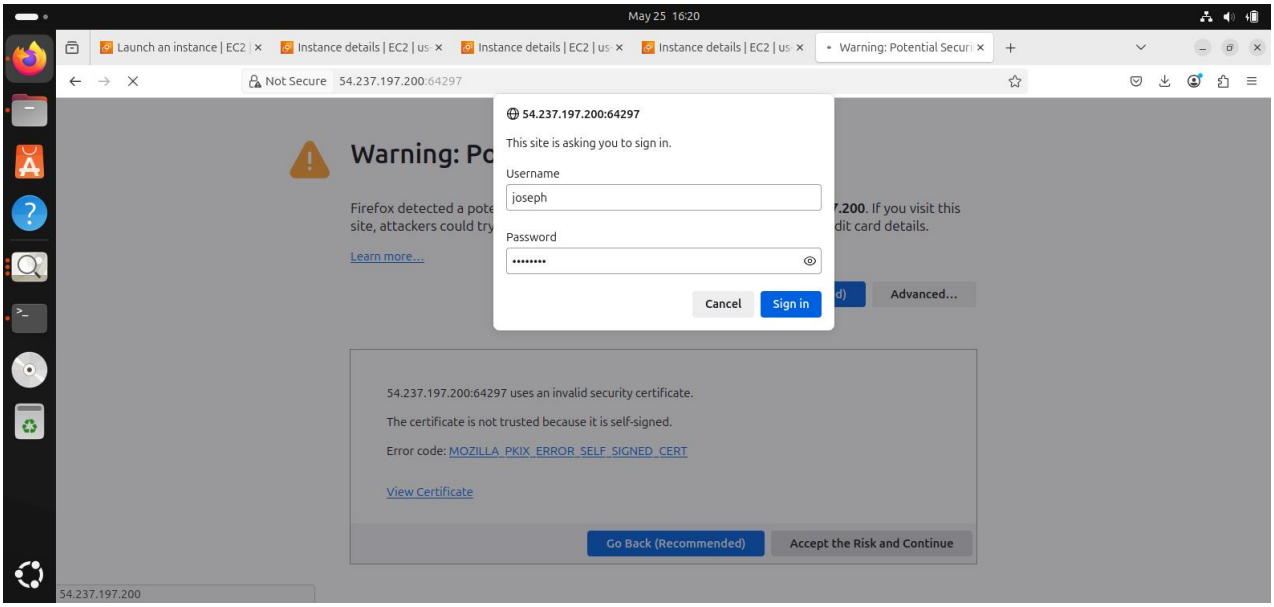
After that add : and the graphical port protocol 64297 then click enter.



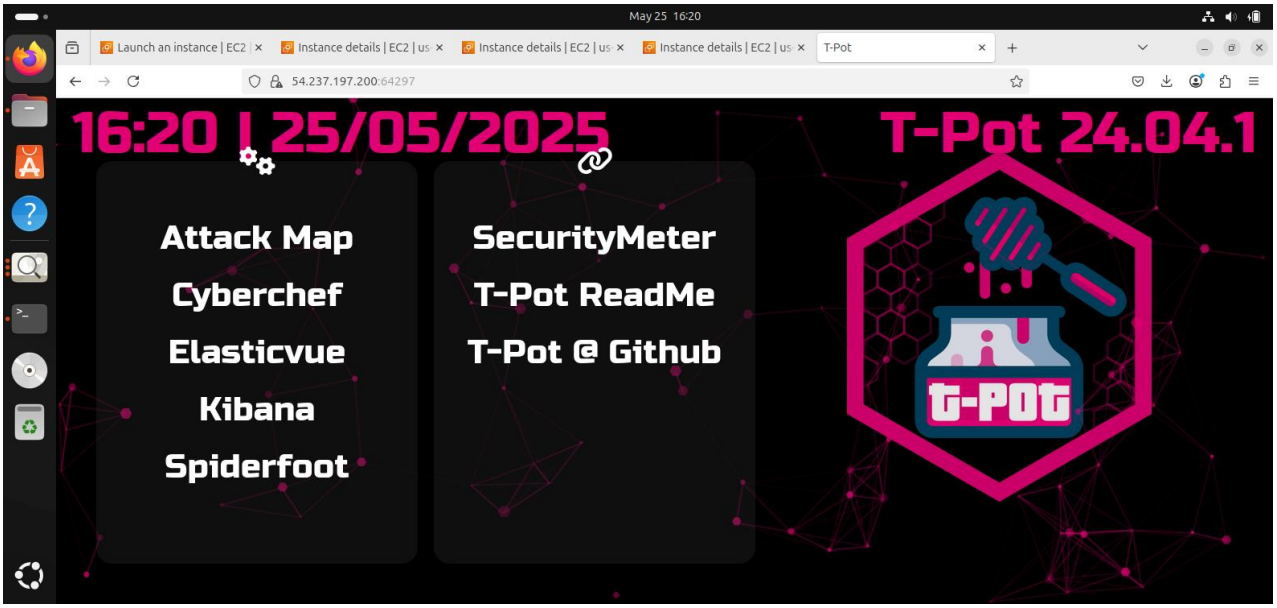
You will get a security risk alert, click on advance…



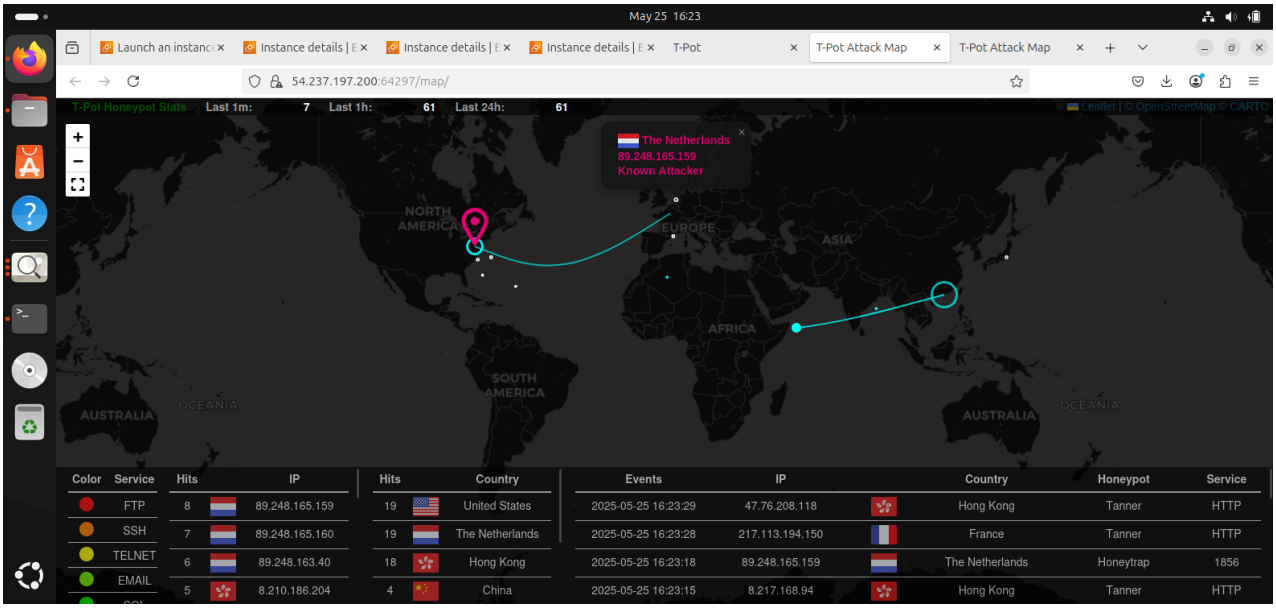
Accept the risk and continue.



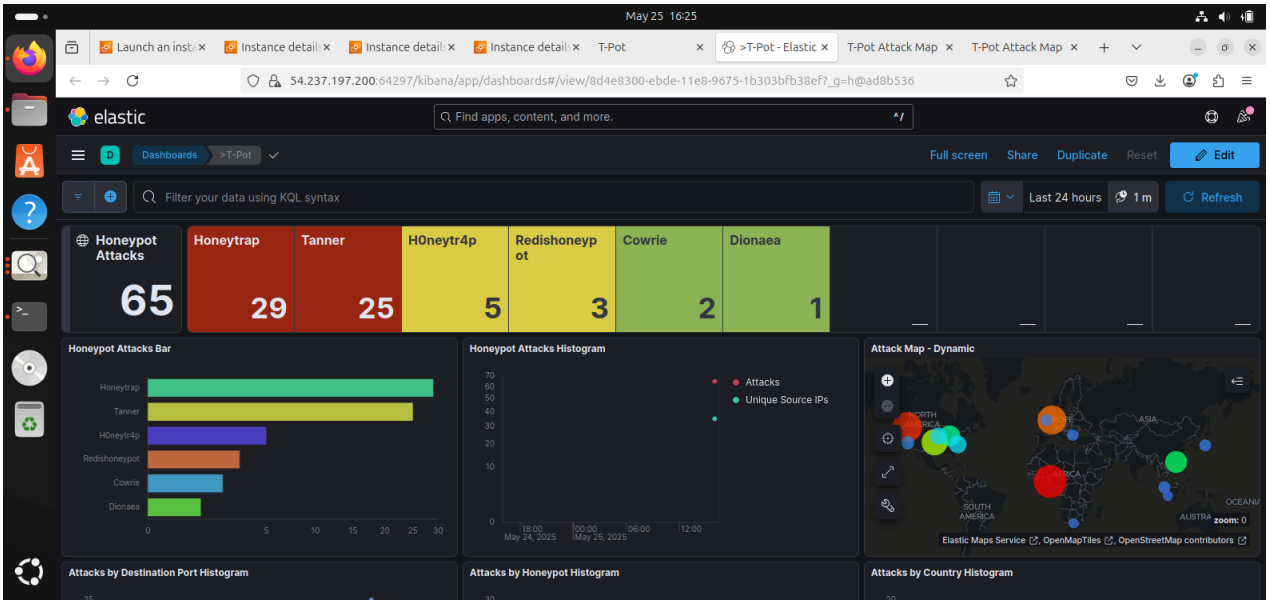
While installing the honeypot you were ask to create a password, sign in with that password.



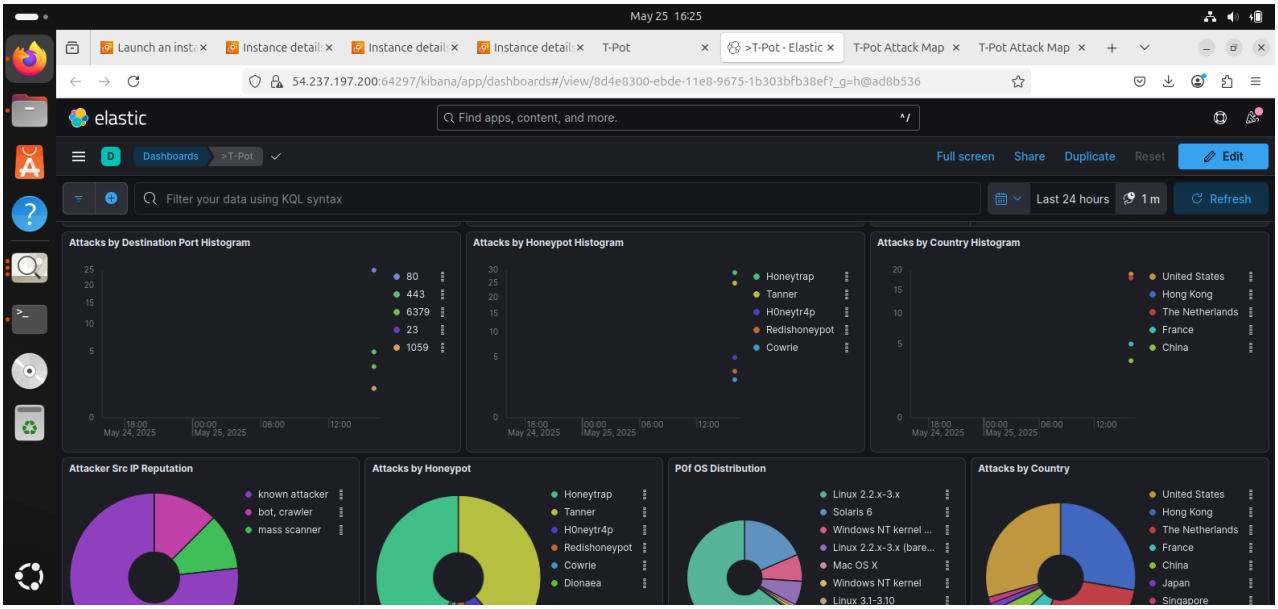
This is the graphical interface of our honeypot, the T-pot honey pot is a type of honey pot that consist if different honeypot and other features such as cryptographic features.



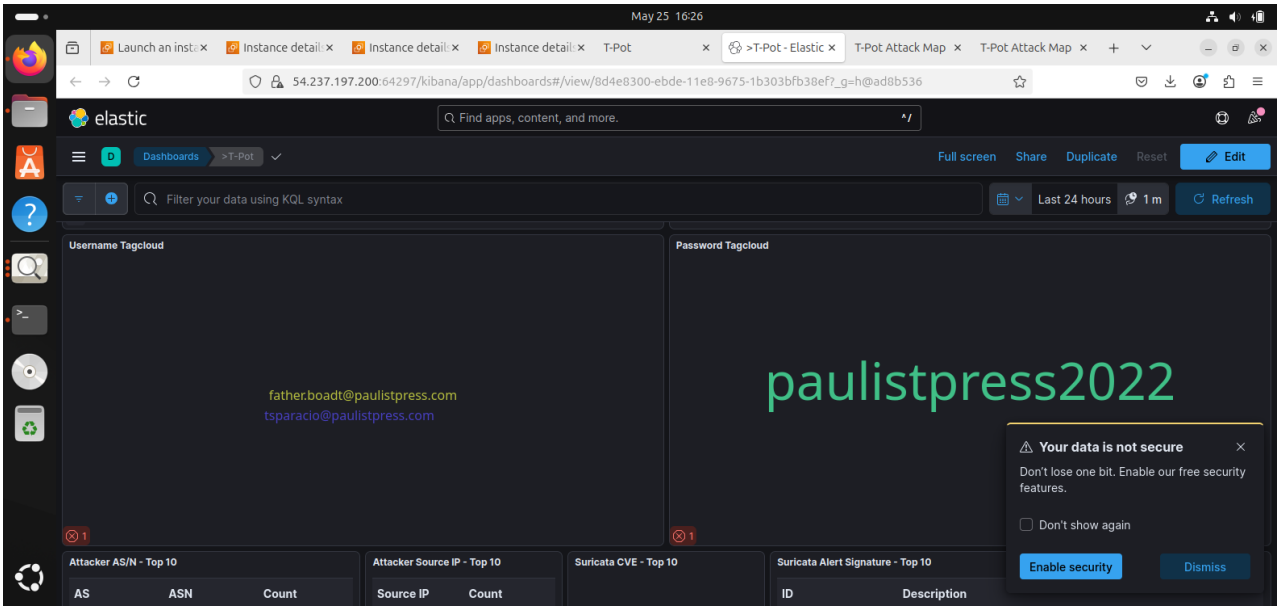
This is the attackers map, this allows us to monitor how attackers get into systems, the blue line on the map signify attacker trying to get into our system, we can also get their IP address and country they are attacking from on the attacker map.



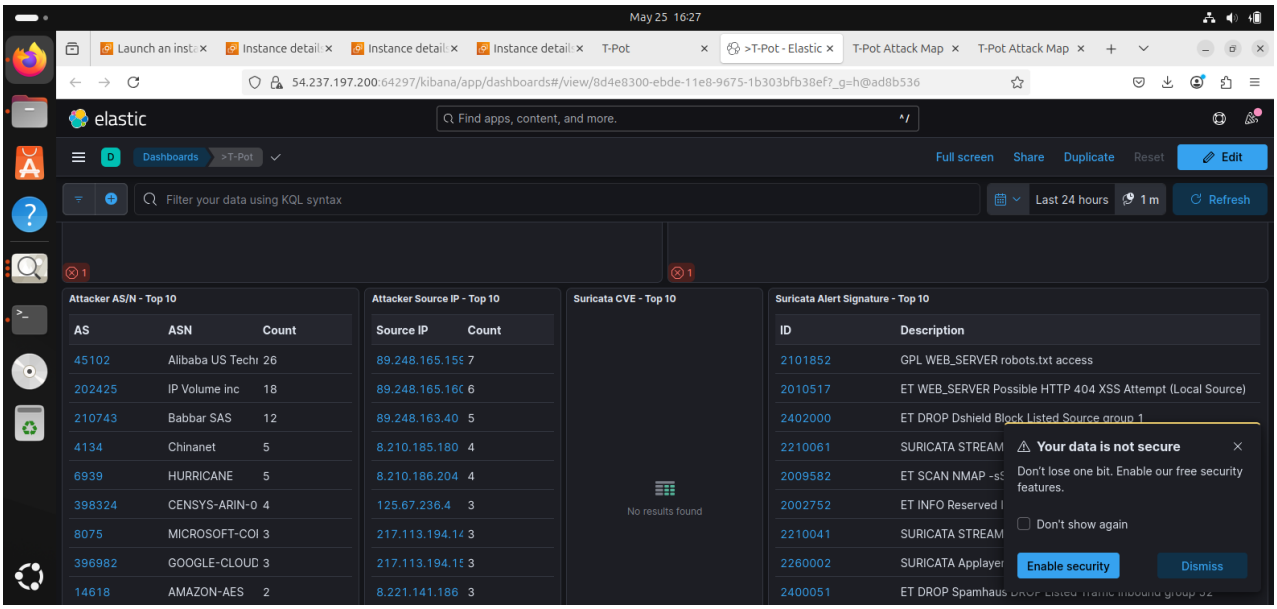
This is kibana it is a dashboard that analyzes and record the attack on the different honey pot on the t-pot platform, scrolling down we can also see all the attackers IP addresses and also the ports they are logging in from, as well as getting the password and username they tried using to get into the honeypot.



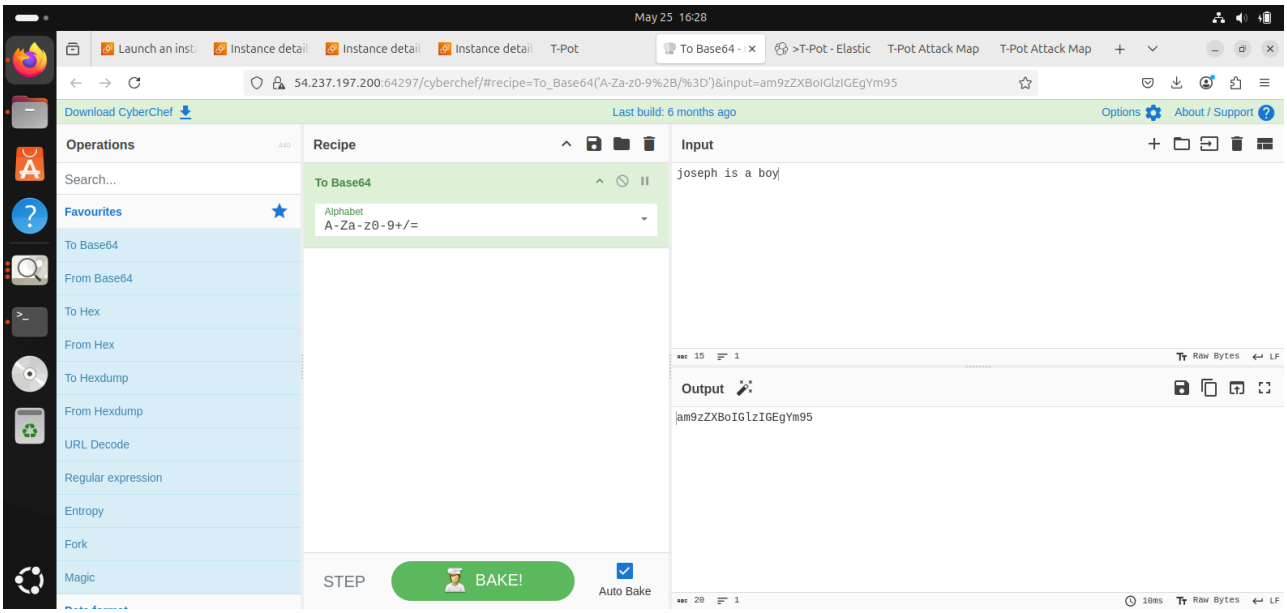
This is a more break down of the attacked been carried out on our honeypot, this include attacker distribution, and their country.



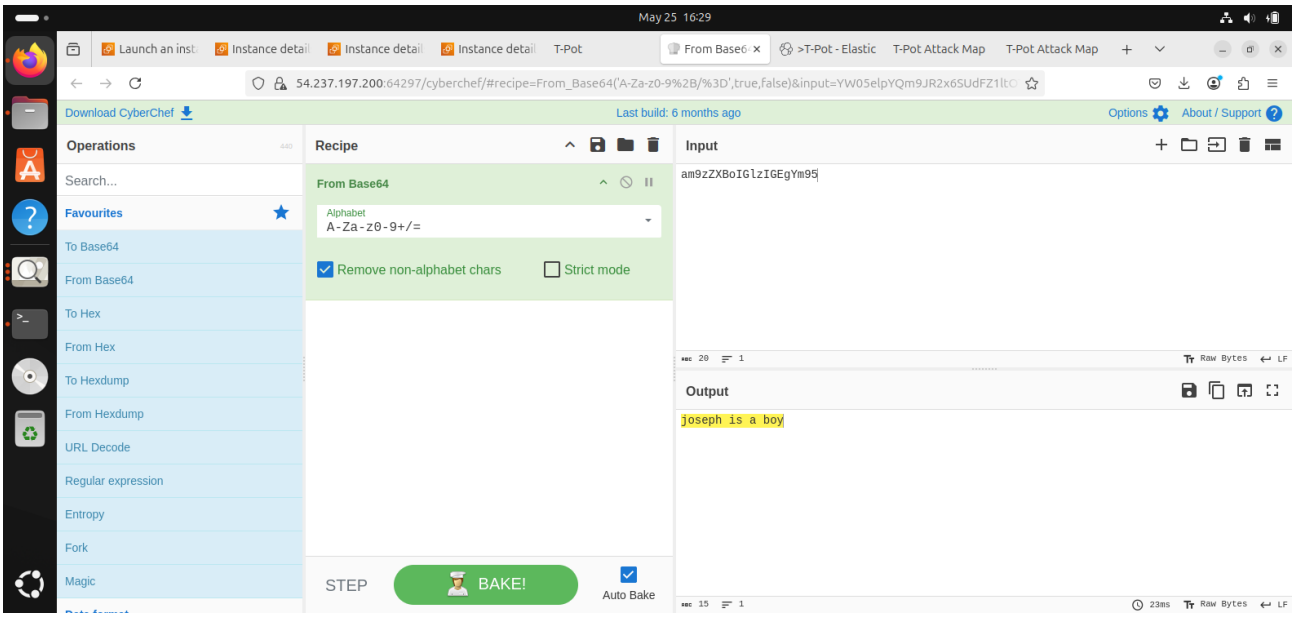
This is the attempted email and password the hacker try using to get in.



This is the details arrangement of the attacker details which include their IP address their ID and their AS and ASN.



This is the in-built spider-foot on this t-pot honeypot, it's a feature that can be used to encrypt and decrypt words, above is a sentence that has just been encrypted.



This above picture shows the decryption of same statement that was encrypted.

This document has presented a structured and detailed methodology for the design, implementation, and deployment of a honeypot system. Through a systematic, step-by-step approach, it has outlined the necessary technical configurations, tools, and best practices required to create an effective honeypot capable of capturing malicious activity and providing insights into attacker methodologies.