How I Turned Azure Into a Cybersecurity Trap

Introduction

Welcome to the **Azure Honeypot Project** — where deception becomes a powerful defense.

In today's digital battlefield, staying one step ahead of attackers is crucial. One clever way to do that is by using a **honeypot**—a deliberately vulnerable, fake system that mimics real network infrastructure to lure in cybercriminals. Think of it as digital bait: while attackers think they're breaching a real target, they're actually walking into a controlled environment where every move they make is recorded and studied.

In this project, I'll take you behind the scenes of how I transformed **Microsoft Azure**, a powerful cloud platform, into a **cybersecurity trap** using a highly sophisticated honeypot solution called **T-Pot**. This isn't just about catching bad actors—it's about learning from them. By observing real-world attack patterns, we can better understand threat behavior and improve our defenses.

Whether you're a student, cybersecurity enthusiast, or professional, this journey will show you just how valuable—and eye-opening—a honeypot can be.

Let's dive into the trap I set in the cloud.

Use-Cases

- Identify attack source, location, and ISP.
- Discover frequently used passwords for brute-force attacks.
- Analyze intruder actions and commands executed.
- Track malware download attempts.
- Detect and analyze malware dropped by intruders.

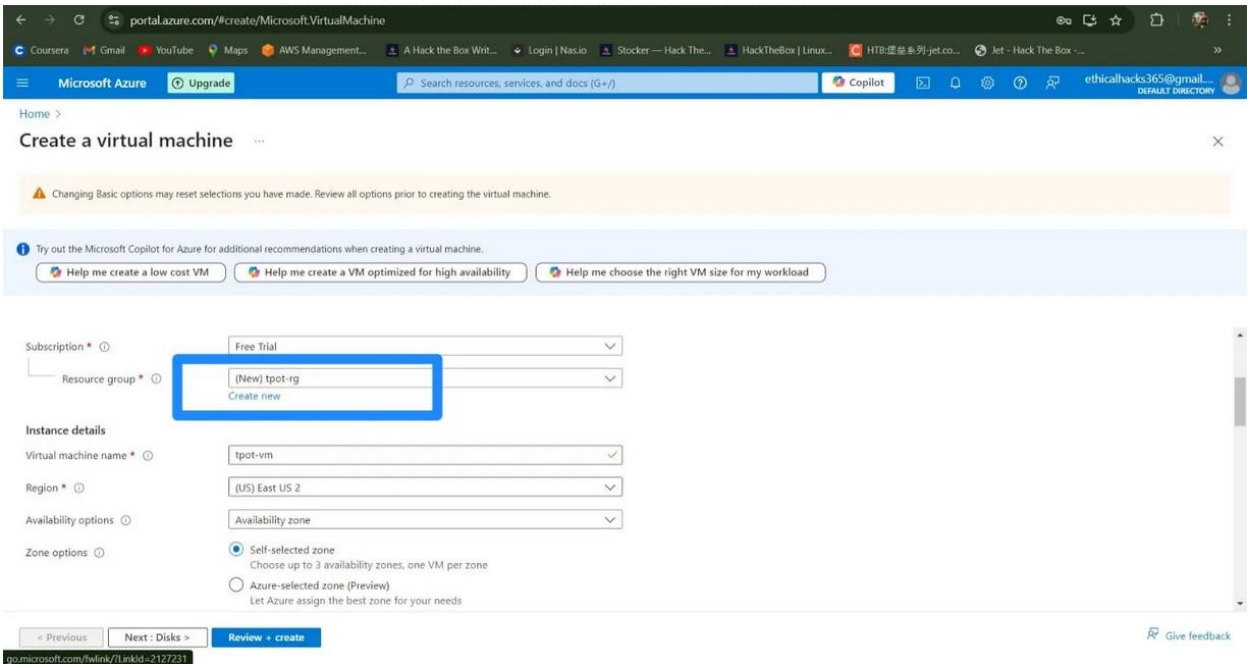
Let's start the project.

The first thing to do is to sign up an **microsoft azure portal.**

NOTE -: The whole project can be done with the free trial account of Microsoft Azure. Azure provides $200 free credit, and this is more than sufficient for this project. It is completely free of charge. So no need to worry :)

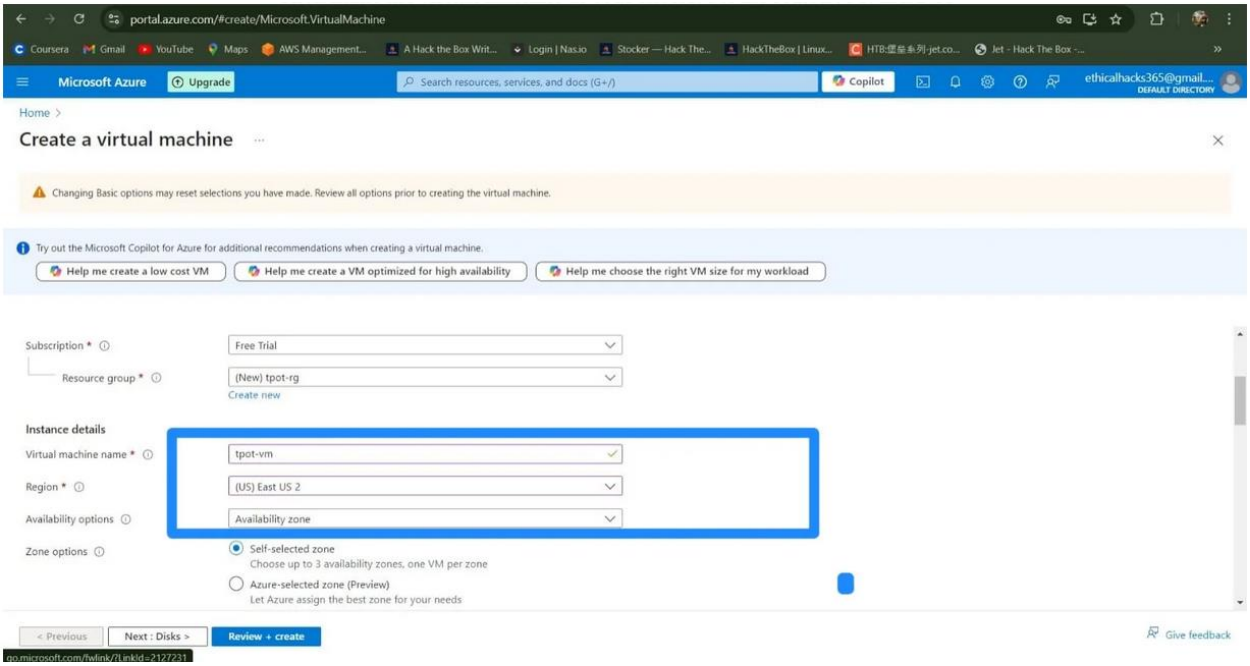
After the creation of account. At the top, search for virtual machine, then click on create VM.

After that create a new resource group and name it “tpot-rg”. ↓

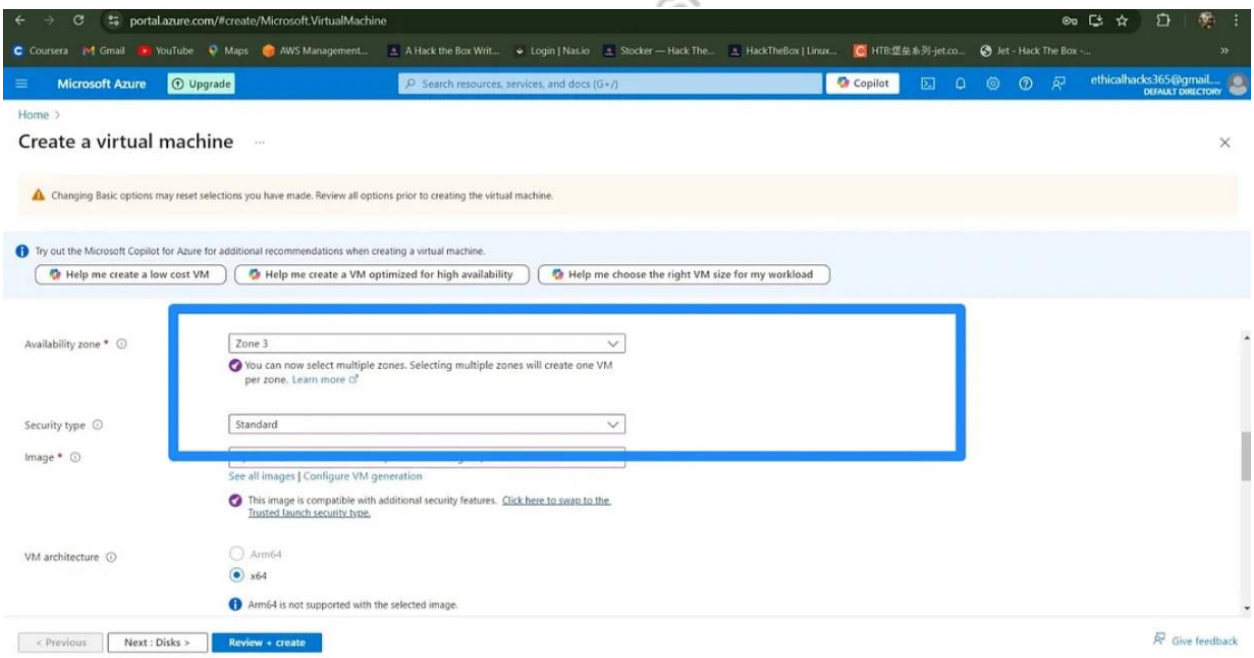


If you ever wanted to delete the entire project, just delete this resource group and everything will be erased completely.

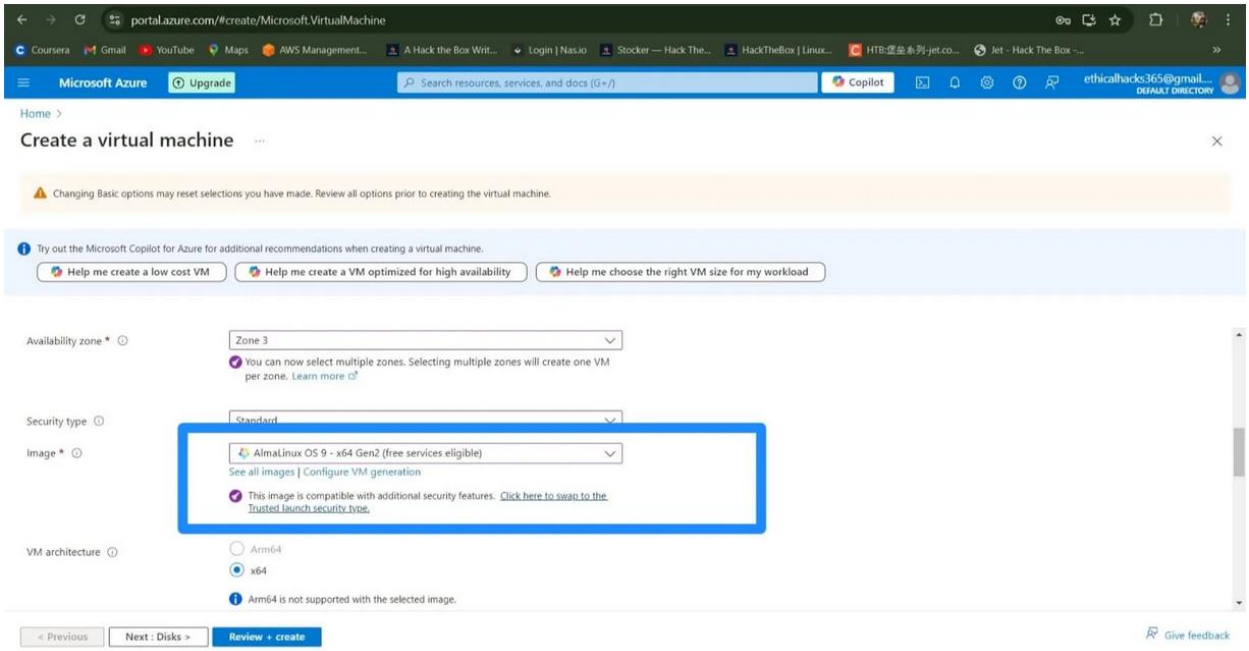
Then name the virtual machine as your choice. Set the region *(US) EAST US 2*. ↓



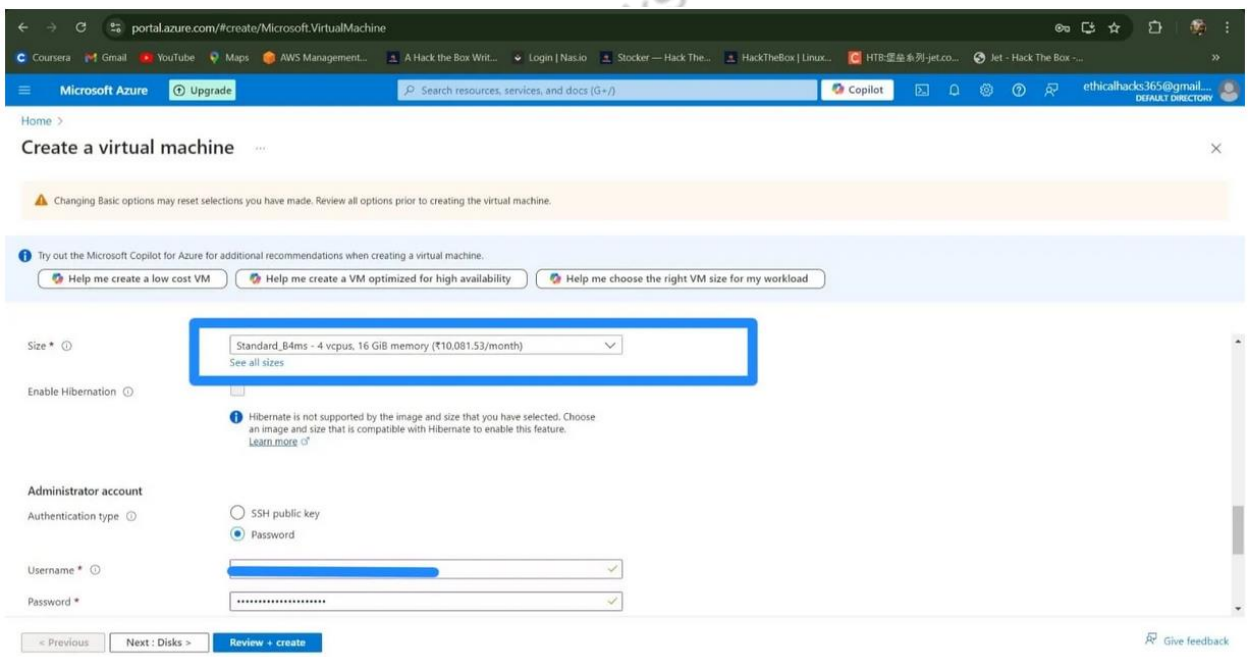
After that select the Availability zone as “Zone 3”. So that we can avail our Almalinux os image and our storage size. Then set the security type to *standard*. ↓



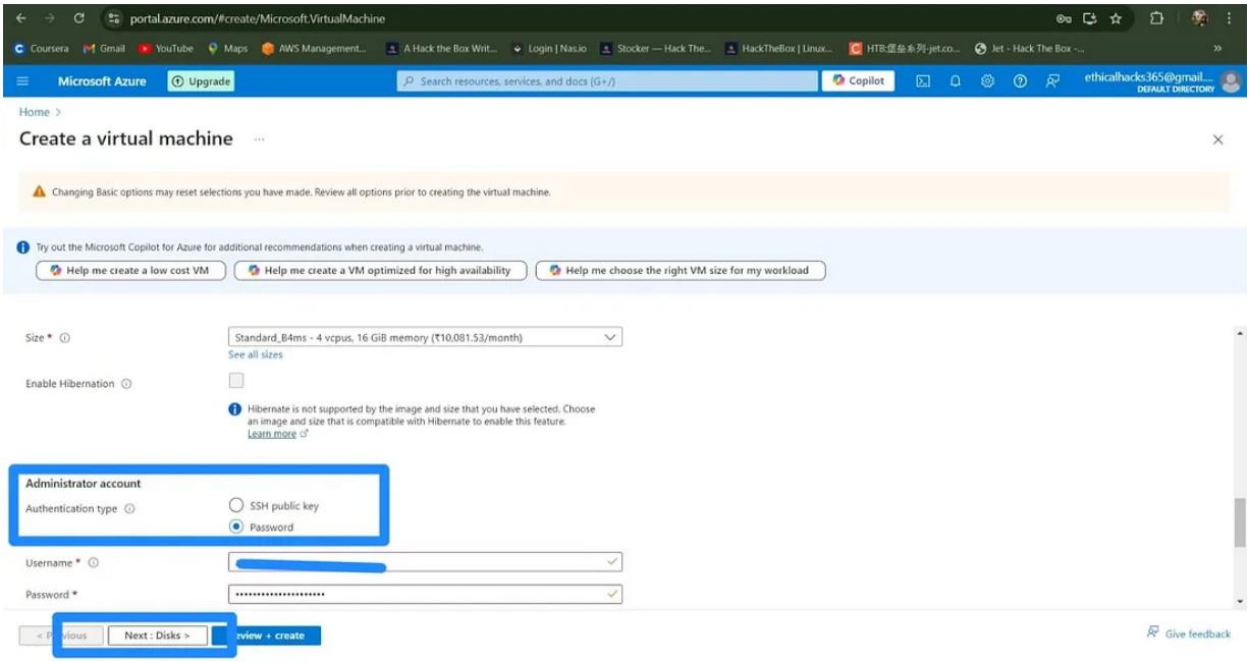
Then select the OS image *AlmaLinux OS 9 -x64 Gen2* which is completely free. ↓



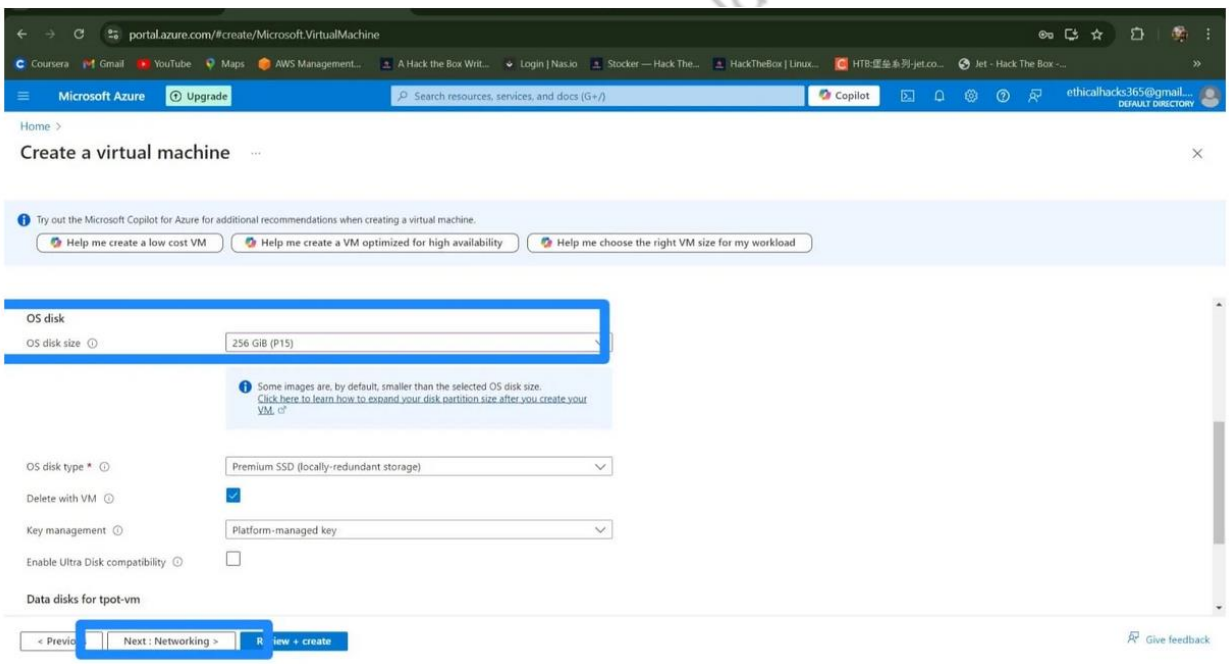
Next thing to do is choose size , here choose *Standard_B4ms-4vcpus, 16 GiB memory (10.081.53/month)*.No need to panic with the money it will be deducted from your free $200 credit:) ↓



Now select the authentication type as “Password.” Then enter username & password as your choice. After that click on Next : Disks > ↓

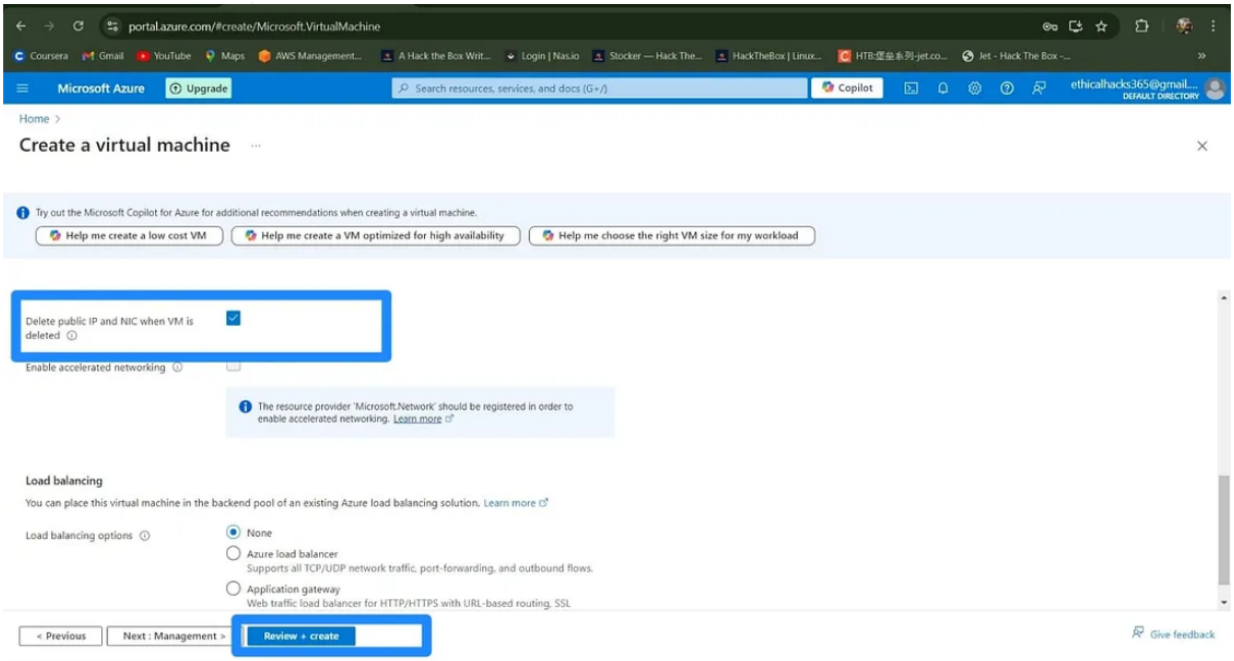


Then change the disk size to 256 GiB (P15), and then select Next : Networking > ↓



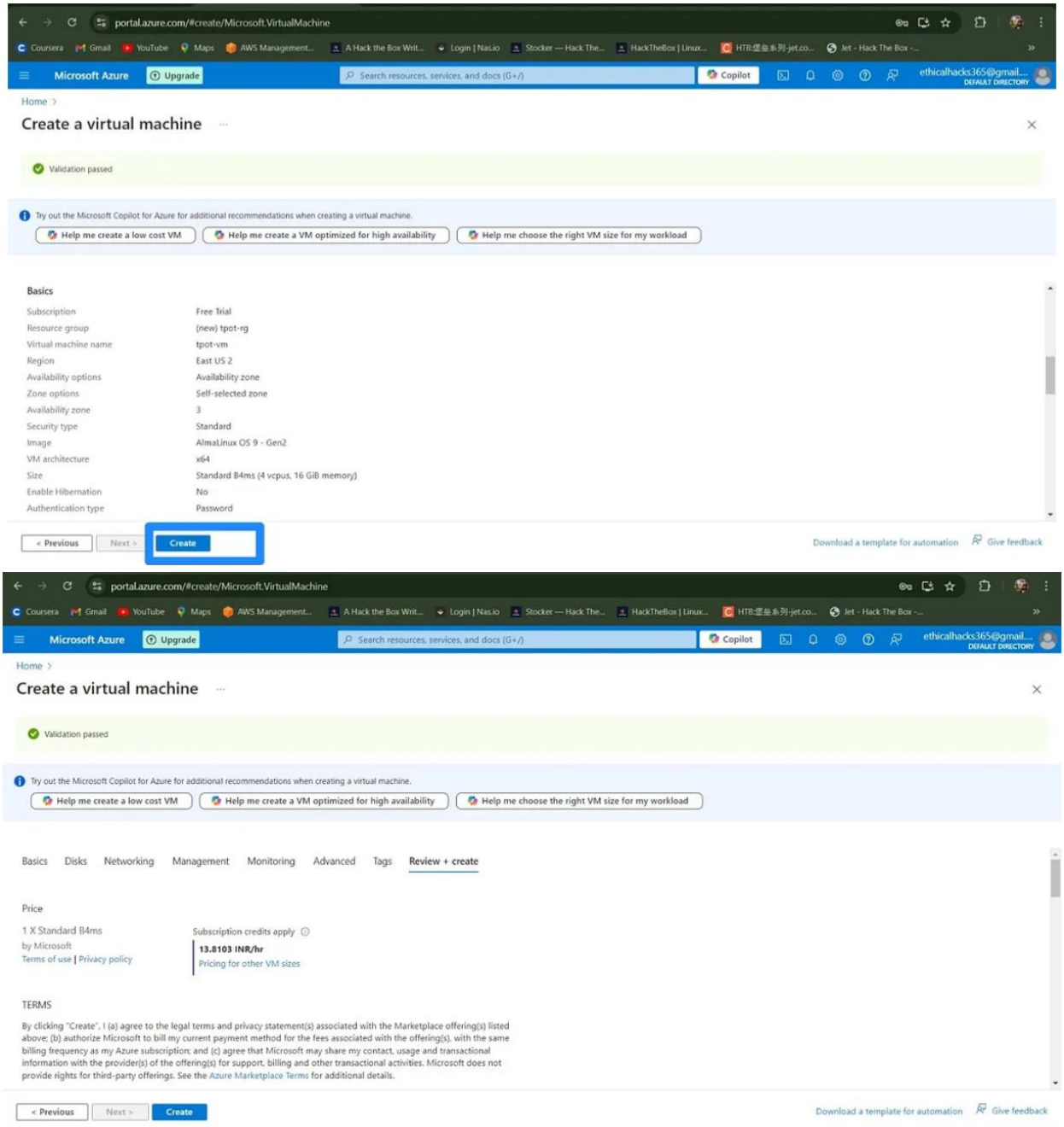
Here, check the box to delete public IP and NIC when VM is deleted.(Most important). Then click on Review + create and wait a few seconds for validation test.

NOTE -: I didn't use a load balancer here because it is a small-scale project, so I am not expecting heavy traffic. If you want to use it. It's completely up to your choices and needs.
↓

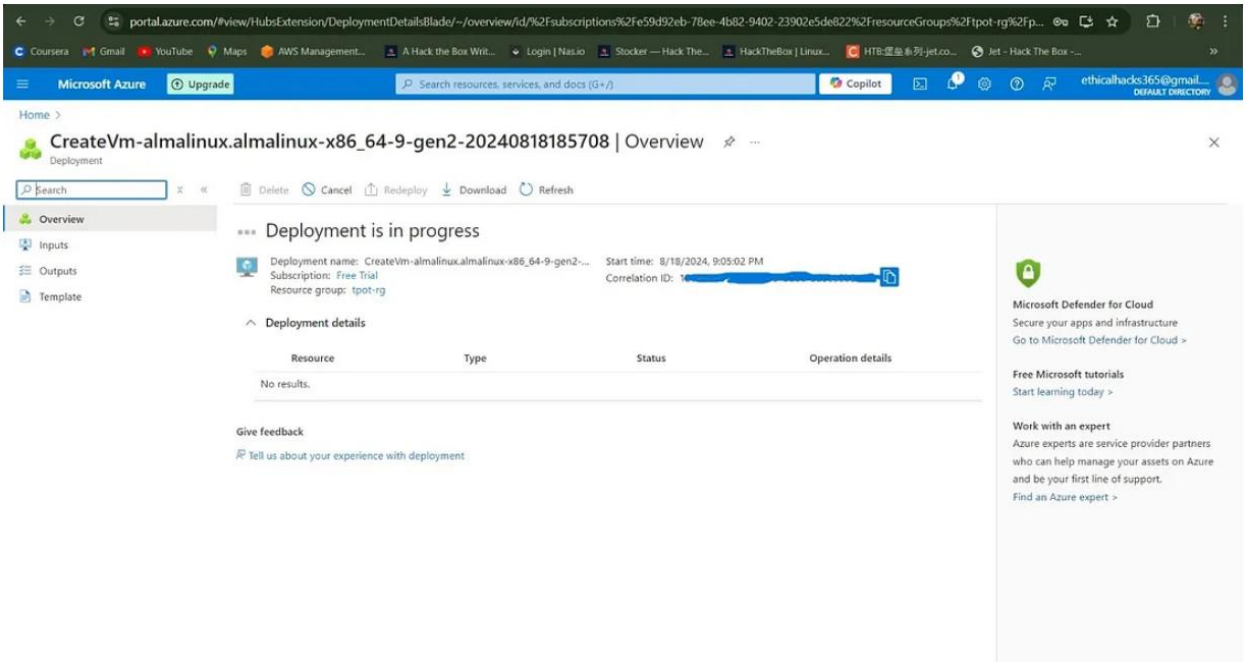


After passing the validation click on Create and wait 2–3 minutes for deployment process.

↓



There is no need to panic by watching the pricing. This will be deducted from the free credit. So Keep Calm and take a deep breathe.



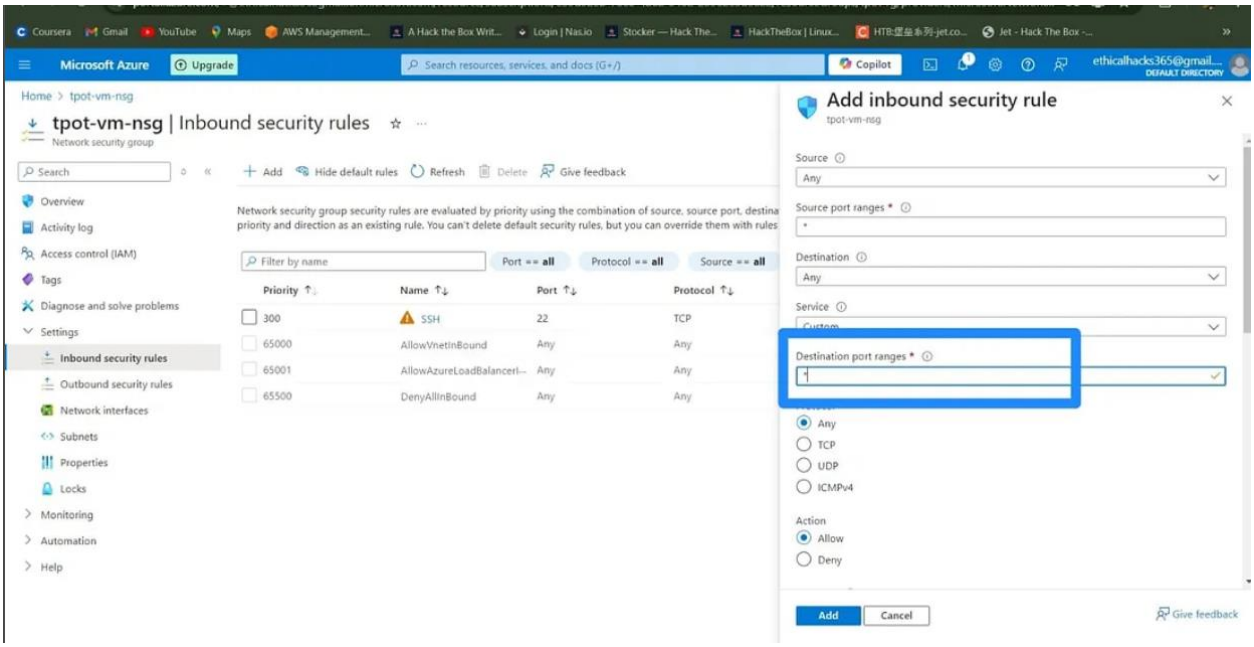
Open traffic flow

Now we need to open up the gates and create a rule to allow all communication into the honeypot. This will allow the attackers to be able to attack the honeypot, so we can collect the data. So let's start

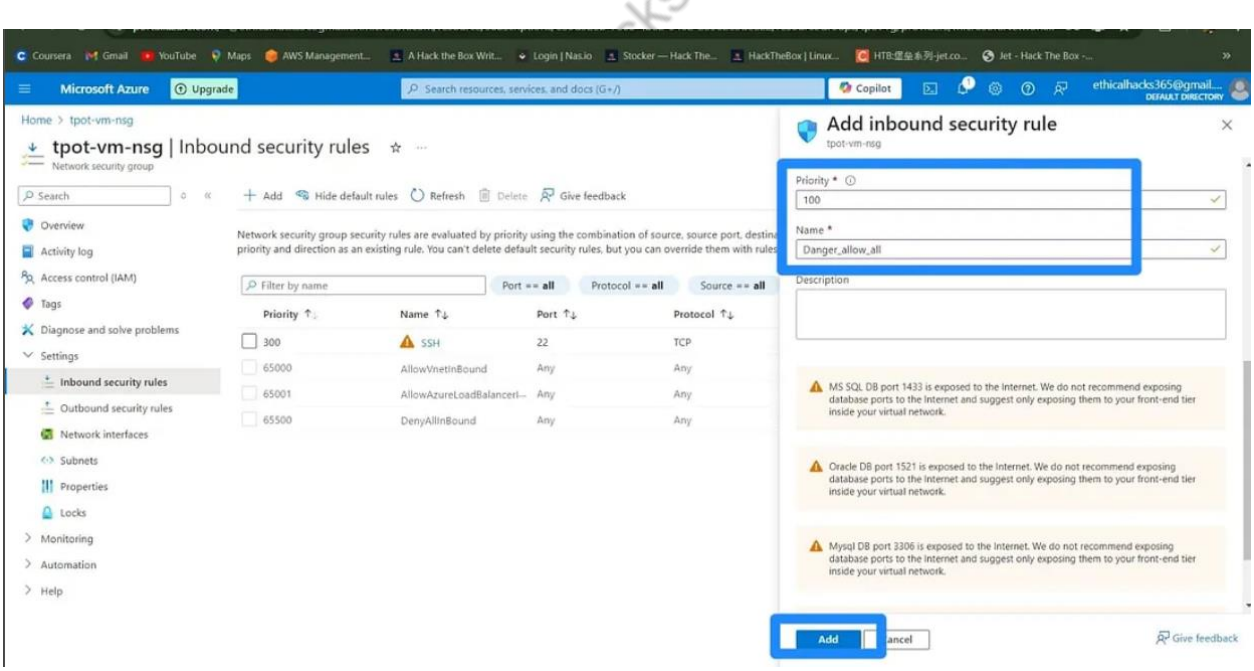
At the search bar type "*tpot-vm-nsg*" make sure you replace tpot-vm with your own vm name. and select the NSG(Network security group resource).

Now select Inbound security rules from left panel under settings and then click on Add. ↓

Now change *Destination port ranges* to "*" which means allow any port. ↓



Now scroll down and change priority to 100. Because rules are processed in priority order. Lower the number higher the priority. Change name to “Danger_allow_all”. This is customizable you can write your own warning message whatever you want. Then click on “Add” ↓



This set of rules on the NSG applies to all resources in the NSG and allows all traffics on all ports inside. This is not recommended anywhere except this project. This is not a good practice at all.

And all set. The cloud configuration part is over. Now it's high time to move to the configuration of honeypot ;)

Grab your coffee guys ☕

Configuring the honeypot

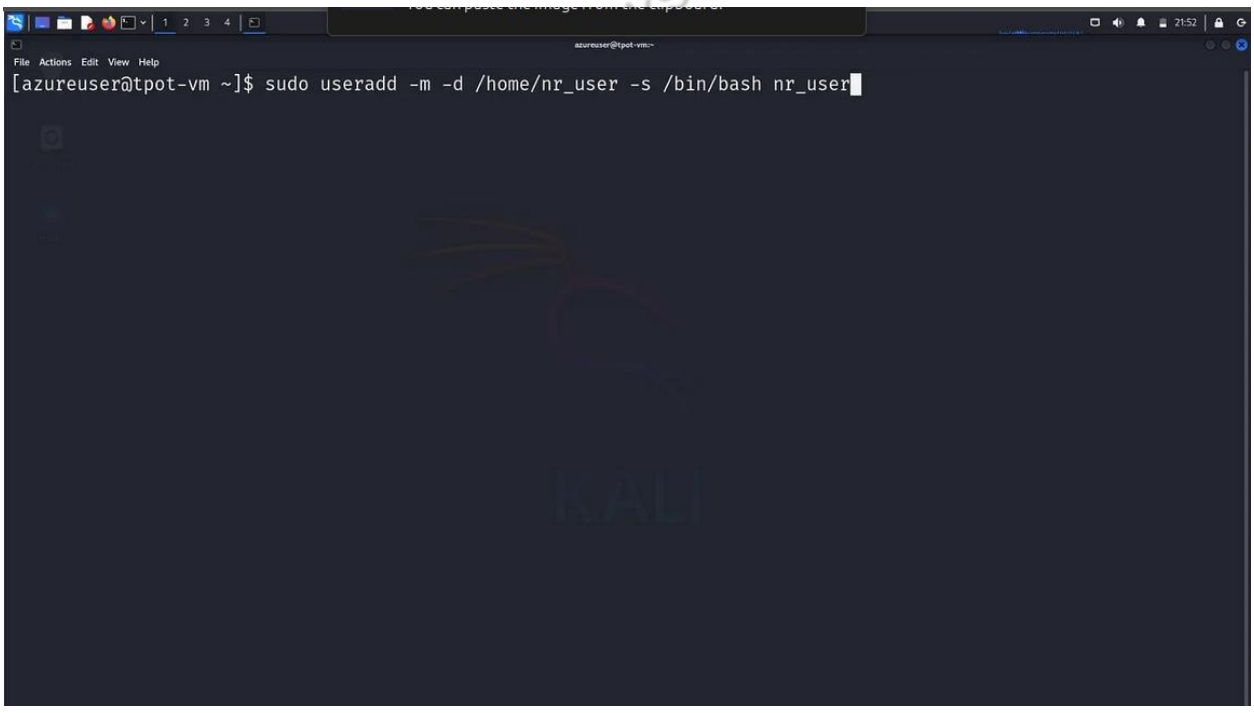
First of all copy your public IP address from your azure virtual machine. After that open your Kali linux or parrot machine or whatever you are using and login to the azure VM through ssh.

Syntax for ssh login-: ssh yourazurevmusername@publicipthatyoucopied

Now after login setup a non-root user with sudo permission.

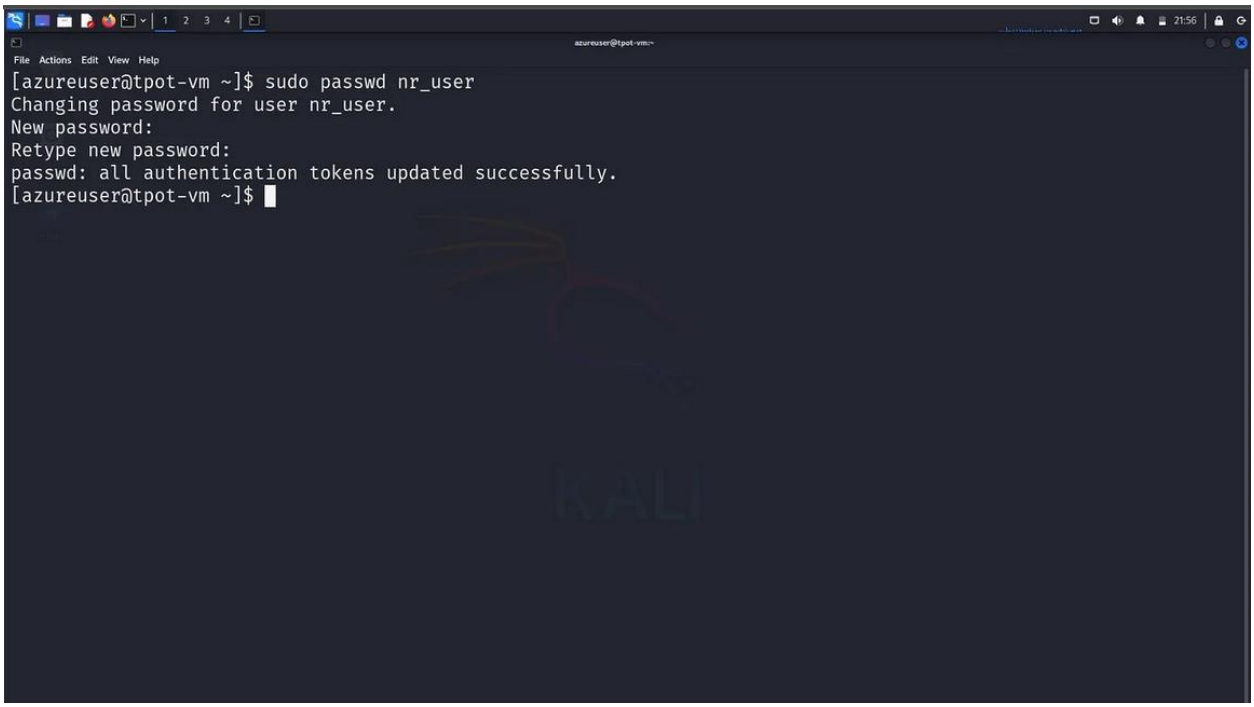
Setting up a non-root user

Syntax for creating non-root user-: sudo useradd -m -d /home/newuser -s /bin/bash newuser ↓

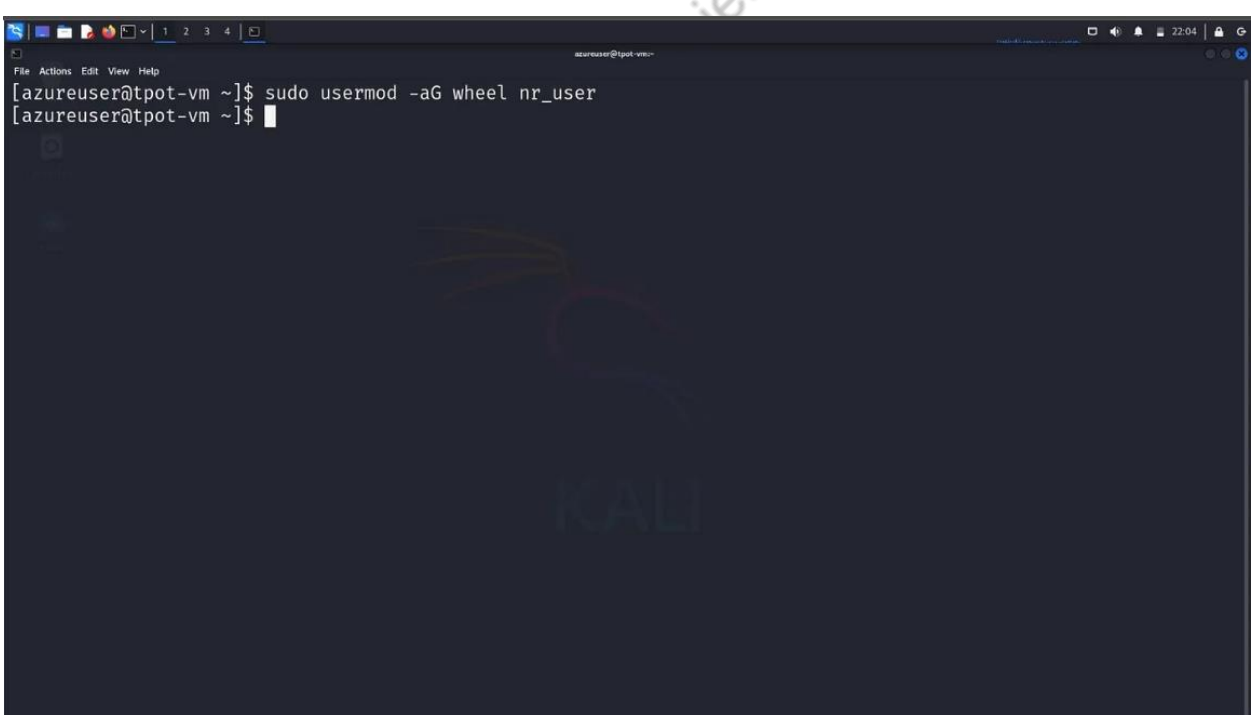


Now set password for that non-root user.

Syntax to setup password for non-root user :- sudo passwd newuser ↓



Now give that non-root user sudo privilege. Syntax-: sudo usermod -aG wheel newuser ↓



NOTE-: In AlmaLinux the non-root users can be granted sudo permission by adding them to the wheel group.

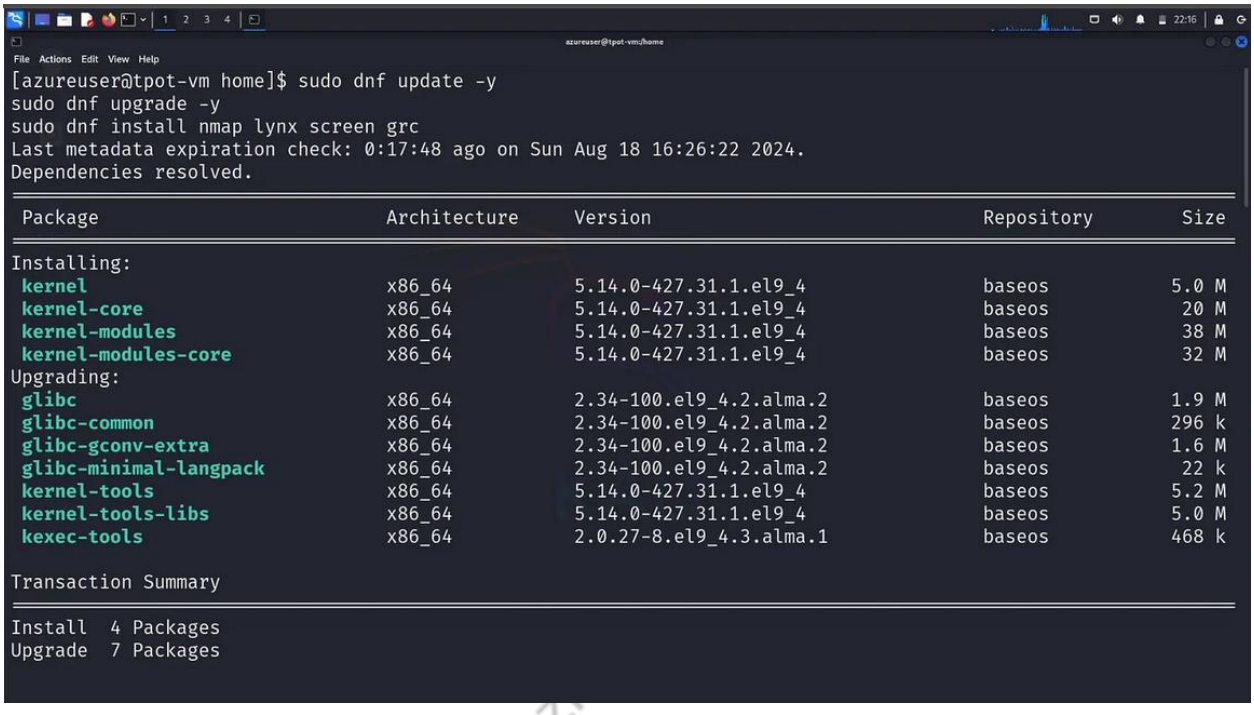
Now update the server and OS and install some packages

Follow the below commands ↓

sudo dnf update -y

sudo dnf upgrade -y

sudo dnf install nmap lynx screen grc



It’s okay if you can’t install grc,screen and lynx package but make sure you have installed nmap.

Now log in as the non-root user:-

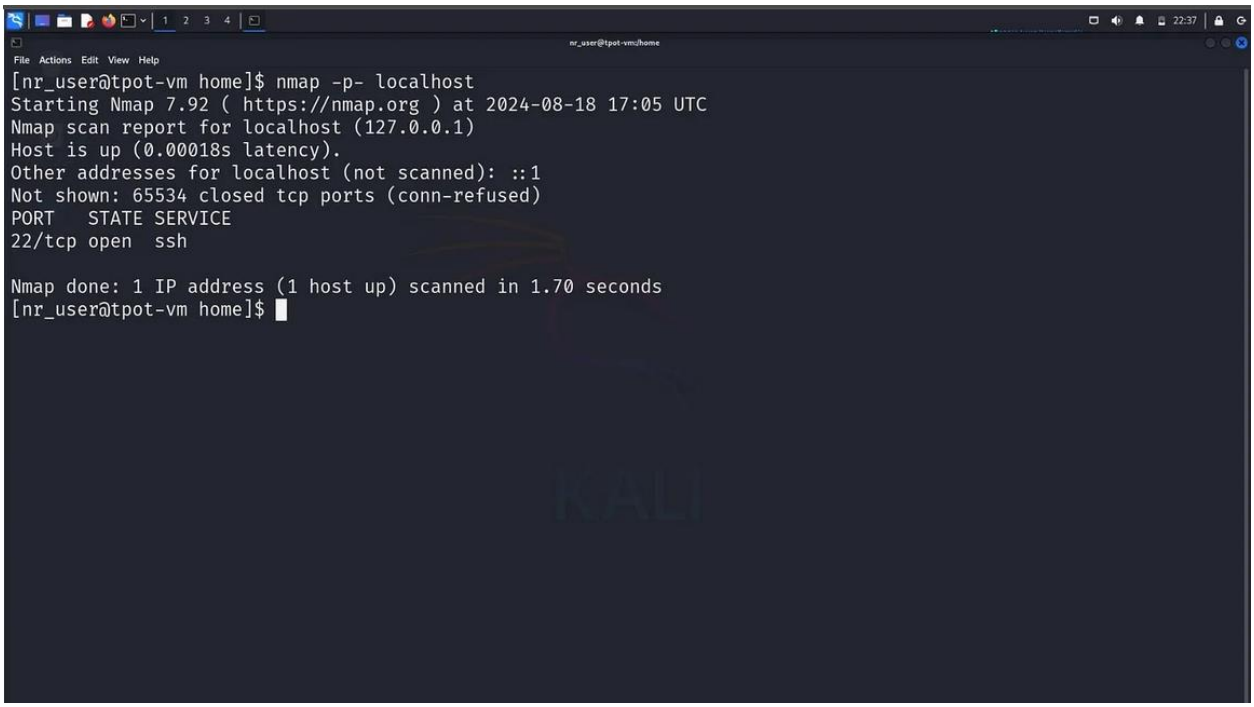
Syntax to login-: su newuser

Enter your password. ↓

Pre-install checks

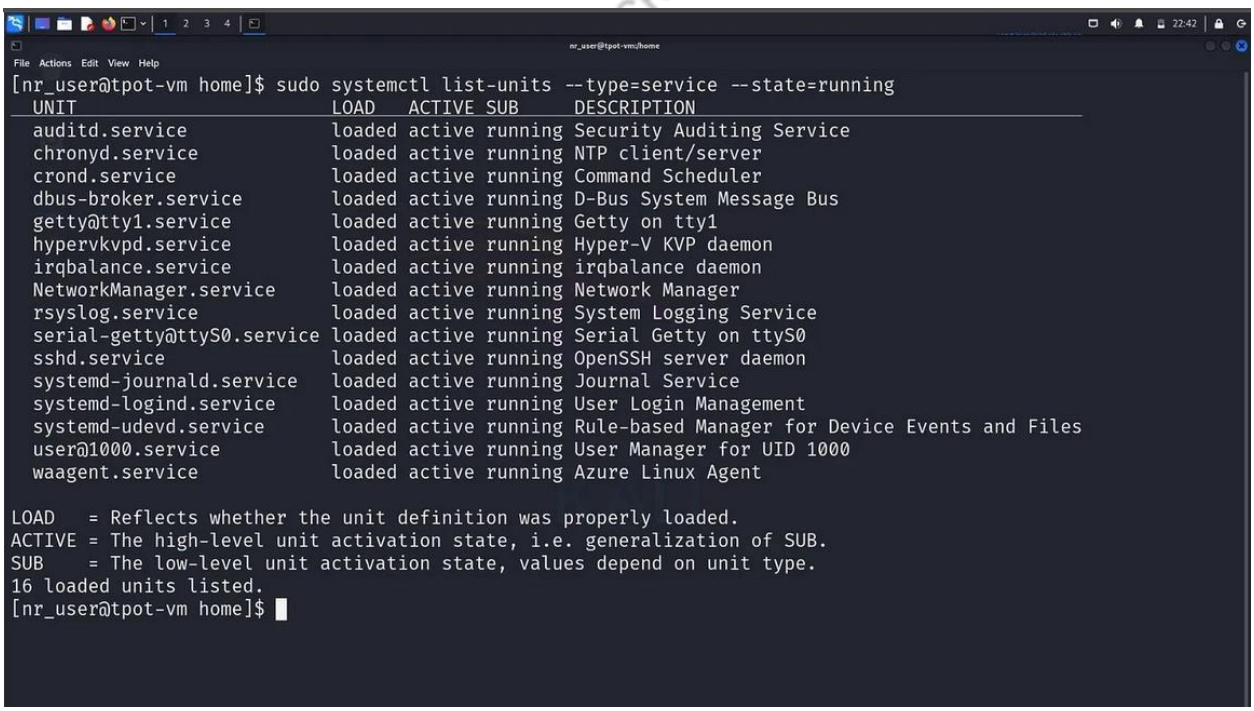
Let’s check no other ports are open other than SSH which we need for remote management.

Syntax for this:- nmap -p- localhost ↓



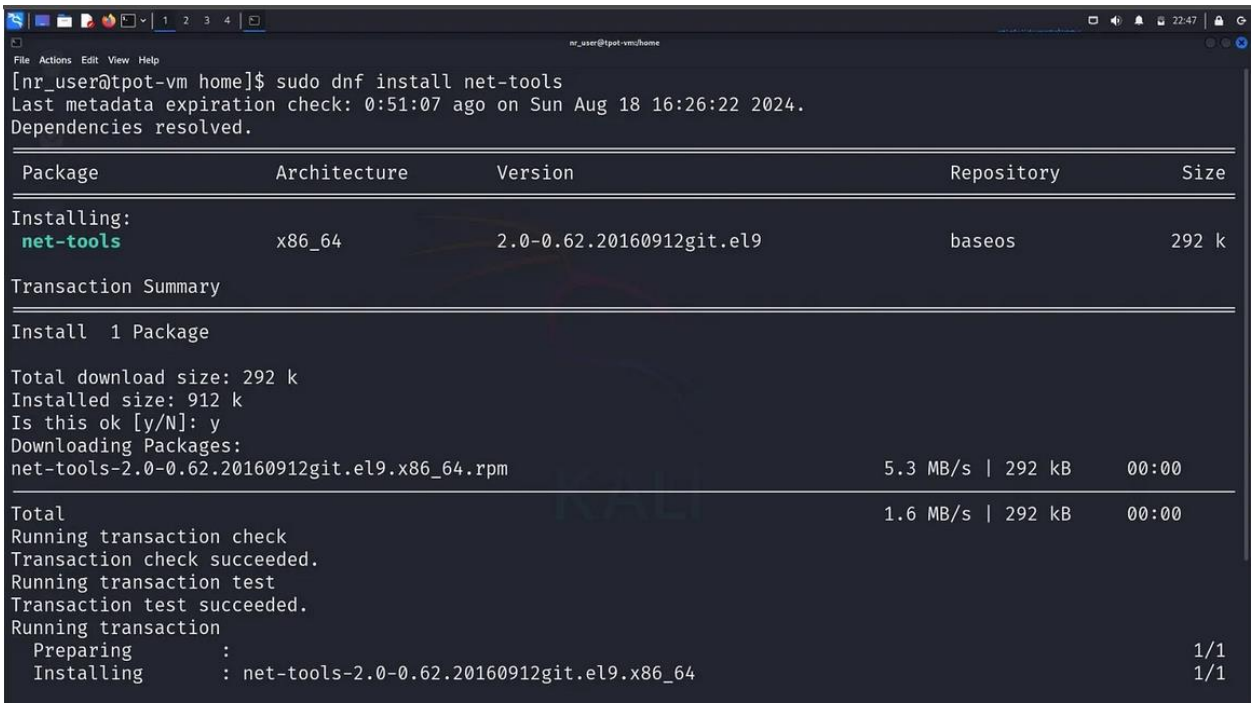
List all currently running services on your AlmaLinux system.

Syntax for this :- sudo systemctl list-units — type=service — state=running ↓



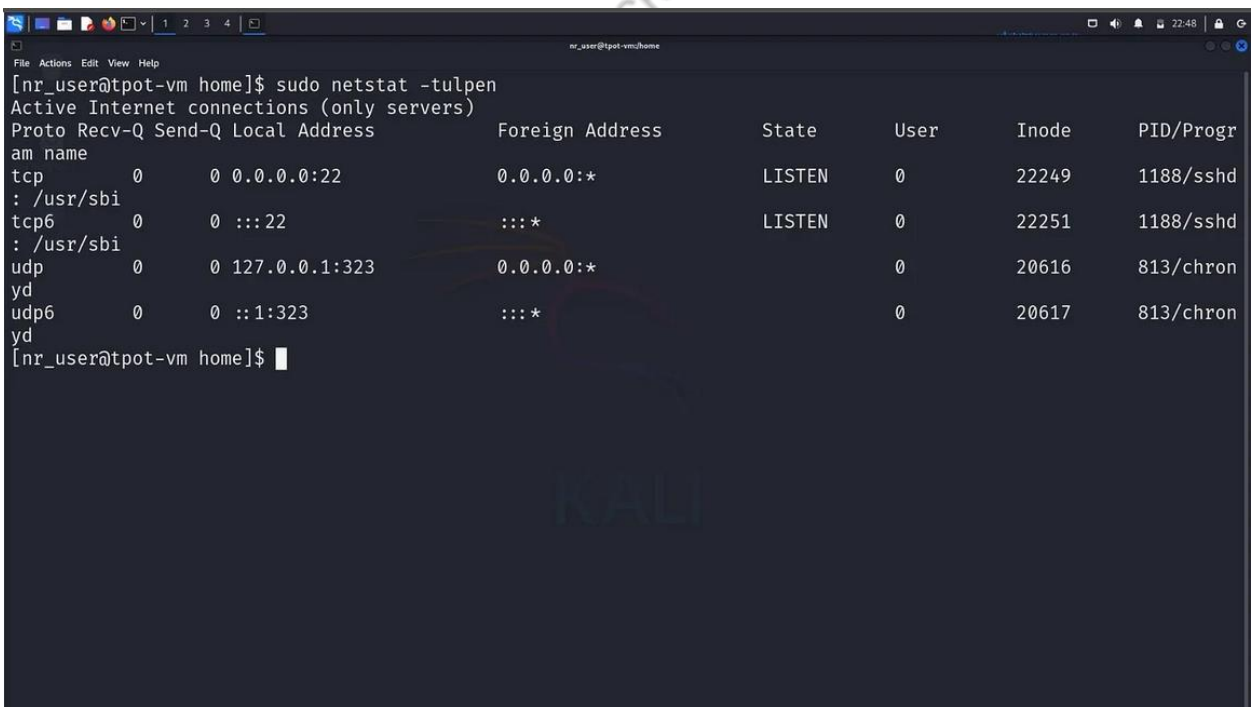
Install netstat tool to check all listening ports on your system installing T-Pot.

Syntax for this :- sudo dnf install net-tools ↓



Now check all listening ports on your system installing T-Pot.

Syntax for this :- sudo netstat -tulpen ↓



Now the show begins :)

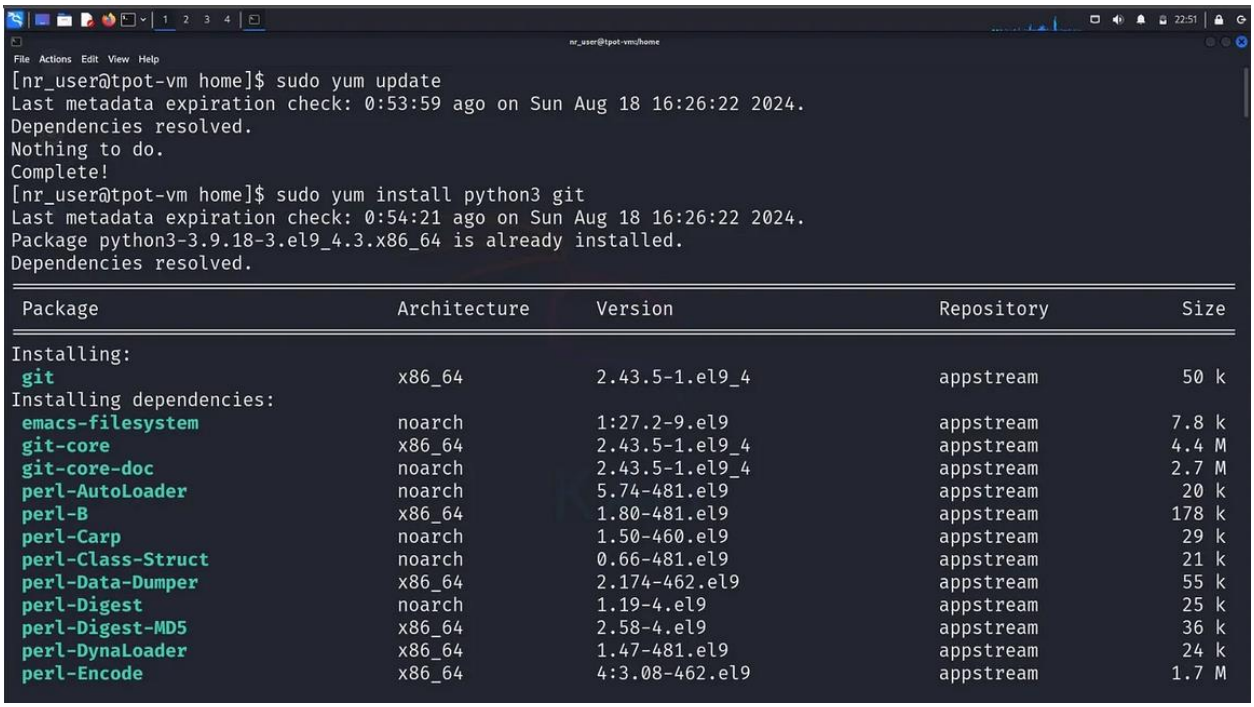
Installation of T-Pot

Install the prerequisite packages.

Follow these commands ↓

sudo yum update

sudo yum install python3 git



Clone the GitHub repository :- git clone https://github.com/telekom-security/tpotce.git ↓

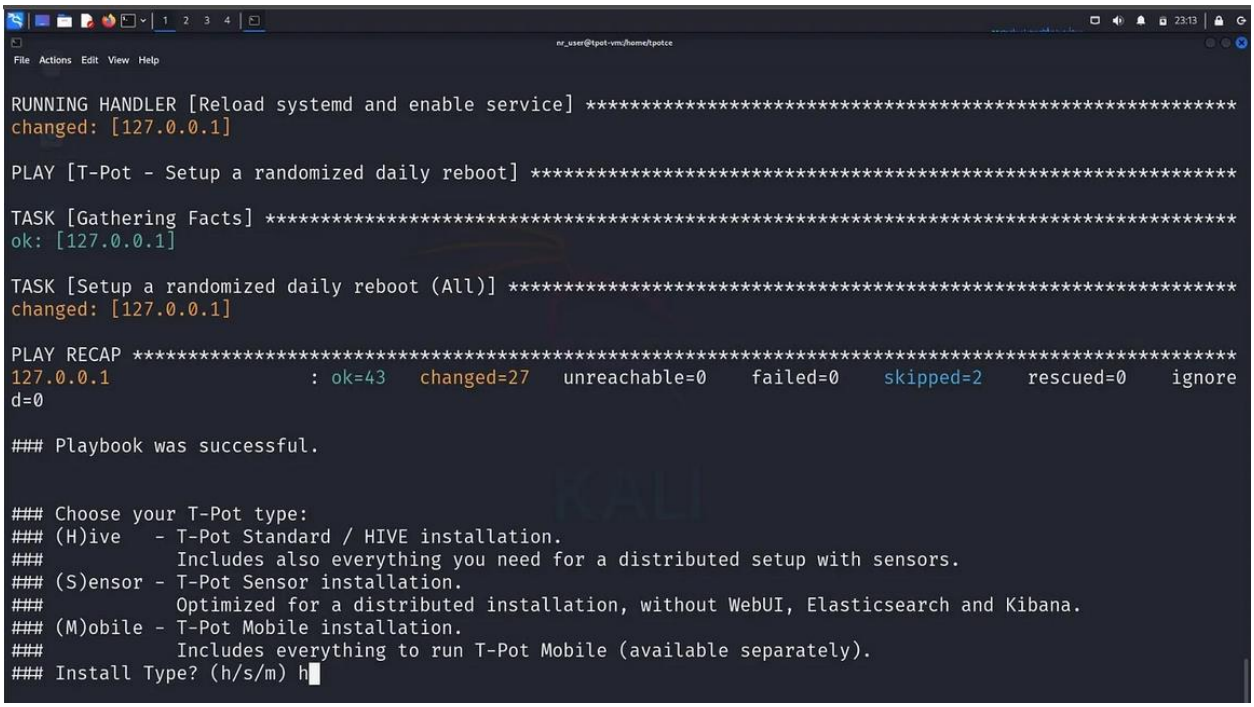
```
[nr_user@tpot-vm home]$ sudo git clone https://github.com/telekom-security/tpotce.git
Cloning into 'tpotce' ...
remote: Enumerating objects: 16162, done.
remote: Counting objects: 100% (174/174), done.
remote: Compressing objects: 100% (124/124), done.
remote: Total 16162 (delta 66), reused 139 (delta 49), pack-reused 15988 (from 1)
Receiving objects: 100% (16162/16162), 278.91 MiB | 71.78 MiB/s, done.
Resolving deltas: 100% (8988/8988), done.
[nr_user@tpot-vm home]$
```

Now browse to the tpotce folder. Syntax :- cd tpotce

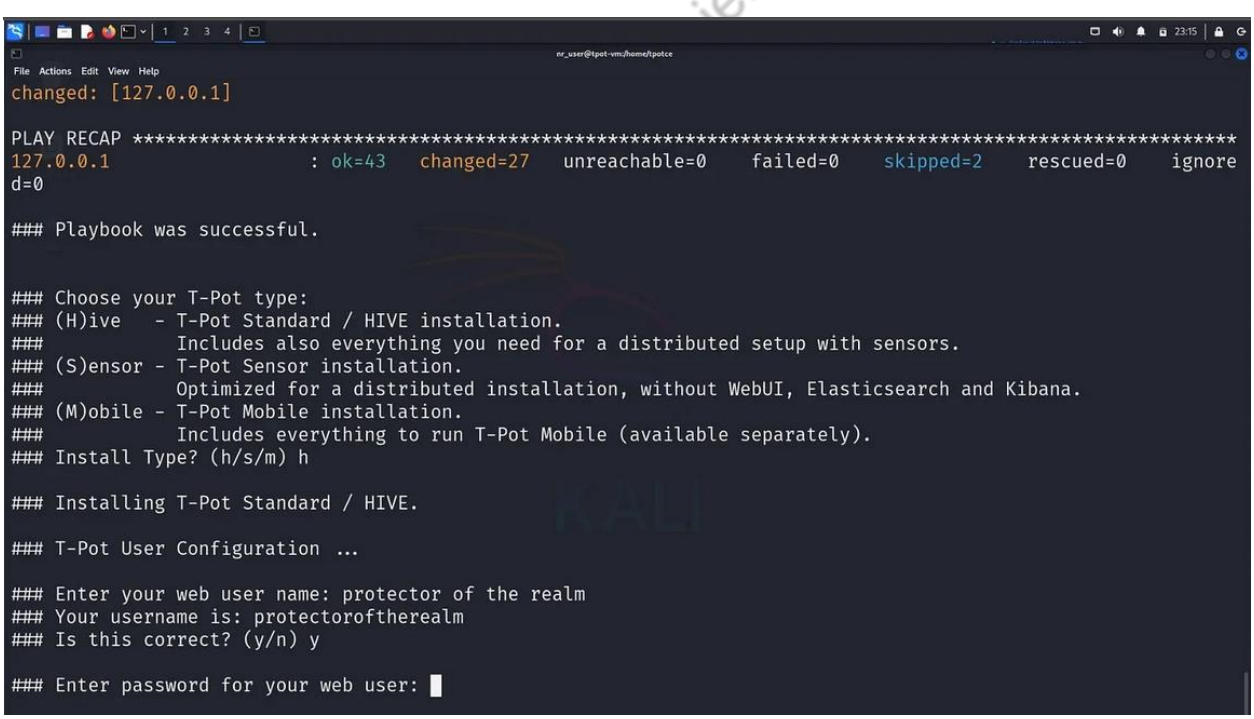
Then run ./install.sh ↓

```
[nr_user@tpot-vm tpotce]$ ./install.sh
 _____      ____        _       ___          _        _ _
|_   _|    |  _ \ ___ | |_    |_ _|_ __  ___| |_ __ _| | |
  | |_____| |_) / _ \| __|    | || '_ \/ __| __/ _` | | |
  | |_____|  __/ (_) | |_     | || | | \__ \ || (_| | | |
  |_|     |_|   \___/ \__|   |___|_| |_|___/\__\__,_|_|_|


### This script will now install T-Pot and all of its dependencies.

### Install? (y/n) y


### Now installing required packages ...

[sudo] password for nr_user:
AlmaLinux 9 - AppStream                                  32 kB/s | 4.2 kB     00:00
AlmaLinux 9 - BaseOS                                     28 kB/s | 3.8 kB     00:00
AlmaLinux 9 - Extras                                     26 kB/s | 3.3 kB     00:00
Package cracklib-2.9.6-27.el9.x86_64 is already installed.
Dependencies resolved.
================================================================================
 Package                        Architecture   Version                 Repository        Size
================================================================================
Installing:
 ansible-collection-redhat-rhel_mgmt
                                noarch         1.1.0-2.el9             appstream         46 k
 ansible-core                   x86_64         1:2.14.14-1.el9         appstream        2.2 M
```

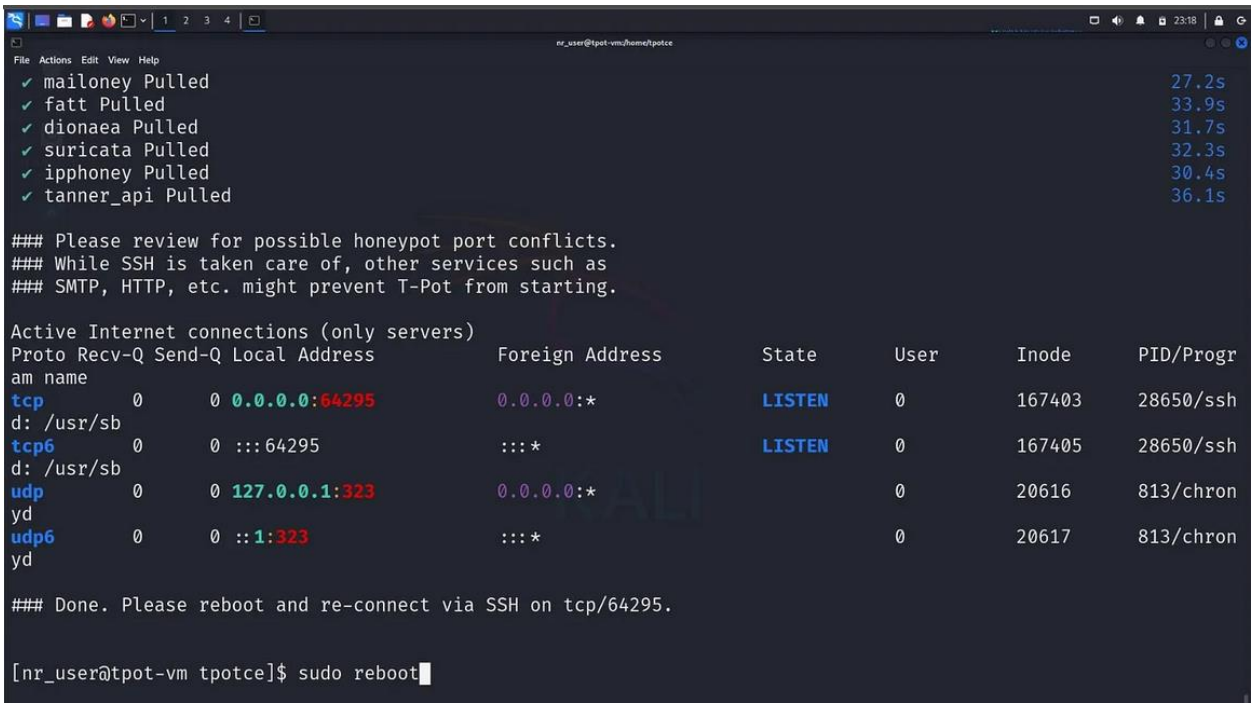
Choose h as installation type for T-Pot Standard / HIVE. ↓



Create a web username and password for your T-Pot web portal. ↓



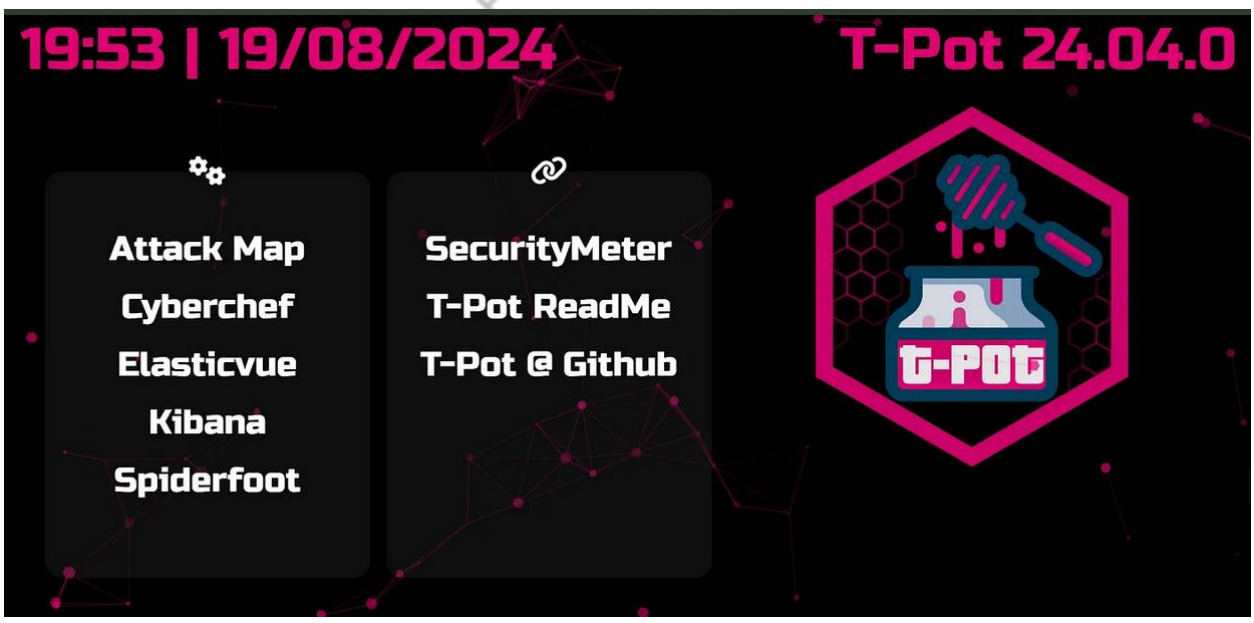
Once the installer has completed the setup successfully, it’s now time to reboot the server. ↓



And all set. Now You are ready.

T-Pot Landing Page

The T-Pot web portal runs on port 64297, head over to https://<yourpublic_ip>:64297/ and login with your newly created T-Pot web username and password. ↓



In the end explore a little t-pot feature :-

That is Kibana in T-Pot is a powerful visualization tool for exploring and analyzing Elasticsearch data, offering a variety of dashboards and visualizations tailored to T-Pot-supported honeypots.

Conclusion

Deploying **T-Pot on Azure** was more than just a technical experiment—it was a deep dive into the world of cyber deception and threat intelligence.

T-Pot proves itself as a powerful, all-in-one honeypot framework, combining multiple tools into a single, cohesive system. Its intuitive dashboards, real-time visualizations, and detailed analytics—especially through Kibana—make monitoring both insightful and engaging.

While it does require a fair amount of system resources, the return is immense. You gain real-world visibility into attack behavior, tactics, and trends—all within a safe, controlled environment. For cybersecurity learners, researchers, and professionals alike, T-Pot is not just a honeypot—it's a window into the minds of attackers.

By turning Azure into a cybersecurity trap, I've learned how attackers think, act, and evolve—and that's knowledge you can't get from textbooks alone.

Whether you're curious about threat intelligence or looking to sharpen your blue-team skills, setting up your own honeypot could be one of the most rewarding and eye-opening projects you ever take on.