

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.

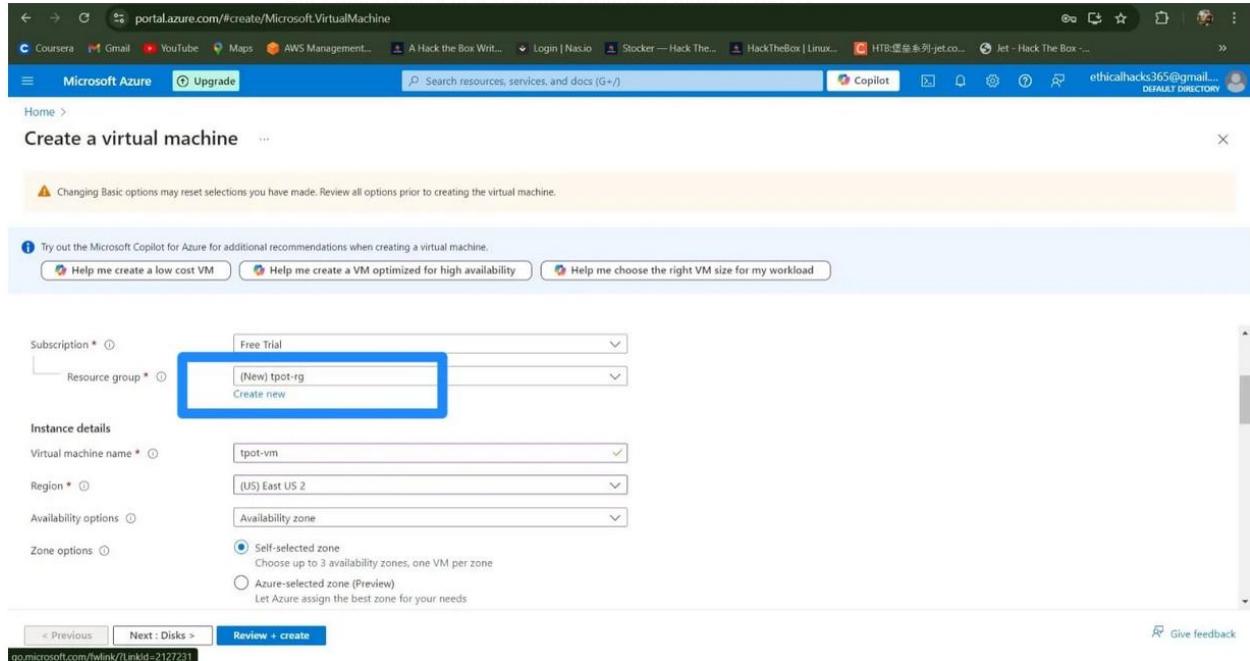
Let's start the project.

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 :)

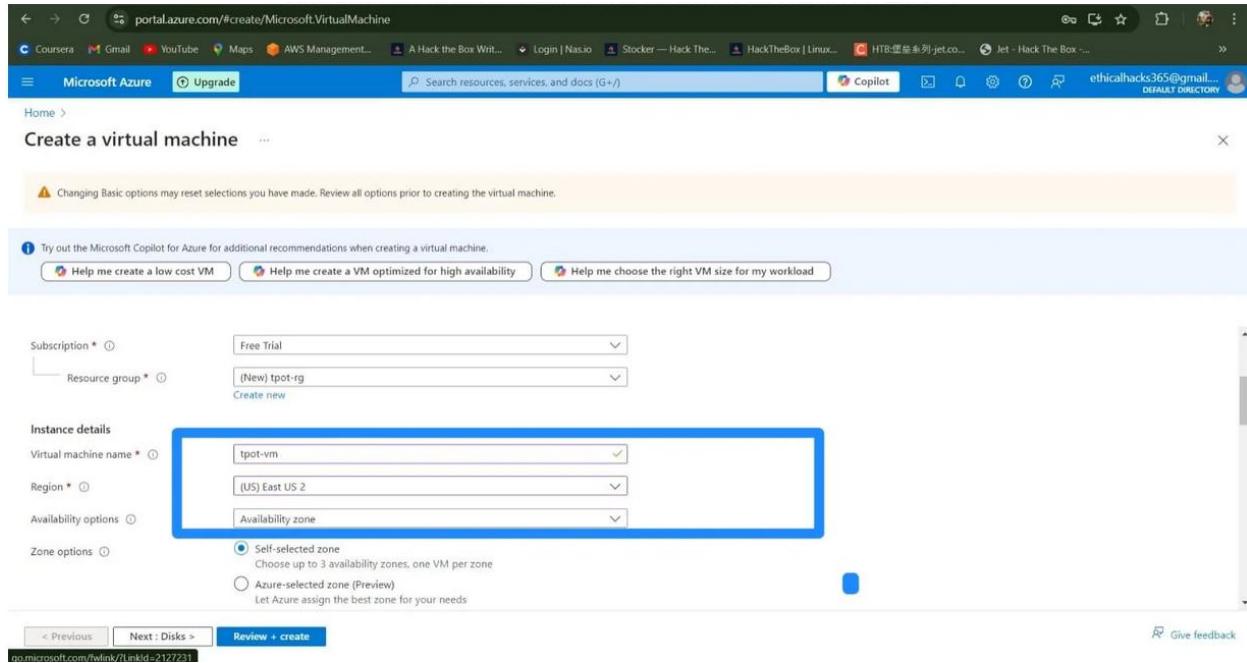
After the creation of account. At the top, search for virtual machine, then click on create VM.

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

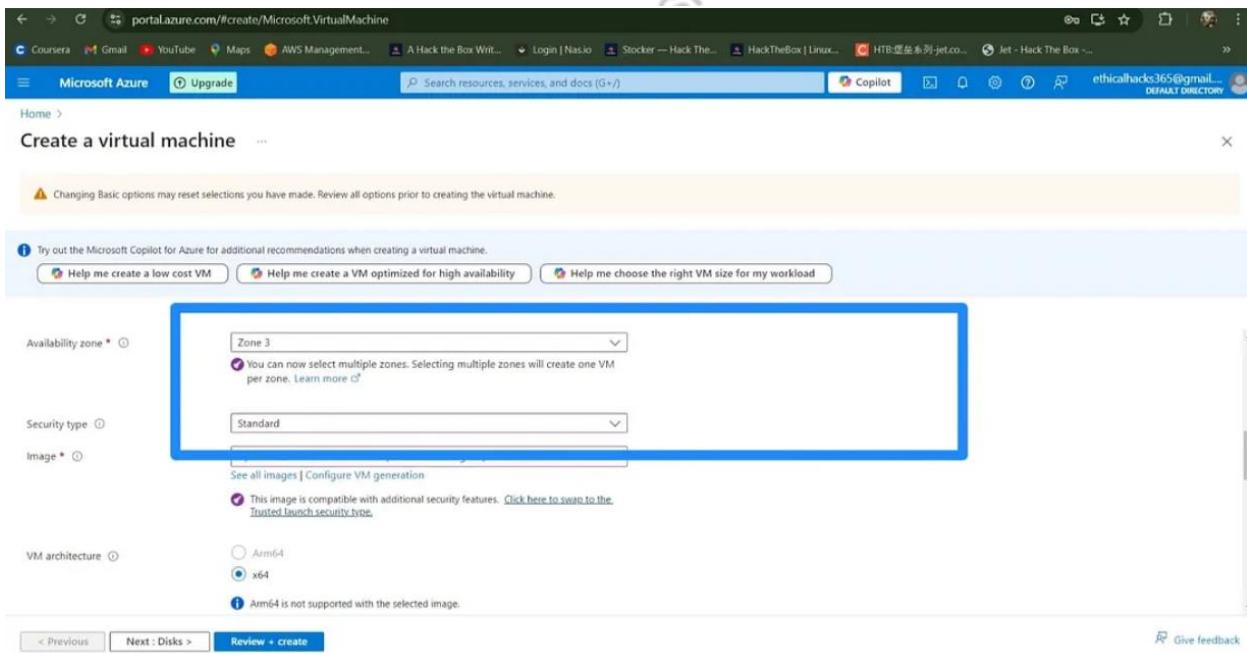


If you ever wanted to delete the entire project, just delete this resource group and everything will be erased completely.

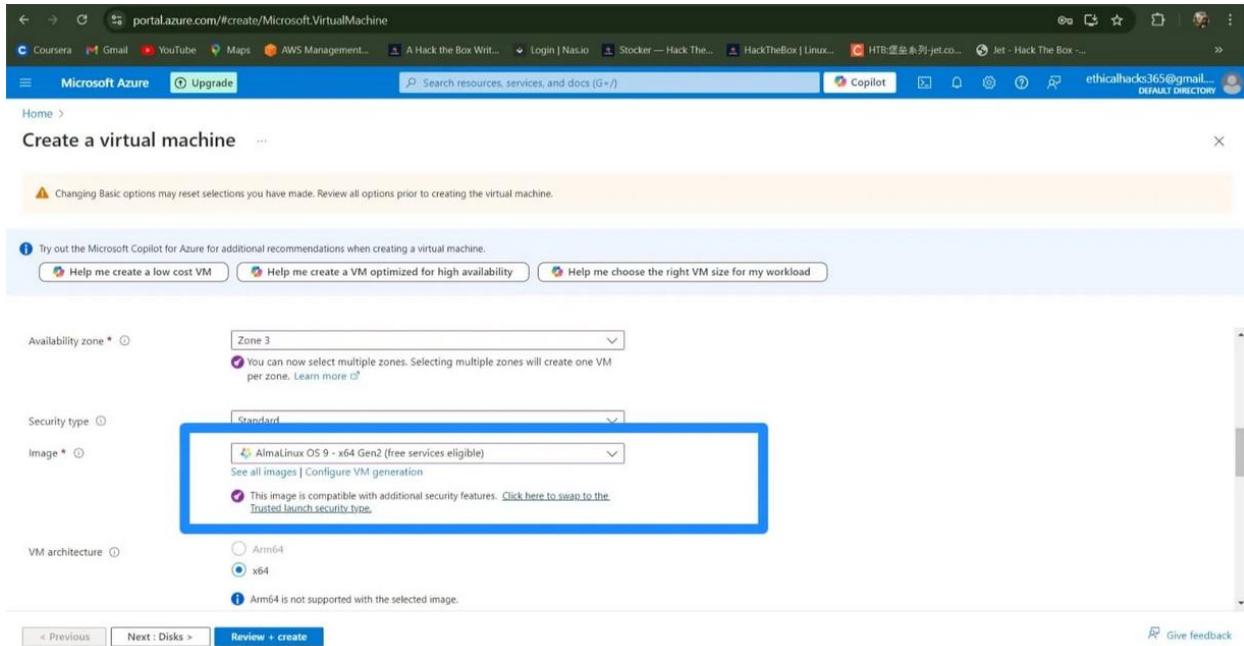
Then name the virtual machine as your choice. Set the region (*US*) EAST US 2. ↓



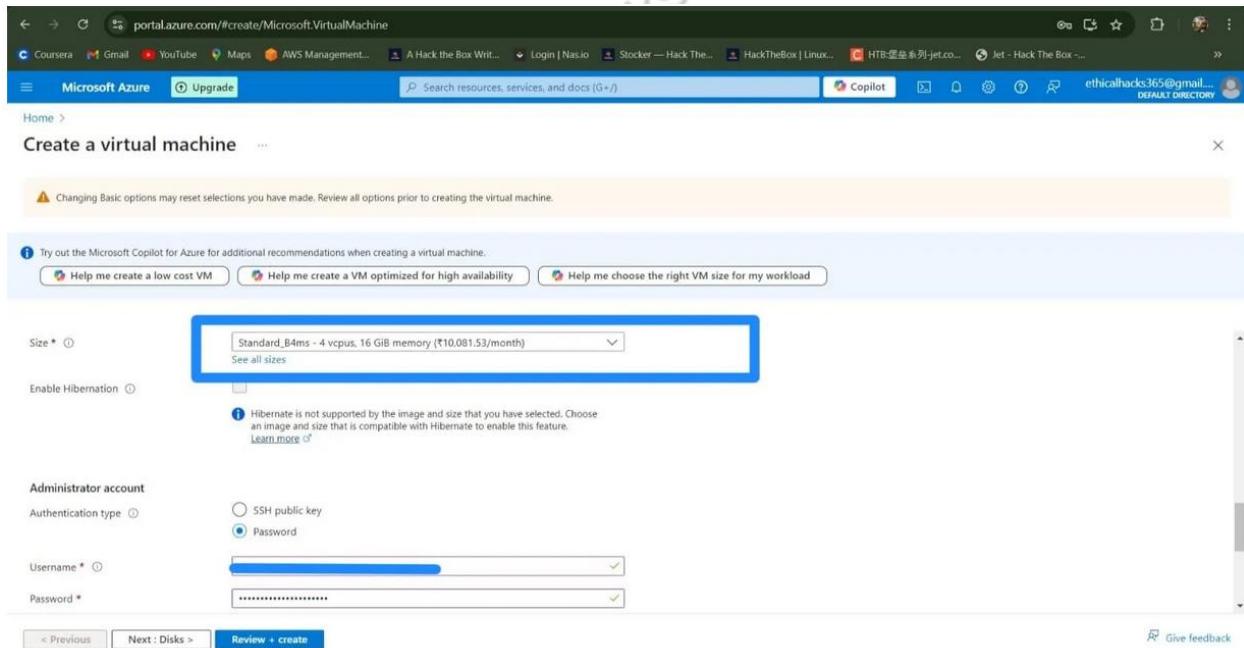
After that select the Availability zone as “Zone 3”. So that we can avail our AlmaLinux os image and our storage size. Then set the security type to *standard*. ↓



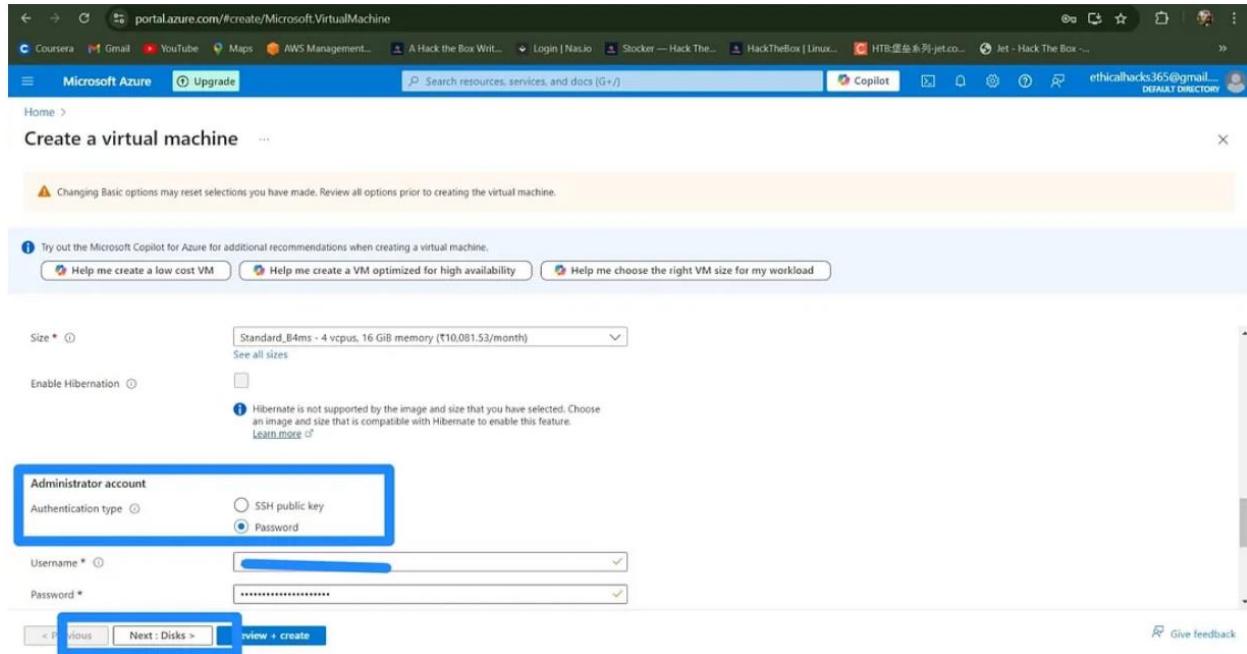
Then select the OS image *AlmaLinux OS 9 -x64 Gen2* which is completely free. ↓



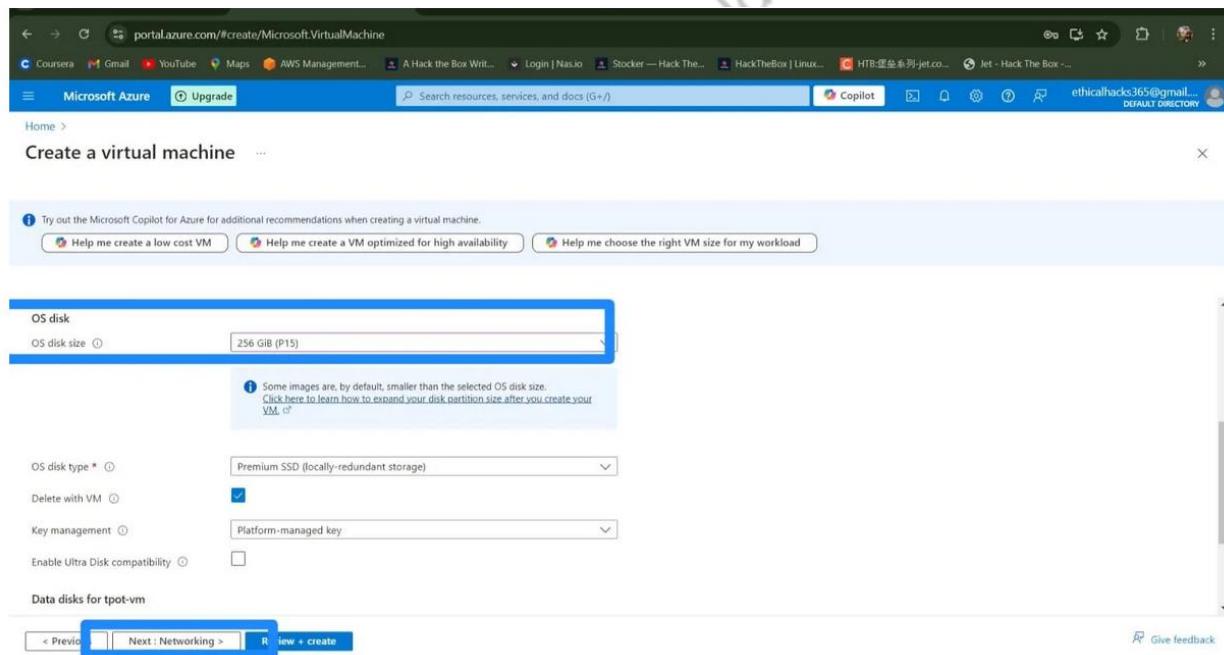
Next thing to do is choose size , here choose **Standard_B4ms-4vcpus, 16 GiB memory (10.081.53/month)**.No need to panic with the money it will be deducted from your free \$200 credit:) ↓



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.

↓

The screenshot shows the 'Create a virtual machine' wizard on the Microsoft Azure portal. The current step is 'Configure networking'. A blue box highlights the 'Delete public IP and NIC when VM is deleted' checkbox, which is checked. Below it, under 'Enable accelerated networking', there is a note: 'The resource provider 'Microsoft.Network' should be registered in order to enable accelerated networking. [Learn more](#)'.

Try out the Microsoft Copilot for Azure for additional recommendations when creating a virtual machine.

Delete public IP and NIC when VM is deleted (?)

Enable accelerated networking (?)

(i) The resource provider 'Microsoft.Network' should be registered in order to enable accelerated networking. [Learn more](#) (?)

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more (?)

Load balancing options (?)

None

Azure load balancer
Supports all TCP/UDP network traffic, port-forwarding, and outbound flows.

Application gateway
Web traffic load balancer for HTTP/HTTPS with URL-based routing, SSL

[< Previous](#) [Next : Management >](#) [Give feedback](#)

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



Validation passed

Try out the Microsoft Copilot for Azure for additional recommendations when creating a virtual machine.

Help me create a low cost VM | Help me create a VM optimized for high availability | Help me choose the right VM size for my workload

Basics

Subscription	Free Trial
Resource group	(new) tpot-rg
Virtual machine name	tpot-vm
Region	East US 2
Availability options	Availability zone
Zone options	Self-selected zone
Availability zone	3
Security type	Standard
Image	AlmaLinux OS 9 - Gen2
VM architecture	x64
Size	Standard B4ms (4 vcpus, 16 GiB memory)
Enable Hibernation	No
Authentication type	Password

< Previous | Next > | Create | Download a template for automation | Give feedback

Validation passed

Try out the Microsoft Copilot for Azure for additional recommendations when creating a virtual machine.

Help me create a low cost VM | Help me create a VM optimized for high availability | Help me choose the right VM size for my workload

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Price

1 X Standard B4ms by Microsoft
Subscription credits apply ⓘ
13.8103 INR/hr
Pricing for other VM sizes

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.

< Previous | Next > | Create | Download a template for automation | Give feedback

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.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with various links like Coursera, Gmail, YouTube, Maps, AWS Management, A Hack The Box Writeup, Login | Nastio, Stocker — Hack The Box, HackTheBox | Linux, HTB:堡垒系列-Jet..., and Jet - Hack The Box. Below the navigation bar, the main header says "Microsoft Azure" and "Upgrade". A search bar is present with the placeholder "Search resources, services, and docs (G+)".

The main content area is titled "CreateVm-almalinux.almalinux-x86_64-9-gen2-20240818185708 | Overview". On the left, there's a sidebar with tabs: "Overview" (which is selected), "Inputs", "Outputs", and "Template". Above the sidebar, there are buttons for "Delete", "Cancel", "Redeploy", "Download", and "Refresh".

The main content area displays a message: "*** Deployment is in progress ***". It shows deployment details: Deployment name: CreateVm-almalinux.almalinux-x86_64-9-gen2..., Start time: 8/18/2024, 9:05:02 PM, Subscription: Free Trial, Resource group: tspot-rg, and Correlation ID: 1e0f... (partially obscured). There's also a progress bar indicating the deployment is in progress.

On the right side of the page, there are several promotional banners:

- Microsoft Defender for Cloud**: Secure your apps and infrastructure. [Go to Microsoft Defender for Cloud >](#)
- Free Microsoft tutorials**: Start learning today! [Start learning today >](#)
- Work with an expert**: Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support. [Find an Azure expert >](#)

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 “*tspot-vm-nsg*” make sure you replace *tspot-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

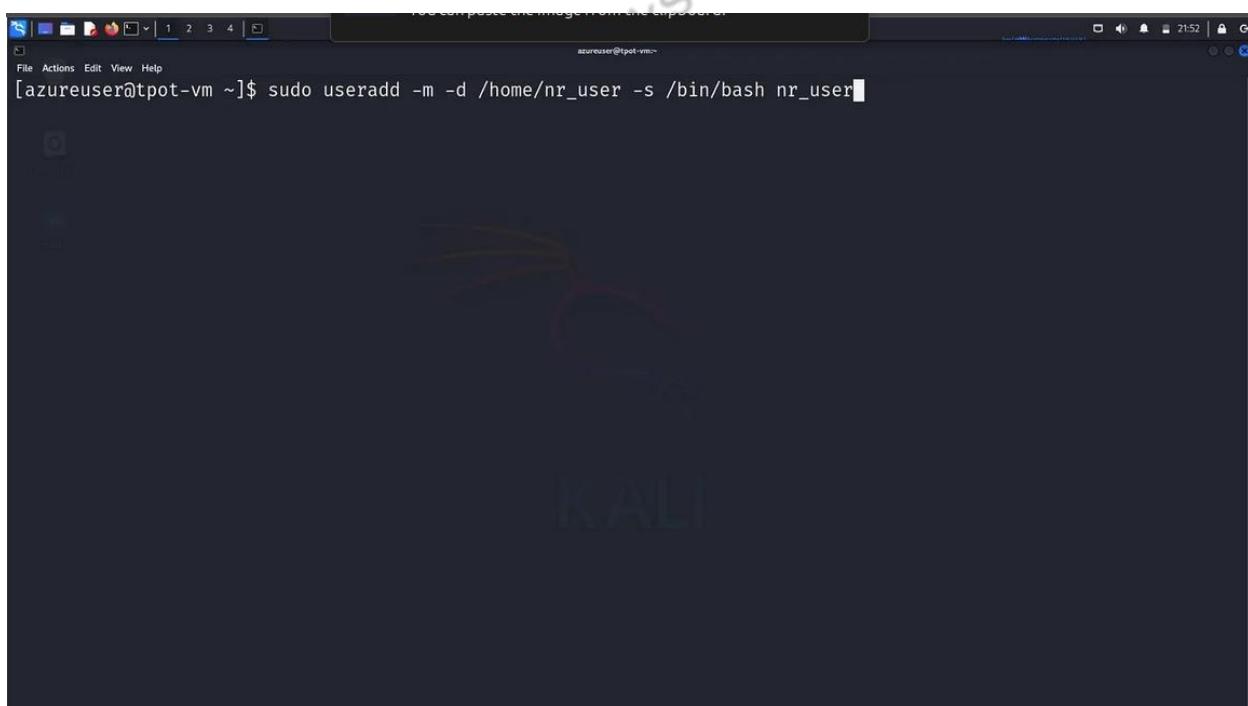
First of all copy your public IP address from your azure virtual machine. After that open your Kali linux or parrot machine or whatever you are using and login to the azure VM through ssh.

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 ↓



A screenshot of a terminal window on a Kali Linux desktop. The window title is 'Terminal'. The terminal prompt shows 'azureuser@tpt-vm ~]\$'. Below the prompt, the command 'sudo useradd -m -d /home/nr_user -s /bin/bash nr_user' is typed and partially visible in the input field. The background of the desktop shows a colorful Kali logo watermark.

Now set password for that non-root user.

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

```
[azureuser@tpot-vm ~]$ sudo passwd nr_user
Changing password for user nr_user.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[azureuser@tpot-vm ~]$
```

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

```
[azureuser@tpot-vm ~]$ sudo usermod -aG wheel nr_user
[azureuser@tpot-vm ~]$
```

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
```

```
[azureuser@tpot-vm ~]$ sudo dnf update -y
[sudo] password for azureuser:
Last metadata expiration check: 0:17:48 ago on Sun Aug 18 16:26:22 2024.
Dependencies resolved.

Package           Architecture   Version      Repository  Size
=====
Installing:
kernel           x86_64        5.14.0-427.31.1.el9_4    baseos      5.0 M
kernel-core       x86_64        5.14.0-427.31.1.el9_4    baseos      20 M
kernel-modules    x86_64        5.14.0-427.31.1.el9_4    baseos      38 M
kernel-modules-core x86_64        5.14.0-427.31.1.el9_4    baseos      32 M
Upgrading:
glibc            x86_64        2.34-100.el9_4.2.alma.2  baseos      1.9 M
glibc-common      x86_64        2.34-100.el9_4.2.alma.2  baseos      296 k
glibc-gconv-extra x86_64        2.34-100.el9_4.2.alma.2  baseos      1.6 M
glibc-minimal-langpack x86_64        2.34-100.el9_4.2.alma.2  baseos      22 k
kernel-tools     x86_64        5.14.0-427.31.1.el9_4    baseos      5.2 M
kernel-tools-libs x86_64        5.14.0-427.31.1.el9_4    baseos      5.0 M
kexec-tools      x86_64        2.0.27-8.el9_4.3.alma.1  baseos      468 k

Transaction Summary

Install  4 Packages
Upgrade  7 Packages
```

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. ↓



A screenshot of a terminal window titled "nr_user@tpot-vm:home". The window shows a command-line interface with the following text:
[azureuser@tpot-vm home]\$ su nr_user
Password:
[nr_user@tpot-vm home]\$ █

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 ↴

```
[nr_user@tpot-vm home]$ nmap -p- localhost
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-18 17:05 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00018s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 65534 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds
[nr_user@tpot-vm home]$
```

List all currently running services on your AlmaLinux system.

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

```
[nr_user@tpot-vm home]$ sudo systemctl list-units --type=service --state=running
UNIT                  LOAD   ACTIVE SUB   DESCRIPTION
audited.service        loaded  active running Security Auditing Service
chronyd.service        loaded  active running NTP client/server
crond.service          loaded  active running Command Scheduler
dbus-broker.service   loaded  active running D-Bus System Message Bus
getty@tty1.service     loaded  active running Getty on tty1
hypervkvpd.service    loaded  active running Hyper-V KVP daemon
irqbalance.service    loaded  active running irqbalance daemon
NetworkManager.service loaded  active running Network Manager
rsyslog.service        loaded  active running System Logging Service
serial-getty@ttyS0.service loaded  active running Serial Getty on ttyS0
sshd.service           loaded  active running OpenSSH server daemon
systemd-journald.service loaded  active running Journal Service
systemd-logind.service loaded  active running User Login Management
systemd-udevd.service  loaded  active running Rule-based Manager for Device Events and Files
user@1000.service      loaded  active running User Manager for UID 1000
waagent.service         loaded  active running Azure Linux Agent

LOAD   = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB   = The low-level unit activation state, values depend on unit type.
16 loaded units listed.
[nr_user@tpot-vm home]$
```

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

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

```
[nr_user@tpot-vm home]$ sudo dnf install net-tools
Last metadata expiration check: 0:51:07 ago on Sun Aug 18 16:26:22 2024.
Dependencies resolved.

Transaction Summary

Install 1 Package

Total download size: 292 k
Installed size: 912 k
Is this ok [y/N]: y
Downloading Packages:
net-tools-2.0-0.62.20160912git.el9.x86_64.rpm           5.3 MB/s | 292 kB   00:00

Total                                         1.6 MB/s | 292 kB   00:00

Preparing :                               1/1
Installing : net-tools-2.0-0.62.20160912git.el9.x86_64      1/1
```

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

Syntax for this :- sudo netstat -tulpen ↴

```
[nr_user@tpot-vm home]$ sudo netstat -tulpen
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      User       Inode PID/Progr
am name
tcp     0      0 0.0.0.0:22              0.0.0.0:*            LISTEN    0        22249  1188/sshd
: /usr/sbi
tcp6    0      0 :::22                  ::::*               LISTEN    0        22251  1188/sshd
: /usr/sbi
udp     0      0 127.0.0.1:323         0.0.0.0:*            LISTEN    0        20616  813/chron
yd
udp6    0      0 ::1:323                ::::*               LISTEN    0        20617  813/chron
yd
[nr_user@tpot-vm home]$
```

Now the show begins :)

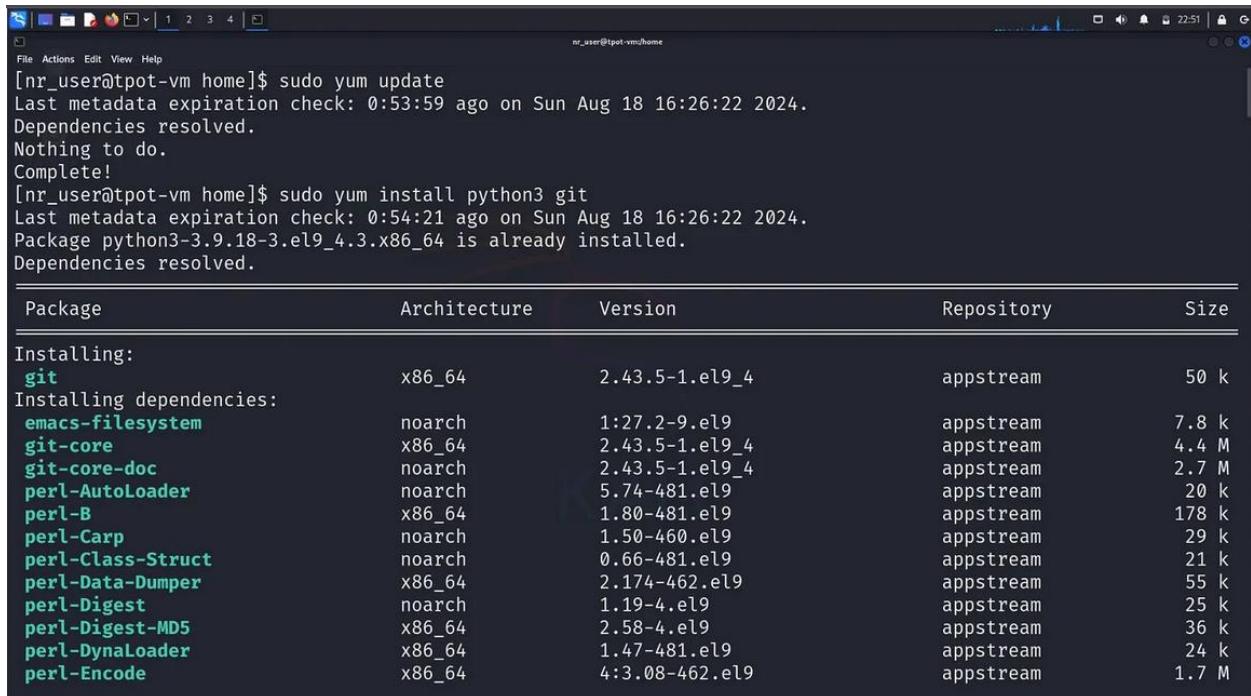
Installation of T-Pot

Install the prerequisite packages.

Follow these commands ↓

`sudo yum update`

`sudo yum install python3 git`



```
[nr_user@tpot-vm home]$ sudo yum update
Last metadata expiration check: 0:53:59 ago on Sun Aug 18 16:26:22 2024.
Dependencies resolved.
Nothing to do.
Complete!
[nr_user@tpot-vm home]$ sudo yum install python3 git
Last metadata expiration check: 0:54:21 ago on Sun Aug 18 16:26:22 2024.
Package python3-3.9.18-3.el9_4.x86_64 is already installed.
Dependencies resolved.
```

Package	Architecture	Version	Repository	Size
Installing:				
<code>git</code>	x86_64	2.43.5-1.el9_4	appstream	50 k
Installing dependencies:				
<code>emacs-filesystem</code>	noarch	1:27.2-9.el9	appstream	7.8 k
<code>git-core</code>	x86_64	2.43.5-1.el9_4	appstream	4.4 M
<code>git-core-doc</code>	noarch	2.43.5-1.el9_4	appstream	2.7 M
<code>perl-AutoLoader</code>	noarch	5.74-481.el9	appstream	20 k
<code>perl-B</code>	x86_64	1.80-481.el9	appstream	178 k
<code>perl-Carp</code>	noarch	1.50-460.el9	appstream	29 k
<code>perl-Class-Struct</code>	noarch	0.66-481.el9	appstream	21 k
<code>perl-Data-Dumper</code>	x86_64	2.174-462.el9	appstream	55 k
<code>perl-Digest</code>	noarch	1.19-4.el9	appstream	25 k
<code>perl-Digest-MD5</code>	x86_64	2.58-4.el9	appstream	36 k
<code>perl-DynaLoader</code>	x86_64	1.47-481.el9	appstream	24 k
<code>perl-Encode</code>	x86_64	4:3.08-462.el9	appstream	1.7 M

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 tptce folder. Syntax :- cd tptce

Then run `./install.sh` ↓

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

```
File Actions Edit View Help nr_user@tpot-vm:~/home/tpotce
RUNNING HANDLER [Reload systemd and enable service] *****
changed: [127.0.0.1]

PLAY [T-Pot - Setup a randomized daily reboot] *****
TASK [Gathering Facts] *****
ok: [127.0.0.1]

TASK [Setup a randomized daily reboot (All)] *****
changed: [127.0.0.1]

PLAY RECAP *****
127.0.0.1 : ok=43    changed=27    unreachable=0    failed=0    skipped=2    rescued=0    ignore
d=0

### Playback was successful.

### Choose your T-Pot type:
### (H)ive - T-Pot Standard / HIVE installation.
###           Includes also everything you need for a distributed setup with sensors.
### (S)ensor - T-Pot Sensor installation.
###           Optimized for a distributed installation, without WebUI, Elasticsearch and Kibana.
### (M)oile - T-Pot Mobile installation.
###           Includes everything to run T-Pot Mobile (available separately).
### Install Type? (h/s/m) h
```

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

```
File Actions Edit View Help nr_user@tpot-vm:~/home/tpotce
changed: [127.0.0.1]

PLAY RECAP *****
127.0.0.1 : ok=43    changed=27    unreachable=0    failed=0    skipped=2    rescued=0    ignore
d=0

### Playback was successful.

### Choose your T-Pot type:
### (H)ive - T-Pot Standard / HIVE installation.
###           Includes also everything you need for a distributed setup with sensors.
### (S)ensor - T-Pot Sensor installation.
###           Optimized for a distributed installation, without WebUI, Elasticsearch and Kibana.
### (M)oile - T-Pot Mobile installation.
###           Includes everything to run T-Pot Mobile (available separately).
### Install Type? (h/s/m) h

### Installing T-Pot Standard / HIVE.

### T-Pot User Configuration ...

### Enter your web user name: protector of the realm
### Your username is: protectoroftherealm
### Is this correct? (y/n) y

### Enter password for your web user: █
```

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

```

File Actions Edt View Help
✓ mailoney Pulled
✓ fatt Pulled
✓ dionaea Pulled
✓ suricata Pulled
✓ ipponey Pulled
✓ tanner_api Pulled

27.2s
33.9s
31.7s
32.3s
30.4s
36.1s

## Please review for possible honeypot port conflicts.
## While SSH is taken care of, other services such as
## SMTP, HTTP, etc. might prevent T-Pot from starting.

Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State   User   Inode PID/Progr
am name
tcp      0      0 0.0.0.0:64295            0.0.0.0:*          LISTEN  0     167403 28650/ssh
d: /usr/sb
tcp6     0      0 :::64295                ::::*          LISTEN  0     167405 28650/ssh
d: /usr/sb
udp      0      0 127.0.0.1:323            0.0.0.0:*          0     20616   813/chron
yd
udp6     0      0 ::1:323                 ::::*          0     20617   813/chron
yd

## Done. Please reboot and re-connect via SSH on tcp/64295.

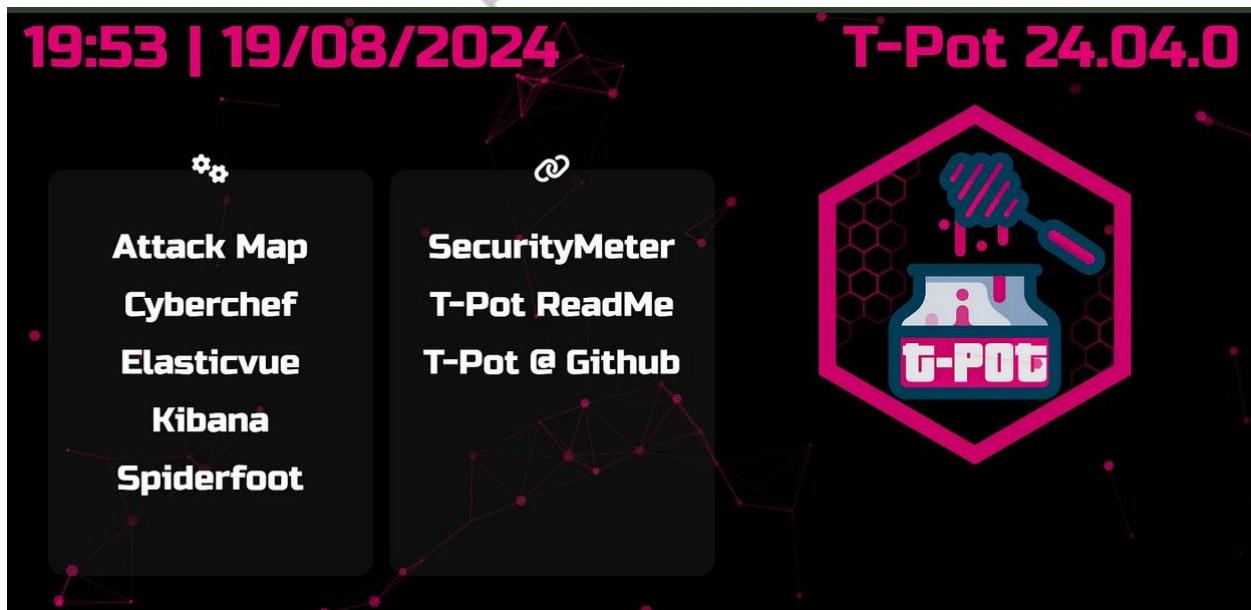
[nr_user@tpot-vm tpotce]$ sudo reboot

```

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.

FiazHackshield