INFRASTUCTURE DEPLOYMENT

GROUP 2

GROUP MEMBERS

Srishti Anand (301313123052)
Roshan Sahu (301313123044)
Rahul Kumar Gupta (301313123039)
Subham Gupta (301313123053)
Leman Kumar Sahu (301313123034)
Aryan (301313123010)

PROJECT DESCRIPTION

Overview

In this project, students will act as the Infrastructure Team of a simulated company.
They will deploy a small-scale enterprise environment using the Microsoft Azure Student Account, consisting of three Linux-based virtual machines.
This phase focuses ONLY on building the core infrastructure and enabling basic logging.

Objective

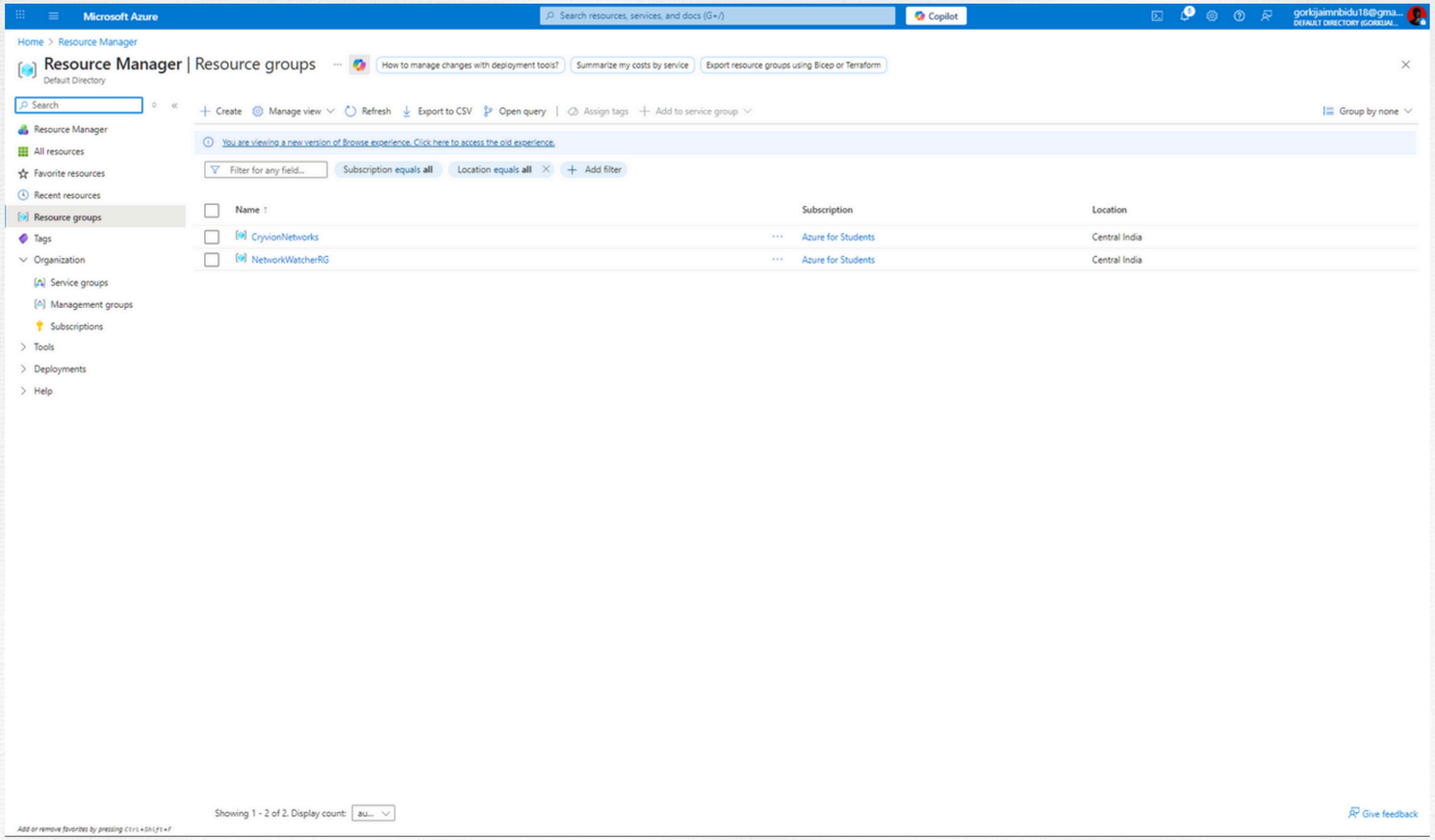
To design and deploy a functional but intentionally unsecured mini-company infrastructure using Linux servers on Azure, enable basic event logging, and prepare the environment for cyber-attacks and SOC analysis in the next phase.

PHASE - 1

CREATE RESOURCE GROUP

The objective for each group of the project is clearly defined and the resource group name should be same as the designated one.
For group 2 it is the same as Cryvion Network.

The following screenshot shows the creation of the Resource group, Cryvion Network.

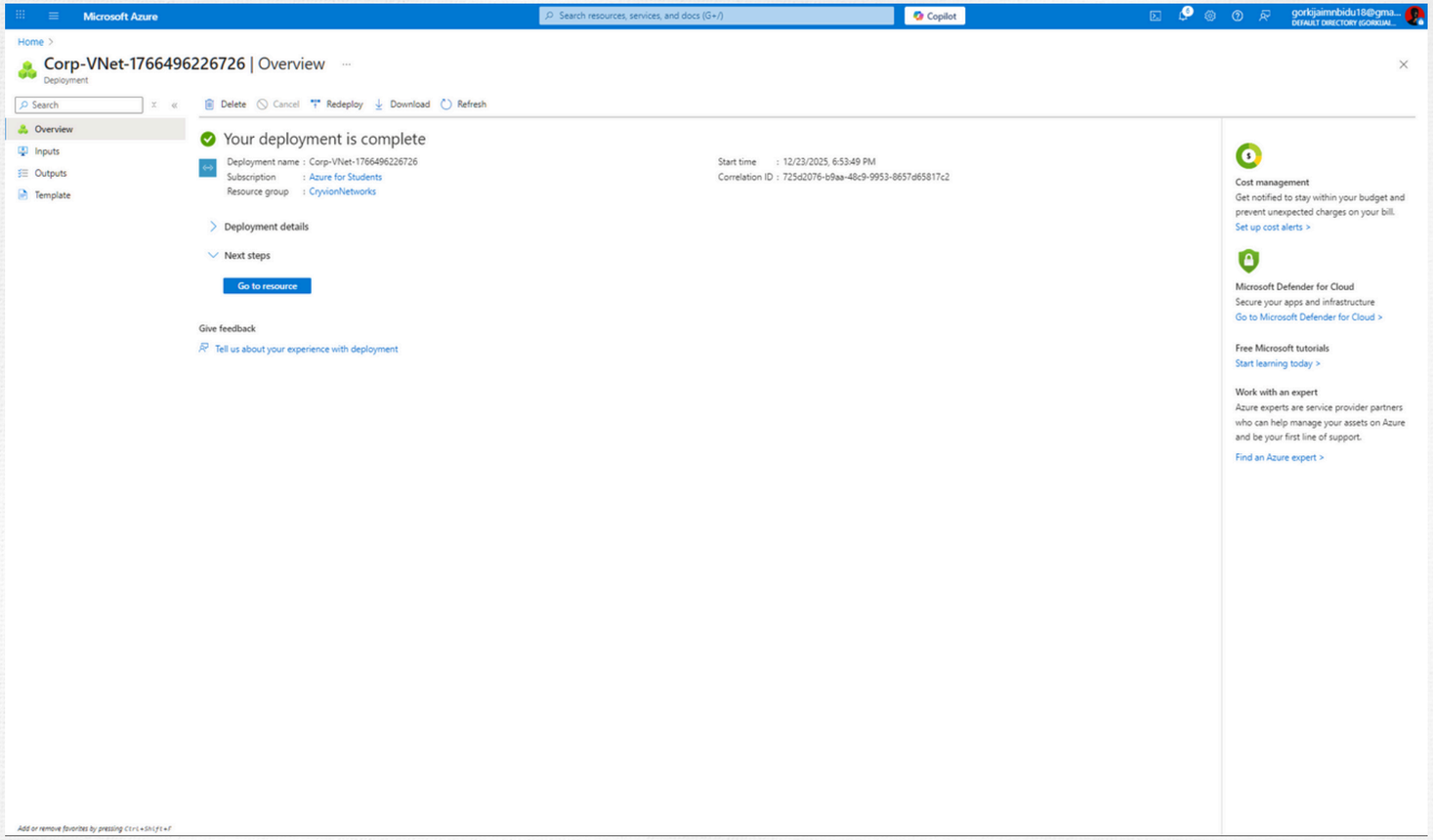


PHASE - 2

CREATE VIRTUAL NETWORK (A)

The virtual machines also require the creation of an isolated environment to work in.

The following screenshot shows the creation of the Virtual network called Corp-VNet.

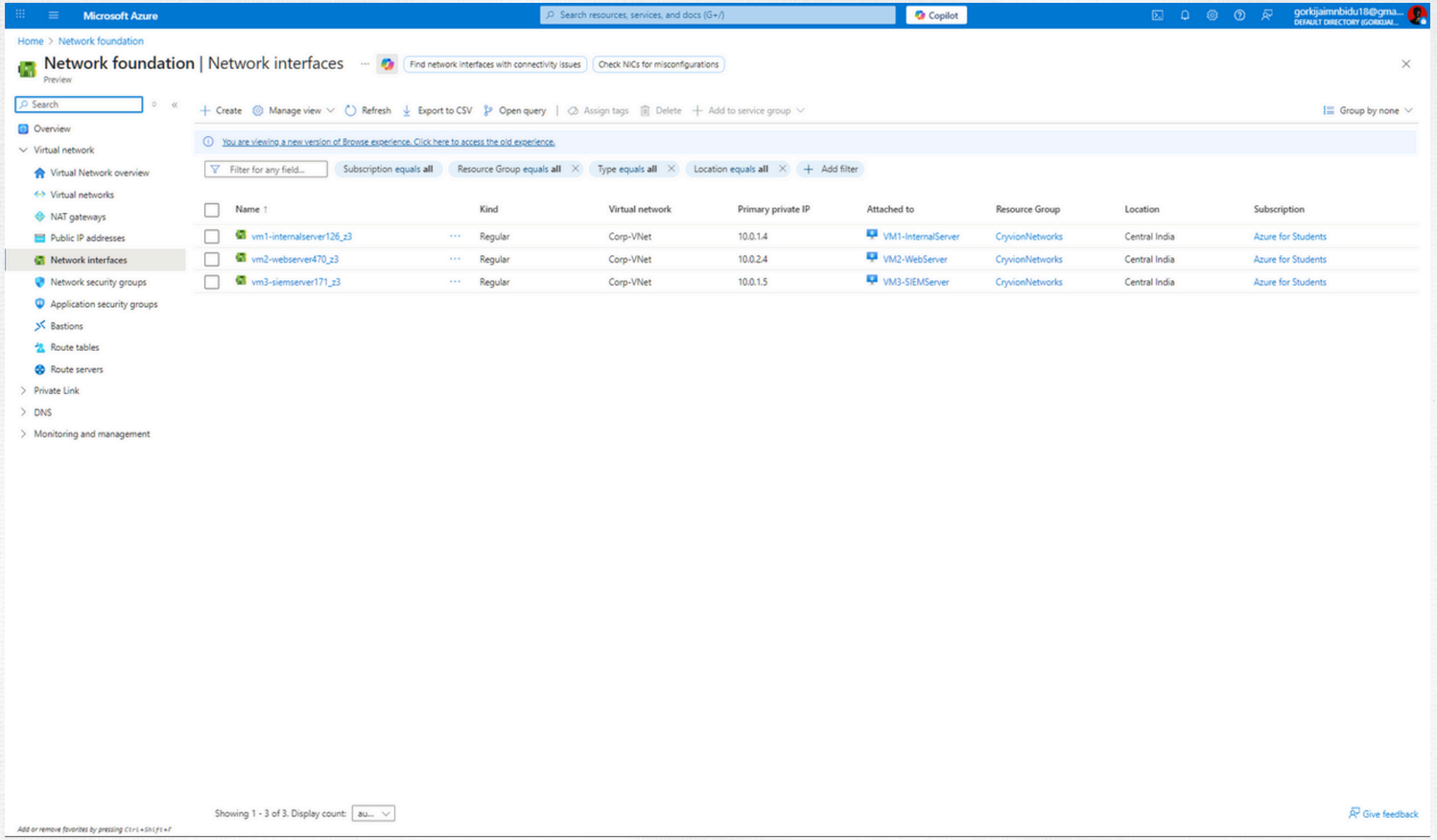


PHASE - 2

CREATE VIRTUAL NETWORK (B)

The virtual machines which will be created will need to have IP addresses on the same subnet for two of the three virtual machines whereas one of the VM’s will be on a separate subnet.

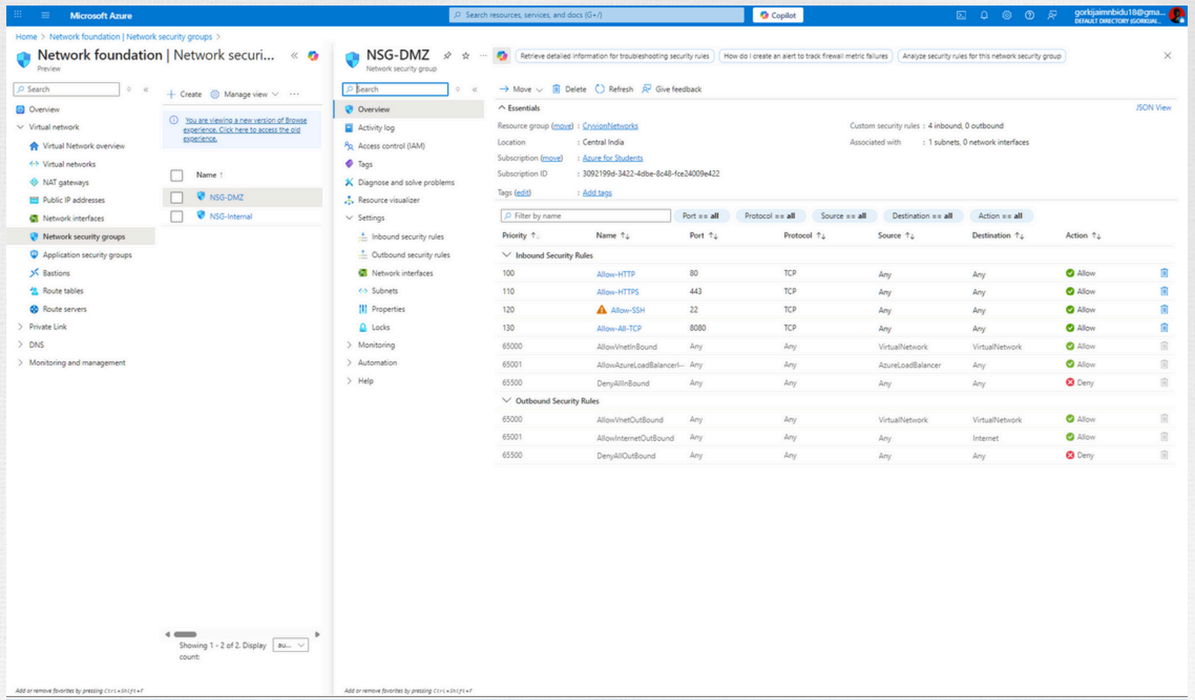
The following screenshot shows the creation of the 3 subnets for 3 separate VM’s.

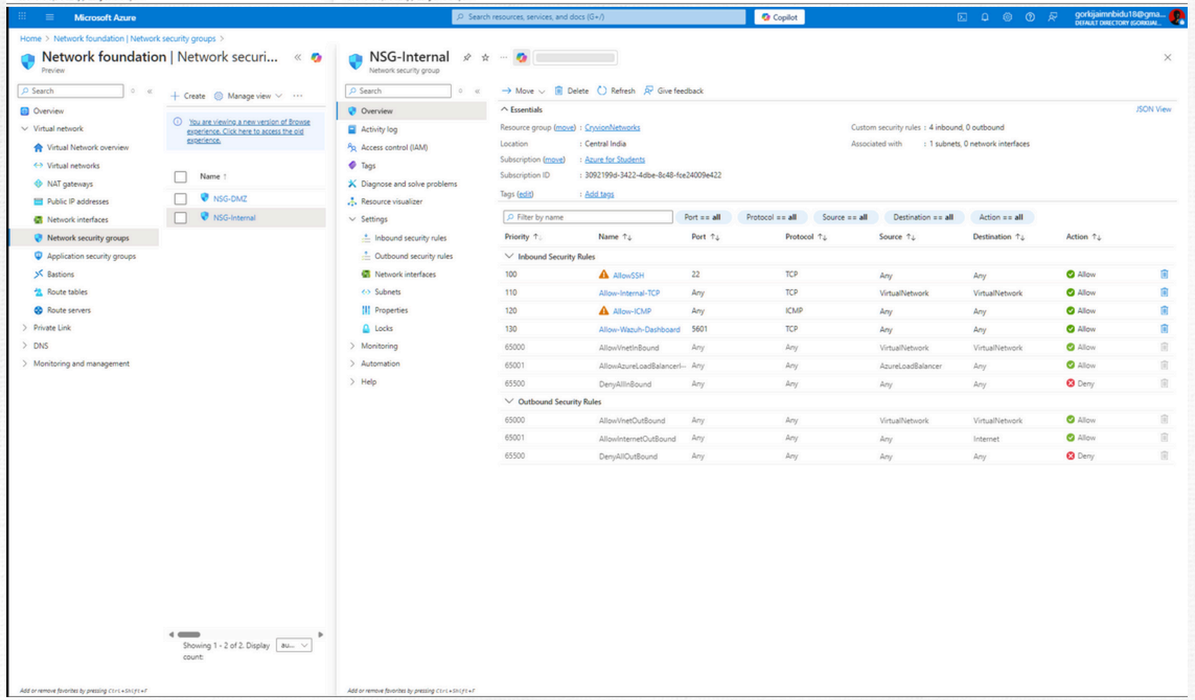


PHASE - 2
CREATE VIRTUAL NETWORK (C)

While creating the subnets we would also require separate Network Security Groups for all the machines, namely one group for the DMZ server and another for the Internal Server and the SIEM Workstation.

The following screenshot shows the creation of the 2 Network security Groups.



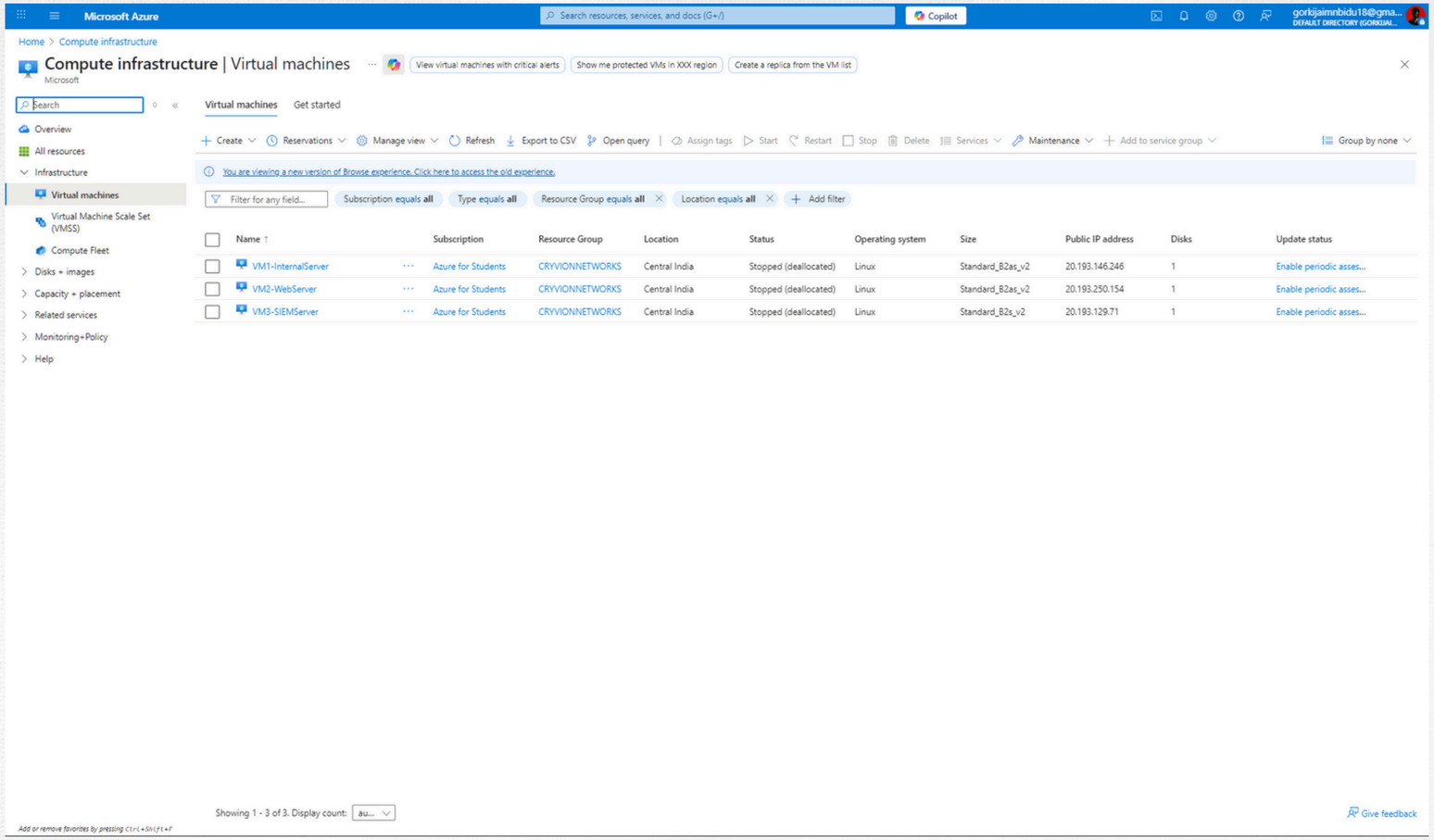


PHASE - 3

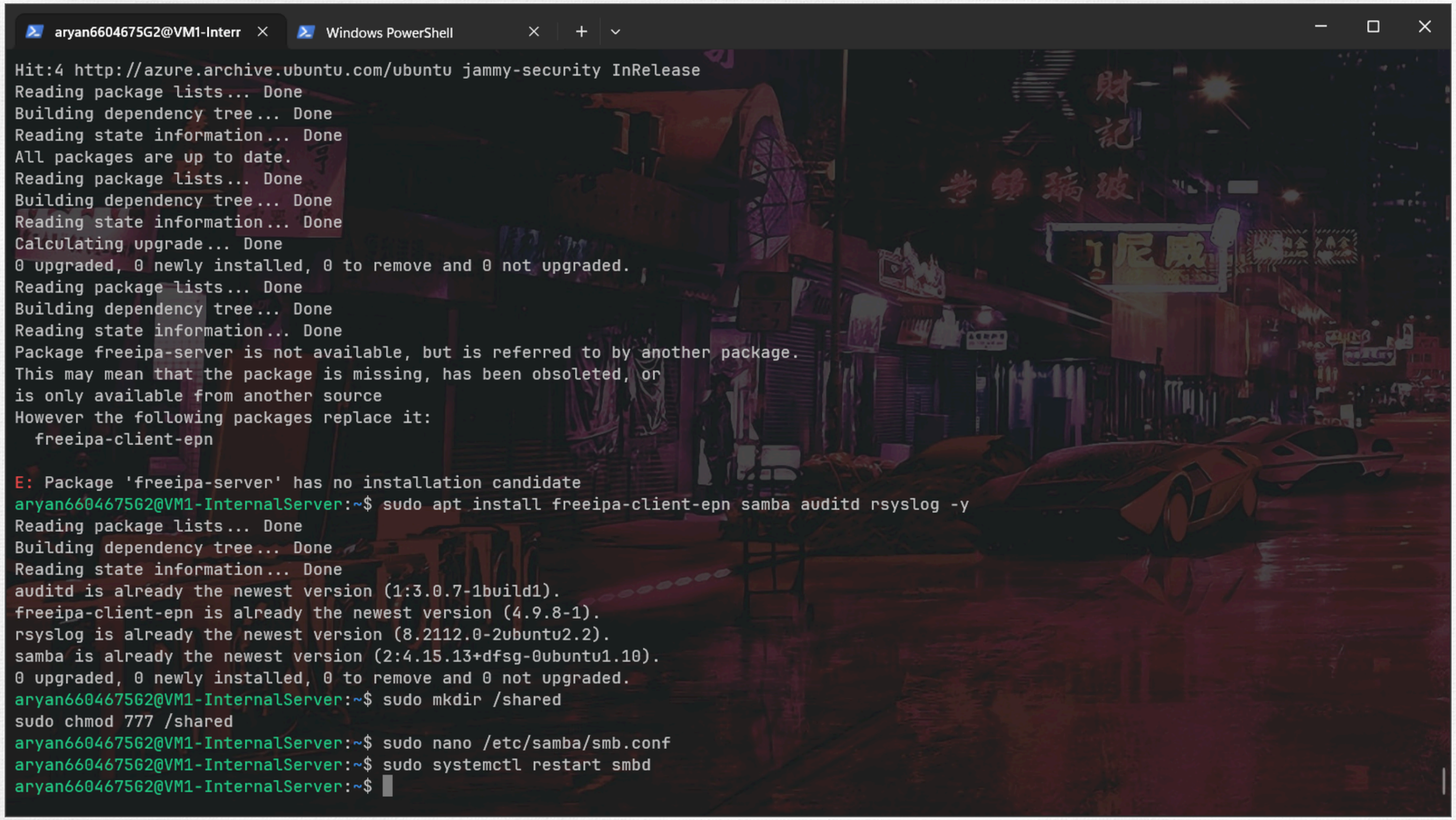
CREATE VIRTUAL MACHINES

The virtual machines would be on the server with different public IP and different internal IP on the same subnet.
The machines on the same subnet would be the Internal Server and SIEM Workstation.
Whereas the DMZ server will be on a different subnet.

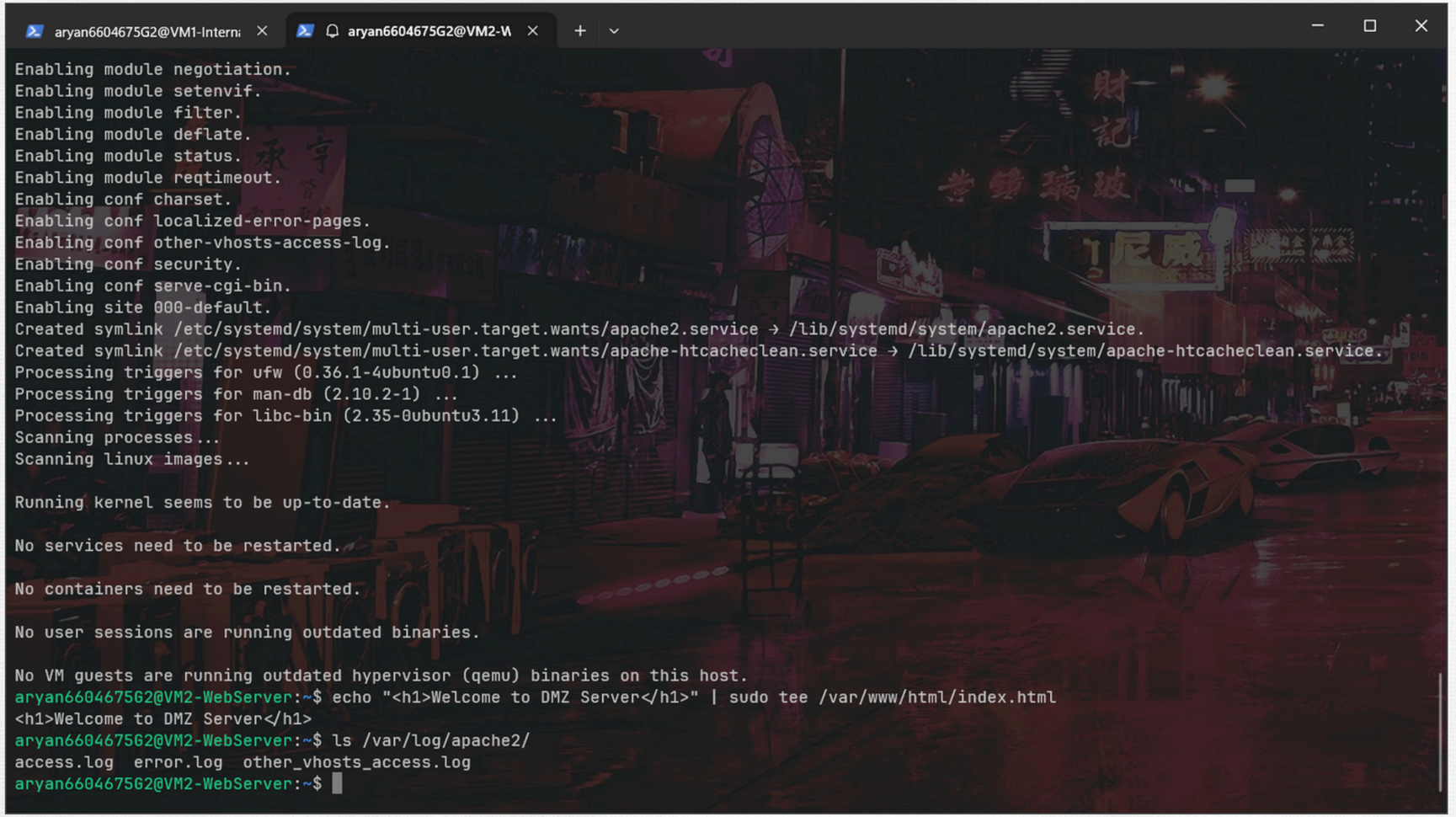
The following screenshot shows the creation of the 3 separate VM's.



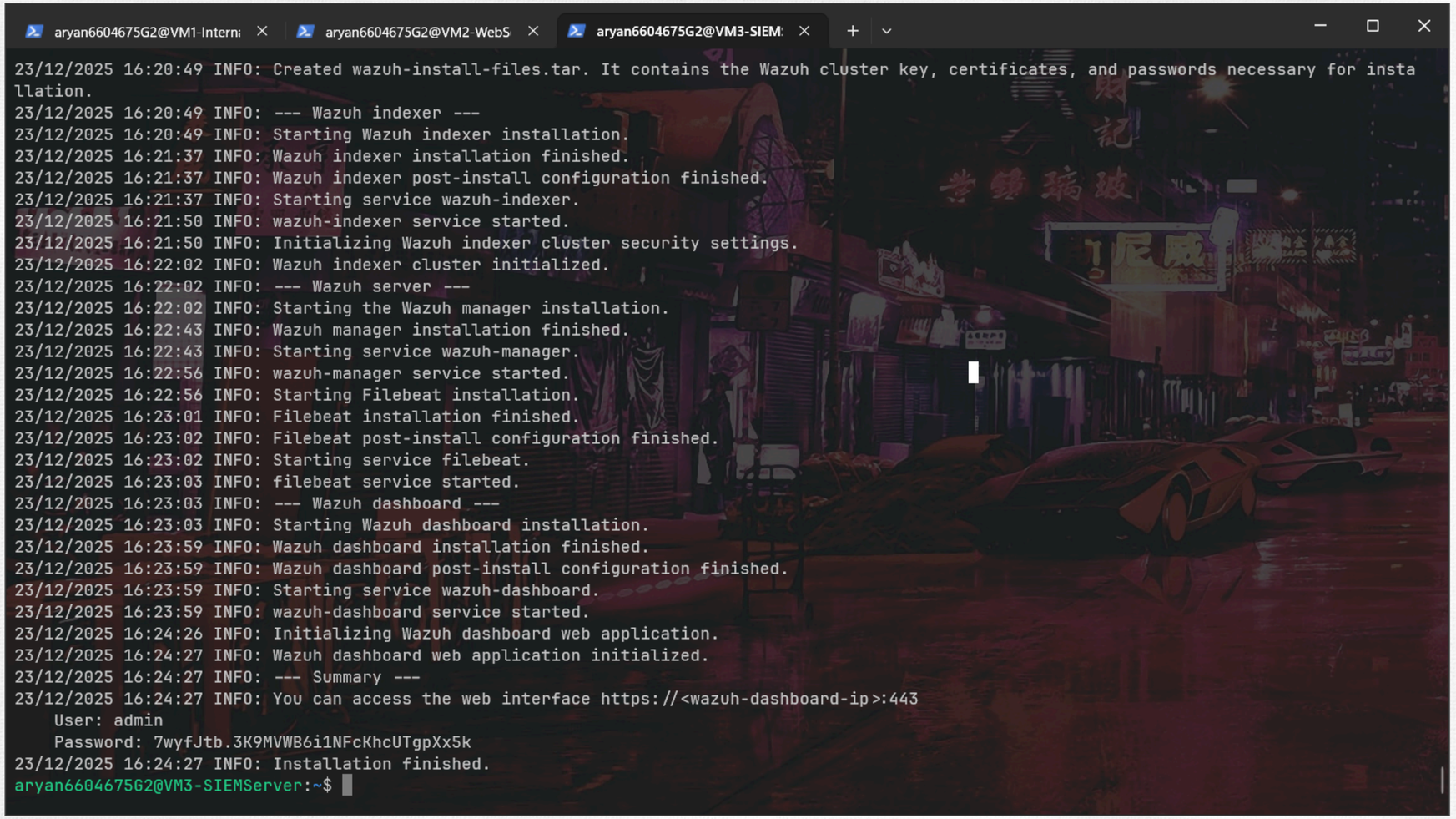
PHASE - 4 (SCREENSHOTS)



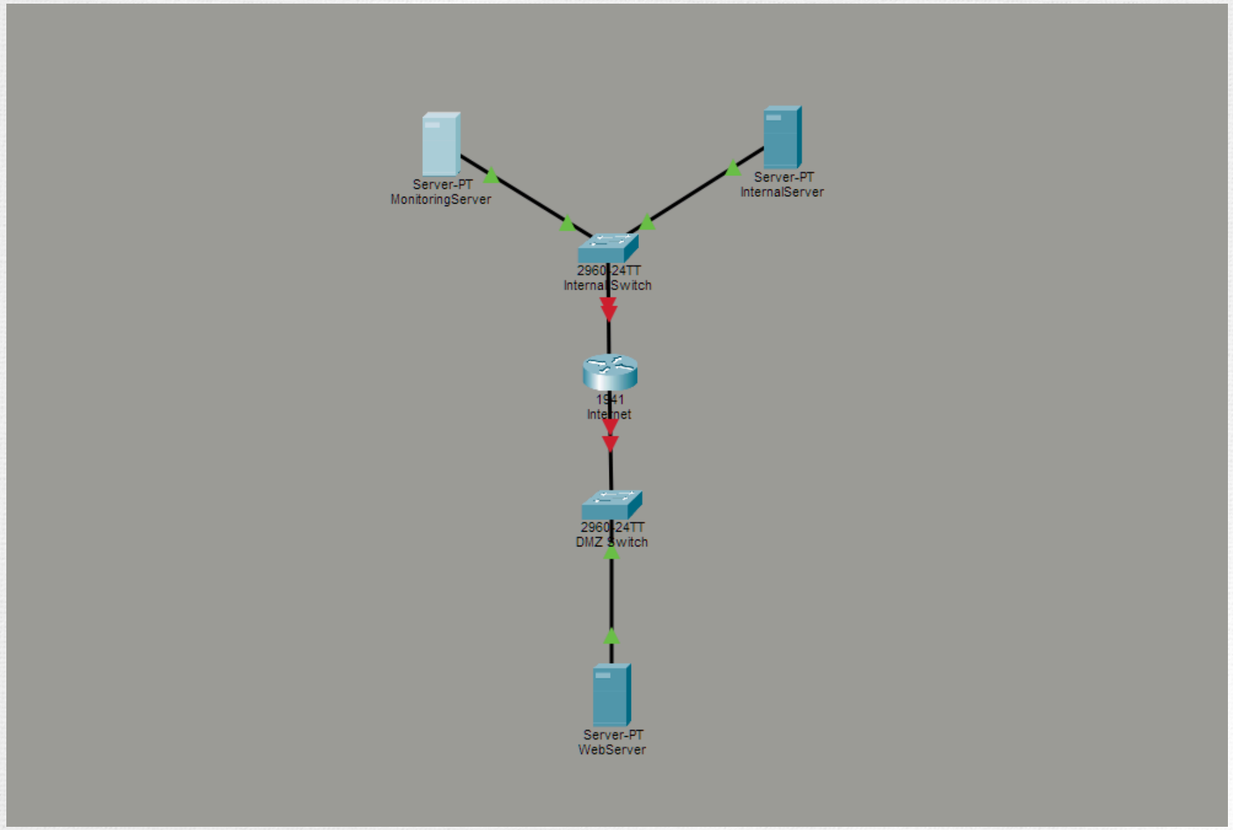
PHASE - 4 (SCREENSHOTS)

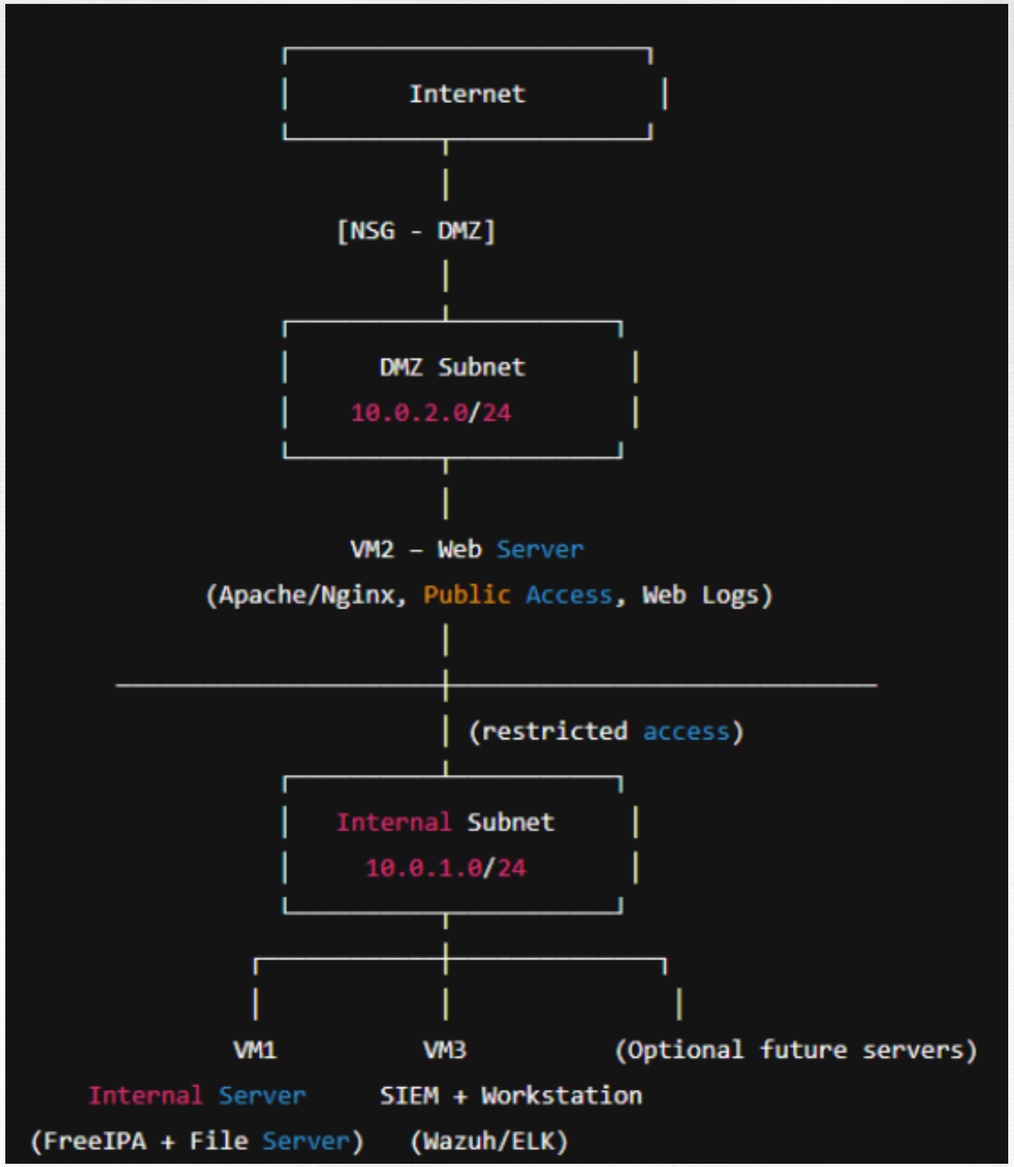


PHASE - 4 (SCREENSHOTS)



PHASE - 5
NETWORK STRUCTURE





CONCLUSION

This project establishes a functional enterprise-style infrastructure deployed on Microsoft Azure, consisting of segmented internal and DMZ networks hosting core services and an external-facing web server.

All systems were deployed using Ubuntu 22.04 and intentionally left without security hardening to reflect realistic baseline environments.
Centralized logging was implemented using Wazuh, enabling effective collection and visibility of system, authentication, audit, and web server logs.

This confirms that the environment is operational, observable, and ready for security testing and SOC analysis in the subsequent project phase.

THANK YOU