**Domain: Cloud Security**

**Question 4: What are the security benefits of defining cloud infrastructure as code?**

IaC has many security benefits which are quite appealing to those working in IT.

In the instance of the project, I deployed Ansible containers to our virtual machines to set up and run preconfigured environments in which we can do various testing, updating and logging activities throughout other virtual machines.

Why I specifically used the IaC approach over manually setting up my environments and individually updating and maintaining them as an alternative were because of the several inherent benefits to IaC. These benefits include:

* Accuracy: Because I was able to push out identical commands and updates to our VM’s within the one configuration file, I was able to limit the amount of mistakes that come with manually doing these things via automation.
* Transparency: The configuration files responsible for deploying the containers are completely visible to any modifications that it may undergo in the future.
* Updates: Updates can be pushed out very quickly as changes only need to be made to the .yml files and have them be redeployed.

For the project, the class specifically used the Ansible playbooks by deploying a configured ansible playbook that would be commanded to run on whichever VM we chose, and we specifically did this by using ansible playbooks (.yml files) and the respective configuration files for each service.

It wasn’t without any disadvantages, however. I personally ran into errors that stalled me long enough that I considered that had I been manually and individually connecting to the VM’s I was working on and installing and deploying my containers there, I would have had less of a headache. And this was simply because since I had an error with one part of my playbook, it halted everything.