**Project Overview**

In the first project week, we configured an ELK stack server in order to set up a cloud monitoring system. This project resulted in tangible deliverables that demonstrates knowledge in cloud, network security, logging and monitoring.

Activities involved the following:

* Create a new vNet in Azure in a different region, within the same Azure resource group.
* Create a peer-to-peer network connection between your vNets.
* Create a new VM in the new vNet that has 2vCPUs and a minimum of 4GiB of memory (elk VM)
* Add the new VM to Ansible’s hosts file in your provisioner VM.
* Create an Ansible playbook that installs Docker and configures an ELK container on the Elk VM
* Run the playbook to launch the container.
* Restrict access to the ELK VM.
* Create a Filebeat configuration file.
* Create an Ansible playbook that copies this configuration file to the DVWA VMs and then installs Filebeat.
* Run the playbook to install Filebeat.
* Confirm that the ELK Stack is receiving logs.
* Use the same method to install Metricbeat.

**Kibana Investigation**

After creation of the ELK stack, three tasks are carried out on the web servers that have Filebeat/Metricbeat installed, to simulate activity and subsequently identify that activity within the log/metric data via the Kibana dashboard

1. Generate a high amount of failed SSH login attempts and verify that Kibana is picking up this activity.

A picture containing calendar

Description automatically generatedThe Elk VM does not have the correct SSH key to be able to SSH into the web servers. By replicating a failed ssh login attempt from the Elk VM (10.1.0.4) to the Web VM’s. below is picked up in the logs in Kibana for the Web Vm’s

1. Generate a high amount of CPU usage on the pen-testing machines and verify that Kibana picks up this data.

By running sudo apt install stress on Web 2 VM’s Linux CLI, the below CPU usage can be found on the metrics tab in Kibana

Chart, treemap chart

Description automatically generated

(Web 2 CPU is @ 100% utilisation as per the stress command)

1. Generate a high amount of web requests to your pen-testing servers and make sure that Kibana is picking them up.

Scatter chart

Description automatically generated with medium confidenceBy using the wget command, this can be used to simulate a DDoS event. However in this instance, there was no noticeable change in load by running wget multiple times for any of the Web server VM’s.