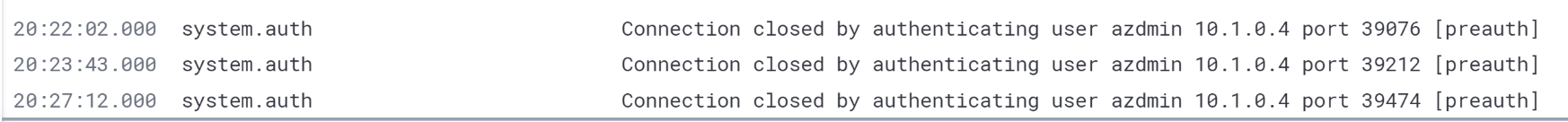
**Kibana Investigation**

In this activity, three tasks are carried out to simulate activity that will be picked in logs for identification in Kibana

You will have three tasks:

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

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

Chart, treemap chart

Description automatically generated

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.