Tiia Maide

December 18, 2020

**Kibana Research Notes**

* The task with Kibana was to look at the system logs and metrics that we set to record via filebeat and metricbeat playbooks
* It was noted that China was accessing the website an extreme amount of time
* On December 10, 2020 @ 1555 attempted to download a RPM file. RPM files are Red Hat Package Managers
* I was able to pinpoint the IP address to 1.145.31.121 and the geo coordinates lat: 28.28980556, lon:81.4370833
* They were using a Windows 8 operating system
* The URL they used: <https://artifactc.elastic.com/downloads/beats/metricbeat/metricbeat-6.3.2-i686.rpm> which they retrieved via Facebook
* The user was attempting to download a Linux package from the website being monitored
* This package isn’t necessarily malicious in itself, but it is dependent on the website itself not having been compromised. It could have been something as simple as a system administrator performing a much-needed update.
* The user should have not used Facebook to get the link to download the Red Hat Package Manger as most likely that would be against company policy.
* It would be my recommendation that this user to be monitored over the next 60 days to ensure they do not doing any malicious activity.

**Testing Metrics on Kibana**

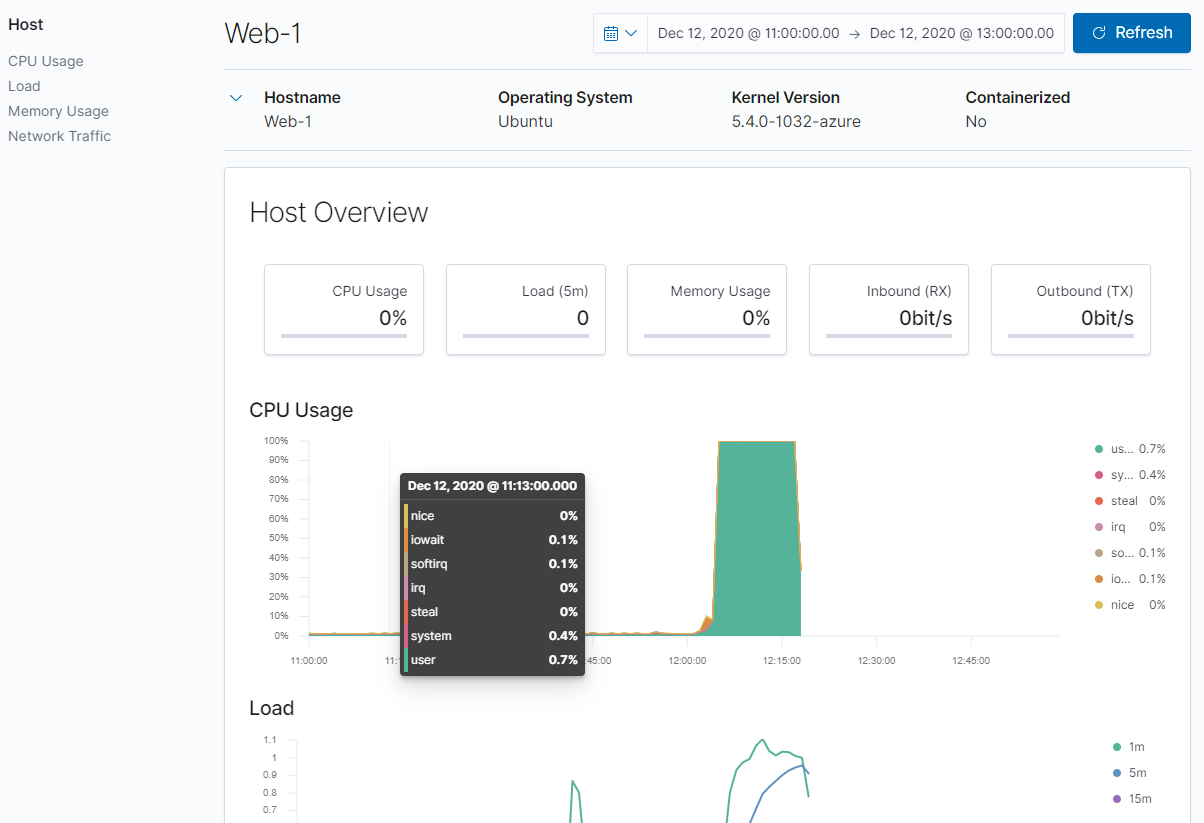
* The next task was to ensure Kibana was recording my logs and metric data.
* The first part was to attempt multiple failed ssh logins – this was done with using the follow command to automate the failed logins for good data: for I in {1..1000}; do ssh [sysadmin@10.0.0.5](mailto:sysadmin@10.0.0.5); done
* I then had to retrieve the metrics data from Kibana to ensure it was picking up all the failed logins.
* The next task was to stress out the system to ensure the Metrics were recorded on Kibana.
* I completed the following commands to conduct a stress test:

ssh [sysadmin@10.0.0.6](mailto:sysadmin@10.0.0.6) (repeated these steps on both servers)

sudo apt install stress

sudo stress –cpu 1

* Below is a screenshot of the results of the stress test on one of my webservers



As we can see the CPU usage sky rocketed when running the stress test.

* The last task was to ensure Kibana was monitoring for high web requests
* This was done by completing the following commands from within my Jump-Box
* Wget ip.10.0.0.6 (this is my web-1 server)
* ls to check that the index.html was downloaded
* for i in {1..1000}; do wget 10.0.0.6; done (this will create 1000 web requests to my server from my Jump-Box
* while true; do wget 10.0.0.6; done (this will create unlimited amount of web requests and would require a ctrl C to quit

Below is the screenshot showing the changes in Kibana 