Asure Cloud Web Servers Stress Test - Monitored by Kabana

We want to generate some data to visualize in Kibana, using the following steps:

1. Use jump-box to attack your web machines in various ways
2. Use a Linux utility to stress the system of a web VM directly
3. Subsequently generate traffic and logs that Kibana will collect
4. View that traffic in various ways inside Kibanna

Three tasks:
1. Generate a high amount of failed SSH login attempts and verify that Kibana is picking up this activity (Filebeats)

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

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

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

Instructions
We will try to SSH to a web machine from our jump box directly without using the Ansible container
1. Log ged into jump-box, then try to ssh to web-1 server
   -Run: `ssh azadmin@10.0.0.10
   Received an error:

```
bash
sysadmin@Jump-Box-Provisioner:~$ ssh sysadmin@10.0.0.5
sysadmin@10.0.0.5: Permission denied (publickey).
```

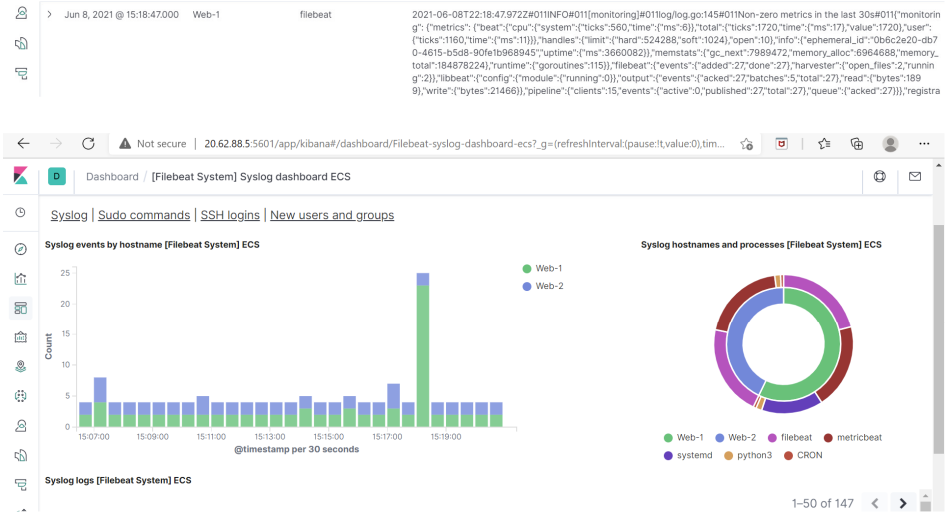
This error was also logged and sent to Kibana.

2. Ran the failed SSH command in a loop to generate failed login log entries
for i in {1..10}; do ssh azadmin@10.0.0.10; done

azadmin@Jump-Box-Provisioner: ~

```
root@3ca40a6a9d6b:/etc/ansible# exit
exit
azadmin@Jump-Box-Provisioner:~$ ssh azadmin@20.83.225.130
^C
azadmin@Jump-Box-Provisioner:~$ ssh azadmin@10.0.0.10
The authenticity of host '10.0.0.10 (10.0.0.10)' can't be established.
ECDSA key fingerprint is SHA256:89HImGbm6HcQPIIKm8Df7hn1Qb8pw2ZkSsOW+3yOcho.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.0.10' (ECDSA) to the list of known hosts.
azadmin@10.0.0.10: Permission denied (publickey).
azadmin@Jump-Box-Provisioner:~$ for i in {1..10}; do ssh azadmin@10.0.0.10; done
azadmin@10.0.0.10: Permission denied (publickey).
azadmin@10.0.0.10: Permission denied (publickey).
azadmin@10.0.0.10: Permission denied (publickey).
azadmin@10.0.0.10: Permission denied (publickey).
azadmin@10.0.0.10: Permission denied (publickey).
azadmin@10.0.0.10: Permission denied (publickey).
azadmin@10.0.0.10: Permission denied (publickey).
azadmin@10.0.0.10: Permission denied (publickey).
azadmin@10.0.0.10: Permission denied (publickey).
azadmin@10.0.0.10: Permission denied (publickey).
azadmin@Jump-Box-Provisioner:~$
```

3. Searched through the logs in Kibana to locate the generated failed login attempts



Linux Stress

Generate a high amount of CPU usage on the pentesting machines and verify Kibana picks up this data

Instructions

1. Started up Ansible container and attached to it

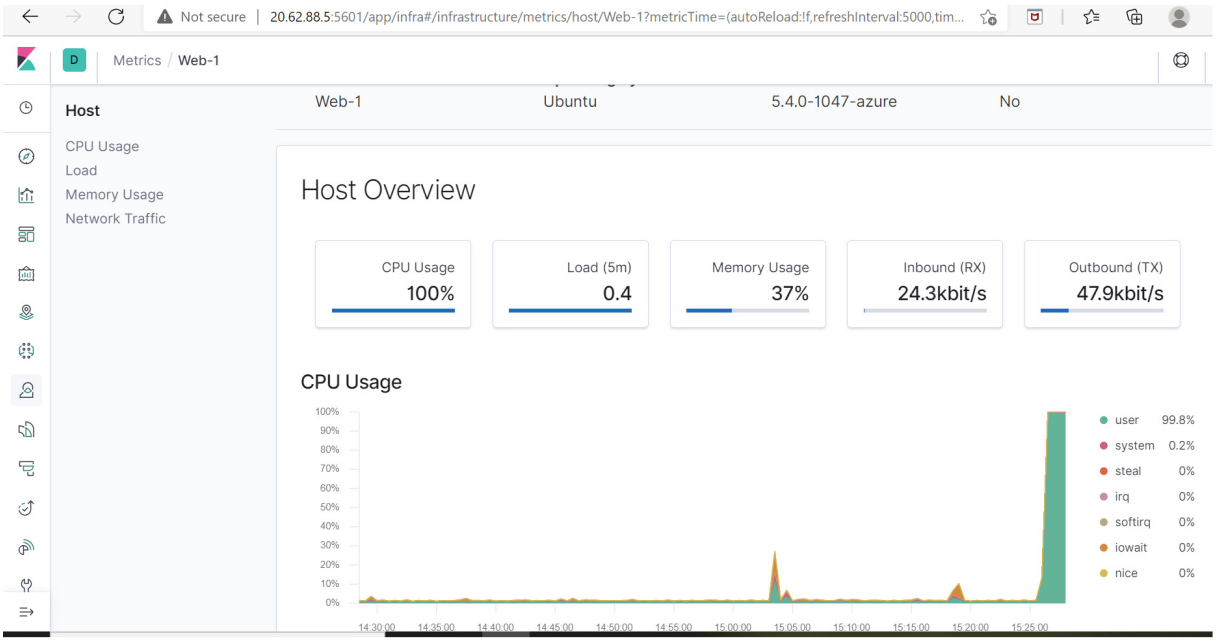
2. SSH'd from Ansible container to Web-1 VM

3. Ran `sudo apt install stress` to install the stress program

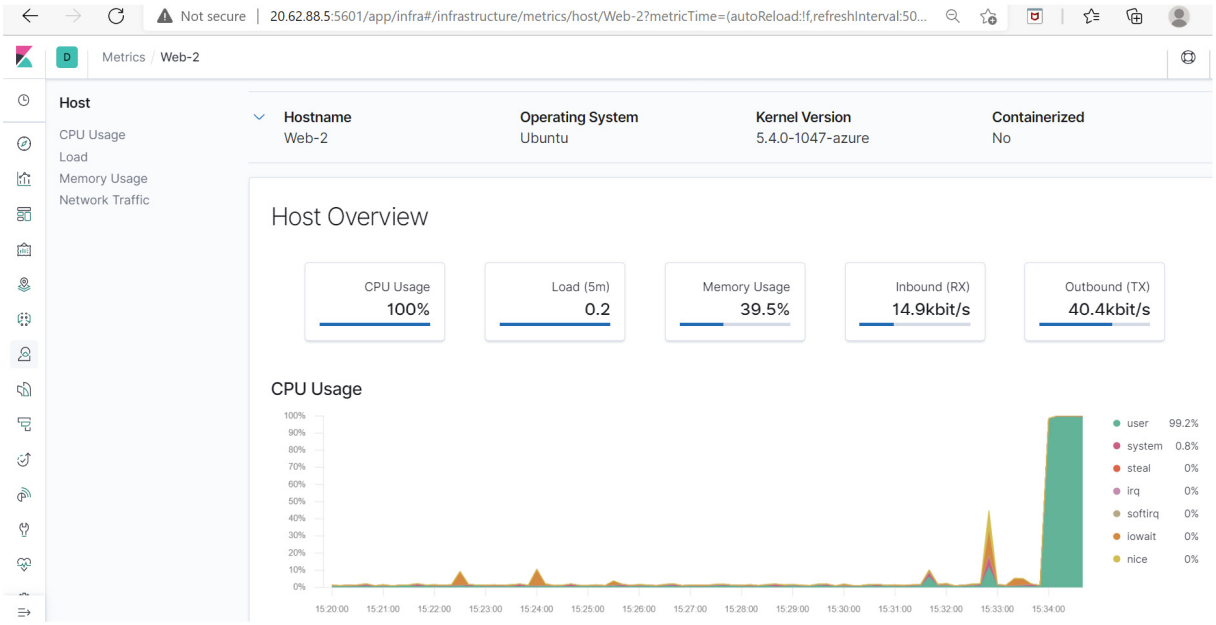
4. Ran `sudo stress --cpu 1` and allow `stress` to run for 4 minutes

5. Viewed the Metrics page for that VM in Kibana. What indicates that CPU usage increased?

Web Server 1



Web Server 2

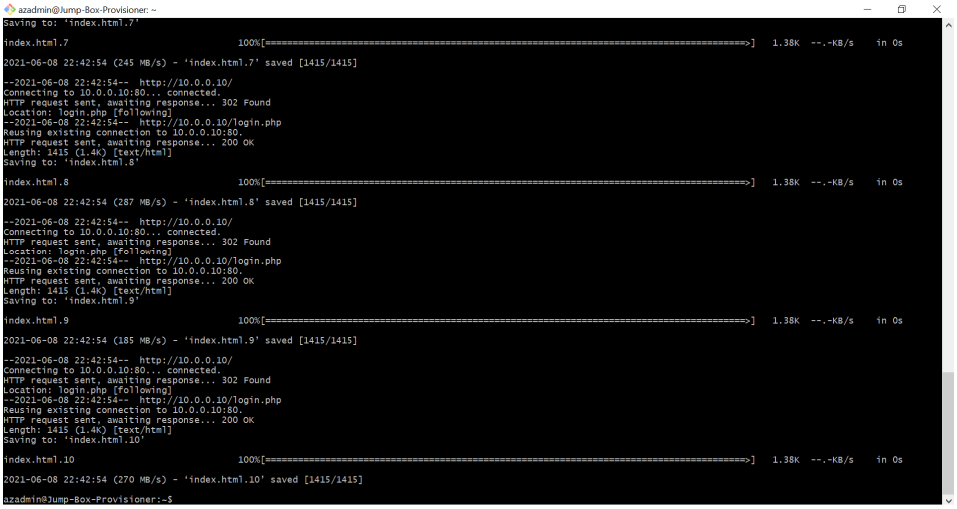


wget-DoS
Generate a high amount of web requests to your pen-testing servers and make sure that Kibana is picking them up

Instructions
We want to generate abnormal data to view by creating a DoS web attack using the wget command

1. Logged into jump box

2. Ran the `wget` command in a loop to generate many web requests
for i in {1..10}; do wget 10.0.0.10; done



5. Metrics page for Web-1 VM that we impacted the Network Traffic Metrics