**rCOMMANDS**

Sudo apt-get update

Sudo systemctl status docker

Sudo systemctl start docker

Sudo apt install docker.io

Sudo docker pull

Sudo docker run-ti

-cyberxsecurity/ansible bash

Sudo docker container list -a

Sudo docker start silly\_fermat

Sudo docker attach silly\_fermat

Sudo docker ps

Ssh-keygen

Cat /root/.ssh/id\_rsa.pub

Ls ~/.ssh/id\_rsa.pub

JumpBox Provisioner

Ls /etc/ansible

Nano /etc/ansible/ansible.cfg

Nano /etc/ansible/hosts

Ansible-playbook “your playbook”= **intall-elk.yml ----** ansible-playbook install-elk.yml

* **In Virtual Machine-- Elk-Venomvito user (ssh Elk\_Venomvito@10.1.0.4)**
  + Curl localhost/setup.php

SSH-KEYS

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC577sXulerCQ4B02jFr1+xK1JLqNzmQKdu8YuGzcwt4oROzPbiFjG/nT2Ve4jeuf7mxitx7jlabw4L3aJonsnGjxgDBaxOCZfjvSxiAOO0uQyrL1JUajDAU/ExNBnwkg5J36npwrJgR7KxIkklqAiLamPIbUSDdR8Hiz32E3BDbZ9rvL33dOZ65lio+BtGRmn88XQCBuNWmOZFDZxn5PH+uDRsifgE7VYNS9b31o7IAidR+id0tsK3XUPtyskj+VmeQTHjmzD5Gsl6YRTsan9CtKfdZC3qrfPGcjWXan9YUMn4CLS+d+8QD0XzudEhxqwzqEH2CQF+d0GX8ZdI6JAT Redadmin@Jump-Box-Provisoner

-Public-IP - 40.83.139.135- ssh Redadmin@40.83.139.135

Jump box provisioner silly\_fermat docker public key:

ssh-rsa  root@0aea55cd764b

**WEEK 13-- DAY 1**

CREATE NEW Vnet

Resource group= Redteam\_Vito\_stallion

Name= Elkstack\_Venomvito

Region= US east

Peering

-EastUS\_Venomvito

-name: Vnet Peering

CREATE A new Virtual Machine

-**Elk-Venomvito**

-Region=US-East

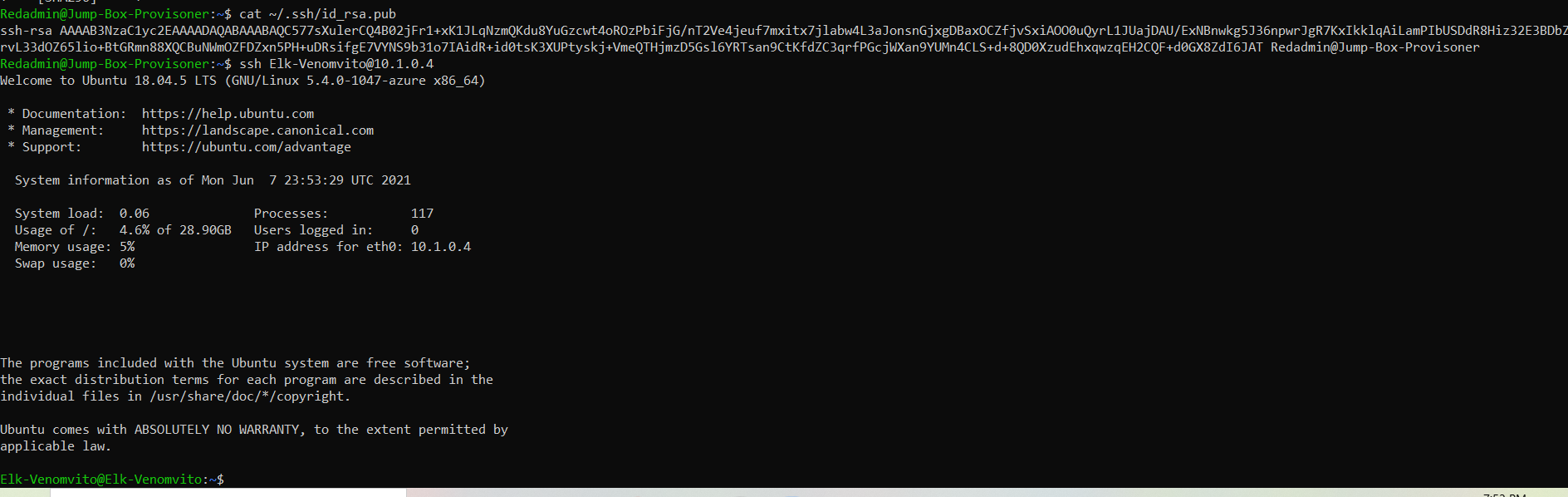
-Username= azadmin

I used PUBLIC key from JumpBox

Public IP= 168.62.188.40

Private IP= 10.1.0.4

* **Ssh Elk-Venomvito@10.1.0.4**



PART 3

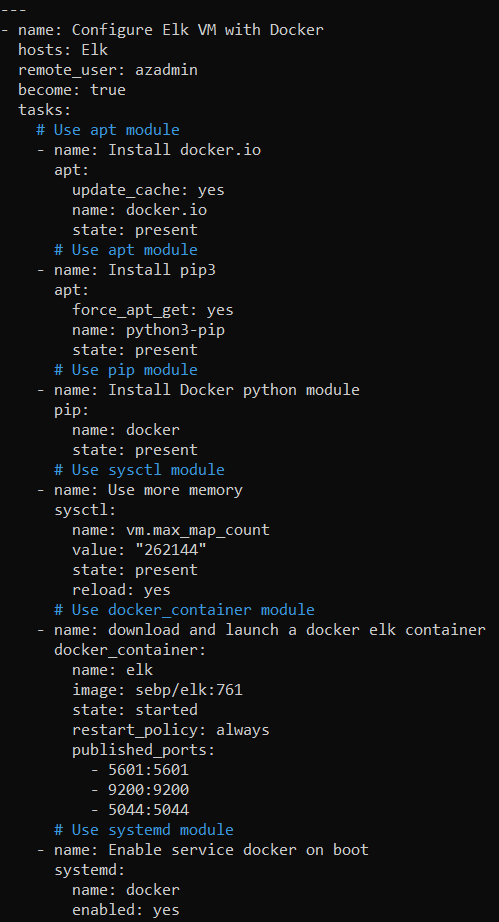
Sudo docker attach silly\_fermat

Ls /etc/ansible/

*Nano /etc/ansible/hosts*

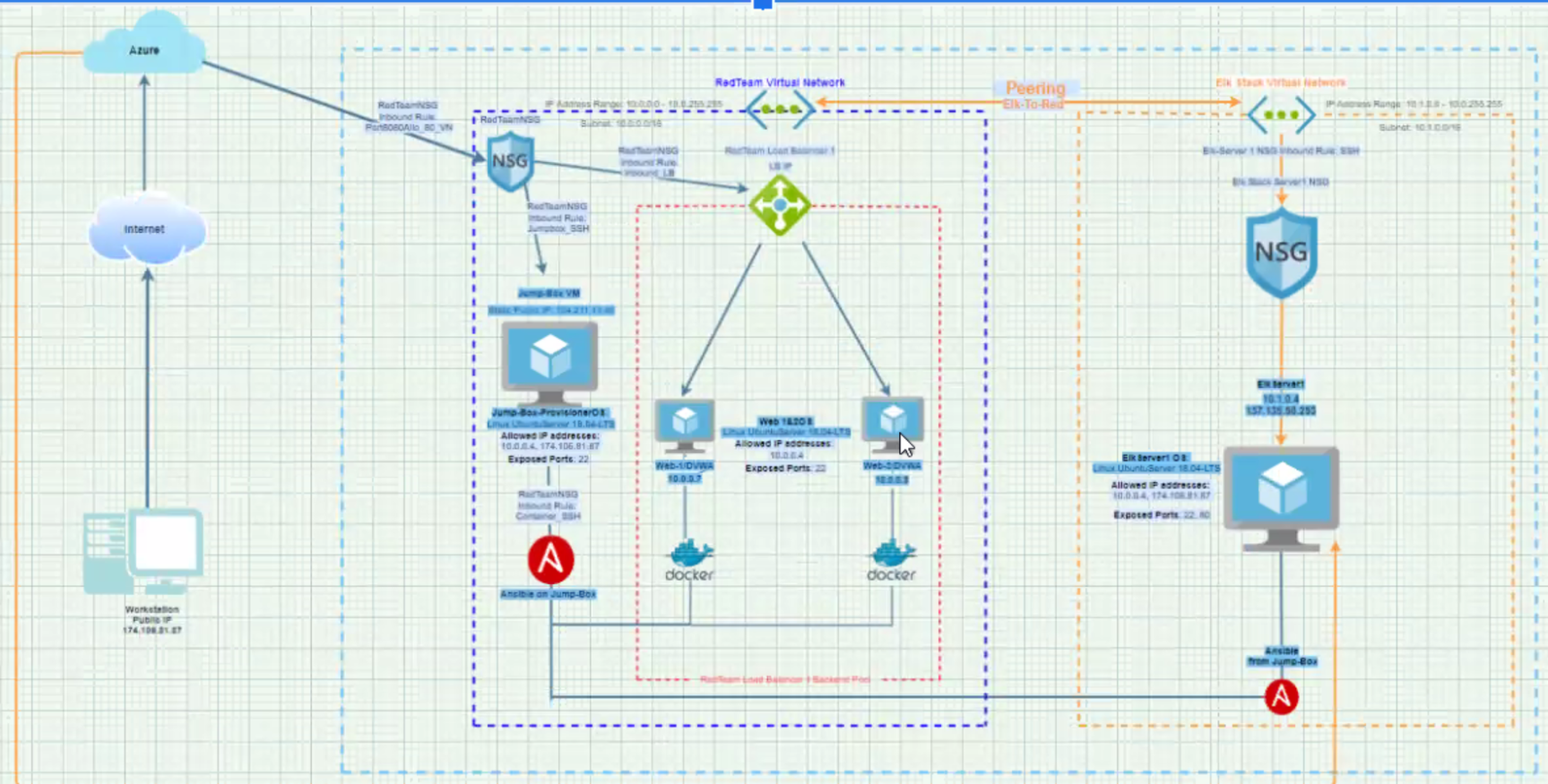
*[Elk]*

+ 10.1.0.4 ansible\_python\_interpreter=/usr/bin/python3

* Sudo docker start silly\_fermat
* Sudo docker attach silly\_fermat
  + Located within root of ansible container
    - Ls /etc/ansible
      * *Ansible.cfg--hosts--install-elk.yml--pentest.yml*
    - Nano install-elk.yml
    - 
    - [http://40.114.117.19:5601/app/kibana #/home](http://40.114.117.19:5601/app/kibana#/home)- not working
    - [http://104.211.8.115:5601/app/kibana](http://104.211.8.115:5601/app/kibana-) - is working

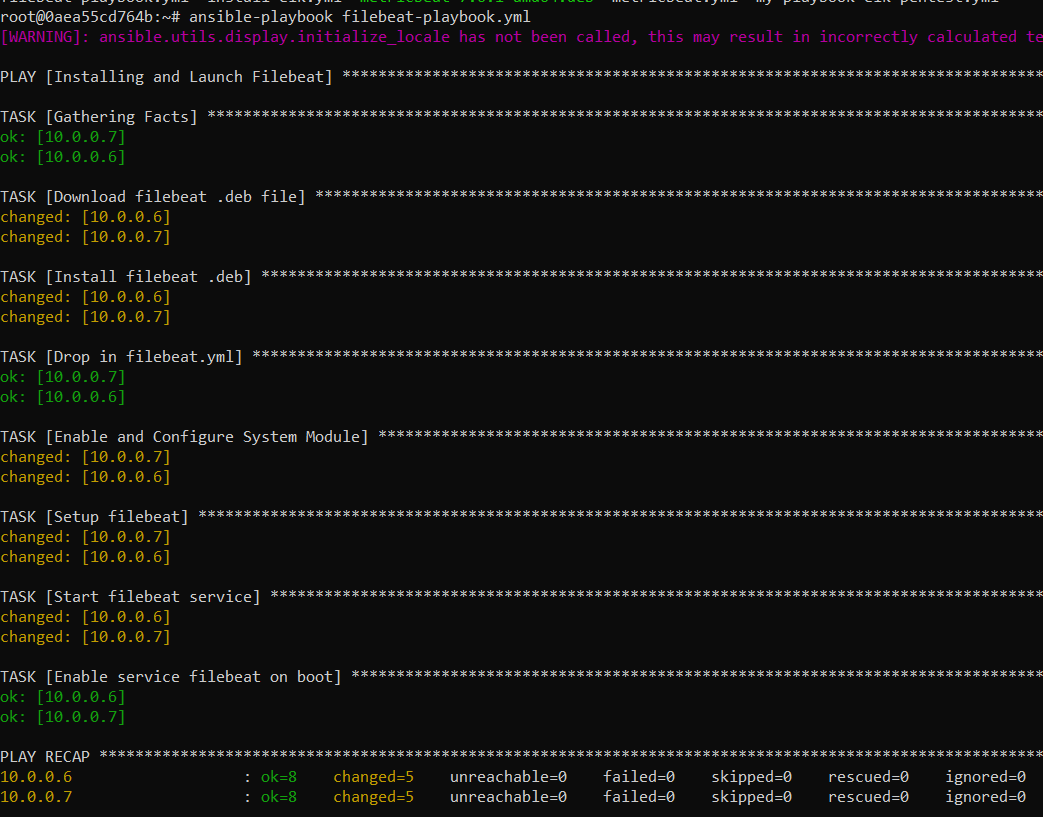
**DAY 2**

**OVERALL TOPOLOGY**

**1.**

**Nano /etc/ansible/filebeat-config.yml**

**Sudo**

****

**BONUS**

**curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.6.1-amd64.deb**

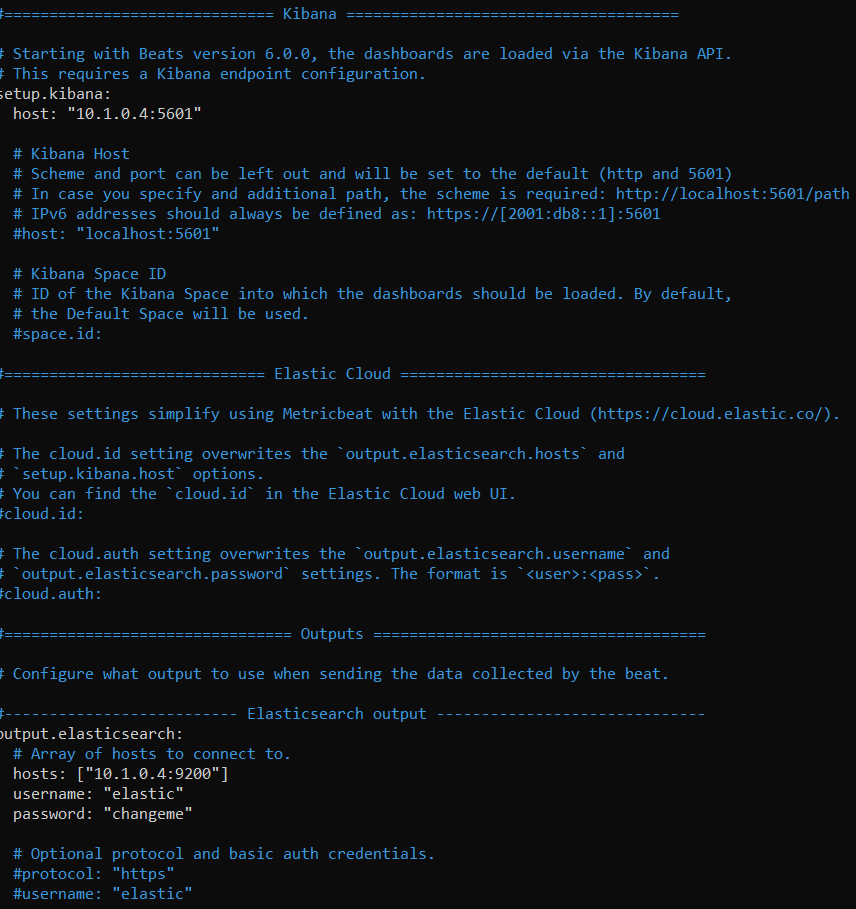
**sudo dpkg -i metricbeat-7.6.1-amd64.deb**

**Downloaded metric file------- chmod +x metric file**

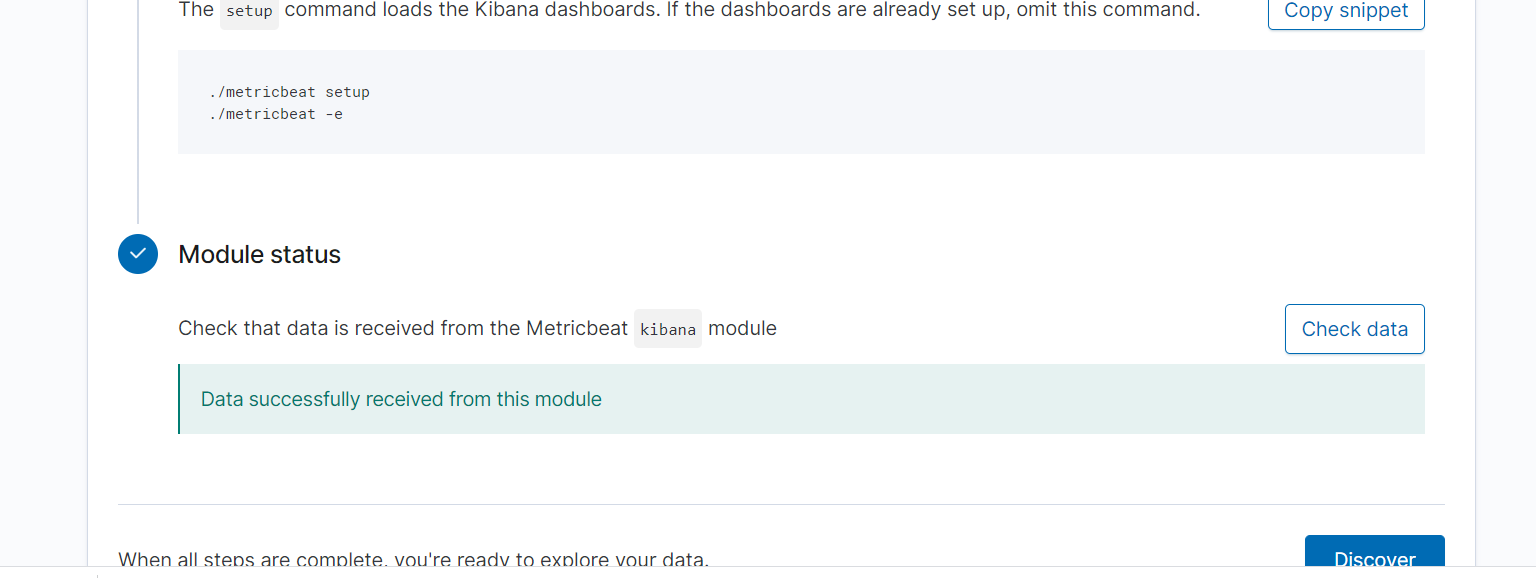
****

**setup - metricbeat-playbook.yml---- edit setup kibana**

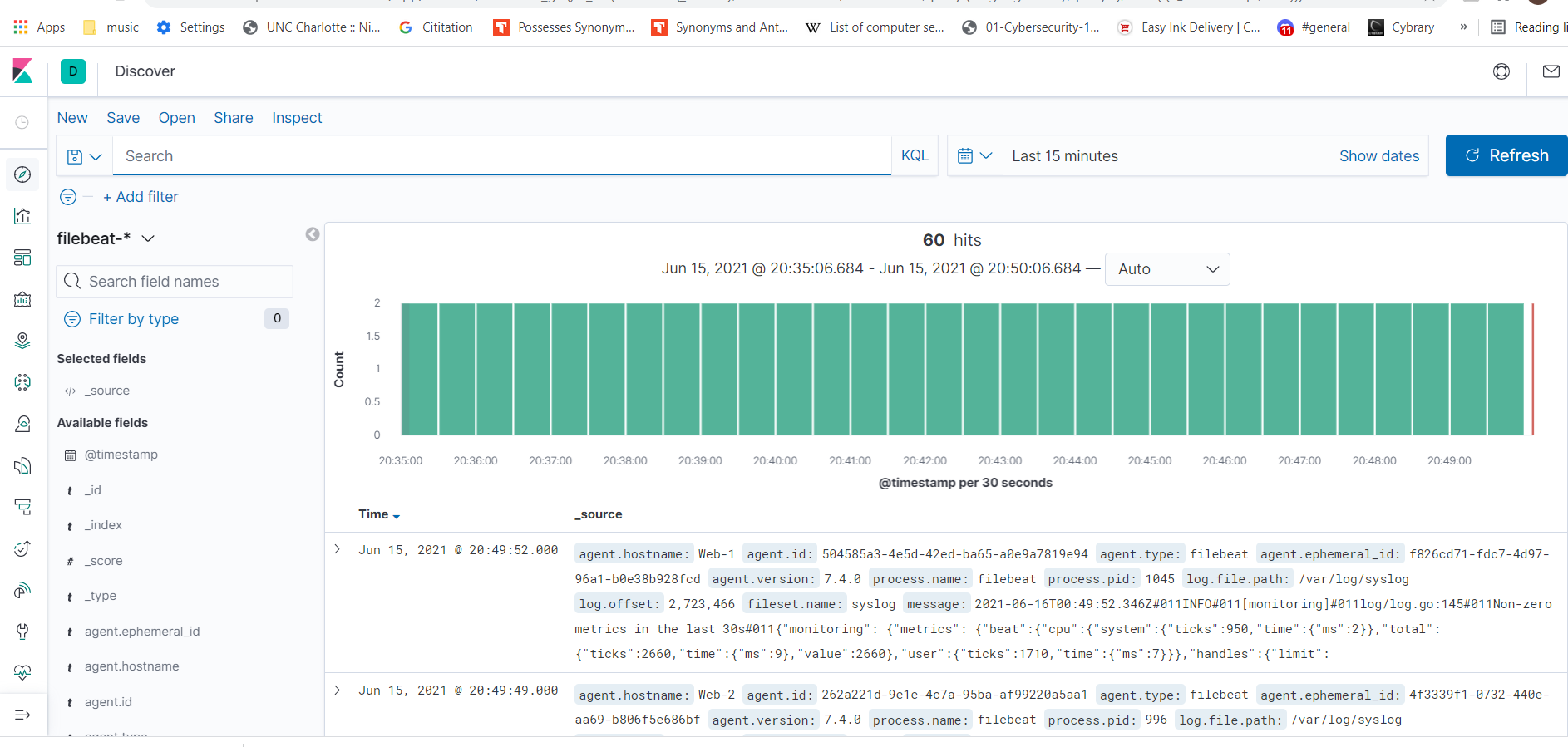
**Host: 10.1.0.4**

****

**Metric beat success**

****

**Discover Metricbeat**

****

**DAY 3**

**Setup github**

**Username: Venomvito**

**Password: stallion26!**