ELK-VNET:

1. Red-Team (Resource Group) - West-US - Address 10.0.0.0/16

Elkserver1396 - Network Interface - 10.0.0.4 and Public IP: 104.210.51.88

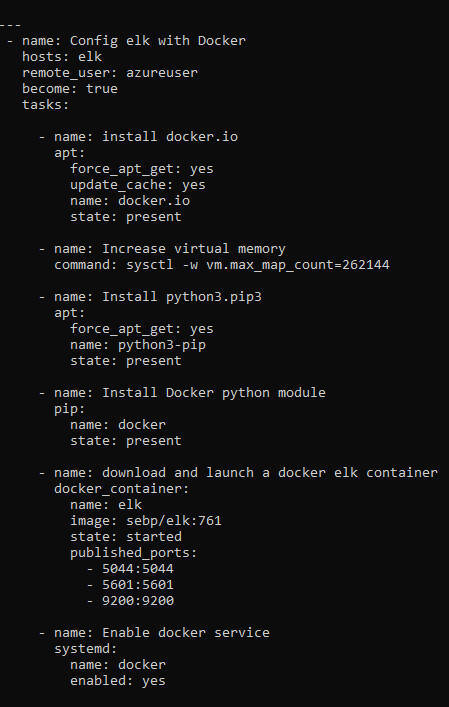
Peering: Elk-to-Red - 10.1.0.0/16

1. Red-Team (Resource Group) - East-US - 10.1.0.0/16

Peering: Red-to-ELK - Elk-VNET - 10.0.0.0/16

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

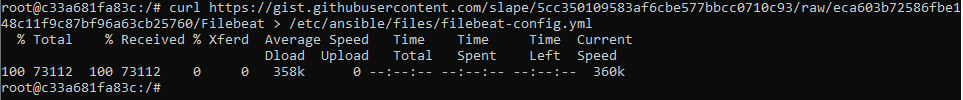
1. LocalPC# ssh [azureuser@13.90.94.255](mailto:azureuser@13.90.94.255) (Prompt change and log in Jumpbox)
2. azureuser@jump-Box: $ sudo docker ps
3. # sudo docker container list -a
4. # Sudo docker start elated\_blackwell
5. # sudo docker attach elated\_blackwell (Prompt changed and log in container)
6. root# cat /root/.ssh/id\_rsa.pub (Copy public key and paste at ELKServer1)
7. # nano /etc/ansible/hosts ([elk] – 10.0.0.4 ansible\_python\_interpreter=/usr/bin/python3)
8. # nano /etc/ansible/ansible.cfg (remote\_user = sysadmin)
9. # nano /etc/ansible/elk.yml (Create play book)



1. #cd /etc/ansible
2. # ansible-playbook elk.yml (Run Playbook for ELK server)
3. <http://104.210.51.88:5601/app/kibana>

Day 2

1. Root# curl https://gist.githubusercontent.com/slape/5cc350109583af6cbe577bbcc0710c93/raw/eca603b72586fbe148c11f9c87bf96a63cb25760/Filebeat > /etc/ansible/files/filebeat-config.yml



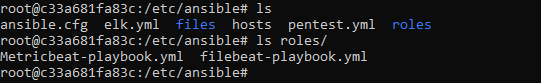
1. Edit file - root # nano /etc/ansible/files/filebeat-config.yml

Ctrl + Shift + - Line number 1106 and 1806

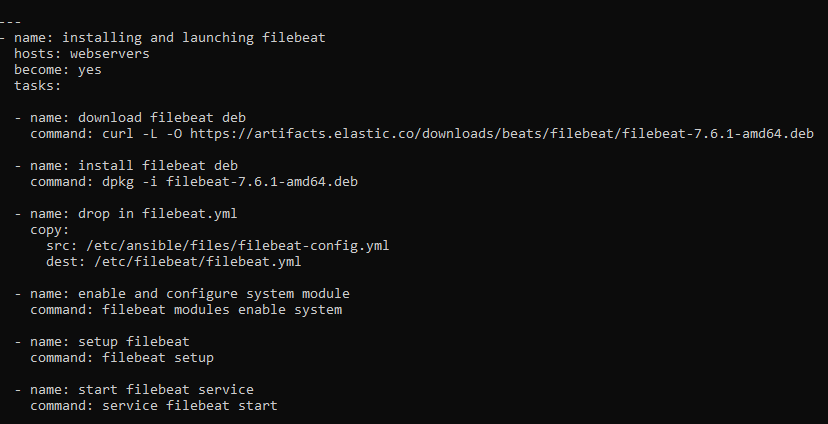




1. Root# ls /etc/ansible/



1. Root# nano /etc/ansible/roles/ filebeat-playbook.yml

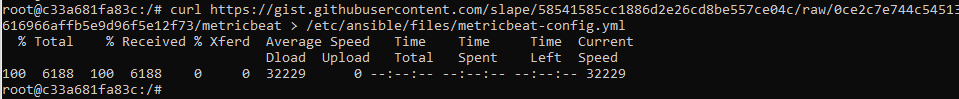


1. Run playbook Root# ansible-playbook filebeat-playbook.yml

Inside the GUI – Kibana - Module Status – Check data (Data successfully received from this module)

1. Download the metricbeat

Root# root@c33a681fa83c:/etc/ansible# curl https://gist.githubusercontent.com/slape/58541585cc1886d2e26cd8be557ce04c/raw/0ce2c7e744c54513616966affb5e9d96f5e12f73/metricbeat > /etc/ansible/files/metricbeat-config.yml



1. Root# nano /etc/ansible/files/metricbeat-config.yml

Set.kibana:

Host: “10.0.0.4:5601”

Output.elasticsearch:

Hosts: [“10.0.0.12:9200”]

Username: “elastic”

Password: “changeme”

1. Root# cd /etc/ansible/roles/

Root# nano Metricbeat-playbook.yml

Root# ansible-playbook Metricbeat.yml

