Josh Brnak

7/12/2020

**ELK Stack Project**

**Project Scope:**

The scope of this project was to create an ELK (Elasticsearch, Logstash, Kibana) stack in an ELK Docker container in a new ELK server virtual machine (VM) in a new virtual network (VNet) peered with an existing Vnet to monitor the existing network’s web servers. The existing Vnet’s web servers are to be monitored using Filebeat and Metricbeat installed on the new ELK server. The previously mentioned are to be implemented using the proper security measures through network security groups (NSG’s) and by adding other infrastructure nodes detailed below.

**Project Workflow:**

1. Create new Vnet, ELK2-Vnet
   1. Create in different location than existing Vnet RedTeam2
2. Create Peer connection between existing Vnet RedTeam2 and new Vnet ELK2-Vnet
3. Create a new VM, ELKServer2
   1. Create in same location as new Vnet
   2. Use same username as webservers
4. Update Inbound Security Rules for the ELKServer2 Network Security Group (NSG) to allow for http connection on ports 5601, 9200, 5044 along with SSH connection on port 22.
5. Update the Ansible hosts file with a new group and IP of the ELK server
6. Create and run playbook to install Docker and a Docker container on ELKServer2
7. SSH into new VM. Start new container (should be elk container).
8. Open the Filebeat configuration file and update Elasticsearch.output and setup.Kibana to the private IP of the ELKServer2
9. Create a playbook to install and launch Filebeat
10. Follow steps 7 and 8 but for Metricbeat
11. Go to URL http://<ELKServer2\_public\_IP>:5601 to verify http connectivity and that filebeat and metricbeat are capturing data.

**Usage Instructions**

To use the ELK stack and filebeat and metricbeat we need to follow these steps:

1. Start the Jump Box, 3 DVWA webservers, and the ELK server virtual machines in Azure
2. Open up the Git Bash terminal
3. ssh into the Jump Box using the Jump Box’s public IP address
4. Get into root in the Jump Box
5. Start the ansible container using appropriate Docker commands
6. ssh into the Elk server using the Elk server’s private IP address
7. Start the Elk container using the appropriate Docker commands
8. At this point filebeat and metricbeat are monitoring the 3 DVWA web servers
9. To view Kibana and the filebeat and metricbeat GUI’s, enter the URL http://<Elk server Public IP>:5601