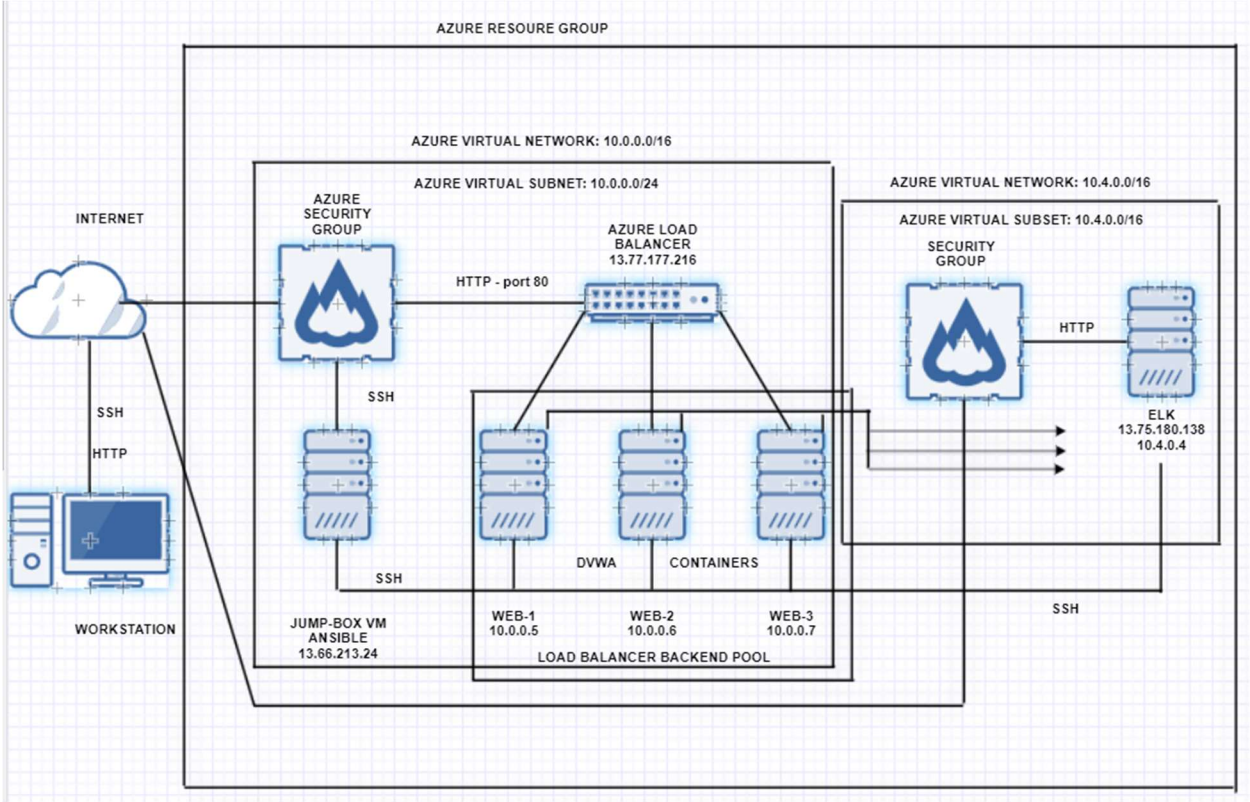
HOMEWORK – GAVIN FAUGHT

Automated ELK Stack Deployment

The files in this repository were used to configure the network depicted below.



These files have been tested and used to generate a live ELK deployment on Azure. They can be used to either recreate the entire deployment pictured above. Alternatively, select portions of the playbook file may be used to install only certain pieces of it, such as Filebeat.

<install-elk.yml>
<installBeats.yml>

This document contains the following details:

- Description of the Topology
- Access Policies
- ELK Configuration
  - Beats in use
  - Machines being monitored
- How to Use the Ansible Build

Description of the Topology

The main purpose of this network is to expose a load-balanced and monitored instance of DVWA, the D*mn Vulnerable Web Application.

Load balancing ensures that the application will be highly available and reliable, in addition to restricting access to the network. Load balancing makes it highly likely that DDOS attacks will not occur. The advantage of a jump box is that any tools in place for the Storage Area Network are maintained on that system.

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the logs and system resources. Filebeat monitors the log files or locations that you specify. It collects log events and forwards them either to Elasticsearch or Logstash for indexing. Metricbeat records metrics from the OS and from services running on the server.

The configuration details of each machine may be found below:

Name	Function	IP Address	Operating System
Jump Box	Gateway	13.66.213.24	Linux
Web-1	Web-server; DVWA container	10.0.0.5	Linux
Web-2	Web-server; DVWA container	10.0.0.6	Linux
Web-3	Web-server; DVWA container	10.0.0.7	Linux
ELK-VM	*	10.4.0.4/13.75.180.138	Linux

* aggregate logs, analyze logs, and create visualizations

The machines on the internal network are not exposed to the public internet. Only the Azure Security Group (firewall) machine can accept connections from the Internet. Access to this machine is only allowed from the following IP address:

108.93.193.108 (the IPv4 address of my home computer)

Machines within the network can only be accessed by the jump box. The machine that allows one access to the ELK VM is the Jump Box VM Ansible container. It's IP address is 13.66.213.24.

A summary of the access policies in place can be found in the table below:

Priority	MS Azure Name	Port	Protocol	Source	Destination
250	SSH	22	TCP	108.93.193.108	Virtual Network
3050	sshFromJumpBox	22	TCP	10.0.0.4	Virtual Network
3060	NewNetworkSecurityGroup[1]	80	Any	108.93.193.108	Virtual Network
3070	LoadBalancertToTheNet	80	TCP	AzureLoadBalancer	Virtual Network
4096	Default-Deny	Any	Any	Any	Any

[1] Firewall

[2] As the priority numbers increase, priority goes down

ELK Configuration

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because it can be run from the command line without the use of configuration files for simple tasks, such as making sure a service is running or to trigger updates or reboots.

The steps for installing and ELK installation playbook include:

1) Making sure Ansible is installed and running
2) Creating an ELK ansible playbook in yaml format (.yml)
3) Run the command “ansible-playbook <yaml file>”

The following screenshot displays the result of running ‘sudo docker ps’ after successfully configuring the ELK instance:

```
Last login: Sat Jul 18 17:00:29 2020 from 10.0.0.4
sysadmin@Elk-RedVM1:~$ sudo docker ps
CONTAINER ID        IMAGE               COMMAND                  CREATED             STATUS              PORTS
                                                                                NAMES
a9acb9cc5406        sebp/elk:761        "/usr/local/bin/star…"   4 days ago          Up 4 days           0.0.0.0:
5044->5044/tcp, 0.0.0.0:5601->5601/tcp, 0.0.0.0:9200->9200/tcp, 9300/tcp   elk
sysadmin@Elk-RedVM1:~$
```

Target Machines & Beats

This ELK server is configured to monitor the following machines: 10.0.0.5, 10.0.0.6, and 10.0.0.7. We have successfully installed Filebeat and Metricbeat. Filebeat collects data about the file system. An example of this is syslog events by hostname. Metricbeat collects machine metrics, measurements about an aspect of a system that tells analysts how “healthy” it is. Common metrics are CPU usage and uptime. Another example of what you see in Metricbeat are the incoming network packets per container.

In order to use the playbook, you will need to have an Ansible control node already configured. Assuming you have such a control node provisioned:

SSH into the control node and follow the steps below:

- Create the install-elk.yml
- Update the installBeats.yml file to include FileBeats and Metricbeat
- Run the playbook (both .yml files), and navigate to http://13.75.180.138:5601/app/kibana#/home to check that the installation worked as expected.