# Cyber-Security-Boot Camp

## Automated ELK Stack Deployment

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

Homework\_12\_JoshuaCutler (1).jpg

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 files may be used to install only certain pieces of it, such as Filebeat.

* elk-playbook
* filebeat-playbook
* metricbeat-playbook
* my-playbook

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 warrants that the application will be highly accessible, in addition to restricting traffic to the network. Load balancers protect network traffic from denial-of-service attacks. Using a jump box has the advantage of reducing attacks by using SSH to protect the infrastructure that's already in it.

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the data and system logs.

* Filebeat screens log files and their locations while forwarding them to Elasticsearch
* Metricbeat uses different metrics and statistics that are then gathered and forwards that information to outputs.

The configuration details of each machine may be found below. Note: Use the [Markdown Table Generator](http://www.tablesgenerator.com/markdown_tables) to add/remove values from the table.

| Name | Function | IP Address | Operating System |

|----------|----------|------------|------------------|

| Jump Box | Gateway | 10.0.0.1 | Linux |

| Web 1 | Web Server | 10.0.0.5 | Linux |

| Web 2 | Web Server | 10.0.0.6 | Linux |

| LB | Load Balancer | 40.77.47.132 | Linux |

| ELK | Elk Server | 10.1.0.4 | Linux |

**Access Policies**

The machines on the internal network are not exposed to the public Internet. Only the ELK server machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

* Home computer SSH port 5601

Machines within the network can only be accessed by JumpBox and home computer.

* Home computer port 5601
* Jumpbox IP: 10.0.0.1

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

| Name | Publicly Accessible | Allowed IP Addresses |

|----------|---------------------|----------------------|

| Jump Box | No | Home Computer from SSH |

| Web 1 | No | 10.0.0.1 from SSH |

| Web 2 | No | 10.0.0.1 from SSH |

| Elk | No | Home IP from port 5601 |

| LB |No | Home IP from port 80 |

**Elk Configuration**

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because…

* It’s simpler to deploy for the use of several apps while composing a playbook instead of writing specific code. Ansible composes containers the way you want them which is time saving.

The playbook implements the following tasks:

* Install Docker.io -Install Python3-pip -Install Docker Module -Increase Virtual Memory
* Download and launch Elk Container

### **Target Machines & Beats**

This ELK server is configured to monitor the following machines:

* Web1: 10.0.0.5
* Web2: 10.0.0.6

We have installed the following Beats on these machines:

-Filebeat and Metricbeat on Elk Stack.

These Beats allow us to collect the following information from each machine:

* Filebeat logs events, while Metricbeat uses metrics, and system statistics gathered from the server.

### Using the Playbook

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:

* Copy the /etc/ansible/files/filebeat-config.yml

file to /etc/ansible/filees/filebeat/filebeat-playbook.yml

* Update the filebeat-playbook.yml file to include... -curl -L -O <https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.6.1-amd64.deb>
* Run the playbook and navigate to Kibana/logs/add log data/system logs/ 5 Module Status/ Check data to check that the installation worked as expected.
* Repeat for Metricbeat

-For ansible, filebeat, and metricbeat, create a

my-playbook.yml,filebeat-playbook.yml and metricbeat-playbook.yml

* To test if the ELK server is running, go to Kibana on the internet and type : "Elk-VM-ExternalIP":5601/app/kibana