## Automated ELK Stack Deployment

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

CyberSec-Project-1\Diagrams\HW12\_Cloud\_Security\_Diagram.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 file may be used to install only certain pieces of it, such as Filebeat.

- filebeat-playbook.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 protected, in addition to restricting distributed denial-of-service (DDos) attacks to the network.

- load balancers protect by shifting attack traffic from the corporate server to a public cloud provider. A jump server or jump box is a system on a network that accesses and manages all the devices in a different zone of security. It is a hardened device that spans two different security zones and enables a controlled means of access between them.

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

- Filebeat is a lightweight shipper for forwarding and centralizing log data. Installed as an agent on your servers. Filebeat monitors the log files or locations that you specify, collects log events, and forwards them either to Elasticsearch or Logstash for indexing.

- Metricbeat takes the metrics and statistics that it collects and ships them to the output that you specify, such as Elasticsearch or Logstash. Metricbeat helps you monitor your servers by collecting metrics from the system and services running on the server, such as: Apache.

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 | 10.1.0.4 | Linux |

| Web1 | | 10.1.0.5 | Linux |

| Web2 | | 10.1.0.6 | Linux |

| ELK\_VM | | 10.2.0.4 | Linux |

### Access Policies

The machines on the internal network are not exposed to the public Internet.

Only the JumpBox machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

- 72.141.33.50

Machines within the network can only be accessed by 20.70.197.215

- Jump Box can access ELK VM through IP address 20.70.197.215

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

| Name | Publicly Accessible | Allowed IP Addresses |

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

| Jump Box | Yes | 10.1.0.5 10.1.0.6 |

| Web1 | No | 10.1.0.4 |

| Web2 | No | 10.1.0.4 |

### Elk Configuration

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

- the main advantage of automating configuration with Ansible is it automates and simplifies repetitive, complex, and tedious operations.

The playbook implements the following tasks:

* Install docker

Sudo -i

Docker ps -a

* download image

docker start objective\_booth

docker attach objective\_booth

* open ansible folder

cd /etc/ansible

ls

* add this in ansible host file

[webservers]  
10.1.0.5 ansible\_python\_interpreter=/usr/bin/python3

10.1.0.6 ansible\_python\_interpreter=/usr/bin/python3

* install yaml file

ansible-playbook ./install-elk.yml

The following screenshot displays the result of running `docker ps` after successfully configuring the ELK instance.

CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES

cf76b58667ce cyberxsecurity/ansible "/bin/sh -c /bin/bas…" 3 weeks ago Exited (127) 6 seconds ago objective\_booth

### Target Machines & Beats

This ELK server is configured to monitor the following machines:

- 10.1.0.4

We have installed the following Beats on these machines:

- Filebeat

- Metricbeat

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

- Filebeat monitors the log files or locations that you specify, collects log events, and forwards them either to Elasticsearch or Logstash for indexing.

- Metricbeat takes the metrics and statistics that it collects and ships them to the output that you specify, such as Elasticsearch or Logstash.

### 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 yaml file to folder.

- Update the host file to include [webservers]

- Run the playbook, and navigate to folder to check that the installation worked as expected.

\_TODO: Answer the following questions to fill in the blanks:\_

- \_Which file is the playbook? Where do you copy it? Filebeat\_playbook.yml is copied to /etc/ansible folder

- \_Which file do you update to make Ansible run the playbook on a specific machine? How do I specify which machine to install the ELK server on versus which to install Filebeat on?\_

host file in /etc/ansible folder is updated with

[webservers]  
10.1.0.5 ansible\_python\_interpreter=/usr/bin/python3

10.1.0.6 ansible\_python\_interpreter=/usr/bin/python3

- \_Which URL do you navigate to in order to check that the ELK server is running? http://20.213.52.194/

\_As a \*\*Bonus\*\*, provide the specific commands the user will need to run to download the playbook, update the files, etc.\_