## Automated ELK Stack Deployment

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

Elk Playbook: <https://github.com/Primus-Palus/cybersecurityhub/blob/main/cybersecurityhub/Ansible/install-elk.yml>

Diagram: Diagram

Description automatically generated

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

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, in addition to restricting access to the network.

What aspect of security do load balancers protect? What is the advantage of a jump box?

* Load balancers prevent situations like DDoS where too much information is being pushed onto the machine.
* Jump Box allows a single point of contact with SSH/HTML/etc and security policies to prevent outside access.

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

- What does Filebeat watch for?

* Filebeat monitors log files or locations and collects log events.

- What does Metricbeat record?

* It periodically collects metrics from the OS and services, and ships them to an output like Elasticsearch.

The configuration details of each machine may be found below.

| Name | Function | IP Address | Operating System |

| |

| Jump Box | Gateway | 10.0.0.1 | Linux |

| Web 1 | Server/Database | 10.0.0.5 | Ansible |

| Web 2 | Server/Database | 10.0.0.6 | Ansible |

| Elk Server | Server/Database | 10.1.0.4 | Ansible |

### Access Policies

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

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

* 97.122.253.220

Machines within the network can only be accessed by jumpbox ansible container.

Which machine did you allow to access your ELK VM? What was its IP address?

* Jumpbox - 104.42.150.220
* Personal Computer - 97.122.253.220

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

* Jump Box
* 104.42.150.220 (Public)

| Name | Publicly Accessible | Allowed IP Addresses |

| Jump Box | Yes | 97.122.253.220 |

| Web 1 | No | 104.42.150.220 |

| Web 2 | No | 104.42.150.220 |

| Elk Server | No | 104.42.150.220 |

### Elk Configuration

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

What is the main advantage of automating configuration with Ansible?

* Makes it easier to set up multiple Ansible containers and install/run processes included.

The playbook implements the following tasks:

In 3-5 bullets, explain the steps of the ELK installation play. E.g., install Docker; download image; etc.\_

* Create Elk VM in Azure
* Install Docker on Elk Server
* Run yml file to install Elk processes, Metricbeat, and Filebeat
* Edit config files
* Edit Hosts.txt

UNABLE TO COMPLETE EVERYTHING DUE TO EXPIRED SUBSCRIPTION AND LOSS OF VIRTUAL NETWORK

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

Update the path with the name of your screenshot of docker ps output](Images/docker\_ps\_output.png)

### Target Machines & Beats

This ELK server is configured to monitor the following machines:

List the IP addresses of the machines you are monitoring:

Web 1 - 137.135.49.146

Web 2 - 137.135.49.146

We have installed the following Beats on these machines:

Specify which Beats you successfully installed

* Filebeat
* Metricbeat

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

In 1-2 sentences, explain what kind of data each beat collects, and provide 1 example of what you expect to see. E.g., `Winlogbeat` collects Windows logs, which we use to track user logon events, etc.

* Metricbeat collects system information, cpu, running processes, etc.
* Filebeat collects data on server usage to include apps, users, connections, file access locations, etc.

### Using the Playbook

Answer the following questions to fill in the blanks:

* Which file is the playbook? Where do you copy it?
  + Filebeat-playbook.yml
  + Metricbeat-playbook.yml
* 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?
  + Hosts.txt
  + By the yml and config files.
* Which URL do you navigate to in order to check that the ELK server is running?
  + http://20.102.126.174:5601/app/kibana