

Billy Smith - CyberSecurity Homework Week 13

03/2021

[**Description of the Topology**](#_t6mee1qa15ba) **6**

[**Access Policies**](#_1093mqmtdvf) **7**

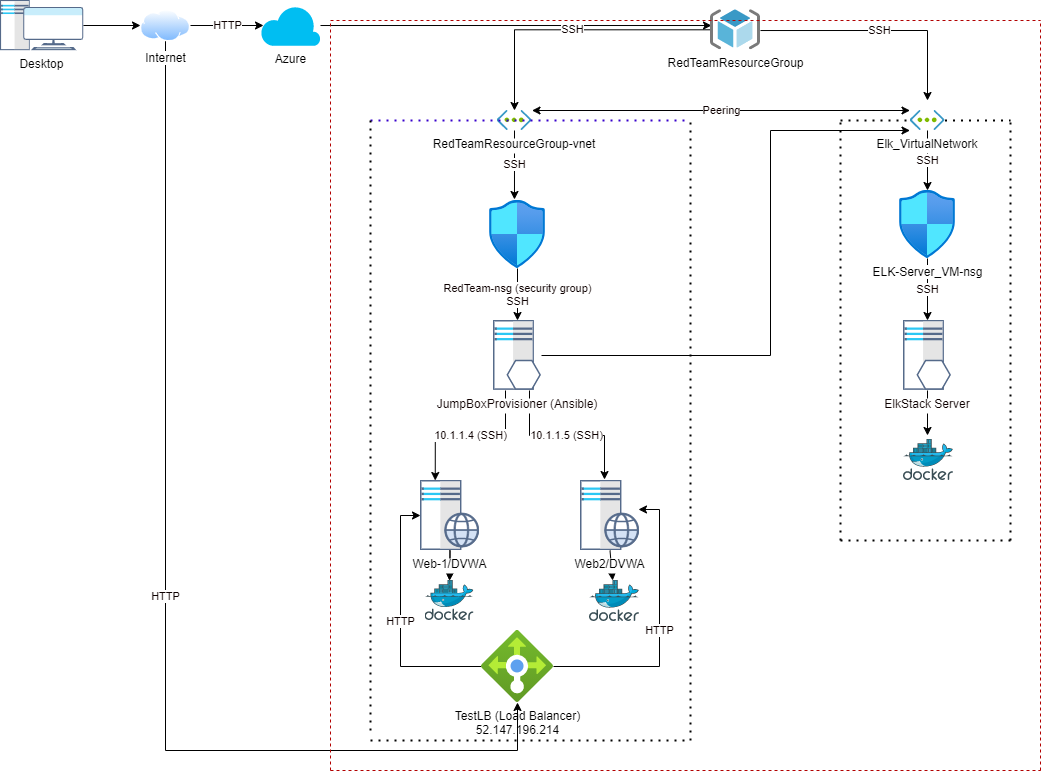
[**Elk Configuration**](#_8qzzeecyq53f) **7**

[**Target Machines & Beats**](#_fxn63zypawmq) **8**

[**Using the Playbook**](#_o3v8j338p52t) **8**

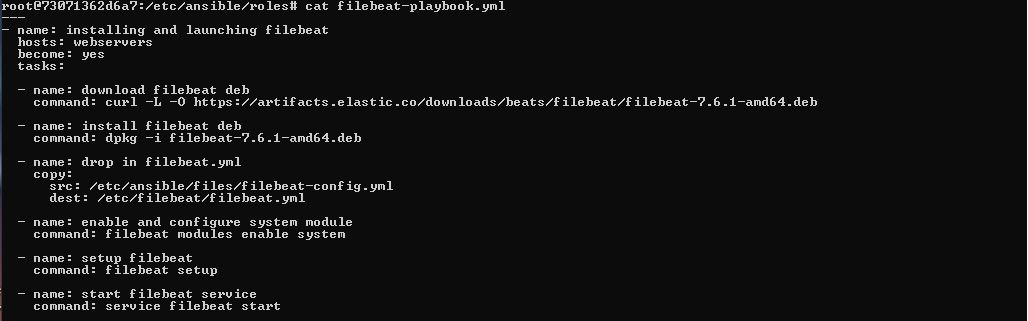
Automated ELK Stack Deployment

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

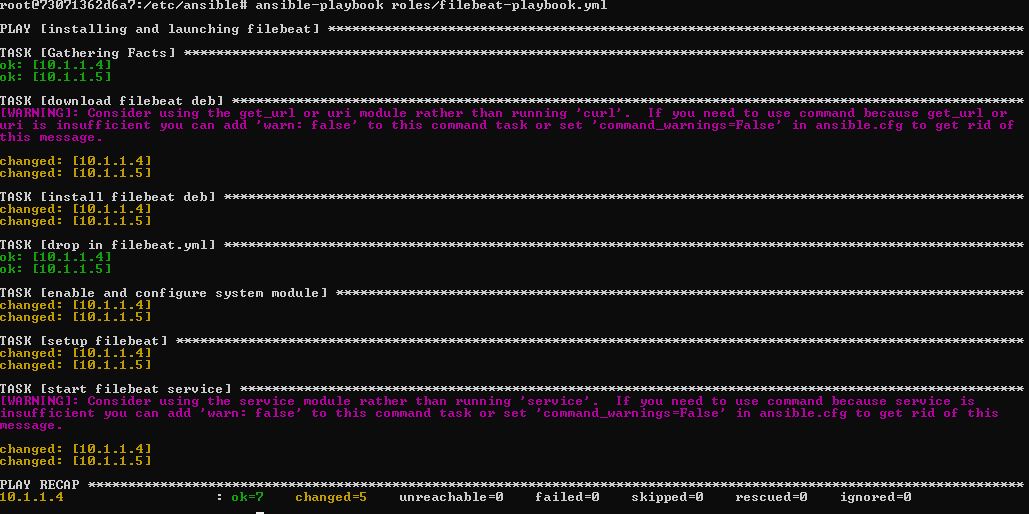


These files have been tested and used to generate a live ELK deployment on Azure. They can be used to either recreate the entire deployment pictured above. Alternatively, select portions of the filebeat\_playbook.yml and metricbeat\_playbook.yml file may be used to install only certain pieces of it,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

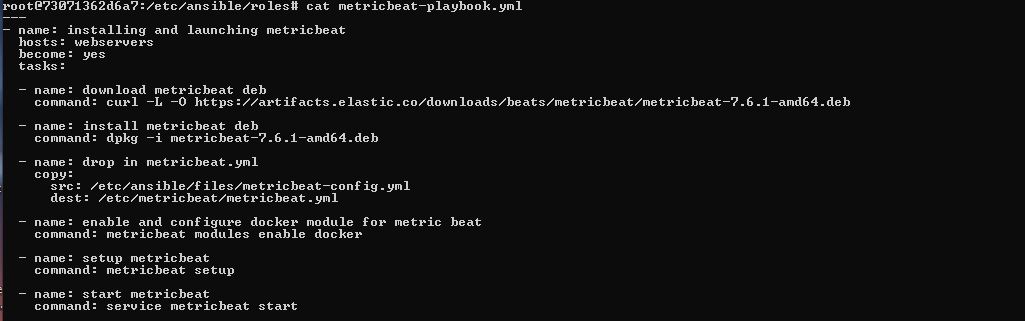
**Filebeat-playbook.yml:**



**Running playbook:**



**Metricbeat-playbook.yml:**



**Running 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 ensures that the application will be highly available, in addition to restricting unapproved access to the network.

The load balancers will address the availability of the web servers as it will monitor the available resources for the servers, and also if the server is available to accept connections. If one of the servers is unavailable, all connections will be sent to surviving servers, until the unavailable server is responding again. Once responding, the server will be put back into the rotation, by the load balancer.

The jump box is designed as a portal into the internal network. With a jump box, traffic trying to enter the internal network can be monitored more effectively and firewall rules are able to be assigned accordingly to less devices.

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the monitored systems and system resources.

Within the ELK server we are collecting system logs for the web servers, using Filebeat. As different resources may send files with minor differences, such as timestamp formatting, using Filebeat along with ElasticSearch/LogStash provides a consistent formatting for the logs to make them easier to read and search through. With this capability, it is easier to go through multiple logs from multiple resources using the same search parameters.

As often the case, we also need to monitor the resources that are being used by a node on the network, over port 5066. With Metricbeat, we are able to collect these resources and take action if we see any nodes reporting resources that are out of line of what we are expecting to see.

The configuration details of each machine may be found below.

| Name | Function | IP Address | Operating System |

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

| Jump Box | Gateway | 10.0.0.1 | Linux Ubuntu |

| Web-1 | Webserver/DVWA | 10.1.1.4 | Linux Ubuntu |

| Web-2 | Webserver/DVWA | 10.1.1.5 | Linux Ubuntu |

| ELK Server | Log Server | 10.3.0.4 | Linux Ubuntu |

# Access Policies

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

Only the jump box machine can accept connections from the Internet. Access to this machine is only allowed from the following IP address: 76.182.5.204

Machines within the network can only be accessed by the jump box. The IP used for jump box access is the internal IP address of 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 | Yes | 76.182.5.204 |

| Web-1 | No | 10.0.0.1 |

| Web-2 | No | 10.0.0.1 |

| ELKStack server config | No | 10.0.0.1 |

| ELKStack server Access | Yes | 76.182.5.204 |

# Elk Configuration

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because it is guaranteed that all exported installs are exactly the same and it is an expected configuration. Any changes or updates that need to be made can be automated and pushed to all configured machines.

This reduces that time to deploy standard configurations and allows for remote deployments.

The playbook implements the following tasks:

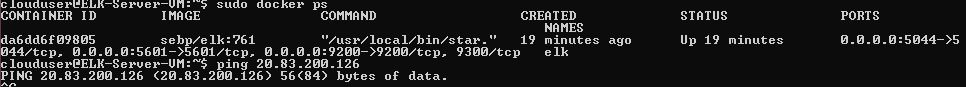
- Downloads the configured image to the destination servers (Docker, Apache, etc)

- Installs the configured image

- Configures the settings, if necessary (ports)

- Starts the software

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



# Target Machines & Beats

This ELK server is configured to monitor the following machines: 10.1.1.4 and 10.1.1.5

We have installed the following Beats on these machines:

We have installed filebeat and metricbeat on the machines that we are going to be monitoring

Filebeat monitors and collects the system logs and presents them to the configured ELK server for analysis and any deemed actions that need to be taken. This can be used to monitor for account creations or log in attempts

Metricbeat, as with Filebeat monitors and collects data from the system it is installed on. The difference is that metricbeat collects information from the operating system and services running on the server, and it presents this information to the ELK 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 filebeat-playbook.yml and metricbeat-playbook.yml files to /etc/ansible/roles.

- Update the hosts file to include headers such as [server] and add the IP addresses/hostnames under the header.

Example:

[webservers]

10.1.1.4

10.1.1.5

[ELK]

10.3.0.4

- Run the playbook, and navigate to http://20.83.200.126:5601/ to check that the installation worked as expected.

# Running the Playbook

The following commands will be used to run the playbook for filebeat and metricbeat:

ansible-playbook roles/filebeat-playbook.yml

ansible-playbook roles/metricbeat-playbook.yml