**Automated-ELK-Stack-Deployment-Project-1**

Jaime Brown

09/23/2021

Cybersecurity Boot Camp

**Automated ELK Stack Deployment**

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

[Project 1 Red-Team Network Diagram](https://github.com/zaidR17/Automated-ELK-Stack-Deployment-Project-1/blob/master/Diagrams/Project%201%20Red-Team%20Network%20Diagram.PNG)

\*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 Project 1 Red-Team Network Diagram file may be used to install only certain pieces of it, such as Filebeat.

[filebeat-playbook.yml](https://github.com/zaidR17/Automated-ELK-Stack-Deployment-Project-1/blob/master/Ansible/filebeat_playbook.yml.txt)

[filebeat-configuration.yml](https://github.com/zaidR17/Automated-ELK-Stack-Deployment-Project-1/blob/master/Linux/filebeat_configuration.yml.txt)

\*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 functional, in addition to restricting high-traffic to the network.
* What aspect of security do load balancers protect?
  + It helps prevent overloading servers as well as optimizes productivity and maximizes uptime.
  + It also adds resiliency by rerouting live traffic from one server to another causing it to eliminate single points of failure from attacks such as DDoS attack.
* What is the advantage of a jump box?

-Jump-box are highly secured computers that are never used for non-admin tasks. -Throughout the years, jump-box has improved into an even more comprehensive/lock-down secure admin workstation to decrease the chances of hackers/malware infection.

\*Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the \_\_\_network and system logs.

* What does Filebeat watch for?
  + It monitors the log files/locations that you specify and forwards them to Elasticsearch/Logstash for indexing.
* What does Metricbeat record?
  + It records metrics/statistics data and transports them to the output that you specifics thru Elasticsearch/Logstash.

\*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-Provisioner | Gateway | 10.1.0.4Private)// [52.143.98.189](https://portal.azure.com/?bundlingKind=DefaultPartitioner&configHash=DRv5SbqTHAR-&env=portal&helppanenewdesign=true&helppanevmproblemcards=false&l=en.en-us&pageVersion=8.202.0.5724084.210910-1523)  (Public) | Linux |
| ELK-VM | Server | 10.2.0.4(Private)//  20.106.140.33  Public) | Linux |
| Web-1 | Server | 10.1.0.5(Private) | Linux |
| Web-2 | Server | 10.1.0.6 (Private) | Linux |

**Access Policies**

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

* Only the jump-Box-Provisioner machine can accept connections from the Internet.
* Access to this machine is only allowed from the following IP addresses:
* 204.98.80.94
  + (LocalHost IP address)

\*Machines within the network can only be accessed by Jump-Box-Provisioner

* Which machine did you allow to access your ELK VM?
  + Jump-Box-Provisioner
* What was its IP address?
  + 10.0.0.4 (Private)
* A summary of the access policies in place can be found in the table below.

| **Name** | **Publicly Accessible** | **Allowed IP Addresses** |
| --- | --- | --- |
| Jump-Box-Provisioner | Yes | 204.98.80.94 |
| ELK-VM\* | No | 10.2.0.4 |
| Web-1\* | No | 10.1.0.5 |
| Web-2\* | No | 10.1.0.6 |

* --All these VMs can only be accessed form the Jump-Box-Provisioner--

**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?
  + One main advantage would be YAML Playbooks. It is the best alternative for configuration management/automation.
  + It is also able to automate complex multi-tier IT application environments.

\*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.\_
  + First I, SSH into the Jump-Box-Provisioner (ssh redadmin@40.117.224.154)
  + Start/Attached to the ansible docker (sudo docker start tender\_morse)/(sudo docker attach tender\_morse)
  + Went to /etc/ansible/roles directory and created the ELK playbook (Elk\_Playbook.yml)
  + Ran the Elk\_Playbook.yml in that same directory (ansible-playbook Elk\_Playbook.yml)
  + Lastly, I SSH into the ELK-VM to verify the server is up and running.

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

[ELK-VM Docker PS](https://github.com/zaidR17/Automated-ELK-Stack-Deployment-Project-1/blob/master/Diagrams/Project%201%20Red-Team%20Network%20Diagram.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 (10.1.0.5)
  + Web-2 (10.1.0.6)
* We have installed the following Beats on these machines:
  + [Filebeat Module Status Screenshot](https://github.com/zaidR17/Automated-ELK-Stack-Deployment-Project-1/blob/master/Images/Filebeat_Module_Status.PNG)
  + [Metricbeat Module Status Screenshot](https://github.com/zaidR17/Automated-ELK-Stack-Deployment-Project-1/blob/master/Images/Metricbeat_Module_Status.PNG)

\*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.\_
  + Filebeat is used to collect log files from specific files on remote machines.
  + Examples of Filebeats can be files that are generated by Apache, Microsoft Azure tools, the Nginx web server, and MySQl databases.
  + Metricbeat collects machine metrics.
  + It is simply a measurement to tell analysts how healthy it is.
  + Examples of Metricbeat can be CPU usage/Uptime

**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:

---Filebeat---

* Copy the filebeat-configuration.yml file to /etc/ansible/roles/files.
* Update the filebeat-configuration.yml file to include the ELK private IP in lines 1106 and 1806.

Run the playbook, and navigate to <http://20.106.140.33:5601/> (ELK-VM public IP) to check that the installation worked as expected.

---Metricbeat---

* Copy the metricbeat-configuration.yml file to /etc/ansible/roles/files.
* Update the metricbeat-configuration.yml file to include the ELK private IP in lines 62 and 96.

Run the playbook, and navigate to http:// 20.106.140.33:5601/ (ELK-VM public IP) to check that the installation worked as expected.

*Answer the following questions to fill in the blanks:*

* \_Which file is the playbook? filebeat-playbook.yml
* \_Where do you copy it? /etc/ansible/roles
* \_Which file do you update to make Ansible run the playbook on a specific machine? /etc/ansible/hosts file (IP of the Virtual Machines).
* \_How do I specify which machine to install the ELK server on versus which to install Filebeat on? I have to specify two separate groups in the etc/ansible/hosts file. One of the groups will be webservers which has the IPs of the VMs that I will install Filebeat to. The other group is named elkservers which will have the IP of the VM I will install ELK to.

\_Which URL do you navigate to in order to check that the ELK server is running? <http://20.106.140.33:5601/>

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