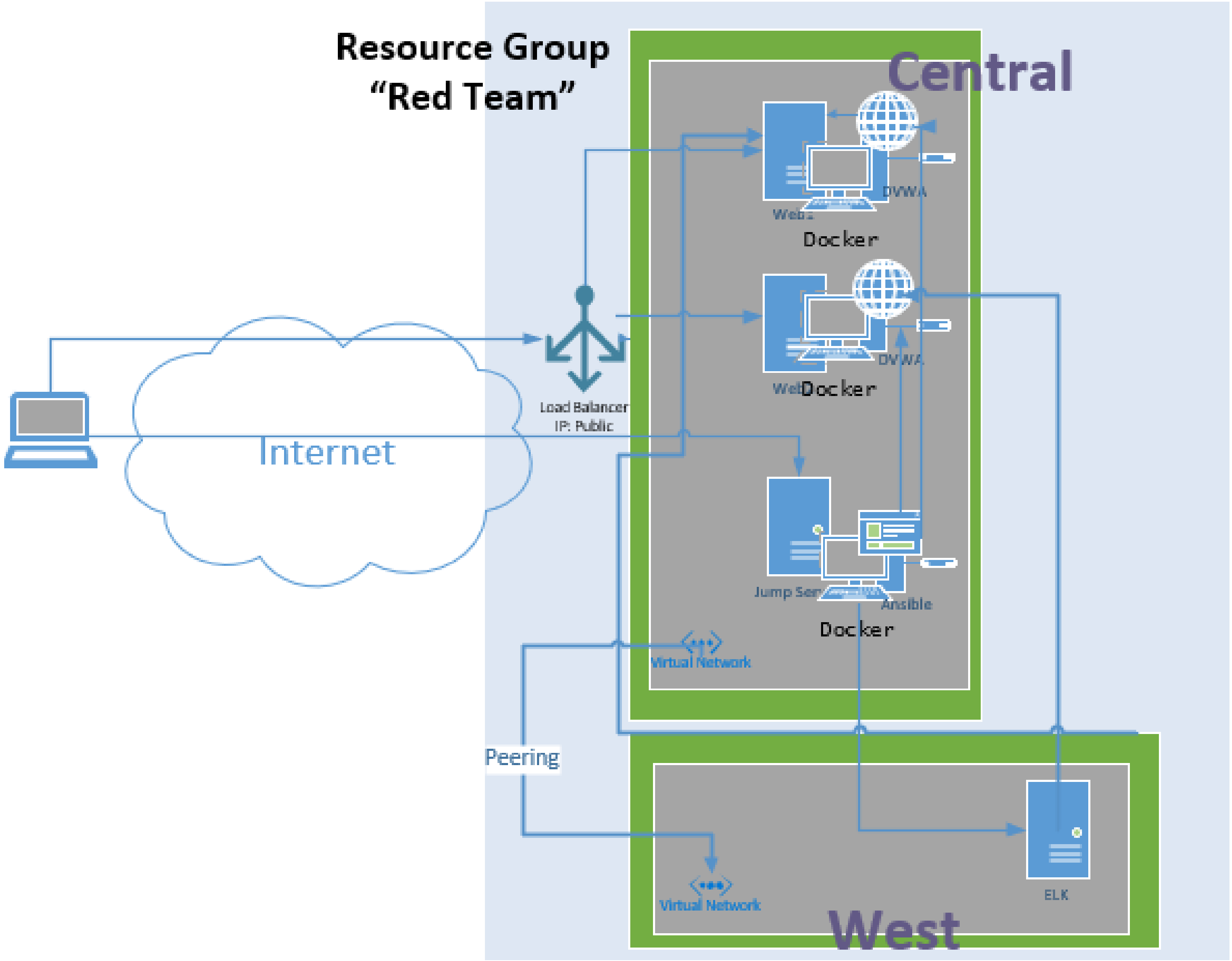
ELK Project

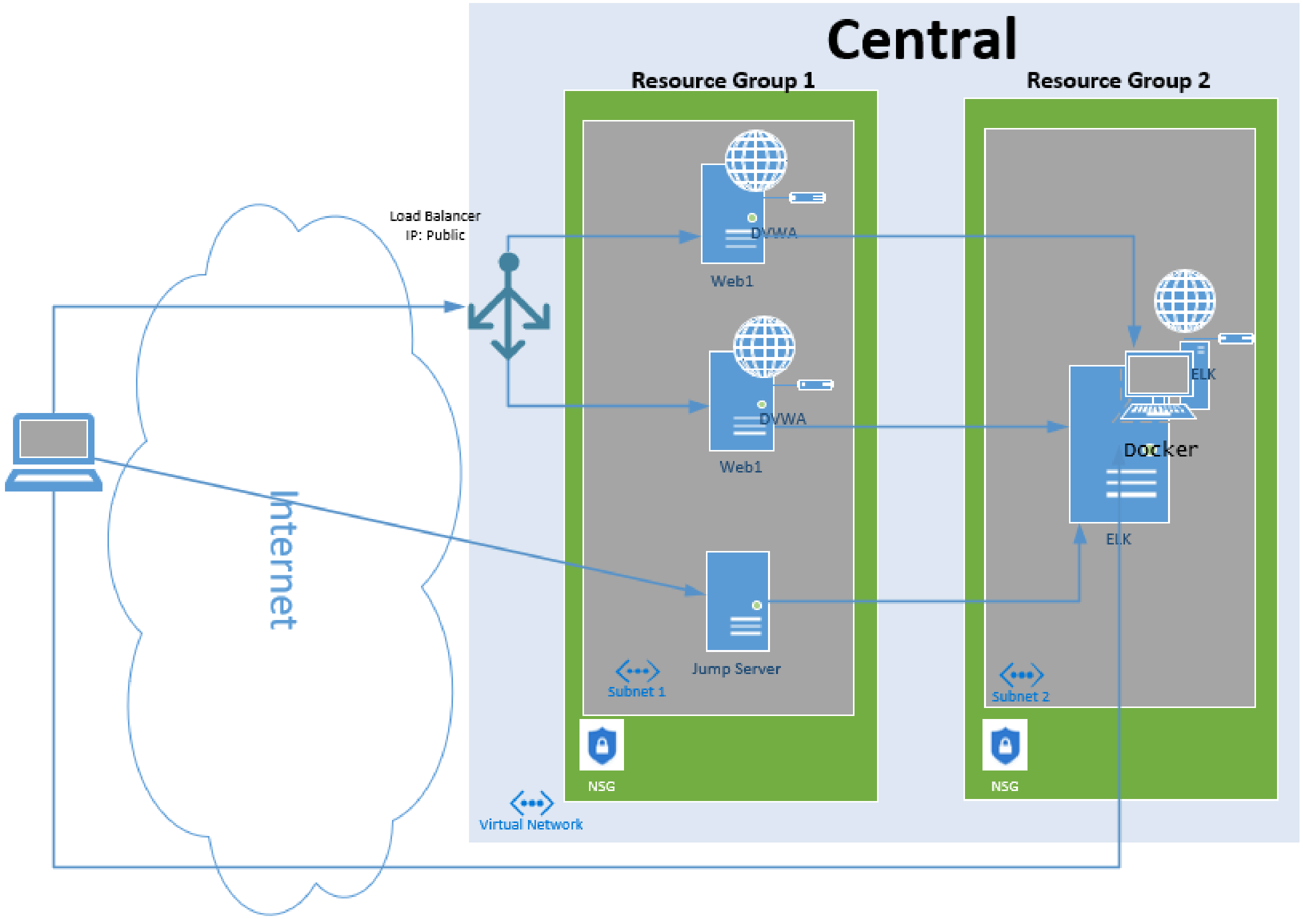
Day 1
Start

Original Project



Resource Group
“Red Team”

New Project


Central
Resource Group 1
Resource Group 2
Load Balancer
IP: Public
DVWA
Web1
DVWA
Web1
Jump Server
Subnet 1
NSG
ELK
Docker
ELK
Subnet 2
NSG
Virtual Network
Internet

Before You Continue Building

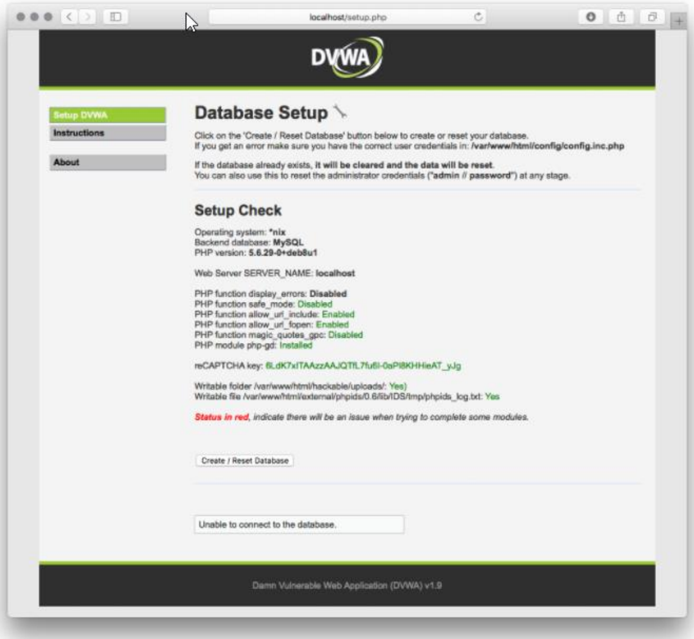
Check DVWA!

DVWA Check

1. Browse to your newly built DVWA Solution

2. Log in using the instructions below and set the difficulty level

machine:



Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: **/var/www/html/config/config.inc.php**

If the database already exists, **it will be cleared and the data will be reset.**
You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

Setup Check

Operating system: ***nix**
Backend database: **MySQL**
PHP version: **5.6.29-0+deb8u1**

Web Server SERVER_NAME: **localhost**

PHP function display_errors: **Disabled**
PHP function safe_mode: Disabled
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module php-gd: Installed

reCAPTCHA key: 6LdK7xITAAzzAAJQTfL7fu6I-0aPl8KHHieAT_yJg

Writable folder /var/www/html/hackable/uploads/: Yes)
Writable file /var/www/html/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt: Yes

***Status in red**, indicate there will be an issue when trying to complete some modules.*

Unable to connect to the database.

Damn Vulnerable Web Application (DVWA) v1.9

Just click on the `Create / Reset database` button and it will generate any aditional configuration needed.

Login with default credentials

https://hub.docker.com/r/vulnerables/web-dvwa

1. Create New Resource Group

2. Create New Subnet in Existing Virtual Network

3. Create New NSG w/ Deny(s)

4. Associate NSG to Subnet

Build a New Virtual Machine

- Create a new VM
  1. Within the new Resource Group
  2. Name it Elk
  3. Ubuntu
  4. B Size – 2 CPU and 4 GB mem
  5. With public IP

Connect and Configure

1. Allow SSH access from the Jumpbox to the new Elk Server
2. Connect to the Elk server from the jumpbox over SSH
3. Run the Elk Bash Script

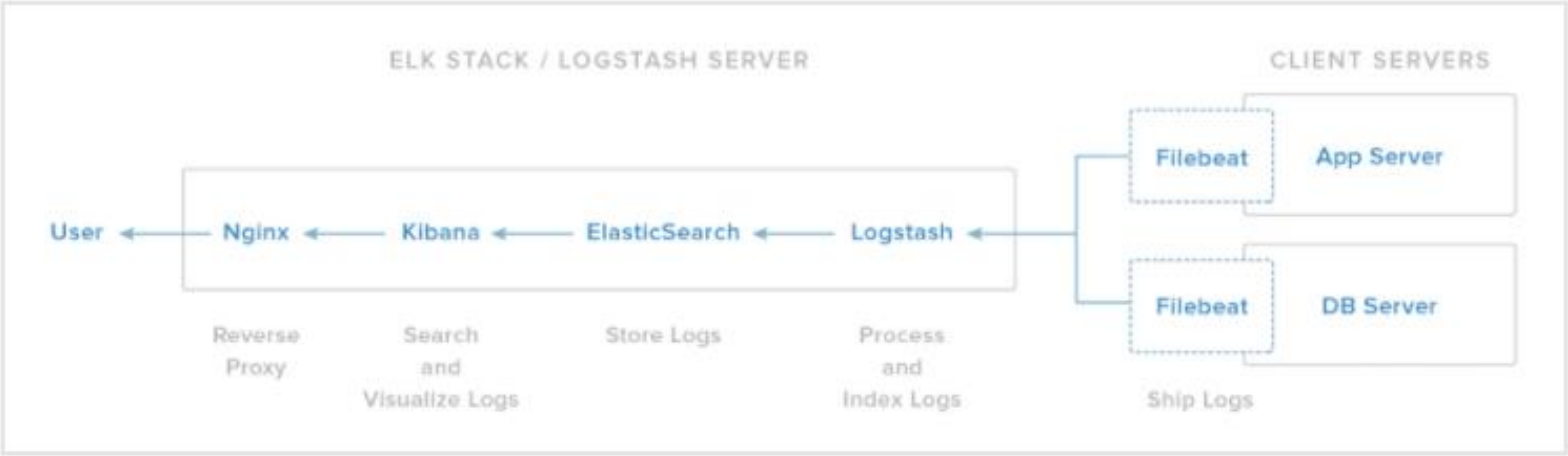
Connect and Logon

1. Allow access to Elk over TCP 5601 from your home network
2. Browse to http://Your_IP:5601/app/kibana
3. Login to change the default password

Day 1
Complete

Day 2
Start

Push Logs from Web Servers to ELK



FileBeat Installation and Configuration

1. SSH into the Web Server through the Jumpbox
2. Execute the FileBeat Script
3. Update the Config File at /etc/filebeat/filebeat.yml
4. Scroll to line #1106 and replace the IP address with the IP address of your ELK machine.
5. Next, Update the Password.

```
output.elasticsearch:
hosts: ["10.1.0.4:9200"]
username: "elastic"
password: "changeme"
```

6. Scroll to line #1806 and replace the IP address with the IP address of your ELK machine.

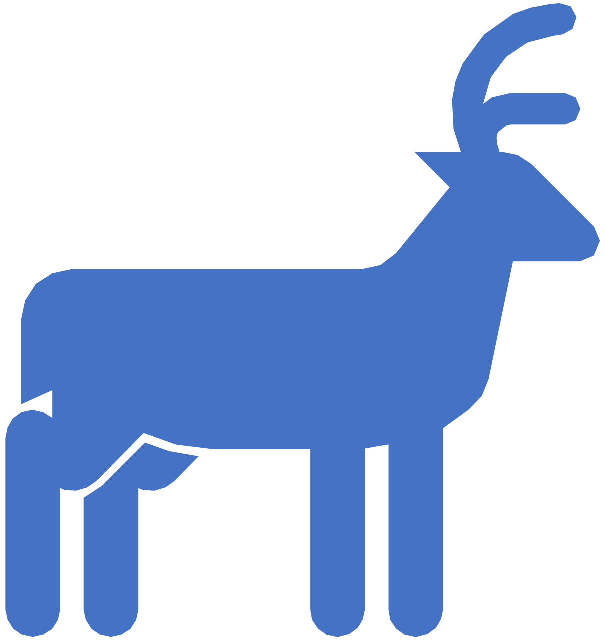
```
setup.kibana:
host: "10.1.0.4:5601"
```

https://www.elastic.co/guide/en/beats/filebeat/6.8/filebeat-installation.html

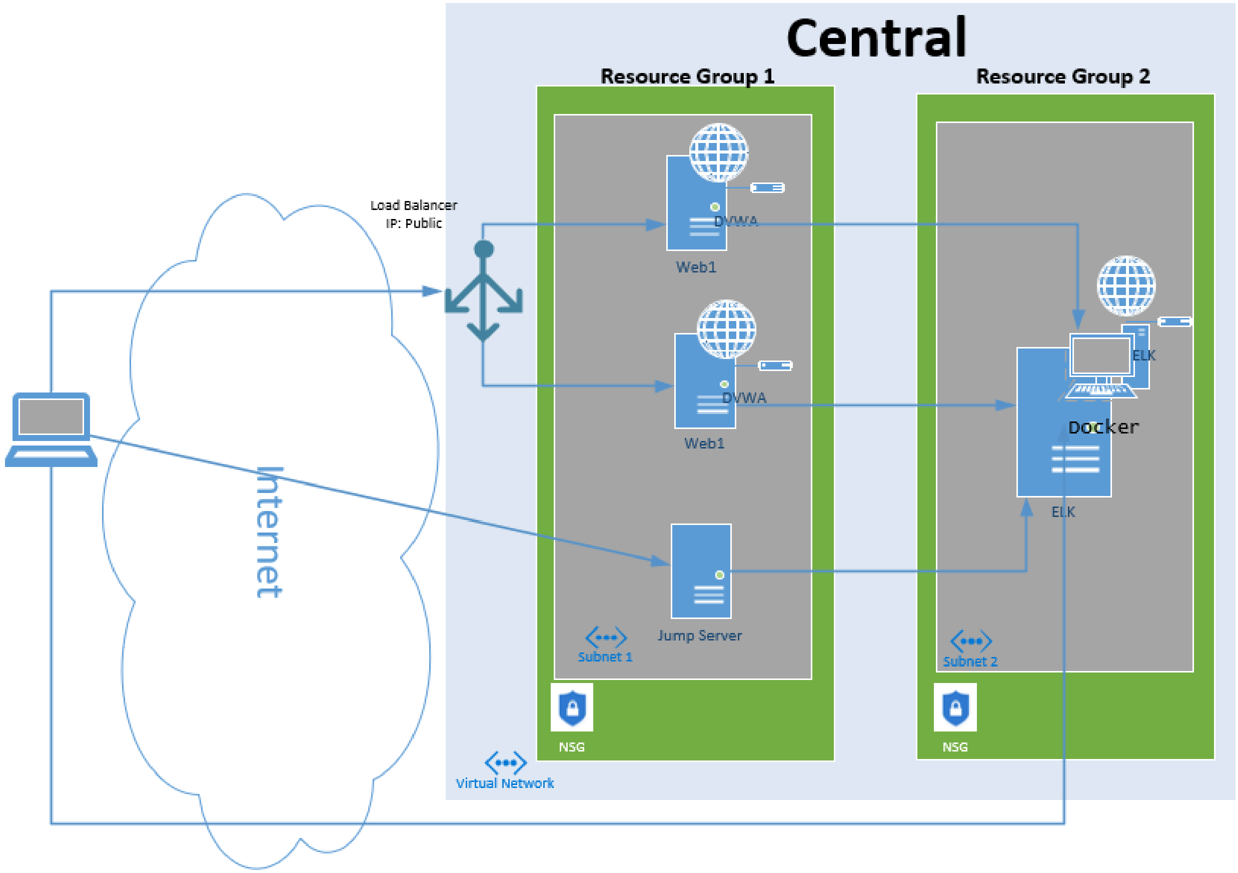
Open Needed Ports

1. Open the needed port from Web Servers to ELK *9200*
2. *After, Start the Filebeat on the Web Server*

```
filebeat modules enable system
filebeat setup
service filebeat start
```



Final Elk Project



Day 2
End

Day 3
Start

Home Work

- Create a Github Repository - https://www.youtube.com/watch?v=XtCcoMd6U_4
- Upload your scripts
- Create a Network Diagram and Upload it

Submit

- Word Document Including
  - Explain what you learned (two or more paragraphs)
  - Link to your Github Repository

Day 3
End