ACTI 4850 – Lab 3 – Security Improvements and Integrations

Instructor	Mike Mulder (mmulder10@bcit.ca)
Total Marks	10
Due Dates	Demo Due by End of Lesson 4 Class (Jan 29th for Set C, Jan. 20th for Set B, Feb. 1 for Set A)

Applicable Requirements

- **REQ1010** – The Enterprise Development Environment shall be prototyped on Microsoft Azure cloud infrastructure.
- **REQ1100** – The Enterprise Development Environment shall provide access to applications on the web through a single web application server acting as a reverse proxy. The reverse proxy will be implemented using Apache2.
  Note: This web application server provides a single point of access from the public internet and can be used for SSL termination.
  Note: For this prototype, this web application server will be used for Confluence and JIRA which run by default on non-standard ports.
- **REQ1110** – The Enterprise Development Environment shall have a Communication capability. The Communication tool will be Slack.
- **REQ1120** – The Communication capability shall be capability of receiving automatic notifications from other tools. For this prototype, notifications will be reported from GitLab.
- **SEC1020** – All web applications and API endpoints shall be encrypted (i.e., https endpoints).
  Note: Self-signed certificates are sufficient for the prototype environment.

Group Work

You will be working on the same Azure cloud environment as the previous lab, shared with your Lab partner. This lab will be done together with your partner.

Reverse Proxy Installation

Step 1 – Create a Virtual Machine in Azure

Create a Linux Virtual Machine (using the Virtual Machines Service) with the following specifications under your Azure for Students subscription:

- Resource group name: Apache
- Virtual machine name: Apache
- Region: (US) East US (or another region where the B1s is available)
- Image: Ubuntu 20.04 LTS – Gen1 or Gen2
- Size: B1s (we don't require a lot of vcpus or memory for apache)
- Authentication Type: SSH public key (create an SSH key if necessary and paste in the public key)
- Inbound Ports: Allow SSH (22)

Leave everything else at the defaults and Create the Virtual Machine. This may take a few minutes.

Create a DNS Name for your Apache Virtual Machine that is named similar to:

acit4850-group<group #>.<region>.cloudapp.azure.com

Add an inbound security rule that allows access to your Virtual Machine on port 80. You can also add one on ports 80 and 443 now as well if you wish as you'll need it later in the lab.

Step 2 – Install Apache2

Login to your Virtual Machine using ssh.

Run the following commands to install Apache2:

- sudo apt update
- sudo apt install apache2

Verify your Apache2 installation:

- apache2 -version

Apache2 version 2.4.x should be installed.

Open up access to Apache on the Ubuntu firewall:

- sudo ufw app list *Note: There are 3 Apache profiles: Apache, Apache Full, Apache Secure*

Open up the Apache profile, which allows access on port 80

- sudo ufw allow 'Apache'

Check the status of Apache2 with the following command:

- sudo systemctl status apache2

The Apache HTTP Server should be started.

On your web browser, check that you can access the Apache server by going to the following URL:

- http://<Your_Virtual_Server_DNS_Name>
- You should see a page titled "Apache2 Ubuntu Default Page"

If you don't see the above page, make sure you have Port 80 open on your VM (i.e., add an Inbound Port Rule).

Step 3 – Configure Apache as a Reverse Proxy for JIRA and Confluence

You need to setup the Apache Reverse Proxy so that JIRA and Confluence are available on the following URLs:

- http://<Your_Virtual_Server_DNS_Name>/jira
- http://<Your_Virtual_Server_DNS_Name>/confluence

Follow the steps here to setup Apache2 as a reverse proxy with Atassian products. Do this for both Confluence and JIRA (if working with a partner). Make sure your VMs are running.

- https://confluence.atlassian.com/kb/proxying-atlassian-server-applications-with-apache-http-server-mod_proxy_http-806032611.html

Notes:

- You DO NOT need to create separate site configurations in the /etc/apache2/sites-available folder. You can just edit the existing 000-default.conf (and later the default-ssl.conf).
- **When you modify configuration files (in Apache, Confluence or JIRA), make a backup first so you have something to compare with or revert back if necessary.**
- You will have to change your root URL for Confluence/JIRA in the admin settings of the applications to be that of the reverse proxy, otherwise users will get warnings that the URL being used doesn't match the one configured in the application.
- You also need to add the Confluence /synchrony endpoint in the VirtualHost of the Apache server

Step 4 – Network Security Groups

Update your Network Security Groups for your Virtual Machines running Confluence and JIRA.

Confluence Virtual Machine

- Change the inbound rules such that access to port 8090 and 8091 is only allowed from the Apache Virtual Machine. Use the public IP of the Apache VM and make sure you reserve that IP when you shutdown that VM.

JIRA Virtual Machine

- Change the inbound rules such that access to port 8080 is only allowed from the Apache Virtual Machine. Use the public IP of the Apache VM and make sure you reserve that IP when you shutdown that VM.

Step 5 – Testing Your Reverse Proxy

Make sure you can now access JIRA and Confluence from the following URLs:

- http://<Your_Apache Virtual_Server_DNS_Name>/jira
- http://<Your_Apache Virtual_Server_DNS_Name>/confluence

And you can no longer access them through their previous URLs directly on the Confluence and JIRA VMs.

Step 6 – Adding a Self-Signed Certificate and SSL

Follow the instructions here to create and configure a self-signed certificate in your Apache web server.

https://www.digitalocean.com/community/tutorials/how-to-create-a-self-signed-ssl-certificate-for-apache-in-ubuntu-20-04

Notes:

- When creating the self-signed certificate, use the DNS name for your Virtual Machine

- **You will have to transfer over your reverse-proxy configurations from Step 3 to your non-ssl configuration file (Apache Virtual Host on port 80) to the ssl-configuration file (Apache Virtual Host on port 443)**
- Update the non-ssl configuration file (000-default.conf) to redirect requests on http port 80 to https port 443 (as per the instructions in the above site)
- You will need to both port 80 and 443 open for inbound access on your Apache Virtual Machine

Step 7 – Testing Your Self-Signed Certificate

Make sure you can now access JIRA and Confluence from the following URLs:

- https://<Your_Virtual_Server_DNS_Name>/jira
- https://<Your_Virtual_Server_DNS_Name>/confluence

Because your SSL certificate is self-signed, you will have to accept the risk of an untrusted certificate. In a production installation you would get rid of this you by having your certified signed by a trusted signing authority (which costs some money depending on the quality of the signature).

Note that if you try to access the URL using http it should redirect you to the URL using https.

GitLab to Slack (or Discord) Integration

Alternately, you can setup a Discord integration instead if you already have a Discord Server.

Follow the instructions here in that case:
https://docs.gitlab.com/ee/user/project/integrations/discord_notifications.html

Create a Slack workspace for you and your partner called acit4850_fall2020_groupX (where X is your group number). Make sure both of you have access.

You will need to startup your GitLab Virtual Machine.

Follow the instructions here to integrate GitLab and Slack:

https://docs.gitlab.com/ee/user/project/integrations/slack.html

- Create a private channel in your Slack workspace called gitlab
- In your existing Project in GitLab, configure it to report notifications to your gitlab Slack channel for the following events:
    - Push
    - Merge Requests

Test that a push of a code change to the project results in a notification message in your Slack channel.

Make sure you shutdown any Azure resources (i.e., the VM) to conserve your credits and free tier usage.

Demo, Grading and Submission

A demo of your lab against the applicable requirements which will determine your grade on the lab. All mandatory requirements must be met otherwise you will receive zero on the lab. You can re-demo the lab if you haven't met the mandatory requirements, up to the last class before the midterm week, but you will lose 20% every week late.

Reqt.	Mandatory	Demo	Marks
REQ1010	Yes	• Show your Azure dashboard (both students). • Show your running VM for the Apache2 web server.	2
REQ1100	Yes	• Show your JIRA instance is accessible though the reverse proxy (if working with a partner). • Show your Confluence instance is accessible through the reverse proxy.	4
REQ1110	Yes	• Demonstrate that a push request to your GitLab repository results in a notification reported to your Slack channel.	2
SEC1020	No	• Your reverse proxy is configured to use an SSL self-signed certificate. • Requests to URLs with http on port 80 are required to https on port 443.	2
Total			**10**

Submit a screenshot of your URLs for Confluence and JIRA in a browser using the reverse proxy and SSL.