Cybersecurity

Project 1 Technical Brief

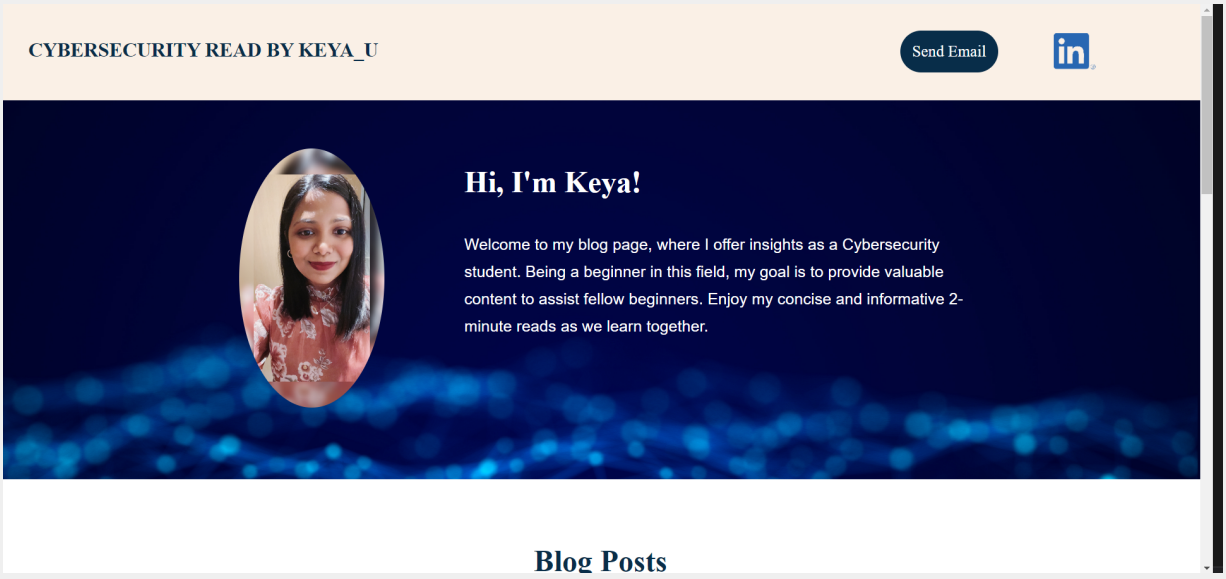
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

```
https://ctrlaltsecure.cloud
```

Paste screenshots of your website created (Be sure to include your blog posts):



Blog Posts

Cloud Computing: From one beginner to another

Cloud Environment

You may have come across the increasing popularity of Cloud Computing and Security, whether through your workplace's recent transition or conversations overheard on public transport. The term computing can seem daunting to comprehend, but allow me to briefly explain its significance and how it revolutionizes business operations. Cloud Computing replaces physical data storage machines with virtual rental alternatives. These virtual storage solutions can be accessed from anywhere in the world through the internet and personal virtual keys. Sounds straightforward, right? Well, that's because it is. Not only does it grant global accessibility, but you can also use multiple devices as long as they support the necessary software. It's a highly flexible system that accommodates changes as you work and prioritizes user-friendliness.There are three main types of Cloud Computing. Firstly, Infrastructure as a Service (IaaS) provides a rental house without any equipment, allowing you to bring and set up your own resources. Basic elements like Virtual Machines and storage are provided to get you started. Secondly, we have Platform as a Service (PaaS), which offers a ready-to-use house where you can access your cloud environment immediately. Finally, Software as a Service (SaaS) eliminates the need for installations or self-maintenance. It resembles accessing an online software application, offering a wide range of applications to choose from directly. Personally, I find SaaS to be my favorite and the most adaptable platform in the realm of cloud computing. With this explanation, both you and I now have a better understanding of Cloud Computing and its various types.

Cloud Security: The Continuum of Cloud Computing

Cloud Envionment Security

As a cybersecurity student, my focus lies in the security aspect of Cloud Computing. Initially, grasping its concept proved challenging, given the notion of data wandering in the cloud and the concerns surrounding its reliability. However, I have found answers to these basic questions, which I hope you will also find here. With a better understanding of Cloud Computing from my previous blog, Cloud Security becomes more comprehensible. It can be likened to fortifying a house with fences, locks, guards, security cameras, and other measures to safeguard our cloud-based Database and overall system. Cloud security encompasses various components, each possessing a unique ability to enhance user safety and reliability. Examples include Data Protection Capabilities, which encrypt both in-transit and at-rest data while offering multi-factor authentication. Access Control Capabilities permit known and configured traffic while imposing necessary restrictions. Moreover, Cloud environments maintain visibility, enabling prompt detection and alerting of vulnerabilities, configuration errors, and security threats. These represent only three of the many components, totaling eight, that form a robust pillar of security for enhanced Cloud Data Security.

Day 1 Questions

General Questions

1. What option did you select for your domain (Azure free domain, GoDaddy domain)?

```
GoDaddy
```

2. What is your domain name?

```
www.ctrlaltsecure.cloud
```

Networking Questions

1. What is the IP address of your webpage?

```
20.211.64.11
```

2. What is the location (city, state, country) of your IP address?

```
Sydney, New South Wales, Australia
```

3. Run a DNS lookup on your website. What does the NS record show?

```
Server:           8.8.8.8
Address:          8.8.8.8#53

Non-authoritative answer:
Name: ctrlaltsecure.cloud
Address: 20.211.64.11
```

Web Development Questions

1. When creating your web app, you selected a runtime stack. What was it? Does it work on the front end or the back end?

```
1 hour runtime stack was selected and it works at the back end.
```

2. Inside the `/var/www/html` directory, there was another directory called assets. Explain what was inside that directory.

```
Asset Directories are made up of files and sub-folders that you can access
through your web browser and the RESTful API. You can view file information,
caching, metadata, and download information by clicking on a file in ProGet
```

```
Web UI.
```

3. Consider your response to the above question. Does this work with the front end or back end?

```
It works in the back end.
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
Tenancy in cloud computing refers to the sharing of computing resources in a private or public environment that is isolated from other users and kept secret.
```

2. Why would an access policy be important on a key vault?

```
A Key Vault access policy determines whether a given security principal, namely a user, application or user group, can perform different operations on Key Vault secrets, keys, and certificates.
```

3. Within the key vault, what are the differences between keys, secrets, and certificates?

```
Certificate assertions are usually short-lived (Eg. 5 to 10 minutes) so if even if intercepted they will provide only limited use. Secrets on the other hand tend to be long-lived. Secrets are symmetric keys so both client and server need to know about it.
```

Cryptography Questions

1. What are the advantages of a self-signed certificate?

```
Self-signed certificates are fast, free, and easy to issue. Self-signed
```

```
certificates are appropriate for development/testing environments and
internal network websites. Self-signed Certificates are simple to modify or
customize; for instance, they can carry more metadata or have greater key
sizes.
```

2. What are the disadvantages of a self-signed certificate?

```
A self-signed SSL certificate does not provide sufficient protection to the
data sent by a browser to the server. Unlike the certificates issued by
reliable certification authorities, the identity of a self-signed SSL is
verified by its owner.
```

3. What is a wildcard certificate?

```
A wildcard certificate is a type of SSL/TLS certificate that can be used to
secure multiple domains (hosts), indicated by a wildcard character (*) in
the domain name field. This can be helpful if you have a lot of domains or
subdomains that you need to secure, as it can save you time and money.Nov
```

4. When binding a certificate to your website, Azure only provides TLS versions 1.0, 1.1, and 1.2. Explain why SSL 3.0 isn't provided.

```
To ensure the safety of the users, Microsoft completely disabled SSL 3.0 in
Azure Websites by default to protect customers from the
vulnerability.Microsoft implemented TLS - 1.1, 1.0 and 1.2.
```

5. After completing the Day 2 activities, view your SSL certificate and answer the following questions:

    a. Is your browser returning an error for your SSL certificate? Why or why not?

```
Yes, the website only supports TLS certificates and not SSL.
```

    b. What is the validity of your certificate (date range)?

```
Issued On   Monday, June 19, 2023 at 8:00:00 PM
Expires On  Wednesday, December 20, 2023 at 6:59:59 PM
```

c. Do you have an intermediate certificate? If so, what is it?

```
Yes, I do have an Intermediate Certificate and it is GeoTrust TLS RSA4096
SHA256 2022 CA1
```

d. Do you have a root certificate? If so, what is it?

```
Yes, I do have a root certificate and it is DigiCert Global Root CA
```

e. Does your browser have the root certificate in its root store?

```
Yes
```

f. List one other root CA in your browser's root store.

```
Microsoft Root Certificate Authority
```

Day 3 Questions

Cloud Security Questions

1. What are the similarities and differences between Azure Web Application Gateway and Azure Front Door?

```
While both Front Door and Application Gateway are layer 7 (HTTP/HTTPS) load
balancers, the primary difference is that Front Door is a nonregional
service whereas Application Gateway is a regional service.
```

2. A feature of the Web Application Gateway and Front Door is "SSL Offloading." What is SSL offloading? What are its benefits?

```
SSL offloading is the process of removing the SSL based encryption from
incoming traffic that a web server receives to relieve it from decryption of
data. Security Socket Layer (SSL) is a protocol that ensures the security of
HTTP traffic and HTTP requests on the internet.
```

3. What OSI layer does a WAF work on?

```
Layer 7 - Application
```

4. Select one of the WAF managed rules (e.g., directory traversal, SQL injection, etc.), and define it.

```
Directory traversal (also known as file path traversal) is a web security
vulnerability that allows an attacker to read arbitrary files on the server
that is running an application. This might include application code and
data, credentials for back-end systems, and sensitive operating system
files.
```

5. Consider the rule that you selected. Could your website (as it is currently designed) be impacted by this vulnerability if Front Door wasn't enabled? Why or why not?

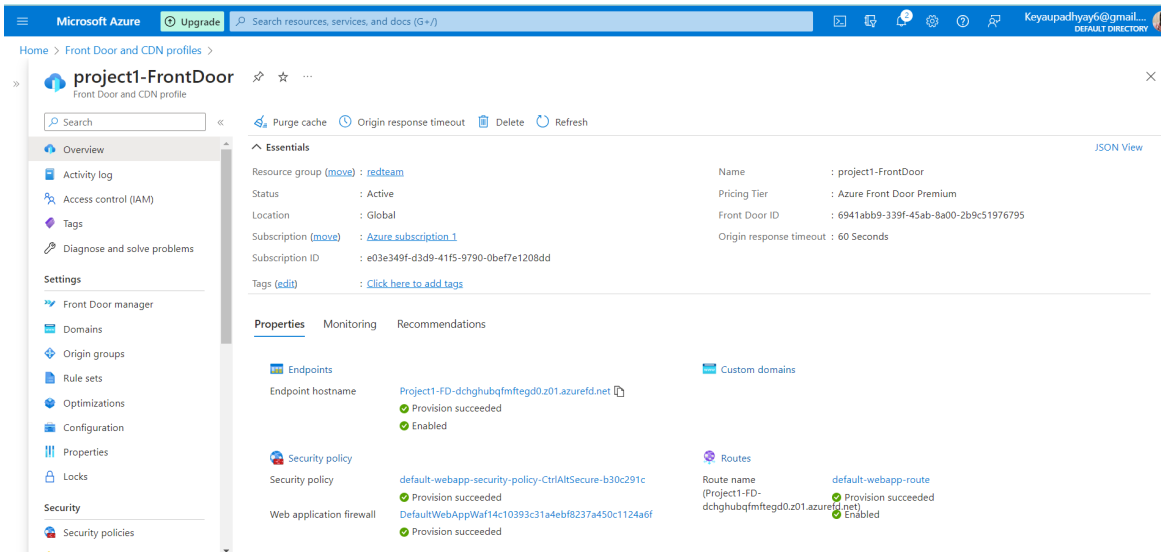
```
Yes, it will be affected as Azure Front Door can prevent attackers from
reaching your application and affecting your application's availability and
performance.
```

6. Hypothetically, say that you create a custom WAF rule to block all traffic from Canada. Does that mean that anyone who resides in Canada would not be able to access your website? Why or why not?

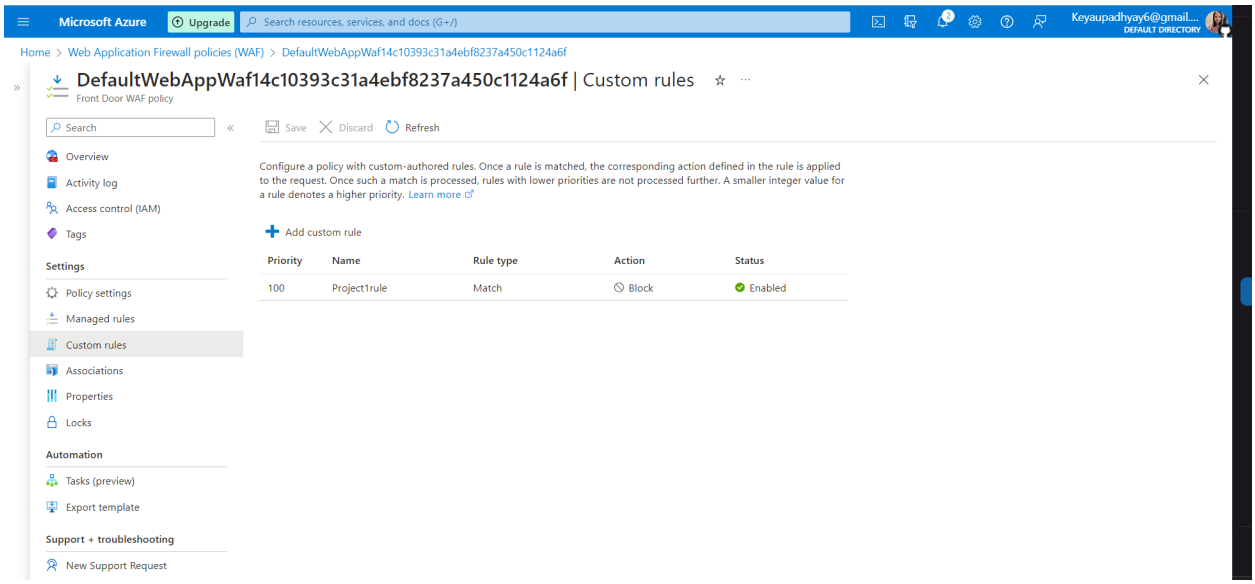
```
Yes, most of the IP addresses from Canada will not be able access the
website but only the authorized users will have access to it.
```

7. Include screenshots below to demonstrate that your web app has the following:

    a. Azure Front Door enabled



b. A WAF custom rule



Disclaimer on Future Charges

Please type "**YES**" after one of the following options:

- ***Maintaining website after project conclusion****: I am aware that I am responsible for any charges that I incur by maintaining my website. I have reviewed the guidance for minimizing costs and monitoring Azure charges.*

YES

- ***Disabling website after project conclusion****: I am aware that I am responsible for deleting all of my project resources as soon as I have gathered all of my web application screen shots and completed this document.*