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://nwresume.azurewebsites.net
```

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

Nick White's Resume | Blog

Send Email

Hi, I'm Nick!

Motivated and detail-oriented Cyber Security professional with a strong passion for protecting digital assets and networks. With a foundational knowledge of industry standard security protocols and techniques, I am eager to leverage my technical and problem-solving skills to help organisations secure their systems. A quick learner who thrives in fast-paced environments.

Blog Posts

Confidential Computing

cloud, cryptography, IBM, azure

Cloud computing has revolutionised the way in which organisations can scale computation by their needs. A major drawback however is storing data away from your premises.
So much trust is required from one organisation to another to allow customers private data to be stored and used off site. One advancement in cryptography could bring us one step closer to making this transaction safer for everybody.
Back in 2018 IBM brought us Confidential Computing, allowing all the computation of data to be made in the cloud without the off site computer ever knowing what data was being processed.
Typically for the computation to occur, the data needs to be unencrypted first into RAM. This can give malicious actors with root access opportunity to grab this data. IBMs solution uses an enclave within its cpu to do this work using an authorization key only authorised software knows.
Other companies such as microsoft have incorporated Confidential Computing into their azure service.
This has also been met with some criticism. Is it ethical for example to utilize Confidential Computing when the owner of the data also cannot access it?
https://newsroom.ibm.com/IBM-Explores-the-Future-of-Cryptography
https://www.ibm.com/topics/confidential-computing

Importance of Security Awareness Training

Training, Education, Phishing, Cybersecurity

With phishing attacks on the rise, security awareness training has never been more important. According to the 2022 IBM Cost of Breach Report, Phishing was the second most common cause of breaches at 16%, costing $4.91m. There are many ways to mitigate risks in preparation for a device becoming compromised within an organisation. Setting up traffic rule alerts, removing admin rights on employee devices, maintaining patched servers and firewalls. However, avoiding users becoming victims in the first place via education is the best strategy. Doing periodic online training modules covering types of phishing attacks is a good way to start. Users need to be aware not just for the organisation and its data, also for their personal data. We are bombarded with suspicious text messages and emails, trying to trick us into clicking on a link to grab our information. Other topics to cover should include:
- Locking screens when a device is unattended.
- Do not leave phones or laptops unattended in public spaces such as cafes or cars.
- Dangers of public wifi.

Simply being aware of the types of ways malicious actors try and steal information means everyone is safer.

Day 1 Questions

General Questions

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

```
Azure Free Domain
```

2. What is your domain name?

```
nwresume.azurewebsites.net
```

Networking Questions

1. What is the IP address of your webpage?

```
20.37.196.202
```

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

```
Sydney, NSW, Australia
```

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

```
nick-mac:~ nick$ nslookup -type=ns nwresume.azurewebsites.net
Server:         192.168.0.1
Address: 192.168.0.1#53

Non-authoritative answer:
nwresume.azurewebsites.net       canonical name = waws-prod-sy3-069.sip.azurewebsites.windows.net.
waws-prod-sy3-069.sip.azurewebsites.windows.net    canonical name =
waws-prod-sy3-069-fba5.australiaeast.cloudapp.azure.com.

Authoritative answers can be found from:
australiaeast.cloudapp.azure.com
        origin = ns1-06.azure-dns.com
        mail addr = msnhst.microsoft.com
        serial = 10001
        refresh = 900
        retry = 300
        expire = 604800
        minimum = 60
```

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?

```
The runtime stack php 8.0 is back end. It is a general purpose scripting
language creating a foundation for this websites development.
```

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

```
This folder contains the css files and images required for the website.
CSS files are style formatting files.
```

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

```
This will interact with the front end - the users experience.
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
A cloud tenant is not unlike a renter in an apartment building. A tenant
hires a space, sharing a building with other tenants. However, their
apartment is not shared with other customers.
The apartment in the cloud tenant scenario is the resources such as virtual
services, storage and applications that are isolated from other customers.
However, like an apartment building, physically it might be shared with
other customers.
Logically however the resources can be scaled up and down as needed.
```

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

```
To continue the analogy, to enter an apartment you might have a swipe card
to access the building and your apartment.
The access policy is the credentials, authorizations such as username and
passwords, certifications and multi factor authentication to allow a cloud
tenant to access their resources.
This can extend to rules to accessing resources such as IP and ranges and
time restrictions.
```

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

```
Within the key vault
A key is what is required for secure connection between the tenant and
resources. For example an asymmetric key which has a private and public key.
The public is given to the service from the tenant. The private key is held
onto.
A secret is an encrypted storage method within the vault that can hold data
such as passwords and strings.
A certificate is used to authenticate the identity of a website and it is
used as part of the process in establishing a secure encrypted connection
between the website and the user. The certificate uses the secrets and keys
as part of the process.
```

Cryptography Questions

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

```
The advantage of a self-signed certificate is complete control. If the webs
server was being built for an internal purpose such as a database or
intranet, self-signed would make sense.
```

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

```
However, if you are a user, surfing the internet and you come across a
self-signed certificate. You might have reason to be wary, as there has been
no third party to back up the authenticity of the certificate. Potentially
the website could be used for malicious activity.
```

3. What is a wildcard certificate?

```
A wildcard certificate simply is a certificate that covers a whole domain. For example for google.com a wildcard cert would also cover example.google.com or test.google.com
```

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.

```
SSL 3.0 has a design flaw. It can be exploited by a vulnerability where the secure protocol version can be downgraded. At this point an attack called a POODLE attack can take place where a man in the middle can intercept data and even modify the data in the transmission.
```

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?

```
It is not returning an error because it is being signed by Microsoft Azure and DigiCert.
```

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

```
28.12.22 to 23.12.23
```

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

```
Microsoft Azure TLS Issuing CA 05 appears to be the intermediate certificate
```

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

```
DigiCert Global Root G2 is the root certificate
```

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

```
Possibly because im on a mac, the browser doesnt store the root certificate however my apple keychain did. So I found the DigitCert Global Root G2 in my
```

```
system root keychain.
```

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

```
Another root cert includes Amazon Root CA 1, SecureTrust CA. Just to name a
couple of many.
```

Day 3 Questions

Cloud Security Questions

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

```
The main difference is that Azure Web Application is regional where as Front
Door is non-regional.
Another difference is that the Application Gateway allows load balancing
between VMs and containers whereas Front Door can load balance between
different scale units/clusters and stamps across regions.
The Azure Web Application Gateway is also purpose built for web applications
whereas Azure Front Door is suitable for many resources.

They are similar in that they reside in front of the web application to
protect it.
They both work in the OSI Layer 7.
They are both load balancers.
They both have features such as URL path-based routing and SSL/TLS
termination.
```

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

```
The SSL Offloading in the load balancing process of either of these methods
decrypts network traffic and then forwards the unencrypted data to the
intended destination.
This takes some of the process work off of the destination's servers.
Creating less load on the servers themselves.
```

```
Using this method can also allow the Load balancer to inspect the traffic
before reaching the servers, potentially  avoiding threats.
```

3. What OSI layer does a WAF work on?

```
Layer 7 - Application Layer
```

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

```
There is an SQL Injection Attack: Common Injection Testing Detected Rule
that is set to block or Anomaly.
This rule is enabled.
If an SQL Injection attack occurs the WAF should detect it and block it from
happening, provided it’s common enough to detect.
An SQL Injection can occur if an open field on the website that can query a
database is used. If the attacker uses a php command in a vulnerable field,
it can hijack something simple like a log in query to act maliciously.
```

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?

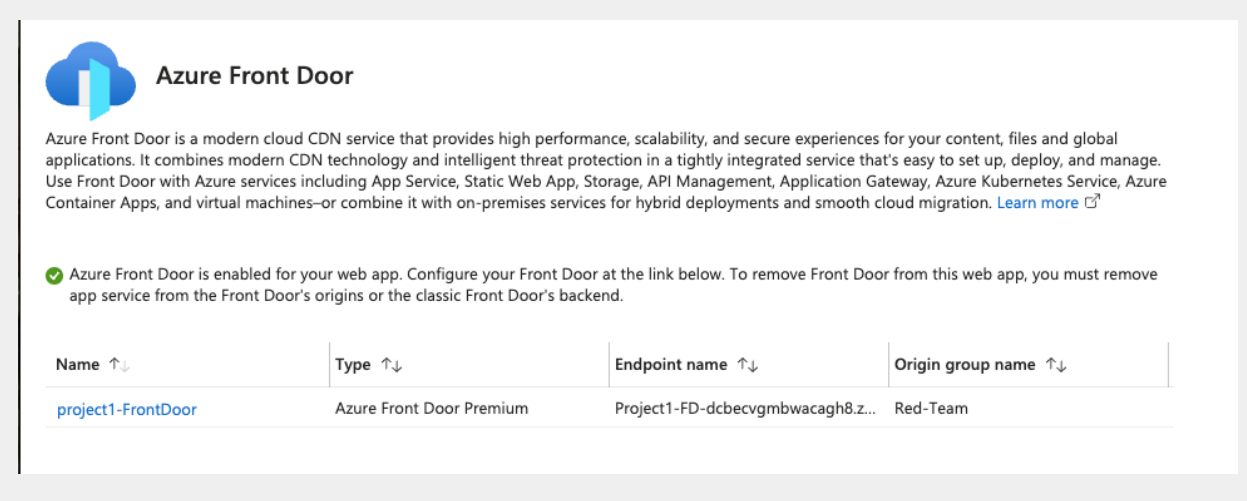
```
I don’t believe there is anywhere on the website to open a command to a
database. There isn’t an area for the malicious actor to query a database.
So even with this rule off, I think it should be safe.
```

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?

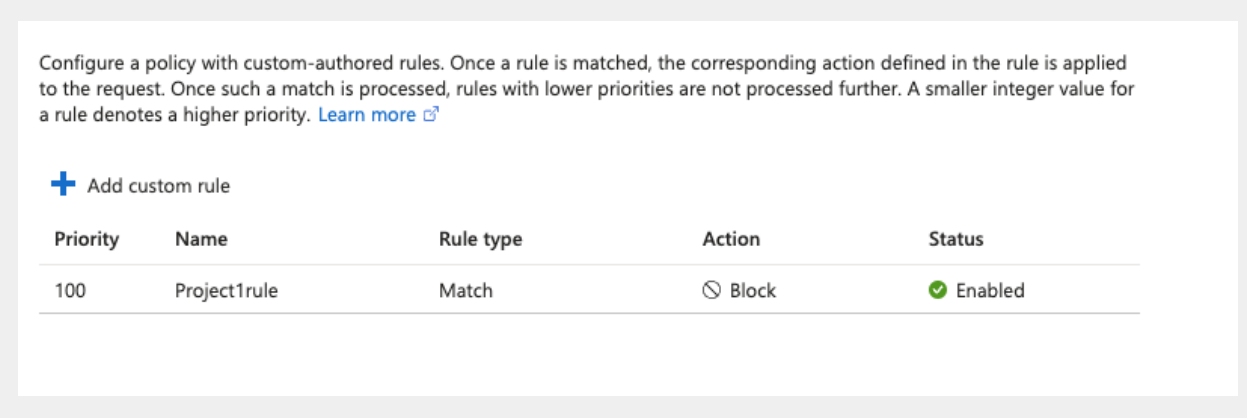
```
Without any work, someone from Canada would not be able to access the
website. However there are other means such as utilizing a VPN to “trick”
the website into thinking you are coming from an approved country.
```

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.*

- ***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.*

YES