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://zantan.azurewebsites.net/
```

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?

```
zantan.azurewebsites.net
```

Networking Questions

1. What is the IP address of your webpage?

```
      20.48.202.168
```

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

Toronto, Ontario, Canada

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

```
20.48.202.168For CNAME
waws-prod-yt1-057-4c85.canadacentral.cloudapp.azure.com.
← waws-prod-yt1-057.sip.azurewebsites.windows.net.
```

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?

```
PHP 8.2.It is a language that works on the back end.
```

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

```
The assets directory contained style sheets, images, and any other support
files needed for the website.
```

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

```
This works with the front end.
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
Companies or individuals who sign up to use your environment are considered tenants.
```

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

```
A key vault is important because it limits users, groups or applications on performing different types of operations to Key Vault secrets, keys, and certificates.
```

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

```
A key is a Cryptographic operation hardware and software. A secret is anything you want to control very vigantly such as API keys, passwords, or certificates. A certificate identifies and provides imperative information about the holder of the certificate.
```

Cryptography Questions

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

```
Self-signed certificates are free, quick and not complex to issue. They are good when building websites, testing the sites and their environments. They are also very easy to manage with internal network websites.
```

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

```
The self-signed certificate doesn't have any trust value nor does it establish identity assurance. The certificate can not be revoked.
```

3. What is a wildcard certificate?

```
A wildcard SSL certificate is a single SSL/TLS certificate that can provide significant time and cost savings, particularly for small businesses. The certificate includes a wildcard character (*) in the domain name field, and can secure multiple subdomains of the primary domain.
```

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 isn't provided due to the vulnerability of the certificate.
```

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?

```
Browser does not return an error due to the fact that the certificate is
verifiable and is installed properly on the host server.
```

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

```
Issued On   Tuesday, December 27, 2022 at 4:12:39 PM
Expires On  Friday, December 22, 2023 at 4:12:39 PM
```

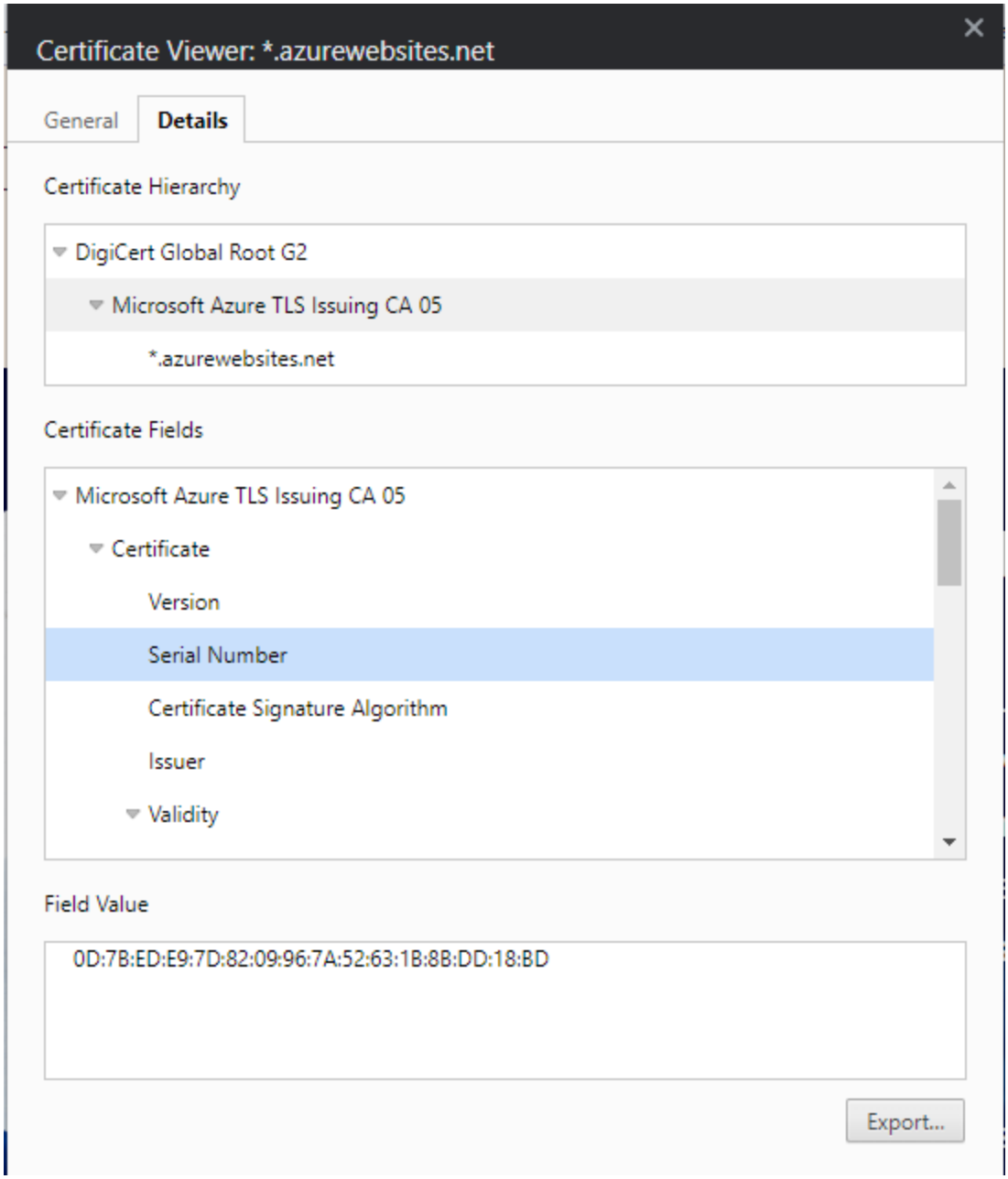
    c. Do you have an intermediate certificate? If so, what is it?

```
The certificate is a TLS. The name is Microsoft Azure TLS Issuing CA 05
```

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

```
The root certificate is a SSL. The name is DigiCert Global Root G2.
```

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



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

```
Another root CA in my browser's root store is GlobalSign.
```

Day 3 Questions

Cloud Security Questions

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

```
Front door is non-regional and the Gateway is regional.
```

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 relieving the web server from the duty of
removing SSL encryption from incoming traffic. This allows the web server
more resources to do other processes.
```

3. What OSI layer does a WAF work on?

```
WAF works on layer 7.
```

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

```
An SQL injection rule statement looks for malicious sql requests that
attackers use to take advantage of your website for a variety of reasons
such as gaining access to your database.
```

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?

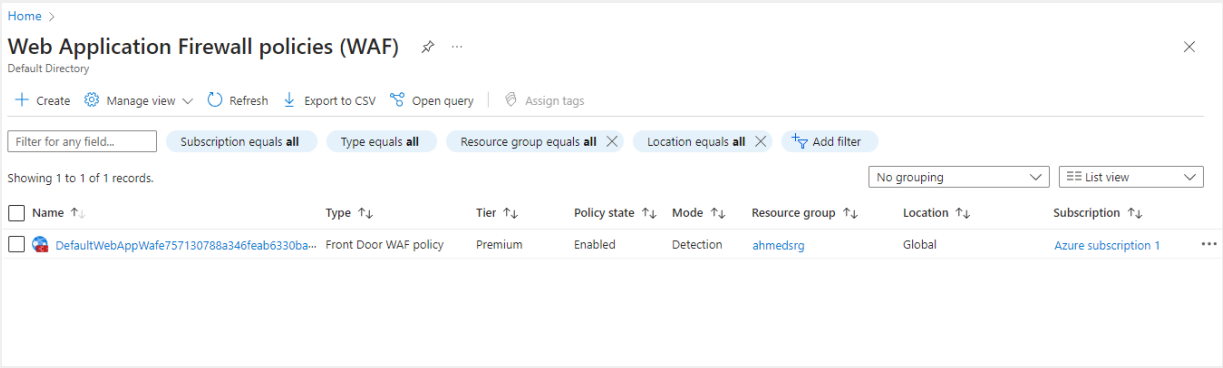
```
Yes, the website would/could be impacted by this vulnerability due to having
Front Door disabled, makes a website vulnerable to attacks such as SQL
injection.
```

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?

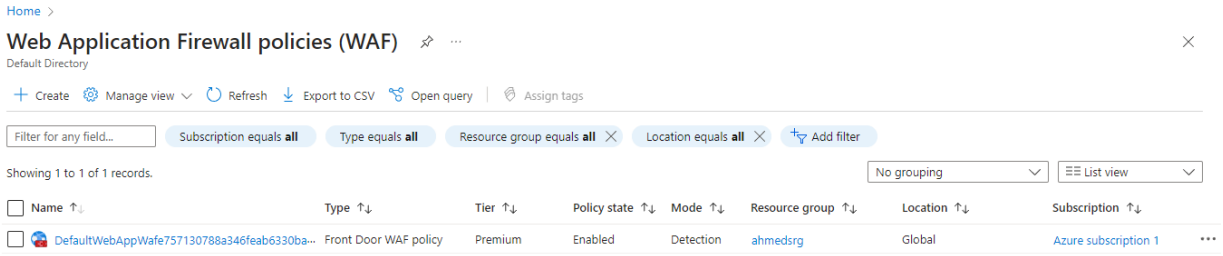
No, using a WAF rule to block all Canadian traffic would not completely block people in Canada from accessing the website. While the WAF rule would block IP addresses originating from Canada, it is not actually possible to know whether the user accessing the website is actually located in Canada. An example of this would be, if someone tried accessing the website from a Canadian IP address in a different country, they would be blocked even though they are not technically in Canada. Users in Canada could also use a VPN to mask their IP address which bypasses the WAF rule allowing them access to the website.

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.*

Ahmed Luhar's CYBER BLOG

Send Email

Hi, I'm Ahmed!

I've always had a fascination with the information technology industry in all the various roles that I have taken over my 40 years of working. I started off in the construction industry as a Brick Mason and worked my way up to Site Manager, then I went on to go to the Printing industry where I experienced some success as well starting as a Sales Representative to my final destination as a C-Suite Executive. Now I am finally back to my original passion and interest in an industry related to Information technology called "Cyber Security." As a result I finally decided to become a part of the Cybersecurity community.

Blog Posts

Cartoons=Malware?

Malware, Botnet, Hinatabot, Cartoon

The trend of hackers using movie references now seems to have shifted to cartoons. A new malware has been named Hinatabot by Akamai institute due to the author naming the script Hinata after the namesake character in an animated TV show called "Naruto." Hinatabot has been shown to be able to take advantage of some vulnerabilities in the Go programming language.

The Next Big Ransomware Family: Clop

Ransomware, Clop, Trendsetter, E-Commerce

One of the more interesting effects of COVID on the world is the sharp increase in cybercrime, especially the use of malicious scripts such as ransomware. One of the most dangerous of these ransomware families is called Clop. Clop has a prolific history of being able to take advantage of unknown zero-day vulnerabilities, the most recent of which was found in a file transfer service by Fortra. Clop is also known to infect a victim's entire network rather than a single computer.

Ahmed Luhar's CYBER BLOG

Send Email

Cartoons=Malware?

Kids have been hooked on many different animated shows over the years from Super Friends (1973) to the more recent anime series within the past few years.

A particular anime series has been of particular note in recent years. The series in question is called "Naruto" and the series itself does not have anything to do with malware or cyber security. It has now been connected to one of the most recent botnets called by the Akamai institute the "Hinatabot" through the name of Hinata who is a character in the series.

Quite the opposite in fact the cartoon series, "Naruto," is a show about cartoon ninjas with seemingly magical powers that allow them to manipulate the elements. The environment also does not seem to have any sort of computer system, moreover, it is hinted that the only technology used in the original series is similar to modern walkie-talkies. The series highlights the lack of technological improvement by implying that the industrial revolution has not happened yet for the inhabitants of the world through the lack of trains and the need for each character to travel long distances on foot jumping through impossibly large trees. However, we all know that the source material doesn't matter for the creative to apply it elsewhere.

The Botnet is based on the programming language of Go, which is a language that was made to possess the "good" traits of several other languages like python and C++. The language itself was developed by Google employees. Some of the focuses of the language include: increasing developer productivity and somehow making better use of networking applications of code. The language also has the advantage of having an adorable mascot, an anthropomorphic gopher. The language is also open-source which has led to other threat actors making other malicious scripts to attack any company that uses this language. The language is used by any corporation that uses google products for any facet of their business.

The Hinatabot has great capabilities in Distributed Denial of Service Attacks (or DDoS) and is capable of taking advantage of specific weaknesses of the Go language. The flaws that were exploited by the malware at the akamai servers were found to be the CVE-2014-8565 flaw and the CVE-2017-17215 flaw. These flaws were also used by the Mirai malware which the experts at Akamai say that the Hinatabot is a descendant of. One mode of attack for the malware is SSH ports through HTTP and UDP protocols, in true DDoS style, however, it can also infect systems through other means such as using infection scripts. The Hinatabot then quietly runs and awaits commands from the threat actor on the command and control server. Amusingly, the author of Hinatabot has reflected the storyline of the character of Hinata in the commands used to interact with the malware. Akamai also warns that the script is still under development and it has greater potential to do more harm.

In conclusion, anyone using the Go language for any aspect of their work should be very watchful of the progress made by the author of the Hinatabot as the future is uncertain. The malware may follow the path of its namesake character who went from an underdog to a professional.

Ahmed Luhar's CYBER BLOG

Send Email

The Next Big Ransomware Family: Clop

The world is becoming a very interesting place with the advent of COVID accelerating many old trends and creating some new ones along the way. The mass adoption of online services in favor of the more brick-and-mortar alternatives is one of the old trends that COVID accelerated a little ahead of schedule according to many experts. The seemingly new and more sizeable audience that did not fully know how to guard themselves online has attracted a generation of new cybercriminals.

One of the most common forms of cyber crimes that modern cybercriminals perpetrate more after COVID would be the perpetrating use of ransomware. One of the most prolific ransomware families that have emerged from this new trend of ransomware is Clop.

Clop has reportedly afflicted over 130 victims in the past 2 months. The developers behind Clop have claimed to take advantage of a previously unknown zero-day exploit in a popular file transfer service. The File Transfer service in question is called GoAnywhere made by Fortra. The attack was not as widespread as the other attacks that happened in the past year as the file transfer service was not a common tool to all businesses. However, many high-ticket companies were affected such as Procter & Gamble and Virgin Group. Some governmental institutions were affected by the attack such as the U.K. Pension Protection fund. Even Rubrik, a secure data recovery service, was affected by the ransomware attack.

However, this is not the first time that Clop has successfully carried out ransomware attacks against high-profile targets. Clop was used to attack several firms in the United States and South Korea resulting in payouts exceeding USD 500 million in 2021. Among the most notable victims of the attack is the large South Korean e-commerce firm, E-Land. South Korea was one of the most attacked countries by Clop ransomware attacks during the period between 2018 to 2020. Interestingly the attacks then were based out of Ukraine, and the US and the South Korean governments worked together to catch the perpetrators.

Clop itself is a ransomware that first evolved from another ransomware family called CrytoMix. and the first group that was discovered to use Clop was called TA505 during a large-scale spear-fishing email campaign. Clop is usually credited to be an example of RaaS or ransomware as a service that is usually considered to have a Russian origin. The ransomware is also historically known to use a verified and digitally signed binary that made it look like a legitimate executable file. Another interesting fact about this ransomware is that it targets a victim's whole network rather than specific computers on the network. Clop has been so successful and prolific in the many attacks that it was utilized for that it is now considered a trendsetter among modern ransomware.

In conclusion, the ransomware Clop seems to be in a long line of ransomware that is used to take advantage of the cybersecurity weaknesses of large organizations, particularly through the mode of phishing emails. Since this ransomware is considered a trendsetter many cybersecurity officers may want to consider looking for malicious scripts on the other computers in the network besides the infected system.