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://skor.azurewebsites.net
```

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

Emerging Threats in Healthcare

Ransomware

As time and cybersecurity evolve, so do the cyber threats at large. CLOP, an alias within the TA505 umbrella, and a new cybercriminal crew named Venus have shifted their focus to targeting executives in healthcare organizations. Venus's first known attack occurred mid-August of this year and quickly made a name for themselves by targeting victims of Remote Desktop Services, then deploying malware to encrypt data on Windows devices. Because this group has been unsuccessful at getting paid out for their ransom attacks they have changed their strategy to framing executives for inside trading by modifying their emails to appear like they are planning to move large volumes of shares. This is no easy task but, the founder of Hold Security says it can be done using Microsoft Outlook .pst files. "It's not going to be forensically solid, but that's not what they care about," Alex Holden said. "It still has the potential to be a huge scandal, at least for a while, when a victim is being threatened with the publication or release of these records." Tripwire Security Firm has advised that several cybercriminal groups are redistributing the ransomware software and to avoid becoming a victim of an attack, practice but do not limit yourself to the following tips: 1. Secure off site backups 2. Running up-to-date security solutions and ensuring that your computers are protected with the latest security patches against vulnerabilities. 3. Using hard-to-crack unique passwords to protect sensitive data and accounts, as well as enabling multi-factor authentication. 4. Encrypting sensitive data wherever possible. 5. Continuously educating and informing staff about the risks and methods used by cybercriminals to launch attacks and steal data. Although these are all great tips for organizations to follow for the prevention of future attacks, another critical point that should be followed is the development and practice of an incident response plan. Practicing real-world attacks will allow your organization to expose and refine weaknesses that an attacker could exploit.

Benefits of Security+ Certification

COMPTia Security+ Certification

Cybersecurity challenges have become a point of focus in organizational development. It is critical to stay up to date with best practices to prevent and protect your organization's programs, networks, and systems from cyber-attacks. With the consistent growth within the industry, the need for professionals in cybersecurity is at an all-time high. The CompTIA Security+ certification is well-respected and internationally accepted in the field of IT. The Security + certification is also a great starting point for security professionals just breaking into the industry. Below I have listed the benefits of the Security+ certification for your consideration. 1. No Experience Needed The CompTIA Security+ certification has no prerequisite education or experience required for beginners looking to start their careers in cybersecurity. 2. Globally Accepted The CompTIA Security+ certification is a globally recognized standard for cybersecurity professionals. Holding the Security+ certification demonstrates a strong foundation in cybersecurity knowledge and skills. 3. Vendor-Neutral It's vendor-neutral, meaning it is not tied to any specific product or service, making it more widely applicable and relevant to a variety of roles and industries. 4. Career Opportunity Holding the CompTIA Security+ certification can open a wide range of career opportunities in the field of cybersecurity. Some potential job titles for professionals with the certification include security analyst, network administrator, and pen tester. 5. Higher Pay Scale Obtaining the Security+ certification can lead to career advancement and higher salaries, as it is often required for job positions and can demonstrate a level of expertise to potential employers. Overall, the CompTIA Security+ certification is a valuable asset for professionals looking to advance their careers in cybersecurity and ensure they have the skills and knowledge to succeed in the field.

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?

```
skor.azurewebsites.net
```

Networking Questions

1. What is the IP address of your webpage?

```
20.211.64.15
```

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?

```
[swish@Jump-Box-Provisoner:~$ nslookup -type=ns skor.azurewebsites.net
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
skor.azurewebsites.net  canonical name = waws-prod-sy3-097.sip.azurewebsites.win
dows.net.
waws-prod-sy3-097.sip.azurewebsites.windows.net canonical name = waws-prod-sy3-0
97-ef32.australiaeast.cloudapp.azure.com.
```

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?

```
I selected PHP 8.1 and it works on the back end to develop dynamic and
interactive web applications.
```

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

```
The assets directory contains a directory named css. Within that directory
there is a file named style.css and its backup style.css.bak. This file
contains the properties on how to layout, display, and style your webpage.
```

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

```
CSS works with the front-end development.
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
A cloud tenant refers to sharing private or public computing resources, in
an inclusive environment, that is protected with confidentiality from other
users.
```

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

```
An access policy is important to determine what permissions are given to
users, applications, or user groups to perform different tasks Key Vault
secrets, keys and certificates/.
```

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

```
The difference is that a private key is imported or generated by a service request by the Key Vault and is stored as an Azure Key. Azure Secrets refer to the account keys or passwords for the private key file. A certificate is simply a managed X.509 certificate that offers life cycle management capabilities.
```

Cryptography Questions

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

```
The advantages of self-signed certificates are that they're free and easy to issue. Also appropriate for internal network websites and for testing, because they’ve no dependencies on others for the issuance of certificates. Lastly, they can be easily modified or customized.
```

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

```
Disadvantages are that they will appear to be untrustworthy to visitors, browsers and operating systems. Self-signed certificates are very risky for financial transactions and more vulnerable to cyberattacks.
```

3. What is a wildcard certificate?

```
This certificate uses the same private key to secure multiple host names related to the primary domain name.
```

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 is deprecated because it is vulnerable to a man-in-the-middle attack. Weakness in its encryption algorithm causes this.
```

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 the SSL certificate is valid
```

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

```
March 14, 2022 - March 9, 2023
```

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

```
Microsoft Azure TLS Issuing CA 01
```

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

```
DigiCert Global Root G2
```

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.

```
AAA Certificate Services
```

Day 3 Questions

Cloud Security Questions

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

```
The similarities between Azure Web Application Gateway and Azure Front Door
are that they both are layer 7 load balancers. The difference is that AFD is
a non-regional service whereas AWA 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 uses devices alternative to the web server, for decryption
and encryption. The benefits of this process allow web servers' performance
to not be affected.
```

3. What OSI layer does a WAF work on?

```
Application Layer 7
```

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

```
SQL injections are a web hacking technique that allows an attacker to insert
malicious code in SQL statements to manipulate the queries within an
application.
```

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?

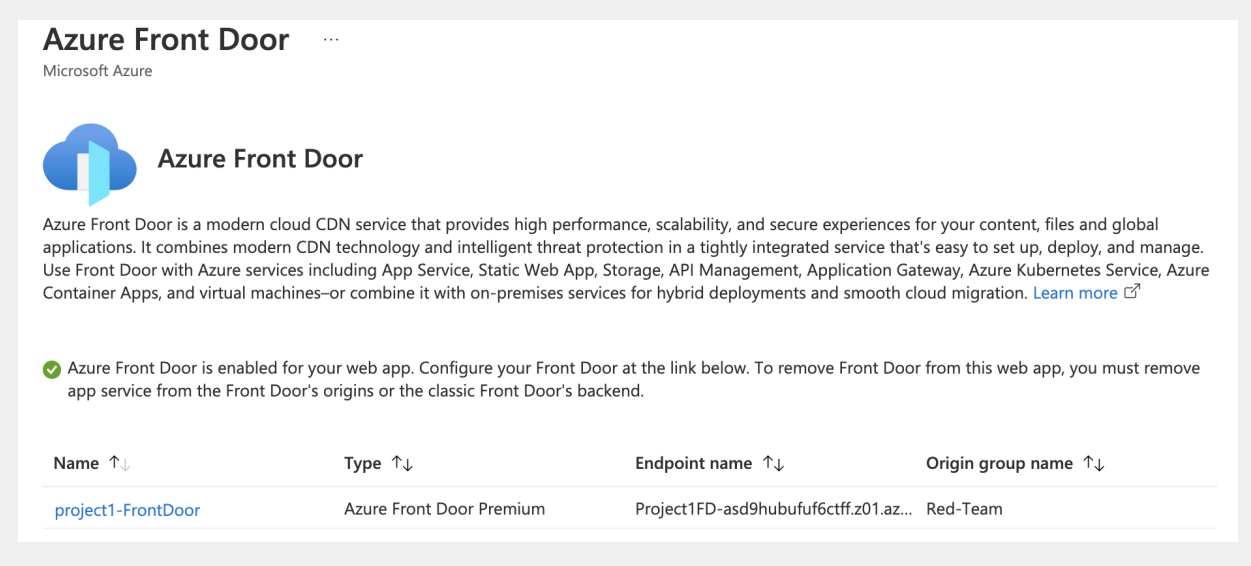
```
Yes, it could be impacted by this vulnerability. AFD is designed to function
as an extra layer of protection at my network's edge. This helps protect my
local network from becoming exposed if my website was compromised by a
threat such as SQL injections.
```

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?

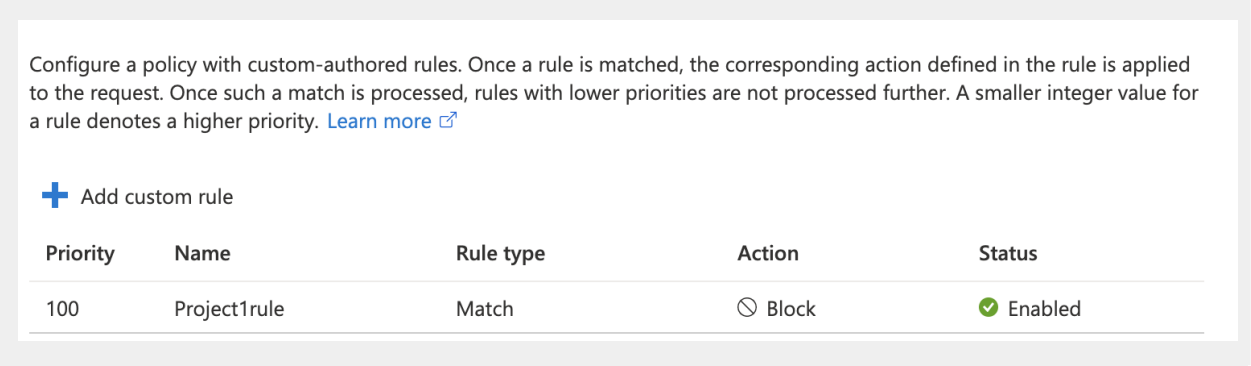
```
This is correct. Anyone with an IP address located in Canada would be
blocked from accessing my website.
```

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.*

- ***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.*