



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://kileysecurityblog.azurewebsites.net/`

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

KILEY'S CYBER SECURITY BLOG

Send Email




Hi, I'm Kiley!

Military "brat" who has traveled the world. 10 years employed with Target, currently an Asset Protection Team Lead, Bachelors degree Pyschology Arizona State University -2017, Current student at the University of Minnesota Cyber Boot Camps-2023, Hobbies include writing, recording music.



Blog Posts

← → ↻ kileysecurityblog.azurewebsites.net



The Psychology of hackers. Are there really personality traits connected to the different types of hackers?

Hackers

After reading through several researches done around this topic, the answer is yes there are claims that may validate the belief that there are certain personality traits that hackers share. Hackers are typically divided within the categories of White hat, gray hat, and black hat. White hats typically are considered "the good guys", those who are trying to help and are pretty much considered ethical hackers. Gray hats typically are considered to be the "Hacktivist" and are considered to be in between. Gray hats are not always ethical but can be out to prove they are right, by hacking into an organization without their permission, and then offering to fix threats possibly charging some kind of fee. Gray hats typically don't have the malicious intent like black hats. Black hats may hack for personal monetary gain, revenge, thrill seeking. Black hats have malicious intent and tend to put malware out that can hold a computer hostage, destroy files, steal all personal info ect. After reading through a research performed out the University of Buffalo, it was interesting to read about the personality traits of hackers. About 439 students were given a survey, from there the categories were formed with the personality traits using their answered questions around their perception of breaking the law and consequences. It was surprising to learn the White hatters even though considered the good guys, they tend to be narcissist. Research showed that Gray hatters oppose authority. Black hatters are legit thrill seekers. Im not sure how accurate this is , but I do pose what would that do in the hiring process. Would organizations use a personality traits test om their employees to determin if they could be a security threat or not?

81°F Mostly clear Search 10:57 PM 6/16/2023



Is Human error the cause of most cyber security breaches?

Security Awareness

Yes, Human error is the cause of most of cybersecurity breaches. According to a report done by IBM, findings concluded that about 95% of cybersecurity breaches are caused by human error. There are different types of human error; Decision based and skilled based. Some examples of these error include sending emails to the wrong recipient. Password problems, are workers using strong passwords, and not reusing old ones? Then there are the physical breaches like "tailgating" which results in authorized access to premises. There are factors that can play into this, mainly a lack of awareness, for some it may be the motive of opportunity. In order to avoid all these factors organizations should have security awareness training in place, making sure employees understand policies, threats that exist and how to avoid making any of these mistakes. Human error resulting in cyber breaches can cost a company loss of trust from the public, financial loss, availability of it services ect.

82°F Mostly clear Search 10:39 PM 6/16/2023

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?

kileysecurityblog.azurewebsites.net

Networking Questions

1. What is the IP address of your webpage?

20.211.64.16

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?

```
MINGW64/c/Users/17065 x + v - □ x
17065@KY MINGW64 ~
$ nslookup -type=ns kileysecurityblog.azurewebsites.net
Server:   cdns01.comcast.net
Address:  2001:558:feed::1

Non-authoritative answer:
kileysecurityblog.azurewebsites.net    canonical name = waws-prod-sy3-101.sip.azurewebsites.windows.net
waws-prod-sy3-101.sip.azurewebsites.windows.net canonical name = waws-prod-sy3-101-06a2.australiaeast.cloudapp.azure.com

australiaeast.cloudapp.azure.com
primary name server = ns1-06.azure-dns.com
responsible mail addr = msnhst.microsoft.com
serial = 10001
refresh = 900 (15 mins)
retry = 300 (5 mins)
expire = 604800 (7 days)
default TTL = 60 (1 min)

17065@KY MINGW64 ~
$ |
```

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 8.0, It works on the backend

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

Inside the assets directory, there are css files, and images files. Css files are the style formats such as background colors, fonts, ect. In images are the jpeg photos I used and images I uploaded in the blog sections, email logo, linkedin logo ect.

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

Front end

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

A cloud tenant can be an organization or individual that uses the cloud resources, manages the resources within a cloud computing environment. Each would operate in their own environment with their own resources allocated, separate from those of the other tenants. This is also referred to as cloud tenancy.

“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”

Gupta, D. (2021, February 26). *Understanding the Difference Between Single-Tenant and Multi-Tenant Cloud [Infographic]*. Loginradius. Retrieved June 18, 2023, from <https://www.loginradius.com/blog/identity/single-tenant-vs-multi-tenant/#::~text=Tenancy%20in%20cloud%20computing%20refers,other%20users%20and%20kept%20secret.>

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

Access policies determine the permission user accounts, groups or applications have to KEY Vaults items”.

(n.d.). *Limit access to Key Vault data*. Azuregithub.io. Retrieved June 18, 2023, from <https://azure.github.io/PSRule.Rules.Azure/en/rules/Azure.KeyVault.AccessPolicy/>

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

Keys are used to encrypt and decrypt data.

Secrets are very sensitive pieces of information/data that has to be stored securely.

Certificates are used for authentication, encryption, and secure communication and contain the information about the organization, device, person ect.

baldwin, msm, richins, J., lichwa, J., kaistrubel, sebansal, & Bapat, A. (2023, April 21). *Azure key vault keys, secrets, and certificates overview*. Azure Key Vault Keys, Secrets, and Certificates Overview | Microsoft Learn.
<https://learn.microsoft.com/en-us/azure/key-vault/general/about-keys-secrets-certificates>

Cryptography Questions

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

The advantage of a self-signed certificate is “they are free, they are suitable for internal sites or testing environments.

They encrypt the incoming and outgoing data with the same ciphers as any other paid ssl certificate”.

<https://sectigostore.com/page/what-is-a-self-signed-certificate/>. What Is a Self Signed Certificate? Know the Advantages and Disadvantages. (2018).

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

The disadvantages of a self-signed certificate is “no browsers and operating systems trust self-signed certificates. The browsers will not show visual indicators of trust like a padlock symbol and HTTPS in front of the domain name. You website visitors have to proceed through a security warning page with error messages to access your website. Warning pages drastically affect the traffic to your website”.

<https://sectigostore.com/page/what-is-a-self-signed-certificate/>. What Is a Self Signed Certificate? Know the Advantages and Disadvantages. (2018).

3. What is a wildcard certificate?

A wildcard certificate “this type of digital certificate offers full encryption for all subdomains and servers under a single domain, making it an affordable and effective solution for most websites”.

https://sectigo.com/ssl-certificates-tls/wildcard?utm_term=ssl%20wildcard%20certificate&utm_campaign=Sectigo%20Retail_SSL_US&utm_source=adwords&utm_medium=ppc&hsa_acc=9165095309&hsa_cam=2046696154&hsa_grp=74035559244&hsa_ad=581419584209&hsa_src=g&hsa_tgt=kwd-92624550&hsa_kw=ssl%20wildcard%20certificate&hsa_mt=e&hsa_net=adwords&hsa_ver=3&gclid=CjwKCAjw-b-kBhB-EiwA4fvKrGy_iRANKFb9bu8B5VxsVK7dC4rwaX8SbT7J08pH9acWeJOcF-VUMxoCrCMQAvD_BwE. SECURE PRIMARY DOMAIN AND UNLIMITED SUBDOMAINS Wildcard SSL Certificates. (2018).

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 and is disabled to ensure user safety and protect customers from vulnerability.

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?

No , Azure had a secure ssl certificate set up already.

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

Thursday March 9th, 2023 to Sunday March 3rd, 2024

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

no

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

Yes, 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?

Similarities:

- both reside on the application layer 7 of the OSI Model
- both reside in the front of you web app in order to protect

- both Primary solution is a load balancer
- the both can incorporate a web application firewall to protect against web vulnerability attacks.
- both have features such as URL path-based routing and SS/TLS termination.

Differences:

- ”The web application Gateway is more regional and is best suited to protect a web application in a single region in your cloud”.
- ” The Azure Front Door is more global and is better suited when you have a variety of regions in a cloud environment”.

14.3 Protecting your App using Azure’s Cloud security features_ed. (n.d.).

Google Docs.

https://docs.google.com/presentation/d/16oMZPbxJiPygsFXrAqiOeCBN3QohfwsJHKT2n1vnD3I/edit#slide=id.gef6b523603_0_981

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

“SSL offloading relieves the burden of encryption and decryption from the server’s metaphoric shoulders”.

-Its benefits include faster loading of the website, reduced latency, traffic control

Mehta, M. (2020a, March 12). *What Is SSL Offloading? Features & Benefits of SSL Offloading*. Sectigostore.

Retrieved June 20, 2023, from

<https://sectigostore.com/blog/what-is-ssl-offloading-features-benefits-of-ssl-offloading/>

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.

“SQL Injection attack rule statement inspects for malicious SQL code. Attackers insert malicious SQL Code into web requests in order to do things like modify your database or extract data from it”.

SQL injection attack rule statement. (n.d.). AWS WAF, AWS Firewall Manager, and AWS Shield Advanced.

Retrieved June 20, 2023, from

<https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-sqli-match.html>

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, when the front door is enabled the WAF policy by default is in detection mode, you can change those settings to prevention. So if the front door is disabled, an SQL injection could go undetected, making the website vulnerable to attacks.

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, if You added the rule to block all traffic from Canada the IP address coming from Canada would not be able to access the website.

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

- a. Azure Front Door enabled

1-LessonPlan/14-Project-1/3 · m...

14.3 Protecting your App using...

My Drive - Google Drive...<Kiley Smith> Project 1 Technic...Azure Front Door - Micros...

portal.azure.com/#view/Microsoft_Azure_AFDX/WebAppIntegrationBlade/id/%2Fsubscriptions%2Fe12b2ac3-4374-41d9-86df-af4bb4cf7355%2FresourceGroups%2F...

Microsoft Azure


Upgrade

Search resources, services, and docs (G+)

Home > App Services > Kileysecurityblog | Networking >

Azure Front Door

Microsoft Azure



Azure Front Door

Azure Front Door is a modern cloud CDN service that provides high performance, scalability, and secure experiences for your content, files and global applications. It combines modern CDN technology and intelligent threat protection in a tightly integrated service that's easy to set up, deploy, and manage. Use Front Door with Azure services including App Service, Static Web App, Storage, API Management, Application Gateway, Azure Kubernetes Service, Azure Container Apps, and virtual machines—or combine it with on-premises services for hybrid deployments and smooth cloud migration. [Learn more](#)

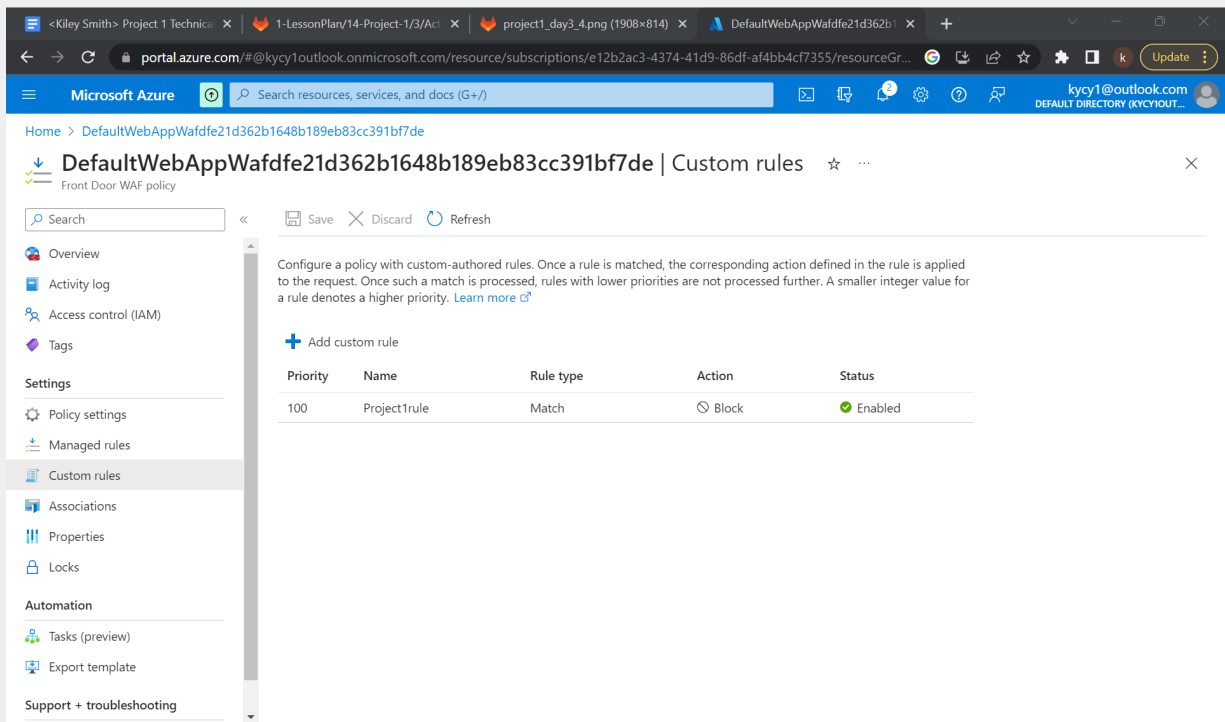
✔ Azure Front Door is enabled for your web app. Configure your Front Door at the link below. To remove Front Door from this web app, you must remove app service from the Front Door's origins or the classic Front Door's backend.

Name ↑↓	Type ↑↓	Endpoint name ↑↓	Origin group name ↑↓
project1-FrontDoor	Azure Front Door Premium	Project1-FD-a4bphzabhrb4h9dkz0...	Red-Team

Add

Close

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.

