



# Cybersecurity

## Project 1 Technical Brief

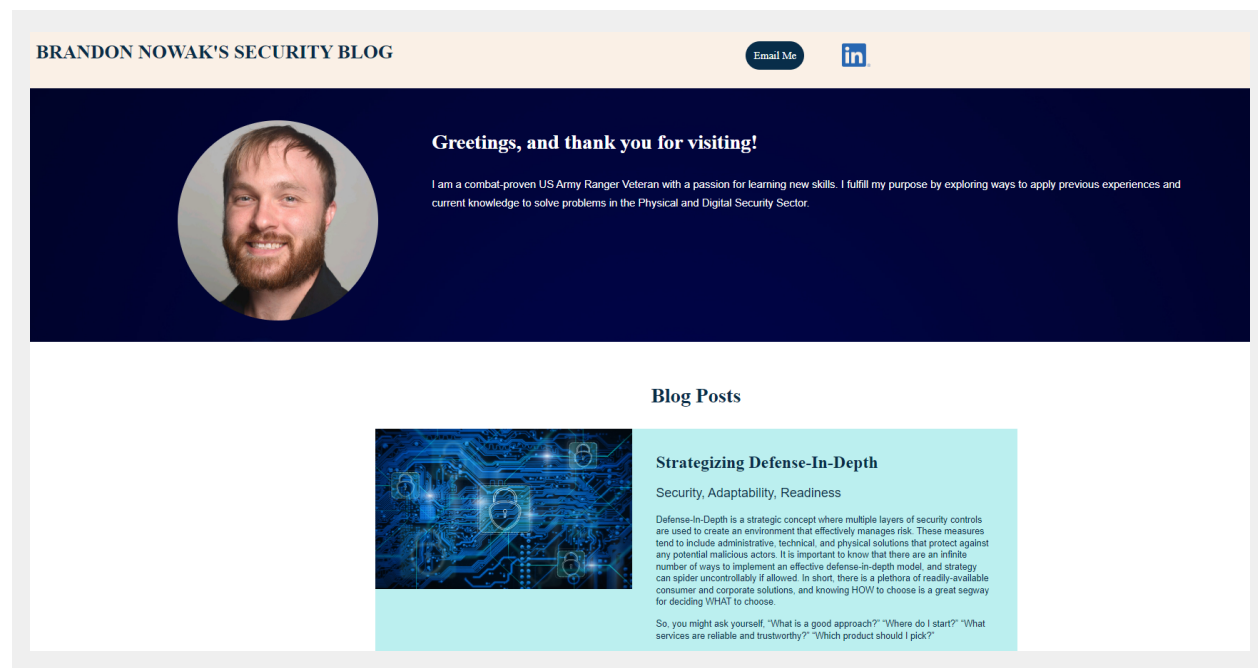
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

### Your Web Application

Enter the URL for the web application that you created:

<https://brandonmnowak.com/>

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



My advice in short form: Keep it simple, define your parameters, set your conditions, and execute your plan of action.

The Army teaches the dynamic concept of METT-TC, an acronym to help define the parameters of a specific mission plan, and stands for Mission, Enemy, Terrain and Weather, Troops Available, Time, and Civilian Considerations. This may sound daunting and overtly militarized, but consider how this applies to your digital footprint:

**Mission:**

Your mission may be something as simple as surfing the web without getting a virus or being blasted by targeted ads, or it can be as intricate as securing a multi-billion-dollar facility and its digital network. Regardless, start your approach by defining what your objective is.

**Enemy:**

Script kiddies, organized crime, nation-state intrusion actors, stalkers, spammers, hackers, unsolicited sales... the list goes on, and is exhausting to dwell on. So, WHO is your enemy, and HOW do they think?

Consider your cause, your mission, and your priorities. The entity that is hostile toward these concepts is most likely your "enemy." Consider making two lists to better understand what is important to you:

List # 1- What DO you care about?

List # 2- What DON'T you care about?

It is much easier to brainstorm how to defend against an enemy when you have clearly defined YOUR goals (since your enemy is defined as those entities in direct and hostile opposition). It is important to note that a Defense-In-Depth solution is an iterative process consistently improving on itself, so don't get burned out by trying to do too much at one time. I recommend ranking about five priorities for each list at a time.

**Terrain and Weather:**

In the Army this is largely in regards to what you wear and where you go. In cyberspace, this is a much broader concept that can be applied to all seven layers of the Open Systems Interconnection (OSI) model and how (1. Physical, 2. Data Link, 3. Network, 4. Transport, 5. Session, 6. Presentation, 7. Application).

**Troops Available:**

Who do you have to defend your domain? Are you the DIY type or do you like to hire a professional? Do you already have a security team? How about the built-in security options that are already included with your devices? "Troops" can imply physical and/or virtual assistance to a problem.

**Time:**

WHEN is the most inconvenient time for you to experience a compromise? Plan for this and have a predetermined course of action for when it happens. Ideally, this is rehearsed to ensure minimal downtime.

**Civilian Considerations:>**

Who else interacts with your on or offline presence? Do you share services with your colleagues or family? A breach may occur through the connection you share with a compromised friend- even if your system is secure. Segmentation is a great way to insulate against this potentiality.

**Final Thoughts:**

The METT-TC model is meant to be a tool for mission and contingency planning. It is an adaptable and flexible approach to problem-solving and system-building. This post is NOT a complete how-to guide; it is meant to get the wheels turning and consider a practical approach to building a layered defense model.



## Data Privacy as Preventative Security

### Minimizing Your Attackable Surface Area

When it comes to online privacy and data protection, there is a myriad of steps you can take to ensure your information remains secure and private. Initially, it is important to define your objectives and prioritize the steps for your personal or business security goals as discussed in my Strategizing Defense-In-Depth post.

At a baseline, you should ALWAYS use strong, unique passwords across all accounts (DO NOT RECYCLE PASSWORDS), incorporate multi-factor authentication (MFA) whenever possible, and regularly change your passwords. Most of these tasks can be accomplished with minimal effort and maximum trust while using a RELIABLE password manager- where your data is most protected from breaches and hackers. At the time of this writing, I prefer Bitwarden (online option) and KeePassXC (offline option) to secure my objective of password privacy and protection. Both options are open-source and accessible across all platforms, have basic and advanced options, can generate random passwords, maintain notes and financial information, and incorporate MFA.

It is important to consider minimizing alternate attack vectors in addition to hardening these basic security features. Simple, inexpensive solutions like shredding documents containing Personally Identifiable Information (PII) and adjusting the privacy settings on your social media accounts are common-sense ways of mitigating vulnerable surface areas. In addition, segmenting and fortifying your home Wi-Fi network and seeking out ways to encrypt your data in motion or at rest will help keep your sensitive data private and secure.

Again, there are an infinite number of ways to develop your security solutions further that we can talk about next time. Remember that the practice of privacy and security is a never-ending task. Keep it simple and stay involved!

## Day 1 Questions

### General Questions

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

GoDaddy domain

2. What is your domain name?

brandonmnowak.com

## Networking Questions

1. What is the IP address of your webpage?

20.119.0.23

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

Washington, Virginia, USA

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

```
C:\Users\Admin>nslookup brandonmnowak.com
Server:    UnKnown
Address:   10.2.0.1

Non-authoritative answer:
Name:      brandonmnowak.com
Address:   20.119.0.23
```

## 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 was the selected runtime stack. It 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 css files and images. Css files control the layout of web pages and describe how HTML elements are to be displayed. (css files included were: style.css, style.css.bak)  
(images files included were: Background.jpg, Image1.jpg, Image2.jpg, LinkedIn-logo.png, RobertSmith-profile.jpg readme)

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

Front End. HTML language is used for front end development and displays the visual aspects of a website.

## Day 2 Questions

### Cloud Questions

1. What is a cloud tenant?

A cloud tenant is the regional location that houses servers providing cloud services.

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

An access policy determines whether an application or user group can perform different operations with keys, secrets, and certificates. It is important to define access policies in order to secure access-control. Note that each key vault can have up to 1024 access policies.

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

Keys are asymmetric algorithms and may be either public or private. Secrets are anything that is sensitive that is not an asymmetric key or certificate such as 256-bit AES symmetric keys or an application token. Certificates on Azure are X.509 v3 and can be self-signed or signed by another trusted certificate, and contain the public key and bind a name to that key.

## Cryptography Questions

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

Advantages of a self-signed certificate are that they are fast, free, easy to use.

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

They are not signed by a reputable Certificate Authority (CA), and, therefore, browsers and operating systems do not trust them.

### 3. What is a wildcard certificate?

A wildcard certificate is a SSL/TLS certificate that includes a wildcard character (\*) in the domain name field and can secure multiple subdomains.

### 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 not provided due to a critical security flaw called Heartbleed that can allow adversaries to remotely compromise a server's private keys or execute code on hardware. This vulnerability is only applicable to SSL 3.0 and above.

### 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, because it is a self-signed certificate and my browser does not trust it. This error was fixed by binding the certificate.

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

01/05/2023 6:00:00 PM to 07/06/2023 6:59:59 PM Central Time

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

GTS CA 1P5 issued by GTS Root R1

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

\*.brandonmnowak.com issued by GTS CA 1P5

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.

GTS Root R1, issued by GlobalSign Root CA

## Day 3 Questions

### Cloud Security Questions

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

Azure Web Application Gateway and Azure Front Door have similar functionality but differ where the WAF is applied. Azure Web Application Gateway applies the WAF filters when it enters your VNET. Azure Front Door applies the WAF filters at edge locations.

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 a load balancer to transfer incoming encrypted traffic from a client in order to relieve the webserver from the encryption/decryption process. The load balancer is positioned between a browser and a webserver and uses the same SSL certificate that is issued to the webserver to complete this task. The benefit of SSL offloading is that encryption/decryption tasks take less time and make the backend work faster.

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.

SQL injection is one of the most common web application attacks and ranks #3 on the OWASP Top Ten. SQL injection is a code injection technique used to manipulate a database query into doing something that it would not normally do.

A WAF managed rule for SQL injection identifies and removes suspicious activity for HTTP GET and POST requests, and, as a result, denies malicious SQL code.

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?

No, my website has no database or login credentials presented from the web application. However, Front Door protects against SQL injection, so if my website contained a database it could be impacted by this vulnerability if Front Door was not enabled.

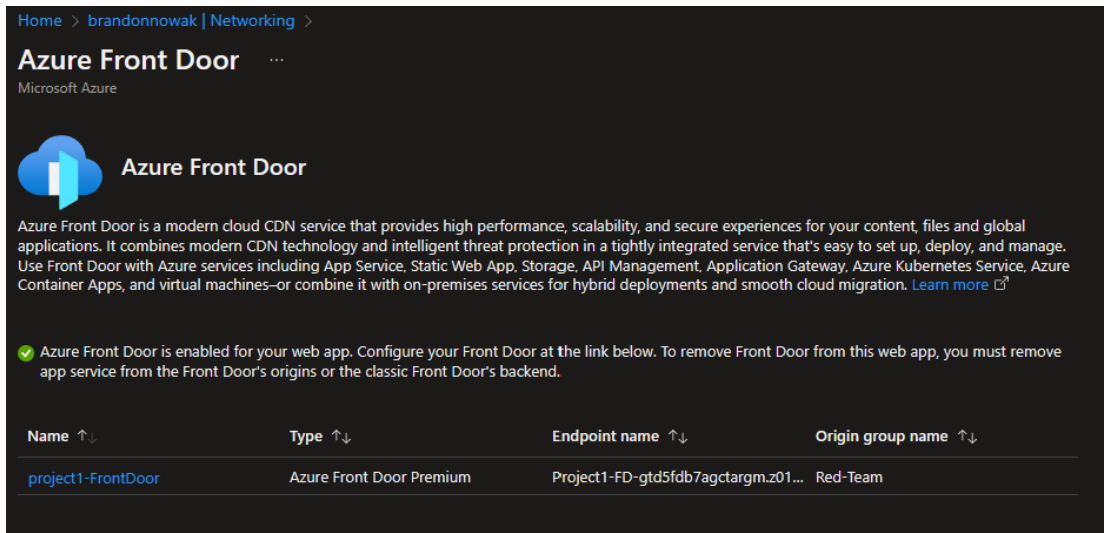


6. Hypothetically, say that you create a custom WAF rule to block all traffic from Canada. Does that mean that anyone who resides in Canada would not be able to access your website? Why or why not?

The custom WAF rule to block all traffic from Canada would only apply to users with a Canadian IP address. Hypothetically, anyone who lives in Canada could use a VPN to circumvent this rule. Conversely, if someone outside of Canada uses a VPN with a Canadian IP address, they would be blocked.

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

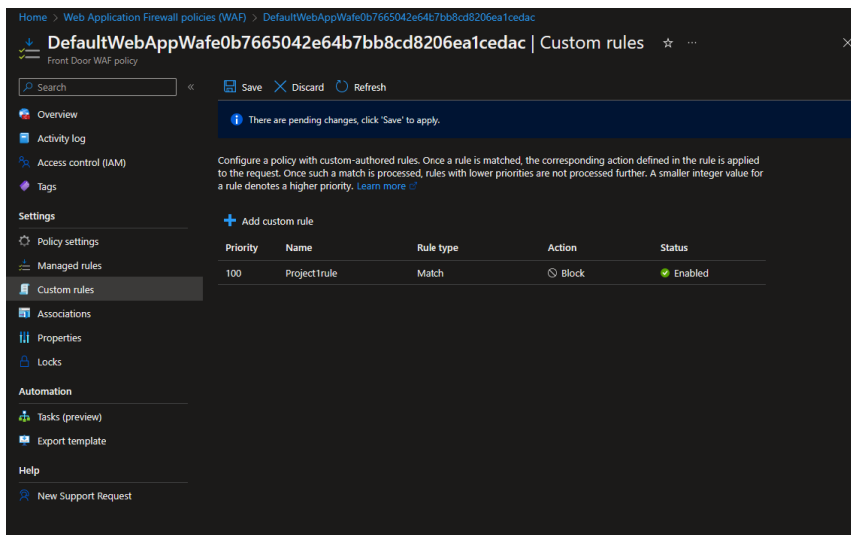
a. Azure Front Door enabled



The screenshot shows the Azure Front Door overview page. At the top, it says "Azure Front Door" and "Microsoft Azure". Below this, there is a description of the service. A green checkmark icon indicates that Azure Front Door is enabled for the web app. Below the text, there is a table with columns: Name, Type, Endpoint name, and Origin group name. The table contains one row with the following data:

Name	Type	Endpoint name	Origin group name
project1-FrontDoor	Azure Front Door Premium	Project1-FD-gtd5fdb7agctargm.z01...	Red-Team

b. A WAF custom rule



The screenshot shows the Azure WAF custom rules page. At the top, it says "DefaultWebAppWafe0b7665042e64b7bb8cd8206ea1cedac | Custom rules". Below this, there is a table with columns: Priority, Name, Rule type, Action, and Status. The table contains one row with the following data:

Priority	Name	Rule type	Action	Status
100	Project1rule	Match	Block	Enabled

## 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