

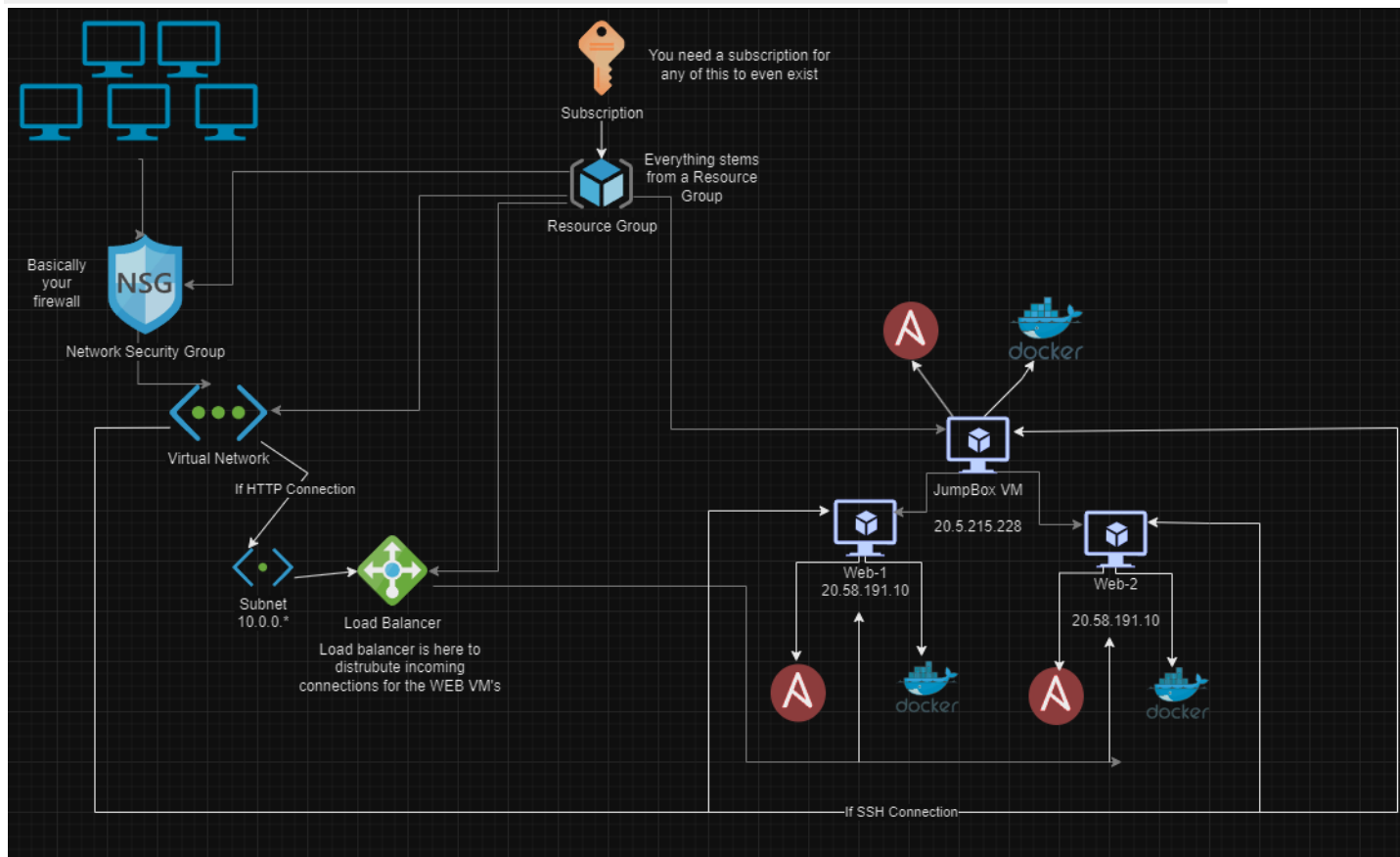


Cybersecurity

Project 1

Web Application

<https://joshsec.azurewebsites.net>





Hi, I'm Joshua!

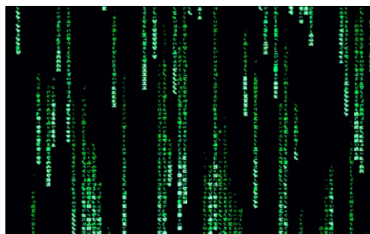
I am Joshua Purl, a dedicated and aspiring cybersecurity professional, eager to make a meaningful impact in the dynamic realm of cybersecurity. Having completed the cybersecurity bootcamp with The University of Sydney, I hold a certificate of completion that attests to my foundational knowledge and practical skills in the field. Furthermore, I have fortified my expertise by achieving the CompTIA Security+ certification, a testament to my commitment to maintaining the highest standards in information security. At the age of 20, I am driven by a passion for cybersecurity and a relentless pursuit of excellence.

Blog Posts



My Goals and Ambition

I consider myself an extremely ambitious individual. In the future im determined to persue senior roles in cloud security whilst also studying to attain my MBA (Masters of Buisness Administration). With these goals in mind i am aiming to take me next few steps towards furthering my career with haste.



My Passion for Offensive Security

Since the beggining of my professional journey ive been extremely interested in the red team and offensive security as a whole. From pwning black box's from vulnhub to capture the flag events and king of the hill. Ive continuously found new and interesting concepts to study and understand leading me to have knowledge of an array of different offensive security concepts.

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?

joshsec.azurewebsites.net

Networking Questions

1. What is the IP address of your webpage?

20.211.64.22

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?

Dns Timeout

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?

A runtime stack typically refers to the combination of technologies and frameworks used to run a web application. This includes both the front end (client-side) and the back end (server-side) components

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

Contains the Styles and `.css` files that are used for specifying things such as font size.

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

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

Cloud tenants are usually an individual or organization that makes use of cloud services to run their applications services off of instead of hosting themselves in order to make use of cloud services advantages such as ease of access, control, storage, monitoring ect.

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

Access policy is crucial in managing certificates, cryptographic keys and other secrets within the key vault.

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

Keys give access and act in similar sense to a password. Secrets are sensitive information and can be a number of things such as passwords, api keys, and connection strings. certificates are proof of authentication and or legitimacy.

Cryptography Questions

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

Self signed certificates provide proof that traffic will be encrypted.

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

The safety of the site is not guaranteed by an authority.

3. What is a wildcard certificate?

A wildcard certificate can be used for multiple subdomains and does not confine to a singular address.

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 significant vulnerabilities and can lead to a compromise of sensitive information as a result azure provides more modern solutions such as TLS 1.0, 1.1, 1.2

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 error is returned. The web application used is attached to the free azure wildcard SSL certificate. If it were a self signed certificate or had no certificate at all it would return an error.

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

1st of August - June 28th

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

No root certificate

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

Yes the website does have a root certificate. A root certificate is the highest level of certificate it represents the trust anchor for the entire certificate chain.

- 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.

Digicert global root

Day 3 Questions

Cloud Security Questions

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

The two main similarities are SSL termination and global load balancing.

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 a process in which runs encryption and decryption tasks from a dedicated hardware device.

3. What OSI layer does a WAF work on?

Application layer 7. WAF is used in order to protect web applications therefore placing it on this level.

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

SQL injections are a certain web application vulnerability where the attacker uses malicious code in the format of SQL to attack a database and to query and return information that shouldn't be accessible.

5. 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?


All regular traffic will be blocked however users using vpn's (virtual private networks) will be able to access the website due to the rule blocking connection only to ip's that identify with the blocked country.

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

- a. Azure Front Door enabled

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 web app 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-g3dpadeae4ahd6ej.z0...	Red-Team

- b. A WAF custom rule

Search <<

Save Discard Refresh

- Overview
- Activity log
- Access control (IAM)
- Tags
- Settings
 - Policy settings
 - Managed rules
 - Custom rules
 - Associations
 - Properties
 - Locks
- Automation
 - Tasks (preview)
 - Export template
- Help
 - Support + Troubleshooting

There are pending changes, click 'Save' to apply.

Configure a policy with custom-authored rules. Once a rule is matched, the corresponding action defined in the rule is applied to the request. Once such a match is processed, rules with lower priorities are not processed further. A smaller integer value for a rule denotes a higher priority. [Learn more](#)

+ Add custom rule

Priority	Name	Rule type	Action	Status
100	Projectrule1	Match	Block	Enabled

Edit custom rule

A custom rule is made up of one or more for a WAF policy are match rules. [Learn more](#)

Custom rule name *

Status

Rule type

Priority *

Conditions

If

Match type ☐

Geo location

Match variable

SocketAddr

Operation

☐ Is ☒ Is not

Country/Region *

3 selected