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://groesintcs.azurewebsites.net/
```

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

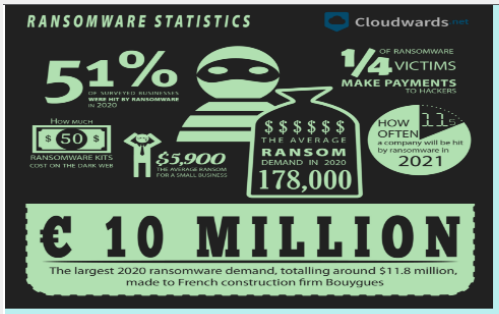
Black Hat ORC: Retail's New Cyberwar

Blackhat OrganizedCrime

Admittedly, I am no expert in Cybersecurity. A few months ago, my idea of what a Red Team vs Blue Team engagement could mean would be a football game between the Wisconsin Badgers and the Michigan Wolverines (Let's Go Bucky!). I too trudged through a few videos from my various jobs regarding the use of strong passwords, protection of personal/proprietary data, and locking your computer when you walk away. Don't write your password on a Post-It note and stick it to your monitor, got it!

I've spent most of my career in what I refer to as the "Law Enforcement Adjacent" sphere, mostly in the world of private sector security, with brief stints in law enforcement and corrections. I spent my time researching, tracking, catching, and dealing with "bad guys." I took my experience into a role in retail, investigating what has come to be known as Organized Retail Crime, where I still catch bad guys. I have just recently researched new opportunities in Cyber/InfoSec...

Organized Retail Crime (ORC) is an epidemic plaguing the U.S. from urban cities to small towns, with estimated losses to businesses of approx. $750,000 for every billion dollars in sales. ORC is estimated to be a greater than $50 Billion industry. Much of the money generated is being funneled into Organized Crime Syndicates, fueling things like the illicit drug trade, human trafficking, and underground, black markets of counterfeit goods. With lax sentencing protocols in many states, Organized Crime Syndicates see it as a low risk/high reward venture to gain capital. Just like in your 401(k), it pays for these criminals to diversify their portfolios...



Black Hat ORC PT 2: Eternity of MaaS-Ive Problems

BlackHat MaaS

This article is going to piggyback off of the idea of my first article, expanding upon the idea that Organized Crime Syndicates (specifically those involved in high-level retail theft) are broadening their horizons with the new technology that is available in this continuously digitizing world. The exposure of Organized Retail Crime as a trend, in media especially, has caused US States and the Federal Government to take legislative measures to address the problem of what have been dubbed "flash robberies" in the media. Communities, Chambers of Commerce, and Retailers have begun to notice and take action to protect their profits and their qualities of life, and Politicians are beginning to answer.

This forces the "bad guys" to pivot their tactics into one of two categories:

- A more "overt" approach, utilizing either "blitz" tactics (the overwhelming numbers of subjects and rapidness seen in the 'flash robbery' videos popular in the media), or using an increase in violence/robbery tactics to accomplish the same end through fear. The same evil Tickle-Me-Elmo, but with bigger horns and more of them...
- A "covert" approach utilizing more underground tactics that can be more out of the limelight approach that allows major actors to hide or use technology to stay off the

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?

```
https://groesintcs.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?

```
Australia East
```

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

```
The Groehlers@DESKTOP-BELCLER MINGW64 ~
$ nslookup type=NS https://groesintcs.azurewebsites.net
*** Can't find server address for 'https://groesintcs.azurewebsites.net':
Server:  rns01.charter.com
Address:  2607:f428:ffff:ffff::1
```

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?

```
PHP8.2 This works on the back end.
```

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

```
Assets are able to change color, background, and other attributes to the
website.
```

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

```
Front End Server
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
A cloud tenant is anyone that is signing up to use your web application as a
Software-as-a-Service environment. Tenant structures are divided into
single-tenant and multi-tenant, with single-tenant running a dedicated
infrastructure for a single app, and multi-tenant is a single cloud serving
multiple businesses.
```

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

```
An access policy is important to manage access to the key vault to limit
access to non-necessary users.
```

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

```
A key allows access to encrypted data (which is either asymmetric or
symmetric), a certificate is a verification mechanism to ensure website
integrity (either provided by a certificate service or self-signed), and a
secret is any piece of data (i.e. a password, a Kubernetes secret, or an
application token) that needs to be protected for application integrity.
```

Cryptography Questions

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

```
The advantages of a self-signed certificate are they are free to set up and
can set up pretty rapidly.
```

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

```
The disadvantages of a self-signed certificate are that most security
software will block websites using self-signed certificates and major search
engines will not index the website.
```

3. What is a wildcard certificate?

```
A wildcard certificate is a single certificate that is used across multiple
websites as a package.
```

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.

```
Azure does not allow SSL 3.0 due to a vulnerability in block cipher mode
padding that allows a POODLE (Padding Oracle On Downgraded Legacy
Encryption) attack to decrypt and extract data.
```

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, since using the Azure Free Domain generates a certificate from Azure.
```

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

```
The certificate is valid from Thursday, March 9, 2023 at 9:05:55 PM to Sunday, March 3, 2024 at 9:05:55 PM.
```

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

```
No, I do not have an intermediate certificate.
```

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

```
Yes, there is a root certificate (DigiCert Global Root G2).
```

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

```
Yes, DigiCert Global Root G2 is in the browser root store.
```

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

```
VeriSign Class 3 Public Primary Certification Authority - G5
```

Day 3 Questions

Cloud Security Questions

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

```
Both Azure Web Application Gateway and Azure Front Door operate on Layer 7 - Application of the OSI Model, their primary solution is as a load balancer, can incorporate web app firewalls, and have multiple additional features in common.

Whereas Web App Gateway is more regional, protecting a single region of the cloud, Azure Front Door is more global.
```

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 removing encryption from incoming traffic to a web server to free up space otherwise used to process decrypting the data via SSL. The advantage is a dedicated additional server is charged with decrypting and encrypting traffic, which adds another layer of protection against DNS-style DDoS attacks.
```

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.

```
Directory traversal allows attackers to read files on backend servers and operating systems, which could allow an attacker to change source code to alter behavior of the application (i.e. altering product images).
```

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?

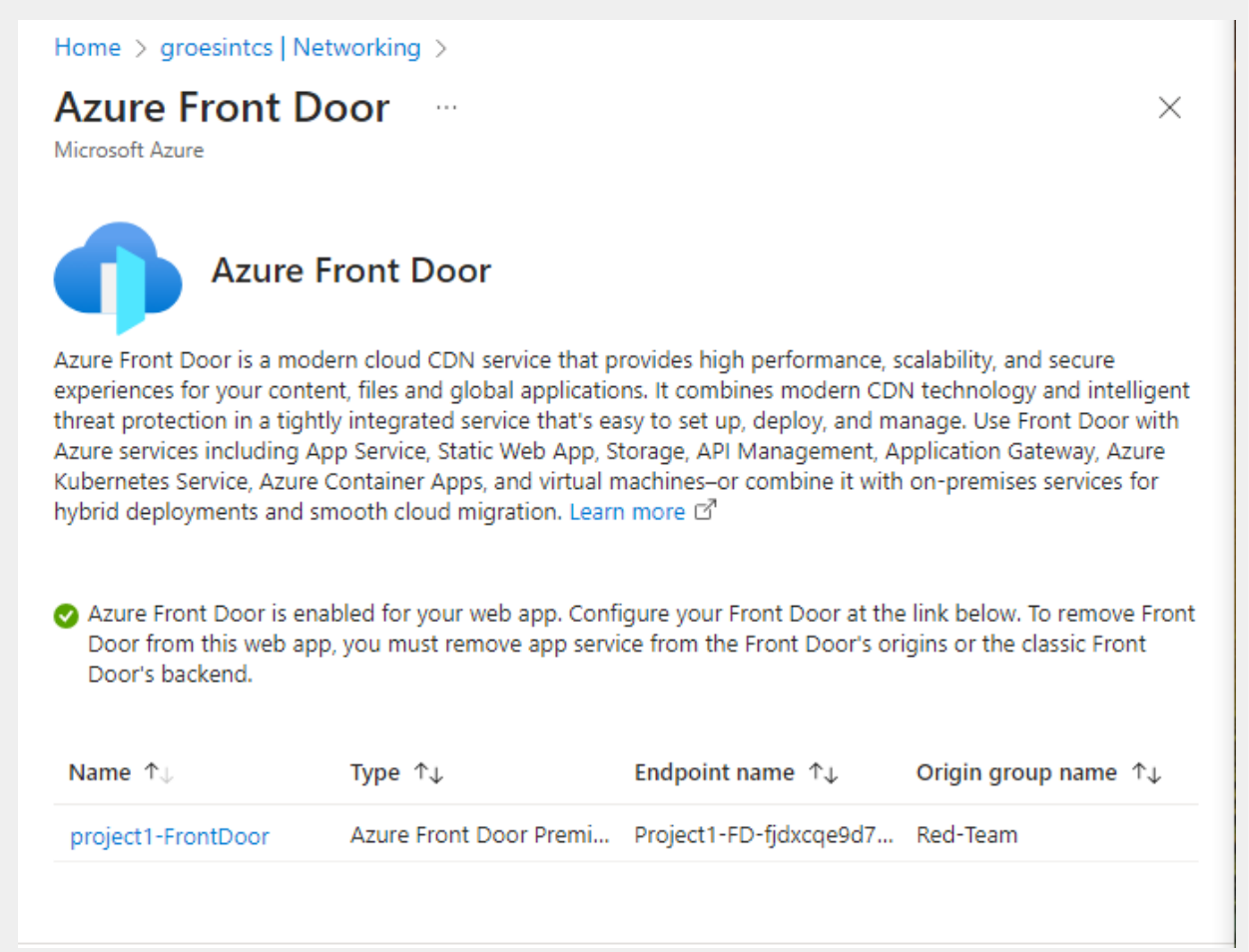
```
My application would be vulnerable to this style of attack, since images for the website are held in the HTML pathway with links out to GoogleDrive, which could be easily manipulated.
```

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?

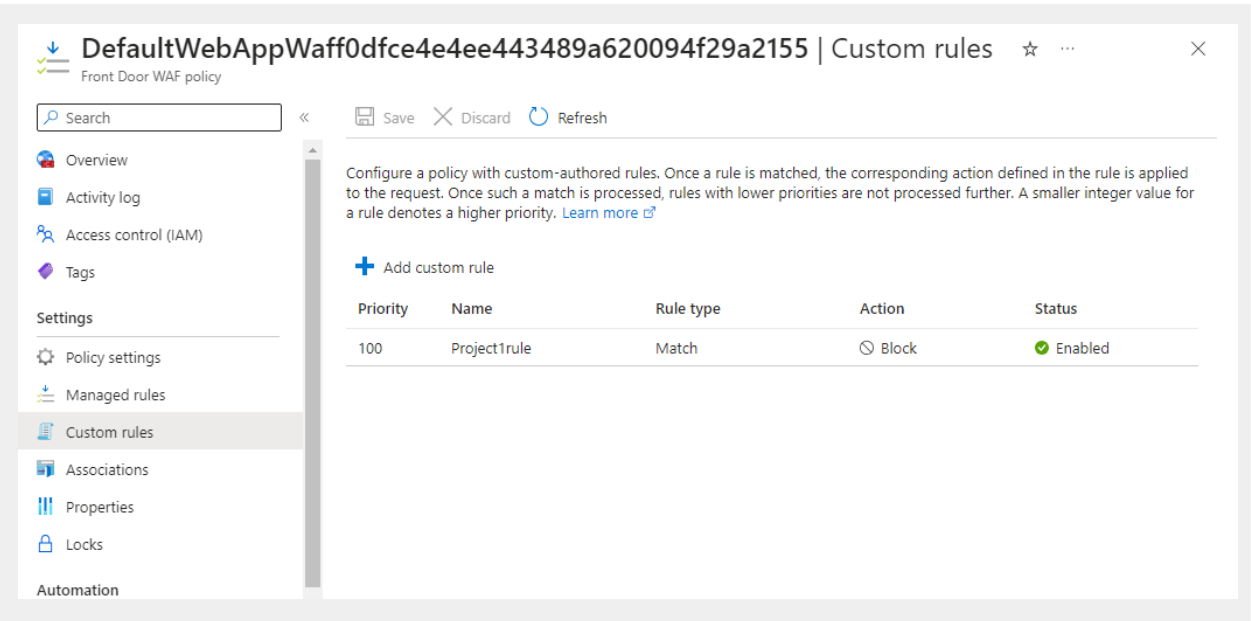
```
No, as users could still access the website via use of a VPN or through location spoofing by changing IP addresses.
```

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.*